1 The Integers

Theorem (Well-Ordering Principle)

Every nonempty set of non-negative integers contain a least element. $\exists a \in S : \forall b \in S, a \leq b$

Proof. Let S be a set of non-negative integers. Suppose S has no smallest element. Then, $0 \notin S$, because otherwise, 0 would be the smallest element. By induction, suppose $0, 1, \ldots, k \notin S$. Then, $k + 1 \notin S$ since otherwise, it would be the smallest element. Therefore, $S = \emptyset$. $\square$

Definition: Divides

Let $a, b \in \mathbb{Z}$. b **divides** a if $a = bc$ for some $c \in \mathbb{Z}$, written as $b \mid a$.

Proposition: Let $a, b \in \mathbb{Z}, a \neq 0$ such that $b \mid a$. Then $|b| \leq |a|$.

Proof. Let $a, b \in \mathbb{Z}$ such that $b \mid a$ and $a \neq 0$. Then there exists some $c \in \mathbb{Z}$ such that $a = bc$. Since $a \neq 0$, b, c are necessarily nonzero. Applying the absolute value to both sides of the equation, we get $|a| = |bc| = |b||c|$. Since $b, c \neq 0$, we have $|b|, |c| > 0$. Then $|b| \leq |b||c| = |bc| = |a|$, so $|b| \leq |a|$. $\square$

Theorem (Division Algorithm)

Let $a, b \in \mathbb{Z}$ such that $b > 0$. There exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < b$.

Proof. **Existence:** Let $a, b \in \mathbb{Z}, b > 0$. Consider the set $S = \{a - bx : x \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$. Consider $b = -|a|$. Then, $a - (-|a|)x \in S$. By the well-ordering principle, choose the smallest $a - bx \in S$ such that $q := x, r := a - bx$. Then, rearranging r and substituting q for x, we get $a = bq + r \in S$. By construction of S, $0 \leq r$. Suppose $r \geq b$. Then, $0 \leq r - b = (a - bx) - b = a - b(x - 1)$. This implies that $r - b < r$, a contradiction, since $r \in S$ was the least element by choice. Therefore, $0 \leq r < b$.

Uniqueness: Suppose we have $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that $a = bq_1 + r_1 = bq_2 + r_2$, where $0 \leq r_1, r_2 < b$. Then, we have

$$\begin{aligned}
bq_1 + r_1 &= bq_2 + r_2 \\
bq_1 + r_1 - (bq_2 + r_2) &= 0 \\
b(q_1 - q_2) + (r_1 - r_2) &= 0 \\
b(q_1 - q_2) &= -(r_1 - r_2) \\
b(q_1 - q_2) &= r_2 - r_1
\end{aligned}$$

Since $0 \leq r_1 < b$, we can rewrite the inequality to be $-b < -r_1 \leq 0$. Then, addint $0 \leq r_2 < b$ to the inequality, we get $-b < r_2 - r_1 < b$. Because $b \mid (r_2 - r_1)$, $(r_2 - r_1)$ must be a multiple of b, but since $-b < r_2 - r_1 < b$, we have that $(r_2 - r_1) = 0b = 0$. Then, $b(q_1 - q_2) = r_2 - r_1 = 0$. This implies that $q_1 = q_2$ and $r_1 = r_2$. Therefore, $q_1, r_1 \in \mathbb{Z}$ are unique. $\square$

Definition: Greatest Common Divisor (gcd)

Let $a, b \in \mathbb{Z}$ and either $a \neq 0$ or $b \neq 0$, but not both. The **greatest common divisor** of a and b is the largest integer dividing a and b. We write $\gcd(a, b)$ or (a, b).

$(a, b) \mid a$ and $(a, b) \mid b$. Further, if $c > 0$ divides a and b, then $0 < c \leq (a, b)$.

Theorem (Bezout's Identity)

Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$, but not both. Suppose $d = (a, b)$. We can find $x, y \in \mathbb{Z}$ such that $ax + by = d$.

Proof. Let $d = (a, b)$. Consider the set $S = \{ax+by : x, y \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$. Consider $x = a, y = b$. Then $ax + by = a^2 + b^2 \geq 0 \in S$, so S is not empty. By the well-ordering principle, choose the least element $s = ax + by \in S$ and consider $a = sq + r$ where $0 \leq r < s$. Rearranging the second equation, we get

$$\begin{aligned} a &= sq + r \\ r &= a - sq \\ &= a - (ax + by)q \\ r &= a(1 - x) + b(-yq) \end{aligned}$$

This implies that $r \in S$ since $0 \leq r$ by definition. We also have that $r < s$, but since s was chosen to be the smallest element in S, this forces $r = 0$. Then, $a = sq + r = sq$, so $s \mid a$. Similarly, $b = st$ for some $t \in \mathbb{Z}$, so $s \mid b$. Since $s \mid a$ and $s \mid b$, $s \leq d$. But $d \mid a$ and $d \mid b$ by definition, so $d \mid s$ which implies that $d \leq s$. Therefore, $d = s = ax + by$. $\square$

Theorem

Let $a, b \in \mathbb{Z}$ and suppose $a \mid bc$ and $(a, b) = 1$. Then $a \mid c$.

