A **Ring** is a set R with two binary operations, called addition and multiplication, usually denoted by the operators '+' and '$\cdot$' respectively, such that

(i) $(R, +)$ forms an abelian group,
(ii) $(R, \cdot)$ forms a monoid,
(iii) multiplication distributes over addition, i.e.,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

for all $a, b, c \in R$.

The additive identity of R is denoted by 0_R, or simply 0 if the ring is clear from context.

The multiplicative identity of R is denoted by 1_R, or simply 1 if the ring is clear from context.

We often write the multiplication by omitting the '$\cdot$' operator, i.e., $ab = a \cdot b$ for all $a, b \in R$. Also, multiplication in R is understood to take precedence over addition, so we might rewrite condition (iii) as follows:

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc$$

for all $a, b, c \in R$.

Let R be a ring.

A subset $S \subseteq R$ is called a **subring** if $1 \in S$ and S closed under addition and multiplication.

Let R and S be rings.

A **ring homomorphism** is a map $\varphi : R \to S$ such that for all $a, b \in R$

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
(ii) $\varphi(ab) = \varphi(a)\varphi(b)$.

Let $\varphi : R \to S$ be a ring homomorphism. The **kernel** of φ is

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0\}.$$

The **image** of φ is

$$\varphi(R) = \{\varphi(r) \mid r \in R\}.$$

A **ring isomorphism** is a bijective ring homomorphism. If there exists an isomorphism between rings R and S, then R and S are said to be **isomorphic**, written $R \cong S$.

Let R be a ring, $I \subseteq R$, and $r \in R$.

We say I is an **ideal** of R if

(i) I is a subring of R,
(ii) $rI \subseteq I$ and $Ir \subseteq I$ for all $r \in R$.

We say I is a **proper ideal** if $I \neq R$.

The ideal $\{0\}$ is called the **trivial ideal** of R, and sometimes denoted by 0.

Let I be an ideal of R. The **quotient ring** of R by I is the set

$$R/I = \{r + I \mid r \in I\}$$

with operations

$$(r+I) + (s+I) = (r+s) + I \quad \text{and} \quad (r+I) \cdot (s+I) = (rs) + I.$$

We often write $\overline{r} = r + I$, and the operations become

$$\overline{r} + \overline{s} = \overline{r+s} \quad \text{and} \quad \overline{r} \cdot \overline{s} = \overline{rs}.$$

Let I, J be ideal of R.

Their **sum** is $I + J = \{a + b \mid a \in I, b \in J\}$.

Their **product** is $IJ = \{\sum a_k b_k \mid a_k \in I, b_k \in J\}$ with finite support, i.e., only finite sums.

Let R be a ring and $A \subseteq R$.

Denote by (A) the smallest ideal of R containing A, called the **ideal generated by** A.

1. If $A, B \subseteq R$, then $(A) + (B) = (A \cup B)$.
2. If $a_1, \ldots, a_n \in R$, then $(a_1) + \cdots + (a_n) = (a_1, \ldots, a_n)$.
3. If $r \in R$, then $(x - r) = \{p(x) \in R[x] \mid p(r) = 0\} = I_r\}$.
4. In $\mathbb{Z}[x]$, $(2, x) = \{2a(x) + xb(x) \mid a(x), b(x) \in \mathbb{Z}[x]\}$ is polynomials on $\mathbb{Z}[x]$ with constants in $2\mathbb{Z}$.
5. In $\mathbb{Q}[x]$, we have $(2, x) = \mathbb{Q}[x]$.

An ideal generated by a single element is called a **principal ideal**, i.e., (a) for $a \in R$.

An ideal generated by a finite set is called a **finitely generated ideal**.

1. Every principal ideal is finitely generated.
2. Every ideal of $\mathbb{Z}$ is principal: ideals are $n\mathbb{Z} = (n)$ for some $n \in \mathbb{Z}$.
3. $(2, x) \subseteq \mathbb{Z}[x]$ is not principal.
4. In $C^0([0, 1])$, the ideal $\{f \mid f(1/2) = 0\}$ is not finitely generated.

