"Ring, Integral Domain"

Dissertation submitted to the Department of Mathematics in partial fulfillment of the requirements for the award of the degree of Master of Science in Mathematics

Mahapurusha Srimanta Sankaradeva Viswavidyalaya

Department of Mathematics

Submitted By:

Ranju Nepal

Roll No: MAT-14/23

Registration No: MSSV-0023-101-001358

M.sc 4^{th} Semester

Session : 2023-2025

Department of Mathematics
MSSV, Nagaon

Under The Guidance:

Dr. Jugal Khargharia, Professor

Department of Mathematics, MSSV, Nagaon

Certificate

This is to certify that the dissertation entitled **"Ring, Integral Domain"**, submitted by **Ranju Nepal**, Roll No. **MAT-14/23**, Registration No. **MSSV-0023-101-001358**, in partial fulfillment for the award of the degree of **Master of Science in Mathematics**, is a bonafide record of original work carried out under my supervision and guidance.

To the best of my knowledge, the work has not been submitted earlier to any other institution for the award of any degree or diploma.

Dr. Jugal Khargharia
Professor
Department of Mathematics
Mahapurusha Srimanta Sankaradeva Viswavidyalaya,Nagaon

Date: Signature of Guide
Place:

Declaration

I, **Ranju Nepal**, hereby declare that the dissertation titled **"Ring,Integral Domain"**, submitted to the Department of Mathematics, **Mahapurusha Srimanta Sankaradeva Viswavidyalaya**, is a record of original work carried out by me under the supervision of **Dr. Jugal Khargharia**,Professor.

This work has not been submitted earlier to any other institution or university for the award of any degree or diploma.

Place: Ranju Nepal
Date: Roll No.: MAT-14/23

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my guide, **Dr. Jugal Khargharia**, Professor, Department of Mathematics, Mahapurusha Srimanta Sankaradeva Viswavidyalaya, for his valuable guidance, continuous support, and encouragement throughout the course of this dissertation.

I also extend my heartfelt thanks to the faculty members of the Department of Mathematics for their constant academic support and the friendly learning environment they provided.

I am deeply grateful to my family and friends for their unwavering moral support and motivation throughout my academic journey. Their encouragement gave me the strength to successfully complete this work.

Lastly, I thank all those who directly or indirectly helped me during this project.

Place: Ranju Nepal
Date: Roll No.: MAT-14/23

Contents

Introduction

In math, we tend to seek patterns and structures which allow us to understand numbers and operations. One such structure is referred to as a ring. In simple terms, a ring is a collection of elements where we can add and multiply in a manner that adheres to certain fundamental rules—such as how we add and multiply whole numbers. Rings enable us to bring familiar arithmetic to more abstract contexts, using this as a gateway to novel ideas and applications.

In a ring, we can also locate smaller subsets that act similarly to rings themselves. They are referred to as subrings. In the same way that a family may have groups inside it, a ring may have subrings inside, which work under the same norms as the big set.

Another significant ring theory concept is the integral domain. This is a type of ring where multiplication works well—namely, if you multiply two non-zero elements, you never obtain zero. This property, that there are no "zero divisors", is quite handy when solving equations and doing problems in number theory and algebra.

By learning about rings, subrings, and integral domains, we start to see the deeper structure that lies behind most mathematical systems. These concepts are not just abstract but also the foundation upon which many real-world applications in computer science, cryptography, and more are built.

1 RING SUB-RING AND INTEGRAL DOMAIN

Definition 1. *A ring R is a nonempty set equipped with two binary operations, addition and multiplication such that for all $a, b, c \in R$*

(i) Under addition associativty hold good ie.

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

(ii) There exists an element $o \in R$

(called additive identity orzero element) such that,

$$a + o = o + a = a$$

(iii) For any $a \in R$ there exists $-a \in R$ such that,

$$a + (-a) = (-a) + a = 0$$

(iv) Under addition comutativity hold good ie.

$$a + b = b + a$$

(v) Under multiplication associativty hold good ie.

$$a(bc) = (ab)c$$

(vi) Both the distributive laws hold good ie.

$$a(b + c) = ab + ac \text{ and } (b + c)a = ba + ca$$

Definition 2. *A ring R is said to be a commutative ring if*

$$ab = ba \qquad \forall a, b \in R$$

Definition 3. *A ring R is said to be a ring with unity if there exists an element $1 \in R$ such that,*

$$a1 = 1a \qquad \forall a \in R$$

Definition 4. *Suppose R is a commutative ring with unity and a be a nonzero element of the ring R. If there exists an element $b \in R$ such that,*

$$ab = 1 \qquad \forall a, b \in R$$

then the element b is said to be the inverse of the element a in the ring R and we write $b = a^{-1}$ and in such a situation the element a is said to be a unit of the ring R.

Definition 5. *Suppose R is a commutative ring and $a, b \in R$ with $a \neq 0$. Then we say that a divides b (or a is a factor of b) if there exists $c \in R$ such that $b = ac$ ie.*

$$a \mid b \Leftrightarrow b = ac \qquad for\ some\ c \in R$$

Example 1. *The set of integers* $\mathbb{Z}$ *is a commutative ring with unity* 1 *under ordinary addition and multiplication in which* 1 *and* -1 *are the only units.*

Example 2. *The set* $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ *is a commutative ring with unity* 1 *under addition* $(mod\ n)$ *and multiplication* $(mod\ n)$ *in which* $U(n) = \{m \mid gcd(m, n) = 1\}$ *is the set of units.*

Example 3. *The set* $\mathbb{Z}[x] = \{f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z}\}$ *is a commutative ring with unity* $f(x) = 1$ *under ordinary addition and multiplication of polynomials.*

Example 4. *The set* $M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ *is a non-commutative ring with unity* $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *under matrix addition and multiplication.*

Example 5. *The set* $2\mathbb{Z}$ *is a commutative ring without unity under ordinary addition and multiplication.*

Theorem 1. (**A fiew basic results**) *Suppose* R *is a ring with unity* 1 *and* $a, b, c \in R$. *Then the following results are hold good.*

(i)	$a0 = 0a = 0$
(ii)	$a(-b) = (-a)b = -(ab)$
(iii)	$(-a)(-b) = ab$
(iv)	$a(b-c) = ab - ac$ *and* $(b-c)a = ba - ca$
(v)	$(-1)a = -a$
(vi)	$(-1)(-1) = 1$

Proof. By the left distributive law we get,

$$\begin{aligned} a0 = a(0+0) = a0 + a0 &\Rightarrow a0 + 0 = a0 + a0 \\ &\Rightarrow ao = 0 \qquad [by\ left\ cancellation\ law] \end{aligned}$$

By the same set of arguments one can see that,

$$0a = 0$$

This complete the proof of (i).
Here we have,

$$(-a)b + ab = (-a + a)b = 0b = 0 \Rightarrow (-a)b = -(ab)$$

Similarly,

$$a(-b) + ab = a(-b + b) = a0 = 0 \Rightarrow a(-b) = -(ab)$$

It follows that,

$$(-a)b = a(-b) = -(ab)$$

This complete the proof of (ii).
Here we have,

$$\begin{aligned}(-a)(-b) = (-a)c = -(ac) \qquad & where\ \ c = -b \\ = -(a(-b)) = -(-(ab)) &= ab\end{aligned}$$

This complete the proof of (iii).
Here we have,

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac$$

By the same set of argument one can see that,

$$(b - c)a = ba - ca$$

This complete the proof of (iv).
Here we have,

$$(-1)a = -(1a) = -a \qquad [\because \ \ 1a = a]$$

This complete the proof of (v).
The proof of (vi) is left as an exercise. □

Theorem 2. *If a ring R has a unit element a(say)then its inverse is unique.*

Proof. If a is a unit of the ring R then we must have $a \neq 0$. If possible let us assume that there exists $b, c \in R$ such that $ab = ba = 1$ and $ac = cb = 1$. Now,

$$\begin{aligned}a(b - c) = ab - ac = 1 - 1 = 0 \Rightarrow b - c = 0 \qquad & [\because \ \ a \neq 0] \\ \Rightarrow b = c &\end{aligned}$$

It follows that the multiplicative inverse of a unit in a ring R is unique. □

Definition 6. *A nonempty subset S of a ring R is said to be a sub-ring of the ring R if S is itself a ring under the binary operations in the ring R.*

Theorem 3. *A nonempty subset S of a ring R is a sub-ring of the ring R if and only if,*

$$\begin{aligned} (i)\ a-b \in S \qquad & \forall a,b \in S \\ and\ (ii)\ ab \in S \qquad & \forall a,b \in S \end{aligned}$$

Proof. If we assume that S is a sub-ring of the ring R then S will itself a ring under the binary operations in the ring R and therefore,

$$\begin{aligned} a,b \in S &\Rightarrow a,-b \in S \\ &\Rightarrow a-b \in S \end{aligned}$$

Further by the closure property under multiplication,

$$a,b \in S \Rightarrow ab \in S$$

It follows that the given conditions are necessary.
Let us assume that S is a nonempty subset of the ring R in which the given conditions are hold good.
By the given condition (i) immediately follows that S is an additive abelian group.Further both the distributive laws and the associative property for the elements of S will hold good, as because $S \subseteq R$ and they are true for the elements of the ring R. It follows that S is itself a ring under the binary operations in the ring R and consequently S is a sub-ring of the ring R.
It follows that the conditions are sufficient.
This complete the proof. □

Example 6. *One can verify that for a ring R we always have two sub-rings namely $\{0\}$ and the ring R itself, what we call trivial sub-rings of the ring R.*

Example 7. *For the ring $\mathbb{Z}_6$ under addition(mod 6) and multiplication(mod 6), one can verify that $S = \{0, 2, 4\}$ is a sub-ring.*

Example 8. *For any positive integer n,*

$$n\mathbb{Z} = \{0. \pm n, \pm 2n, \pm 3n, \cdots\}$$

is a sub-ring of the ring of integers $\mathbb{Z}$ under ordinary addition and multiplication.

