Ring Theory

1.1. Definitions and examples

Definition 1.1.1 A ring R is a nonempty set together with two binary operation $+$ and **.**(called addition and multiplication defined on R) if satisfying the following axioms:

(1) $(R, +)$ is an abelian group,
(2) $(R, .)$ is semi-group,
(3) the distributive law hold in R: $for\ all\ a, b, c \in R$,
$a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$

Example. $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ and $(\mathbb{C}, +, .)$ are ring.

Definition 1.1.2. The ring $(R, +, .)$ is called commutative if multiplication is commutative $(a.b = b.a, for\ all\ a, b \in R.$

Remark. The identity of the operation + in a ring is usually written 0 and called zero.

Definition 1.1.3. The ring R is said to be ring with identity 1_R if $a.1 = 1.a = a\ for\ all\ a \in R$.

Example:
$(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ and $(\mathbb{C}, +, .)$ are commutative ring with identity.

Definition 1.1.4. Let R be a ring with identity. An element $a \in R$ is called a unit (or an invertible element) if there exists $b \in R$ such that $ab = 1 = ba$. We denoted the set of all unit elements in R by R^*.

Theorem 1.1.5. Let R be a ring with identity. Then $(R^*, .)$ is a group.
Proof. Since $1_R \in R^*$, then R^* is a non-empty set.
Now we prove that the axioms of group are satisfies:

1- let $x, y \in R^*$, that is each of $x\ and\ y$ has inverse multiplication. Hence $(x.y)(y^{-1}.x^{-1}) = x.(y.y^{-1}).x^{-1} = x.1_R.x^{-1} = x.x^{-1} = 1_R$ and $(y^{-1}.x^{-1}).(x.y) = y^{-1}.(x^{-1}.x).y = y^{-1}.1_R.y = y^{-1}.y = 1_R$.

This implies that $y^{-1}.x^{-1}$ is invers of $x.y$ and $x.y \in R^*$. Hence the set R^* is closed under multiplication.

2- associative law are holds because $(R, +, .)$is ring.
3- $1_R \in R^*$ is identity element.
4- If $x \in R^*$, then $x.x^{-1} = x^{-1}.x = 1_R \Rightarrow x^{-1} \in R^*$.
$(R^*, .)$ is group.

Example.(1) In $(Z_6, +_6, ._6)$ we see $(Z_6^* = \{1, 5\}$ and $(Z_6^*, ._6)$ is an abelian group.

(2) Let X be a non-empty set. If $P(X)$ is a power set of X, then show that $(P(X), \Delta, \cap)$

Is a commutative ring with identity?

(3) Let $M_2(\mathbb{R}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}\right\}$be the square matrix of $\mathbb{R}$. Show that $(M_2(\mathbb{R}), +, .)$ a ring with identity.

Definition 1.1.6. Let $(R, +, .)$ be a ring. For all $a \in R$ and for all integer n define

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n-times} & if\ n > 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{|n|-times} & if\ n < 0 \\ 0_R & if\ n = 0 \end{cases}$$

and define

$$a^n = \underbrace{a.a\ldots a}_{n-times} \qquad if\ n > 0$$

If R with identity, then $a^0 = 1_{R.}$

If R with identity and a has a multiplicative inverse, then

$$a^n = \underbrace{a^{-1}.a^{-1}\ldots a^{-1}}_{|n|-times} \qquad if\ n < 0$$

Theorem 1.1.7. Let $(R, +, .)$ be a ring, for $a, b \in R$ and arbitrary integers n and m the following hold:

1- $(n + m)a = na + ma,$
2- $n(a + b) = ma + mb,$
3- $(nm)a = n(ma).$

Theorem 1.1.8. Let $(R, +, .)$ be a ring and 0_R be a zero element. The for all $a, b, c \in R$ the following hold:

1- $a.0_R = 0_R.a = 0_R.$
2- $a.(-b) = (-a).b = -(a.b).$
3- $(-a).(-b) = a.b.$
4- $a.(b - c) = a.b - a.c.$

Proof. 1- Since $a.0_R = a.(0_R + 0_R) = a.0_R + a.0_R.$

Thus,

$$\begin{aligned} a0_R + a0_R &= a(0_R + 0_R) = a0_R \\ \Rightarrow (a0_R + a0_R) + (-(a0_R)) &= a0_R + (-(a0_R)) \\ \Rightarrow a0 + (a0 + (-(a0))) &= 0 \qquad \text{because } a0_R + (-(a0_R)) = 0_R \end{aligned}$$

$\Rightarrow a0_R + 0_R = 0_R$ because $a0_R + (-(a0_R)) = 0_R$

$\Rightarrow a0_R = 0_R$ because $a0_R + 0_R = a0_R$.

Similarly, $0_R a = 0_R$.

2-H.w

3-By (2) we get $(-a).(-b) = -\big(a.(-b)\big) = -\big(-(a.b)\big) = a.b$.

4-H.w

Corollary 1.1.9. Let $(R,+,.)$ be a ring with identity such that $R \neq \{0_R\}$. Then the element 0_R and 1_R are distinct.

Proof. Suppose $R \neq \{0_R\}$,. Let $a \in R$ be such that $a \neq 0$. Suppose $0_R = 1_R$.
It follows $a = a.1_R = a.0_R = 0_R$, a contradiction. Thus, $0_R \neq 1_R$.

Corollary 1.1.10. Let $(R,+,.)$ be a ring with identity such that $R \neq \{0_R\}$. Then for all $a \in R$, the following are hold:

1- $(-1).a = -a$ and
2- $(-1).(-1) = 1$.

Definition 1.1.11. Let $(R,+,.)$ be a ring and let S be a non empty subset of R ($i.e\ \emptyset \neq S \subseteq R$). If $(S,+,.)$ is itself a ring, then $(S,+,.)$ is said to a subring of $(R,+,.)$.

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

Definition 1.1.12. Let $(R,+,.)$ be a ring and $\emptyset \neq S \subseteq R$. Then $(S,+,.)$ is a subring of $(R,+,.)$ if and only if

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

Examples.

1- $(Z,+,.)$ is a subring of $(R,+,.)$ and $(Q,+,.)$.
2- $(Z_e,+,.)$ is a subring of $(Z,+,.)$.
3- Let R denote the set of all functions $f: R^{\#} \longrightarrow R^{\#}$. The sum $f+g$ and the product $f.g$ of two function $f, g \in R$ are defined by
$(f+g)(x) = f(x) + g(x)$,
$(f.g)(x) = f(x).g(x), x \in R^{\#}$
Suppose $(R,+,.)$ is the commutative ring of function of above. Define

$$S = \{f \in R \mid f(1) = 0\}.$$

Definition 1.1.13. The center of a ring $(R,+,.)$, denoted by $\boldsymbol{cent}\ (\boldsymbol{R})$, is the set

$Cent(R) = \{ c \in R \mid c.x = x.c, \text{ } for\ all\ x \in R\}.$

Remark. If $(R, +, .)$ is comuutaive, then $cent(R) = R$.

Theorem 1.1.14. Let $(R, +, .)$ be a ring. Then $(cent\ (R), +, .)$ is a subring of $(R, +, .)$.
Proof. Since $a. 0_R = 0_R. a, for\ all\ a \in R$, then $0_R \in cent\ (R)$, hence $cent(R) \neq \emptyset$.
Let $x, y \in cent(R)$. To prove that $x - y \in cent(R)$.
For all $a \in R$, then

$$(x - y). a = x. a - y. a = a. x - a. y = a(x - y).$$

Therefore $x - y \in cent(R)$, and
$(x. y). a = x. (y. a) = x(a. y) = (x. a). y = (a. x). y = a. (x. y).$
Therefore $x. y \in cent(R)$, hence $(cent\ (R), +, .)$ is a subring of $(R, +, .)$.

