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

i. $(R, +)$ 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.

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

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

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

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

3. Let R denote the set of all functions $f: \mathbb{R} \longrightarrow \mathbb{R}$. 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 Hom G be the set of all homomorphisms from $(G, *)$ into itself. (Hom $G, \circ$) is a semigroup with identity, then the triple (Hom $G, +, \circ$) forms a ring with identity.

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

(Hom $G, +$) is a commutative group.

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

$$= \big(f(x) * g(x)\big) * \big(f(y) * g(y)\big) = (f+g)(x) * (f+g)(y),$$

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

$$[f\circ(g+h)](x) = f\big((g+h)(x)\big) = f\big(g(x) * h(x)\big)$$

$$= f\big(g(x)\big) * f(h(x))$$

$$= (f\circ g)(x) * (f\circ h)(x) = (f\circ g + f\circ h)(x).$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

<u>Corollary(2-2):</u> If $(R, +, \cdot)$ be a ring with identity and $R \neq \{0\}$, then $0 \neq 1$, $(-1) \cdot a = -a$

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

$a = a \cdot 1 = a \cdot 0 = 0 \Longrightarrow a = 0$, but $a \neq 0$ by assumption, thus $0 \neq 1$

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

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

<u>Corollary(2-3):</u> 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 $1 = 1\cdot 1^* = 1^*$

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

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

<u>Theorem(2-5):</u> 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 $a, b \in U \Longrightarrow \exists a^{-1}, b^{-1} \in U \ni a\cdot a^{-1} = a^{-1}\cdot a = 1$

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

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

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

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

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

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

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

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

$\Longrightarrow$ the operation of addition is a commutative on S

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

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

$\Longrightarrow$ $(S, +, \cdot)$ 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

$\cdot_6$	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

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

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

(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) $\left(S = \left\{a + b\sqrt{5} : a, b \in \mathbb{Z}\right\}, +, \cdot\right)$ is a subring of $(\mathbb{R}, +, \cdot)$.

(9) Let $(R, +, \cdot)$ be a ring and $M = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in R\}$, 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 $(Z_n, +_n, \cdot_n)$ 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 $(\mathbb{Z}, +, \cdot)$:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Thus, $r \cdot 1 = r \ \ \forall r \in R \Longrightarrow R \subseteq I$, but $I \subseteq R \Longrightarrow I = R$ 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 $(\bigcap I_i\,,+,\cdot)$.

Proof: $0 \in I_i \Longrightarrow 0 \in \bigcap I_i \Longrightarrow \bigcap I_i \neq \emptyset$

Let $a, b \in \bigcap I_i$ and $r \in R \Longrightarrow a, b \in I_i \Longrightarrow a - b, r \cdot a$ and $a \cdot r \in I_i$

$\Longrightarrow a - b, r \cdot a$ 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 $(Z_{12}, +_{12}, \cdot_{12})$

$\langle 4 \rangle = \{0,4,8\}, \langle 6 \rangle = \{0,6\} \Longrightarrow \langle 4 \rangle \cup \langle 6 \rangle = \{0,4,6,8\}$ 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

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

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

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

<u>Theorem(5-19):</u> 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 $0\neq m\in I \Longrightarrow -m\in I$, suppose n the least positive integer in I

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

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

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

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

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

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

Since $\langle a\rangle\subseteq\langle a_i\rangle[i=1,2,..,n], a=r_i\cdot a_i$ 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 $r \cdot b = r \cdot (s_i \cdot a_i) = (r \cdot s_i) \cdot a_i \in \langle a_i \rangle \Longrightarrow \langle b \rangle \subseteq \langle a_i \rangle$

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 cose $0+I=I$, 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

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

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

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.

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

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

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, $f: R \longrightarrow R'$. 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 $f: R \longrightarrow R'$ be the function that maps each element of R onto the zero element $0'$ of $(R', +', \cdot')$.

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

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

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

Example(7-3): The mapping $f: \mathbb{Z} \longrightarrow \mathbb{Z}_e$ 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 $(Z_n, +_n, \cdot_n)$, the ring of integers modulo n. Define $f: \mathbb{Z} \longrightarrow \mathbb{Z}_n$ 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 $f_a: R \longrightarrow R$ 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: $(2)\quad a + (-a) = 0$

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

<u>Theorem(7-7):</u> 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 $(R, +, \cdot)$.

<u>Theorem(7-8):</u> 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 $f:\mathbb{Z}\longrightarrow R$ 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.

Definition(7-11): A ring $(R,+,\cdot)$ is embedded in a ring $(R',+',\cdot')$ if there exists some subring $(S,+',\cdot')$ of $(R',+',\cdot')$ such that $(R,+,\cdot)\cong(S,+',\cdot')$.

Theorem(7-12): Any ring can be embedded in a ring with identity.

Proof: Let $(R,+,\cdot)$ be an arbitrary ring and

$$R\times\mathbb{Z}=\{(r,n): r\in R, n\in\mathbb{Z}\}$$

Define

$$(a,n)+(b,m)=(a+b,n+m),$$

$$(a,n)\cdot(b,m)=(a\cdot b+m\cdot a+n\cdot b,n\cdot m),$$

The triple $(R \times \mathbb{Z}, +, \cdot)$ forms a ring. This ring has multiplicative identity, namely the pair $(0,1)$; for

$$(a, n) \cdot (0,1) = (a \cdot 0 + 1 \cdot a + n \cdot 0, n \cdot 1) = (a, n),$$

$$(0,1) \cdot (a, n) = (a, n).$$

Next, consider the subset $R \times 0$ of $R \times \mathbb{Z}$ consisting of all pairs of the form $(a, 0)$. Since

$$(a, 0) - (b, 0) = (a - b, 0), \quad (a, 0) \cdot (b, 0) = (a \cdot b, 0)$$

Therefore, $(R \times 0, +, \cdot)$ is a subring of $(R \times \mathbb{Z}, +, \cdot)$.

The proof is completed by showing $(R \times 0, +, \cdot)$ is isomorphic to the given ring $(R, +, \cdot)$. To this end, define the function $f: R \longrightarrow R \times 0$ by taking

$$f(a) = (a, 0).$$

The function f is a one-to-one mapping of R onto the set $R \times 0$.

