Rings of Arithmetical Functions under the Operations of Pointwise Addition and Dirichlet Composition

A Project Thesis for the Award of the Degree of B.Sc (Hon's) in Mathematics of Jagannath University

Submitted by,
Radita Hossain
ID NO. : B150302034

Department of Mathematics
Jagannath University
Dhaka-1100
Bangladesh

March, 2022

Contents

Chapter 1

Introduction to Groups

1.1 Group

1.1.1 Definition

A group is a set G, together with a binary operation o, satisfying the following conditions:

1. **Closure law:** $aob \in G \ \forall \ a, b \in G$.
2. **Associative law:** $(aob)oc = ao(boc) \ \forall \ a, b, c \in G$
3. **Existence of identity:** There exists an $e \in G$ such that $aoe = eoa = a \ \forall \ a \in G$.
4. **Existence of inverse:** For each a $\in G$, there exists $aob \in G$ such that $aob = boa = e$.

We will refer to G as a group under o. The element e is called the identity element of the group. If $a \in G$, and $aob = boa = e$, then b is called the inverse of a, and we write $b = a^{-1}$.

1.1.2 Example of Groups

Example 1

Let G be a group under the binary operation addition. Then the following properties hold in G :

(i) $\forall a, b \in G \Rightarrow a + b \in G$
(ii) $\forall a, b, c \in G \Rightarrow (a + b) + c = a + (b + c)$
(iii) $\exists \ 0 \in G$ such that $a + 0 = 0 + a = a, \forall a \in G$
(iv) $a \in G \Rightarrow -a \in G \Rightarrow a + (-a) = (-a) + a = 0.$
i.e. $(R_o, .)$ is a group.

Solution:

Since the usual multiplication is a binary operation in R_o , then clearly the following laws hold in R_o:

(i) $\forall a, b \in R_o \Rightarrow ab \in R_o$

(ii) $\forall a, b, c \in R_o \Rightarrow (ab)c = a(bc)$

(iii) $\exists 1 \in R_o$ such that $a1 = 1a = a, \forall a \in R_o$, where 1 is called the unit element of R_o.

(iv) $a \in R_o \Rightarrow \exists\ a^{-1}$ such that $aa^{-1} = a^{-1}a = 1$.

Thus $(R_o, .)$ is a group under multiplication.

1.2 Abelian Group

1.2.1 Definition

A group (G, o) is called Abelian or commutative if:

$\forall a, b \in G \Rightarrow aob = boa.$

1.2.2 Examples of Abelian Group

Example 1:

Let G be a group under the binary operation multiplication. If

$\forall a, b \in G \Rightarrow ab = ba$, then G is called an Abelian Group under the binary operation multiplication.

Example 2:

Let G be a group under the binary operation addition. If

$\forall a, b \in G \Rightarrow a + b = b + a$, then G is called an Abelian Group under the binary operation addition.

Example 3:

The group $(\mathbf{Z}, +)$ is an additive Abelian Group since $\forall a, b \in \mathbf{Z} \Rightarrow a + b = b + a$. Similarly the groups $(\mathbf{Q}, +), (\mathbf{R}, +), (\mathbf{C}, +)$ are all additive abelian Groups.

1.3 Order of a Group

1.3.1 Definition

Let (G, o) be a group. Then by the order of G is the number of elements in the set G. The order of G is denoted by $o(G)$. A finite group is of finite order and an infinite group is of infinite order.

1.3.2 Examples

Example 1:

(i) The multiplicative group $G = (1, -1)$ is a finite group of order 2 i. e. $o(G) = 2$ since the number of elements in G are 2.

(ii) The multiplicative group $G = (1, -1, i, -i)$ is a group of order 4 i. e. $o(G) = 4$.

These two groups are finite group since the order of each is finite.

Example 2:

The algebraic system $(\mathbf{Z}, +), (\mathbf{Q}, +), (\mathbf{R}, +)$ are all groups of infinite order since the number of elements in each is infinite.

1.4 Order of an element of a group

1.4.1 Definition

Let (G, o) be a group and $a \in G$. Then the order of 'a' is the least positive integer n such that $a^n = e$ (the identity element of G). The order of 'a' is denoted by $o(a)$.

Theorem 1

The order of the element of a group is 1.

Proof:

Let G be a group and e be the identity element of G. Then since $e^1 = e$ (identity) or $1e = e$ (identity) , so $o(e) = 1$

Thus the order of the identity element of any group is always 1.

Theorem 2

For any two elements a, b of a group, the order of ab is the same as the ba.

Proof:

Let G be a group and e be the identity element in G.
Let $a, b \in G$
Then $ab, ba \in G$
Now we have $(a^{-1})a = e$
Thus $ba = e(ba) = (a^{-1})a(ba)$
$= a^{-1}(ab)a$
$\Rightarrow o(ba) = o(a^{-1}(ab)a) = o(ab)$.
Hence $o(ab) = o(ba)$.

1.5 General Properties of Groups

Theorem 1 (Uniqueness of identity in a group)

Let (G, o) be a group. Then the identity element e in G is unique.

Proof:

If possible, let e and e' be two identity elements in G. Then we have
,
e an identity $\Rightarrow eoe' = e'oe = e'$.............(1)
e' an identity $\Rightarrow eoe' = e'oe = e$.............(2)
Then (1) and (2) $\Rightarrow e = e'$.
Hence the identity element in a group is unique.

Theorem 2 (Uniqueness of inverse in a group)

The inverse of each element in a group is unique.

Proof:

Let (G, o) be a group. Let e be the identity of G, Let a be an arbitrary element in G. If possible let b and c be the inverses of a. Then we have
$aob = boa = e$........(i) and

$aoc = coa = e........(ii)$
But we have,
$b = boe$ [e is the identity]
$= bo(aoc)$ [by (ii)]
$= (boa)oc$ [o is associative]
$= eoc$ [by (i)]
$= c$ [e is the identity]
Thus the inverse of each element of a group is unique.

Theorem 3 (Cancellation law)

Let (G, o) be a group. Then show that: $\forall a, b, c \in G$,
(i) $aob = aoc \Rightarrow b = c$ [Left cancellation law]
(ii) $boa = coa \Rightarrow b = c$ [Right cancellation law]

Proof:

Let e be the identity of G.
Since $a \in G \Rightarrow \exists a^{-1} \in G$ such that
$a^{-1}oa = aoa^{-1} = e$......................(1)

(i)

$aob = aoc \Rightarrow a^{-1}o(aob) = a^{-1}o(aoc)$
$\Rightarrow (a^{-1}oa)ob = (a^{-1}oa)oc$ [by associative law]
$\Rightarrow eob = eoc$
$\Rightarrow b = c$
Thus $\forall a, b, c \in G, aob = aoc \Rightarrow b = c.$

(ii)

$boa = coa \Rightarrow (boa)oa^{-1} = (coa)oa^{-}1$
$\Rightarrow bo(aoa^{-1}) = co(aoa^{-1})$ [by associative law]
$\Rightarrow boe = coe$ [by (1)]
$\Rightarrow b = c$ [e is the identity]
Thus $\forall a, b, c \in G, boa = coa \Rightarrow b = c.$

Theorem 4 (Inverse identity)

Let (G, o) be a group. Then show that $(a^{-1})^{-1} = a, \forall a \in G$.

