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 **Properties of Ideals in Ring Theory** under the guidance of Dr. K. N. Darji, Assistant Professor, Department of Mathematics, SIR P. T. SCIENCE COLLEGE, MODASA during the year 2022-2023.

Roll. No.	NAME
3438	Pritiben Dineshbhai Rathod
3439	Refyu Ashvinbhai Bodat
3440	Riya Mukeshbhai Patel
3441	Rukaiyabanu Altafhusen Dudhmal
3442	Rushabhkumar Manharbhai Patil

DR.K.N.DARJI

(GUIDE)

(H.O.D.)

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

Page: 1

Quotient Rings

Definition:

If R is a ring and I is a two-sided ideal, the quotient ring of R mod I is the group of cosets $\frac{R}{I}$ with the operations of coset addition and coset multiplication. Here $(R/I, +, \cdot)$ is called quotient ring.

Theorem:-

If I is an ideal in a ring R, then the set, $R/I = \{I+a \,/\, a \in R\}$ of cosets of I in a ring R is a ring under the following binary operations.

$\Rightarrow$ For any $I+a,\ I+b \in R/I$, $a, b \in R$.

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

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

R/I is a commutative ring with unity, If R is a commutative ring with unity.

English Example:-(1)

Find the number of element is a quotient ring from given. Since $\frac{R}{I} = \{I+a \,/\, a \in R\}$

$M_{2\times 2}(\mathbb{Z})/I = \{I+P \,/\, P \in M_{2\times 2}(\mathbb{Z})\}$, where

$$I = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big/ a, b, c, d \in (\mathbb{Z})\right\}$$

Solution:

Since $R/I = \{I + a \mid a \in R\}$

$M_{2\times2}(\mathbb{Z})/I = \{I + P \mid P \in M_{2\times2}(\mathbb{Z})\}$, where
$I = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in (\mathbb{Z})\}$

Suppose,
$$P = \begin{pmatrix} p & l \\ r & s \end{pmatrix}, \quad p, r, l, s \in \mathbb{Z}$$

$$= \begin{pmatrix} 2q_1 + r_1 & 2q_2 + r_2 \\ 2q_3 + r_3 & 2q_4 + r_4 \end{pmatrix}, \text{ where}$$
$$0 \le r_1, r_2, r_3, r_4 \le 1$$

$$= \begin{pmatrix} 2q_1 & 2q_2 \\ 2q_3 & 2q_4 \end{pmatrix} + \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}$$

Since, $\begin{pmatrix} 2q_1 & 2q_2 \\ 2q_3 & 2q_4 \end{pmatrix} \in I$

$$I + P = I + \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}, \text{ where } 0 \le r_i \le 1, \; i = 1 \text{ to } 4$$

Thus, $M_{2\times2}(\mathbb{Z})/I = \{I + \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \mid 0 \le r_i \le 1 \; i = 1 \text{ to } 4\}$

Has each r_i assume two possibilities values 0 & 1, the number of matrices of the form $\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}$, $0 \le r_i \le 1$, $i = 1$ to 4 is 16.

Thus, the number of element is a quotient ring is 16.

Theorem:

If I is a two-sided ideal in R, then R/I has the structure of a ring under coset addition and multiplication.

$\Rightarrow$ Suppose that I is a two-sided in R. let $r, s \in I$.

$$\Rightarrow ((r+I)(s+I))(t+I) = (rs+I)(t+I)$$
$$= (rs)t + I \qquad (\because \text{Associative prop})$$
$$= r(st) + I$$
$$= (r+I)(st+I)$$
$$= (r+I)((s+I)+(t+I))$$

Theorem:

Let R be a ring, and let I be an ideal.

(a) If R is a commutative ring, so is R/I.

(b) If R has multiplicative identity 1, then $1+I$ is a multiplicative identity for R/I. In this case, if $r \in R$ is a unit, then so is $r+I$, and $(r+I)^{-1} = r^{-1}+I$.

$\Rightarrow$ (a) let $r+I, s+I \in R/I$. Since R is commutative.

$$(r+I)(s+I) = rs+I = sr+I = (s+I)(r+I) \quad (\because \text{Associative prop})$$

Therefore, R/I is commutative

$\Rightarrow$ (b) Suppose R has a multiplicative identity 1. let $r \in R$. Then $(r+1)(1+I) = r \cdot 1 + I = r+I$ and

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

Therefore, $1+I$ is the identity of R/I

If $r \in R$ is a unit, then

Page: 4

$(r^{-1}+I)(r+I) = r^{-1}r + I = 1+I$ and

$(r+I)(r^{-1}+I) = rr^{-1}+I = 1+I$.

Therefore, $(r+I)^{-1} = r^{-1}+I$.

