

Ring Theory

References:

- Introduction to Modern Abstract Algebra, by David M. Burton.
- Contemporary abstract algebra, by Gallian and Joseph.
- Groups and Numbers, by R. M. Luther.
- A First Course in Abstract Algebra, by J. B. Fraleigh.
- Group Theory, by M. Suzuki.
- Abstract Algebra Theory and Applications, by Thomas W. Judson.
- Abstract Algebra, by I. N. Herstein.
- Basic Abstract Algebra, by P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul.

1. Definitions and Examples of Rings

Definition(1-1):

A ring is an ordered triple $(R, +, \cdot)$ consisting of a non-empty set R and two binary operations $+$ and \cdot on R such that

- $(R, +)$ is a commutative group,

- ii. (R, \cdot) is a semigroup (satisfies the axioms i, ii of group),
- iii. The two operations are related by the distributive laws

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

$$(b + c) \cdot a = (b \cdot a) + (c \cdot a) \forall a, b, c \in R.$$

Definition(1-2):

A commutative ring is a ring in which (R, \cdot) is a commutative.

Examples(1-3):

1. Each one of the following is a commutative ring:

$$(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{Z}, +, \cdot), (\mathbb{Z}_e, +, \cdot).$$

2. The set $R = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ is a commutative ring with identity.

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3} \in R,$$

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3} \in$$

$$R, \forall a, b, c, d \in \mathbb{Z}$$

$$1 = 1 + 0\sqrt{3} \in R.$$

3. Let R denote the set of all functions $f: \mathbb{R} \rightarrow \mathbb{R}$. The sum $f + g$ and product $f \cdot g$ of two functions $f, g \in R$ are defined as usual, by the equations

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

$$(f \cdot g)(x) = f(x) \cdot g(x), x \in \mathbb{R}.$$

The triple $(R, +, \cdot)$ is a commutative ring with identity.

4. The triple $(R, +, \circ)$ is not a ring.

The left distributive law $f \circ (g + h) \neq (f \circ g) + (f \circ h)$.

5. Let $(G, *)$ be an arbitrary commutative group and $\text{Hom } G$ be the set of all homomorphisms from $(G, *)$ into itself. $(\text{Hom } G, \circ)$ is a semigroup with identity, then the triple $(\text{Hom } G, +, \circ)$ forms a ring with identity.

$$(f + g)(x) = f(x) * g(x), x \in G$$

$(\text{Hom } G, +)$ is a commutative group.

$$\begin{aligned} (f + g)(x * y) &= f(x * y) * g(x * y) = f(x) * f(y) * g(x) * g(y) \\ &= (f(x) * g(x)) * (f(y) * g(y)) = (f + g)(x) * (f + g)(y), \end{aligned}$$

So that $f + g \in (\text{Hom } G, +)$.

$$\begin{aligned} [f \circ (g + h)](x) &= f((g + h)(x)) = f(g(x) * h(x)) \\ &= f(g(x)) * f(h(x)) \\ &= (f \circ g)(x) * (f \circ h)(x) = (f \circ g + f \circ h)(x). \end{aligned}$$

Therefore, $f \circ (g + h) = f \circ g + f \circ h$.

6. The triple $(Z_n, +_n, \cdot_n)$ is a commutative ring with identity.

7. Consider the set $R = \mathbb{R} \times \mathbb{R}$ of ordered pairs of real numbers. We define addition and multiplication in R by the formulas

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \cdot (c, d) = (ac, bd).$$

$(R, +, \cdot)$ is a commutative ring with identity.

8. The triple $(Z_4, +_4, \cdot_4)$ is a commutative ring with identity.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

\cdot_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Here, we have $2 \cdot_4 2 = 0$, the product of nonzero elements being zero.

Note also that $2 \cdot_4 1 = 2 \cdot_4 3$, yet it is clearly not true that $1 = 3$. The multiplicative semigroup (Z_4, \cdot_4) does not satisfy the cancellation law.

9. The triple $(\mathbb{C}, +, \cdot)$ is a commutative ring with identity.

10. The triple $(M_2(\mathbb{R}), +, \cdot)$ is a ring with identity, but not commutative.

11. The triple $(\mathbb{Z}_o, +, \cdot)$ is not ring, since the sum of two odds equal into even number.

2. Basic Properties of Rings

Theorem(2-1): If $(R, +, \cdot)$ be a ring, then

$$(1) \quad a \cdot 0 = 0 \cdot a = 0$$

$$(2) \quad (-c) \cdot a = -c \cdot a, \quad a(-c) = -a \cdot c$$

$$(3) \quad a \cdot b = (-a) \cdot (-b), \quad \forall a, b \in R$$

Proof: (1) $a \cdot (b - c) = a \cdot b - a \cdot c \dots (*)$

$$(b - c) \cdot a = b \cdot a - c \cdot a, \quad \forall a, b, c \in R \dots (*)$$

Substitute $b = c$ in $(*)$, we get $a \cdot (b - b) = a \cdot b - a \cdot b \Rightarrow a \cdot 0 = 0 \quad \forall a \in R$

$$(b - b) \cdot a = b \cdot a - b \cdot a \Rightarrow 0 \cdot a = 0.$$

Proof: (2) Substitute $b = 0$ in $(*)$ and by using (1), we have

$$a \cdot (0 - c) = a \cdot 0 - a \cdot c \Rightarrow a \cdot (-c) = -a \cdot c$$

$$(0 - c) \cdot a = -c \cdot a; \quad \forall a, c \in R.$$

Proof: (3) Substitute $a = -a$ in (2), we get

$$a \cdot (-c) = -a \cdot c$$

$$(-a) \cdot (-c) = -(-a) \cdot c$$

$$(-a) \cdot (-c) = -(-a \cdot c) = a \cdot c$$

Corollary(2-2): If $(R, +, \cdot)$ be a ring with identity and $R \neq \{0\}$, then

$$0 \neq 1, \quad (-1) \cdot a = -a$$

Proof: since $R \neq \{0\} \Rightarrow \exists a \in R \ni a \neq 0$, suppose that $0 = 1$

$$a = a \cdot 1 = a \cdot 0 = 0 \Rightarrow a = 0, \text{ but } a \neq 0 \text{ by assumption, thus } 0 \neq 1$$

To prove $(-1) \cdot a = -a$

$$(-1) \cdot a = -(1 \cdot a) = -a$$

Corollary(2-3): If $(R, +, \cdot)$ be a ring, if R has an identity element, then it is a unique.

Proof: let $1, 1^*$ are two identity elements of R , then $1 = 1 \cdot 1^* = 1^*$

Corollary(2-4): If a_1, a_2 are two inverses of a in a ring $(R, +, \cdot)$ with identity, then $a_1 = a_2$

Proof: $a_2 = a_2 \cdot 1 = a_2 \cdot (a \cdot a_1) = (a_2 \cdot a) \cdot a_1 = 1 \cdot a_1 = a_1$

Theorem(2-5): If $(R, +, \cdot)$ be a ring with identity and U be a set of units of R , then (U, \cdot) is a group.

Proof: $U \neq \emptyset$, since $\exists 1 \in U$

Let $a, b \in U \implies \exists a^{-1}, b^{-1} \in U \ni a \cdot a^{-1} = a^{-1} \cdot a = 1$

$$b \cdot b^{-1} = b^{-1} \cdot b = 1$$

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1$$

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot 1 \cdot b = b^{-1} \cdot b = 1$$

This means $a \cdot b \in U$

Since (R, \cdot) is associative, then (U, \cdot) is associative (since $U \subseteq R$)

Therefore, (U, \cdot) is a group.

3. Subrings, Examples and Properties

Definition(3-1): Let $(R, +, \cdot)$ be a ring and $S \subseteq R$ be a nonempty subset of R . If the triple $(S, +, \cdot)$ is itself a ring, then $(S, +, \cdot)$ is said to be a subring of $(R, +, \cdot)$.

Theorem(3-2): Let $(R, +, \cdot)$ be a ring and $\emptyset \neq S \subseteq R$. Then the triple $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$ if and only if

- (1) $a - b \in S \forall a, b \in S$ (closed under differences),
- (2) $a \cdot b \in S \forall a, b \in S$ (closed under multiplication).

Proof: (\implies) let $(S, +, \cdot)$ be a subring of $(R, +, \cdot) \implies (S, +)$ is a subgroup of $(R, +)$

$$\implies x - y \in S \forall x, y \in S$$

Since $(S, +, \cdot)$ is a subring of $(R, +, \cdot) \implies x \cdot y \in S \forall x, y \in S$.

(\impliedby) let $a - b \in S, a \cdot b \in S \forall a, b \in S \implies (S, +)$ is a subgroup of $(R, +)$

Since the operation of addition is a commutative on R , $S \subseteq R$

\Rightarrow the operation of addition is a commutative on S

$\Rightarrow (S, +)$ is an abelian subgroup of $(R, +)$

Also, similarly the associative and distributed the multiplication on addition are true on S since $S \subseteq R$.

$\Rightarrow (S, +, \cdot)$ is a subring of $(R, +, \cdot)$.

Examples(3-3):

(1) Every ring $(R, +, \cdot)$ has two trivial subrings; for, if 0 denotes the zero element of the ring $(R, +, \cdot)$, then both $(\{0\}, +, \cdot)$ and $(R, +, \cdot)$ are subrings of $(R, +, \cdot)$.

(2) In the ring of integers $(\mathbb{Z}, +, \cdot)$, the triple $(\mathbb{Z}_e, +, \cdot)$ is a subring, while $(\mathbb{Z}_o, +, \cdot)$ is not.

(3) Consider $(\mathbb{Z}_6, +_6, \cdot_6)$ the ring of integers modulo 6. If $S = \{0, 2, 4\}$, then $(S, +_6, \cdot_6)$, whose operation tables are given at the below, is a subring of $(\mathbb{Z}_6, +_6, \cdot_6)$.