Solve the following problems

Q1/ In a ring $(Z, \oplus, \odot)$, where $a \oplus b = a + b - 1$ and $a \odot b = a + b - ab$, $for\ all\ a, b \in Z$. Find zero element and identity element.

Q2/ Let R denote the set of all functions $f: R^{\#} \longrightarrow R^{\#}$. The sum $f + g$ and the product $f. g$ of

two function $f, g \in R$ are defined by
$(f + g)(x) = f(x) + g(x), \qquad (f. g)(x) = f(x). g(x), x \in R^{\#}.$
Show that $(R, +, .)$ is the commutative ring.

Q3/ Let $(R, +, .)$ be an arbitrary ring. In R define a new binary operation * by
$a * b = a. b + b. a\ for\ all\ a, b \in R.$ Show that $(R, +, *)$ is a commutative ring.
Q4/ Show that the multiplicative identity in a ring with unity R is unique.

Q5/ Suppose that R is a ring with unity and that $a \in R$ is a unit of R. Show that the multiplicative

inverse of a is unique.

Q6/ Let (3Z , +) be an abelian group under usual addition where $3Z = \{3n \mid n \in Z\}$. Show that $(3Z, +, \odot)$ is a commutative ring with identity 3, where $a \odot b = \frac{ab}{3}, for\ all\ a, b \in 3Z.$
Q6/ Let $(R, +, .)$ be a ring which has the property that $a^2 = a\ for\ every\ a \in R.$ Prove that $(R, +, .)$ is a commutative ring. [Hint: First show $a + a = 0, for\ any\ a \in R$].

Q7/ Prove that a ring R is commutative if and only if

$$a^2 - b^2 = (a + b)a - b), for\ all\ a, b \in R.$$

Q8/ Prove that a ring R is commutative if and only if

$$(a + b)^2 = a^2 + 2ab + b^2, for\ all\ a, b \in R.$$

Q9/ Let R be the set of all ordered pairs of nonzero real numbers. Determine whether $(R,+,.)$ is a commutative ring with identity.

(a) $(a,b)+(c,d) = (ac, bc+d)$, $(a,b).(c,d) = (ac, bd)$

(b) $(a,b)+(c,d) = (a+c, b+d)$, $(a,b).(c,d) = (ac, ad+bc)$.

Q10/ Find all units in the rings

1- $(Z_9, +_9, \times_9)$. 2- $Z \times Z$ 3- $Z_3 \times Z_3$ 4- $Z_4 \times Z_6$.

Q11/ Is Z_2 a subring of Z_6? Is $3Z_9$ a subring of Z_9?

1.2. Some type of rings.

Definition 1.2.1. A nonzero element a in a ring R is called a zero divisor if there exists $b \in R$ such that $b \neq 0$ and $ab = 0$.
In particular, a is a left divisor of zero and b is a right divisor of zero.

Definition 1.2.2. An integral domain is a commutative ring with identity which does not have divisors of zero.

Examples. $(Z,+,.)$, $(Q,+,.)$ and $(Z_p, +_p, ._P)$ are integral domain but $(Z_6, +_6, ._6)$is not integral domain.

Definition 1.2.3. An element a of a ring $(R,+,.)$ is said to be a nilpotent if there exists a positive integer n such that $a^n = 0$.

Example. Find nilpotent element in Z_8 and $Z_4 \times Z_6$.

The nilpotent element in Z_8 are 0, 2, 4 and 6.

The nilpotent element in Z_4 are 0 and 2, and the nilpotent element in Z_6 is 0 , hence The nilpotent element in $Z_4 \times Z_6$ are (0, 0) and (2, 0).

Theorem 1.2.4. Let $(R,+,.)$ be a commutative ring with identity. Then $(R,+,.)$ is an integral domain if and only if the cancellation law holds for multiplication.

Proof. We suppose that R is an integral domain **.** Let $a, b, c \in R$ such that $a \neq 0$ and

$a.b = a.c$. Hence $b = c$.

Conversely, suppose that the cancellation law holds and $.b = 0$ **.**

If the element $a \neq 0$, then by Theorem 2.1.6 we have $a.0 = 0$, hence

$a.b = 0 = a.0$, consequently $b = 0$. That is R has no divisors of zero and R commutative with identity, we get R is an integral domain.

Corollary 1.2.5. Let $(R, +, .)$ be an integral domain. Then the only solution of the equation $a^2 = a$ are $a = 0$ and $a = 1$.

Proof. Clearly 0 is the solution of the equation $a^2 = a$.

Now , if $a^2 = a \; and \; a \neq 0$, since $a = a.1$ and $a.a = a^2 = a = a.1$, hence by cancellation law we get $a = 1$.

Definition 1.2.6. A ring $(R, +, .)$ is said to be a division ring(skew field) if it is a ring with identity in which every nonzero element has a multiplicative inverse.

Definition 1.2.7. A field is a commutative ring with identity in which each nonzero element has an inverse under multiplication.

Examples:

1- $(Q, +, .)$, $(R, +, .)$ and $(\mathbb{C}, +, .)$ are field(field of rational numbers, field of real numbers, field of Complex numbers) .

2- $(Z_n, +_n, ._n)$ is a field if and only if n is a prime number.
3- $(Z, +, .)$ is an integral domain but not a field.

Theorem 1.2.8. Every field is an integral domain**.**

Proof. Let $(R, +, .)$ be a field. Then R is a commutative ring with identity.

Let $a, b \in R \; and \; a.b \; = \; 0 \; with \; a \neq 0$.

Since R is a field, then the element a has an inverse.. The hypothesis a.b =0 yields

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

That is R contains no divisors of zero. Hence R is an integral domain**.**

Theorem 1.2.9. Any finite integral domain is a field**.**

Proof. Let $(R, +, .)$ be an integral domain contains n distinct elements say $x_1, x_2, \dots, x_n$.

Let $x \neq 0$ be any element of R, consider the elements $x.x_1, x.x_2, \dots, x.x_n \in R$. These products are all distinct because

If $x.x_i = x.x_j, for\ i \neq j \Longrightarrow x.(x_i - x_j) = 0$, but $x \neq 0 \Longrightarrow x_i - x_j = 0 \Longrightarrow x_i = x_j$,
which is contradiction to $x_1, x_2, \dots, x_n$ are all distinct.
Since $1 \in R$, then $x.x_k = 1$ for some k and $x.x_k = x_k.x = 1 \Longrightarrow x$ has multiplicative inverse and $x^{-1} = x_k$. That is $(R, +, .)$ is a field.

Theorem 1.2.10. The ring $(Z_n, +_n, ._n)$of integers modulo n is a field if and only if n is a prime number.
Proof. Suppose that R is a field. To prove that n is a prime number.
If n is not prime, then $n = a.b$ where $0 < a < n\ and\ 0 < b < n$. It follows

$$[a]._n [b] = [a.b] = [n] = [0] .$$

Since $[a] \neq [0]$, $[b] \neq [0]$. This means that the system $(Z_n, +_n, ._n)$is not an integral domain and hence not a field.
Conversely suppose that n is a prime number. To prove that $(Z_n, +_n, ._n)$ is a field, enough to show that is an integral domain.
Let $[a], [b] \in Z_n$ and $[a]._n [b] = [0] \Longrightarrow [a.b] = [0] = [n]$

$$\Longrightarrow a.b \equiv 0(mod\ \ n) \Longrightarrow a.b = kn, for\ some\ integer\ k$$

$$\Longrightarrow n\ divides\ a.b \Longrightarrow p\ divides\ a\ or\ p\ dividea\ b \Longrightarrow$$

$$a \equiv 0(mod\ n) or\ b \equiv 0(\ mod\ n) \Longrightarrow [a] = [0] or\ [b] = [0]$$

Hence $(Z_n, +_n, ._n)$ has no divisors of zero, that is $(Z_n, +_n, ._n)$ is an integral domain.

Definition 1.2.11. Let $(R, +, .)$ be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then the smallest such integer is called the characteristic of the ring. If no such positive integer exists, then we say (R, +, .) has characteristic zero.