Proof. Because $(a, b) = 1$, we can write $1 = ax + by$. Also, since $a \mid bc$, there exists some $z \in \mathbb{Z}$ such that $bc = az$. Then

$$\begin{aligned} c &= cax + cby \\ &= a(cx) + (bc)y \\ &= a(cx) + a(zy) \\ c &= a(cx + zy) \end{aligned}$$

Therefore, $a \mid c$. $\square$

Corollary

Let $a, b, c \in \mathbb{Z}$ and $(a, b) = 1$. If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Proof. Since $(a, b) = 1$, we have $ax + by = 1$. By definition, since $a \mid c$ and $b \mid c$, there exist $n, m \in \mathbb{Z}$ such that $c = na$ and $c = mb$. Then, we have

$$\begin{aligned}
1 &= ax + by \\
c &= cax + cby \\
&= (bm)ax + (an)by \\
&= (ba)mx + (ab)ny \\
c &= ab(mx + ny)
\end{aligned}$$

so $ab \mid c$. $\square$

1.1 Prime Numbers

Definition: Prime

A nonzero non-unit integer p is **prime** if its only divisors are $\pm 1, \pm p$.

Theorem

Let $p \in \mathbb{Z} \setminus \{0, \pm 1\}$. The following statements are equivalent.

(1) p is prime.

(2) If $p \mid bc$, then $p \mid b$ or $p \mid c$ where $b, c \in \mathbb{Z}$.

Proof. (1) $\implies$ (2) Suppose p is prime and $p \mid bc$. If $p \mid b$, we are done, so suppose $p \nmid b$. Then, $(p, b) = 1$, so we have

$$\begin{aligned}
1 &= px + by \\
c &= cpx + cby \\
&= p(cx) + (bc)y \\
&= p(cx) + (pn)y && p \mid bc \implies bc = pn, n \in \mathbb{Z} \\
&= p(cx) + p(ny) \\
c &= p(cx + ny)
\end{aligned}$$

so $p \mid c$.

(2) $\implies$ (1) To prove the reverse implication, suppose the contrapositive: "If p is not prime, then there exist some $b, c \in \mathbb{Z}$ such that $p \mid bc$ but $p \nmid b$ and $p \nmid c$". Suppose $p \in \mathbb{Z} \setminus \{0, \pm 1\}$ is not prime; i.e. p is composite. Then, p can be written as its unique factorization $q_1 q_2 \cdots q_n$ where $n \geq 2$ and each q_i is prime. Choose $b = q_1$ and $c = q_2 \cdots q_n$. Then $p \mid bc$ because $bc = p$ and $p \mid p$, but $p \nmid b$ and $p \nmid c$ because $|p| > |b|$ and $|p| > |c|$ respectively. $\square$

Theorem

Let $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. n can be written as a product of primes.

Proof. Consider $n > 1$. Let S be the set of positive integers greater than 1 that cannot be written as a product of primes. Suppose for the sake of contradiction that S is nonempty. Then by the well-ordering principle, we can choose a least element $m \in S$. By definition, m is not prime or a product of primes. Because m is not prime, we can find some divisor $a \in \mathbb{Z}$ such that $a \neq \pm 1, \pm m$; i.e. we can find such an a such that $a \mid m$. Then, we can write $m = ab$ for some $b \in \mathbb{Z}$. By definition, $|a| \leq |m|$ and $|b| \leq |m|$. Without loss of generality, assume $a, b > 0$. Note that $b \neq 1$ since otherwise, $a = m$. So, $1 < a, b < m$ and $a, b \notin S$. Because $a, b \notin S$, they are either prime or products of primes. But $m = a \cdot b$, so m is a product of primes, a contradiction. Therefore, $S = \emptyset$, so n can be written as a product of primes. $\square$

Theorem (Fundamental Theorem of Arithmetic

Let $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Suppose $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ where each p_i, q_j is prime. Then,

(1) $r = s$.

(2) There is a unique permutation σ on $\{1, \ldots, r\}$ such that $p_i = \pm q_{\sigma(i)}$.

Proof. Let $n \in \mathbb{Z} \setminus \{0, 1\}$. Without loss of generality, suppose n is positive and $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ where each p_i, q_j is prime. Then $p_1 \mid q_1 \cdots q_s$. In particular, $p_1 \mid q_j$ for some $j \leq s$. Because q_j is prime, we necessarily have that $q_j = |p_1|$. Without loss of generality reindex $j = 1$ to get $q_1 = |p_1|$. Then, $p_1 \cdot (p_2 \cdots p_r) = p_1 \cdot (q_2 \cdots q_s) \implies p_2 \cdots p_r = q_2 \cdots q_s$. By induction, we have that $p_r = q_r$. If $r < s$, by the above, we have that $1 = q_{r+1} \cdots q_s$, which implies $q_j = 1$ for each j. A similar argument is said for $s < r$. In either case, we have a contradiction. Therefore, $r = s$ and there is a unique permutation σ on $\{1, \ldots, r\}$ such that $p_i = q_{\sigma(i)}$. $\square$

1.2 Modular Arithmetic

Definition: Well-Defined Functions

A function $f : X \to Y$ is **well-defined** if, for all $a, b \in X$, we have $f(a) = f(b)$ whenever $a = b$.

Pick $m \in \mathbb{Z}$ to be nonzero. The **Division Algorithm** says that for any $a, b \in \mathbb{Z}$, we can write $a = q_1 m + r_1, b = q_2 m + r_2$ for unique $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ where $0 \leq r_1, r_2 < |m|$.

Definition: Modulo

Define a relation R_m on $\mathbb{Z}$ by saying $(a, b) \in R_m$ if and only if $r_1 = r_2$ (alternatively written as $a \sim b$ if and only if $r_1 = r_2$). We write this as $a \equiv b \pmod{m}$.

Proposition: For any $m \in \mathbb{Z}$ nonzero, R_m is an equivalence relation.

Proof. Let R_m be the relation defined above for $m \in \mathbb{Z}$ nonzero.

(1) For any $a \in \mathbb{Z}$, write $a = bq + r$. Then, since $r = r$, $a \equiv a \pmod{m}$, R_m is reflexive.