$+_6$	0	2	4
0	0	2	4

2	2	4	0
4	4	0	2

6	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

- (4) Let $S = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$. Then $(S, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$, since for $a, b, c, d \in \mathbb{Z}$, we get

$$(a + b\sqrt{3}) - (c + d\sqrt{3}) = (a - c) + (b - d)\sqrt{3} \in S,$$

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3} \in S.$$

- (5) The triple $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$.
- (6) Let the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$, then the triple $(n\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Z}, +, \cdot)$.
- (7) $(\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}, +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$.
- (8) $(S = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$.

(9) Let $(R, +, \cdot)$ be a ring and $M = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in R \right\}$, then

$(M, +, \cdot)$ is a subring of $(M_2(R), +, \cdot)$.

(10) $(S = \{2a : a \in \mathbb{Z}\}, +, \cdot)$ is a subring of $(\mathbb{Z}, +, \cdot)$. We note that $1 \in \mathbb{Z}$, but $1 \notin S$.

(11) Give example to ring with identity and subring with different identity.

Take $(M_2(\mathbb{Z}), +, \cdot)$ and $(S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Z} \right\}, +, \cdot)$

The identity of $(M_2(\mathbb{Z}), +, \cdot)$ is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

The identity of $(S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Z} \right\}, +, \cdot)$ is $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

4. Characteristic of the Ring and Related Concepts

Definition(4-1): Let $(R, +, \cdot)$ be an arbitrary ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then the least positive integer with this property is called the characteristic of the ring.

If no such positive integer exists (that is, $na = 0$ for all $a \in R$ implies $n = 0$), then we say $(R, +, \cdot)$ has characteristic zero.

Example(4-2): the rings of integers, rational numbers and real numbers are standard examples of characteristic zero.

Example(4-3): the ring $(P(X), \Delta, \cap)$ is of characteristic two.

Since $A \Delta B = (A - B) \cup (B - A)$

$2A = A \Delta A = (A - A) \cup (A - A) = \emptyset$ for every subset A of X .

Theorem(4-4): Let $(R, +, \cdot)$ be a ring with identity. Then $(R, +, \cdot)$ has characteristic $n > 0$ if and only if n is the least positive integer for which $n \cdot 1 = 0$.

Proof: if the ring $(R, +, \cdot)$ is of characteristic $n > 0$, it follows trivially that $n \cdot 1 = 0$. If $m \cdot 1 = 0$, where $0 < m < n$, then

$$ma = m(1 \cdot a) = (m1) \cdot a = 0 \cdot a = 0$$

For every element $a \in R$. This would mean the characteristic of $(R, +, \cdot)$ is less than n , an obvious contradiction. The converse is established in much the same way.

Example(4-5): the characteristic of the ring $(\mathbb{C}, +, \cdot)$ is zero.

Example(4-6): the characteristic of the ring $(\mathbb{Z}_n, +_n, \cdot_n)$ is n .

Example(4-7): the characteristic of the ring $(Z_4 \times Z_6, \oplus, \otimes)$ is 12.

5. Ideals and their Properties

Definition(5-1): A subring $(I, +, \cdot)$ of the ring $(R, +, \cdot)$ is an ideal of $(R, +, \cdot)$ if and only if $r \in R$ and $a \in I$ imply both $r \cdot a \in I$ and $a \cdot r \in I$.

Definition(5-2): Let $(R, +, \cdot)$ be a ring and I a nonempty subset of R . Then $(I, +, \cdot)$ is an ideal of $(R, +, \cdot)$ if and only if

- (1) $a, b \in I$ imply $a - b \in I$,
- (2) $r \in R$ and $a \in I$ imply both $r \cdot a \in I$ and $a \cdot r \in I$.

Example(5-3): In any ring $(R, +, \cdot)$, the trivial subrings $(R, +, \cdot)$ and $(\{0\}, +, \cdot)$ are both ideals.

Remark(5-4): A ring which contains no ideals except these two is said to be simple. Any ideal different from $(R, +, \cdot)$ is a proper.

Example(5-5): The subring $(\{0,3,6,9\}, +_{12})$ is an ideal of $(Z_{12}, +_{12}, \cdot_{12})$, the ring of integers modulo 12.

Example(5-6): For a fixed integer $a \in \mathbb{Z}$, let $\langle a \rangle$ denote the set of all integral multiples of a , that is,

$$\langle a \rangle = \{na : n \in \mathbb{Z}\}$$

The following relations show the triple $(\langle a \rangle, +, \cdot)$ to be an ideal of the ring of integers $(\mathbb{Z}, +, \cdot)$:

$$na - ma = (n - m)a,$$

$$m(na) = (mn)a, \quad n, m \in \mathbb{Z}.$$

Example(5-7): $\langle 2 \rangle = \mathbb{Z}_e$, the ring of even integers $(\mathbb{Z}_e, +, \cdot)$ is an ideal of $(\mathbb{Z}, +, \cdot)$.

Example(5-8): Suppose $(R, +, \cdot)$ is the commutative ring of functions $f: \mathbb{R} \rightarrow \mathbb{R}$. The sum $f + g$ and product $f \cdot g$ of two functions $f, g \in R$ are defined as usual, by the equations

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

$$(f \cdot g)(x) = f(x) \cdot g(x), \quad x \in \mathbb{R}.$$

Define

$$I = \{f \in R : f(1) = 0\}.$$

For functions $f, g \in I$ and $h \in R$, we have

$$(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$$

And also

$$(h \cdot f)(1) = h(1) \cdot f(1) = h(1) \cdot 0 = 0.$$

Since both $f - g$ and $h \cdot f$ belong to I , $(I, +, \cdot)$ is an ideal of $(R, +, \cdot)$.

Example(5-9): Let $(M_2(\mathbb{R}), +, \cdot)$ be a ring, then $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}, +, \cdot)$ is a left ideal of $(M_2(\mathbb{R}), +, \cdot)$, but it is not right ideal of $(M_2(\mathbb{R}), +, \cdot)$.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I \Rightarrow \emptyset \neq I \subseteq M_2(\mathbb{R})$$

$$\text{Let } \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \in I \text{ and } \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(\mathbb{R})$$

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a - c & 0 \\ b - d & 0 \end{pmatrix} \in I$$

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ax + by & 0 \\ az + bw & 0 \end{pmatrix} \in I$$

Therefore, $(I, +, \cdot)$ is a left ideal of $(M_2(\mathbb{R}), +, \cdot)$

$(I, +, \cdot)$ is not right ideal of $(M_2(\mathbb{R}), +, \cdot)$, since

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in I$$

$$\text{But } \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin I$$

Example(5-10): Let $(R, +, \cdot)$ be the set of all functions on \mathbb{R} , then $I = \{f \in R: f(3) = 0\}$ is an ideal of $(R, +, \cdot)$.

Example(5-11): Prove or disprove, the triple $(\mathbb{Z}, +, \cdot)$ is an ideal of $(\mathbb{Q}, +, \cdot)$.

Theorem(5-12): If $(I, +, \cdot)$ is a proper ideal of a ring $(R, +, \cdot)$ with identity, then no element of I has a multiplicative inverse; that is, $I \cap R^* = \emptyset$.

Proof: suppose $0 \neq a \in I \ni a^{-1}$ exists

$$a^{-1} \cdot a = 1 \in I \text{ (since } I \text{ is closed under multiplication)}$$

Thus, $r \cdot 1 = r \forall r \in R \Rightarrow R \subseteq I$, but $I \subseteq R \Rightarrow I = R$ this is contradiction. (I a proper).

Theorem(5-13): If $(I_i, +, \cdot)$ is an arbitrary indexed collection of ideals of the ring $(R, +, \cdot)$, then so also is $(\cap I_i, +, \cdot)$.

Proof: $0 \in I_i \Rightarrow 0 \in \cap I_i \Rightarrow \cap I_i \neq \emptyset$

Let $a, b \in \cap I_i$ and $r \in R \Rightarrow a, b \in I_i \Rightarrow a - b, r \cdot a$ and $a \cdot r \in I_i$

$$\Rightarrow a - b, r \cdot a \text{ and } a \cdot r \in \bigcap I_i$$

Therefore, $(\bigcap I_i, +, \cdot)$ is an ideal of $(R, +, \cdot)$.

Example(5-14): Prove or disprove, the union of two ideals is an ideal.

Solution: In general, it is not true, for example, in $(Z_{12}, +_{12}, \cdot_{12})$

$\langle 4 \rangle = \{0, 4, 8\}, \langle 6 \rangle = \{0, 6\} \Rightarrow \langle 4 \rangle \cup \langle 6 \rangle = \{0, 4, 6, 8\}$ is not ideal, since

$$6 - 4 = 2 \notin \langle 4 \rangle \cup \langle 6 \rangle$$

Note(5-15): Consider $(R, +, \cdot)$ be a ring and $\emptyset \neq S \subseteq R$. Define the set

$$\langle S \rangle = \bigcap \{I : S \subseteq I; (I, +, \cdot) \text{ is an ideal of } (R, +, \cdot)\}.$$

$$\langle S \rangle \neq \emptyset, \text{ since } S \subseteq \langle S \rangle$$

Theorem(5-16): The triple $(\langle S \rangle, +, \cdot)$ is an ideal of the ring $(R, +, \cdot)$,

known as the ideal generated by the set S .

Example(5-17): $(Z_{18}, +_{18}, \cdot_{18})$, find $\langle S \rangle$ where $S = \{0, 9\}$.

Theorem(5-18): If $(R, +, \cdot)$ is a commutative ring with identity and $a \in R$, then the principle ideal $(\langle a \rangle, +, \cdot)$ generated by a is such that $\langle a \rangle = \{r \cdot a : r \in R\}$.

Theorem(5-19): If $(I, +, \cdot)$ is an ideal of the ring $(\mathbb{Z}, +, \cdot)$, then $I = \langle n \rangle$ for some nonnegative integer n .

Proof: If $I = \{0\}$, the theorem is trivially true, for the zero ideal $(\{0\}, +, \cdot)$ is the principal ideal generated by 0.

