SIRP.T.SCIENCECOLLEGE,MODASA

(Managed by THE M. L. GANDHI HIGHER EDUCATION SOCIETY)

Certificate

This is to certify that the following students of B.Sc.(Sem-IV) has successfully completed the project entitled **Basic properties of Ring Theory** under the guidance of Dr. K. N. Darji, Assistant Professor, Department of Mathematics, SIR P. T. SCIENCE COLLEGE, MODASA during year 2022-2023.

Roll. No.	NAME
3424	Kunalsinh Jagatsinh Jadeja
3425	Mahammadhazim Sirajhusen Kankroliya
3427	Manubhai Ranjitbhai Vanjara
3428	Mayurkumar Ganpatbhai Damor
3429	Mayurkumar Somabhai Bariya

DR.K.N.DARJI

(GUIDE)

(H.O.D.)

Head
Mathematics Department
Sir P.T.Science College,Modasa

SIRP.T.SCIENCECOLLEGE,MODASA

(Managed by THE M. L. GANDHI HIGHER EDUCATION SOCIETY)

Certificate

This is to certify that the following students of B.Sc.(Sem-IV) has successfully completed the project entitled **Basic properties of Ring Theory** under the guidance of Dr. K. N. Darji, Assistant Professor, Department of Mathematics, SIR P. T. SCIENCE COLLEGE, MODASA during year 2022-2023.

Roll. No.	NAME
3424	Kunalsinh Jagatsinh Jadeja
3425	Mahammadhazim Sirajhusen Kankroliya
3427	Manubhai Ranjitbhai Vanjara
3428	Mayurkumar Ganpatbhai Damor
3429	Mayurkumar Somabhai Bariya

DR.K.N.DARJI

(GUIDE)

(H.O.D.)

Head
Mathematics Department
Sir P.T.Science College,Modasa

Defination of a Ring : Suppose R is the non-empty set equipped with two binary operations Called addition and multiplication and denoted by ' + ' and ' . ' respectively

i.e., For all $a,b \in R$

Then this is algebraic structure $(R, +, .)$ is called a ring , if the following postulates are satisfied:

(1) Addition is associative

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

(2) Addition is commutative

i.e., $a+b = b+a \ \forall \ a,b \in R$

(3) There exist an element denoted by 0 on R such that

$0+a = a \ \forall \ a \in R$

(4) To each element a in R there exist an element -a in R such that

$(-a) + a = 0$

(5) Multiplication is associative

i.e., $a.(b.c) = (a.b).c \ \forall \ a,b,c \in R$

(6) Multiplication is distributive with respect to addition

i.e., for all a,b,c in R

$a.(b+c) = a.b+a.c$ (Left distributive law)

and $(b+c).a = b.a+c.a$ (Right distributive law)

Defination of ring with unity : If in a ring R there exist an element denoted by 1 such that $1.a=a=a.1 \ \forall \ a \in R$, Then R is called a ring with unit element.

The element $1 \in R$, is called the unit element of the ring.

Obviouly 1 is the multiplicative identity of R. Thus if a ring possesses multiplicative identity , then it is a ring with unity.

Defination of commutative ring : If in a ring R, The multiplication composition is also commutative i.e., we have $a.b = b.a \ \forall \ a,b \in R$, Then R is called a commutative ring.

Defination of devision ring : A ring R is called a division ring if the set of non-zero elements of R form a group under multiplication.

Theorem : If R is a ring , Then for all $a,b,c \in R$

1) $a.0 = 0.a = 0$
2) $a(-b) = -(ab) = (-a)b$
3) $(-a)(-b) = ab$
4) $a(b-c) = ab - ac$
5) $(b-c)a = ba - ca$

Theorem : For elements **a** and **b** of a ring R and for integers $m,n \in Z$

1) $n(a+b)=na+nb$
2) $(m+n)a=ma+na$
3) $n(ma)=(nm)a$

Theorem : For elements **a** and **b** of a ring R and for positive integers **m** and **n**