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

$$f(a \cdot b) = (a \cdot b, 0) = (a, 0) \cdot (b, 0) = f(a) \cdot f(b).$$

Thus, $(R, +, \cdot) \cong (R \times 0\ , +, \cdot)$.

8. Fundamental Theorems of Homomorphisms of Rings.

<u>Theorem(8-1):</u> (The first fundamental theorem of homomorphism of ring)

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

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

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

To prove that Ψ is well define

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

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

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

To prove that Ψ is a homomorphism

$$\Psi[(x+ker\varphi)+(y+ker\varphi)] = \Psi[(x+y)+ker\varphi]$$

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

Also

$$\Psi[(x+ker\varphi)\cdot(y+ker\varphi)]=\Psi[(x\cdot y)+ker\varphi]$$

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

To prove Ψ is an onto

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

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

To prove Ψ is an one-to-one

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

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

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

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

$$kerf=\{0,2\},\qquad \frac{Z_4}{kerf}=\{\{0,2\},\{1,3\}\}$$

The operation tables for the quotient ring $(\frac{Z_4}{kerf},+,\cdot)$ 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, $(\frac{Z_4}{kerf}, +, \cdot) \cong (Z_2, +_2, \cdot_2)$

<u>Theorem(8-3):</u> (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 $\varphi: H \longrightarrow \frac{(H+I)}{I}$ defined by $\varphi(a) = a + I \ \forall a \in H$

To prove that φ is a homomorphism

$$\forall a, b \in H, \varphi(a+b) = (a+b) + I = (a+I) + (b+I)$$

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

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

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

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

By the first theorem, we get

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

$$ker\varphi = \{x \in H: \varphi(x) = I\} = \{x \in H: x + I = I\} = \{x \in H: x \in I\}$$

$$= \{x \in H: x \in H \cap I\} = H \cap I$$

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

<u>Theorem(8-4):</u> 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 $y \in \varphi(R), \exists x \in R \ni y = \varphi(x)$

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

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

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

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

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

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

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

<u>Theorem(8-5):</u> (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 $\varphi: \frac{R}{J} \longrightarrow \frac{R}{I}$ defined by $\varphi(r + J) = r + I,\ \forall r \in R, r + J \in \frac{R}{J}$

To show that φ is a homomorphism

$$\varphi[(x + J) + (y + J)] = \varphi[(x + y) + J] = (x + y) + I$$

$$= (x + I) + (y + I) = \varphi(x + J) + \varphi(y + J)$$

Also

$$\varphi[(x+J)\cdot(y+J)] = \varphi[(x \cdot\cdot y)+J] = (x\cdot y)+I$$

$$= (x+I)\cdot(y+I) = \varphi(x+J)\cdot\varphi(y+J)$$

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

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

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

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

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

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

<u>**Theorem(9-1):**</u> 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 $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$.

Example(9-8): Let I, J, K be ideals in a ring $(R, +, \cdot)$ with $I \subseteq K$, then

$$I + (J \cap K) = (I + J) \cap K$$

Solution: let $x \in I + (J \cap K)$

$\Longrightarrow x = a + b \ni a \in I, b \in J \cap K \Longrightarrow b \in J, b \in K$

$b \in J \Longrightarrow x = a + b \in I + J,$ also

$b \in k, a \in I \subseteq K \Longrightarrow x = a + b \in K \Longrightarrow x = a + b \in (I + J) \cap K$

$\Longrightarrow I + (J \cap K) \subseteq (I + J) \cap K$

Let $y \in (I + J) \cap K \Longrightarrow y \in I + J, y \in K$

$\Longrightarrow y = a + b, a \in I, b \in J$

$I \subseteq K \Longrightarrow a \in K, b = y - a \in K \Longrightarrow b \in J \cap K$

$\Longrightarrow y = a + b \in I + (J \cap K)$

$\Longrightarrow (I + J) \cap K \subseteq I + (I \cap K)$

$\Longrightarrow \; I + (J \cap K) = (I + J) \cap K$

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:($\Longrightarrow$) 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 $b = c$

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

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

$b \neq 0 \Longrightarrow a = 0$

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.

Corollary(10-5): In an integral domain, all the nonzero elements have the same additive order, which is the characteristic of the domain.

Proof: suppose the integral domain $(R, +, \cdot)$ has positive characteristic n.

Any $a \in R (a \neq 0)$ will then possess a finite additive order m, with $m \leq n$.

But $0 = ma = (m1) \cdot a \Longrightarrow m1 = 0$, since $(R, +, \cdot)$ is free of zero divisors.

Corollary(10-6): 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.

$n = n_1 n_2$ 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(10-7): 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(10-8): 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(10-9): 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(10-10): The triple $(\mathbb{Z},+,\cdot)$ is an integral domain, since $(\mathbb{Z},+,\cdot)$ is a commutative with identity .

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

Example(10-11): 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 $[a],[b]\in Z_p\ni[a]\cdot_p[b]=[0]\Longrightarrow[a\cdot b]=[0]\Longrightarrow\frac{p}{a\cdot b}$

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

Example(10-12): $(M_n(R),+,\cdot)$ is not an integral domain, since it is not commutative ring.

Example(10-13): Solve the equation $x^2-4x+3=0$ in a ring $(Z_{12},+_{12},\cdot_{12})$.

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

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

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

Since

$$2 \cdot_{12} 6 = 3 \cdot_{12} 4 = 3 \cdot_{12} 8 = 4 \cdot_{12} 9 = 6 \cdot_{12} 6 = 6 \cdot_{12} 8 = 6 \cdot_{12} 10$$
$$= 9 \cdot_{12} 8 = 0$$

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(10-14): 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 $x = 0 \Longrightarrow x^5 = 0 \Longrightarrow y^5 = 0 \Longrightarrow y = 0.$

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

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

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

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

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

By $(*)$, we get

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

Corollary(10-15): Let $(R, +,\cdot)$ be a ring with identity and $u \in R$ is an invertible, then u is not zero divisor.

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

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

Also,

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

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

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.

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

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

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

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

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

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

Example(11-5): The field 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

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

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

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

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

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

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

$\Longrightarrow [s]$ 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

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

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

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

<u>Theorem(11-10):</u> 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.