A proper ideal M is called a **maximal ideal** if the only ideals containing M are M and R.

Two ideals I and J of the ring R are said to be **comaximal** if $I + J = R$.

1. $n\mathbb{Z}, m\mathbb{Z} \subseteq \mathbb{Z}$ are comaximal if and only if n and m are coprime.

A proper ideal P is called a **prime ideal** if $ab \in P$ implies that either $a \in P$ or $b \in P$.

1. If $n \in \mathbb{Z}_{\geq 0}$, then $(n) = n\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ if and only if n is a prime number.

A subset $S \subseteq R$ called a **multiplicative subset** if $1 \in S$ and $ab \in S$ for all $a, b \in S$.

A subset $S \subseteq R$ called a **multiplicative subset** if $(S, \cdot)$ is a submonoid of $(R, \cdot)$.

1. $R^\times$ is a multiplicative subset of R.
2. If R is an integral domain, then $R \setminus \{0\}$ is a multiplicative subset of R.
3. If P is a prime ideal of R, then $R \setminus P$ is a multiplicative subset of R.

Let S be a multiplicative subset of the ring R.

Define the equivalence relation $\sim$ on $R \times S$ by

$$(a, s) \sim (b, t) \iff u(at - bs) = 0 \text{ for some } u \in S.$$

Denote the equivalence class $\overline{(a, s)} \in S^{-1}R$ by $\frac{a}{s}$. Then

$$\frac{a}{s} = \frac{b}{t} \iff u(at - bs) = 0 \text{ for some } u \in S.$$

The **localization of** R **at** S is the set

$$S^{-1}R = \{\tfrac{a}{s} \mid a \in R, s \in S\}$$

with operations

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{and} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

If R is an integral domain and $S^{-1} = R \setminus \{0\}$, then $S^{-1}R$ is the **fraction field** of R, denoted $\operatorname{Frac} R$ (sometimes called the quotient field, denoted $\operatorname{Quot}(R)$).

Given $a \in R$ non-nilpotent, take $S = \{a^n \mid n \in \mathbb{Z}_{\geq 0}\}$. Then $S^{-1}R$ is called the **localization of** R **at the element** a and denoted by R_a.

For a P is a prime ideal of R, denote by $R_P = (R \setminus P)^{-1}R$ the **localization of** R **at the prime ideal** P.

1. $\operatorname{Frac} \mathbb{Z} \cong \mathbb{Q}$.
2. $\{1\}^{-1}R \cong R$.
3. If $0 \in S$, then $S^{-1}R = 0$.
4. Fix $N \in \mathbb{Z}_{\geq 0}$, $S = \{N^n \mid n \in \mathbb{Z}_{\geq 0}\}$, then $S^{-1}\mathbb{Z} = \{m/N^n \mid m \in \mathbb{Z}, n \in n \in \mathbb{Z}_{\geq 0}\}$.
5. If p is a prime number and $S = \mathbb{Z} \setminus (p)$, then $S^{-1}\mathbb{Z} = \{m/n \mid m \in \mathbb{Z}, \gcd(n, p) = 1\}$

Let S be a multiplicative subset of the ring A.

There is a natural ring homomorphism

$$\begin{aligned} A &\to S^{-1}A, \\ a &\mapsto \frac{a}{1}. \end{aligned}$$

This map has the following universal property: If $f : A \to B$ is a ring homomorphism such that $f(S) \subseteq B^\times$, then there exists a unique ring homomorphism $S^{-1}A \to B$ such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr] & & B \\ & S^{-1}A \arrow[ur, dashed, "!"'] & \end{tikzcd}$$

Let R be an integral domain.

Any function $N : R \to \mathbb{Z}_{\geq 0}$ with $N(0) = 0$ is called a **norm**. If $N(a) > 0$ for $a \neq 0$, then N is called a **positive norm**.