Example 9. *The set of Gaussian integers,*

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\}$$

is a sub-ring of the ring $\mathbb{C}$ under ordinary addition and multiplication of complex numbers.

Definition 7. *Let R be a commutative ring and $a(\neq 0) \in R$. Then a is said to be a zero divisor if there exists $b(\neq 0) \in R$ such that $ab = 0$.*

Example 10. *Let us consider the commutative ring $\mathbb{Z}_{10}$ under addition(mod 10) and multiplication(mod 10).*
In this ring one can note that $2(\neq 0), 5(\neq 0) \in \mathbb{Z}_{10}$ whereas $2.5(mod\ 10) = 0$.
It follows that 2 and 5 both are zero divisors in this ring.
One can verify that 6 is also a zero divisor in this ring.

Definition 8. *An integral domain is a commutative ring with unity having no zero divisor.*

Remark 1. *In case of an integral domain R for $a, b \in R$ if $ab = 0$ then either $a = 0$ or $b = 0$.*

Example 11. *The ring of integers $\mathbb{Z}$ under ordinary addition and multiplication is an integral domain.*

Theorem 4. *Let R be an integral domain and $a, b, c \in R$. Then,*

$$ab = ac \Rightarrow b = c$$

provided $a \neq 0$.

Proof. Suppose that R is an integral domain and $a, b, c \in R$ such that $ab = ac$ with $a \neq 0$.
Now,

$$\begin{aligned} & a(b-c) = ab - ac \\ & \Rightarrow a(b-c) = 0 \qquad\qquad [\because ab = ac] \\ & \Rightarrow (b-c) = 0 \quad [\because a \neq 0\ R\ is\ without\ zero\ divisor] \\ & \Rightarrow b = c \end{aligned}$$

This complete the proof. □

Definition 9. *A field is a commutative ring with unity in which every nonzero element is a unit.*

Remark 2. *One should note that every field is an integral domain for if F is a field and $a, b \in F$ such that $ab = 0$ then if $a \neq 0$ means a is a unit of F ie. $a^{-1} \in F$. But then,*

$$\begin{aligned} ab = 0 &\Rightarrow a^{-1}(ab) = 0 \\ &\Rightarrow (a^{-1}a)b = 0 \\ &\Rightarrow b = 0 \end{aligned}$$

It follows that F is without zero divisor and consequently F is an integral domain.
However an integral domain may not be a field. For instance the ring of integers $\mathbb{Z}$ is an integral domain whereas it is not a field.In true test and colour every nonzero element except the identity element(1)is not a unit in this ring.

Theorem 5. *A finite integral domain is a field.*

Proof. Let D be a finite integral domain with unity 1 and a be a nonzero element of D. We need to prove that a is a unit of D. If $a = 1$ then we are through as because the identity element has its own inverse. Suppose that $a \neq 1$. By the closure property under multiplication in D we have $a, a^2, a^3, \cdots \in D$. Since D is finite, for some positive integers $i, j \ \ (i > j)$,

$$\begin{aligned} a^i = a^j &\Rightarrow a^{i-j} = 1 \\ &\Rightarrow aa^{i-j-1} = 1 \\ &\Rightarrow a^{-1} = a^{i-j-1} \in D \end{aligned}$$

It follows that a is a unit of the integral domain D.
This complete the proof. □

Remark 3. *For every prime p, $\mathbb{Z}_p$ is a field.*

Proof. We know that $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ is a finite commutative ring with unity 1 under addition(mod p) and multiplication(mod p).
In order to prove that $\mathbb{Z}_p$ is an integral domain it is sufficient to prove that $\mathbb{Z}_p$ is without zero divisor.
For any $a, b \in \mathbb{Z}_p$ we have,

$$\begin{aligned} ab = 0 &\Rightarrow ab = pk \quad for\ some\ positive\ integer\ k \\ &\Rightarrow p \mid ab \\ &\Rightarrow p \mid a\ \ or\ \ p \mid b \\ &\Rightarrow a = 0\ \ or\ \ b = 0 \end{aligned}$$

It follows that $\mathbb{Z}_p$ is a finite integral domain and hence it is a field.
This complete the proof. □

Definition 10. *The characteristic of a ring R is the least positive integer n such that $nx = 0 \quad \forall x \in R$.*
If no such positive integer exists then we say that the ring R is of characteristic 0.
The characteristic of a ring R is denoted by $char(R)$.

Remark 4. *The characteristic of the ring of integers $\mathbb{Z}$ under ordinary addition and multiplication is 0 ie. $char(\mathbb{Z}) = 0$.*
The characteristic of the ring $\mathbb{Z}_n$ under addition(mod n)and multiplication(mod n) is n for n is the least positive integer such that for any $i \in \mathbb{Z}_n$ we have $ni(mod\ n) = 0$.

Theorem 6. *Let R be a ring with unity 1. If 1 is of infinite order under addition then the characteristic of the ring R is 0. If 1 is of order n under addition then the characteristic of the ring R is n.*

Proof. If the multiplicative identity 1 is of infinite order then there exists no positive integer n such that $n1 = 0$ and hence $char(R) = 0$.
Suppose that $\mid 1 \mid = n$ under addition ie. n is the least positive integer such that $n1 = 0$. Now for any $x \in R$ we have,

$$\begin{aligned} nx &= x + x + x + \cdots n\ \ summands \\ &= 1x + 1x + 1x + \cdots n\ \ summands \\ &= (1 + 1 + 1 + \cdots n\ \ summands)x \\ &= (n1)x \\ &= 0 \qquad\qquad [\because\ \ n.1 = 0] \end{aligned}$$

It follows that $char(R) = n$.
This complete the proof. □

Theorem 7. *The characteristic of an integral domain is either zero or a prime.*

Proof. Let D be an integral domain with unity 1.
In case 1 is of infinite order then $char(D) = 0$.
Suppose that $\mid 1 \mid = n$. We need to prove that n is a prime. Suppose that $n = pq$ where p, q are primes and $1 \leq p, q \leq n$.
Since $\mid 1 \mid = n$ under addition therefore n is the least positive integer such that $n1 = 0$.
Now,

$$\begin{aligned} n1 = 0 &\Rightarrow (pq)1 = 0 \\ &\Rightarrow (p1)(q1) = 0 \\ &\Rightarrow p1 = 0\ \ or\ \ q1 = 0 \qquad\qquad [\ \because\ \ D\ \ is\ \ without\ \ zero\ \ divisor] \end{aligned}$$

In case $p1 = 0$ we must have $p = n$, because $p \leq n$ and n is the least positive integer such that $n1 = 0$.
In case $q1 = 0$ by the same set of argument one can see that $q = n$.
It follows that n is a prime.
This complete the proof. □

2 IDEAL AND FACTOR RING

Definition 11. *A sub-ring A of a ring R is said to be an ideal (two sided ideal) if the sub-ring A absorbs the elements in the ring R ie. $rA = \{ra \mid r \in R \text{ and } a \in A\} \subseteq A$ and $Ar = \{ar \mid r \in R \text{ and } a \in A\} \subseteq A$.*

Theorem 8. *A nonempty subset A of a ring R is an ideal of the ring if and only if,*

$$\begin{aligned} &(i)\ a - b \in A && \forall a, b \in A \\ &(ii)\ ra, ar \in A && \forall r \in R \text{ and } \forall a \in A \end{aligned}$$

The proof is left as an exercise.