<u>Theorem(12-1):</u> 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 $0 < a < n.gcm(a,n) = 1 \Longrightarrow \exists r, s \in \mathbb{Z} \ni a \cdot r + n \cdot s = 1$

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

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: $(\Longrightarrow)$ 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 $(R, +, \cdot) \Longrightarrow I \neq \{0\}$ and $I \neq R$

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

But, this is contradiction.

$(\Longleftarrow)$ 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 $1 \in \langle a\rangle, \exists r' \in R \ni r' \cdot a = 1$

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

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

Theorem(12-7): Let f be a homomorphism from the field $(F, +,\cdot)$ onto the field $(F', +',\cdot')$. Then either f is the trivial homomorphism or else $(F, +,\cdot)$ and $(F', +',\cdot')$ are isomorphic.

Proof: since $(kerf, +,\cdot)$ is an ideal of $(F, +,\cdot)$, either $kerf = \{0\}$ or $kerf = F$.

If $kerf = \{0\} \Longrightarrow f$ is a one-to-one, in which case $(F, +,\cdot) \cong (F', +',\cdot')$ via f.

If $kerf = F$, then each element of $(F, +,\cdot)$ must map onto zero; that is, f is the trivial homomorphism.

Definition(12-8): By a subfield of the field $(F, +,\cdot)$ is meant any subring $(F', +,\cdot)$ of $(F, +,\cdot)$ which is itself a field.

Example(12-9): The ring $(\mathbb{Q}, +, \cdot)$ is a subfield of the field $(\mathbb{R}, +, \cdot)$.

Theorem(12-10): 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 $a \cdot b^{-1} \in F'$.

Theorem(12-11): Let the integral domain $(R, +, \cdot)$ be a subring of the field $(F, +, \cdot)$. If the set F' is defined by

$$F' = \{a \cdot b^{-1} : a, b \in R; b \neq 0\},$$

then the triple $(F', +, \cdot)$ forms a subfield of $(F, +, \cdot)$ such that $R \subseteq F'$. In fact, $(F', +, \cdot)$ is the smallest subfield containing R.

Proof: if $a, b \in R$ with $b \neq 0$, $a \cdot b^{-1} \in F$

Since $1 = 1 \cdot 1^{-1} \in F', F' \neq \emptyset$

Let $x, y \in F'$, we have

$$x = a \cdot b^{-1}, y = c \cdot d^{-1}, a, b, c, d \in R, b \neq 0, d \neq 0$$

$$x - y = (a \cdot d - b \cdot c) \cdot (b \cdot d)^{-1} \in F'$$

If $y \neq 0, c \neq 0$,

$$x \cdot y^{-1} = (a \cdot d) \cdot (c \cdot b)^{-1} \in F'$$

Note(12-12): Let $(R, +, \cdot)$ be an integral domain and K the set of ordered pairs,

$$K = \{(a, b): a, b \in R; b \neq 0\}.$$

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

Theorem(12-13): The relation $\equiv$ is an equivalence relation in K.(**check** 1,2)

That is to say

(1) $(a, b) \equiv (a, b)$,

(2) If $(a, b) \equiv (c, d)$, then $(c, d) \equiv (a, b)$,

(3) If $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$, then $(a, b) \equiv (e, f)$.

The least obvious statement is (3). In this case, the hypothesis $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$ implies that

$$a \cdot d = b \cdot c, \ c \cdot f = d \cdot e.$$

Multiplying the first of these equations by f and the second by b, we obtain

$$a \cdot d \cdot f = b \cdot c \cdot f = b \cdot d \cdot e,$$

and, from the commutativity of multiplication, $a \cdot f \cdot d = b \cdot e \cdot d$. Since $d \neq 0$, this factor may be cancelled to yield $a \cdot f = b \cdot e$. But then $(a, b) \equiv (e, f)$.

Note(12-14): We label those elements which are equivalent to the pair (a, b) by the symbol $[a, b]$; in other words,

$$[a, b] = \{(c, d) \in K : (a, b) \equiv (c, d)\}$$

$$= \{(c, d) \in K : a \cdot d = b \cdot c\}.$$

$$[a, b] +' [c, d] = [a \cdot d + b \cdot c, b \cdot d],$$

$$[a, b] \cdot' [c, d] = [a \cdot c, b \cdot d].$$

let $[a, b] = [a', b']$ and $[c, d] = [c', d']$. From the equations

$$a \cdot b' = b \cdot a', \qquad c \cdot d' = d \cdot c'$$

it follows that

$$(a \cdot d + c \cdot b) \cdot (b' \cdot d') - (a' \cdot d' + c' \cdot b') \cdot (b \cdot d)$$

$$= (a \cdot b' - b \cdot a') \cdot (d \cdot d') + (c \cdot d' - d \cdot c') \cdot (b \cdot b')$$

$$= 0 \cdot (d \cdot d') + 0 \cdot (b \cdot b') = 0$$

Thus, by the definition of equality of classes,

$$[a \cdot d + c \cdot b, b \cdot d] = [a' \cdot d' + c' \cdot b', b' \cdot d'],$$

Proving addition to be well-defined. In much the same way, one can show that

$$[a \cdot c, b \cdot d] = [a' \cdot c', b' \cdot d'].$$

Lemma(12-15): The triple $(F, +', \cdot')$ is a field, generally known as the field of quotients of the integral domain $(R, +, \cdot)$.

Proof: the multiplicative identity , where a is any nonzero element is

$$[a, a] \cdot' [c, d] = [a \cdot c, a \cdot d] = [c, d]$$

with $[c, d]$ in F.

$[0, b]$ as the zero element while $[-a, b]$ is the negative of $[a, b]$.

To show $[a, b] \neq [0, b], a \neq 0$ has an inverse under multiplication.

$$[a, b] \cdot' [b, a] = [a \cdot b, b \cdot a] = [a \cdot b, a \cdot b].$$

Since $a \cdot b \neq 0$, $[a \cdot b, a \cdot b]$ is the identity element, so that $[a, b]^{-1} = [b, a]$.

Theorem(12-16): The integral domain $(R, +,\cdot)$ can be embedded in its field of quotients $(F, +', \cdot')$.