Proof:

We have,

$aoa^{-1} = e$
$\Rightarrow aoa^{-1} = a^{-1}oa$ $[((a^{-1})^{-1}oa^{-1} = e]$
$\Rightarrow a = (a^{-1})^{-1}$ [by right cancellation law]
Thus $(a^{-1})^{-1} = a$

Theorem 5 (Reversal law for inverse)

Let (G, o) be a group. Then show that $(aob)^{-1} = b^{-1}oa^{-1}, \forall a, b \in G$.

Proof:

Let a and b be two arbitrary elements of G. Then a^{-1} and b^{-1} are inverses of a and b respectively. Now by definition we have $(aob)^-1$ is the inverse of aob. Let e be the identity of G. Then we have,

$(aob)o(boa^{-1}) = [(aob)ob^{-1}]oa^{-1}$ .... [o is positive]
$=[ao(bob^{-1})oa^{-1}$ .... [o is associative]
$=[aoe]oa^{-1}$ ....[$bob^{-1} = e$]
$=[aoa^{-1}]$ .... [e is the identity]
$=e$ ....[$aoa^{-1} = e$]
Again we have,
$(b^{-1}oa^{-1})o(aob) = [(b^{-1}oa^{-1})oa]ob$...............[$o$ is associative]
$= [b^{-1}o(a^{-1}oa)]ob$..............[o is associative]
$= (b^{-1}oe)ob$......................[$a^{-1}oa = e$]
$= b^{-1}ob$...................[e is the identity]
$= e$..........................[$b^{-1}ob = e$]
Thus $(aob)^{-1} = b^{-1}oa^{-1}$.

Theorem 6

For any two elements a, b of a multiplicative group G, $(ab)^2 = a^2b^2$ if and only if G is abelian.

Proof:

Let $(ab)^2 = a^2b^2$. We shall show that G is abelian.

Now, $(ab)^2 = a^2b^2$
$\Rightarrow (ab)(ab) = (aa)(bb)$
$\Rightarrow a(ba)b = a(ab)b$

$\Rightarrow (ba)b = (ab)b$; by left cancellation law
$\Rightarrow ba = ab$; by right cancellation law
$\Rightarrow G$ is abelian.

Conversely, let G is abelian. We shall show that for any $a, b \in G, (ab)^2 = a^2b^2$.

Now $(ab)^2 = (ab)(ab)$
$= a(ba)b$
$= a(ab)b$; [G is abelian ,so ab=ba]
$= (aa)(bb)$
$= a^2b^2$

Hence Proved.

Theorem 7

If for every element in a group G is its own inverse,then G is abelian.

Proof:

Let G be a multiplicative group.

For any $a, b \in G$, we have their inverses $a^{-1}, b^{-1} \in G$ and let e be the identity element of G.

$a, b \in G \Rightarrow ab \in G$, by closure law
$\Rightarrow a = a^{-1}, b = b^{-1}$
and $ab = (ab)^{-1}$
Now $ab = (ab)^{-1}$
$= b^{-1}a^{-1}$; $[(aob)^{-1} = b^{-1}oa^{-1}]$
$=ba$
$\Rightarrow ab = ba$

Hence the group G is abelian.

Theorem 8

If G is a group such that $(ab)^i = a^ib^i$ for three consecutive integers for all $a, b \in G$, then G is abelian.

Proof:

Let $m, m+1, m+2$ be three consequtive integers for which
$(ab)^m = a^mb^m, (ab)^{m+1} = a^{m+1}b^{m+1}, (ab)^{m+2} = a^{m+2}b^{m+2}$
$\Rightarrow (ab)^{m+1}(ab) = (a^{m+1}a)(b^{m+1}b)$
$\Rightarrow a^{m+1}b^{m+1}(ab) = a^{m+1}(ab^{m+1})b$

$\Rightarrow b^{m+1}(ab) = (ab^{m+1})b$; By left cancellation law
$\Rightarrow (b^{m+1}a)b = (ab^{m+1})b$
$\Rightarrow b^{m+1}a = ab^{m+1}$; By right cancellation law
$\Rightarrow a^m(b^{m+1}a) = a^m(ab^{m+1})$; By left multiplication with a^m
$\Rightarrow a^m b^m(ba) = a^{m+1}b^{m+1}$
$\Rightarrow (ab)^m(ba) = (ab)^{m+1}$
$\Rightarrow (ab)^m(ba) = (ab)^m aab$
$\Rightarrow ba = ab$; By left cancellation law.
$\Rightarrow ab = ba$
Hence G is abelian.

Theorem 9

The left identity is also the right identity.

Proof:

Let e be the left identity of a group G. Then for any $a \in G$ we have
$eoa = a$......(1)

We shall prove that e is the right identity . For this it is enough to show that
$aoe = a$.......(2)
If a^{-1} is the left inverse of a, then
$a^{-1}oa = e$.....(3)
By associative law in G we have
$a^{-1}o(aoe) = (a^{-1}oa)oe$
$= eoe$, by (3)
$= e = a^{-1}oa$, by (3)
$\Rightarrow a^{-1}o(aoe) = a^{-1}oa$
$\Rightarrow aoe = a$, by left cancellation law.
which is same as of (2).
Thus the left identity is also the right identity.

Theorem 10

A set G with a binary composition denoted multiplicatively is a group iff
(i) the composition is associative
(ii) the equations $ax = b$ and $ya = b$ has unique solutions in G.

Proof:

First suppose that G is a group. We shall prove that the conditions (i) and (ii) hold.

Since G is a group, so associative law hold in G and thus the condition (i) is satisfied.

For condition (ii) we have $a, b \in G \Rightarrow a^{-1} \in G$ and $a^{-1}b \in G$.

Now putting $a^{-1}b$ for x in the left side of $ax = b$ we get

$a(a^{-1}b) = (aa^{-1})b$, by associative law

$= eb$, where e is the identity element of G.

$= b$

Therefore $x = a^{-1}b$ satisfy the equation $ax = b$.

For uniqueness: If possible let $x = x_1$ and $x = x_2$ are two solutions of $ax = b$. Then

$ax_1 = b = ax_2$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x_1 = x_2$, by left cancellation law

Therefore the equation $ax = b$ has a unique solution.