Example 12. *In a ring R the subsets $\{0\}$ and R are always ideal of the ring R, what we call trivial ideals of the ring R.*

Example 13. *For any positive integer n, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \cdots\}$ is an ideal of the ring of integers $\mathbb{Z}$ under ordinary addition and multiplication.*

Example 14. *Suppose R is a commutative ring with unity 1. Then for any $a \in R$ the set $< a >= \{ra \mid r \in R\}$ is an ideal of the ring R what we call a principal ideal of the ring R generated by the element a.*

Proof. Suppose that $ra, sa \in < a >$ so that $r, s \in R$.
now,

$$ra - sa = (r - s)a \in < a > \qquad [\ \because r - s \in R]$$

Also,

$$s(ra) = (sr)a \in < a > \qquad [\ \because rs \in R]$$

It follows that $< a >$ is an ideal of the ring R. □

Example 15. *Consider the ring $\mathbb{R}[x] = \{f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{R}\}$ under ordinary addition and multiplication of polynomials. Suppose that $A \subseteq \mathbb{R}[x]$ containing those polynomials with the constant term $a_0 = 0$ then A is an ideal of the ring $\mathbb{R}[x]$ and $A =< x >$.*

Proof. From the definition,

$$A = \{f(x) \in \mathbb{R}[x] \mid f(x) = a_1x + a_2x^2 + \cdots + a_nx^n\}$$

Suppose that $f(x) = a_1x+a_2x^2+\cdots+a_nx^n$ and $g(x) = b_1x+b_2x^2+\cdots+b_mx^m$ be any two elements of A.
Without loss of generality we can assume that $m \leq n$ so that,

$$f(x) - g(x) = (a_1 - b_1)x + (a_2 - b_2)x^2 + \cdots + (a_m - b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n$$

It follows that $f(x) - g(x) \in A$.
For any $h(x) = c_0 + c_1x + c_2x^2 + \cdots + c_kx^k \in \mathbb{R}[x]$ we have,

$$\begin{aligned} h(x)f(x) &= (c_0 + c_1x + c_2x^2 + \cdots + c_kx^k)(a_1x + a_2x^2 + \cdots + a_nx^n) \\ &= 0c_0 + (c_0a_1)x + (c_0a_2 + c_1a_1)x^2 + \cdots + (c_0a_n + c_1a_{n-1} + \cdots + c_{n-1}a_1x^n) \in A \end{aligned}$$

It follows that A is an ideal of the ring $\mathbb{R}[x]$.
For any $f(x) = a_1x + a_2x^2 + \cdots + a_nx^n \in A$ we have,

$$\begin{aligned} f(x) &= a_1x + a_2x^2 + \cdots + a_nx^n \\ &= (a_1 + a_2x + \cdots + a_nx^{n-1})x \\ &= f'(x).x \ \ where \ \ f'(x) = a_1 + a_2x + \cdots + a_nx^{n-1} \in \mathbb{R}[x] \end{aligned}$$

It follows that $A \subseteq < x >$.
On the other hand for any $p(x) \in < x >$ there exists $q(x) = c_0 + c_1x + c_2x^2 + \cdots + c_sx^s \in \mathbb{R}[x]$ such that,

$$\begin{aligned} p(x) &= q(x).x \\ &= (c_0 + c_1x + c_2x^2 + \cdots + c_sx^s).x \\ &= c_0x + c_1x^2 + c_2x^3 + \cdots + c_sx^{s+1} \in A \end{aligned}$$

It follows that $< x > \subseteq A$ and hence $A = < x >$. □

Example 16. *Let R be the ring of all real valued functions of a real variable and S be the set of all differentiable functions. Then S is a sub-ring of R but S is not an ideal of the ring R.*

Proof. Clearly $R = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ is a ring under point wise addition and point wise multiplication of functions ie.

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) && \forall x \in \mathbb{R} \\ (fg)(x) &= f(x)g(x) && \forall x \in \mathbb{R} \end{aligned}$$

It is given that,

$$S = \{f : \mathbb{R} \to \mathbb{R} \mid f' exists\}$$

For any $f, g \in S$ we have $(f-g)' = f' - g'$ and $(fg)' = fg' + gf'$. It follows that $f - g \in S$ and $fg \in S$ and consiquently S is a sub-ring of the ring R. Let us choose an element $f \in R$ so that f' does not exists.Then for any $g \in S$ we have $(fg)' = fg' + gf'$. It follows that $(fg)'$ does not exists and hence $fg \notin S$. Thus S is not an ideal of the ring R. □

At this point we would like to raise a pertinent question. Whether the concept of the principal ideal can be generalized or not? Honestly speaking the answer is affirmative. Yes one can do so as given in the following definition.

Definition 12. *Suppose that R is a commutative ring with unity and $a_1, a_2, \cdots, a_n \in R$. Then $I =< a_1, a_2, \cdots, a_n >= \{\sum_{i=1}^{n} r_i a_i \mid r_i \in R\}$ is an ideal of the ring R, what we call the ideal generated by the elements $a_1, a_2, \cdots, a_n$.*

Definition 13. *Let A be an ideal of a ring R. We now consider the set $R/A = \{r + A \mid r \in R\}$.Then R/A is a ring under the operations define by,*

$$\begin{aligned} &(r+A)+(s+A) = (r+s)+A && \forall r, s \in R \\ &\text{and } (r+A)(s+A) = (rs)+A && \forall r, s \in R \end{aligned}$$

with A as the zero element,what we call the factor ring or the quotient ring.

Proof. Let us first verify that the multiplication as defined above is well defined. For this we choose $r, r', s, s' \in R$ such that,

$$\begin{aligned} & r + A = r' + A \quad \text{and} \quad s + A = s' + A \\ & \Rightarrow r - r' + A = A \quad \text{and} \quad s - s' + A = A \\ & \Rightarrow r - r' = a \quad \text{and} \quad s - s' = b \text{ where } a, b \in A \\ & \Rightarrow r = r' + a \quad \text{and} \quad s = s' + b \\ & \Rightarrow rs = r's' + r'b + s'a + ab \\ & \Rightarrow (rs) + A = (r's') + A \end{aligned}$$

Since A is an ideal of the ring R therefore $r'b + s'a + ab \in A$ and hence $(r'b + s'a + ab) + A = A$.It follows that the multiplication is well defined. Suppose that A be a sub-ring of the ring R but it is not an ideal. Then there exists $a \in A$ and $r \in R$ such that $ra \notin A$. It follows that $ra + A \neq A$ which means that $(r + A)(s + A) \neq A$. But $(r + A)(a + A) = (r + A)A = (r + A)(0 + A) = r0 + A = A$. Thus we arrived into a contradiction, which leads us to a conclusion that A must be an ideal in order to enjoy a well defined multiplication. □

Example 17. *Let us consider the ring of integers $\mathbb{Z}$ under ordinary addition and multiplication. For the ideal $4\mathbb{Z}$ of the ring $\mathbb{Z}$ we can enjoy the factor ring $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$ in which the addition and multiplication are defined by,*

$$(m + 4\mathbb{Z}) + (n + 4\mathbb{Z}) = (m + n)(mod\ 4) + 4\mathbb{Z}\ where\ 0 \leq m, n \leq 3$$
$$and\ (m + 4\mathbb{Z})(n + 4\mathbb{Z}) = (mn)(mod\ 4) + 4\mathbb{Z}$$

Remark 5. *One should note that both the ring $\mathbb{Z}$ and the ideal $4\mathbb{Z}$ contains infinitely many distinct elements whereas the factor ring $\mathbb{Z}/4\mathbb{Z}$ contains only four elements.This is why one can readily deal with a factor ring and a good number of information in respect of the ring can be drawn from the factor ring.*

Example 18. *Let us consider the ring of Gaussian integers $\mathbb{Z}[i]$ and the principal ideal $A =< 2 - i >$. Then the elements of the factor ring $\mathbb{Z}[i]/A$ will be of the form $a + ib + A$ where $a, b \in \mathbb{Z}$.*
Since $2 - i \in A$ therefore $2 - i + A = A$.It follows that $2 - i = 0$ ie. $i = 2$.But then $4 = -1$ and hence $5 = 4 + 1 = -1 + 1 = 0$. Thus the element $3 + 4i + A = 11 + A = (2 \times 5 + 1) + A = 1 + A$.
It follows that,

$$\mathbb{Z}[i]/A = \{0 + A, 1 + A, 2 + A, 3 + A, 4 + A\}$$

Here we again meet a finite factor ring whereas both the ring and the ideal in question are infinite.