Let $0 \neq m \in I \Rightarrow -m \in I$, suppose n the least positive integer in I

Thus, $\langle n \rangle \subseteq I$, any integer $k \in I \Rightarrow k = qn + r$ where $q, r \in \mathbb{Z}, 0 \leq r < n$

Since $k, qn \in I \Rightarrow k - qn = r \in I \Rightarrow r = 0 \Rightarrow k = qn$

Thus every member of I is a multiple of $n \Rightarrow I \subseteq \langle n \rangle \Rightarrow I = \langle n \rangle$.

Theorem(5-20): Let a_1, a_2, \dots, a_n be nonzero element of a principal ideal ring $(R, +, \cdot)$. Then $(\cap \langle a_i \rangle, +, \cdot) = (\langle a \rangle, +, \cdot)$, where a is a least common multiple of a_1, a_2, \dots, a_n .

Proof: $(\cap \langle a_i \rangle, +, \cdot)$ is an ideal of $(R, +, \cdot)$.

But every ideal of $(R, +, \cdot)$ is a principle ideal; $\exists a \in R \ni \langle a \rangle = \cap \langle a_i \rangle$

Since $\langle a \rangle \subseteq \langle a_i \rangle [i = 1, 2, \dots, n], a = r_i \cdot a_i$ for some $r_i \in R$.

So, a is a common multiple of a_1, a_2, \dots, a_n .

Let b any common multiple of a_1, a_2, \dots, a_n , say $b = s_i \cdot a_i$, $s_i \in R$ [$i = 1, 2, \dots, n$]

If $r \in R$, then $r \cdot b = r \cdot (s_i \cdot a_i) = (r \cdot s_i) \cdot a_i \in \langle a_i \rangle \Rightarrow \langle b \rangle \subseteq \langle a_i \rangle$

Therefore, $\langle b \rangle \subseteq \bigcap \langle a_i \rangle = \langle a \rangle$ and b must be a multiple of a , thus a is a least common multiple of a_1, a_2, \dots, a_n .

Example(5-21): Consider the principal ideal $(\langle 4 \rangle, +, \cdot)$ and $(\langle 6 \rangle, +, \cdot)$ generated by the integers 4 and 6 in the ring $(\mathbb{Z}, +, \cdot)$. Then $(\langle 4 \rangle \cap \langle 6 \rangle, +, \cdot) = (\langle 12 \rangle, +, \cdot)$, where 12 is the least common multiple of 4 and 6.

6. Quotient Ring and Related Concepts.

Notes(6-1): Let $(I, +, \cdot)$ is an ideal of the ring $(R, +, \cdot)$, then

- (1) $a + I = \{a + i : i \in I\}$,
- (2) $(a + I) + (b + I) = (a + b) + I$,
- (3) $(a + I) \cdot (b + I) = (a \cdot b) + I$.

Theorem(6-2): If $(I, +, \cdot)$ is an ideal of the ring $(R, +, \cdot)$, then $(\frac{R}{I}, +, \cdot)$ is a ring, known as the quotient ring of R by I .

The zero element of $(\frac{R}{I}, +, \cdot)$ is the coset $0 + I = I$, while $-(a + I) = (-a) + I$.

Example(6-3): In the ring $(\mathbb{Z}, +, \cdot)$ of integers, consider the principal ideal $(\langle n \rangle, +, \cdot)$, where n is a nonnegative integer. The coset of $\langle n \rangle$ in \mathbb{Z} take the form

$$a + \langle n \rangle = \{a + kn : k \in \mathbb{Z}\}$$

$$(\mathbb{Z}_n, +_n, \cdot_n) \cong \left(\frac{\mathbb{Z}}{\langle n \rangle}, +, \cdot \right)$$

Example(6-4): The triple $(6\mathbb{Z}, +, \cdot)$ is an ideal of the ring $(2\mathbb{Z}, +, \cdot)$, then

$$\frac{2\mathbb{Z}}{6\mathbb{Z}} = \{0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$$

is a ring with an identity.

Example(6-5): Let $(R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}, +, \cdot)$ be a ring and $(I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z} \right\}, +, \cdot)$ is an ideal of the ring $(R, +, \cdot)$, then $(\frac{R}{I}, +, \cdot)$ is a commutative ring with identity.

$$\frac{R}{I} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + I : a, b \in \mathbb{Z} \right\}$$

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + I = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$$

7. Homomorphisms of Ring. Examples and Properties

Definition(7-1): Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be two rings and f a function from R into R' ; in symbols, $f: R \rightarrow R'$. Then f is said to be a ring homomorphism from $(R, +, \cdot)$ into $(R', +', \cdot')$ if and only if

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

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

for every pair of elements $a, b \in R$.

Example(7-2): Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be arbitrary rings and $f: R \rightarrow R'$ be the function that maps each element of R onto the zero element $0'$ of $(R', +', \cdot')$.

$$f(a + b) = 0' = 0' + ' 0' = f(a) + ' f(b),$$

$$f(a \cdot b) = 0' = 0' \cdot ' 0' = f(a) \cdot ' f(b), \quad a, b \in R.$$

As with the case of groups, this mapping is called the trivial homomorphism.

Example(7-3): The mapping $f: \mathbb{Z} \rightarrow \mathbb{Z}_e$ defined by $f(a) = 2a$ is not a homomorphism from $(\mathbb{Z}, +, \cdot)$ into $(\mathbb{Z}_e, +, \cdot)$,

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

but

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

Example(7-4): Consider $(\mathbb{Z}, +, \cdot)$, the ring of integers, and $(\mathbb{Z}_n, +_n, \cdot_n)$, the ring of integers modulo n . Define $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$ by taking $f(a) = [a]$; that is, map each integer into the congruence class containing it. Then

$$f(a + b) = [a + b] = [a] +_n [b] = f(a) +_n f(b),$$

$$f(a \cdot b) = [a \cdot b] = [a] \cdot_n [b] = f(a) \cdot_n f(b),$$

so that f is a homomorphism mapping.

Example(7-5): Let $(R, +, \cdot)$ be any ring with identity. For each invertible element $a \in R^*$, the function $f_a: R \rightarrow R$ given by

$$f_a(x) = a \cdot x \cdot a^{-1}$$

is a homomorphism from $(R, +, \cdot)$ into itself. Indeed, if $x, y \in R$, we see that

$$f_a(x + y) = a \cdot (x + y) \cdot a^{-1} = a \cdot x \cdot a^{-1} + a \cdot y \cdot a^{-1} = f_a(x) + f_a(y),$$

$$f_a(x \cdot y) = a \cdot (x \cdot y) \cdot a^{-1} = (a \cdot x \cdot a^{-1}) \cdot (a \cdot y \cdot a^{-1}) = f_a(x) \cdot f_a(y),$$

Theorem(7-6): Let f be a homomorphism from the ring $(R, +, \cdot)$ into the ring $(R', +', \cdot')$. Then the following hold:

- (1) $f(0) = 0'$, where $0'$ is the zero element of $(R', +', \cdot')$.
- (2) $f(-a) = -f(a)$ for all $a \in R$.
- (3) The triple $(f(R), +', \cdot')$ is a subring of $(R', +', \cdot')$.
- (4) $f(1) = 1'$.
- (5) $f(a^{-1}) = f(a)^{-1}$ for each invertible element $a \in R$.
- (6) If S is a subring in R , then $f(S)$ is a subring in R' .
- (7) If I is an ideal in R , then $f(I)$ is an ideal in R' .
- (8) If T is a subring in R' , then $f^{-1}(T)$ is a subring in R .
- (9) If J is an ideal in R' , then $f^{-1}(J)$ is an ideal in R .

Proof: (1) $f(0 + 0) = f(0) +' f(0)$

$$f(0) = f(0) +' f(0)$$

$$f(0) + '0' = f(0) + 'f(0) \Rightarrow f(0) = 0'$$

Proof: (2) $a + (-a) = 0$

$$f(a + (-a)) = f(0) \Rightarrow f(a) + 'f(-a) = 0' \Rightarrow f(-a) = -f(a)$$

Theorem(7-7): If f is a homomorphism from the ring $(R, +, \cdot)$ into the ring $(R', +', \cdot')$, then the triple $(\ker(f), +, \cdot)$ is an ideal of $(R, +, \cdot)$.

Proof: $\ker(f) = \{a \in R : f(a) = 0'\}$

$0 \in \ker(f)$, since $f(0) = 0' \Rightarrow \ker(f) \neq \emptyset$

Let $a, b \in \ker(f) \Rightarrow f(a) = 0' = f(b)$

$$f(a - b) = f(a) - f(b) = 0' - 0' = 0' \Rightarrow a - b \in \ker(f)$$

If $r \in R, a \in \ker(f) \Rightarrow f(r \cdot a) = f(r) \cdot 'f(a) = f(r) \cdot 0' = 0'$.

Thus, $r \cdot a \in \ker(f) \Rightarrow (\ker(f), +, \cdot)$ is an ideal of $(R, +, \cdot)$.

Theorem(7-8): If f is a homomorphism from the ring $(R, +, \cdot)$ into the ring $(R', +', \cdot')$, then f is a monomorphism iff $\ker(f) = \{0\}$.

Example(7-9): Consider an arbitrary ring $(R, +, \cdot)$ with identity element 1 and the mapping $f: \mathbb{Z} \rightarrow R$ given by $f(n) = n1$. Then f is a homomorphism from the ring of integers $(\mathbb{Z}, +, \cdot)$ into the ring $(R, +, \cdot)$:

$$f(n + m) = (n + m)1 = n1 + m1 = f(n) + f(m),$$

$$f(n \cdot m) = (n \cdot m)1 = (n \cdot m)1^2 = (n1) \cdot (m1) = f(n) \cdot f(m).$$

Theorem(7-10): That $\ker(f) = \{n \in \mathbb{Z}: n1 = 0\} = \langle m \rangle$ for some nonnegative integer m .