Proof: Consider the subset F' of F consisting of all element of the form $[a, 1]$,

Where 1 is the multiplicative identity of $(R, +,\cdot)$:

$$F' = \{[a, 1]: a \in R\}$$

Let $f: R \longrightarrow F'$ be the onto mapping defined by

$$f(a) = [a, 1], \forall a \in R$$

Since $[a, 1] = [b, 1]$ implies $a \cdot 1 = 1 \cdot b$ or $a = b$, we see that f is a one-to-one function.

$$f(a + b) = [a + b, 1] = [a, 1] +' [b, 1] = f(a) +' f(b),$$

$$f(a \cdot b) = [a \cdot b, 1] = [a, 1] \cdot' [b, 1] = f(a) \cdot' f(b).$$

Therefore, $(R, +,\cdot) \cong (F, +', \cdot')$.

Note(12-17): Any member $[a, b]$ of F can be written in the form

$$[a,b]=[a,1]\cdot'[1,b]=[a,1]\cdot'[b,1]^{-1}.$$

Note(12-18): It should also be observed that for any $a\neq 0$, we have

$$[a,1]\cdot'[b,a]=[a\cdot b,a]=[b,1].$$

Note(12-19): The field of quotients constructed from the integral domain $(\mathbb{Z},+,\cdot)$ is, of course, the rational number field $(\mathbb{Q},+,\cdot)$.

Definition(12-20): A field which does not have any proper subfields is called a prime field.

Example(12-21): 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 $a\cdot a^{-1}=1$.

$n=n\cdot 1^{-1}\in F\ \forall n\in\mathbb{Z}$: 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(12-22): For every prime p, the field $(Z_p,+_p,\cdot_p)$ of integers modulo p is a prime field. The reasoning here depends on the fact that the additive group $(Z_p, +_p)$ of $(Z_p, +_p, \cdot_p)$ is a finite group of prime order, and therefore has no nontrivial subgroups.

Theorem(12-23): Any prime field $(F, +, \cdot)$ is isomorphic either to $(\mathbb{Q}, +, \cdot)$, the field of rational numbers, or to one of the fields $(Z_p, +_p, \cdot_p)$, where p is a prime number.

Proof: let 1 be the identity element of $(F, +, \cdot)$ and define the mapping $f: \mathbb{Z} \longrightarrow F$ by

$$f(n) = n1 \ \ \forall n \in \mathbb{Z}$$

Then f is a homomorphism from $(\mathbb{Z}, +, \cdot)$ onto the subring $(f(\mathbb{Z}), +, \cdot)$ consisting of integral multiples of 1, we see that

$$(\frac{\mathbb{Z}}{kerf}, +, \cdot) \cong (f(\mathbb{Z}), +, \cdot).$$

But the triple $(kerf, +, \cdot)$ is an ideal of $(\mathbb{Z}, +, \cdot)$ a principal ideal ring, $kerf = \langle n \rangle$ for some nonnegative integer n. if $n \neq 0$, then n must in fact be a prime. Suppose $n = n_1 n_2$ where $1 < n_i < n (i = 1,2)$. Since $n \in kerf$,

$$(n_1 1) \cdot (n_2 1) = (n_1 n_2) 1 = n1 = 0,$$

yielding the contradiction that the field $(F,+,\cdot)$ has divisors of zero.

Therefore, n is the characteristic of $(F,+,\cdot)$ and as such must be prime. So

(1) $(f(\mathbb{Z}),+,\cdot) \cong \left(\frac{\mathbb{Z}}{\langle p\rangle},+,\cdot\right) = (Z_p,+_p,\cdot_p)$ for some prime p, or

(2) $(f(\mathbb{Z}),+,\cdot) \cong \left(\frac{\mathbb{Z}}{\langle 0\rangle},+,\cdot\right) = (\mathbb{Z},+,\cdot)$.

Suppose first that $(f(\mathbb{Z}),+,\cdot) \cong (Z_p,+_p,\cdot_p)$ the subring $(f(\mathbb{Z}),+,\cdot)$ must itself be a field. But $(F,+,\cdot)$ contains no proper subfield. $f(\mathbb{Z}) = F$ and $(F,+,\cdot) \cong (Z_p,+_p,\cdot_p)$.

Next, $(f(\mathbb{Z}),+,\cdot) \cong (\mathbb{Z},+,\cdot)$, the subring $(f(\mathbb{Z}),+,\cdot)$ is an integral domain, but not a field. The hypothesis $(F,+,\cdot)$ is a prime field, then implies

$$F = \{a \cdot b^{-1} : a,b \in f(\mathbb{Z}); b \neq 0\}$$

$$= \{(n1)\cdot(m1)^{-1} : n,m \in \mathbb{Z}; m \neq 0\}.$$

The fields $(F,+,\cdot)$ and $(\mathbb{Q},+,\cdot)$ are isomorphic under the mapping $g\left(\frac{n}{m}\right) = (n1)\cdot(m1)^{-1}$.

Corollary(12-24): Every field contains a subfield which isomorphic either to the field $(\mathbb{Q},+,\cdot)$ or to one of the fields $(Z_p,+_p,\cdot_p)$, 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: $(\Longrightarrow)$ 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

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

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

$(\Longleftarrow)$ 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 $f: \mathbb{R} \longrightarrow \mathbb{R}$. 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.

Zorns Lemma(13-4): Let M be a nonempty family of subsets of some fixed set with the property that for each chain χ in M, the union $\bigcup \chi$ also belongs to M. Then M contains a set which is maximal in the sense that it is not properly contained in any member of M.

Theorem(13-5): (Krull-Zorn). In a commutative ring with identity, each proper ideal is contained in a maximal ideal.

Proof: let $(I,+,\cdot)$ be any proper ideal of $(R,+,\cdot)$. Define

$$M=\{J: I\subseteq J; (J,+,\cdot) \text{ is a proper ideal of } (R,+,\cdot)\}.$$

$M\neq\emptyset$, since $I\in M$. Let a chain $\{I_i\}$ in M. Notice that $\bigcup I_i\neq R$, since $1\notin I_i$ for any i.