Definition 14. *A prime ideal P of a commutative ring R is a proper ideal of the ring R such that,*

$$ab \in P \Rightarrow a \in P\ or\ b \in P \qquad\qquad \forall a, b \in R$$

Definition 15. *A maximal ideal of a commutative ring R is a proper ideal of the ring R such that for any ideal A of R,*

$$M \subseteq A \subseteq R \Rightarrow M = A\ or\ A = R$$

Theorem 9. *Let R be a commutative ring with unity and A be an ideal of the ring R.Then R/A is an integral domain if and only if A is a prime ideal.*

Proof. Suppose that R/A is an integral domain.We need to show that A is a prime ideal of the ring R. We now have,

$$\begin{aligned} ab \in A &\Rightarrow ab + A = A \\ &\Rightarrow (a + A)(b + A) = A \\ &\Rightarrow a + A = A\ or\ b + A = A \qquad [\ \because R/A\ is\ an\ integral\ domain] \\ &\Rightarrow a \in A\ or\ b \in A \end{aligned}$$

It follows that A is a prime ideal of the ring R.
Conversely suppose that A be a prime ideal of the ring R and $a, b \in R$ such that,

$$\begin{aligned}(a+A)(b+A) = A &\Rightarrow (ab+A) = A \\ &\Rightarrow ab \in A \\ &\Rightarrow a \in A \ \ or \ \ b \in A \qquad [\ \because A \ is \ a \ prime \ ideal] \\ &\Rightarrow a + A = A \ \ or \ \ b + A = A\end{aligned}$$

It follows that R/A is without zero divisor and hence it is an integral domain. □

Theorem 10. *Let R be a commutative ring with unity and A be an ideal of the ring R. Then R/A is a field if and if A is a maximal ideal of the ring R.*

Proof. Suppose that R/A is a field and B is an ideal of the ring R such that $A \subset B$. Then there exists $b \in B$ such that $b \notin A$.
We now have,

$$\begin{aligned}b \notin A &\Rightarrow b + A \neq A \\ &\Rightarrow \ there \ exists \ c \in R \ such \ that \ (c+A)(b+A) = 1 + A \ [\ \because \ R/A \ is \ a \ field] \\ &\Rightarrow 1 - bc \in A \\ &\Rightarrow 1 - bc \in B \qquad [\ \because \ A \subset B] \\ &\Rightarrow 1 - bc + bc \in B \qquad [\ \because bc \in B] \\ &\Rightarrow 1 \in B \\ &\Rightarrow B = R\end{aligned}$$

It follows that A is a maximal ideal of the ring R.
Conversely suppose that A is a maximal ideal of the ring R. We need to prove that R/A is a field, for which it is sufficient to prove that every nonzero element of R/A is a unit of R/A.
Let $b + A \in R/A$ and $b + A \neq A$. We now consider the set $B = \{br + a \mid r \in R \ and \ a \in A\}$. One can easily verify that B is an ideal of the ring R and $A \subset B$. Since A is a maximal ideal of the ring R therefore $B = R$. It follows that for some $c \in R$,

$$\begin{aligned}bc + a = 1 &\Rightarrow bc + a + A = 1 + A \\ &\Rightarrow (b+A)(c+A) = 1 + A\end{aligned}$$

It follows that $b + A$ is a unit of R/A and hence R/A is a field. □

3 RING HOMOMORPHISM AND RING ISOMORPHISM

Definition 16. *Let R and S be any two rings and $\phi : R \to S$ be a function that preserves the binary operations in the rings R and S ie.*

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b) \qquad \forall a, b \in R$$

is said to be a ring homomorphism.
If a ring homomorphism $\phi : R \to S$ is a bijection then it is said to be a ring isomorphism and in such case we say that the rings R and S are isomorphic to each other and we denote it by $R \approx S$.

Definition 17. *If $\phi : R \to S$ is a ring homomorphism then the subset $\{r \in R \mid \phi(r) = 0\}$ of the ring R is said to be the kernal of the homomorphism ϕ and it is denoted by $ker(\phi)$.*

$$\therefore \ ker(\phi) = \{r \in R \mid \phi(r) = 0\}$$

Example 19. *Consider the rings $\mathbb{Z}$ and $\mathbb{Z}_n$ and define a function $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by,*

$$\phi(k) = k(mod\, n) \qquad \forall k \in \mathbb{Z}$$

For any $k, s \in \mathbb{Z}$ we have,

$$\phi(k+s) = (k+s)(mod\, n) = k(mod\, n) + s(mod\, n) = \phi(k) + \phi(s)$$
$$\text{and } \phi(ks) = (ks)(mod\, n) = k(mod\, n)s(mod\, n) = \phi(k)\phi(s)$$

It follows that $\phi : \mathbb{Z} \to \mathbb{Z}_n$ is a ring homomorphism

Example 20. *The mapping $\phi : \mathbb{C} \to \mathbb{C}$ defined by,*

$$\phi(a+ib) = a - ib \ ie.\ \phi(z) = \overline{z} \qquad \forall z = a + ib \in \mathbb{C}$$

is a ring homomorphism.

Example 21. *A positive integer n with decimal expression $\cdot a_k a_{k-1} \cdots a_1 a_0$ is divisible by 9 if and only if $a_k + a_{k-1} + \cdots + a_1 + a_0$ is divisible by 9.*
Solution: *Let us consider the function $\alpha : \mathbb{Z} \to \mathbb{Z}_9$ defined by,*

$$\alpha(n) = n(mod\, 9) \qquad \forall n \in \mathbb{Z}$$

We have already shown that $\alpha : \mathbb{Z} \to \mathbb{Z}_9$ is a ring homomorphism.
But,

$$\begin{aligned}
& n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10^1 + a_0 \\
9 \mid n & \Leftrightarrow \alpha(n) = 0 \\
& \Leftrightarrow \alpha(a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10^1 + a_0) = 0 \\
& \Leftrightarrow \alpha(a_k)(\alpha(10))^k + \alpha(a_{k-1})(\alpha(10))^{k-1} + \cdots + \alpha(a_1)\alpha(10) + \alpha(a_0) = 0 \\
& \Leftrightarrow \alpha(a_k) + \alpha(a_{k-1} + \cdots + \alpha(a_1) + \alpha(a_0)) = 0 \qquad [\because \alpha(10) = 1] \\
& \Leftrightarrow \alpha(a_k + a_{k-1} + \cdots + a_1 + a_0) = 0 \\
& \Leftrightarrow 9 \mid (a_k + a_{k-1} + \cdots + a_1 + a_0)
\end{aligned}$$

Theorem 11. *Let R and S be any two rings and $\phi : R \to S$ be a ring homomorphism. Let A be a sub-ring of the ring R and B be an ideal of the ring S. Then,*
(1)For any $r \in R$ and for any positive integer n,

$$\phi(nr) = n\phi(r) \text{ and } \phi(r^n) = (\phi(r))^n$$

(2) $\phi(A) = \{\phi(a) \mid a \in A\}$ is a sub-ring of the ring S.
(3) $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of the ring R.
(4)If R is commutative then $\phi(R)$ is commutative.
(5) $ker(\phi)$ is an ideal of the ring R.
(6) ϕ is one one if and only if $ker(\phi) = \{0\}$
(7)If the ring R has the unity 1 and $S \neq \{0\}$ and ϕ is onto then $\phi(1)$ is the unity of the ring S.
(8)If A is an ideal of the ring R and ϕ is onto then $\phi(A)$ is an ideal of the ring S.
(9)If $\phi : R \to S$ is an isomorphism then $\phi^{-1} : S \to R$ is an isomorphism.

Proof. (1)For $n = 2$, since ϕ is a ring homomorphism therefore we get, $\phi(2r) = \phi(r + r) = \phi(r) + \phi(r) = 2\phi(r)$.
It follows that the result is true for $n = 2$. Let us assume that the result is true for any positive integer $k < n$. We now have,

$$\begin{aligned}
\phi((k+1)r) &= \phi(kr + r) \\
&= \phi(kr) + \phi(r) && [\because \ \phi \ is \ a \ ring \ homomorphism] \\
&= k\phi(r) + \phi(r) && [\because \ the \ result \ is \ true \ for \ n = k] \\
&= (k+1)\phi(r)
\end{aligned}$$

It follows that the result is true for $(k + 1)$ and therefore by mathematical induction the result is true for any positive integer n.