Again, for the equation $ya = b$ we have

$a \in G \Rightarrow a^{-1} \in G$

$b, a^{-1} \in G \Rightarrow ba^{-1} \in G$.

Now putting ba^{-1} for y in the left side of $ya = b$ we get

$(ba^{-1})a = b(a^{-1}a)$, by associative law

$= be$, where e is the identity element of G.

$= b$

Therefore $y = ba^{-1}$ satisfy the equation $ya = b$.

For Uniqueness: If possible, let y_1 and y_2 are two solutions of $ya = b$. Then

$y_1 a = b = y_2 a$

$\Rightarrow y_1 a = y_2 a$

$\Rightarrow y_1 = y_2$, by right cancellation law

Therefore, The equation $ya = b$ has a unique solution.

Conversely, suppose that conditions (i) and (ii) hold. We shall prove that G is a group. For this we only need to show that identity exists and every element of G has a inverse.

Existence of identity: Putting $b = a$ in $ax = b$ and $ya = b$ we have

$ax = a$ and $ya = a$

$\Rightarrow ax = ae_1$ and $ya = e_2 a$

where e_1 and e_2 are left and right identity of G.

$\Rightarrow x = e_1$ and $y = e_2$
Therefore $ae_1 = a$.....(1) and $e_2a = a$.....(2)
Now $be_1 = (ya)e_1 = y(ae_1) = ya = b$......(3), by (1)
and $e_2b = e_2(ax) = (e_2a)x = ax = b$......(4), by (2)
(3) and (4) are true for all $b \in G$.
Taking $b = e_2$ in (3) and $b = e_1$ in (4) we get
$e_2e_1 = e_2$ and $e_2e_1 = e_1$
$\Rightarrow e_1 = e_2 = e$, say
Thus unique identity exists in G.

Existence of inverse: The equations $ax = b$, $ya = b$ have unique solution. Choosing $b = e$ we get
$ax = e$ and $ya = e$
These equations have unique solution. Let the solutions in G are $x = c$ and $y = d$. Then
$ac = e$ and $da = e$.......(5)
$\Rightarrow d(ac) = de$
$\Rightarrow (da)c = d$
$\Rightarrow ec = d$
$\Rightarrow c = d$
From (5), $ac = e = ca$
$\Rightarrow c$ is the inverse of $a \Rightarrow c = a^{-1}$.
Since $c \in G$, so $a^{-1} \in G$
Thus inverse exists in G.
This proves that G is a group.

1.6 Some Problems on Group

Problem 1

$(R, +)$ is a group under the usual addition $(+)$ in R.

Solution:

We have $R = x : x \in QUQ'$.
Since the usual addition is a binary operation in R, then clearly the following laws hold in R:
(i) $\forall a, b \in R \Rightarrow a + b \in R$ since the sum of two real numbers is also a real number.
(ii) $\forall a, b, c \in R \Rightarrow (a + b) + c = a + (b + c)$
(iii) $\exists 0 \in R$ such that $a + 0 = 0 + a = a, \forall a \in R$

(iv) $a \in R \Rightarrow \exists -a \in R$ such that $a + (-a) = (-a) + a = 0$.

Thus $(R, +)$ satisfies each of the axioms of a group and therefore it is a group.

Problem 2

The set $G = \{1, -1\}$ forms a finite multiplicative abelian group.

Solution:

Given that $G = \{1, -1\}$

(i) **Closure law:** $1.(-1) = -1 \in G \Rightarrow$ closure law satisfied.

(ii) **Associative law:** $(-1.1).1 = -1.(1.1)$

$(1.1).(-1) = 1.(1.(-1))$ and so on.

$\Rightarrow$ Associative law satisfied.

(iii) **Existence of identity**: There exists the unique element 1 in G such that

$1.(-1) = (-1).1 = -1 \in G$

$\Rightarrow$ 1 is the identity element of G.

$\Rightarrow$ Identity element exists.

(iv)**Existence of inverse:** $1^{-1} = \frac{1}{1} = 1 \in G$

and $(-1)^{-1} = \frac{1}{-1} = -1 \in G$

Also, $1.1^{-1} = 1^{-1}.1 = 1.1 = 1$

and $(-1).(-1)^{-1} = (-1)^{-1}.(-1) = (-1).(-1) = 1$

$\Rightarrow$ Inverse exists and every element of G has an inverse in G.

(v)**Commutative law:** $1.(-1) = (-1).1 = -1$

$\Rightarrow$ commutative law hold in G.

(vi) Number of elements of $G = 2 =$finite.

Hence $G = \{1, -1\}$ forms a finite multiplicative abelian group.

Problem 3

If a and x are two elements of a group G such that $axa = b$, then $x =?$.

Solution:

Given that $axa = b$

$\Rightarrow a^{-1}(axa) = a^{-1}b$

$\Rightarrow (a^{-1}a)(xa) = a^{-1}b$

$\Rightarrow e(xa) = a^{-1}b$

$\Rightarrow xa = a^{-1}b$
$\Rightarrow xaa^{-1} = a^{-1}ba^{-1}$
$\Rightarrow xe = a^{-1}ba^{-1}$
$\Rightarrow x = a^{-1}ba^{-1}$. **(Ans)**

Chapter 2

Introduction to Rings

2.1 Ring

2.1.1 Definition

A ring is a nonempty set R equipped with two operations called addition (+) and multiplication (.) that satisfies the following properties:

(1) (R,+) is an abelian group, i.e

(i) **Closure Property of Addition:**

$\forall a, b \in R \Rightarrow a + b \in R$

(ii) **Associative Property of Addition:**

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

(iii) **Existence of Additive Identity:**

$\exists\ 0 \in R$ such that $a + 0 = 0 + a = a, \forall a \in R$

(iv) **Existence of Additive Inverse:**

for each $a \in R\ \exists -a \in R$ such that $a + (-a) = (-a) + a = 0$

(v) **Commutative Law of Addition:**

$a + b = b + a, \forall a, b \in R$

(2) (R,*) is a semi group i.e,

(i)Closure property of multiplication:

$\forall a, b \in R \Rightarrow ab \in R$

(ii)Associative law of multiplication:

$(ab)c = a(bc), \forall a, b, c \in R$

(3) multiplication distributes addition,i.e,

(i)Distributive Law:

Left Distributive : $a(b + c) = ab + ac, \forall a, b, c \in R$
Right Distributive : $(a + b)c = ac + bc, \forall a, b, c \in R$

2.1.2 Example of Rings

Some example of Rings are given below:
1. ($\mathbf{Z}$ +, .), ($\mathbf{Q}$,+, .), ($\mathbf{C}$,+, .) are ring.
2. The set of all 2×2 matrix with entries integers is a ring with respect to the operations matrix addition and matrix multiplication.
3. Set of all even integers is a ring with respect to addition and multiplication composition.