Let $a,b\in\bigcup I_i$ and $r\in R\Longrightarrow\exists i,j$ for which $a\in I_i, b\in I_j$

The collection $\{I_i\}$ forms a chain, either $I_i\subseteq I_j$ or else $I_j\subseteq I_i$; say, for definiteness, $I_i\subseteq I_j$. But $(I_j,+,\cdot)$ is an ideal, so $a-b\in I_j\subseteq\bigcup I_i$. For the same reason , $r\cdot a\in I_j$. This shows the triple $(\bigcup I_i\,,+,\cdot)$ to be a proper ideal of the ring $(R,+,\cdot)$. $I\subseteq\bigcup I_i$, hence $\bigcup I_i\in M$.

Thus, on the basis of Zorns Lemma, M contains a maximal element N. The triple $(N,+,\cdot)$ is a proper ideal of the ring $(R,+,\cdot)$ with $I\subseteq N$. $(N,+,\cdot)$ is a maximal ideal. To see this, suppose $(J,+,\cdot)$ is any ideal of $(R,+,\cdot)$ for which $N\subset J\subseteq R$. Since N is a maximal element of M, the set $J\notin M$, the ideal $(J,+,\cdot)$ must be improper, which implies $J=R$. We therefore conclude $(N,+,\cdot)$ is a maximal ideal of $(R,+,\cdot)$.

<u>Corollary(13-6):</u> An element is invertible if and only if it belongs to no maximal ideal.

Definition(13-7): Let $(R,+,\cdot)$ be a ring and $a \in R$, then a is said to be an idempotent element, if $a^2 = a$.

Theorem(13-8): 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(13-9): 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 $\left(\frac{R}{I},+,\cdot\right)$ is a field.

Proof: ($\Longrightarrow$) let $(I,+,\cdot)$ be a maximal ideal of $(R,+,\cdot)$. Since $(R,+,\cdot)$ is a commutative ring with identity, the quotient ring $\left(\frac{R}{I},+,\cdot\right)$ 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 $\left(\frac{R}{I},+,\cdot\right)$ is a field.

($\Longleftarrow$) suppose $\left(\frac{R}{I},+,\cdot\right)$ 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 $a+I\neq 0+I$. $\left(\frac{R}{I},+,\cdot\right)$ 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 $a\cdot b\in J, 1\in J, J=R$.

<u>**Example(13-10):**</u> 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 $\left(\frac{\mathbb{Z}_e}{\langle 4\rangle}, +,\cdot\right)$,

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

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

Definition(13-10): 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(13-11): Find the set of all nilpotent elements of $(\mathbb{Z}, +,\cdot)$ and $(Z_9, +_9,\cdot_9)$.

Example(13-12): If $(R, +,\cdot)$ is an integral domain, then the zero element is the only nilpotent of R.

Example(13-13): The converse of example (13-12) is no true in general, for example $0 \in Z_6$ is a nilpotent, but $(Z_6, +_6,\cdot_6)$ is not an integral domain.

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

Example(13-16): Find the set of idempotent elements in $(\mathbb{Z},+,\cdot)$ and $(Z_6,+_6,\cdot_6)$.

Example(13-17): 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: $(\Longrightarrow)$ if $(R,+,\cdot)$ is an integral domain

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

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

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

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

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

<u>Example(14-7):</u> In $(Z_n, +_n,\cdot_n)$, an ideal $(\langle p\rangle, +,\cdot)$ is a prime.

<u>Example(14-8):</u> The prime ideals of $(Z_{12}, +_{12},\cdot_{12})$ are $(\langle 2\rangle, +_{12},\cdot_{12})$ and $(\langle 3\rangle, +_{12},\cdot_{12})$.

<u>Example(14-9):</u> Find all prime and maximal ideals of $(Z_{15}, +_{15},\cdot_{15})$.

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 $\left(\frac{R}{I},+,\cdot\right)$ is an integral domain.

Proof: $(\Longrightarrow)$ 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.

$(\Longleftarrow)$ 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.

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

<u>**Theorem(14-13):**</u> 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: $(\Longrightarrow)$ 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.

($\Longrightarrow$) 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 rad R, is the set

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

If 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, rad $\mathbb{Z} = \{0\}$.

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

Theorem(14-20): Let $(I,+,\cdot)$ be an ideal of the ring$(R,+,\cdot)$. Then the set $I \subseteq \text{rad}\, R$ if and only if each element of the coset $1+I$ has an inverse in R.

Proof: $(\Longrightarrow)$ assume that $I \subseteq \text{rad}\, R$ and that there is $a \in I$, for which $1+a$ is not invertible. The element $1+a$ must belong to some maximal ideal $(M,+,\cdot)$ of the ring $(R,+,\cdot)$. Since $a \in \text{rad}\, R$, $a \in M$, and therefore $1=(1+a)-a \in M$. But this means $M=R$, which is clearly impssible.

$(\Longleftarrow)$ suppose each element of the coset $1+I$ has an inverse in R, but $I \nsubseteq \text{rad}\, R$. There exist a maximal ideal $(M,+,\cdot)$ of $(R,+,\cdot)$ with $I \nsubseteq M$. If $a \in I, a \notin M$, $\langle M,a \rangle = R$.

$$1 = m + r \cdot a$$

Let $m \in M, r \in R$, $m = 1 - r \cdot a \in 1 + I$, so that m possesses an inverse. The conclusion is untenable, since no proper ideal contains an invertible element.

Theorem(14-21): In any ring $(R,+,\cdot)$ an element $a \in \text{rad}\, R$ if and only if $1 + r \cdot a$ has an inverse for each $r \in R$.

Corollary(14-22): An element a is invertible in the ring $(R,+,\cdot)$ if and only if the coset $a+\text{rad}\,R$ is invertible in the quotient ring $\left(\frac{R}{\text{rad}\,R},+,\cdot\right)$.

Proof: ($\Leftarrow$) assume the coset $a+\text{rad}\,R$ has an inverse in $\left(\frac{R}{\text{rad}\,R},+,\cdot\right)$, so that

$$(a+\text{rad}\,R)\cdot(b+\text{rad}\,R)=1+\text{rad}\,R$$

for some $b\in R$. Then $a\cdot b-1\in\text{rad}\,R$. With r = 1, to conclude that $a\cdot b=1+1\cdot(a\cdot b-1)$ is invertible: this means a has an inverse.

($\Longrightarrow$) (**check**)

Corollary(14-23): The only idempotent in the radical of the ring $(R,+,\cdot)$ is 0.