We say R is a **Euclidean domain** if there is a norm N on R such that for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that

$$a = qb + r, \quad r = 0 \text{ or } N(r) < N(b).$$

The element q is called the **quotient** and r the **remainder** of the division of a by b.

1. $\mathbb{Z}$ is a Euclidean domain with $N(a) = |a|$.
2. A field is a Euclidean domain with the zero norm.
3. If F is a field, $F[x]$ is a Euclidean domain with $N(p(x)) = \deg p(x)$.

Let R be a commutative ring and $a, b \in R$ with $b \neq 0$.

a is said to be a **multiple** of b if there exists an element $x \in R$ with $a = bx$. Then b is said to **divide** a or be a **divisor** of a, written $b \mid a$.

A **greatest common divisor** (gcd) of a and b is a nonzero element d such that

(i) $d \mid a$ and $d \mid b$,
(ii) if $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

In which case, we denote $d = \gcd(a, b)$.

1. If R is a PID, $a, b \in R$ with $b \neq 0$, then $(a, b) = (d)$ for some $d \in R$. Moreover, d is a gcd of a and b.

A **principal ideal domain** (PID) is an integral domain in which every ideal is principal.

1. $\mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not.

Let R be an integral domain.

A nonzero, non-unit element $r \in R$ is called **irreducible** in R if

$$r = ab \implies a \in R^\times \text{ or } b \in R^\times,$$

and **reducible**, otherwise.

A nonzero element $p \in R$ is called **prime** in R if (p) is a prime ideal of R. Equivalently, a nonzero, non-unit element $p \in R$ is prime if

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Two elements $a, b \in R$ are said to be **associate** in R if $a = ub$ for some $u \in R^\times$.

A **unique factorization domain** (UFD) is an integral domain R in which every nonzero, non-unit element $r \in R$ has the following:

(i) $r = p_1 \cdots p_n$ where each p_i is irreducible in R,

(ii) this decomposition is unique up to associates, i.e., if $r = q_1 \cdots q_m$ is another factorization into irreducibles, then $m = n$ and there is a renumbering such that p_i is associate to q_i for $i = 1, \ldots, n$.

A ring R is called **Noetherian** if every ideal is finitely generated.

An integer a is called a **primitive root** mod n if $\overline{a}$ is a generator of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 1. (First Isomorphism Theorem) Let $\varphi : R \to S$ be a ring homomorphism.

1. $\ker \varphi$ is an ideal of R,
2. $\varphi(R)$ is a subring of S,
3. $R/\ker\varphi \cong \varphi(R)$.

If I is an ideal of R, then the natural projection

$$\begin{aligned} \pi : R &\to R/I \\ r &\mapsto r + I \end{aligned}$$

is a surjective ring homomorphism with $\ker \pi = I$.

Theorem 2. (Second Isomorphism Theorem) Let A be a subring and I be an ideal of R.

1. $A + I$ is a subring of R,
2. $A \cap I$ is an ideal of A and I is an ideal of $A + I$,
3. $(A + I)/I \cong A/(A \cap I)$.

Theorem 3. (Third Isomorphism Theorem) Let I and J be ideals of R with $I \subseteq J$.

1. J/I is an ideal of R/I,
2. $(R/I)/(J/I) \cong R/J$.

Theorem 4. (Fourth Isomorphism Theorem) Let I be an ideal of R. The map

$$\begin{aligned} \{\text{ideals of } R \text{ containing } I\} &\to \{\text{ideals of } R/I\} \\ J &\mapsto J/I \end{aligned}$$

is an inclusion preserving bijection.

Theorem 5. (Chinese Remainder Theorem) Let $I_1, \ldots, I_n$ be ideals of R. The map

$$\begin{aligned} \varphi : R &\to R/I_1 \times \cdots \times R/I_n \\ r &\mapsto (r + I_1, \ldots, r + I_n) \end{aligned}$$

is a ring homomorphism with $\ker\varphi = I_1 \cap \cdots \cap I_n$.

