Definition D1: A ring is a set of elements with two binary operations, called addition and multiplication, such that:

- Addition is closed
- Addition is commutative
- Addition is associative
- There exists an additive identity. (Do NOT call it 0 unless we have the uniqueness theorem)
- There exist additive inverses (Do NOT call them $-a$ unless we have the uniqueness theorem)
- Multiplication is closed
- Multiplication is associative
- Multiplication distributes over addition

Definition D2: Let R be a ring and $S \subseteq R$. S is said to be a subring of R if S is itself a ring with the same operations as R.

Theorem T1: Let a, b, and c be elements of a ring R. If $a + b = a + c$, then $b = c$.

Theorem T2: Let a and b be elements of a ring R. Then $a + x = b$ always has a unique solution.

Theorem T3: Let R be a ring. If $a + 0_1 = a$ and $a + 0_2 = a$ for all elements $a \in R$, then $0_1 = 0_2$.

Theorem T4: For each element a in a ring R, it's additive inverse is unique.

Theorem T5: Let a be an element of a ring R and denote the additive identity as 0. Then $a \cdot 0 = 0 \cdot a = 0$.

Theorem T6: Let R be a ring and let $a, b \in R$. Denote the additive inverse of each element $c \in R$ as $-c$, no matter what c is. Then $a(-b) = (-a)b = -(ab)$.

Theorem T7: Let R be a ring, and S a subset of R. S is a subring if and only if all of the following are satisfied for all elements $a, b \in S$:

1. $S \neq \emptyset$
2. $a, b \in S \Rightarrow a + b \in S$
3. $a, b \in S \Rightarrow a \cdot b \in S$
4. $a \in S \Rightarrow -a \in S$

Definition D2: Let R be a ring. A multiplicative identity of R is an element $s \in R$ such that $sr = rs = r$ for all $r \in R$. (Do NOT call it "1" until you justify that notation by proving that it is unique.)

Theorem T8: Let R be a ring. If R has a multiplicative identity, then it is unique.

Definition D3: Let R and S be rings. A function $\varphi: R \to S$ is called a ring homomorphism if is satisfies:

1. $\varphi(r + s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$.
2. $\varphi(rs) = \varphi(r)\varphi(s)$ for all $r, s \in R$.

Definition D4: Let R and S be rings. A ring homomorphism $\varphi: R \to S$ is called a ring isomorphism if is also one-to-one and onto. In this case R and S have an identical structure as rings.

Definition D5: Let R be a ring. An element $b \neq 0$ in R is called a zero divisor if there is another nonzero element $a \in R$ such that $ab = 0$.

Definition D6: A ring that is commutative with unity and no zero divisors is called an integral domain.

Theorem T9: Let R be an integral domain and suppose $a \neq 0$. If $ab = ac$, then $b = c$.

Definition D7: Let R be a ring with unity and $x \in R$. If there is some element $y \in R$ such that $xy = 1$, we say that x is invertible, or a unit. The set of all units of R is denoted either $U(R)$ or R^*.

Definition D8: Let R be a commutative ring and $a, b \in R$. We say that a and b are associates of each other if there is some $u \in R^*$ such that $a = ub$.

Definition D9: An integral domain in which every nonzero element is invertible is called a field.

Theorem T10: Let n be an integer at least 2. $\mathbb{Z}_n$ is a field if and only if p is prime.

Theorem T11: $x \in \mathbb{Z}_m$ is a unit if and only if $\gcd(x, m) = 1$.

Theorem T12: Let p be a prime number and $0 \neq x \in \mathbb{Z}_p$. Then $x^{p-1} = 1$ in $\mathbb{Z}_p$.

Theorem T13: Let R be a finite integral domain. Then R is a field.

Definition D10: Let R be a commutative ring. An ideal I of R is a subring that satisfies $xr \in I$ for all $x \in I$ and $r \in R$.

Definition D11: A principal ideal is an ideal with a single generator: $\langle a \rangle := \{ar | r \in R\}$. A ring is called a principal ideal domain (PID) if every ideal is principal.

Theorem T14a: Let R be a commutative ring with identity. Fix two elements $a, b \in R$. If $\langle a \rangle \subseteq \langle b \rangle$, then $a = bt$ for some $t \in R$.

Theorem T14b: Let R be a commutative ring with identity. Fix two elements $a, b \in R$. If $a = bt$ for some $t \in R$, then $\langle a \rangle \subseteq \langle b \rangle$.

Theorem T15a: Let R be a commutative ring with unity and $r \in R$. If $\langle r \rangle = R$, then r is a unit.

Theorem T15b: Let R be a commutative ring with unity and $r \in R$. If r is a unit, then $\langle r \rangle = R$.

Theorem T16a: Let R be an integral domain and let $r, s \in R$. If $\langle r \rangle = \langle s \rangle$, then r and s are associates.