Proof: let $a\in\text{rad}\,(R)$ with $a^2=a$. Taking $r=-1$ in the preceding theorem, we see that $1-a$ has an inverse in R; say

$$(1-a)\cdot b=1, b\in R$$

$$a=a^2+a\cdot b-a\cdot b=a\cdot(a+a\cdot b-b)=a\cdot(a-1)=0$$

Corollary(14-24): Let N denote the set of all noninvertible elements of R. Then the triple $(N,+,\cdot)$ is an ideal of the ring $(R,+,\cdot)$ if and only if $N = \text{rad } R$.

Proof: $(\Longrightarrow)$ $\text{rad } R \subseteq N$ clearly holds. Suppose $\mathrm{a} \in \mathrm{N}$. $(N,+,\cdot)$ is an ideal of the ring $(R,+,\cdot)$, then $\mathrm{r} \cdot \mathrm{a} \in \mathrm{N}, \mathrm{r} \in \mathrm{R}$. $1 + \mathrm{r} \cdot \mathrm{a} \notin \mathrm{N}$, for otherwise

$$1 = (1 + \mathrm{r} \cdot \mathrm{a}) - (\mathrm{r} \cdot \mathrm{a}) \in \mathrm{N}$$

So $1 + \mathrm{r} \cdot \mathrm{a}$ must be invertible, $\mathrm{a} \in \text{rad } R$. This shows $\mathrm{N} \subseteq \text{rad } R$, then $\mathrm{N} = \text{rad } R$.

$(\Longleftarrow)$ is clear.

Theorem(14-25): For any ring $(R,+,\cdot)$, the quotient ring $\left(\frac{R}{\text{rad } R},+,\cdot\right)$ is semisimple.

Proof: suppose $\mathrm{a} + I \in \text{rad } (\frac{R}{I})$

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

is invertible in $\frac{R}{I}$ for each $r \in R$. There exists a coset $b + I$, such that

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

$$b + a \cdot r \cdot b - 1 \in I = \text{rad } R$$

$$b + a \cdot r \cdot b = 1 + 1 \cdot (b + a \cdot r \cdot b - 1)$$

has an inverse $c \in R$. But

$$(1 + r \cdot a) \cdot (b \cdot c) = (b + a \cdot r \cdot b) \cdot c = 1$$

so that $1 + r \cdot a$ is invertible in R. $a \in \text{rad } R$.

Definition(14-26): 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(14-27): Show that, $(I = \langle 4 \rangle, +_{12}, \cdot_{12})$ is a primary ideal of $(Z_{12}, +_{12}, \cdot_{12})$.

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

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

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

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

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

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

⋮

Therefore, I is a primary ideal.

Theorem(14-28): 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 $a.b \in I$

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(14-29): Prove or disprove, every primary ideal is a prime.

Solution: In general, it is not true, for example: in $(Z_{12}, +_{12}, \cdot_{12})$ 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(14-30): Every maximal ideal is a primary ideal. (**check**)

Theorem(14-31): 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: $\Longrightarrow$) suppose I is a primary.

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

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

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

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

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

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

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

$a, b \in I \Longrightarrow a.b + I = I \Longrightarrow (a + I) \odot (b + I) = I$

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

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

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

Thus, I is a primary ideal.

15. Polynomials Rings. Examples and Basic Properties.

Definition(15-1): For an arbitrary ring $(R,+,\cdot)$. The set of polynomials over R may be regarded as the set

$$\text{poly } R = \{(a_0, a_1, \dots, a_n, 0,0, \dots) : a_k \in R, n \geq 0\}$$

$$f = (a_0, a_1, a_2, \dots) \text{ and } g = (b_0, b_1, b_2, \dots)$$

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots).$$

$$f \cdot g = (a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, \dots)$$

$$= (c_0, c_1, c_2, \dots),$$

Where

$$c_k = \sum_{i+j=k} a_i \cdot b_j = a_0 \cdot b_k + a_1 \cdot b_{k-1} + \cdots + a_k \cdot b_0$$

Theorem(15-2): The triple $(\text{poly } R,+,\cdot)$ forms a ring, known as the ring of polynomials over R. Furthermore, the ring $(\text{poly } R,+,\cdot)$ is commutative with identity if and only if $(R,+,\cdot)$ is a commutative ring with identity.

Definition(15-3): If $f(x) = a_0 + a_1 x + \cdots + a_n x^n, a_n \neq 0$ is a nonzero polynomial in $R[x]$(the set of $\text{poly } R$), we call the coefficient a_n the leading coefficient of $f(x)$ and the integer n, the degree of the polynomial.

Theorem(15-4): Let $(R,+,\cdot)$ be an integral domain and $f(x), g(x)$ be two nonzero elements of $(R[x],+,\cdot)$. Then

(1) deg $\left(f(x)\cdot g(x)\right) \leq$deg$f(x)$ +deg$g(x)$, and

(2) either $f(x)+g(x)=0$ or deg $(f(x)+g(x)) \leq$ max{deg$f(x)$,deg$g(x)$}.

Example(15-5): Consider $(Z_8,+_8,\cdot_8)$. Taking

$$f(x)=1+2x,$$

$$g(x)=4+x+4x^2$$

we then have $f(x)\cdot g(x)=4+x+6x^2$, so that

$$\deg\left(f(x)\cdot g(x)\right)=2<1+2=\deg f(x)+\deg g(x).$$

Theorem(15-6): (Division Algorithm). Let $(R,+,\cdot)$ be a commutative ring with identity and $f(x), g(x)\neq 0$ be polynomials in $R[x]$, with the leading coefficient of $g(x)$ an invertible element. Then there exist unique polynomials $q(x), r(x)\in R[x]$ such that

$$f(x)=q(x)\cdot g(x)+r(x),$$

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

Theorem(15-7): (Remainder Theorem). Let $(R,+,\cdot)$ be a commutative ring with identity. If $f(x) \in R[x]$ and $a \in R$, then there is a unique polynomial $q(x)$ in $R[x]$ such that $f(x) = (x-a)\cdot q(x) + f(a)$.