If I_i and J_j are comaximal for $i \neq j$, then this map is surjective and $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$, so

$$R/(I_1 \cdots I_n) \cong R/I_1 \times \cdots \times R/I_n.$$

Corollary 1. Let n be a positive integer and let $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

Corollary 2. Given $a_1, \ldots, a_n, c_1, \ldots, c_n \in \mathbb{Q}$ with $a_i \neq a_j$ for $i \neq j$. There exists a polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(a_j) = c_j$ for $j = 1, \ldots, n$.

If I is an ideal of R, then $I = R$ if and only if I contains a unit.

R is a field if and only if it has no nontrivial proper ideals, i.e., its only ideals are 0 and R.

If R is a field, then any nonzero ring homomorphism with domain R is an injection.

(id) Every proper ideal is contained in a maximal ideal.

(comm) An ideal M is maximal if and only if R/M is a field.

(comm) An ideal P is prime if and only if R/P is an integral domain.

(comm) Every maximal ideal is a prime ideal.

Every ideal in a Euclidean domain is principal.

Every nonzero prime ideal in a PID is maximal.

$R[x]$ is a PID if and only if R is a field.

Let R be an integral domain, $r \in R$. If r is prime in R, then r is irreducible in R.

A PID is a UFD.

In a UFD, an element is prime if an only if it is irreducible.

In a UFD, every nonzero non-unit has a prime factorization, unique up to associates.

Lemma 1. (Gauss' Lemma) Let R be a UFD with fraction field F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

$R[x]$ is a UFD if and only if R is a UFD.

If R is an integral domain and $r \in R$, then r is irreducible/prime in R if and only if it is irreducible/prime in $R[x]$.

Corollary 3. Let R be a UFD with fraction field F. If $p(x) \in R[x]$, then $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $F[x]$ and the gcd of its coefficients is 1. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

If R is a UFD and $p(x) \in R[x]$, then $(p(x))$ is a prime ideal of $R[x]$ if and only if $p(x)$ is irreducible in $R[x]$.

If F is a field and $p(x) \in G[x]$, then $(p(x))$ is a maximal ideal of $F[x]$ if and only if $p(x)$ is irreducible in $F[x]$.

Let F be a field and $p(x) \in F[x]$. Then $p(x)$ has a degree one factor if and only if $p(x)$ has a root in F.

Let F be a field. Then a polynomial of $F[x]$ of degree two or three is reducible if and only if it has a root in F.

Let R be an integral domain, I be a proper ideal of R, and $p(x) \in R[x]$ be a monic polynomial. If $\overline{p(x)} \in (R/I)[x]$ cannot be factored into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proposition 1. (Eisenstein's Criterion) Let R be an integral domain, P be a prime ideal of R, and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$ with $n \geq 1$. If $a_{n-1}, \ldots, a_1, a_0 \in P$ and $a_0 \notin P^2$, then $f(x)$ is irreducible in $R[x]$.

Corollary 4. (Eisenstein's Criterion for $\mathbb{Z}[x]$) Let p be a prime in $\mathbb{Z}$ and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$. If $p \mid a_j$ for $j = 0, 1, \ldots, n-1$ but $p \nmid a_0$, then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

A ring is Noetherian if and only if every ascending chain of R eventually stabilizes, i.e, for all sequences $\{I_j\}_{j \in \mathbb{N}}$ of ideals of R with $I_j \subseteq I_{j+1}$, there exists $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.

Let R be a Noetherian ring. If I is an ideal of R, then R/I is Noetherian. If S is a multiplicative subset of R, then $S^{-1}R$ is Noetherian.

Theorem 6. (Hilbert's Basis Theorem) If R is a Noetherian ring, then so is $R[x]$.

Theorem 7. (Primitive Root Theorem) Let F be a field. Then any finite subgroup of $F^\times$ is cyclic. In particular if p is a prime number, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Let $n \geq 2$ be an integer. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 2, 4, p^m, 2p^m$ where p is an odd prime and m is a positive integer.