By the same set of arguments one can prove the other part of the result.
(2)For any $\phi(a), \phi(b) \in \phi(A)$ we have,

$$\begin{aligned}\phi(a), \phi(b) \in \phi(A) &\Rightarrow a, b \in A \\ &\Rightarrow a-b, ab \in A \qquad [\because\ A\ is\ a\ sub-ring\ of\ the\ ring\ R] \\ &\Rightarrow \phi(a-b) = \phi(a) - \phi(b),\ \ \phi(ab) = \phi(a)\phi(b) \in \phi(A)\end{aligned}$$

It follows that $\phi(A)$ is a sub-ring of the ring S.
(3)Suppose that $s, t \in \phi^{-1}(B)$ and $r \in R$. We now have,

$$\begin{aligned}&s, t \in \phi^{-1}(B)\ \ and\ \ r \in R \Rightarrow \phi(s), \phi(t) \in B\ \ and\ \ \phi(r) \in S \\ &\Rightarrow \phi(s) - \phi(t), \phi(r)\phi(s), \phi(s)\phi(r) \in B\ [\because\ B\ is\ an\ ideal\ of\ the\ ring\ S] \\ &\Rightarrow \phi(s-t), \phi(rs), \phi(sr) \in B \qquad [\because\ \phi\ is\ a\ ring\ homomorphism] \\ &\Rightarrow s-t, rs, sr \in \phi^{-1}(B)\end{aligned}$$

It follows that $\phi^{-1}(B)$ is an ideal of the ring R.
(4)Suppose that the ring R is a commutative ring and $\phi(a), \phi(b) \in \phi(R)$. Then we have,

$$\begin{aligned}\phi(a), \phi(b) \in \phi(R) &\Rightarrow a, b \in R \\ &\Rightarrow ab = ba \qquad [\because\ R\ is\ commutative] \\ &\Rightarrow \phi(ab) = \phi(ba) \\ &\Rightarrow \phi(a)\phi(b) = \phi(b)\phi(a)\end{aligned}$$

It follows that $\phi(R)$ is a commutative ring.
(5)From the definition we have,

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

We now have,

$$\begin{aligned}0 + 0 = 0 &\Rightarrow \phi(0+0) = \phi(0) \\ &\Rightarrow \phi(0) + \phi(0) = 0 + \phi(0) \\ &\Rightarrow \phi(0) = 0 \qquad [by\ right\ cancellation\ law\ in\ (S, +)]\end{aligned}$$

It follows that $0 \in ker(\phi)$ and therefore one can conclude that $ker(\phi)$ is a nonempty subset of the ring R.
For any $x, y \in ker(\phi)$ and $r \in R$we have,

$$\begin{aligned}&\phi(x-y) = \phi(x) - \phi(y)\ \ and\ \ \phi(rx) = \phi(r)\phi(x)\ \ and\ \ \phi(xr) = \phi(x)\phi(r) \\ &\Rightarrow \phi(x-y) = \phi(rx) = \phi(xr) = 0 \qquad [\because\ \phi(x) = 0 = \phi(y)]\end{aligned}$$

It follows that $x-y, rx, xr \in \ker(\phi)$ and hence $ker(\phi)$ is an ideal of the ring R.
(6)Suppose that $ker(\phi) = \{0\}$ and r, s are any two elements of the ring R. Now,

$$\begin{aligned}\phi(r) = \phi(s) &\Rightarrow \phi(r-s) = 0 \\ &\Rightarrow r - s \in ker(\phi) \\ &\Rightarrow r - s = 0 \qquad\qquad [\because\ ker(\phi) = \{0\}] \\ &\Rightarrow r = s\end{aligned}$$

It follows that the function $\phi : R \to S$ is one one.
Conversely suppose that the function $\phi : R \to S$ is one one. We need to prove that $ker(\phi) = \{0\}$.
Clearly $\{0\} \subseteq ker(\phi)$. For any $x \in ker(\phi)$ we must have $\phi(x) = 0 = \phi(0)$ and since ϕ is one one therefore $x = 0$ and hence $ker(\phi) \subseteq \{0\}$. It follows that $ker(\phi) = \{0\}$.
(7)Suppose that the ring R is with unity 1 and $\phi : R \to S$ is onto and $S \neq \{0\}$. For any $s(\neq 0) \in S$ there exists $r \in R$ such that $\phi(r) = s$. We now have,

$$s\phi(1) = \phi(r)\phi(1) = \phi(r) = s$$

On the other hand if $s(= 0) \in S$ then obviously $s\phi(1) = 0 = s$.
It follows that $\phi(1)$ serve as the identity of the ring S
(8)Suppose that A is an ideal of the ring R and the function $\phi : R \to S$ is onto. Then for any $s \in S$ there exists $r \in R$ such that $\phi(r) = s$. We now have,

$$\begin{aligned}\phi(a), \phi(b) \in \phi(A) &\Rightarrow a, b \in A \\ &\Rightarrow a - b, ra, ar \in A \quad [\because\ A \textit{ is an ideal of the ring } R] \\ &\Rightarrow \phi(a-b), \phi(ra), \phi(ar) \in \phi(A) \\ &\Rightarrow \phi(a) - \phi(b), s\phi(a), \phi(a)s \in \phi(A)\end{aligned}$$

It follows that $\phi(A)$ is an ideal of the ring S.
(9)Left as an exercise. □

Theorem 12. (***First isomorphism theorem***) *Let $\phi : R \to S$ be a ring homomorphism. Then $R/ker(\phi) \approx \phi(R)$.*

Proof. Let us define a function $f : R/ker(\phi) \to \phi(R)$ by,

$$f(rker(\phi)) = \phi(r) \qquad\qquad \forall r \in R$$

For any $r, r' \in R$ we have,

$$\begin{aligned} f(rker(\phi)) = f(r'ker(\phi)) &\Rightarrow \phi(r) = \phi(r') \\ &\Rightarrow \phi(r - r') = 0 \\ &\Rightarrow (r - r') \in ker(\phi) \\ &\Rightarrow rker(\phi) = r'ker(\phi) \end{aligned}$$

Again for any $s \in \phi(R)$ there exists $r \in R$ such that $s = \phi(r) = f(rker(\phi))$. It follows that the function $f : R/ker(\phi) \to \phi(R)$ is a bijection.
On the other hand any $r, r' \in R$ we have,

$$\begin{aligned} f(rker(\phi) + r'ker(\phi)) &= f((r + r')ker(\phi)) \\ &= \phi(r + r') \\ &= \phi(r) + \phi(r') \qquad [\because \ \phi \ is \ a \ ring \ homomorphism] \\ &= f(rker(\phi)) + f(r'ker(\phi)) \end{aligned}$$

Also,

$$\begin{aligned} f((rker(\phi))(r'ker(\phi))) &= f((rr')ker(\phi)) \\ &= \phi(rr') \\ &= \phi(r)\phi(r') \\ &= f(rker(\phi))f(r'ker(\phi)) \end{aligned}$$

It follows that the function $f : R/ker(\phi) \to \phi(R)$ is a ring isomorphism and consequently $R/ker(\phi) \approx \phi(R)$.
This complete the proof. □

Theorem 13. *Every ideal of a ring R is the kernal of a homomorphism on the ring R.*

Proof. Suppose A be an ideal of the ring R.Consider the mapping $\phi : R \to R/A$ defined by,

$$\phi(r) = r + A \qquad \forall r \in R$$

One can note that,

$$\begin{aligned} x \in ker(\phi) &\Leftrightarrow \phi(x) = A(the \ zero \ element \ of \ the \ ring \ R/A) \\ &\Leftrightarrow x + A = A \\ &\Leftrightarrow x \in A \end{aligned}$$

It follows that, $ker(\phi) = A$.
This complete the proof. □

Theorem 14. *Let R be a ring with unity 1. Then the mapping $\phi : \mathbb{Z} \to R$ defined by,*

$$\phi(n) = n.1 \qquad\qquad \forall n \in \mathbb{Z}$$

is a ring homomorphism.

Proof. For any $m, n \in \mathbb{Z}$ one can see that $\phi(m+n) = (m+n).1 = m.1+n.1 = \phi(m)+\phi(n)$. On the other hand $\phi(mn) = (mn).1 = (m.1)(n.1) = \phi(m)\phi(n)$. It follows that the function $\phi : \mathbb{Z} \to R$ is a ring homomorphism.
This complete the proof. □

Corollary 1. *If R is a ring with unity 1 and $char(R) = n(> 0)$ then the ring R has a sub-ring isomorphic to $\mathbb{Z}_n$. If $char(R) = 0$ then the ring R has a sub-ring isomorphic to $\mathbb{Z}$.*

Proof. It is given that R is a ring with unity 1. We consider the set $S = \{k.1 | k \in \mathbb{Z}\}$. Then the mapping $\phi : \mathbb{Z} \to S$ defined by,

$$\phi(k) = k.1 \qquad\qquad \forall k \in \mathbb{Z}$$

is a ring homomorphism for which one can conclude that $\phi(\mathbb{Z}) = S$ is a sub-ring of the ring R.
Suppose that $char(R) = n(> 0)$. Then $\phi(n) = n.1 = 0$. It follows that $n \in ker(\phi)$ and hence $ker(\phi) \subseteq < n >$.
On the other hand,

$$\begin{aligned} r \in < n > &\Rightarrow r = nk \qquad for\ some\ k \in \mathbb{Z} \\ &\Rightarrow \phi(r) = \phi(n)\phi(k) \\ &\Rightarrow \phi(r) = 0 \\ &\Rightarrow r \in ker(\phi) \end{aligned}$$