(2) Take $a, b \in \mathbb{Z}$ and assume $a \equiv b \pmod{m}$. By the division algorithm, we can write $a = q_1 m + r_1, b = q_2 m + r_2$. By assumption, $a \equiv b \pmod{m}$, so $r_1 = r_2$. Since equality is symmetric, $r_1 = r_2 \iff r_2 = r_1$, so $b \equiv a \pmod{m}$. R_m is symmetric.

(3) Pick $a, b, c \in \mathbb{Z}$ and assume $a \equiv b \pmod{m}, b \equiv c \pmod{m}$. By the division algorithm, we can write $a = q_1 m + r_1, b = q_2 m + r_2, c = q_3 m + r_3$. By assumption, $r_1 = r_2$ and $r_2 = r_3$. Since equality is transitive, $r_1 = r_2, r_2 = r_3 \implies r_1 = r_3$, so $a \equiv c \pmod{m}$. R_m is transitive.

Since R_m satisfies $(1) - (3)$, R_m is an equivalence relation. □

Definition: Equivalence Class

If R is an equivalence relation on a set S, then S can be written as the union of equivalence classes. The **equivalence class** of x is the set $[x] := \{y \in S : (x, y) \in R\}$.

Note: The equivalence classes of R_m are $[0], [1], \ldots, [m-1]$.

Definition: Equivalence Relation

A relation R on a set S is any subset of $S \times S$. An ***equivalence relation*** is a relation with the following properties:

1. Reflexivity: For any $a \in S$, $(a, a) \in R$ (alternatively written as $a \sim a$).
2. Symmetry: For any $(a, b) \in S \times S$, $(a, b) \in R$ implies $(b, a) \in R$ (alternatively written as $a \sim b \implies b \sim a$).
3. Transitivity: For any $a, b, c \in S$, if $(a, b), (b, c) \in R$, then $(a, c) \in R$ (alternatively written as $a \sim b, b \sim c \implies a \sim c$).

Definition: Congruent Modulo n

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}$ be positive. We say a and b are **congruent modulo** n if $n|(a-b)$, written as $a \equiv b \pmod{n}$.

The **integers modulo** n is the set of equivalence classes modulo n, written as $\mathbb{Z}/n, \mathbb{Z}_n, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/(n)$.

Definition: Operations on $\mathbb{Z}/n$

Let $n \in \mathbb{Z}$ and $[a], [b] \in \mathbb{Z}/n$. Define

- → $[a] + [b] = [a+b]$
- → $[a][b] = [ab]$
- → For $k \geq 0$, $[a]^k = [a^k]$

Proposition: The operations above are well-defined.

Proof. Let $n \in \mathbb{Z}$ and $[a], [a'], [b], [b'] \in \mathbb{Z}/n$ where $[a] = [a'], [b] = [b']$. Then ($[a] = [a']$ and $[b] = [b']$ implies $n \mid (a - a')$ and $n \mid (b - b')$, so $n \mid (a - a') + (b - b') = (a + b) - (a' + b')$. Therefore, $[a + b] = [a' + b']$. Similarly,

$$\begin{aligned} ab - a'b' &= ab + 0 - a'b' \\ &= ab + (-ab' + ab') - a'b' \\ &= (ab - ab') + (ab' - a'b') \\ ab - a'b' &= a(b - b') + b'(a - a') \end{aligned}$$

Since $n \mid (a - a')$ and $n \mid (b - b')$, $n \mid ab - a'b'$, so $[ab] = [a'b']$. □

Proposition: Let $[a], [b], [c] \in \mathbb{Z}/n$. Then the following properties hold:

(1) $[a] + [b] = [b] + [a]$

(2) $[a] + ([b] + [c]) = ([a] + [b]) + [c]$

(3) $[a] + [0] = [a]$

(4) There exists $x \in \mathbb{Z}$ such that $[a] + x = [0]$

(5) $[a][b] = [b][a]$

(6) $[a]([b][c]) = ([a][b])[c]$

(7) $[a][1] = [a]$

(8) $[a]([b] + [c]) = [a][b] + [a][c]$

Proof. Let $[a], [b], [c] \in \mathbb{Z}/n$. Then the following properties hold:

(1) $\underline{[a]+[b]} = [a+b] = [b+a] = \underline{[b]+[a]}$

(2) $\underline{[a]+([b]+[c])} = [a]+[b+c] = [a+b+c] = [a+b]+[c] = \underline{([a]+[b])+[c]}$

(3) $\underline{[a]+[0]} = [a+0] = \underline{[a]}$

(4) Take $x \in \mathbb{Z}$ such that $x = n - a$. Then, $\underline{[a]+x} = [a]+[n-a] = [a-n-a] = [n] = \underline{[0]}$.

(5) $\underline{[a][b]} = [ab] = [ba] = \underline{[b][a]}$

(6) $\underline{[a]([b][c])} = [a][bc] = [abc] = [ab][c] = \underline{([a][b])[c]}$

(7) $\underline{[a][1]} = [a \cdot 1] = [a]$

(8) $\underline{[a]([b]+[c])} = [a][b+c] = [a \cdot (b+c)] = [ab+ac] = [ab]+ac] = \underline{[a][b]+[a][c]}$

$\square$

Definition: Unit and Inverse

Let $n > 1$ be an integer. Consider $[a] \in \mathbb{Z}/n$. If there exists $[b] \in \mathbb{Z}/n$ such that $[a][b] = [1]$, then we say $[a]$ is a **unit** and $[b]$ is the **inverse** of $[a]$, written as $[a]^{-1}$.

Theorem

Let $p > 1$ be an integer. The following statements are equivalent:

(1) p is prime.

(2) Each nonzero $[a] \in \mathbb{Z}/p$ has an inverse.