Example. The rings Z, Q, R, C have characteristic 0.

Theorem 1.2.12. : Let $(R, +, .)$ be a ring with identity. Then$(R, +, .)$ has characteristic $n > 0$ if and only if n is the least positive integer for which $n.1 = 0$.
Proof: If the ring $(R, +, .)$ is of characteristic $n > 0$, it follows that $n.1 = 0$.
Where $m.1 = 0$, where $0 < m < n$, then
$m.a = m.(1.a) = (m.1).a = 0.1 = 0$ for every $a \in R$. This mean The characteristic of $(R, +, .)$ is less than n, which is contradiction.
Conversely, Let n be the least positive integer in which $n.1 = 0$.
Let $a \in R, a \neq 0$.

$$n.a = n.(1.a) = (n.1).a = 0.a = 0$$

Then $(R, +, .)$ has characteristic $n > 0$.

Corollary 1.2.13. The characteristic of an integral domain $(R, +, .)$ is either zero or a prime.
Proof. Let $(R, +, .)$ be a positive characteristic n and assume that n is not a prime

Then n can be written as $n = a.b$ with $1 < a, b < n$.
By Theorem 1.2.12 we have $0 = n.1 = (a.b).1^2 = (a.1).(b.1)$.
Since by hypothesis $(R, +, .)$ is without zero divisors, then either $a.1 = 0$ *or* $b.1 = 0$. But this contradicts the choice of n as the least positive integer such that $n.1 = 0$.
Hence the characteristic of $(R, +, .)$ must be prime.

Example. Show that the characteristic of the ring $(P(X), \Delta, \cap)$ is equal two.
Since $\emptyset$ is the zero element of the ring $\big(P(X), \Delta, \cap\big)$.
Now for all $A \in P(X)$, then
$2A = A \Delta A = (A - A) \cup (A - A) = \emptyset$.
From the definition of characteristic, then the characteristic of $(P(X), \Delta, \cap)$ is 2.

Solve the following problems

Q1/ Give an example of a division ring which is not a field.

Q2/ Prove that $T = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \ a, b, c \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$.

Q3/ In $(Z_{12}, +_{12}, \times_{12})$, find (i) $(2)^2 +_{12} (9)^{-2}$.

Q4/ Suppose that a and b belong to a commutative ring and ab is a zero-divisor. Show that either a or b is a zero-divisor.

Q5/ Complete the operation tables for the ring $R = \{a, b, c, d\}$:

+	a	b	c	d
	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

.	a	b	c	d	
a	a	a	a	a	
b	a	b			
c	a			a	
d	a	b	c		

Is R a commutative ring? Does it have a unity? What is its characteristic?
Hint. $c.b = (b + d).b$; $c.c = c.(b + d)$; etc.

Q6/ Let R and S be commutative rings. Prove or disprove the following statements.

(a) An element $(a, b) \in R \times S$ is nilpotent if and only if a nilpotent in R and b is nilpotent in S.

(b) An element $(a, b) \in R \times S$ is a zero divisor if and only if a is a zero divisor in R and b is a zero divisor in S.

Q7/ Show that $Q[\sqrt{2}] = \{a + b\sqrt{2} \in R \mid a, b \in Q\}$ is a subfield of the field R.

1.3. Ideals and Quotient rings.

Definition 2.3.1. A subring $(I,+,.)$ of the ring $(R,+,.)$ is an ideal of $(R,+,.)$ if and only if $r \in R$ and $a \in I$ imply both $r.a \in I$ and $a.r \in I$.

Definition 2.3.2. Let $(R,+,.)$ be a ring. Let I be a nonempty subset of R.
(i) I is called a left ideal of R if for all $a,b \in I$ and for all $r \in R, a-b \in I, ra \in I$.
(ii) I is called a right ideal of R if for all $a,b \in I$ and for all $r \in R, a-b \in I, ar \in I$.
(iii) I is called a (two-sided) ideal of R if I is both a left and a right ideal of R.

Remark. In a commutative ring , every right ideal is left ideal.
Examples.

1) The subring $(\{0,2,4\},+_6,\cdot_6)$ is an ideal of $(Z_6,+_6,\cdot_6)$.
2) The trivial subrings $(R,+,.)$ and $(\{0\},+,.)$ of the ring $(R,+,.)$ are both ideals.
   Any ideal different from $(R,+,.)$ is called proper ideal.

3) In the ring $(Z,+,.)$, $I=<a>=\{na|\, n\in Z\}$ for a fixed integer . Then I is an ideal of $(Z,+,.)$ because $na-ma=(n-m)a\in I$ and $m(na)=(mn)a\in$, where $n,m\in Z$.
4) $(Z,+,.)$ is not ideal of $(Q,+,.)$ but $(Z,+,.)$ is a subring of $(Q,+,.)$.
   Since $1\in Z$ and $\frac{1}{2}\in Q$, then $1.\frac{1}{2}=\frac{1}{2}\notin Z$. Then $(Z,+,.)$ is not ideal of $(R,+,.)$.
5) Let $(M_2(R),+,.)$ be the square matrix ring over the field of real number. Then $(cent\ (R),+,.)$ is not an ideal.

Definition 2.3.3. A ring which contains no ideals except trivial ideals is said to be a simple ring.

Definition 2.3.4. Let $(R,+,.)$ be a commutative ring with identity. An ideal $(I,+,.)$ is called a principal ideal of the ring $(R,+,.)$ if generated by a single element a and denoted by $I=(a)=\{r.a \mid r\in R\}$.

Example. In the ring $(Z,+,.)$ the ideal $(2)=\{2.r \mid r\in Z\}=2Z$ is a principal ideal generated by 2 and $(3)=\{3.r \mid r\in Z\}=3Z$ is a principal ideal generated by 3.

Theorem 2.3.5. If $(I,+,.)$ is an ideal of the ring $(Z,+,.)$, then $I=(n)$ for some nonnegative integer n.
Proof. If $I=(0)$, then the theorem is true.
Suppose then that $I\neq(0)$, that is there exists $0\neq m \in I$. Since I is an ideal, then $-m \in I$, so I contains positive integers.
Let n be the least positive integer in I. We claim $I=(n)$.
Since $n \in I$ and $(I,+,.)$ is an ideal of $(Z,+,.)$, then $kn\in I$, for all $k \in Z$, that is $(n)\subseteq I$.
On the other hand, any integer $k \in I$. By division Algorithm there exists $q,r \in Z$ such that $k=qn+r$, where $0\le r<n$.
Since k and qn are members of I, it follows that $k-qn=r\in I$.
Our n be a least integer implies $r=0$, and consequently $k=qn \Longrightarrow k\in(n)$
Therefore $I=(n)$.

Definition 2.3.6. Let $(R,+,.)$ be a commutative ring with identity. A ring $(R,+,.)$ is called a principal ideal ring if every ideal is principal.

Theorem 2.3.7. Let $(R,+,.)$ be a ring with identity element and I be an ideal of R containing identity element .Then $I = R$.
Proof . Since I is an ideal of R, then $I \subseteq R$.
Let $\in R$, then $r = r.1 \in I$ (because I is an ideal of R) $\Longrightarrow r \in I \Longrightarrow R \subseteq I \Longrightarrow I = R$.