Proof: Applying the division algorithm to $f(x)$ and $x-a$, we obtain

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

where $r(x) = 0$ or deg $r(x) <$ deg $(x-a) = 1$. It follows in either case that $r(x)$ is a constant polynomial $r \in R$. Substituting a for x, we have

$$f(a) = (a-a)\cdot q(a) + r(a) = 0 + r = r.$$

Corollary(15-8): (Factorization Theorem). The polynomial $f(x) \in R[x]$ is divisible by $x-a$ if and only if a is a root of $f(x)$.

Proof: since $f(x) = (x-a)\cdot q(x)$ if and only if $f(a) = 0$.

Theorem(15-9): Let $(R,+,\cdot)$ be an integral domain and $f(x) \in R[x]$ be a nonzero polynomial of degree n. Then $f(x)$ has at most n distinct roots in R.

Proof: when $\deg f(x) = 0$, the result is trivial, since $f(x)$ cannot have any roots. If $\deg f(x) = 1$, say $f(x) = ax + b, a \neq 0$, then $f(x)$ has at most one root; indeed, if a is invertible, $-a^{-1}\cdot b$ is only root of $f(x)$.

Now, suppose the theorem is true for all polynomials of degree $n-1 \geq 1$, and let deg $f(x) = n$. If $f(x)$ has a root r, then

$$f(x) = (x-r) \cdot q(x),$$

where the polynomial $q(x)$ has degree $n-1$. Any root r_1 of $f(x)$ distinct from r must be a root of $q(x)$, for, by substitution

$$f(r_1) = (r_1 - r) \cdot q(r_1) = 0$$

and, since $(R,+,\cdot)$ has no zero divisors, $q(r_1) = 0$. $q(x)$ has at most $n-1$ distinct roots. As the only roots of $f(x)$ are r and those of $q(x)$, $f(x)$ cannot have more than n distinct roots in R.

<u>**Corollary(15-10):**</u> Let $f(x)$ and $g(x)$ be nonzero polynomials of degree $\leq n$ over the integral domain $(R,+,\cdot)$. If there exist $n+1$ distinct elements $a_k \in R(k = 1,2,\dots,n+1)$ for which$f(a_k) = g(a_k)$, then $f(x) = g(x)$.

Proof: the polynomial $h(x) = f(x) - g(x)$ is such that deg $h(x) \leq n$ and has at least $n+1$ distinct roots in R. This is impossible unless $h(x) = f(x) - g(x) = 0$, or $f(x) = g(x)$.

Example(15-11): Consider the polynomial $x^p - x \in Z_p[x]$, where p is a prime number. Since the nonzero elements of $(Z_p, +_p, \cdot_p)$ form a cyclic group, under multiplication, of order $p-1$, we must have $a^{p-1} = 1$ or $a^p = a$ for every $a \neq 0$. But the last equation clearly holds when $a = 0$, so that every element of Z_p is a root of the polynomial $x^p - x$.

Theorem(15-12): Let $(\mathbb{C}, +, \cdot)$ be the field of complex numbers. If $f(x) \in \mathbb{C}[x]$ is a polynomial of positive degree, then $f(x)$ has at least one root in $\mathbb{C}$.

Corollary(15-13): If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree $n > 0$, then $f(x)$ can be expressed in $\mathbb{C}[x]$ as a product of n (not necessarily distinct) linear factors.

Theorem(15-14): If $(F, +, \cdot)$ is a field, then the ring $(F[x], +, \cdot)$ is a principal ideal domain.

Proof: $(F[x], +, \cdot)$ is an integral domain. To see that any ideal $(I, +, \cdot)$ of $(F[x], +, \cdot)$ is principal. If $I = \{0\}$, the result is trivially true, since $I = \langle 0 \rangle$. Otherwise, there is some nonzero polynomial $p(x)$ of lowest degree in I. For each polynomial $f(x) \in I$, we may use the Division Algorithm to write $f(x) = q(x) \cdot p(x) + r(x)$, where either $r(x) = 0$ or deg $r(x) <$

deg $p(x)$. Now, $r(x) = f(x) - q(x) \cdot p(x)$ lies in I; if the degree of $r(x)$ were less than that of $p(x)$, a contradiction to the choice of $p(x)$.$r(x) = 0$ and $f(x) = q(x) \cdot p(x) \in \langle p(x) \rangle$; hence, $I \subseteq \langle p(x) \rangle$. But the opposite inclusion clearly holds, so that $I = \langle p(x) \rangle$.

Corollary(15-15): A nontrivial ideal of $(F[x], +, \cdot)$ is maximal if and only if it is a prime ideal.

Definition(15-16): A nonconstant polynomial $f(x) \in F[x]$ is said to be irreducible in $F[x]$ if and only if $f(x)$ cannot be expressed as the product of two polynomials of positive degree. Otherwise, $f(x)$ is reducible in $F[x]$.

Example(15-17): Any linear polynomial $f(x) = ax + b, a \neq 0$, is irreducible in $F[x]$. Indeed, since the degree of a product of two nonzero polynomials is the sum of the degree of the factors, it follows that a representation

$$ax + b = g(x) \cdot h(x),$$

with $0 < \deg g(x) < 1, 0 < \deg h(x) < 1$ is impossible. Thus, every reducible polynomial has degree at least 2.

Example(15-18): The polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, where $(\mathbb{Q}, +, \cdot)$ is the field of rational numbers. Otherwise, we have

$$x^2 - 2 = (ax + b) \cdot (cx + d)$$

$$= (ac)x^2 + (ad + bc)x + bd,$$

where the coefficients $a, b, c, d \in \mathbb{Q}$. Accordingly,

$$ac = 1, \;\; ad + bc = 0, \;\; bd = -2,$$

$c = \frac{1}{a}, d = \frac{-2}{b}$. Substituting in the relation $ad + bc = 0$, we obtain

$$0 = \frac{-2a}{b} + \frac{b}{a} = \frac{(-2a^2 + b^2)}{ab}$$

Thus, $-2a^2 + b^2 = 0$, or $(\frac{b}{a})^2 = 2$, which is impossible because $\sqrt{2}$ is not a rational number.

Theorem(15-19): If $(F, +, \cdot)$ is a field, the following statements are equivalent:

(1) $f(x)$ is an irreducible polynomial in $F[x]$.

(2) The principal ideal $(\langle f(x) \rangle, +, \cdot)$ is a maximal (prime) ideal of $(F[x], +, \cdot)$.