(3) If $[ab] = [0]$, then either $[a] = [0]$ or $[b] = [0]$

Proof. Let $p > 1$ be an integer.
(1) $\implies$ (2) Take $[a] \in \mathbb{Z}/p$ to be nonzero. Then $p \nmid a$ since p is prime. That is, $(p, a) = 1$. Then $px + ay = 1$, or $[1] = [px + ay] = [px] + [ay]$. But $[px] = [p][x] = [0][x] = [0] \in \mathbb{Z}/p$, so $[1] = [0] + [ay] = [ay] = [a][y]$. Then, $[y]$ is the inverse of $[a]$. Since $[a]$ was arbitrary, this holds for all $[a] \in \mathbb{Z}/p$.

(2) $\implies$ (3) Let $[a], [b] \in \mathbb{Z}/p$ and suppose $[ab] = [0]$. If $[a] = 0$, we are done, so suppose $[a] \neq 0$. Then, $[a]$ has an inverse, so $[a]^{-1}[ab] = [a]^{-1}[a][b] = [1][b] = [b] = [0]$. Therefore, either $[a] = [0]$ or $[b] = [0]$.

(3) $\implies$ (1) Suppose for the sake of contradiction that p is not prime; i.e. p is composite. Then we can find a divisor $a > 0$ such that $a \neq \pm 1, \pm p$. That is, $|1| < a < |p|$. Let $p = ab$. Then $1 < a, b < p$, but $[ab] = [p] = [0]$, a contradiction. $\square$

Theorem

Let $n > 1$ be an integer and $[a] \in \mathbb{Z}/n$. Then $[a]$ has a multiplicative inverse if and only if $(a, n) = 1$.

Proof. ($\implies$) Suppose $[a]$ has a multiplicative inverse. Then there exists $[x] \in \mathbb{Z}/n$ such that $[a][x] = [1]$. Then

$$\begin{aligned}
[1] &= [a][x] \\
&= [ax] + [0] \\
&= [ax] + [ny] && [ny] = [0] \in \mathbb{Z}/n, y \in \mathbb{Z} \\
[1] &= [ax + ny]
\end{aligned}$$

so $(a, n) = 1$.

($\impliedby$) Suppose $(a, n) = 1$. Then $ax + ny = 1$ for some $x, y \in \mathbb{Z}$, but $[ny] = [0] \in \mathbb{Z}/p$, so $[ax] = [a][x] = [1]$, where $[x]$ is the multiplicative inverse of $[a]$. $\square$

Theorem Chinese Remainder Theorem

Let $m, n \in \mathbb{Z}$ be coprime and positive. Let $a, b \in \mathbb{Z}$. We can find $x \in \mathbb{Z}$ such that

$$\begin{aligned}
x &\equiv a \pmod{m} \\
x &\equiv b \pmod{n}
\end{aligned}$$

Moreover, if y is another solution, then $y \equiv x \pmod{mn}$.

Proof. Let $m, n \in \mathbb{Z}$ such that $(n, m) = 1$. Then we can write $na + mb = 1$ for some $a, b \in \mathbb{Z}$. Set $x := c(na) + d(mb)$. Then

$$\begin{aligned}
[x]_m &= [cna]_m + [dmb]_m \\
&= [n(cn)]_m + [m(db)]_m \\
&= [a(cn)]_m + [0] && [m(db)]_m = [0] \in \mathbb{Z}/m \\
[x]_m &= [a]_m
\end{aligned}$$

so $[x]_m = [a]_m$. Similarly, $[x]_n = [b]_n$. So we have

$$\begin{aligned}
x &\equiv a \pmod{m} \\
x &\equiv b \pmod{n}
\end{aligned}$$

Let y be another solution. Then $[y]_m = [x]_m$ so $m \mid y - x$. Similarly, $n \mid y - x$. But since $(n, m) = 1$, we have that $mn|y - x$, or $[y]_{mn} = [x]_{mn}$. So $y \equiv x \pmod{mn}$. $\square$

Theorem Chinese Remainder Theorem (General)

Let $m_1, \ldots, m_n \in \mathbb{Z}$ be positive and pairwise relatively prime (i.e., $(m_i, m_j) = 1$ when $i \neq j$). Let $a_1, \ldots, a_n \in \mathbb{Z}$. We can find x such that

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Moreover, if y is another solution, then $y \equiv x \mod m_1 m_2 \cdots m_n$

Proof. We will induct on $n \in \mathbb{N}$.
Base case: At $n = 2$, we have $m_1, m_2 \in \mathbb{Z}$ where $(m_1, m_2) = 1$. Then, we can find $p, q \in \mathbb{Z}$ such that $m_1 p + m_2 q = 1$. Then, because $m_2 q \equiv 0 \pmod{m_2}$, we have $m_1 \equiv 1 \pmod{m_2}$. Similarly, $m_2 \equiv 1 \pmod{m_1}$. Consider $x = (m_2 q)r + (m_1 p)s$ for $r, s \in \mathbb{Z}$. Then, since $(m_2 q)r \equiv 0 \pmod{m_2}$, we have $x \equiv (m_1 p)s \equiv s \pmod{m_2}$. Similarly, $x \equiv (m_2 q)r \equiv r \pmod{m_1}$. So, $x \equiv r \pmod{m_1}$ and $x \equiv s \pmod{m_2}$. Now suppose y is another solution. Then, we have $y \equiv x \pmod{m}$, which implies that $m_1 | (y - x)$ and similarly, $m_2 | (y - x)$. Then because $(m_1, m_2) = 1$, we have that $m_1 m_2 | (y - x)$, so $y \equiv x \pmod{m_1 m_2}$.