Example: (2)

(A quotient ring of the integers) the set of even integers $\langle 2\rangle = 2\mathbb{Z}$ is an ideal in $\mathbb{Z}$. From the quotient ring $\frac{\mathbb{Z}}{2\mathbb{Z}}$.

Construct the addition and multiplication tables for the quotient ring.

Here are some cosets:

$2+2\mathbb{Z}$, $-15+2\mathbb{Z}$, $841+2\mathbb{Z}$.

But two cosets $a+2\mathbb{Z}$ and $b+2\mathbb{Z}$ are the same exactly when a and b differ by in even integer. Every even integer differ from 0 by an even integer. Every odd integer differs from 1 by an even integer. Every so there are really only two cosets (up to renaming): $0+2\mathbb{Z} = 2\mathbb{Z}$ and $1+2\mathbb{Z}$.

Here are the addition and multiplication tables:

$+$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$0+2\mathbb{Z}$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$1+2\mathbb{Z}$	$1+2\mathbb{Z}$	$0+2\mathbb{Z}$

$\cdot$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$0+2\mathbb{Z}$	$0+2\mathbb{Z}$	$0+2\mathbb{Z}$
$1+2\mathbb{Z}$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$

You can see that $\frac{\mathbb{Z}}{2\mathbb{Z}}$ is isomorphic to $\mathbb{Z}_2$.

In general, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is isomorphic to $\mathbb{Z}_n$. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
This example gives a formal construction of $\mathbb{Z}_n$ as the quotient ring $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Example:- (3) $\mathbb{Z}_3[x]$ is the ring of polynomials with coefficients in $\mathbb{Z}_3$. Consider the ideal $\{2x^2+x+2\}$.

(a) How many elements in the quotient ring $\frac{\mathbb{Z}_3[x]}{\{2x^2+x+2\}}$?

(b) Reduce the following product in $\frac{\mathbb{Z}_3[x]}{\{2x^2+x+2\}}$ to the form $(ax+b)+\{2x^2+x+2\}$: $(2x+1+\{2x^2+x+2\})\cdot(x+1+\{2x^2+x+2\})$.

(c) Find $[x+2+\{2x^2+x+2\}]^{-1}$ in $\frac{\mathbb{Z}_3[x]}{\{2x^2+x+2\}}$.

The ring $\frac{\mathbb{Z}_3(x)}{\{2x^2+x+2\}}$ is analogous to $\mathbb{Z}_n = \frac{\mathbb{Z}}{\{n\}}$.

Solution:

(a) By the Division Algorithm, any $f(x) \in \mathbb{Z}_3[x]$ can be written as, $f(x) = (2x^2+x+2)q(x) + r(x)$, where $\deg r(x) < \deg(2x^2+x+2)$.

This means that $r(x) = ax+b$, where $a, b \in \mathbb{Z}_3$. Then
$f(x) + \langle 2x^2+x+2\rangle = [(2x^2+x+2)q(x) + r(x)] + \langle 2x^2+x+2\rangle = (ax+b) + \langle 2x^2+x+2\rangle$
Since there are 3 choices for a and 3 choices for b, there are 9 cosets.

(b) First, multiply the coset representatives:

$$(2x+1)(x+1) = 2x^2+1.$$

Dividing $2x^2+1$ by $2x^2+x+2$, I get

$$2x^2+1 = (2x^2+x+2)(1) + (2x+2).$$

Then
$2x^2+1+\langle 2x^2-x+2\rangle = [(2x^2+x+2)(1)-(2x+2)]+\langle 2x^2-x+2\rangle = \langle 2x^2+x+2\rangle$.

(c) To find multiplicative inverse in Z_n. use quotient rings of polynomial rings.

$2x^2+x+2$	$-$	$2x$
$x+2$	$2x$	1
2	$2x+1$	0

① $(2x^2+x+2)-(2x)(x+2)=2$ (1) $(2x^2+x+2)+(x)(x+2)=2$

② $(2x^2+x+2)+(2x)(x+2)=1$ ② $(2x^2+x+2)+(2x)(x+2)+\langle 2x^2+x+2\rangle = 1+\langle 2x^2+x+2\rangle$

$$2x(x+2)+\langle 2x^2+x+2\rangle = 1+\langle 2x^2+x+2\rangle$$

$$[x+2+\langle 2x^2+x+2\rangle]^{-1} = 2x+\langle 2x^2+x+2\rangle.$$

* **Example:- (4)**

In the ring $Z_2 \times Z_{10}$, consider the principal ideal $\langle(1,5)\rangle$. (a) List the elements of $\langle(1,5)\rangle$.
(b) List the elements of the cosets of $\langle(1,5)\rangle$
(c) Is the quotient ring $\frac{Z_2 \times Z_{10}}{\langle(1,5)\rangle}$ a field?