8. Fundamental Theorems of Homomorphisms of Rings.

Theorem(8-1): (The first fundamental theorem of homomorphism of ring)

Let φ be a homomorphism from $(R, +, \cdot)$ into $(R, +, \cdot)$, then

$$\left(\frac{R}{\ker \varphi}, +, \cdot \right) \cong (\varphi(R), +, \cdot)$$

Proof: let $\Psi: \frac{R}{\ker \varphi} \rightarrow \varphi(R)$ defined by $\Psi(x + \ker \varphi) = \varphi(x) \quad \forall x \in R$

To prove that Ψ is well define

$$\forall x + \ker \varphi, y + \ker \varphi \in \frac{R}{\ker \varphi}, x + \ker \varphi = y + \ker \varphi$$

$$(x - y) + \ker\varphi = \ker\varphi \Rightarrow (x - y) \in \ker\varphi$$

$$\Rightarrow \varphi(x - y) = 0 \Rightarrow \varphi(x) = \varphi(y) \Rightarrow \Psi(x + \ker\varphi) = \Psi(y + \ker\varphi)$$

To prove that Ψ is a homomorphism

$$\begin{aligned}\Psi[(x + \ker\varphi) + (y + \ker\varphi)] &= \Psi[(x + y) + \ker\varphi] \\ &= \varphi(x + y) = \varphi(x) + \varphi(y) = \Psi(x + \ker\varphi) + \Psi(y + \ker\varphi)\end{aligned}$$

Also

$$\begin{aligned}\Psi[(x + \ker\varphi) \cdot (y + \ker\varphi)] &= \Psi[(x \cdot y) + \ker\varphi] \\ &= \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = \Psi(x + \ker\varphi) \cdot \Psi(y + \ker\varphi)\end{aligned}$$

To prove Ψ is an onto

$$\text{If } z \in \text{Im}\varphi \Rightarrow \exists r \in R \ni z = \varphi(r), r + \ker\varphi \in \frac{R}{\ker\varphi}$$

$$\ni \Psi(r + \ker\varphi) = \varphi(r) = z$$

To prove Ψ is an one-to-one

$$\Psi(x + \ker\varphi) = \Psi(y + \ker\varphi) \Rightarrow \varphi(x) = \varphi(y)$$

$$\Rightarrow \varphi(x - y) = 0 \Rightarrow x - y \in \ker\varphi \Rightarrow (x - y) + \ker\varphi = \ker\varphi$$

$$\Rightarrow x + \ker\varphi = y + \ker\varphi \Rightarrow \left(\frac{R}{\ker\varphi}, +, \cdot\right) \cong (\varphi(R), +, \cdot)$$

Example(8-2): Let $f: Z_4 \rightarrow Z_2$ be a function defined by $f(0) = f(2) = 0, f(1) = f(3) = 1$.

$$\ker f = \{0,2\}, \quad \frac{Z_4}{\ker f} = \{\{0,2\}, \{1,3\}\}$$

The operation tables for the quotient ring $\left(\frac{Z_4}{\ker f}, +, \cdot\right)$ are as shown:

+	{0,2}	{1,3}
{0,2}	{0,2}	{1,3}
{1,3}	{1,3}	{0,2}

·	{0,2}	{1,3}
{0,2}	{0,2}	{0,2}
{1,3}	{0,2}	{1,3}

Therefore, $\left(\frac{Z_4}{\ker f}, +, \cdot\right) \cong (Z_2, +_2, \cdot_2)$

Theorem(8-3): (The second fundamental theorem of homomorphism of ring)

Let $(R, +, \cdot)$ be a ring, I be an ideal of R and H be a subring of R , then

$$\frac{(H + I)}{I} \cong \frac{H}{(H \cap I)}$$

Proof: Let $\varphi: H \rightarrow \frac{(H+I)}{I}$ defined by $\varphi(a) = a + I \forall a \in H$

To prove that φ is a homomorphism

$$\begin{aligned} \forall a, b \in H, \varphi(a + b) &= (a + b) + I = (a + I) + (b + I) \\ &= \varphi(a) + \varphi(b) \end{aligned}$$

Also

$$\varphi(a \cdot b) = (a \cdot b) + I = (a + I) \cdot (b + I) = \varphi(a) \cdot \varphi(b)$$

To prove that φ is an onto

$$\forall x + I \in \frac{(H + I)}{I} \ni x \in H + I, x = a + i \ni a \in H, i \in I$$

$$x + I = (a + i) + I = a + I \Rightarrow \varphi(x) = \varphi(a) = x + I$$

By the first theorem, we get

$$\frac{H}{\ker\varphi} \cong \frac{(H+I)}{I}$$

$$\begin{aligned} \ker\varphi &= \{x \in H: \varphi(x) = I\} = \{x \in H: x + I = I\} = \{x \in H: x \in I\} \\ &= \{x \in H: x \in H \cap I\} = H \cap I \end{aligned}$$

Therefore, $\frac{(H+I)}{I} \cong \frac{H}{(H \cap I)}$.

Theorem(8-4): Let $(R, +, \cdot)$ be a ring with identity and φ be a homomorphism from $(R, +, \cdot)$ into $(\varphi(R), +', \cdot')$, then

- (1) $\varphi(1)$ is an identity of $(\varphi(R), +', \cdot')$.
- (2) $\varphi(x^{-1})$ is an inverse $\varphi(x)$ in $(\varphi(R), +', \cdot')$.

Proof: (1) if $y \in \varphi(R), \exists x \in R \ni y = \varphi(x)$

$$1 \cdot x = x \cdot 1 = x \Rightarrow \varphi(1 \cdot x) = \varphi(x \cdot 1) = \varphi(x)$$

$$\varphi(1) \cdot' \varphi(x) = \varphi(x) \cdot' \varphi(1) = \varphi(x)$$

$$\varphi(1) \cdot' y = y \cdot' \varphi(1) = y \Rightarrow \varphi(1) \in \varphi(R)$$

Thus, $\varphi(1)$ is an identity element of $(\varphi(R), +', \cdot')$

Proof: (2) $x \cdot x^{-1} = x^{-1} \cdot x = 1 \Rightarrow \varphi(x \cdot x^{-1}) = \varphi(x^{-1} \cdot x) = \varphi(1)$

$$\varphi(x) \cdot' \varphi(x^{-1}) = \varphi(x^{-1}) \cdot' \varphi(x) = \varphi(1) \Rightarrow \varphi(x^{-1}) \in \varphi(R)$$

Hence, $\varphi(x^{-1})$ is an inverse of $\varphi(x)$ in $\varphi(R)$.

Theorem(8-5): (The third fundamental theorem of homomorphism of ring)

If I, J be two ideals in $(R, +, \cdot)$ with $J \subseteq I$, then $\frac{R}{I} \cong \frac{\frac{R}{J}}{\frac{I}{J}}$.

Proof: let $\varphi: \frac{R}{J} \rightarrow \frac{R}{I}$ defined by $\varphi(r + J) = r + I, \forall r \in R, r + J \in \frac{R}{J}$

To show that φ is a homomorphism

$$\begin{aligned}\varphi[(x + J) + (y + J)] &= \varphi[(x + y) + J] = (x + y) + I \\ &= (x + I) + (y + I) = \varphi(x + J) + \varphi(y + J)\end{aligned}$$

Also

$$\begin{aligned}\varphi[(x + J) \cdot (y + J)] &= \varphi[(x \cdot y) + J] = (x \cdot y) + I \\ &= (x + I) \cdot (y + I) = \varphi(x + J) \cdot \varphi(y + J)\end{aligned}$$

To prove $\ker\varphi = \frac{I}{J}$

Let $r + J \in \ker\varphi \Rightarrow \varphi(r + J) = I, \varphi(r + J) = r + I$

$$r + I = I \Rightarrow r \in I \Rightarrow r + J \in \frac{I}{J} \Rightarrow \ker\varphi \subseteq \frac{I}{J}$$

Let $z + J \in \frac{I}{J}, z \in I, \varphi(z + J) = z + I = I \Rightarrow z + J \in \ker \varphi \Rightarrow \frac{I}{J} \subseteq \ker \varphi$

Hence, $\frac{R}{I} \cong \frac{\frac{R}{J}}{\frac{I}{J}}$.

9. Properties of Ideals and Quotient Ring by Using Homomorphisms.

Theorem(9-1): Let I, J be two ideals in a ring $(R, +, \cdot)$, then $I + J$ is an ideal in a ring $(R, +, \cdot)$.

Proof: $I + J = \{x \in R : x = a + b; a \in I, b \in J\}$

$$\emptyset \neq I + J \subseteq R, 0 = 0 + 0 \in I + J$$

$$x, y \in I + J, x = a + b, a \in I, b \in J, y = c + d, c \in I, d \in J$$

$$x - y = (a + b) - (c + d) = (a - c) + (b - d) \in I + J$$

$$r \in R, r \cdot x = r \cdot (a + b) = r \cdot a + r \cdot b \in I + J$$

$$x \cdot r = (a + b) \cdot r = a \cdot r + b \cdot r \in I + J$$

Therefore, $I + J$ is an ideal in a ring $(R, +, \cdot)$.

Theorem(9-2): Let I, J be two ideals in a ring $(R, +, \cdot)$, then $I \cap J$ is an ideal in a ring $(R, +, \cdot)$.

Proof: $I \cap J = \{x \in R: x \in I, x \in J\}$

$$\emptyset \neq I \cap J \subseteq R, 0 \in I, 0 \in J, 0 \in I \cap J$$

$$x, y \in I \cap J, x, y \in I, x, y \in J, x - y \in I, x - y \in J, x - y \in I \cap J$$

$$a \in R, y \in I \cap J, y \in I, y \in J, a \cdot y, y \cdot a \in I, a \cdot y, y \cdot a \in J$$

$$a \cdot y \in I \cap J, y \cdot a \in I \cap J$$

Hence, $I \cap J$ is an ideal in a ring $(R, +, \cdot)$.

Theorem(9-3): Let I, J be two ideals in a ring $(R, +, \cdot)$, then $I \cdot J$ is an ideal in a ring $(R, +, \cdot)$.