Inductive step: At $n = n + 1$, we have $m_1, m_2 \in \mathbb{Z}$ where $(m_1, m_2) = 1$. Then by the inductive hypothesis, we have a set of n pairwise coprime integers $m_1, \cdots, m_n$ where $x' \equiv a_i \pmod{m_i}$ for each $i = 1, \cdots, n$. Define $M = \prod_{i=1}^{n} m_i$ and consider $x = x' + sM$ for some $s \in \mathbb{Z}$. Then since $m_i | M$ implies $sM \equiv 0 \pmod{m_i}$ and from the inductive hypothesis, $x' \equiv a_i \pmod{m_i}$, we have $x \equiv x' + sM \equiv x' \equiv a_i \pmod{m_i}$ for $i = 1, \cdots, n$. At m_{n+1}, because $m_{n+1} \nmid M$, we can choose an $s \in \mathbb{Z}$ such that $x \equiv x' + sM \equiv a_{n+1} \pmod{m_{n+1}}$. Now suppose y is another solution. Then $y \equiv x' \pmod{M}$ and $y \equiv a_{n+1} \pmod{m_{n+1}}$. Since $(M, m_{n+1}) = 1$, by the inductive hypothesis, we have that $y \equiv x \pmod{M m_{n+1}}$, so $y \equiv x \pmod{m_1 m_2 \cdots m_{n+1}}$. $\square$

2 Rings

Definition: Ring

A **ring** R is a nonempty subset with two operations, addition $(+)$ and multiplication $(\cdot)$ such that, for all $a, b, c \in R$, the following properties hold:

(1) $a + b \in R$

(2) $a + (b + c) = (a + b) + c$

(3) $a + b = b + a$

(4) There exists $0 \in R$ such that $0 + a = a + 0 = a$ for all $a \in R$.

(5) For all $a \in R$, there exists $-a$ such that $(-a) + a = a + (-a) = 0$.

(6) $a \cdot b \in R$

(7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(8) $a \cdot (b + c) = a \cdot b + a \cdot c$

(9)* There exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

*A set satisfying (1) - (8) is called a **nonunital ring**. If the set also satisfies (9), it is called a **unital ring**.

→ A ring is **commutative** if, for all $a, b \in R$, $a \cdot b = b \cdot a$.

→ An element $a \in R$ is a **zero divisor** if there exists a nonzero $b \in R$ such that $a \cdot b = 0$ or $b \cdot a = 0$.

→ An element $a \in R$ is a **unit** if there exists $b \in R$ such that $a \cdot b = b \cdot a = 1$, and is called the *inverse* of a, written as a^{-1}.

Proposition: Let $n > 1$, $a \in \mathbb{Z}$. If $(a, n) = 1$, $[a]$ is a unit. Otherwise, it is a zero divisor.

Proof. Let $n > 1$ and $a \in \mathbb{Z}$. There are two cases.

Case i $(a, n) = 1$. Then $ax + ny = 1$ so $[ax] = [a][x] = [1]$ where $[x]$ is the inverse of $[a]$, so $[a]$ is a unit.

Case ii $(a, n) \neq 1$. Then $(a, n) = d$ for $d > 1$. Then, $ax + ny = d$ so $[ax] = [d]$. Since $d|n$, $n = dm$ for some $m \in \mathbb{Z}$. Then since $[d] = [dm] = [0]$, we get $[ax] = [a][x] = [0]$, where $[x]$ is nonzero, so $[a]$ is a zero divisor.

□

Proposition: Let R be a ring and $a, b, c \in R$. The following hold:

(1) The additive identity is unique.

(2) An additive inverse is unique.

(3) If $a + b = a + c$, then $b = c$.

(4) The multiplicative identity is unique.

(5) If a is a unit, then its inverse is unique.

(6) $0 \cdot a = a \cdot 0 = 0$

(7) $(a)(-b) = -ab = (-a)(b)$

(8) $-(-a) = a$

(9) $-(a + b) = -a - b$

(10) $-(a - b) = -a + b$

(11) $(-a)(-b) = ab$

Proof. Let R be a ring. Then

(1) Let $0, 0' \in R$ be two additive identities. Then $\underline{0} = 0 \cdot 0' = 0' \cdot 0 = \underline{0'}$.

(2) Let $a \in R$ have two additive inverses $b, c \in R$. Then
$\underline{b} = 0 + b = (c + a) + b = c + (a + b) = c + 0 = \underline{c}$.

(3) Let $a + b = a + c$. Then $(-a + a) + b = (-a + a) + c \to 0 + b = 0 + c \to b = c$.

(4) $1, 1' \in R$ be two multiplicative identities. Then $\underline{1} = 1 \cdot 1' = 1' \cdot 1 = \underline{1'}$.

(5) Let $a \in R$ be a unit with two multiplicative inverses $b, c \in R$. Then
$\underline{b} = b \cdot 1 = b \cdot (ac) = (ba) \cdot c = 1 \cdot c = \underline{c}$.

(6) Let $a \in R$. Then $0 = (a + a) \cdot 0 = a0 + a0 = a0$. Similarly, $0 = 0a$.

(7) Let $a, b \in R$. Then $a0 = a(b + (-b)) = ab + (a)(-b) \implies (a)(-b) = -ab$. Similarly, $(-a)(b) = -ab$.

(8) Let $a \in R$. Then
$\underline{-(-a)} = 0 - (-a) = (a + (-a)) + (-(-a)) = a + ((-a) - (-a)) = a + 0 = \underline{a}$.

(9) Let $a, b \in R$. Then

$$\begin{aligned}
-(a+b) &= 0 - (a+b)) \\
&= 0 + 0 - (a+b)) \\
&= (a-a) + (-b+b) - (a+b) \\
&= a + (-a-b) + b - (a+b) && a - b = a + (-b) \\
&= (-a-b) + (a+b) - (a+b) \\
&= (-a-b) + 0 \\
-(a+b) &= -a - b
\end{aligned}$$

(10) Let $a, b \in R$. Then $\underline{-(a-b)} = -(a+(-b)) = -a-(-b) = \underline{-a+b}$.