Theorem 2.3.8. If $(I,+,.)$ is a proper ideal of a ring $(R,+,.)$ with identity, then no element of I has a multiplicative inverse; that is $\cap R^{*} = \emptyset$.
Proof. Suppose to the contrary that there is $0 \neq a \in I$ such that a^{-1}exists.
Since I is an ideal, then $1 = a.a^{-1} \in I \Longrightarrow I = R$, contradiction the hypothesis that I is a proper subset of R

ITheorem 2.3.9. If $(I_1,+,.)$ and $(I_2,+,.)$ are two ideals of the ring $(R,+,.)$, then $(I_1 \cap I_2,+,.)$ is also an ideal.
Proof. Since $(I_1,+,.)$ and $(I_2,+,.)$ are ideals of the ring $(R,+,.)$, then $0 \in I_1$ and $0 \in I_2$, hence $0 \in I_1 \cap I_2$. This implies that $I_1 \cap I_2 \neq \emptyset$.
Suppose $a,b \in I_1 \cap I_2$ and $r \in R$. Then $a,b \in I_1$ and $a,b \in I_2$.
As the $(I_1,+,.)$ and $(I_2,+,.)$ are ideals of the ring $(R,+,.)$, it follows from definition
$a-b \in I_1, ar \in I_1$ and $ra \in I_1$, and also $a-b \in I_2, ar \in I_2$ and $ra \in I_2$.
Hence $a-b \in I_1 \cap I_2, ar \in I_1 \cap I_2$ and $ra \in I_1 \cap I_2$, which implies that $(I_1 \cap I_2,+,.)$ is an ideal of $(R,+,.)$.

Theorem 3.2.10. Let (R, +, .) be a commutative ring with identity. Then (R, +, .) is a field if and only if (R, +, .) has no nontrivial ideals.

Quotient rings

We now give the analogue of quotient groups for rings. Let R be a ring and I an ideal of R. Let $x \in R$.
Let $x + I$ denote the set $x + I = \{x + a \mid a \in I\}$.
The set $x + I$ is called a coset of I .For $x,y \in R$, By Theorem 6.1, $x + I = y + I$ if and only if $x - y \in I$.
Let R/I denote the set $R/I = \{x + I \mid x \in R\}$. Because $I = 0 + I \in R/I, R/I$ is a nonempty set.
Define the operations + and · on R/I as follows:
$for\ all\ x + I,\ y + I \in R/I$
$(x + I) + (y + I) = (x + y) + I$, and $(x + I) \cdot (y + I) = xy + I$.
We leave it as an exercise for verify that + and · are binary operations on R/I .
Under these binary operations $(R/I,+,\cdot)$ satiesfies the properties of a ring.
Let us verify some of these properties.
Let $x + I, y + I, z + I \in R/I$. Now

$$(x+I)+((y+I)+(z+I))=(x+I)+((y\ +\ z)+I\ )=(x\ +(y\ +\ z))\ +\ I$$
$$=((x\ +\ y)+z)+I,$$
$$=((x\ +y)+I\ )+(z\ +\ I\ )=((x\ +\ I\ )+(y\ +\ I\ ))\ +\ (z\ +\ I\ ).$$

This shows that + is associative in $/I$. Similarly, + is commutative. Next, note that $0+I\ =\ I$ is the additive identity and for $+I\ \in\ R/I$, $(-x)+I$ is the additive inverse of $x\ +\ I$. As in the case of the associativity for +,
we can show that · is associative.
Next, let us verify one of the distributive law. Now

$$(x\ +\ I\ )\ \cdot\ ((y\ +\ I\ )+(z\ +\ I\ ))\ =\ (x\ +\ I\ )\ \cdot\ ((y\ +\ z)+I\ )=(x(y\ +\ z))\ +\ I$$
$$=(xy\ +\ xz)+I=(xy+I\ )+(xz\ +\ I\ )$$
$$=((x\ +\ I\ )\ \cdot\ (y\ +\ I\ ))\ +\ ((x\ +\ I\ )\ \cdot\ (z\ +\ I\ )).$$

In a similar manner, we can verify the right distributive property.

Theorem 2.3.10. If $(I,+,.)$ is an ideal of $(R,+,.)$, then the ring $(R/I\ ,+,\cdot)$ is ring, known as the quotient ring of R by I.

Definition 2.3.11. An ideal $(I,+,.)$ of the ring $(R,+,.)$ is a prime ideal if for all $a,b\ \in\ R, a.b\in I$ implies either $a\ \in I\ or\ b\ \in I$.

Example.(1) The ideal $((3),+,.)$ of the ring $(Z,+,.)$ is a prime ideal.
(2) A commutative ring with identity is an integral domain if and only if the zero ideal is a prime ide

Theorem 2.3.12. Let $(I,+,.)$ be a proper ideal of the ring $(R,+,.)$. Then $(I,+,.)$ is a prime ideal if and only if the quotient ring $(R/I,+,.)$ is an integral domain.
Proof. First, take $(I,+,.)$ to be a prime ideal of $(R,+,.)$. Since $(R,+,.)$ is a
commutative ring with identity, so is the quotient ring $(R/I,+,.)$. It remains to show $(R/I,+,.)$ has no divisor of zero. For this, assume that
$(a\ +\ I).(b\ +\ 1)=\ I\Longrightarrow a\cdot\ b\ +\ I\ =\ I\Longrightarrow a.b\in I$. Since $(I,+,.)$ is a prime ideal,
hence $a\in I\ or\ b\in I\Longrightarrow a+I=I\ or\ b+I=I$, hencc $(R/\ I,+,.)$ is without zero divisors.
To prove the converse, suppose $(R/\ I,+,.)$ is an integral domain and $a.b\in I$. Then we have
$a.b+I=I\Longrightarrow(a\ +\ I)\,.\,(b\ +\ I)\ =\ I.$
By hypothesis , $(R/\ I,+,.)$ contains no divisors of zero, that either
$a\ +\ I\ =I\ or\ b\ +\ I\ =\ I\Longrightarrow a\in I\ or\ b\in I$. That is $(I,+,.)$is a prime ideal.

Theorem 2.3.13. Let $(Z,+,.)$ be the ring of integers and $n\ >\ 1$. Then the principal ideal $((n).+,.)$ is prime if and only if n is a prime number.
Prool. First, suppose $((n),+,.)$ is a prime ideal of $(Z,+,.)$. If the integer n is not prime, then $n\ =\ p.q$, where $1<p,q<n$. This implies the $p.q\in(n)$ and such that $((n),+,.)$
Is a prime ideal, this implies $p\in(n)or\ q\in(n)$ and this contradiction to the hypothesis of p and q are less than n, therefore n must be a prime number.

Conversely, suppose n is a prime number and a, b two integers such that $a.b \in (n)$ with $a \notin (n)$.
Since $a.b \in (n) \Longrightarrow n|a.b$ and sine n is a prime number implies that $n \nmid a \longrightarrow n|b \Longrightarrow b \in (n)$, therefore $((n), +, .)$ is a prime ideal.

Definition 2.3.14. An ideal $(I, +, .)$ of the ring $(R, +, .)$ is a maximal ideal provided $I \neq R$ and whenever $(J, +, .)$ is an ideal of $(R, +, .)$ with $I \subset J \subseteq R$, then $J = R$.
Remark. An element is invertible is not belongs to maximal ideal.