It follows that $< n > \subseteq ker(\phi)$ and hence $< n >= ker(phi)$.. Thus by first isomorphism theorem $\mathbb{Z}/ < n > \approx S$. But $\mathbb{Z}/ < n > \approx \mathbb{Z}_n$ and hence $S \approx \mathbb{Z}_n$.
Suppose that $char(R) = 0$ then $\mathbb{Z}/ < 0 > \approx S$. But $\mathbb{Z}/ < 0 > \approx \mathbb{Z}$. It follows that $S \approx \mathbb{Z}$.
This complete the proof. □

Corollary 2. *A field always contains $\mathbb{Z}_p$ or $\mathbb{Q}$ where p is some prime.*

Proof. It is well known fact that the characteristic of a field is either a prime or zero. Suppose that F is a field and $char(F) = p$(a prime). Then F has a sub-ring S(say) such that $S \approx \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a field therefore S is a sub-field

of the field F which is isomorphic to $\mathbb{Z}_p$. In simple words one can conclude that the field F contains $\mathbb{Z}_p$.
In case $char(F) = 0$ then F has a sub-ring S(say) such that $S \approx \mathbb{Z}$.
Suppose that,

$$T = \{ab^{-1} | a, b \in S \ and \ b \neq 0\} \subset F$$

From the construction of T one can conclude that $T \approx \mathbb{Q}$ and hence the field F has a sub-field isomorphic to the field of rationals $\mathbb{Q}$. In other words one can say that F contains $\mathbb{Q}$.
This complete the proof. □

4 FIELD OF QUOTIENTS

Suppose that D be an integral domain ie. D is a commutative ring with unity 1 and D is without zero divisor.
Let us choose the set, $S = \{(a, b) | a, b \in D \ and \ b \neq 0\}$.
We now define a relation $\sim$ in the set S by,

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc \qquad \forall\, a, b, c, d \in D \ \ b \neq 0 \ and \ d \neq 0$$

For any $(a, b) \in S$ we always have $ab = ab$ for which $(a, b) \sim (a, b)$.
It follows that the relation $\sim$ is reflexive one.
For any $(a, b), (c, d) \in S$ we have,

$$\begin{aligned} (a, b) \sim (c, d) &\Rightarrow ad = bc \\ &\Rightarrow cb = da \\ &\Rightarrow (c, d) \sim (a, b) \end{aligned}$$

It follows that the relation $\sim$ is symmetric one.
For any $(a, b), (c, d), (r, s) \in S$ we have,

$$\begin{aligned} (a, b) \sim (c, d) \ and \ (c, d) \sim (r, s) &\Rightarrow ad = bc \ and \ cs = dr \\ &\Rightarrow (ad)(cs) = (bc)(dr) \\ &\Rightarrow as = br \\ &\Rightarrow (a, b) \sim (r, s) \end{aligned}$$

It follows that the relation $\sim$ is transitive one.
It follows that the relation $\sim$ is an equivalence relation in the set S.
Let F be the collection of all equivalence classes under the equivalence relation

$\sim$ *and we denote an equivalence class containing* (x, y) *by* x/y. *We define addition and multiplication in* F *by,*

$$a/b + c/d = (ad + bc)/bd \text{ and } a/b.c/d = ac/bd$$

Let us try to show that the operations as defined above are well defined. Suppose that $(a, b), (a', b'), (c, d), (c', d') \in S$ *such that* $a/b = a'/b'$ *and* $c/d = c'/d'$.
Now,

$$\begin{aligned}(ad + bc)b'd' &= adb'd' + bcb'd' \\ &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') \ [\because a/b = a'/b' \text{ and } c/d = c'/d'] \\ &= (a'd' + c'b')(bd)\end{aligned}$$

It follows that,

$$(ad + bc)/bd = (a'd' + c'b')/b'd' \Rightarrow a/b + c/d = a'/b' + c'/d'$$

It follows that addition is well defined.
On the other hand, $(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd)$. *It follows that,*

$$ac/bd = a'c'/b'd' \Rightarrow a/b.c/d = a'/b'.c'/d'$$

It follows that the multiplication in F *is also well defined.*
One can verify that F *is a field under the binary operations as defined. Further one can note that,*

$$\begin{aligned}1 \text{ is the unity unity of } D \Rightarrow 0/1 \text{ is the zero element of } F \\ a/b \in F \Rightarrow -a/b \in F \text{ which is the negative of } a/b \\ a/b(\neq 0/1) \in F \Rightarrow b/a \text{ is the multiplicative inverse of } a/b\end{aligned}$$

Finally one can see that the mapping $\phi : D \to F$ *define by,*

$$\phi(a) = a/1 \qquad \forall\, a \in D$$

is an isomorphism for any $a, b \in D$,

$$\begin{aligned}\phi(a + b) &= (a + b)/1 = a/1 + b/1 = \phi(a) + \phi(b) \\ \phi(ab) &= (ab)/1 = a/1b/1 = \phi(a)\phi(b)\end{aligned}$$

It follows that $D \approx \phi(D)$ *ie.* D *is isomorphic to an integral domain of* F. *In simple words one can say that the field* F *contains the integral domain* D.
At this point one can note that from the integral domain of integers $\mathbb{Z}$ *employing the above mentioned binary operations the construction of the field of rationals* $\mathbb{Q}$ *can be completed.*

5 POLYNOMIAL RINGS

Let us consider a commutative ring R and we consider the set of polynomials,

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 |\ a_i \in R,\ \ 0 \leq i \leq n\}$$

Let us choose any two elements $f(x), g(x)$ of $R[x]$ given by,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$and\ g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

We define addition and multiplication in the set $R[x]$ by,

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

where $s = max\{m, n\}$ and $a_i = 0\ \ for\ \ i > n$ and $b_i = 0\ \ for\ \ i > m$.
Also,

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0$$

where

$$c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k\ \ for\ \ 0 \leq k \leq (m+n)$$

One can verify that $R[x]$ is a ring under addition and multiplication as defined above with the zero element $o(x) = 0$ and the identity element $I(x) = 1$ what we call the ring of polynomials with the coefficients in the ring R.

Definition 18. *For an element $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in the ring $R[x]$ with $n \neq 0$, we say that the degree of $f(x)$ is n and we denote it by $deg(f(x))$ while a_n is said to be the leading coefficient of the polynomial $f(x)$.*
In case the leading coefficient $a_n = 1$(the multiplicative identity of the ring R)we term $f(x)$ as a monic polynomial.

Theorem 15. *If D is an integral domain then $D[x]$ is also an integral domain.*

Proof. AS D is assumed an integral domain it is a commutative ring with unity without zero divisor. It follows that $D[x]$ is a commutative ring with unity $I(x) = 1$.
Let us consider two nonzero elements of $D[x]$ given by,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$and\ \ g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

with $a_n \neq 0$ and $b_m \neq 0$.
By definition the leading element of $f(x)g(x)$ is given by $a_n b_m \neq 0$ as because $a_n, b_m \in D$ and D is an integral domain, consequently $f(x)g(x) \neq 0$.It follows that $D[x]$ is without zero divisor and hence $D[x]$ is an integral domain.
This complete the proof. □

Theorem 16. *Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ such that,*

$$f(x) = q(x)g(x) + r(x) \ \textit{where} \ r(x) = 0 \ \textit{or} \ deg(r(x)) < deg(g(x))$$

Proof. In case $f(x) = 0$ or $deg(f(x)) < deg(g(x))$ we write,

$$f(x) = 0g(x) + f(x)$$

where $q(x) = 0$ and $r(x) = f(x)$.
Let us assume that $n = deg(f(x)) \geq deg(g(x)) = m$ and let,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ \textit{with} \ a_n \neq 0$$
$$\textit{and} \ g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \ \textit{with} \ b_m \neq 0$$

Dividing $f(x)$ by $g(x)$ we get,

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + f_1(x) \ \textit{where} \ deg(f_1(x)) < deg(f(x))$$

Since $deg(f_1(x)) < deg(f(x))$ by induction hypothesis there exists $q_1(x)$ and $r_1()x$ such that,

$$f_1(x) = q_1(x)g(x) + r_1(x) \ \textit{where} \ r_1(x) = 0 \ \textit{or} \ deg(r_1(x)) < deg(g(x))$$