Proof: $I \cdot J = \{x \in R: x = \sum_{i=1}^n x_i \cdot y_i; x_i \in I, y_i \in J, n \in \mathbb{Z}^+\}$

$$\emptyset \neq I \cdot J \subseteq R, 0 = 0 \cdot 0 \in I \cdot J$$

$$x, y \in I \cdot J, x = \sum_{i=1}^n x_i \cdot y_i; x_i \in I, y_i \in J, n \in \mathbb{Z}^+$$

$$y = \sum_{j=1}^m x_j' \cdot y_j'; x_j' \in I, y_j' \in J, m \in \mathbb{Z}^+$$

$$x - y = \sum_{i=1}^n x_i \cdot y_i - \sum_{j=1}^m x_j' \cdot y_j' = \sum_{i=1}^n x_i \cdot y_i + \sum_{j=1}^m (-x_j') \cdot y_j' \in I \cdot J$$

$$y \in I \cdot J, a \in R, a \cdot y = a \cdot \left(\sum_{j=1}^m x_j' \cdot y_j' \right) = \sum_{j=1}^m (a \cdot x_j') \cdot y_j' \in I \cdot J$$

$$y \cdot a = \left(\sum_{j=1}^m x_j' \cdot y_j' \right) \cdot a = \left(\sum_{j=1}^m x_j' \cdot (y_j' \cdot a) \right) \in I \cdot J$$

Thus, $I \cdot J$ is an ideal in a ring $(R, +, \cdot)$.

Theorem(9-4): Let $J \subseteq I$ be two ideals in a ring $(R, +, \cdot)$, then $\frac{I}{J}$ is an ideal in a ring $(R, +, \cdot)$.

Proof: $\frac{I}{J} = \{x \in R : x \cdot J \subseteq I\}$

$$\emptyset \neq \frac{I}{J} \subseteq R, 0 \cdot J = \{0\} \subseteq I, \{0\} \in \frac{I}{J}$$

$$x, y \in \frac{I}{J}, x = a \cdot J, y = b \cdot J$$

$$x - y = a \cdot J - b \cdot J = (a - b) \cdot J \subseteq I, x - y \in \frac{I}{J}$$

$$r \in R, r \cdot x = r \cdot (a \cdot J) = (r \cdot a) \cdot J \subseteq I$$

Hence, $\frac{I}{J}$ is an ideal in a ring $(R, +, \cdot)$.

Theorem(9-5): Let $(R, +, \cdot)$ be a commutative ring, then \sqrt{I} is an ideal in $(R, +, \cdot)$ contains I .

Proof: $\emptyset \neq \sqrt{I} = \{x \in R: \exists n \in \mathbb{Z}^+; x^n \in I\} \subseteq R, 0 \in I, 0 \in \sqrt{I}$

$$x, y \in \sqrt{I}, x^n \in I, y^m \in I$$

$$(x - y)^{m+n-1} \in I, x - y \in \sqrt{I}$$

$$x \in \sqrt{I}, a \in R, x^n \in I, (a \cdot x)^n \in I, a \cdot x \in \sqrt{I}$$

To show $I \subseteq \sqrt{I}$

$$y \in I, y^1 \in I, y \in \sqrt{I}$$

Example(9-6): Find $\sqrt{\langle 6 \rangle}$.

Example(9-7): Show that $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$.

10. Zero Divisors Elements and Integral Domains.

Definition(10-1): A ring $(R, +, \cdot)$ is said to have divisors of zero if there exist nonzero elements $a, b \in R$ such that the product $a \cdot b = 0$.

Theorem(10-2): A ring $(R, +, \cdot)$ is without divisors of zero if and only if the cancellation law holds for multiplication.

Proof:(\implies) Assume $(R, +, \cdot)$ contains no divisors of zero.

let $a, b, c \in R \ni a \neq 0, a \cdot b = a \cdot c$, then

$$a \cdot (b - c) = a \cdot b - a \cdot c = 0$$

Since $a \neq 0$, $(R, +, \cdot)$ has no zero divisors, $b - c = 0$ or $b = c$

(\impliedby) suppose that the cancellation law holds and $a \cdot b = 0$

If $a \neq 0$, then $a \cdot b = a \cdot 0 \implies b = 0$.

$$b \neq 0 \implies a = 0$$

This shows $(R, +, \cdot)$ is free of divisors of zero.

Corollary(10-3): Let $(R, +, \cdot)$ be a ring with identity which has no zero divisors. Then the only solutions of the equation $a^2 = a$ are $a = 0$ and $a = 1$.

Proof: if $a^2 = a = a \cdot 1$, with $a \neq 0$, then $a = 1$.

Definition(10-4): An integral domain is a commutative ring with identity which does not have divisors of zero.

Theorem(10-5): The characteristic of an integral domain $(R, +, \cdot)$ is either zero or a prime number.

Proof: let $(R, +, \cdot)$ be of positive characteristic n and assume that n is not a prime.

$$n = n_1 n_2 \text{ with } 1 < n_i < n (i = 1, 2).$$

$$0 = n1 = (n_1 n_2)1 = (n_1 n_2)1^2 = (n_1 1) \cdot (n_2 1).$$

Since $(R, +, \cdot)$ is without zero divisors, either $n_1 1 = 0$ or $n_2 1 = 0$.

But this is contradiction, n the least positive integer such that $n1 = 0$.

Hence, we are led to conclude that the characteristic must be prime.

Example(10-6): Let $(M_2(R), +, \cdot)$ be a ring. Then $\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}, c, d \in R$ is a right zero divisor and $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, a, b \in R$ is a left zero divisor in $(M_2(R), +, \cdot)$.

Solution: $\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Example(10-7): The number 2 is a zero divisor in a ring $(Z_4, +_4, \cdot_4)$ and the numbers 2,3 are zero divisors in a ring $(Z_6, +_6, \cdot_6)$. (**check**)

Example(10-8): Let $(S = \{(a, b): a, b \in \mathbb{Z}\}, +, \cdot)$ be a commutative ring with identity and define

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$$

The identity element with $+$ is $(0,0)$, and the identity with \cdot is $(1,1)$.

Also, $(1,0)$ is a zero divisor, since

$$(1,0) \cdot (0,1) = (0,0)$$

$$(0,1) \neq (0,0), (1,0) \neq (0,0).$$

Example(10-9): The triple $(\mathbb{Z}, +, \cdot)$ is an integral domain, since $(\mathbb{Z}, +, \cdot)$ is a commutative with identity .

$$x, y \in \mathbb{Z} \ni x \cdot y = 0 \implies x = 0 \text{ or } y = 0 .$$

Example(10-10): Let $(Z_p, +_p, \cdot_p)$ be a ring, where p is a prime number, then $(Z_p, +_p, \cdot_p)$ is an integral domain.

Solution: the triple $(Z_p, +_p, \cdot_p)$ is a commutative with identity [1].

To show $(Z_p, +_p, \cdot_p)$ has no zero divisors.

Let $[a], [b] \in Z_p \ni [a] \cdot_p [b] = [0] \Rightarrow [a \cdot b] = [0] \Rightarrow \frac{p}{a \cdot b}$

But p is a prime number, $\Rightarrow \frac{p}{a}$ or $\frac{p}{b} \Rightarrow [a] = [0]$ or $[b] = [0]$.

Example(10-11): $(M_n(R), +, \cdot)$ is not an integral domain, since it is not commutative ring.

Example(10-12): Solve the equation $x^2 - 4x + 3 = 0$ in a ring $(Z_{12}, +_{12}, \cdot_{12})$.

Solution: $x^2 - 4x + 3 = 0 \Rightarrow (x - 3)(x - 1) = 0 \Rightarrow x = 3, x = 1$.

But, in $(Z_{12}, +_{12}, \cdot_{12})$, we have

$$[0] \cdot_{12} [a] = [a] \cdot_{12} [0] = [0]$$

Since

$$\begin{aligned} 2 \cdot_{12} 6 &= 3 \cdot_{12} 4 = 3 \cdot_{12} 8 = 4 \cdot_{12} 9 = 6 \cdot_{12} 6 = 6 \cdot_{12} 8 = 6 \cdot_{12} 10 \\ &= 9 \cdot_{12} 8 = 0 \end{aligned}$$

So,

$$(9 - 3)(9 - 1) = 6 \cdot_{12} 8 = 0$$

$$(7 - 3)(7 - 1) = 4 \cdot_{12} 6 = 0$$

Hence, $\{1,3,7,9\}$ is a set of solution of $x^2 - 4x + 3 = 0$ in $(Z_{12}, +_{12}, \cdot_{12})$.

Example(10-13): Let $(R, +, \cdot)$ is an integral domain with $x, y \in R \ni x^5 = y^5$ and $x^7 = y^7$. Show that $x = y$.

Solution: If $x = 0 \Rightarrow x^5 = 0 \Rightarrow y^5 = 0 \Rightarrow y = 0$.

Let $x \neq 0$, $x^7 = y^7 \Rightarrow x^5 \cdot x^2 = y^5 \cdot y^2$

$\Rightarrow x^5 \cdot x^2 = x^5 \cdot y^2 \Rightarrow x^5 \cdot (x^2 - y^2) = 0$

Since, $(R, +, \cdot)$ is an integral domain and $x \neq 0$

$\Rightarrow x^5 \neq 0 \Rightarrow x^2 - y^2 = 0 \Rightarrow x^2 = y^2 \Rightarrow x^6 = y^6 \dots (*)$

$x^7 = y^7 \Rightarrow x^6 \cdot x = y^6 \cdot y$

By $(*)$, we get

$$x^6 \cdot (x - y) = 0, x \neq 0, x^6 \neq 0 \Rightarrow x - y = 0 \Rightarrow x = y$$

Corollary(10-14): Let $(R, +, \cdot)$ be a ring with identity and $u \in R$ is an invertible, then u is not zero divisor.