2.1.3 Various Types of Ring

Trivial Ring:

The singleton set $\{0\}$ is a ring with addition and multiplication given by $0 + 0 = 0$ and $0.0 = 0$.
This ring is called the trivial ring.
It is also called the zero ring or the null ring.

Non-trivial Ring:

A ring which is not a trivial ring is called a non-trivial ring. The non-trivial ring contains at least two elements, the additive identity 0 and a non zero element.

Commutative Ring:

A ring R is called a commutative ring if the multiplication composition in R is commutative, i.e, if

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

Example: The ring $(R, +, .)$ is a commutative ring of real numbers.

Ring with Zero Divisors:

A ring $(R, +, .)$ is said to be a ring with zero divisors if it is possible to find at least two elements a and b of R such that, $a \neq 0, b \neq 0$ but $ab = 0$.

Example: The set of all 2×2 matrix with entries integers is a ring with zero divisors.

Integral Doamin:

A ring $(R, +, .)$ is said to be an integral domain if it is a commutative ring with unity and without zero divisors.

Example: $(\mathbf{Z}, +, .), (\mathbf{R}, +, .), (\mathbf{C}, +, .)$ are integral domain.

Field:

A ring $(R, +, .)$ is said to be a field if it is a commutative ring with unity in which every non-zero element has a multiplicative inverse.

Example: $(\mathbf{Z}, +, .), (\mathbf{Q}, +, .), (\mathbf{C}, +, .)$ are field.

2.1.4 Properties of Rings

Theorem 1

Let R be a ring whose compositions have been denoted by additively and multiplicatively. Let $a, b, c \in R$, then

(i) $a.0 = 0.a = 0$ where 0 is the additive identity in R.

(ii) $(-a).b = a.(-b) = -(ab), \forall \ a, b \in R$.

(iii) $(-a)(-b) = ab, \forall \ a, b \in R$.

(iv) $a(b - c) = ab - ac, \forall \ a, b, c \in R$.

(v) $(b - c)a = ba - ca, \forall \ a, b, c \in R$.

(vi) $-(a + b) = (-a) + (-b), \forall a, b \in R$.

Proof (i):

Using the property of 0 in R,We may write

$a + 0 = 0 + a = a$................(1)
If $a = 0$, then (1)$\Rightarrow$ $0 + 0 = 0$.........(2)
Now, $a.(0 + 0) = a.0$ [by (2)]
$\Rightarrow$ $a.0 + 0.a = a.0$ [by LDL]
$\Rightarrow$ $a.0 = 0$......(3) [by Cancellation Law]
Again, $(0 + 0).a = 0.a$ [by(2)]
$\Rightarrow$ $0.a + a.0 = 0.a$
$\Rightarrow$ $0.a = 0$...(4) [by Cancellation law]
Thus (3)and (4)$\Rightarrow$ $a.0 = 0.a = 0$, $\forall$ a$\in$ R
Hence (i) is proved.

Proof (ii):

We have,

$(a + (-a)) = (-a) + a = 0$............(5)
and
$b + (-b) = (-b) + b = 0$...........(6)
By (1) we have, $a.0 = 0 \Rightarrow a.(b + (-b)) = 0$ [by (6)]
$\Rightarrow ab + a(-b) = 0$ [by LDL]
$\Rightarrow a.(-b) = -(ab)$..........(7)
Again by (i) we have,
$0.b = 0 \Rightarrow (a + (-a)).b = 0$ [by (5)]
$\Rightarrow ab + (-a).b = 0$ [by RDL]
$\Rightarrow (-a)b = -(ab)$...(8)
Thus (7) and (8) we have, $(-a)b = a(-b) = -(ab)$, $\forall\ a, b \in R$
Hence (ii) is proved.

Proof (iii):

We have,$(-a)(-b) = -(a(-b))$ [by (2)]
$= -(-(ab))$ [by(2)]
$= ab$ [Because $-(-x) = x$, $\forall\ x \in$ R]
Thus $\forall\ a, b \in$ R $\rightarrow (-a)(-b) = ab$
Hence (iii) is proved.

Proof (iv):

We have, $b - c = b + (-c) \; \forall \; b, c \in R$

Then, $a(b - c) = a(b + (-c)) = ab + a(-c)$ [by LDL]

$= ab - ac$ [by (ii)]

Thus $\forall \; a, b, c \in R \rightarrow a(b - c) = ab - ac$

Hence (iv) is proved.

Proof (v):

Again,$(b - c)a = (b + (-c))a$[Because $b - c = b + (-c)$]

$= ba + (-c)a$ [by RDL]

$= ba - ca$

Thus $\forall \; a, b, c \in$ R) $\Rightarrow (b - c)a = ba - ca$

Hence (v) is proved.

Proof (vi):

We have

$(a + b) + [(-a) + (-b)]$

$= (b + a) + [(-a) + (-b)]$; by commutative law of addiction in R.

$= b + [a + (-a) + (-b)]$, by associative law

$= b + [0 + (-b)]$

$= b + (-b)$

$= 0$

$\Rightarrow (-a) + (-b) = -(a + b)$; By inverse law

$\Rightarrow -(a + b) = (-a) + (-b)$.

Hence (vi) is proved.

Theorem 2

If R is a commutative ring of characteristic p, a prime then for any $a, b \in R, (a + b)^p = a^p + b^p$.

Proof:

Given R is a commutative ring. So for any $a, b \in R$, we have $ab = ba$.

Again, $(a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2$

$= a^2 + 2ab + b^2$,

$(a + b)^3 = (a + b)(a + b)^2$

$= (a + b)(a^2 + 2ab + b^2)$

$= a^3 + a(2ab) + ab^2 + ba^2 + b(2ab) + b^3$
$= a^3 + 2a^2b + ab^2 + a^2b + 2ab^2 + b^3$
$= a^3 + 3a^2b + 3ab^2 + b^3$
$= a^3 +^3 c_1a^{3-1}b^1 +^3 c_2a^{3-2}b^2 + b^3$
Thus, by binomial theorem we have
$(a+b)^p = a^p +^p c_1a^{p-1}b +^p c_2a^{p-2}b^2 + ... +^p c_ra^{p-r}b^r + ... + b^p$......(1)
Now, $^pc_r = \frac{p!}{r!(p-r)!} = \frac{p(p-1)!}{r!(p-r)!}$

Here p is a prime, so p and $r!(p-r)!$ have no common factor except 1. Therefore , $r!(p-r)!$ must be a factor of $(p-1)!$.

Thus, ^pc_r= some integral multiple of p
$= pn$, for some integer $n > 0$.
Now for $1 \leq r \leq (p-1)$ we have
$^pc_ra^{p-r}b^r = pna^{p-r}b^r = 0$
$\Rightarrow$ All terms except the first and last terms in the right side of (1) vanish.