* **Solution:** (a) Note that the additive subgroup generated by $(1,5)$ has only two elements.
$\therefore \langle(1,5)\rangle = \{(0,0),(0,5),(1,0),(1,5)\}$.

(b) Since, the ideal has 4 elements and ring has 20 there must be 5 cosets.

$\langle(1,5)\rangle = \{(0,0),(0,5),(1,0),(1,5)\}$

$(0,1)+\langle(1,5)\rangle = \{(0,1),(0,6),(1,1),(1,6)\}$

$(0,2)+\langle(1,5)\rangle = \{(0,2),(0,7),(1,2),(1,7)\}$

$(0,3)+\langle(1,5)\rangle = \{(0,3),(0,8),(1,3),(1,8)\}$

$(0,4)+\langle(1,5)\rangle = \{(0,4),(0,9),(1,4),(1,9)\}$

Page :
Date :

(c) Note that $(0,1) + \langle(1,5)\rangle$ is the identity.

$[(0,2) + \langle(1,5)\rangle][(0,3) + \langle(1,5)\rangle] = (0,1) + \langle(1,5)\rangle$.

$[(0,4) + \langle(1,5)\rangle][(0,4) + \langle(1,5)\rangle] = (0,1) + \langle(1,5)\rangle$.

since every nonzero cosets has a multiplicative inverse, the quotient ring is a field.

***Example:- (5)**

If $I = \{a, c\}$ in the ring $R = \{a, b, c, d\}$ defined as follows:

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

Then, the R/I has only two elements, namely I & $I+b$

Solution:-

We know that $R/I = \{I + a / a \in R\}$

Now, $I = \{a, c\}$

$I+a = \{a+c, c+a\} = \{a, c\} = I$

$I+b = \{a+b, c+b\} = \{b, d\}$

$I+c = \{a+c, c+c\} = \{c, a\} = I$

$I+d = \{a+d, c+d\} = \{d, b\} = I+b$

Thus R/I has only two elements which are I and $I+b$.

Homorphism of rings :-

Definition Homomorphism into :-

A mapping f from a ring R into a ring R' is said to be homomorphism of R into R' if

(i) $f(a+b) = f(a) + f(b) \quad \forall\ a, b \in R$

(ii) $f(ab) = f(a) \cdot f(b)$ for all $a, b \in R$.

Homomorphism onto :-

A mapping f from a ring R onto a ring R' is said to be a homomarphism of R onto R' if

(i) $f(a+b) = f(a) + f(b) \quad \forall\ a, b \in R$

(ii) $f(ab) = f(a) \cdot f(b)$ for all $a, b \in R$

Also then R' is said to be a homomorphism image of R.

Theorem :-

For a homomorphism $\phi : (R, +, \cdot) \to (R^*, \oplus, \odot)$

(i) $\phi(0) = 0^* =$ zero element of R^*

(ii) $\phi(-a) = -\phi(a)$, $a \in R$

(iii) For a subgroup H of $(R, +)$, $\phi(H)$ is a subgroup of $(R^*, \oplus)$

(iv) For a subgroup H^* of $(R^*, \oplus)$, $\phi^{-1}(H^*)$ is subgroup of $(R, +)$.

Theorem :-

Let ϕ be a homomorphic mapping of a ring R into a ring R'. Let S' be the homomorphic image of R in R'. Then S' is a subring of R'.

Example:

The zero map $\phi:(R,+,\cdot)\to(R,+,\cdot) \ni \phi(a)=0 \;\forall\; a\in R$ is a homomorphism.

Example :-

The identity map $\phi:(R,+,\cdot)\to(R,+,\cdot)$ is a homomorphism.

Example :-

The mapping $\phi:(Z(\sqrt{2}),+,\cdot)\to(Z(\sqrt{2})+,\cdot)$ such that $\phi(a)=\phi(m+n\sqrt{2})=m-n\sqrt{2}$ for all $a=m+n\sqrt{2}\in Z\sqrt{2}$, is a homomorphism.

Example :-

The mapping $\phi:(Z,+,\cdot)\to(Z_n,+_n,\cdot_n)$ such that $\phi(m)=[m]$, $m\in Z$ is a homomorphism.

The language of friendship is not words but meanings.

Example :-

For an ideal I of a ring R, the mapping $\phi : R \to R/I$ where $\phi(a) = I + a$, $a \in R$, is an onto homomorphism.

Theorem :-

If $\phi : (R, +, \cdot) \to (R^*, \oplus, \odot)$ is a homomorphism, then

(i) For a subring U of R $\phi(U)$ is a subring of R^*

(ii) For an ideal I of R $\phi(I)$ is an ideal of $\phi(R^*)$ (or of R^*)

(iii) For a subring U^* of R^*, $\phi^{-1}(U^*)$ is a subring of R

(iv) For an ideal I^* of $\phi(R^*)$, $\phi^{-1}(I^*)$ is an ideal of R.