Proof: let $r \in R \ni u \cdot r = 0 \Rightarrow u^{-1}(u \cdot r) = u^{-1}(0) = 0$

$\Rightarrow (u^{-1} \cdot u) \cdot r = 0 \Rightarrow 1 \cdot r = 0 \Rightarrow r = 0$

Also,

$$r \cdot u = 0 \implies (r \cdot u) \cdot u^{-1} = (0) \cdot u^{-1}$$

$$\implies r \cdot (u \cdot u^{-1}) = r \cdot 1 = 0 \implies r = 0.$$

11. Fields and their properties

Definition(11-1): A ring $(F, +, \cdot)$ is said to be a field provided the pair $(F - \{0\}, \cdot)$ forms a commutative group.

Example(11-2): Both $(\mathbb{R}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ are fields. (check)

Example(11-3): The triple $(F = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}, +, \cdot)$ is a field.

$$0 = 0 + 0\sqrt{3}, \quad 1 = 1 + 0\sqrt{3}$$

$$(a + b\sqrt{3})^{-1} = \frac{1}{(a + b\sqrt{3})} = \frac{1}{(a + b\sqrt{3})} \frac{a - b\sqrt{3}}{a - b\sqrt{3}}$$

$$= \frac{a}{a^2 - 3b^2} + \frac{-b}{a^2 - 3b^2} \sqrt{3} \in F$$

Example(11-4): The triple $(\mathbb{R} \times \mathbb{R}, +, \cdot)$, is a field. Where

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

The pair $(1,0)$ is the multiplicative identity and $(0,0)$ is the zero element of the ring.

Now, suppose $(a, b) \neq (0,0)$, either $a \neq 0$ or $b \neq 0$, so that $a^2 + b^2 > 0$; thus

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = \left(\frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ab}{a^2 + b^2} \right) = (1,0)$$

Example(11-5): The field \mathbb{R} contains a subring which is isomorphic to the ring of real numbers.

$$\mathbb{R} \times 0 = \{(a, 0) : a \in \mathbb{R}\}$$

It follows that $(\mathbb{R}, +, \cdot) \cong (\mathbb{R} \times 0, +, \cdot)$ via the mapping f defined by

$$f(a) = (a, 0), a \in \mathbb{R} \text{ (check)}$$

Example(11-6): The triple $(Z_p, +_p, \cdot_p)$ is a field.

Let $[0] \neq [a] \in Z_p \Rightarrow \gcd(a, p) = 1$

$$\Rightarrow \exists s, t \in \mathbb{Z} \ni a \cdot s + p \cdot t = 1$$

$$\Rightarrow [a] \cdot_p [s] +_p [p] \cdot_p [t] = [1]$$

$$\Rightarrow [a] \cdot_p [s] = [1]$$

$\Rightarrow [s]$ is a multiplicative inverse of $[a]$.

Example(11-7): The triple $(\mathbb{C}, +, \cdot)$ is a field. (**check**)

Corollary(11-8): In a field $(F, +, \cdot)$, with $0 \neq a, b \in F$, then there exist a unique element x satisfies $a \cdot x + b = 0$.

Proof: $(F, +)$ is an abelian group, then

$$a \cdot x + b = 0 \Leftrightarrow a \cdot x = -b \Leftrightarrow x = a^{-1}(-b) = -a^{-1} \cdot b$$

Example(11-9): The triple $(\mathbb{R}, *, \circ)$ is a field, where $*, \circ$ are defined by

$$a * b = a + b + 1, a \circ b = a \cdot b + a + b \forall a, b \in \mathbb{R} \text{ (**check**)}$$

Theorem(11-10): If $(F, +, \cdot)$ is a field and $a, b \in F$ with $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Proof: if $a = 0$, the theorem is already established.

Suppose that $a \neq 0$ and prove that $b = 0$.

$$a^{-1} \in F, a \cdot b = 0$$

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b.$$

12. More Results of Fields and Integral Domains.

Theorem(12-1): Any finite integral domain $(R, +, \cdot)$ is a field.

Proof: suppose $a_1, a_2, \dots, a_n \in R$ and $0 \neq a \in R$

$a \cdot a_1, a \cdot a_2, \dots, a \cdot a_n$ are all distinct, for if $a \cdot a_i = a \cdot a_j$, then $a_i = a_j$ by the cancellation law. So each element of R is of the form $a \cdot a_i$.

In particular, $\exists a_i \in R \ni a \cdot a_i = 1$; since multiplication is commutative, we have $a_i = a^{-1}$. This shows that every nonzero element of R is invertible, so $(R, +, \cdot)$ is a field.

Example(12-2): Prove or disprove, every integral domain is a field.(check)

Example(12-3): Prove or disprove, every ring is a field.(check)

Example(12-4): Prove or disprove, every ring is an integral domain.(check)

Theorem(12-5): The ring $(Z_n, +_n, \cdot_n)$ of integers modulo n is a field if and only if n is a prime number.

Proof: We first show that if n is not prime, then $(Z_n, +_n, \cdot_n)$ is not a field.

Thus assume $n = a \cdot b$, where $0 < a < n$ and $0 < b < n$.

$$[a] \cdot_n [b] = [a \cdot b] = [n] = [0],$$

Both $[a] \neq 0, [b] \neq 0$. This means that $(Z_n, +_n, \cdot_n)$ is not an integral domain, and hence not a field.

Suppose that n is a prime number. To show that $(Z_n, +_n, \cdot_n)$ is a field.

Let $[a] \in Z_n$, where $0 < a < n$. $\text{gcm}(a, n) = 1 \implies \exists r, s \in \mathbb{Z} \ni a \cdot r + n \cdot s = 1$

$$[a] \cdot_n [r] = [a \cdot r] +_n [0] = [a \cdot r] +_n [n \cdot s] = [a \cdot r + n \cdot s] = [1],$$

Showing the congruence class $[r]$ to be the multiplicative inverse of $[a]$.

Therefore, $(Z_n, +_n, \cdot_n)$ is a field.

Theorem(12-6): Let $(R, +, \cdot)$ be a commutative ring with identity. Then $(R, +, \cdot)$ is a field if and only if $(R, +, \cdot)$ has no nontrivial ideals.

Proof: (\implies) Assume first that $(R, +, \cdot)$ is a field. We wish to show that the trivial ideals $(\{0\}, +, \cdot)$ and $(R, +, \cdot)$ are its only ideals.

Let $(I, +, \cdot)$ be nontrivial ideal of $(R, +, \cdot) \implies I \neq \{0\}$ and $I \neq R$

$\implies \exists 0 \neq a \in I$, since $(R, +, \cdot)$ is a field $\implies \exists a^{-1} \in R \ni a^{-1} \cdot a = 1 \in I$

$I \implies I = R$

But, this is contradiction.

(\Leftarrow) suppose that $(R, +, \cdot)$ has no nontrivial ideals.

Let $a \in R$, consider the principal idea $(\langle a \rangle, +, \cdot)$ generated by a :

$$\langle a \rangle = \{r \cdot a : r \in R\}$$

Now $(\langle a \rangle, +, \cdot)$ cannot be the zero ideal, since $a = a \cdot 1 \in \langle a \rangle$, with $a \neq 0$.

If $(\langle a \rangle, +, \cdot) = (R, +, \cdot)$: that is, $\langle a \rangle = R$, since $1 \in \langle a \rangle$, $\exists r' \in R \ni r' \cdot a = 1$

$$\Rightarrow r' = a^{-1}$$

Hence each nonzero element of R has a multiplicative inverse in R .

Definition(12-7): By a subfield of the field $(F, +, \cdot)$ is meant any subring $(F', +, \cdot)$ of $(F, +, \cdot)$ which is itself a field.

Example(12-8): The ring $(\mathbb{Q}, +, \cdot)$ is a subfield of the field $(\mathbb{R}, +, \cdot)$.

Theorem(12-9): The triple $(F', +, \cdot)$ is a subfield of $(F, +, \cdot)$ if and only if the following hold:

- (1) F' is a nonempty subset of F with at least one nonzero element.
- (2) $a, b \in F'$ implies $a - b \in F'$.
- (3) $a, b \in F'$, where $b \neq 0$, implies $a \cdot b^{-1} \in F'$.

Definition(12-10): A field which does not have any proper subfields is called a prime field.

Example(12-11): The field of rational numbers, $(\mathbb{Q}, +, \cdot)$, is a prime field.

To see this, suppose $(F, +, \cdot)$ is a subfield of $(\mathbb{Q}, +, \cdot)$ and let $0 \neq a \in F$.

Since $(F, +, \cdot)$ is a subfield, it must contain the product $a \cdot a^{-1} = 1$.

$n = n \cdot 1^{-1} \in F \quad \forall n \in \mathbb{Z}$: in other words, F contains all the integers. It follows then that every rational number $\frac{n}{m} = n \cdot m^{-1}, m \neq 0$, also belongs to F , so that $F = \mathbb{Q}$.

Example(12-12): For every prime p , the field $(\mathbb{Z}_p, +_p, \cdot_p)$ of integers modulo p is a prime field. The reasoning here depends on the fact that the additive group $(\mathbb{Z}_p, +_p)$ of $(\mathbb{Z}_p, +_p, \cdot_p)$ is a finite group of prime order, and therefore has no nontrivial subgroups.

Remark(12-13): Every field contains a subfield which isomorphic either to the field $(\mathbb{Q}, +, \cdot)$ or to one of the fields $(\mathbb{Z}_p, +_p, \cdot_p)$, p a prime.

13. Maximal Ideals. Examples, Properties and Results.

Definition(13-1): An ideal $(I, +, \cdot)$ of the ring $(R, +, \cdot)$ is a maximal ideal provided $I \neq R$ and whenever $(J, +, \cdot)$ is an ideal of $(R, +, \cdot)$ with $I \subset J \subseteq R$, then $J = R$.

Theorem(13-2): Let $(\mathbb{Z}, +, \cdot)$ be the ring of integers and $n > 1$. Then the principal ideal $(\langle n \rangle, +, \cdot)$ is maximal if and only if n is a prime number.