Definition 2.3.14. An ideal $(I, +, .)$ of the ring $(R, +, .)$ is a maximal ideal provided $I \neq R$ and whenever $(J, +, .)$ is an ideal of $(R, +, .)$ with $I \subset J \subseteq R$, then $J = R$.
Remark. An element is invertible is not belongs to maximal ideal.
2-$((6), +, .)$ is not a maximal ideal since $(6) \subset (3) \subset Z$
3-$(2Z \times \{0\}, +, .)$ is a prime ideal of the ring $(Z \times Z, +, .)$ but is not a maximal ideal since $2Z \times \{0\} \subset 2Z \times 2Z \subset Z \times Z$.
4- $(\{0\}, +, .)$ is a prime ideal of the ring $(Z, , .)$ but not a maximal ideal.
Theorem 2.3.15. Let $(I, +, .)$be aproper ideal of the commutative ring with identity $(R, +, .)$. Then $(I, +, .)$ is a maximal ideal if and only if the quotient ring $(R/I, +, .)$ is a field.
Proof. Let $(I, + ..)$ be a maximal ideal of $(R. +, .)$. Since $(R, +, .)$ is a commutative ring with identity, then the quotient ring $(R/I, +, .)$ is also a commutative ring with identity. It remains to show that every non-zero elemnt in R/I has inverse.
$a + I \in R/I \; such \; that \; a + I \neq I \Longrightarrow a \notin I.$
Since $((a), +, .)$ is an ideal of $(R, +, .)$, the $((a) + I, +, .)$ is an ideal of $(R, +, .)$ and $a \notin I \Longrightarrow I \subset (a) + I$. By suppose $(I, +, .)$ is a maximal ideal, then $(a) + I = R$.
$R = \big((a), I\big) = \{a.r + b \mid b \in I, r \in R\}$.
Since $1 \in R \Longrightarrow 1 \in (a) + I \Longrightarrow 1 = a.r + b, r \in R\,, b \in I \Longrightarrow b = 1 - a.r \in I$.
That is $1 - a.r \in I \Longrightarrow 1 + I = a.r + I = (a + I).(r + I)$.
Therefore $a + I$ has an inverse, consequently $(R/I, +, .)$ is a field.
Conversely, suppose $(R/I, +, .)$ is It field and $(J. +, .)$ is any ideal of $(R, +, .)$ such that $I \subset J \subseteq R$.
Since $I \subset J$, then there exist an element $a \in J \; and \; a \notin I \Longrightarrow a + I \neq I$.
Since $(R/I, +, .)$ is a field, then $a + I$ has an inverse say $b + I$, therefore

$$(a + I).(b + I) = 1 + I \Longrightarrow a.b + I = 1 + I \Longrightarrow 1 - a.b \in I \subset J \Longrightarrow 1 - a.b \in J$$

Since $a.b \in J \Longrightarrow 1 \in J \Longrightarrow J = R$. Hence $(I, +, .)$ is a maximal ideal.

Definition 2.3.16. A ring $(R, +, .)$ is called a local ring if has only one maximal ideal.

Definition 2.3.17. The **radical** of a ring $(R, +, .)$, denoted by $rad\, R$, is the set
$rad(R) = \cap \{M : (M, +, .) is \; a \;\; amximal \; ideal \; of \;\; ring \; (R, +, .)\}$.
If $rad\,(R) = \{0\}$, then we say $(R, +, .)$ is a ring without radical or is a semi-

simple ring.

Example. In $(Z_{12}, +_{12}, \cdot_{12})$, find $rad(Z_{12})$

Remark. $(rad\ (R), +, .)$ is an ideal of $(R, +, .)$.

Definition 2.3.18. An ideal $(I, +, .)$ of a ring $(R, +, .)$ is said to be a **primary ideal** if $a.b \in I$ with $a \notin I$ implies $b^n \in I$ for some positive integer n.

Example. An ideal $\big((4), +, .\big)$ of $(Z, +, .)$ is a primary.

Definition 2.3.19. An element a of a ring $(R, +, .)$ is said to be a nilpotent if there exists a positive integer n such that $a^n = 0$.

Theorem 2.3.19. Let $(I, +, .)$ be an ideal of a ring $(R, +, .)$. Then $(I, +, .)$ is a primary if and only if every zero divisor of the quotient ring $(R/I, +, .)$ is nilpotent.

Proof. Suppose $(I, +, .)$is a primary ideal and $a + I$ is a zero divisor in R/I.

That is there exists a npnzero element $b + I$ such that

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

Since $b \notin I\ and\ (I, +, .)$ is a primary, then there exists a positive integer n such that $a^n \in I \Longrightarrow a^n + I = I \Longrightarrow (a + I)^n = I$. Hence $a + I$ is nilpotent element in R/I.

Conversely, suppose every zero divisor is nilpotent.

Let $a, b \in R$ such that $a.b \in I$ with $a \notin$ I. We must to sow that $b^n \in I$, for some $n \in Z^+$.

If $b \in I$, it is trivial.

If $b \notin I \Longrightarrow b + I \neq I$. Since $(a + I).(b + I) = a.b + I = I$, hence $b + I$ is divisor of zero.

By hypothesis $b + I$ is a nilpotent element, that is there exist a positive integer n such that $b^n + I = (b + I)^n = I \Longrightarrow b^n \in I$, consequently $(I, +, .)$is primary.

2.4. Homomorhpisms

Definition 2.4.1. Let $(R, +, .)$ and $(R', +', .')$ 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 $(R, +, .)$ into $(R', +', .')$ if and only if

1- $f(a + b) = f(a) +' f(b)$,
2- $f(a \cdot b) = f(a) .' f(b)$

for every $a, b \in R$.

Example. Let $f: (R, +, .) \longrightarrow (R', +', .')$ be the function defined by

$$f(a) = 0', for\ all\ a \in R$$

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

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

Hence f is a ring homomorphism.

Example. Let $f: (Z, +, .) \longrightarrow (Z_e, +, .)$ be the function defined by

$$f(a) = 2a\ , for\ all\ a \in R$$

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

$$f(a \cdot b) = 2(a.b) = 2a.b \neq f(a).f(b), a.b \in R.$$

Hence f is not a ring homomorphism.

Definition. A homomorphism f from the ring (R, +, .) in to ring (R', +', .') is called an isomorphism if f is one to one and onto**.**
If there exist an isomorphism function between two rings, then is said an isomorphic and denoted by $(R, +, .) \cong (R', +', .')$.

Theorem 2.4.2. Let f be a homomorphism from the ring $(R, +, .)$ into the ring $(R', +', .')$. Then the following hold: .

1) $f(0) = 0'$, where $0'$ is the zero element of $(R', +', .')$.
2) $f(-a) = -f(a) for\ all\ a \in R$.
3) The triple $(f(R), +', .')$ is a subring of $(R', +', .')$.

If, in addition, $(R, +, .)$ and $(R', +', .')$. are rings with identity elements 1 and 1', respectively, and $f(R) = R'$, then

4) $f(1) = 1'$,
5) $f(a^{-1}) = f(a)^{-1}$ for each invertible element $a \in R$.

Proof. Similar of Theorem 8.4

Theorem .

1- Let $f : (R, +, .) \longrightarrow (S, +, .)$ and $g : (S, +, .) \longrightarrow (T, +, .)$ be two homomorphisms. Then $g \circ f : (R, +, .) \longrightarrow (T, +, .)$ is also a homomorphism.

2- Let $f : (R, +, .) \longrightarrow (S, +, .)$ be a homomorphism. Then Let $f^{-1} : (S, +, .) \longrightarrow (R, +, .)$ Is also homomorphism.

Proof. 1. Let $x, y \in R$. Then

$g \circ f(x + y) = g\big(f(x + y)\big) = g\big(f(x) + f(y)\big) = g\big(f(x)\big) + gf(y)) = g \circ f(x) + g \circ f(y)$, and

$$g \circ f(x.y) = g\big(f(x.y)\big) = g\big(f(x).f(y)\big) = g\big(f(x)\big).gf(y)) = g \circ f(x).g \circ f(y).$$

Hence $g \circ f$ is ahomomorphism.

Proof. 2. Since f is a one to one and onto function, then so is f^{-1}.

Let $x,\ y \in S$. Then there exists $r,\ t \in R$ such that $f(r) = x\ and\ f(t) = y$.

Since $x + y = f(r) + f(t) = f(r + t)$, thus we get

$f^{-1}(x + y) = r + t = f^{-1}(x) + f^{-1}(y)$.

and $x.y = f(r).f(t) = f(r.t)$, thus we get

$f^{-1}(x.y) = r.t = f^{-1}(x).f^{-1}(y)$.

Therefore f^{-1} is a homomorphism.

Theorem 2.4.3. Let f be a homomorphism from the ring $(R, +, .)$ into the ring $(R', +', .')$. Then

1- If $(S, +, .)$ is a subring of $(R, +, .)$, then $(f(S), +', .')$ is a subring of $(R', +', .')$.