1) $a^m a^n = a^{m+n}$
2) $(a^m)^n = a^{mn}$

If elements **a** and **b** are commutative , then

3) $a^m b^m = b^m a^m$
4) $(ab)^n = a^n b^n$

Theorem : For elements **a** and **b** of a ring R and for a positive integer n,

$a(nb) = n(ab)$ and $(nb)a = n(ba)$

Theorem : If **a** and **b** are commutative elements of a ring R, then for each $n \in$ **N**

$(a+b)^n = a^n + {}^nc_1 a^{n-1}b + {}^nc_2 a^{n-2}b^2 + ... + b^n$

Where ${}^nc_r = \frac{n!}{r!(n-r)!}$.

Example : The set **R** consisting of a single element 0 with two binary operations defined by 0+0=0 and 0.0=0 is a ring . This ring is called the **null ring** or the **Zero ring** .

Example : The set **I** of all integers is a ring with respect to addition and multiplication of integers as the two ring composition. This ring is called The ring of integers .

Example : The set 2I of all even integers is a commutative ring without unity , the addition and multiplication of integers being the two ring compositions .

Example : The set **Q** of all rational numbers is a commutative ring with unity, the addition and multiplication of rational numbers being the two ring compositions .

Example : The set **R** of all real numbers is a commutative ring with unity, the addition and multiplication of real numbers being the two ring compositions .

Example : The set **C** of all complex numbers is a commutative ring with unity, the addition and multiplication of complex numbers being the two ring composition .

Example : The set M n x n matrices with their elements as real numbers (rational numbers, complex numbers, integers) is a non-commutative ring with unity, with respect to addition and multiplication of matrices as the two ring compositions.

Example : The set R={0,1,2,3,4,5} is a commutative ring with respect to ' $+_6$ ' and ' x_6 ' as the two ring compositions.

In a ring it is possible that the product of two non-zero elements is equal to the zero element.

e.g. $2 \times_6 3 = 0$

also the number of elements in R is finite

therefore this is an example of a finite ring .

Example : The set **Z**[i] = {a+bi / a,b ∈ **Z**} is a commutative ring with unity under usual addition and multiplication .

Example : (1) A ring R is commutative if $a^2 = a$ for each a € R.

(2) A ring R is commutative if $a^3 = a$ for each a € R.

Example : $Q(\sqrt{7})=\{a+b\sqrt{7} / a,b \in Q\}$ is a field under usual addition and multiplication.

Example : $(Z_p, +_p, x_p)$ is a field for prime P.

Defination of zero divisor : A non-zero element of a ring R is called a zero divisor if there exists an element b≠0 € R Such that either ab=0 or ba=0.

Rings without zero divisor : A ring R is without zero divisors if the product of two non-zero elements of R is zero,

i.e. if ab=0 ⇒ a=0 or b=0

On the other hand if in a ring R there exist non-zero elements **a** and **b** such that ab=0, Then R is said to be a ring with zero divisors.

Example : Suppose M is a ring of all 2x2 matrices with their elements as integers, The addition and multiplication of matrices being the two ring compositions. Then M is a ring with zero divisors.

Example : The ring ({0,1,2,3,4,5} , $+_6$, x_6) is a ring with zero divisors.

We have $2x_63=0$, $3x_64=0$

i.e. The product of two non-zero integers can not be equal to the zero integers.

Cancelation laws in a ring : If R is a ring then R is an abelian group with respect to addition.

For addition composition The cancellation laws hold in all rings.

Therefore the question of cancellation laws holding in a ring arises only for the multiplication composition.

We say that cancellation laws hold in a ring R if $a \neq 0$, $ab=ac \Rightarrow b=c$

And $a \neq 0$, $ba=ca \Rightarrow b=c$ Where $a,b,c \in R$

Theorem : A ring R is without zero divisors if and only if the cancellation laws hold in R

i.e. R is without zero divisors $\Leftrightarrow$ Cancellation laws hold in R.

Defination of integral domain : A ring is called an integral domain if it (1) is commutative , (2) has unit element , (3) is without zero divisors.