Proof: (\Rightarrow) suppose $(\langle n \rangle, +, \cdot)$ is a maximal ideal of $(\mathbb{Z}, +, \cdot)$. If the integer n is not prime, then $n = n_1 n_2$, where $1 < n_1 \leq n_2 < n$. This implies the ideals $(\langle n_1 \rangle, +, \cdot)$ and $(\langle n_2 \rangle, +, \cdot)$ are such that

$$\langle n \rangle \subset \langle n_1 \rangle \subset \mathbb{Z}, \quad \langle n \rangle \subset \langle n_2 \rangle \subset \mathbb{Z},$$

contrary to the maximality of $(\langle n \rangle, +, \cdot)$

(\Leftarrow) assume that n is prime.

If the ideal $(\langle n \rangle, +, \cdot)$ is not maximal in $(\mathbb{Z}, +, \cdot)$, then either $\langle n \rangle = \mathbb{Z}$ or else there exists some proper ideal $(\langle m \rangle, +, \cdot)$ with $\langle n \rangle \subset \langle m \rangle \subset \mathbb{Z}$. The first

case is immediately ruled out by the fact that 1 is not a multiple of a prime number.

The alternative possibility $\langle n \rangle \subset \langle m \rangle$ means $n = km$ for some integer $k > 1$; this also is untenable, since n is prime, not composite. We therefore conclude that $(\langle n \rangle, +, \cdot)$ is a maximal ideal.

Example(13-3): Let R denote the collection of all functions $f: \mathbb{R} \rightarrow \mathbb{R}$.

For two such functions f and g , we have

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x)g(x), x \in \mathbb{R}.$$

Then $(R, +, \cdot)$ is a commutative ring with identity. Consider

$$M = \{f \in R: f(0) = 0\}.$$

The triple $(M, +, \cdot)$ forms an ideal of $(R, +, \cdot)$; we observe that it is a maximal ideal.

Remark(13-4): An element is invertible if and only if it belongs to no maximal ideal.

Definition(13-5): Let $(R, +, \cdot)$ be a ring and $a \in R$, then a is said to be an idempotent element, if $a^2 = a$.

Theorem(13-6): In a ring $(R, +, \cdot)$ having exactly one maximal ideal $(M, +, \cdot)$, the only idempotent elements are 0 and 1.

Proof: assume the theorem is false; that is, suppose there exists an idempotent $a \in R$ with $a \neq 0, 1$. The relation $a^2 = a$ implies $a \cdot (1 - a) = 0$, so that a and $1 - a$ are zero divisors. Hence, neither the element a nor $1 - a$ is invertible in R . But this means the principle ideals $(\langle a \rangle, +, \cdot)$ and $(\langle 1 - a \rangle, +, \cdot)$ are both proper ideals of the ring $(R, +, \cdot)$. As such, they must be contained in $(M, +, \cdot)$: $\langle a \rangle \subseteq M$ and $\langle 1 - a \rangle \subseteq M$, both a and $1 - a$ lie in M ,

$$1 = a + (1 - a) \in M$$

This leads at once to the contradiction $M = R$.

Theorem(13-7): Let $(I, +, \cdot)$ be a proper ideal of the commutative ring $(R, +, \cdot)$ with identity. Then $(I, +, \cdot)$ is a maximal ideal if and only if the quotient ring $(\frac{R}{I}, +, \cdot)$ is a field.

Proof: (\Rightarrow) let $(I, +, \cdot)$ be a maximal ideal of $(R, +, \cdot)$. Since $(R, +, \cdot)$ is a commutative ring with identity, the quotient ring $(\frac{R}{I}, +, \cdot)$ also has these

properties. If $a + I \neq 0 + I$, then $a \notin I$. The ideal $(\langle I, a \rangle, +, \cdot)$ generated by I and a must be the whole ring $(R, +, \cdot)$:

$$R = \langle I, a \rangle = \{i + r \cdot a : i \in I, r \in R\}.$$

The identity element 1 , $1 = i' + r' \cdot a$, $1 - r' \cdot a \in I$

$$1 + I = r' \cdot a + I = (r' + I) \cdot (a + I),$$

$r' + I = (a + I)^{-1}$. Hence $(\frac{R}{I}, +, \cdot)$ is a field.

(\Leftarrow) suppose $(\frac{R}{I}, +, \cdot)$ is a field and $(J, +, \cdot)$ is any ideal of $(R, +, \cdot)$ such that $I \subset J \subseteq R$. Since I is a proper subset of J , there exists an element $a \in J$ with $a \notin I$. The coset $a + I \neq 0 + I$. $(\frac{R}{I}, +, \cdot)$ is a field,

$$(a + I) \cdot (b + I) = 1 + I$$

for some coset $b + I \in \frac{R}{I}$. $1 - a \cdot b \in I \subset J$. But $a \cdot b \in J$, $1 \in J$, $J = R$.

Example(13-8): Consider the ring of even integers $(\mathbb{Z}_e, +, \cdot)$, a commutative ring without identity. In this ring, the principle ideal $(\langle 4 \rangle, +, \cdot)$ generated by the integer 4 is a maximal ideal.

Solution: if n is any element not in $\langle 4 \rangle$, then n is an even integer not divisible by 4; the greatest common divisor of n and 4 must be 2. We have

$$\langle\langle 4 \rangle, n\rangle = \langle 2 \rangle = \mathbb{Z}_e,$$

This reasoning shows that there is no ideal of $(\mathbb{Z}_e, +, \cdot)$ contained between $(\langle 4 \rangle, +, \cdot)$ and $(\mathbb{Z}_e, +, \cdot)$.

Now note that in $(\frac{\mathbb{Z}_e}{\langle 4 \rangle}, +, \cdot)$,

$$(2 + \langle 4 \rangle) \cdot (2 + \langle 4 \rangle) = 0 + \langle 4 \rangle.$$

The ring $(\frac{\mathbb{Z}_e}{\langle 4 \rangle}, +, \cdot)$ therefore has divisors of zero and cannot be a field.

Definition(13-9): Let $(R, +, \cdot)$ be a ring and $a \in R$, then a is said to be a nilpotent element, if there exists a positive integer n such that $a^n = 0$.

Example(13-10): Find the set of all nilpotent elements of $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Z}_9, +_9, \cdot_9)$.

Example(13-11): If $(R, +, \cdot)$ is an integral domain, then the zero element is the only nilpotent of R .

Example(13-12): The converse of example (13-13) is not true in general, for example $0 \in \mathbb{Z}_6$ is a nilpotent, but $(\mathbb{Z}_6, +_6, \cdot_6)$ is not an integral domain.

Example(13-13): Let $(R, +, \cdot)$ be a ring and $a \in R$. If a is a nilpotent and $a \neq 0$, then a is a zero divisor.

Example(13-14): The converse of example (13-15) is not true in general, for example $2 \in Z_6$ is a zero divisor, but it is not nilpotent.

Example(13-15): Find the set of idempotent elements in $(\mathbb{Z}, +, \cdot)$ and $(Z_6, +_6, \cdot_6)$.

Example(13-16): Find all the maximal ideals in $(Z_{12}, +_{12}, \cdot_{12})$.

14. Prime Ideals. Examples, Properties and Results.

Definition(14-1): An ideal $(I, +, \cdot)$ of the ring $(R, +, \cdot)$ is a prime ideal if for all $a, b \in R, a \cdot b \in I$ implies either $a \in I$ or $b \in I$.

Example(14-2): The prime ideals of the ring $(\mathbb{Z}, +, \cdot)$ are precisely the ideals $(\langle p \rangle, +, \cdot)$, where p is a prime number, together with the trivial ideals $(\{0\}, +, \cdot)$ and $(\mathbb{Z}, +, \cdot)$.

Theorem(14-3): A commutative ring with identity $(R, +, \cdot)$ is an integral domain if and only if the zero ideal $(\{0\}, +, \cdot)$ is a prime ideal.

Proof: (\Rightarrow) if $(R, +, \cdot)$ is an integral domain

Let $a, b \in R$ and $a \cdot b \in \{0\} \Rightarrow a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$, since

$(R, +, \cdot)$ is an integral domain $\Rightarrow a \in \{0\}$ or $b \in \{0\} \Rightarrow \{0\}$ is a prime ideal

(\Leftarrow) let $\{0\}$ is a prime ideal and $a.b = 0 \Rightarrow a.b \in \{0\} \Rightarrow$ either $a \in \{0\}$ or $b \in \{0\}$, since $\{0\}$ is a prime ideal $\Rightarrow a = 0$ or $b = 0 \Rightarrow (R, +, \cdot)$ is an integral domain.

Example(14-4): Let $(F, +, \cdot)$ be a field, then $(\{0\}, +, \cdot)$ and $(F, +, \cdot)$ are only prime ideals in $(F, +, \cdot)$.

Example(14-5): the triples $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ and $(\mathbb{Z}_p, +_p, \cdot_p)$, where p is a prime have trivial prime ideals.

Example(14-6): The prime ideals of $(\mathbb{Z}, +, \cdot)$ are $(\langle p \rangle, +, \cdot), (\{0\}, +, \cdot)$ and $(\mathbb{Z}, +, \cdot)$.

Example(14-7): In $(\mathbb{Z}_n, +_n, \cdot_n)$, an ideal $(\langle p \rangle, +, \cdot)$ is a prime.

Example(14-8): The prime ideals of $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ are $(\langle 2 \rangle, +_{12}, \cdot_{12})$ and $(\langle 3 \rangle, +_{12}, \cdot_{12})$.

Example(14-9): Find all prime and maximal ideals of $(\mathbb{Z}_{15}, +_{15}, \cdot_{15})$.

Theorem(14-10): Let $(I, +, \cdot)$ be a proper ideal of the commutative ring $(R, +, \cdot)$ with identity. Then $(I, +, \cdot)$ is a prime ideal if and only if the quotient ring $(\frac{R}{I}, +, \cdot)$ is an integral domain.