It follows that $f(x) = (a_n b_m^{-1} x^{n-m} + q_1(x))g(x) + r_1(x)$ and therefore one can write $f(x) = q(x)g(x) + r(x)$ where $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ and $r(x) = r_1(x)$ wherein $q(x)$ and $r(x)$ satisfies our desired properties.
If possible let us assume that,

$$f(x) = q(x)g(x) + r(x) \ \textit{where} \ r(x) = 0 \ \textit{or} \ deg(r(x)) < deg(g(x))$$
$$\textit{and} \ f(x) = q'(x)g(x) + r'(x) \ \textit{where} \ r'(x) = 0 \ \textit{or} \ deg(r'(x)) < deg(g(x))$$

It follows that $r'(x) - r(x) = g(x)(q(x) - q'(x))$ and hence $r'(x) - r(x) = 0$ or $deg(r'(x) - r(x))$ is equal to that of $g(x)$, for the right side is product of $g(x)$ and a polynomial $q(x) - q'(x)$. But $deg(r'(x)) < deg(g(x))$ and $deg(r(x)) < deg(g(x))$ because of which $deg(r'(x) - r(x)) \ngeq deg(g(x))$ and hence $r'(x) - r(x) = 0$ ie. $r(x) = r'(x)$ and consequently $q(x) = q'(x)$.
This complete the proof. □

Corollary 3. *If F is a field and $f(x) \in F[x]$ then $f(a)$ is the reminder in the division of $f(x)$ by $(x-a)$.*

Proof. By division algorithm, there exists unique $q(x)$ and $r(x)$ such that,

$$f(x) = (x-a)q(x) + r(x) \ \ where \ \ r(x) = 0 \ \ or \ \ deg(r(x)) < 1 = deg(x-a)$$

But $deg(r(x)) < 1$ means $r(x)$ is a constant polynomial.Taking $x = a$ one can see that $r(a) = f(a)$.
This complete the proof. □

Corollary 4. *Let F be a field and $a \in F$. Then a is a zero for any $f(x) \in F[x]$ if and only if $(x-a)$ is a factor of $f(x)$.*

Proof. Suppose that a is a zero of the polynomial $f(x)$ in the field F ie. $f(a) = 0$. But $f(a)$ is the reminder while one divides $f(x)$ by $(x-a)$. It follows that $f(x) = (x-a)q(x)$ for some $q(x) \in F[x]$ and consequently $(x-a)$ is a factor of $f(x)$.
Conversely suppose that $(x-a)$ is a factor of the polynomial $f(x)$ ie. $f(x) = (x-a)q(x)$. Substituting $x = a$ one can see that $f(a) = 0$. It follows that a is a zero of $f(x)$ in the field F.
This complete the proof. □

Theorem 17. *A polynomial of degree n over a field F has at most n zeros,counting the multiplicity.*

Proof. Here we proceed to prove the result by employing induction on n.
Clearly a polynomial of degree zero is a constant and hence it has no zero in the field F.
Suppose that $f(x)$ is a polynomial of degree n and a is a zero of $f(x)$ of multiplicity k. Then we must have $f(x) = (x-a)^k q(x)$ for some $q(x) \in F[x]$. In case $f(x)$ has no zero other than a then we are through.
Let $b(\neq a)$ is a zero of $f(x)$ in the field F. But then, $0 = f(b) = (b-a)^k q(b)$. It follows that $q(b) = 0$ ie. b is a zero of the polynomial $q(x)$ in the field F. It follows that any zero of $f(x)$ is also a zero of $q(x)$ and vice versa and of same multiplicity. But $deg(q(x)) = n - k < n$ and hence by induction $q(x)$ has $n-k$ zeros,counting the multiplicity. It follows that the number of zeros of the polynomial $f(x)$ in the field F is $n-k+k = n$, counting the multiplicity.
This complete the proof. □

Definition 19. *An integral domain D is said to be a Principal Ideal Domain(PID) if every ideal of D is a principal ideal ie. if A is an ideal of D then there exists $a \in D$ such that,*

$$A =< a >= \{ra | r \in D\}$$

Theorem 18. *Let F be a field. Then $F[x]$ is a principal ideal domain.*

Proof. Since F is a field therefore $F[x]$ is an integral domain.
Suppose that A is an ideal of $F[x]$. If $A = \{0\}$ then one can write $A =< 0 >$ ie. A is a principal ideal generated by the zero element of the field.
Suppose that $A \neq \{0\}$. Then there exists $g(x)(\neq 0) \in A$ with minimal degree, for which $< g(x) > \subseteq A$.
Suppose that $f(x) \in A$. Then by division algorithm there exists $q(x)$ and $r(x)$ such that,

$$f(x) = q(x)g(x) + r(x) \ \ where \ \ r(x) = 0 \ \ or \ \ deg(r(x)) < deg(g(x))$$

But then $r(x) = f(x) - q(x)g(x) \in A$. As we have assumed that $g(x) \in A$ with minimal degree and $deg(r(x)) < deg(g(x))$ therefore $r(x) = \{0\}$. It follows that $f(x) = q(x)g(x) \in < g(x) >$ and hence $A \subseteq < g(x) >$.
Thus we can conclude that $A =< g(x) >$ ie. A is a principal ideal and consequently $F[x]$ is a principal ideal domain.
This complete the proof. □

Definition 20. *Let D be an integral domain and $f(x)$ is a non zero and non unit element of $D[x]$. Then $f(x)$ is said to be irreducible over D if for $g(x), h(x) \in D[x]$,*

$$f(x) = g(x)h(x) \Rightarrow either \ \ g(x) \ \ or \ \ h(x) \ \ is \ \ a \ \ unit \ \ in \ \ D[x]$$

A non zero and non unit element $f(x)$ in $D[x]$ is said to be reducible if it is not irreducible.

Remark 6. *In case F is a field, a non-constant element $f(x) \in F[x]$ is said to be irreducible if $f(x)$ can not be expressible as product of two polynomials of lower degree.*

Example 22. *Consider the polynomial $f(x) = 2x^2 + 4$.*
If one will consider $\mathbb{Q}[x]$ then $f(x) = 2(x^2 + 2)$ and 2 is a unit over $\mathbb{Q}$ and hence $f(x)$ is irreducible in $\mathbb{Q}[x]$.
But if one will consider $f(x) \in \mathbb{Z}[x]$ then $f(x) = 2(x^2+2)$ is reducible because neither 2 nor $x^2 + 2$ is a unit in $\mathbb{Z}[x]$.

Example 23. *The polynomial $f(x) = x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ but it is reducible in $\mathbb{R}[x]$.*

Theorem 19. ***(Reducibility test for degree 2 or 3)*** *Let F be a field. If $f(x) \in F[x]$ and degree of $f(x)$ is 2 or 3 then $f(x)$ is reducible over F if $f(x)$ has a zero in F.*

Proof. Let $f(x)$ be reducible in $F[x]$ so that there exists $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$. Then $deg(g(x))$ and $deg(h(x))$ must be less than that of $f(x)$. But it is presumed that $deg(f(x))$ is 2 or 3. Since $deg(f(x)) = deg(g(x)) + deg(h(x))$ therefore $deg(g(x))$ or $deg(h(x))$ must be 1. Let $deg(g(x)) = 1$ and $g(x) = ax + b$ where $a, b \in F$. One can note that every zero of $g(x)$ is also a zero of $f(x)$ and $-a^{-1}b$ is a zero of $g(x)$ and hence a zero of $f(x)$.
Conversely suppose that $f(a) = 0$ for some $a \in F$. But then $(x - a)$ is a factor of $f(x)$ and consequently $f(x)$ is reducible over F.
This complete the proof. □

Definition 21. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}$. Then the greatest common divisor of $a_n, a_{n-1}, \cdots, a_1, a_0$ is said to be the content of the polynomial $f(x)$.*
In case the content of a non zero polynomial $f(x) \in \mathbb{Z}[x]$ is 1 then we say that $f(x)$ is a primitive polynomial.

Lemma 1. ***(Gauss's lemma)*** *The product of two primitive polynomials is a primitive one.*

Proof. Let $f(x), g(x)$ be any two primitive polynomials. Our intention is to show that $f(x)g(x)$ is also a primitive polynomial.
On the contrary let us assume that $f(x)g(x)$ is not a primitive polynomial and p be a prime which divide the content of $f(x)g(x)$. Let $\overline{f}(x), \overline{g}(x)$ and $\overline{fg}(x)$ be the polynomials obtain from $f(x), g(x)$ and $f(x)g(x)$ by reducing their coefficients by $mod\, p$ respectively. One can conclude that $\overline{f}(x), \overline{g}(x) \in \mathbb{Z}_p$ such that,

$$\begin{aligned}\overline{f}(x)\overline{g}(x) = \overline{f(x)g(x)} = 0 &\Rightarrow \overline{f}(x) = 0 \ \ or \ \ \overline{g}(x) = 0 \\ &\Rightarrow p\ divides\ each coefficient\ of\ f(x) \\ &\qquad or\ p\ divides\ each\ coefficients\ of\ g(x) \\ &\Rightarrow f(x)\ is\ not\ primitive\ or\ g(x)\ is\ not\ primitive\end{aligned}$$

This contradicts our initial assumption that both $f(x)$ and $g(x)$ are primitive and from this cotradiction one can conclude that $f(x)g(x)$ is primitive one.
This complete the proof. □

Theorem 20. *Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$ then $f(x)$ is reducible over $\mathbb{Z}$.*

Proof. Let us assume that $f(x)$ is reducible over $\mathbb{Q}$ ie. there exists $g(x), h(x) \in \mathbb{Q}[x]$ such that $f(x) = g(x)h(x)$.