Defination of inversible element in a ring with unity : In a ring every element possesses inverse.

Therefore the question of an element being inversible or not arise only with respect to multiplication.

If R is a ring with unity , Then an element $a \in R$ is called inversible , if there exist $b \in R$ sach that $ab=1=ba$.

Also then we write $b=a^{-1}$.

Defination of field : A ring R with at least two elements is called a field if it (1) is commutative ,

(3) Has unity , (3) is such that each non-zero element possesses multiplicative inverse.

Example : The ring of rational numbers (Q , + , x) is a field since it is a commutative ring with unity and each non-zero element is inversible.

$(\{0,1,2,3,4,5\}, +_5, x_5)$ is an example of a finite field.

Examples : (1) 1 and -1 are the only two inversible elements of the ring of all integers.

(2)nxn non-singular matrices with real numbers as elements are the only inversible elements of the ring of all nxn matrices with elements as real numbers.

Theorem : A non-zero element [m] of ring $(Z_n , +_n , x_n)$ is a zero divisor iff m and n are not relatively prime.

Corollary : For given prime p, The ring $(Z_p , +_p , x_p)$ has no zero divisor.

Theorem : A field is an integral domain.

Theorem : A finite integral domain is a field.

Theorem : A finite division ring is a field.

Theorem : A non-empty subset K of a field F is a subfield of F iff

1) $a-b \in K$ for $a,b \in K$ and
2) $ab^{-1} \in K$ for $a,b \neq 0 \in K$.

Division ring or skew field

A ring R with at least two elements is called a division ring or skew field if it (1)has unity,(2) is such that each non zero element possesses multiplicative inverse.

<u>NOTE</u>: Every field is also a division ring but a division ring is a field if it is also commutative.

THEOREM: Every field is an integral domain.

THEOREM: A skew field has no divisors of zero.

THEOREM: A finite commutative ring without zero divisors is a field. <u>OR</u>

Every finite integral domain is a field.

EXAMPLE:

1) If a,b,c,d are elements of a ring R then evaluate (a+b)(c+d).
2) Prove that if $a,b \in R$ then $(a+b)^2=a^2+ab+ba+b^2$ where by x^2 we mean xx.
3) If a,b are any elements of a ring R prove that
   a. -(-a)= a
   b. -(a+b)= -a-b
   c. -(a-b)= -a+b
4) If a,b,c,d are any elements of aring R prove that

   (a-b)(c-d)=(ac+bd)-(ad+bc).
5) If R is a system satisfying all the conditions for a ring with unit element with the possible exception of a+b=b+a prove that the axiom a+b =b+a must hold in R and that R is thus a ring.
6) If R is a ring such that $a^2=a$ for all $a \in R$ prove that
   a. a+a=0 for all $a \in R$ i.e each element of R is its own additive inverse.
   b. $a+b=0 \rightarrow a=b$.
   c. R is a commutative ring.

7) Prove that the set M of 2×2 matrices over the field of real numbers is a ring with respect to matrix , addition and multiplication is it a commutative ring with unity element? Find the zero element does this ring possess zero divisor?

8) Do the following sets form integral domains with respect to ordinary addition and multiplication? If so state if they are fields.

a. The set of numbers of the form b√2 with b rational.

b. The set of even integers.

c. The set of positive integers.

9) Show that the set of numbers of the form a+b√2 with a and b as rational numbers is a field.

10) Prove that the set I(√2)of all real numbers of the form a+b√2 with a and b as integers is an integral domain with respect to ordinary addition and multiplication is it a field?

11) A Gaussian integer is a complex number a+ib where a and b are integer. Show that the set J[i] of Gaussian integers forms a ring under ordinary addition and multiplication of complex numbers is it an integral domain is it a field ?

12) Prove that the totality R of all ordered pairs (a,b) of real numbers is a commutative ring with zero divisors under the addition and multiplication of ordered pairs defined as

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

b) (a,b)(c,d)=(ac,bd) for all (a,b)(c,d) ∈ R.