Proof: (\Rightarrow) take $(I, +, \cdot)$ is a prime ideal. Since $(R, +, \cdot)$ is a commutative ring with identity, so is the quotient ring $\left(\frac{R}{I}, +, \cdot\right)$. Assume that

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

$a \cdot b \in I$. Since $(I, +, \cdot)$ is a prime ideal, $a \in I$ or $b \in I$. But this means either $a + I = I$ or $b + I = I$, hence $\left(\frac{R}{I}, +, \cdot\right)$ is without zero divisors.

(\Leftarrow) suppose $\left(\frac{R}{I}, +, \cdot\right)$ is an integral domain and $a \cdot b \in I$.

$$(a + I) \cdot (b + I) = a \cdot b + I = I.$$

By hypothesis, $\left(\frac{R}{I}, +, \cdot\right)$ contains no divisors of zero, so that either $a + I = I$ or $b + I = I$. So $a \in I$ or $b \in I$, therefore $(I, +, \cdot)$ is a prime ideal.

Theorem(14-11): In a commutative ring with identity, every maximal ideal is a prime ideal.

Proof: Assume $(I, +, \cdot)$ is a maximal ideal of the ring $(R, +, \cdot)$ and that $a \cdot b \in I$ with $a \notin I$. $(I, +, \cdot)$ is a maximal implies that $R = \langle I, a \rangle$. Hence there exist elements $i \in I, r \in R$ for which

$$1 = i + r \cdot a.$$

Since both $a \cdot b$ and i are in I , we conclude

$$b = (i + r \cdot a) \cdot b = i \cdot b + r \cdot (a \cdot b) \in I,$$

from which it is clear that $(I, +, \cdot)$ is a prime ideal.

Example(14-12): The ring $(\mathbb{Z}_e, +, \cdot)$, where $(\langle 4 \rangle, +, \cdot)$ forms a maximal ideal which is not prime.

Theorem(14-13): Let $(R, +, \cdot)$ be a principal ideal domain. A (nontrivial) ideal of $(R, +, \cdot)$ is prime if and only if it is a maximal ideal.

Proof: (\Rightarrow) suppose $(I, +, \cdot)$ is any ideal with $\langle a \rangle \subset I \subseteq R$. Since $(R, +, \cdot)$ is a principal ideal ring, there exists $b \in R$ for which $I = \langle b \rangle$. Now $a \in I = \langle b \rangle$, hence $a = r \cdot b, r \in R$. But $(\langle a \rangle, +, \cdot)$ is a prime ideal, so either $r \in \langle a \rangle$ or $b \in \langle a \rangle$. $b \in \langle a \rangle$ leads to the contradiction $\langle b \rangle \subseteq \langle a \rangle$. Therefore $r \in \langle a \rangle$, which implies $r = s \cdot a, s \in R$, or $a = r \cdot b = (s \cdot a) \cdot b$. Since $a \neq 0$ and $(R, +, \cdot)$ is an integral domain, we have $1 = s \cdot b$. This means $1 \in \langle b \rangle = I$, or $I = R$. Since no ideal lies between $(\langle a \rangle, +, \cdot)$ and $(R, +, \cdot)$, we conclude that $(\langle a \rangle, +, \cdot)$ is a maximal ideal.

(\Leftarrow) from theorem (14-5).

Corollary(14-14): A nontrivial ideal of the ring $(\mathbb{Z}, +, \cdot)$ is prime if and only if it is maximal.

Definition(14-15): A nonzero element a of the ring $(R, +, \cdot)$ is called a prime element of R if a is not invertible and in every factorization $a = b \cdot c$ with $b, c \in R$, either b or c is invertible.

Theorem(14-16): Let $(R, +, \cdot)$ be a principal ideal domain. The ideal $(\langle a \rangle, +, \cdot)$ is a prime (maximal) ideal of $(R, +, \cdot)$ if and only if a is a prime element of R .

Proof: (\Leftarrow) suppose a is a prime element of R and $(I, +, \cdot)$ is any ideal for which $\langle a \rangle \subset I \subseteq R$. By hypothesis, $(R, +, \cdot)$ is a principal ideal ring, so there is $b \in R$ with $I = \langle b \rangle$. As $a \in \langle b \rangle$, $a = r \cdot b$ for some $r \in R$. Since a is a prime element that either r or b is invertible. $b = r^{-1} \cdot a \in \langle a \rangle$, which implies $I = \langle b \rangle \subseteq \langle a \rangle$, an obvious contradiction. The element b must be invertible, so that $\langle b \rangle = R$. This argument shows that $(\langle a \rangle, +, \cdot)$ is a maximal ideal of $(R, +, \cdot)$ and prime.

(\Rightarrow) Let $(\langle a \rangle, +, \cdot)$ be a prime ideal of $(R, +, \cdot)$. Assume that a is not a prime element of R . Then $a = b \cdot c$, where $b, c \in R$, and neither b nor c is invertible. Now if $b \in \langle a \rangle$, $b = r \cdot a$, $r \in R$, and $a = b \cdot c = (r \cdot a) \cdot c$. From the cancellation law, $r \cdot c = 1$. But this contradiction that c is invertible. By the same reasoning, if c lies in $\langle a \rangle$, then $b \cdot c \in \langle a \rangle$, with

$b \notin \langle a \rangle, c \notin \langle a \rangle$, $(\langle a \rangle, +, \cdot)$ is a prime ideal. Hence our supposition is false and a must be a prime element of R .

Definition(14-17): The radical of a ring $(R, +, \cdot)$, denoted by $\text{rad } R$, is the set

$$\text{rad } R = \bigcap \{M : (M, +, \cdot) \text{ is a maximal ideal of } (R, +, \cdot)\}.$$

If $\text{rad } R = \{0\}$, then we say $(R, +, \cdot)$ is a ring without radical or is a semisimple ring.

Example(14-18): The ring of integers $(\mathbb{Z}, +, \cdot)$ is a semisimple ring.

Solution: the maximal ideals of $(\mathbb{Z}, +, \cdot)$ are the principal ideals $(\langle p \rangle, +, \cdot)$, where p is a prime; that is,

$$\text{rad } \mathbb{Z} = \bigcap \{ \langle p \rangle : p \text{ a prime number} \}.$$

Since no nonzero integer is divisible by every prime, $\text{rad } \mathbb{Z} = \{0\}$.

Example(14-19): Find $\text{rad } (Z_{15})$ and $\text{rad } (Z_{23})$.

Definition(14-20): An ideal $(I, +, \cdot)$ of a ring $(R, +, \cdot)$ is called a primary ideal, if for all $a, b \in R$ such that $a, b \in I$, implies that, if $a \notin I$, then $b^n \in I$ or if $b \notin I$, then $a^n \in I$, for some $n \in \mathbb{Z}^+$.

Example(14-21): Show that, $(I = \langle 4 \rangle, +_{12}, \cdot_{12})$ is a primary ideal of $(Z_{12}, +_{12}, \cdot_{12})$.

Solution: $I = \langle 4 \rangle = \{0, 4, 8\}, Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$$2 \cdot_{12} 6 = 0 \in I \Rightarrow 6 \notin I, 2^2 = 4 \in I$$

$$10 \cdot_{12} 2 = 8 \in I \Rightarrow 2 \notin I, 10^2 = 4 \in I$$

$$6 \cdot_{12} 8 = 0 \in I \Rightarrow 6 \notin I, 8 \in I$$

$$6 \cdot_{12} 6 = 0 \in I \Rightarrow 6 \notin I, 6^2 = 0 \in I$$

$$4 \cdot_{12} 5 = 8 \in I \Rightarrow 5 \notin I, 4 \in I$$

⋮

Therefore, I is a primary ideal.

Theorem(14-22): Every prime ideal is a primary.

Proof: Let $(I, +, \cdot)$ be a prime ideal of a ring $(R, +, \cdot)$.

Let $a, b \in R$ such that $a \cdot b \in I$

If $a \notin I$, then $b \in I$ (since I is a prime ideal)

Thus, $b^n \in I$, so I is a primary ideal.

Example(14-23): Prove or disprove, every primary ideal is a prime.

Solution: In general, it is not true, for example: in $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ the ideal $(I = \langle 4 \rangle, +_{12}, \cdot_{12})$ is a primary ideal, but it's not a prime ideal, since $2 \cdot_{12} 2 = 4 \in I$, but $2 \notin I$.

Example(14-24): In a commutative ring with identity, every maximal ideal is a primary ideal. (**check**)

Theorem(14-25): Let $(I, +, \cdot)$ be a proper ideal of a commutative ring with identity $(R, +, \cdot)$, then I is a primary iff all zero divisors in $\frac{R}{I}$ are nilpotent elements.

Proof: \Rightarrow) suppose I is a primary.

Let $a + I \in \frac{R}{I}$ such that $a + I$ is a zero divisor

$\Rightarrow a + I \neq I, \exists b + I \neq I \in \frac{R}{I}$ such that $(a + I) \odot (b + I) = I \Rightarrow a \cdot b + I = I \Rightarrow a \cdot b \in I$

$b + I \neq I \Rightarrow b \notin I \Rightarrow a^n \in I$, for some $n \in \mathbb{Z}^+$ (since I is a primary ideal)

$\Rightarrow a^n + I = I \Rightarrow (a + I)^n = I$

So, all zero divisors in $\frac{R}{I}$ are nilpotent elements.

\Leftrightarrow) suppose all zero divisors in $\frac{R}{I}$ are nilpotent elements.

Let $a, b \in R$ such that $a, b \in I, a \notin I \Rightarrow a + I \neq I$

$a, b \in I \Rightarrow a \cdot b + I = I \Rightarrow (a + I) \odot (b + I) = I$

If $b + I = I \Rightarrow b \in I \Rightarrow I$ is a prime ideal $\Rightarrow I$ is a primary ideal.

If $b + I \neq I \Rightarrow b + I$ is a zero divisor $\Rightarrow b + I$ is a nilpotent element.

$\Rightarrow \exists n \in \mathbb{Z}^+$ such that $(b + I)^n = I \Rightarrow b^n + I = I \Rightarrow b^n \in I$

Thus, I is a primary ideal.