Thus from (1) we get
$(a+b)^p = a^p + 0 + 0 + ... + 0 + b^p$
$\Rightarrow (a+b)^p = a^p + b^p$.

Theorem 3

If(R,+,.) is a Ring with unity 1, then
(i)$a(-1) = (-1)a = -a \ \forall \ a \in R$
(ii)$(-1)(-1) = 1$

Proof (i):

Since 1 is the unity of R then,
$1 + (-1) = (-1 + 1 = 0$.........(1)
$\Rightarrow a.1 = 1.a = a \ \forall \ a \in R$..........(2)
Now we have ,
$a.0 = 0.a = 0 \ \forall \ a \in R$
$\Rightarrow a(1 + (-1)) = a((-1) + 1) = 0$ [By (1)]
$\Rightarrow a.1 + a(-1) = a(-1) + a.1 = 0$ [by distributive law]
$\Rightarrow a + a(-1) = a(-1) + a = 0$ [by (2)]
$\Rightarrow a(-1) = -a$............(3)
Similarly,
$0.a = 0$
$\Rightarrow (1 + (-1))a = ((-1) + 1)a = 0$
$\Rightarrow 1.a + (-1)a = (-1)a + 1.a = 0$

$\Rightarrow a + (-1)a = (-1)a + a = 0$
$\Rightarrow (-1)a = -a$........(4)
Thus (3) and (4) $\Rightarrow a(-1) = (-1)a = -a$.........(5)
Hence $a(-1) = (-1)a = -a$, $\forall\ a \in R$.

Proof (ii):

We have, $\forall\ a, b \in R \Rightarrow (-a)(-b) = ab$........(6)
If $a = b = -1$,then (6) $\Rightarrow (-1)(-1) = (1)(1) = 1.1 \Rightarrow (-1)(-1) = 1$.

2.1.5 Characteristic of a Ring

Definition:

The characteristic of a ring R is the smallest positive integer n, if it exists, such that $n.a = 0\ \forall a \in R$ In case, such an n does not exist,we say that the ring R is of characteristic 0 or of infinite characteristic.

Example:

Some examples of characteristic of rings are given below:
1. In the ring Z of all integers there exist no positive integer for which
$n.a = 0\ \forall a \in Z$
So, Z is of infinite characteristic.
2. In a ring $(Z_5 = \{0, 1, 2, 3, 4\},\ +_5, \times_5)$ it is clear that 5 is the least positive integer such that
$5 \times_5 a = 0\ \forall a \in Z_5$.
So Z_5 is of characteristic 5.

2.1.6 Some Problems on Ring

Problem 1

Let R be a ring such that $a^2 = a$ for all $a \in R$. Then
(i) $2a = 0$ for all $a \in R$
(ii) $ab = ba$ for all $a, b \in R$.

Solution:

Given that R is a ring such that
$a^2 = a, \forall a \in R$
(i) Now $a \in R \Rightarrow a + a \in R$
$\Rightarrow (a + a)^2 = a + a$, by given condition
$\Rightarrow (a + a)(a + a) = a + a$
$\Rightarrow (a + a)a + (a + a)a = a + a$
$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a$
$\Rightarrow (a + a) + (a + a) = (a + a) + 0$
$\Rightarrow a + a = 0$, by left cancellation law.
$\Rightarrow 2a = 0$
$(ii) a, b \in R \Rightarrow ab \in R \Rightarrow ab + ab \in R$
$\Rightarrow 2(ab) = 0$
$\Rightarrow ab + ab = 0........(1)$
Let $a, b \in R$. Then $a^2 = a, b^2 = b$ and $(a + b)^2 = a + b$
Now $(a + b)^2 = a + b$
$\Rightarrow (a + b)(a + b) = a + b$
$\Rightarrow (a + b)a + (a + b)b = a + b$, by distributive law
$\Rightarrow (a^2 + ba) + (ab + b^2) = a + b$
$\Rightarrow (a + ba) + (ab + b) = a + b$
$\Rightarrow (a + b) + (ab + ba) = (a + b) + 0$
$\Rightarrow ba + ab = 0$, by left cancellation law
$\Rightarrow ba + ab = ab + ab$, by (1)
$\Rightarrow ba = ab$, by right cancellation law
Therefore $ab = ba$.

Problem 2

A ring R with $x^2 = x, \forall x \in R$ must be commutative.

Solution:

Given $x^2 = x, \forall x \in R$ So, $(x + x)^2 = x + x$
$\Rightarrow (x + x)(x + x) = x + x$
$\Rightarrow (x + x)x + (x + x)x = x + x$; by distributive law.
$\Rightarrow (x^2 + x^2) + (x^2 + x^2) = x + x$
$\Rightarrow (x + x) + (x + x) = (x + x) + 0,$
$\Rightarrow x + x = 0......(1)$; by left cancellation law of addition.
Let $a, b \in R$. Then $a^2 = a, b^2 = b$ and $(a + b)^2 = a + b$

Now $(a+b)^2 = a+b$
$\Rightarrow (a+b)(a+b) = a+b$
$\Rightarrow (a+b)a + (a+b)b = a+b$; by distributive law
$\Rightarrow (a^2+ba) + (ab+b^2) = a+b$
$\Rightarrow (a+ba) + (ab+b) = a+b$;
$\Rightarrow (a+b) + (ba+ab) = (a+b)+0$
$\Rightarrow ba+ab = 0$; by left cancellation law.
$\Rightarrow ba+ab = ba+ba$; by (1)
$\Rightarrow ab = ba$; by left cancellation law.
Therefore R is commutative.

Problem 3

Let 'addition' and 'multiplication' be defined on the set Z of integers by $aob = a+b-1$ and $a*b = a+b-ab$ respectively. Then $(Z, o, *)$ is a commutative ring with unity.

Solution:

We know that the addition of two or more integers is a integer and the product of two or more integers is also a integer.
For commutative group:
(i) Closure property: For any $a, b \in \mathbf{Z}$ we have
$a+b-1 \in \mathbf{Z}$ and $a+b-ab \in \mathbf{Z}$
$\Rightarrow aob \in \mathbf{Z}$ and $a*b \in \mathbf{Z}$
$\Rightarrow \mathbf{Z}$ is closed under o and $*$.
(ii)Associative law: For any $a, b, c \in \mathbf{Z}$ we have
$(aob)oc = (a+b-1)oc$
$= a+b-1+c-1 = a+b+c-2$
$ao(boc) = ao(b+c-1) = a+b+c-1-1 = a+b+c-2$
Therefore $(aob)oc = ao(boc)$.
$\Rightarrow$ Associative law satisfied.
(iii) Existence of additive idenity : Let e be the identity element. Then $aoe = eoa = a$
$\Rightarrow a+e-1 = e+a-1 = a$
$\Rightarrow a+e-1 = a$
$\Rightarrow a+e-1 = a+0$
$\Rightarrow e-1 = 0$, by left cancellation law
$\Rightarrow e = 1$
Therefore $e = 1$ is the identity of o.