13) Let C be the set of the ordered pairs (a,b) of real numbers. Define addition and multiplication in C by the equation

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

b) (a,b)(c,d)=(ac-bd,bc+ad)

Prove that C is a field.

14) Show that the set R of all real valued continuous functions defined in the closed interval [0,1] is a commutative ring with unity with respect to the addition and multiplication of functions defined pointwise as follows:

a) (f+g)(x)=f(x)+g(x)

b) & (fg)(x)=f(x)g(x) where f,g are any two members of R.

15) Give an example of a skew field which is not a field.

16) Let p be a prime number prove that the set of integers I_p, I_p= {0,1,2,3,......,p-1} forms a field with respect to addition and multiplication modulo p.

17) Prove that the set of residue classes modulo p is a commutative ring with respect to addition and multiplication of residue classes further show that the ring of residue classes modulo p is a field if and only if p is prime.

Isomorphism of rings

A ring R is said to be isomorphic to another ring R` if there exists a one-one mapping f of R onto R` such that

f(a+b)=f(a)+f(b),f(ab)=f(a)f(b) for all a,b ϵ R.

Also such a mapping f is said to be an isomorphism of R onto R`.

I. If a ring R is isomorphic to another ring R` we shall write in symbols R≅R.

II. Also R` is said to be an isomorphic image of R.

Example:

1. Let R be the ring of integers under ordinary addition and multiplication. Let R` be the set of all even integers let us define multiplication in R` to be denoted by 'Φ' by the relation aΦb=ab/2

   Where ab is the ordinary multiplication of two integers a and b.

   I. Prove that(R`,+, Φ) is a commutative ring where + stands for ordinary addition of integers.

   II. Prove that R is isomorphic to R`.

   III. What acts as the unit element of R`?

Properties of isomorphism of rings

Theorem: If f is an isomorphism of a ring R onto a ring R` then

1. The image of the zero of R is the zero of R\`.

2. The image of the negative of an element of R is the negative of the image of that element i.e. f (-a) =-f (a) for all a ϵ R.

3. If R is commutative ring then R\` is also a commutative ring.

4. If R is without zero divisors then R\` is also without zero divisors.

5. If R is with unit element then R\` is also with unit element.

6. If R is a field then R\` is also a field.

7. If R is a skew field then R\` is also a skew field.

Transference of ring structure

Theorem: If f is an one-one mapping of a ring R onto a set R with two compositions denoted additively and multiplicatively such that f(a+b)=f(a)+f(b),f(ab)=f(a)f(b) for all a,b ϵ R then the set R\` is a ring for the two compositions.

Subring

Let R be a ring A non empty subset S of the R is said to be a subring of R if S is closed with respect to the operations of addition and multiplication in R and S itself is a ring for these operations.

Conditions for a subring:

The necessary and sufficient conditions for a non empty subset S of a ring R to be a subring of R are

1. a ϵ S, b ϵ s⇒a-b ϵ S

2. a,b ϵ S ⇒ ab ϵ S

Theorem: The intersection of two subrings is a subring.

Theorem: An arbitrary intersection of subrings is a subring.

Theorem: The intersection of the family of subring which contain a given subset M of a ring R is the smallest subring containing the subset M.

Examples:

1. The set of integers is a subring of the ring of rational numbers.
2. The set of all m×m matrices over the field of rational number is a subring of all m×m matrices over the field of real numbers.
3. Let R be the ring of all 2×2 matrices over the field of real numbers.Let M be a subset of R and let the elements of M be matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ then M is a subring of R.
4. Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2×2 matrices with integral elements.
5. Let R be the ring of integers let m be any fixed integer and let S be any subset of R such that s = {.....,-3m,-2m,-m,0,m,2m,3m,.......} then S is a subring of R.

Subfields:

Let F be a field.A non empty subset K of the set F is said to be a subfield of F if K is closed with respect to the operations of addition and multiplication in F and K itself is a field for these operation.

Theorem: The necessary and sufficient conditions for a non empty subset K of a field F to be a subfield of F are

1. $a \in K, b \in K \Rightarrow a-b \in K$
2. $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in OK$