(11) Let $a, b \in R$. Then $\underline{(-a)(-b)} = a(-(-b)) = \underline{ab}$.

□

2.1 Subrings

Definition: Subring

Let R be a ring. A **subring** $S \subseteq R$ is a subset such that S forms a ring with the same operations and same identities as R. If S forms a nonunital ring with the same operations or forms a ring but $1_s \neq 1_R$, S is a **nonunital subring**.

Let R be a ring. $S \subseteq R$ is a subring of R if and only if it satisfies the following:

(1) $1_R \in S$

(2) S is closed under addition.

(3) S is closed under multiplication.

(4) If $a \in S$, then $-a \in S$.

Definition: Integral Domain

A commutative ring R is an **integral domain** if it has no nonzer zero divisors. That is, if $a, b \in R$ and $ab = 0$, then $a = 0$ or $b = 0$.

Proposition: Let R be an integral domain and $a, b, c \in R$. If $ac = bc$ for $c \neq 0$, then $a = b$.

Proof. Suppose $ac = bc$. Then $ac - bc = 0 \to (a-b)c = 0$. because R is an integral domain, $(a-b) = 0$ or $c = 0$. But since $c \neq 0$ by assumption, $(a-b) = 0$ which implies that $a = b$. □

Definition: Field

Let R be a commutative ring. If all nonzero elements of R are units, R is a field.

Proposition: Every field is an integral domain.

Proof. Let R be a field. Since all nonzero elements of R are units, they cannot be zero divisors. $\square$

Theorem

Every finite integral domain is a field.

Proof. Let R be a finite integral domain $R = \{r_1, \ldots, r_n\}$. Take $r_i \in R$ to be nonzero. Consider $r_iR = \{r_ir_1, \ldots, r_ir_n\} \subseteq R$. Then, $|r_iR| \leq |R|$ since $r_iR \subseteq R$. Take $r_ir_j, r_ir_k \in r_iR$ such that $r_ir_j = r_ir_k$. Then because $r_i \neq 0$, we have $r_ir_j - r_ir_k = 0$, or $(r_j - r_k)r_i = 0$. Since $r_i \neq 0$ by assumption, $(r_j - r_k) = 0 \to r_j = r_k$. So $R \subseteq r_iR$ which implies $|R| \leq |r_iR|$. Because $|r_iR| \leq |R|$ and $|r_iR| \geq |R|$, $|r_iR| = |R|$. $\square$

Definition: Homomorphism

Let R, S be rings. A function $f : R \to S$ is a **ring homomorphism** if

(1) $f(a + b) = f(a) + f(b)$

(2) $f(a \cdot b) = f(a) \cdot f(b)$

(3)* $f(1_R) = 1_S$

*A function satisfying (1), (2), but not (3) is a **nonunital ring homomorphism**.

Proposition: Let R, S be rings and $f : R \to S$ a ring homomorphism. Given $a, b \in R$, the following hold:

(1) $f(0_R) = 0_S$

(2) $f(-a) = -f(a)$

(3) $f(a - b) = f(a) - f(b)$

(4) If $a \in R$ is a unit, then $f(a)$ is a unit and $f(a^{-1}) = [f(a)]^{-1}$.

Proof. Let R, S be rings and $f : R \to S$ a ring homomorphism.

(1) Take any $a \in R$. Then $\underline{f(a) + 0_S} = f(a + 0_R) = \underline{f(a) + f(0_R)}$, so $f(0_R) = 0_S$.

(2) $\underline{0_S} = f(0_R) = f(a+(-a)) = \underline{f(a) + f(-a)}$, so $f(a)+f(-a) = 0_S \implies f(-a) = -f(a)$.

(3) $\underline{f(a - b)} = f(a + (-b)) = f(a) + f(-b) = f(a) + (-f(b)) = \underline{f(a) - f(b)}$.

(4) Let $a \in R$ be a unit. Then there exists $a^{-1} \in R$ such that $aa^{-1} = 1$. Then $\underline{1_S} = f(1_R) = f(aa^{-1}) = \underline{f(a)f(a^{-1})}$ and $\underline{1_S} = f(1_R) = f(a^{-1}a) = \underline{f(a^{-1})f(a)}$, so $f(a)$ is a unit and define $[f(a)]^{-1} := f(a^{-1})$ to get $f(a^{-1}) = [f(a)]^{-1}$.

$\square$

Definition: Isomorphism

Let $f : R \to S$ be a ring homomorphism. f is an isomorphism if f is a bijection. Then R and S are isomorphic, written as $R \simeq S$.

Definition: Kernel and Image

Let $f : R \to S$ be a ring homomorphism.

→ The **kernel** of f is defined as $\ker(f) := \{a \in R : f(a) = 0_S\}$.

→ The **image** of f is defined as $\mathrm{Im}(f) := \{f(a) : a \in R\}$.

Proposition: Given a ring homomorphism $f : R \to S$, the image of f is a subring of S and the kernel of f is a nonunital subring of R.

Proof. Let $f : R \to S$ be a ring homomorphism. Then
$\mathrm{Im}(f)$ **is a subring of** S**:** Given $f(a), f(b) \in \mathrm{Im}(f)$, we have the following:

(1) $f(a) + f(b) = f(a + b) \in \mathrm{Im}(f)$.

(2) $f(a)f(b) = f(ab) \in \mathrm{Im}(f)$.

(3) $-f(a) = f(-a) \in \mathrm{Im}(f)$.