Existence of additive inverse: Let a' be the additive inverse of $a \in \mathbf{Z}$. Then

$aoa' = a'oa = e$

$\Rightarrow a + a' - 1 = 1$

$\Rightarrow a' = 2 - a$

Thus every element of $\mathbf{Z}$ has an inverse in $\mathbf{Z}$.

Commutative law: Let $a, b \in \mathbf{Z}$. Then

$aob = a + b - 1 = b + a - 1 = boa$

Thus (Z, o) is a commutative(abelian) group.

Multiplication $*$ is associative: For $a, b, c \in \mathbf{R}$ we have

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

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

$= a + b - ab + c - ac - bc + abc$

$= a + b + c - ab - ac - bc + abc$

$(a * b) * c = a * (b * c)$

$\Rightarrow$ Multiplication $*$ is associative.

(vii) Multiplication $*$ is distributed in addition o :

$a * (boc) = a * (b + c - a)$

$=a + b + c - 1 - a(b + c - 1)$

$= 2a + b + c - ab - ac - 1......(1)$

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

$= (a + b - ab) + (a + c - ac) - 1$

$= 2a + b + c - ab - ac - 1.......(2)$

$(aob) * c = (a + b - 1) * c$

$= a + b - 1 + c - (a + b - 1)c$

$= a + b + 2c - ac - bc - 1......(3)$

$a * cob * c = (a + c - ac)o(b + c - bc)$

$(a + c - ac) + (b + c - bc) - 1$

$= a + b + 2c - ac - bc - 1......(4)$

From (1) and $(2), (3)$, and (4) we have

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

and $(aob) * c = a * cob * c$

Hence the multiplication is distributed in addition.

(viii) For unity: Let m be the identity for multiplication $*$. Then for any $a \in \mathbf{Z}$ we have

$a * m = m * a = a$

$\Rightarrow a + m - am = a + 0$

$\Rightarrow m - am = 0$

$\Rightarrow m(1 - a) = 0$

$\Rightarrow m = 0 \in \mathbf{Z}$
$\Rightarrow 0$ is the unity of the ring $(Z, o, *)$.
Thus, $(\mathbf{Z}, o, *)$ is a commutative ring with unity.

Problem 4

If R is a ring with unity satisfying $(ab)^2 = a^2b^2 \ \forall \ a, b \in R$ then R is commutative.

Proof:

Since R is a ring with unity,that is $1 \in R$. Then $a \in R, b\in R \Rightarrow a \in R,\ b+1 \in R.$
$\Rightarrow [a(b+1)]^2 = a^2(b+1)^2 \qquad [(ab)^2 = a^2b^2\ ,\ \forall\ a, b \in R]$
$\Rightarrow a(b+1)a(b+1) = a^2(b+1)(b+1)$
$\Rightarrow (ab+a)(ab+a) = a^2[(b+1)b+(b+1)1]$ [By distributive law]
$\Rightarrow ab(ab+a) + a(ab+a) = a^2(b^2+b+b+1)$ [By distributive law]
$\Rightarrow (ab)^2 + aba + a^2b + a^2 = a^2b^2 + a^2b + a^2b + a^2$ [By distributive law]
$\Rightarrow a^2b^2 + aba + a^2b + a^2 = a^2b^2 + a^2b + a^2b + a^2$
$\Rightarrow aba = a^2b ...(1)$ [By cancelation of addition]
Replacing a by $a+1$ in (1)
$(a+1)b(a+1) = (a+1)^2b \Rightarrow (a+1)(ba+b) = (a+1)(a+1)b$
$\Rightarrow a(ba+b) + 1(ba+b) = (a+1)(ab+b)$
$\Rightarrow aba + ab + ba + b = a(ab+b) + 1(ab+b)$ [By(1)]
$\Rightarrow ab + ba = ab + ab$ [by cancellation law]
$\Rightarrow ba = ab$ [by cancellation law]
Hence $ab = ba, \forall\ a, b \in R$ and therefore R is commutative.

2.2 Subring

2.2.1 Definiton

A non-empty subset S of R is a subring if $a, b \in$S$\Rightarrow$a - b, $ab \in$S.
So S is closed under subtraction and multiplication.

2.2.2 Examples of Subring:

1. The subsets $0, 2, 4$ and $0, 3$ are subrings of $\mathbf{Z}_6$.

2. The set $a + bi \in \mathbf{C}$ where $a, b \in \mathbf{Z}$ forms a subring of $\mathbf{C}$.

3. The set $a + b * \sqrt{5}$ where $a, b \in Z$ is a subring of the ring $\mathbf{R}$. The set $x + y * \sqrt{5}$ where $x, y \in Q$ is also a subring of $\mathbf{R}$.

2.2.3 Properties of Subring

Theorem 1:

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

(i) $a, b \in$S⇒a–b∈S

(ii) $a, b \in S \Rightarrow ab \in$S

Proof:

To prove that the conditions are necessary let us suppose that S is a subring of R. Obviously S is a group with respect to addition, therefore $b \in$S⇒–b∈S.

Since S is closed under addition,

$a \in$S, $a \in$S,–b∈S

$\Rightarrow a + (-b) \in$S

$\Rightarrow a–b \in S$

Also S is closed with respect to multiplication,

$a \in$S, $b \in$S

$\Rightarrow ab \in$S

Now to prove that the conditions are sufficient, let S be a non-empty subset of R for which the conditions (i) and (ii) are satisfied.

From condition (i) $a \in S \Rightarrow a–a \in$S

$\Rightarrow 0 \in$S

Hence additive identity is in S. Now $0 \in$S, $a \in$S

$\Rightarrow 0–a \in$S

$\Rightarrow -a \in$S

i.e. each element of S possesses additive inverse.

Let $a, b \in$S then $-b \in$S and then from condition (i) $0 \in$S, $-b \in$S

$\Rightarrow a–(-b) \in$S

$\Rightarrow (a + b) \in$S

Thus S is closed under addition, and S being a subset of R, associative and commutative laws of multiplication over addition holds in S . Thus S is a subring of R.