Theorem T16b: Let R be an integral domain and let $r, s \in R$. If r and s are associates, then $\langle r \rangle = \langle s \rangle$.

Theorem T17a: Let R be a commutative ring with unity. If R is a field then its only ideals are $\{0\}$ and R itself.

Theorem T17b: Let R be a commutative ring with unity. If its only ideals are $\{0\}$ and R itself then R is a field.

Theorem T18: $\mathbb{Z}$ is a PID.

Theorem T19: Let $\varphi: R \to S$ be a ring homomorphism. Then $\varphi(0_R) = 0_S$

Theorem T20: Let $\varphi: R \to S$ be a ring homomorphism. Then $\varphi(-a) = -\varphi(a)$ for all $a \in R$.

Theorem T21: Let $\varphi: R \to S$ be a ring homomorphism. Then $\varphi(a - b) = \varphi(a) - \varphi(b)$.

Theorem T22: Let $\varphi: R \to S$ be a ring homomorphism. Assume R has unity, φ is onto and $S \neq \{0_S\}$. Then $\varphi(1_R) = 1_S$.

Theorem T23: Let $\varphi: R \to S$ be a ring homomorphism. Assume R has unity, φ is onto and $S \neq \{0_S\}$. Then if $a \in R$ is a unit, then $\varphi(a)$ is as well. Furthermore, $\left(\varphi(a)\right)^{-1} = \varphi(a^{-1})$.

Theorem T24: Let $\varphi: R \to S$ be a ring homomorphism. Then $\varphi(R)$ is a ring.

Definition D12: Let $\varphi: R \to S$ be a ring homomorphism. Then the kernel of φ is $\ker(\varphi) \coloneqq \{r \in R | \varphi(r) = 0_S\}$

Definition D13: Let $\varphi: R \to S$ be a ring homomorphism. The preimage of an element $s \in S$ is

$$\varphi^{-1}(s) \coloneqq \{r \in R | \varphi(r) = s\}$$

Theorem T25a: Let $\varphi: R \to S$ be a ring homomorphism. Then $\ker(\varphi)$ is a subring of R.

Theorem T25b: Let $\varphi: R \to S$ be a ring homomorphism. Then $\ker(\varphi)$ is an ideal of R.

Definition D14: Let R be a ring, $r \in R$, and I an ideal of R. The coset of I determined by r is:

$$I + r \coloneqq \{a + r | a \in I\}$$

Theorem T26: Let $\varphi: R \to S$ be a ring homomorphism. Assume $s \in \varphi(R)$ and $r \in \varphi^{-1}(s)$. Then:

$$\varphi^{-1}(s) = \ker(\varphi) + r$$

Theorem T27a: Let $\varphi: R \to S$ be a ring homomorphism. If φ is injective, then $\ker(\varphi) = \{0_R\}$

Theorem T27b: Let $\varphi: R \to S$ be a ring homomorphism. If $\ker(\varphi) = \{0_R\}$, then φ is injective.

Theorem T28a: Let I be an ideal of a commutative ring R. Assume $a, b \in I$. If $I + a \subseteq I + b$, then $I + a = I + b$.

Theorem T28b: Let I be an ideal of a commutative ring R. Assume $a, b \in I$. If $I + a \cap I + b \neq \emptyset$, then $I + a = I + b$.

Theorem T28c: Let I be an ideal of a commutative ring R. Assume $a, b \in I$. If $I + a = I + b$, then $a - b \in I$

Theorem T29d: Let I be an ideal of a commutative ring R. Assume $a, b \in I$. If $a - b \in I$, then $I + a = I + b$.

Theorem T29e: Let I be an ideal of a commutative ring R. Assume $a, b \in I$. Then $|I + a| = |I + b|$

Definition D15a: Let I be an ideal of a commutative ring R. Assume $a, b \in I$. Addition of cosets is defined as:

$$(I + a) + (I + b) \coloneqq I + (a + b)$$

Definition D15b: Let I be an ideal of a commutative ring R. Assume $a, b \in I$. Multiplication of cosets is defined as:

$$(I + a) \cdot (I + b) \coloneqq I + (a \cdot b)$$

Theorem T30a: Let I be an ideal of a commutative ring R. Addition of cosets of I is well defined.

Theorem T30b: Let I be an ideal of a commutative ring R. Multiplication of cosets is well defined.

Definition D16: Let R be a commutative ring and I an ideal of R. We define R mod I as:

$$R/I \coloneqq \{I + r | r \in R\}$$

Theorem T31: Let R be a commutative ring and I an ideal of R. Then R/I is a ring.

Definition D17: Let R be a commutative ring and I an ideal of R. The natural homomorphism from R to R/I is:

$$\begin{aligned} v: R &\to R/I \\ a &\mapsto I + a \end{aligned}$$

Theorem T32: Let R be a commutative ring and I an ideal of R. Denote the natural homomorphism from R to R/I as v. Then $\ker(v) = I$.