Without loss of generality we can assume that $f(x)$ is primitive because we can divide both $f(x)$ and $g(x)$ by the content of $f(x)$.
Let a be the LCM of the denominators of the coefficients of $g(x)$ and b be the LCM of the denominators of the coefficients of $h(x)$. Then,

$$abf(x) = (ag(x))(bh(x)) \; and \; ag(x), bh(x) \in \mathbb{Z}[x]$$

If c_1 is the content of $ag(x)$ then $ag(x) = c_1 g_1(x)$ where $g_1(x) \in \mathbb{Z}[x]$.
If c_2 is the content of $ah(x)$ then $ah(x) = c_2 h_1(x)$ where $h_1(x) \in \mathbb{Z}[x]$.
Further both $g_1(x)$ and $h_1(x)$ are primitive. Since $f(x)$ is primitive the content of $abf(x)$ is ab. Since the product of any two primitive polynomials is again a primitive polynomial therefore $g_1(x)h_1(x)$ is a primitive one and the content of $c_1c_2g_1(x)h_1(x)$ is c_1c_2.It follows that $ab = c_1c_2$ and consequently $f(x) = g_1(x)h_1(x)$ where $g_1(x), h_1(x) \in \mathbb{Z}[x]$ and $deg(g_1(x)) = deg(g(x))$ and $deg(h_1(x)) = deg(h(x))$.
This complete the proof. □

Theorem 21. ***(Mod p irreducible test)*** *Let p be a prime and $f(x) \in \mathbb{Z}[x]$ with $deg(f(x)) \geq 1$. Let $\overline{f}(x) \in \mathbb{Z}_p$ be the polynomial obtain from $f(x)$ by reducing each coefficient of $f(x)$ by mod p. If $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $deg(\overline{f}(x)) = deg(f(x))$ then $f(x)$ irreducible over $\mathbb{Q}$.*

Proof. Let $deg(\overline{f}(x)) = deg(f(x))$ and $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$. Our intention is to prove that $f(x)$ is irreducible over $\mathbb{Q}$.
On the contrary let us assume that $f(x)$ is reducible over $\mathbb{Q}$. Then $f(x)$ is reducible over $\mathbb{Z}$ ie. there exists $g(x), h(x) \in \mathbb{Z}[x]$ such that,

$$f(x) = g(x)h(x) \;\; where \;\; deg(g(x)) < deg(f(x)) \;\; and \;\; deg(h(x)) < deg(f(x))$$

Let $\overline{g}(x)$ and $\overline{h}(x)$ be the polynomials in $\mathbb{Z}_p$ obtain from $g(x)$ and $h(x)$ by reducing each coefficient by *mod p*. But then $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ where $deg(\overline{g}(x)) \leq deg(g(x)) < deg(f(x)) = deg()\overline{f}(x)$ and $deg(\overline{h}(x)) \leq deg(h(x)) < deg(f(x)) = deg()\overline{f}(x)$. It follows that $\overline{f}(x)$ is reducible over $\mathbb{Z}_p$ which is a contradiction to our initial assumption that $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$. This contradiction leads us to the conclusion that $f(x)$ is irreducible over $\mathbb{Q}$.
This complete the proof. □

Theorem 22. ***(Eisensteins Criterion)*** *Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$. If there exists a prime p such that $p \nmid a_n$, $p|a_i \quad \forall i = 0, 1, \cdots, a_{n-1}$ but $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof. On the contrary let us assume that $f(x)$ is reducible over $\mathbb{Q}$. Then $f(x)$ is reducible over $\mathbb{Z}$ and consequently there exists $g(x), h(x) \in \mathbb{Z}[x]$ such

that $f(x) = g(x)h(x)$ *where* $1 \leq deg(g(x))$ *and* $1 \leq deg(h(x)) < n = deg(f(x))$. Let,

$$g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$$
$$and\ \ h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$$

Since $f(x) = g(x)h(x)$ therefore $a_0 = b_0 c_0$ and since $p|a_0$ but $p^2 \nmid a_0$ therefore p will divide any one of a_0 and b_0 but not the both.
Suppose that $p \nmid c_0$ and $p|b_0$.
Again $a_n = b_r c_s$ and since $p \nmid a_n$ therefore $p \nmid b_r$ and $p \nmid c_s$. It follows that for some $t \in \{0, 1, \cdots, n-1\}$ we must have $p \nmid b_t$.
But,

$$a_t = b_t c_0 + b_{t-1}c_1 + \cdots + b_0 c_t$$

Since $p|a_t$ therefore p will divide each of the summands on the right,specially $p|b_t c_0$. Thus we arrived in a contradiction because $p \nmid b_t$ and $p \nmid c_0$. This contradiction leads us to the conclusion that $f(x)$ is irreducible over $\mathbb{Q}$.
This complete the proof. □

Theorem 23. *Let F be a field and $p(x) \in F[x]$. Then $< p(x) >$ is a maximal ideal of $F[x]$ if and only if $p(x)$ is irreducible over F.*

Proof. Let $< p(x) >$ be a maximal ideal in $F[x]$. Clearly $p(x)$ is neither zero nor a unit in $F[x]$ because $< p(x) > \neq \{0\}$ and $< p(x) > \neq F[x]$.
If possible suppose that $p(x) = f(x)g(x)$ is a factorization of $p(x)$ over F. But then $p(x) \in < g(x) >$ and therefore $< p(x) > \subseteq < g(x) > \subseteq F[x]$. Since $< p(x) >$ is a maximal ideal in $F[x]$ therefore $< p(x) > = < g(x) >$ or $< g(x) > = F[x]$.
In case $< p(x) > = < g(x) >$, then $deg(g(x)) = deg(p(x))$ and consequently $deg(f(x)) = 0$ ie. $f(x)$ is a nonzero constant in the field ie. $f(x)$ is a unit in $F[x]$.
In case $< p(x) > = F[x]$, then $1 \in < g(x) >$ and consequently for some $h(x) \in F[x]$ ie. $g(x)h(x) = 1$ ie. $g(x)$ is a unit in $F[x]$.
It follows that $p(x)$ is not not reducible ie. irreducible over the field F.
□

6 Conclusion

Through this dissertation, we understood the basic algebraic structures of rings and integral domains, their definition, properties, and importance in abstract algebra. Starting from the basic structure of rings, we examined different examples such as commutative and non-commutative rings and explained their key operations and identities. We further specialized our interest to integral domains, a subclass of commutative rings with no zero divisors, which underpin many higher mathematical developments, notably field theory and number theory.

By this investigation, we saw how integral domains generalize the intimate arithmetic of integers into more comprehensive algebraic systems while maintaining essential properties like the cancellation law and integrity of multiplication. The connection between rings and integral domains not just deepens our knowledge of algebraic structures but also builds a bridge to advanced subjects like factorization, polynomial rings, and module theory.

This text illustrates the beauty and power of abstract algebra in pure and applied mathematics. By establishing a firm foundation in rings and integral domains, we pave the way to further studies of fields, vector spaces, and algebraic number theory. Subsequent research could include the use of these structures in cryptography, coding theory, and computer algebra systems, where their algebraic properties play a significant role.

BIBLIOGRAPHY

Hungerford, T.W. (1974). Algebra. Springer-Verlag.

Herstein, I.N. (1975). Topics in Algebra (2nd ed.). Wiley.

Fraleigh, J.B. (1976). A First Course in Abstract Algebra. Addison-Wesley.

Rotman, J.J. (1995). An Introduction to the Theory of Groups (4th ed.). Springer.

Nagpaul, S.R. (1998). Foundations of Abstract Algebra. PHI Learning.

Tignol, J.P. (2001). Galois' Theory of Algebraic Equations. World Scientific.

Lang, S. (2002). Algebra (Revised 3rd ed.). Springer.

Gallian, J.A. (2016). Contemporary Abstract Algebra (9th ed.). Cengage Learning.

Singh, S. (2020). Basic Abstract Algebra. Springer India.