Theorem 2

The necessary and sufficient conditions that a non-empty subset S of a ring R to be a subring of R to be a subring of R are
$(i) S + (-S) = S$
$(ii) SS \subset S$

Proof:

First suppose that S is a subring of a ring R.
(i) Let $a + (-b) \in S + (-S)$. Then $a \in S, -b \in S$
$\Rightarrow a \in S, b \in S$,
$\Rightarrow a - b \in S$, since S is a subring
$\Rightarrow a + (-b) \in S$
Therefore, $S + (-S) \subset S$.....(1)
Again, let $a \in S$. Then $a, 0 \in S$, since 0 is the zero element of S.
$\Rightarrow a \in S, -0 \in S$
$\Rightarrow a + (-0) \in S + (-S)$
$\Rightarrow a \in S + (-S)$
Therefore, $S \subset S + (-S)$.....(2)
From (1) and (2) we have $S + (-S) = S$.
(ii) Let $ab \in SS$. Then $a \in S$ and $b \in S$
$\Rightarrow ab \in S$, since S is closed under multiplication.
Therefore, $SS \subset S$.
Conversely, Suppose that the conditions (i) and (ii) hold. We shall prove that S is a subring of R.
Let $a, b \in S$. Then $ab \in SS \subset S$, by condition (i)
$\Rightarrow ab \in S$
By condition $(i), S + (-S) = S$
$\Rightarrow S + (-S) \in S$
For any $a, b \in S \Rightarrow a \in S, -b \in S$
$\Rightarrow a + (-b) \in S + (-S) \subset S$
$\Rightarrow a - b \in S$
Thus, $a, b \in S$ we have shown that $a - b \in S$ and $ab \in S$.
Hence S is a subring of the ring R.

Theorem 3

The intersection of two subring is again a subring.

Proof:

Let R_1 and R_2 are two subring of a ring R. Let $a, b \in R_1 \cap R_2$. Then
$a, b \in R_1 \Rightarrow a - b \in R_1, ab \in R_1$
$a, b \in R_2 \Rightarrow a - b \in R_2, ab \in R_2$
since, R_1 and R_2 are subrings.
Thus $\forall a, b \in R_1 \cap R_2$
$\Rightarrow a - b \in R_1 \cap R_2$
$ab \in R_1 \cap R_2$
Therefore $R_1 \cap R_2$ is a subring of R.

Theorem 4

The union of two subrings of a ring is not always a subring.

Proof:

Let $(R_1, +, .)$ and $(R_2, +, .)$ be two subrings of a ring $(R, +, .)$.
Then R_1 is a subring $\Rightarrow R_1$ is a group.
Then R_2 is a subring $\Rightarrow R_2$ is a group.
But $R_1 \cup R_2$ is not necessarily a subgroup. We know that $R_1 \cup R_2$ is a subgroup when $R_1 \cup R_2 \subset R_1$ or $R_1 \cup R_2 \subset R_2$.
Hence $(R_1 \cup R_2, +, .)$ is not always a subring of R.

2.2.4 Some Problems on Subring

Problem 1

An example that the union of two subring is not necessarily a subring.

Solution:

Let
$Z = \{... -3, -2, -1, 0, 1, 2, 3, ...\}$
$R_1 = \{... -6, -4, -2, 0, 2, 4, 6, ...\}$
$R_2 = \{... -9, -6, -3, 0, 3, 6, 9, ...\}$
$R_3 = \{... -12, -8, -4, 0, 4, 8, 12, ...\}$

Then R_1, R_2, R_3 are all subrings of Z.
Now $R_1 \cup R_2 = \{... - 9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9, ...\}$
$3, 4 \in R_1 \cup R_2$ but $3 + 4 = 7 \notin R_1 \cup R_2$
$\Rightarrow R_1 \cup R_2$ is not closed under addition and
so $R_1 \cup R_2$ is not subring of Z.
Again, $R_1 \cup R_3 = \{..., -6, -4, -2, 0, 2, 4, 6, ...\} = R_1$
$\Rightarrow R_3 \subset R_1 \Rightarrow R_1 \cup R_3$ is a subring of Z.

Problem 2

If $(R, +, .)$ is a ring, then
$Z(R) = \{x \in R : xy = yx, \forall y \in R\}$ is a subring of R.

Solution:

Given $Z(R) = \{x \in R : xy = yx, \forall y \in R\}$.
Let $a, b \in Z(R)$. Then $a, b \in R$
$\Rightarrow a - b \in R$ and $ab \in R$.........(1)
Also $ay = ya$ and $by = yb, \forall y \in R$
$\Rightarrow ay - by = ya - yb$
$\Rightarrow (a - b)y = y(a - b)$........(2)
$\Rightarrow a - b \in R$..........(3)
By definition of $Z(R)$ we have $a - b \in R \Rightarrow a - b \in Z(R)$.
Again, $(ab)y = a(by)$
$=a(yb)$, [by=yb]
$=(ay)b$
$=(ya)b$, [ay=ya]
$=y(ab)$
$\Rightarrow ab \in Z(R)$
Thus, we have proved that
$a, b \in Z(R) \Rightarrow a - b \in Z(R)$ and $ab \in Z(R)$
Hence $Z(R)$ is a subring of $(R, +, .)$.

2.3 Ideal of a Ring

2.3.1 Definition

Left Ideal: Let R be a ring. Then a subring S of R is called a left ideal of R if

$rs \in S$, $\forall r \in R$ and $s \in S$ **Right Ideal:** Let R be a ring. Then a subring S of R is called a right ideal of R if

$sr \in S$, $\forall s \in S$ and $r \in R$

Ideal (Two sided ideal)**:** Let R be a ring. Then a subring S of R is called an ideal (or two sided ideal) of R if

$rs \in S$ and $sr \in S$, $\forall r \in R$ and $s \in S$

2.3.2 Examples of Ideal of a ring

Example 1: Let $Z = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}$

and $E = \{... - 4, -2, 0, 2, 4, ...\}$

Then the subring E is an ideal of the ring Z.

Example 2: $S = ma, a \in Z$ is a both sided ideal of Z where m is an arbitrary but fixed positive integers and Z is a ring of all integers.

2.3.3 Properties of Ideal of a ring

Theorem 1

The intersection of two ideals of a ring R is an ideal of R.

Proof:

Let S_1 and S_2 be two ideals of a ring R. We shall prove that $S_1 \cap S_2$ is an ideal of R.

Let $a, b \in S_1 \cup S_2$. Then $a, b \in S_1$ and $a, b \in S_2$.

Given S_1 and S_2 are ideals, so they are subring of R.

$a, b \in S_1 \Rightarrow a - b \in S_1$ and $ab \in S_1$

$a, b \in S_2 \Rightarrow a - b \in S_2$ and $ab \in S_2$

$a - b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$

$\Rightarrow S_1 \cap S_2$, is a subring of R.

Also, let $a \in S_1 \cap S_2$ and $r \in R$, then $a \in S_1 \Rightarrow ar \in S_1$ and $ra \in S_1$ and $a \in S_2, r \in R$

$\Rightarrow ar \in S_2$ and $ra \in S_2$, since S_1 and S_2 are ideals of R.

Thus $ar \in S_1 \cap S_2$ and $ra \in S_1 \cap S_2$

Hence $S_1 \cap S_2$ is an ideal of R.