2- If $(S', +', .')$ is a subring of the ring $(R', +', .')$, then $(f^{-1}(S), +, .)$ is a subring of $(R, +, .)$.
3- If $(I, +', .')$ is an ideal of the ring $(S, +', .')$, then $(f^{-1}(I), +, .)$ is an ideal of $(R, +, .)$.
4- If $f(R) = S$ and $(J, +, .)$ is an ideal of $(R, +, .)$, then $(f(J), +', .')$ is an ideal of $(S, +', .')$.

Proof. 1- $f(S) = \{ f(x)\colon\ x \in S\}$

Since $e \in S$, then $f(e) \in f(S) \Longrightarrow f(S) \neq \emptyset$.

Let $f(x),\ f(y) \in f(S), for\ x, y \in S$.

Now $f(x) - f(y) = f(x - y) \in f(S)$, Since $x - y \in S$, and

$f(x).f(y) = f(x.y) \in f(S)$, Since $x.y \in S$

Therefore by Definition 2.1.12, we get $f(S)$ is a subring of R'.

3- By part (2) $(f^{-1}(I),\ *)$ is a subring of $(R, +, .)$.
To show that $(f^{-1}(I), +, .)$ is an ideal of $(R, +, .)$, such that

$$f^{-1}(I) = \{ r \in R: f(r) \in I\}$$

Now suppose $x, y \in f^{-1}(I) \Longrightarrow f(x), f(y) \in I$.
Since f is a homomorphism and $(I, +', .')$ is a subring of $(R', +', .')$, then we have
$f(x - y) = f(x) - f(y) \in I$, Since $(I, +', .')$ is an ideal of $(R', +', .')$.
Therefore $x - y \in f^{-1}(I)$, and
Let $r \in R \Longrightarrow f(r) \in R'\ and\ x \in f^{-1}(I) \Longrightarrow f(x) \in I$.

Since $(I, +', .')$ is an ideal of $(R', +', .')$, then $f(r).'f(x), f(x).'f(r) \in I$.
Hence since f is a homomrphism, we get
$f(r.x) = f(r).'f(x) \in I \Longrightarrow r.x \in f^{-1}(I)$ and
$f(x.r) = f(x).'f(r) \in I \Longrightarrow x.r \in f^{-1}(I)$
Therefore $(f^{-1}(I), +, .)$ is an ideal of $(R, +, .)$.

Example. $f: (\mathbb{Q}, +, .) \longrightarrow (\Re, +, .)$defined by $f(x) = x, for\ all\ x \in \mathbb{Q}$ is a homomorphism and $f(\mathbb{Q}) = \mathbb{Q}$ but $(\mathbb{Q}, +, .)$ is not an ideal of $(\Re, +, .)$.

Definition 2.4.4. Let f be a homomorphism from the ring $(R, +, .)$ into the ring $(R', +', .')$. Then **kerenel of f,** denoted by $ker\ f$, is the set

$\ker f = \{x \in R : \ f(x) = e'\}$.

Theorem 2.4.5. If f is a homomorphism from the ring $(R, +, .)$ into the ring $(R', +', .')$, then $(ker\ f, +, .)$ is an ideal of $(R, +, .)$.

Proof. Since $(\{e'\}, +', .')$ is an ideal $(R', +', .')$ and $\ker f = f^{-1}(\{e'\})$, then by Theorem 2.4.3 $(\ker f, +, .)$ is an ideal of the ring $(R, +, .)$.

Theorem 2.4.5. Let f be a homomorphism from the field $(F, +, .)$on to the field $(F', +', .')$. Then either f is the trivial homomorphism or else $(F, +, .)$
and $(F', +', .')$ are isomorphic.
Proof. By The Theorem 2.4.4 $(ker\ f, +, .)$ is an ideal of the field $(F, +, .)$.
Since $(F, +, .)$ is a field has no ideal other than $(F, +, .)$ itself and $(\{0\}, +, .)$.
Hence either the set $ker\ f = \{0\}$ or else $ker\ (f) = F$.
If $ker\ (f) = F$, then $f(x) = 0, for\ all\ x \in F$ and this contradication for $f(1) = 1$, hence $\ker f = \{0\}$ and this implies that f is one-to-one. Therefore f is an isomorphism, consequently $(F, +, .) \cong (F', +', .')$.

Definition 2.4.6. We said that $(F', +, .)$is a subfield of the field $(F, +, .)$ is meant any subring of $(F, +, .)$ which is itself a field.

Example. The ring $(\mathbb{Q}, +, .)$ of rational numbers is a subfield of the field $(\Re, +, .)$.

Is equivalent to
The triple $(F', +, .)$ will be a subfield of the field $(F, +, .)$ provided
(1) $(F', +)$ is a subgroup of the additive group $(F, +)$ and
(2) $(F' - \{O\}, \cdot)$ is a subgroup of the multiplicative group $(F - \{O\}, \cdot)$.

Definition 2.4.7. A ring $(R, +, .)$ is imbedded in a ring $(R', +', .')$ if there exists some subring $(S, +', .')$ of $(R', +', .')$ such that $(R, +, .) \cong (S, +', .')$.

The field of quotient of an integral domain.

Let D be an integral domain.

$D \times D = \{(a,b) : a,b \in D\}$. Let S be the subset of $D \times D$ given by

$S = \{(a,b) : a,b \in D, b \neq 0\}$. Define a relation on S as follows:

Two elements (a,b) and (c,d) in S are equivalent (denoted by $(a,b) \sim (c,d)$) if

$$ad = bc.$$

Lemma 2.4.8. The relation $\sim$ is an equivalence relation.

Proof.

(1) Reflexive: $(a,b) \sim (c,d)$, since multiplication in D is commutative.

(2) Symmetric: Suppose that $(a,b) \sim (c,d)$, then $ad = bc$. Hence $cb = da$, consequently $(c,d) \sim (a,b)$.

(3) Transitive: suppose that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $ad = bc$ and $cf = de$, so

$$afd = fad = fbc = bfc = bde = bed \text{ } (D \text{ is commutative})$$

since $d \neq 0$ and D is an integral domain, hence $afd = bed \leftrightarrow af = be$

$\leftrightarrow (a,b) \sim (e,f)$. From (1), (2) and (3) we get that $\sim$ is an equivalence

relation.

Hence it gives a partition of S in to equivalence class. We write the equivalence class of (a,b) by $[(a,b)]$.

Let $F = \{[(a,b)] : (a,b) \in S\}$. Define addition and multiplication on F as follows:

$[(a,b)] + [(c,d)] = a.d + b.c, b.d]$ and

$[(a,b)].`[(c,d)] = [(a.c, b.d)]$.

Now we show that the operations defined above is well-defined.

First note that if $[(a,b)]$ and $[(c,d)] \in F$, then $b \neq 0$ and $d \neq 0$. Since D is an integral domain, then $bd \neq 0$, so both $[(a.d + b.c, b.d)]$ and $[(a.c, b.d)] \in F$.

To show that the multiplication (.`) is well-defined, suppose that

$(a,b) \sim (a_1, b_1)$ and $(c,d) \sim (c_1, d_1)$. We have two show that $[(a,b)]\,[(c,d)] = [(a_1,b_1)]\,[(c_1,d_1)]$.

$ab_1 = a_1 b$ and $cd_1 = c_1 d \rightarrow ab_1\, cd_1 = b_1 a\, d_1 c \rightarrow ab_1\, cd_1 = b_1 a\, d_1 c$. This means that

$(a_1 c_1, b_1 d_1) \sim (ac, bd)$ which means that the multiplication is well-defined .

Theorem 2.4.9. Let D be an integral domain and $S = \{(a,b) : a, b \in D , b \neq 0\}$.

Define a relation on S as follows: $(a,b) \sim (c,d))$ $if\ ad = bc$. Then

$F = \{[(a,b)] : (a,b) \in S\}$ is a field with addition and multiplication defined as follows: $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$ and $[(a,b)]\,[(c,d)] = [(ac,bd)]$.