(4) $f(1_R) = 1_S \in \mathrm{Im}(f)$.

so $\mathrm{Im}(f)$ is a subring of S.

$\ker(f)$ **is a nonunital subring of** R**:** Given $a, b \in \ker(f)$, we have the following:

(1) $f(a + b) = f(a) + f(b) = 0_S + 0_S \in \ker(f)$.

(2) $f(ab) = f(a)f(b) = 0_s \cdot 0_S \in \ker(f)$.

(3) $f(-a) = -f(a) = -0_S = 0_S \in \ker(f)$.

(4) $f(0_R) = 0_S \in \ker(f)$.

so $\ker(f)$ is a nonunital subring of R. □

Proposition: Let $f : R \to S$ be a ring homomorphism. Then, for any $a \in \ker(f)$ and $b \in R$, we have $ab, ba \in \ker(f)$.

Proof. $\underline{f(ab)} = f(a)f(b) = 0_S \cdot f(b) = \underline{0_S} = f(b) \cdot 0_S = f(b)f(a) = \underline{f(ba)} \in \ker(f)$. □

Definition: Initial Object

$\mathbb{Z}$ is the **initial object**. Let R be any ring. Then, there is a unique homomorphism $f : \mathbb{Z} \to R$. At $n = 1$, $1 \mapsto 1_R$. At $n = n + 1$, $n + 1 \mapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} + 1_R$. The same is true for $n < 0$. f as defined above is a well-defined ring homomorphism.

Definition: Ideal

Let R be a ring and $I \subseteq R$ a nonempty subset. I is an **ideal** of R if I is a nonunital subring such that for all $a \in I$ and $x \in R$, $xa, ax \in I$. This is often called the "absorbing property".

Remark: The kernel of any ring homomorphism is an idea. Further, all ideal can be realized as the kernel of a ring homomorphism.

Definition: Principal Ideal

Let R be a commutative ring and $a \in R$. The **principal ideal** (a) is an ideal where $(a) := \{ar : r \in R\}$. We say "*a generates I*". Note that $(a) \iff aR$.

Theorem

Let R be a commutative ring and $a \in R$. Then the principal ideal (a) is an ideal.

Proof. Suppose (a) is the principal ideal. Then, $0 = a \cdot 0 \in (a)$. Given $ar_1, ar_2 \in (a)$, $ar_1 + ar_2 = a(r_1 + r_2) \in (a)$. Take $ar \in (a)$. Then $-ar = a(-r) \in (a)$. Take $ar_1 \in (a), r \in R$. Then $(ar_1)r = a(r_1 r) \in (a)$. Because (a) is a nonunital subring with the absorbing property, it is an ideal. □

Theorem

Let R be a ring and $I_1, \ldots, I_k$ be ideals. Then

(1) $I_1 + \cdots + I_k = \{i_1 + \cdots + i_k : i_j \in I_j\}$ is an ideal.

(2) $I_1 \cap \cdots \cap I_k$ is an ideal.

Proof. Let R be a ring, and $I_1, \cdots, I_k$ be ideals.

$I_1 + \cdots + I_k = \{i_1 + \cdots + i_k : i_j \in I_j\}$ **is an ideal.**

1. Since I_j is an ideal, $0 \in I_j$ so we get $0 + \cdots 0 = 0 \in I_1 + \cdots + I_k$.

2. Take two elements $a, b \in I_1 + \cdots + I_k$. We can rewrite a, b as, $a = p_1 + \cdots + p_k$ and $b = q_1 + \cdots + q_k$ for $p_j, q_j \in I_j$. Then $a + b = (p_1 + \cdots + p_k) + (q_1 + \cdots + q_k) = (p_1 + q_1) + \cdots + (p_k + q_k)$, and since $p_j + q_j \in I_j$ for all $j \leq k$, we get $a + b \in I_1 + \cdots + I_k$.

3. Take any $a \in I_1 + \cdots + I_k$. We can rewrite a as, $a = p_1 + \cdots + p_k$ for $p_j \in I_j$. Consider an element $r \in R$. Then, $ar = (p_1 + \cdots + p_k)r = p_1 r + \cdots + p_k r$. Similarly, $ar = r(p_1 + \cdots + p_k) = rp_1 + \cdots + rp_k$. Since I_j is an ideal, $p_j r, rp_j \in I_j$. Then $ar, ra \in I_1 + \cdots + I_k$.

4. Let $a := a_1 + \cdots + a_k \in I_1 + \cdots + I_k$. Since I_j is an ideal, there exists $-a \in I_j$, so we get $-a_1 + \cdots + -a_k = -(a_1 + \cdots + a_k) = -a \in I_1 + \cdots + I_k$.

Because $I_1 + \cdots + I_k$ satisfies (1) - (4), $I_1 + \cdots + I_k$ is an ideal.

$I_1 \cap \cdots \cap I_k$ is an ideal.

1. Since I_j is an ideal, $0 \in I_j$, so $0 \in I_1 \cap \cdots \cap I_k$.
2. Take two elements $a, b \in I_1 \cap \cdots \cap I_k$. Then since each I_j is an ideal, $a + b \in I_j$. So, $a + b \in I_1 \cap \cdots \cap I_k$.
3. Take any $a \in I_1 \cap \cdots \cap I_k$. Consider an element $r \in R$. Then, since each I_j is an ideal, $ar, ra \in I_j$. Therefore, $ar, ra \in I_1 \cap \cdots \cap I_k$.
4. Take any $a \in I_1 \cap \cdots \cap I_k$. Then, since I_j is an ideal, $-a \in I_j$, so $-a \in I_1 \cap \cdots \cap I_k$.