(3) The quotient ring $\left(\frac{F[X]}{\langle f(x)\rangle},+,\cdot\right)$ is a field.

Theorem(15-20): (Unique Factorization Theorem). Each polynomial $f(x) \in F[x]$ of positive degree is the product of a nonzero element of F and irreducible monic polynomial of $F[x]$.

Corollary(15-21): If $f(x) \in \mathbb{R}[x]$ is of positive degree, then $f(x)$ can be factored into linear and irreducible quadratic factors.

Theorem(15-22): (Kronecker). If $f(x)$ is an irreducible polynomial in $F[x]$, then there is an extension field of $(F,+,\cdot)$ in which $f(x)$ has a root.

Corollary(15-23): If the polynomial $f(x) \in F[x]$ is of positive degree, then there exists an extension field of $(F,+,\cdot)$ containing a root of $f(x)$.

Example(15-24): Consider $(Z_2,+_2,\cdot_2)$, the field of integers modulo 2, and the polynomial $f(x) = x^3 + x + 1 \in Z_2[x]$. Since neither of the elements 0 or 1 is a root of $x^3 + x + 1, f(x)$ is irreducible in $Z_2[x]$. Thus, the existence of an extension of $(Z_2,+_2,\cdot_2)$, specifically the field

$$\left(\frac{Z_2[x]}{\langle f(x)\rangle},+,\cdot\right)$$

in which the given polynomial has a root. Denoting this root by λ, the discussion above tells us that

$$\frac{Z_2[x]}{\langle f(x)\rangle} = \{a + b\lambda + c\lambda^2 : a, b, c \in Z_2\}$$

$$= \{0,1, \lambda, 1 + \lambda, \lambda^2, 1 + \lambda^2, \lambda + \lambda^2, 1 + \lambda + \lambda^2\},$$

where, of course, $\lambda^3 + \lambda + 1 = 0$.

$$\lambda^3 = -(\lambda + 1) = \lambda + 1, \qquad \lambda^4 = \lambda^2 + \lambda$$

$$(1 + \lambda + \lambda^2) \cdot (a + b\,\lambda + c\lambda^2) = 1$$

$$(a + b + c) + a\lambda + (a + b)\lambda^2 = 1$$

$$a + b + c = 1, \quad a = 0, \quad a + b = 0$$

with solution $a = b = 0, c = 1$; therefore, $(1 + \lambda + \lambda^2)^{-1} = \lambda^2$.

Finally, note that $x^3 + x + 1$ factors completely into linear factors in $\frac{Z_2[x]}{\langle f(x)\rangle}$ and has the three roots λ, λ^2, and $\lambda + \lambda^2$:

$$x^3 + x + 1 = (x - \lambda) \cdot (x - \lambda^2) \cdot (x - (\lambda + \lambda^2)).$$

Example(15-25): The quadratic polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$. For, If $x^2 + 1$ were reducible, it would be of the form

$$x^2 + 1 = (ax + b) \cdot (cx + d) = acx^2 + (ad + bc)x + bd,$$

where $a, b, c, d \in \mathbb{R}$. It follows at once that $ac = bd = 1$ and $ad + bc = 0$ therefore $bc = -(ad)$, and

$$1 = (ac)(bd) = (ad)(bc) = -(ad)^2$$

or, $(ad)^2 = -1$, which is impossible.

The extension field $(\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle}, +, \cdot)$ is described by

$$\frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle} = \{a + b\lambda : a, b \in \mathbb{R}; \lambda^2 + 1 = 0\}$$

$$(a + b\lambda) + (c + d\lambda) = (a + c) + (b + d)\lambda$$

$$(a + b\lambda) \cdot (c + d\lambda) = (ac - bd) + (ad + bc)\lambda + bd(\lambda^2 + 1)$$

$$= (ac - bd) + (ad + bc)\lambda$$

Theorem(15-26): If $f(x) \in F[x]$ is a polynomial of positive degree, then there exists an extension field $(F', +, \cdot)$ of $(F, +, \cdot)$ in which $f(x)$ factors completely into linear polynomials.

Corollary(15-27): Let $f(x) \in F[x]$ with deg $f(x) = n > 0$. Then there exists an extension of $(F, +, \cdot)$ in which $f(x)$ has n roots.

Example(15-28): Let us consider the polynomial $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2) \cdot (x^2 - 3)$ over the field $(\mathbb{Q}, +, \cdot)$ of rational numbers.

We first extend $(\mathbb{Q}, +, \cdot)$ to the field $(F_1, +, \cdot)$, where

$$F_1 = \frac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle} = \{a + b\lambda : a, b \in \mathbb{Q}; \lambda^2 - 2 = 0\}$$

and obtain the factorization

$$f(x) = (x - \lambda) \cdot (x + \lambda) \cdot (x^2 - 3)$$

$$= (x - \sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 - 3)$$

$f(x)$ does not factor completely, since the polynomial $(x^2 - 3)$ is irreducible in $F_1[x]$. For, suppose $x^2 - 3$ has a root in F_1, say $c + d\sqrt{2}$, with $c, d \in \mathbb{Q}$. Substituting, we find that

$$(c^2 + 2d^2 - 3) + 2cd\sqrt{2} = 0$$

$$c^2 + 2d^2 - 3 = 0, \;\; cd = 0$$

This equation implies that either $c = 0$ or $d = 0$; but neither c nor d can be zero, since otherwise we would have $d^2 = \frac{3}{2}$ or $c^2 = 3$, which is impossible. Thus $x^2 - 3$ remains irreducible in $F_1[x]$.

In order to factor $f(x)$ into linear factors, it is necessary to extend the coefficient field further. We therefore constant the extension $(F_2, +, \cdot)$, where

$$F_2 = \frac{F_1[x]}{\langle x^2 - 2 \rangle} = \{\alpha + \beta\mu : \alpha, \beta \in F_1; \mu^2 - 3 = 0\}$$

The elements of F_2 may be expressed in the form

$$\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right)\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$f(x) = (x - \lambda) \cdot (x + \lambda) \cdot (x - \mu) \cdot (x + \mu)$$

$$= (x - \sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x - \sqrt{3}) \cdot (x + \sqrt{3})$$

Observe that the four roots all lie in F_2.