Proof.

(1) + is a commutative :

$$[(a,b)] + [(c,d)] = [(ad+bc,bd)] = [(cd+da,db)] = [(c,d)] + [(a,b)].$$

(2) It is easy to show that + is a associative

(3) [(0,1)] is identity for addition in F:$[(a,b)] + [(0,1)] = [(a+0,b)] = [(a,b)]$

(4) $[(-a,b)]$ is an additive inverse of $[(a,b)]$ in F:

$[(a,b)] + [(-a,b)] = [(ab-ba,b^2)] = [(0,b^2)] = [(0,1)]$ (since $(0,b^2) \sim (0,1)$ because $0 .1 = 0. b^2$) Thus $[(a,b)] + [(-a,b)] = [(0,1)]$.

(5) It is easy to show that multiplication is a associative.

(6) [(1,1)] is identity for multiplication in F :

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

(7) Multiplication is commutative

(8) The distributive law hold in F

(9) Let $[(a,b)] \in F$ and $[(a,b)] \neq [(0,1)]$ hence $a \neq 0$ because if $a = 0$, then $a\ 1 = b\ 0 = 0$, so $(a,b) \sim (0,1)$, consequently $[(a,b)] = [(0,1)]$ which is a contradiction .

Thus a is a non zero element in F. Now $[(a,b)]\,[(b,a)] = [(ab,ba)] = [(1,1)] \Leftrightarrow [(b,a)]$ is a multiplicative inverse of $[(a,b)]$. Hence F is a field. This field called the field of quotients of R.
the quotient field of an integral domain (D,+, .`) is the smallest field containing D as a subring.

Example. The field of quotients of Z, is the ring of integers is Q

Theorem 2.4.10. The integral domain (R, +, .) can be imbedded in its of quotients

(F, +', .').

Proof. Consider the subset F' of F consisting of all elements of the form $[a,1]$, where 1 is the multiplicative identity of (R, +, .):

$F' = \{ [a,1] : a \in R\}$. Now it is must be show that $(F', +', .')$ is a subring.

Let $f : R \to F'$ be onto mapping defined by $f(a) = [a,1]$, for each $a \in R$.
Since the condition $[a,1] = [b,1]$ implies $a.1 = b.1$ or $a = b$, we see f is one to one.

Now we show that f is homomorphism:
$f(a + b) = [a + b, 1] = [a, 1] +' [b, 1] = f(a) +' f(b)$ and
$f(a . b) = [a . b, 1] = [a, 1] .' [b, 1] = f(a) .' f(b)$
Accordingly $(R, +, .) \cong (F', +', .')$.

Theorem 2.4.11. (First isomorphism theorem)
If f is a homomorphism from the ring $(R, +, .)$ onto the ring $(R', +', .')$. Then

$$\left({R}/{\ker f}, +, '\right) \cong (R', +', .').$$

Proof. Put $ker\ f = K$. We define a function φ: ${R}/{K} \longrightarrow R'$ by

$\varphi(x + K) = f(x), \;\; for\ x \in R.$

We must show that R is well defined, suppose $x + K = y + K \Longrightarrow x - y \in K = \ker f$.
Therefore $f(x - y) = e'$. But f is homomorphism, then
$f(x) - f(y) = e' \Longrightarrow f(x) = f(y) \Longrightarrow \varphi(x + K) = \varphi(y + K)$.
Hence φ is well defined.
Now to show that φ is a homomorphism, suppose that

$$\begin{aligned}\varphi\big((x + K) + (y + K)\big) &= \varphi\big((x + y) + K\big)\\ &= f(x + y)\\ &= f(x) +' f(y)\\ &= \varphi(x + K) +' \varphi(y + K).\end{aligned}$$

$$\begin{aligned}\varphi\big((x + K).(y + K)\big) &= \varphi\big((x.y) + K\big)\\ &= f(x.y)\\ &= f(x).' f(y)\\ &= \varphi(x + K).' \varphi(y + K).\end{aligned}$$

Hence φ is a homomorphism.
Let $\varphi(x + K) = \varphi(y + K) \Longrightarrow f(x) = f(y) \Longrightarrow f(x) - f(y) = e'$.
Since f is a homomorphism, therefore
$f(x) - f(y) = e' \Longrightarrow f(x - y) = e' \Longrightarrow x - y \in K \Longrightarrow x + K = y + K$.
Hence φ is one-to-one.
Finally, for all $z \in R'$ there exists $y \in R$ such that $z = f(y) = \varphi(y + K)$.
Hence φ is onto. Therefore φ is an isomorphism and $\left({R}/{K}, +, .\right) \cong (R', +', .')$.
Remark. If f is not onto, then $(R/Kerf, +, .) \cong (f(R), +', .')$.

Theorem 2.4.12. (second isomorphism theorem)
If $(S, +, .)$ is a subring of the ring $(R, +, .)$ and $(I, +, .)$ is an ideal of $(R, +, .)$, then $S + I/I \cong S/S \cap I$.
Proof. Similarly to prove Theorem 9.3

Theorem 2.4.13. (Third isomorphism theorem)

If $(I,+,.)$ and $(J,+,.)$ are two ideals of the ring $(R,+,.)$ and $I \subset J$, then $(J/I\,,+,.)$ is an ideal of the ring $(R/I\,,+,.)$ and $\frac{R/I}{J/I} \cong R/J$.

Proof. Similarly to prove Theorem 9.4.

Chapter Three
Polynomial rings

The polynomial ring R[x] in indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ with $n \geq 0$ and $a_i \in R$, That is $R[x] = \{ a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 : n \geq 0 \text{ and } a_i \in R \}$.

If $a_n \neq 0$, then the polynomial is of degree n , $a_n x^n$ is the leading term, and a_n the leading coefficient. Addition of polynomial is component wise

$\sum_{i=0}^{n} a_i\, x^i + \sum_{i=0}^{n} b_i\, x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$ (where a_n and b_n may be zero in order for addition of polynomials of different degree to be defined).

Multiplication performed by first defined a x^i b x^i = ab x^{i+j} and then extended to all polynomials by distributive law , in general

$(\sum_{i=0}^{n} a_i\, x^i) \times (\sum_{i=0}^{n} b_i\, x^i) = \sum_{i=0}^{n+m} (\sum_{i=0}^{k} (a_i\, b_{k-i}) x^k)$.

Two polynomials $p(x) = a_0+a_1x+\ldots+a_nx^n$ and $q(x) = b_0+b_1x+\ldots+b_nx^n$, are equal if $a_i = b_i$ for each i. The ring R appears in R[x] as the constant polynomials.

If g(x) is a polynomial over a ring R, then degree g(x) denoted deg g(x).

If R[x] has unity 1 and you must have x(x = (0, 1, 0, 0, …))

2+ x^2 in Z[x] (i.e (2, 0, 1, 0, 0, …)).

If R is a ring with two determinates, then we can form (R[x])[y] = R[x, y]

The ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in the n indeterminate x with coefficients in R.

Theorem 3.1. The triple (R[x], +, .) forms a ring, known as the ring of polynomials over R.

Examples. (1) Let $f(x) = 1+3x+2x^5$ a polynomial, then the leading coefficient of f(x) = 2, deg f(x) = 3.

(2) In Z_2[x]. If f(x) = x + 1, then we have
(x + 1) + (x + 1) = 2x + 2 = 0, and
$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1$

Remark . Let R be a ring.

(1) If R is a commutative , then so is R[x].

(2) If R is a ring with identity 1_R, then R[x] is a ring with identity and the identity element is $1_{R[x]} = 1_R + 0_R + \ldots$

(3) don't write 1_R when appear as coefficient for a polynomial, as follows: $x^3 + x^2 + 2x + 2$ $(1.x^3 + 1.x^2 + 2x + 2)$.