Because $I_1 \cap \cdots \cap I_k$ satisfies (1) - (4), $I_1 \cap \cdots \cap I_k$ is an ideal. □

Definition: Multiple Generators

Let R be a commutative ring and $a_1, \ldots, a_k \in R$. The ideal generated by $a_1, \cdots a_k$ is geiven by $(a_1) + \cdots + (a_k)$ and is written as $(a_1, \ldots, a_k)$.

Proposition: Let F be a field. The only ideal of F are $\{0\}$ and F.

Proof. Let I be a nonzero ideal of F and take $a \in I$. Then, $1 = aa^{-1} \in I$. Because $1 \in I$, $F = (1) = I$. □

2.2 Quotient Rings

Preface: To generalize the construction of $\mathbb{Z}/n$ to general rings, consider the following: given an ideal $I \subseteq R$, define equivalence where $a \sim b$ if $a - b \in I$. We can then inherit $(+, \cdot)$ from R. Given two equivalence classes $[a], [b]$, define $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$.

Definition: Congruent Modulo I

Let R be a ring, $I \subseteq R$ and ideal, and $a, b \in I$. a and b are **congruent modulo** I if $a - b \in I$. We write $a \equiv b \pmod{I}$, or $a + I = b + I$.

Remark: The notation $a + I := \{a + x : x \in I\}$ is precisely the congruence class modulo I containing a.

Proposition: Let R be a ring and $I \subseteq R$ an ideal. Congruence modulo I is an equivalence relation.

Proof. Let R be a ring and $I \subseteq R$ an ideal.

(1) For any $a \in R$, $a - a = 0 \in I$, so $a \equiv a \pmod{I}$.

(2) Take $a, b \in R$ such that $a \equiv b \pmod{I}$. Then $a - b \in I$. Since I is an ideal, $-(a - b) = b - a \in I$, so $b \equiv a \pmod{I}$.

(3) Let $a, b, c \in R$ such that $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$. Then $a - b, b - c \in I$. Then $(a - b) + (b - c) = a + (-b + b) - c = a - c \in I$, so $a \equiv c \pmod{I}$.

Since congruence modulo I satisfies $(1) - (3)$, it is an equivalence relation. □

Theorem

Let R be a ring, $a, b, c, d \in R$, and $I \subseteq R$ and ideal. Suppose $a \equiv c \pmod{I}$, $b \equiv d \pmod{I}$. Then $a + b \equiv c + d \pmod{I}$ and $ab \equiv cd \pmod{I}$.

Proof. Since $a - c, b - d \in I$, we have that $(a - c) + (b - d) = (a + b) - (c + d) \in I$. Then by definition, we have $a + b \equiv c + d \pmod{I}$. Now consider the following:

$$\begin{aligned} ab - cd &= ab + 0 - cd \\ &= ab + (-bc + bc) - cd \\ &= (ab - bc) + (bc - cd) \\ ab - cd &= b(a - c) + c(b - d) \end{aligned}$$

Since $a - c, b - d \in I$, $ab - cd \in I$, so $ab \equiv cd \pmod{I}$. $\square$

Notation: $(a + I) + (b + I) = (a + b) + I$ and $(a + I)(b + I) = ab + I$.

Definition: Quotient Ring

Let R be a ring, $a, b \in$, and $I \subseteq R$ and ideal. The **quotient ring** R/I is the set of congruence classes modulo I with $(+, \cdot)$ defined as $(a + I) + (b + I) = (a + b) + I$ and $(a + I)(b + I) = ab + I$ respectively.

Proposition: R/I is a ring.

Proof. I'm not checking all 9 axioms lol. $\square$

Theorem

Let R be a ring and $I \subseteq R$ and ideal. If R is commutative, then R/I is commutative.

Proof. Take $a + I, b + I \in R/I$. Then $(a + I)(b + I) = ab + I$ and $(a + I)(b + I) = ab + I$, so $ab + I = ba + I \implies (a + I)(b + I) = (b + I)(a + I)$. $\square$

Note: If R/I is commutative, it does ***not*** imply that R is commutative. For example, if $I = R$, then $R/I \simeq \{0\}$.

Definition: Canonical Projection

Let R be a ring, $I \subseteq R$ and ideal. Consider $\pi : R \to R/I$ such that $\pi(a) = a + I$. This map is the **canonical projection**.

Theorem

Let R be a ring, $I \subseteq R$ and ideal. The canonical projection $\pi : R \to R/I$ is a surjective ring homomorphism with $\ker(\pi) = I$.

Proof. Let R be a ring, $I \subseteq R$ and ideal. Let $\pi : R \to R/I$ be the canonical projection from R to R/I. Then

(1) $\pi(a+b) = (a+b) + I = (a+I) + (b+I) = \pi(a) + \pi(b)$.

(2) $\pi(a \cdot b) = (a \cdot b) \cdot I = (a \cdot I) \cdot (b \cdot I) = \pi(a) \cdot \pi(b)$.

(3) $\pi(1_R) = 1 + I = 1_{R/I}$.

so π is a ring homomorphism. Take $a+I \in R/I$. Then $\pi(a) = a+I$. Moreover, if $b \in [a+I]$, then $\pi(b) = a + I$. So π is surjective. Finally, let $a \in I$. Then $\pi(a) = a + I$ but $a \equiv 0 \pmod{I}$, so we have $\pi(a) = a+I = 0_R + I = I$. So, $\ker(\pi) \subseteq I$. Now suppose $\pi(a) = 0_R + I$. Then $[a+I] = [0_R + I]$, or $a \equiv 0_R \pmod{I}$. We can rewrite this to get $a - 0_R = a \in I$, so $I \subseteq \ker(\pi)$. Because $\ker(\pi) \subseteq I$ and $I \subseteq \ker(\pi)$, $\ker(\pi) = I$. □