(4) In general if f(x) and g(x) are two polynomials over a ring R, then

(1) $\deg(f(x) + g(x)) \leq \max \{\deg f(x) , \deg g(x) \}$.

(2) $\deg (f(x) . g(x)) \leq \deg f(x) + \deg g(x)$.

Example. Let $f(x) =1+5x+2x^4$ and **g**$(x) = 1+4x^2$ be two polynomials in $Z_8[x]$.
The leading coefficient of f(x) = 2, deg f(x) = 4 and deg g(x) = 2.
$f(x). g(x) = 1+4x^2+5x +4x^3+ 2x^4$
$\rightarrow \deg((f(x)+ \deg g(x))=7 \neq \deg((f(x). \deg g(x))=4$, and
$f(x) + g(x) = 2+5x+4x^2+2x^4$, $\deg (f(x) + g(x)) = 4$.

Theorem 2.3 . Let (R , + , .) be an integral domain and f(x) , g(x) be two nonzero elements of (R[x] , + , .) then : $\deg (f(x).g(x)) = \deg f(x) + \deg g(x)$.

Proof : suppose f(x) , g(x) $\in$ R[x] with deg f(x) =n and deg g(x) =m , so that

$f(x) = a_o + a_1x + \ldots + a_nx^n \qquad , a_n \neq 0$

$g(x) = b_o + b_1x + \ldots + b_mx^m \qquad , b_m \neq 0$

from the definition of multiplication

$f(x) . g(x) = a_o . b_o + (a_o .b_1+ a_1 . b_o) x + \ldots + (a_n . b_m) x^{n+m}$

since $a_n \neq 0$ and $b_m \neq 0$ and R is an integral domain , then $a_n . b_m \neq 0$

accordingly, $f(x) . g(x) \neq 0$ and $\deg(f(x).g(x)) = n+m = \deg f(x) +\deg g(x)$

Corollary 2.4 . Let (R, + , .) be an integral domain. Then (R[x], + , .) is an integral domain.
proof . We have if (R , + .) is a commutative ring with identity , then so is (R[x] , + , .) . To see that (R, +, .) has no divisors , let $f(x) \neq 0$, $g(x) \neq 0$ in R[x] . Then $\deg (f(x).g(x)) = \deg f(x) + \deg g(x)>0$, hence the product cannot be the zero polynomial

Theorem 2.5. (**Division algorithm**)
Let (R, +, .) be a commutative ring with identify and let $f(x) = a_n x^n + a_{n-1} x^{n-1} +\ldots +a_0$ and $g(x) = b_m x^m + b_{n-1} x^{m-1} +\ldots +b_0$, be two elements in R[x], with both a_n , b_n non zero elements of R and m > 0 and the leading coefficient of g(x) is invertible. Then there are unique polynomials q(x) and r(x) in R[x] such that $f(x)=q(x) g(x) + r(x)$, with r(x) = 0 or degree r(x) < degree g(x).

Examples.

(1) Consider $f(x) = x^4 - 3x^3 + x^{2 -} 3x + 1$ in $Z_5[x]$ and let $g(x)= x^2 +2x -6$. To find q(x) and r(x), divide f(x) by g(x),

$$
\begin{array}{r|l}
 & \quad\quad\quad\quad\quad x^2 - x - 3 \\
\hline
x^2 - 2x + 3 & x^4 - 3x^3 + 2x^2 \\
 & \underline{+x^4 - 2x^3 + 3x^2} \\
 & \quad\quad -x^3 - x^2 + 4x \\
 & \quad\quad \underline{-x^3 + 2x^2 - 3x} \\
 & \quad\quad\quad\quad -3x^2 + 2x - 1 \\
 & \quad\quad\quad\quad \underline{-3x^2 + x - 4} \\
 & \quad\quad\quad\quad\quad\quad x + 3
\end{array}
$$

So $x^4 - 3x^3 + x^2 - 3x + 1 = (x^2 - 2x + 3)(x^2 – 3x + 3) + (3x + 5)$, remembering that the coefficients are in Z_5. Then $q(x) = x^2 -3x +3$, and $r(x) = 3x+5$.

(2)Consider $f(x) = x^4 + 3x^3 + 2x + 4$ in $Z_5[x]$ and let $g(x)= x - 1$. To find q(x) and r(x), divide f(x) by g(x),

Definition 2.6. Let (R, +, .) be a ring with identity and $f(x) = a_n x^n + a_{n-1} x^{n-1} +\dots +a_0 \in R[x]$. Then if $r \in R$ we define f(r) by $f(r) = a_n r^n + a_{n-1} r^{n-1} +\dots +a_0 \in R$.

Example. Let $f(x) = x^3+4x^2+3 \in Q(x)$. Then $f(2) = 8+4(4)+3=27$

Definition 2.7. Let R be a commutative ring and f(x) a polynomial over R.
Any element $r \in R$ such that $f(r) = 0$ is a zero of f(x) in R(or r is a root of f(x)).

Definition 2.8. Let R be a commutative ring with identity and f(x), g(x) be non zero polynomials in R[x]. Then g(x) is said to be a factor of f(x), if there exists a non zero polynomial $h(x) \in R[x]$ such that $f(x) = h(x) g(x)$.

Example. Let $f(x) = (x-1)(x+5)$ be a polynomial of Z[x]. Then (x-1) is a factor of f(x).

Proposition 2.9. Let f(x) be a polynomial over a commutative ring with identity and a be an element in R. Then a is a root of f(x) if and only if (x-a) is a factor of f(x).
Proof. Suppose (x-a) is a factor of f(x). Then there exists a polynomial q(x) such that $f(x) =q(x) (x-a)$. Then $f(a)= q(a) 0$ which implies $f(a) = 0$, and a is a root of f(x).

Conversely, suppose f(a) =0. By division algorithm, there exist q(x) and r(x) in R[x] such that f(x) =q(x)(x-a)+ r(x) , deg r(x) < deg (x-a) or r(x) =0.
Since deg (x-a) =1, then r(x) is a constant polynomial.
But 0= f(a) = q(a)(a - a)+r(a) = r(a).Hence r(x) =0, consequently f(x) = q(x) (x-a).

Definition 2.10. The element r is a root of multiplicity m of f(x) if $(x-a)^m \mid f(x)$ but $(x-a)^{m+1} \nmid f(x)$. A zero of multiplicity 1 is called simple zero.

Theorem 2.11. (Fundamental theorem of algebra):
If f(x) is a non constant polynomial over the field of complex numbers, then f(x) has at least one root in C.

Theorem 2.12. Let R be an integral domain, f(x) be a non zero polynomial over R. If deg f(x) = n, then f(x) has at most n distinct roots R.
Proof. We proved by induction on the degree of f(x). When deg f(x) = 0, then there exists $0 \neq a_0 \in R$ such that $f(x) = a_0$. This means f(x) has no root in R.
If deg f(x) = 1, then there exists $0 \neq a_1 \in R$ such that $f(x) = a_0 + a_1x$. This means f(x) has at most one root in R; indeed, if a_1 is invertible, $-a_1^{-1}.a_0$ is the 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 r is a root of f(x), then there exists $q(x) \in R[x]$ such that f(x) = (x-r)q(x), where q(x) of degree n-1.
Any root t of f(x) distinct from r must be a root of q(x), by substitution, we have
f(t) = (r – t)q(t) = 0. Since R has no zero divisors, then q(t) = 0. From hypotheses , q(x) has at most n-1 distinct roots. As the only roots of f(x) are r and those of q(x).
That is f(x) cannot have more than n distict roots in R.

The following example shows that the condition that R is an integral domain is the last theorem is necessary.
Example. Consider the ring $R = Z_2 \times Z_2$ .Clearly R is not an integral domain.
Now consider the polynomial $f(x) = x^2 + x$.
It is not difficult to show that every element of $Z_2 \times Z_2$ is a root of f(x). where
$Z_2 \times Z_2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$. So f(x) has four roots.