Theorem 2

Let S_1, S_2 be ideal of a ring R and let

$S_1 + S_2 = \{s_1 + s_2 : s_1 \in S_1, s_2 \in S_2\}$

Then $S_1 + S_2$ is an ideal of R generated by $S_1 \cup S_2$.

Proof:

Let $a_1 + a_2 \in S_1 + S_2, b_1 + b_2 \in S_1 + S_2$. Then

$a_1, b_1 \in S_1$ and $a_2, b_2 \in S_2$.

We have $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2)$. Since S_1 is an ideal,

therefore $a_1, b_1 \in S_1 \to a_1 - b_1 \in S_1$.

Simillary $a_2 - b_2 \in S_2$.

$(a_1 - b_1) + (a_2 - b_2) \in S_1 + S_2$

$(a_1 + a_2) - (b_1 + b_2) \in S_1 + S_2$ is a subgroup of the additive group of R.

Let r be any element of R, then

$r(a_1 + a_2) = ra_1 + ra_2 \in S_1 + S_2$ since $r \in R, a_1 \in S_1 \to ra_1 \in S_1$ and similarly $ra_2 \in S_2$

Simillary $(a_1 + a_2)r = a_1r + a_2r \in S_1 + S_2$ since $a_1r \in S_1, a_2r \in S_2$.

Hence $S_1 + S_2$ is an ideal of R. Since $0 \in S_1$ and also $0 \in S_2$, therefore obviously

$S_1 \subseteq S_1 + S_2$ and $S_2 \subseteq S_1 + S_2$.

$S_1 \cup S_2 \subseteq S_1 + S_2$

Thus $S_1 + S_2$ is an ideal of R containing $S_1 \cup S_2$, Also if S_1 is an ideal of R containing $S_1 \cup S_2$ then S must contain $S_1 \cup S_2$ .Thus $S_1 + S_2$ is the smallest ideal of R containing

$S_1 + S_2 = S_1 \cup S_2$.

2.3.4 Some problems on Ideal of a ring

Problem 1

Every ideal S of a ring R is a subring of R.

Solution:

Let S be an ideal so $\forall a, b \in S \to a - b \in S$.....(1)

Since S is an ideal so

$sr \in S, rs \in S, s \in S, r \in R$

Also $S \subseteq R$, this can be written $as, sr \in S, rs \in S, s \in S, r \in S$
So closure property satisfied.
Hence S is a subring.

Problem 2

If S is an ideal of a ring R and T is an subring of R. Then S is an ideal of $S + T$.

Proof:

Since S is ideal of $R \rightarrow S$ is a subring of R .

Let $a + x, b + y \in S + T$ where $a, b \in S$ and $x, y \in T$. Now since S is a subring

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

Again T is a subring

$\Rightarrow x - y, xy \in S$.

Now we have $(a + x) - (b + y) = (a - b) + (x - y) \in S + T$......(1).

Again We have $(a + x)(b + y) = a(b + y) + x(b + y) = (ab + ay + xb) + xy$......(2)

Now since S is an ideal of R, then $a, b \in S$,thus

(2) $\Rightarrow (a + x)(b + y) \in S + T$........(3)

Hence (1) and (2) $\Rightarrow S + T$ is a subring of R. Now since T is a subring of R and therefore $0 \in T$. Then for any $a \in S$ we have $a = a + 0 \in S + T \Rightarrow S \subseteq S + T$.

Now since $S \subseteq S + T$ and $S + T$ is a subring of $S + T$.

Again since S is an ideal of R and $S + T \subseteq S$ is an ideal of $S + T$.

Problem 3

If R is a finite commutative ring with unity element then every prime ideal of R is a maximal ideal of R.

Solution:

Let R be a finite commutative ring with unit element.

Let S be a prime ideal of R. Then we need to prove that S is a maximal ideal of R.

Since S is a prime ideal of R, therefore the residue class ring R/S is an integral domain. Now

$R/S = \{S + a : a \in R\}$

Since R is a finite ring therefore R/S is a finite integral domain. But every finite domain is a field, therefore R/S is a field.

Since R is a commutative ring with unity and R/S is a field.

Therefore S is a maximal ideal of R.

Chapter 3

Arithmetical Function and it's Properties

3.1 Arithmetical Function

3.1.1 Definition

An arithmetical function is a function defined on the positive integers which takes values in the real or complex numbers.

For every arithmetic functions f, g addition is defined in the classical way

$(f + g)(n) = f(n) + g(n)$.

3.1.2 Examples of Arithmetical Functions

$\tau(n)$: the number of divisors of n.

$\sigma(n)$: the sum of the divisors of n.

$\epsilon(n)$: the function defined by setting $\epsilon(n)$ =1 for every $n \in \mathbf{N}$.

$\phi(n)$: the numbers of natural numbers not exceeding n and coprime to n.

$\omega(n)$: the number of distinct prime factors of n.

3.1.3 Properties of Arithmetical Function

Theorem 1

The set of arithmetic functions with addition $(A, +)$ is an integral domain.

Proof:

First let us show that A together with addition forms an abelian group

(i) Commutativity: Let $f, g \in A$ and $n \in N$.
$(f+g)(n) = f(n) + g(n) = g(n) + f(n) = (g+f)(n)$

(ii) Associativity: Let $f, g, h \in A$ and $n \in N$
$(f+(g+h))(n) = f(n) + (g+h)(n)$
$= f(n) + g(n) + h(n)$
$= (f+g)(n) + h(n)$
$= ((f+g)+h)(n)$

(iii) Identity: $0(n) = 0$ for every $n \in N$, if $f \in A$ and $n \in N$ then:
$(f+0)(n) = f(n) + 0(n)$
$= f(n) + 0$
$= f(n)$, $\forall f(n) \in S$.

(iv)Inverse: $(-f)(n) = -f(n)$ for any $n \in N$ we have:
$(f+(-f))(n) = f(n) + (-f)(n)$
$= f(n) + (-f(n))$
$= 0$
$= 0(n)$, $\forall f(n) \in S$.

Also A has no zero divisors.

Thus $(A, +)$ is an integral domain.

Theorem 2

If f and g are arithmetical functions we have:
(a) $(f+g)' = f' + g'$.
(b) $(f * g)' = f' * g + f * g'$
(c) $(f^{-1})' = -f^{-1} * (f * f)^{-1}$, provided that $f(1) \neq 0$.

Proof:

If f and g are arithmetical functions then the derivative of f and g is defined as
$f'(n) = f(n) logn$, $n \geq 1$
$g'(n) = g(n) logn$, $n \geq 1$

(a) By the definition of derivative, we have $(f+g)'(n) = (f+g)(n)logn$
$= (f(n)+g(n))logn$
$= f(n)logn + g(n)logn$
$= f'(n) + g'(n).$

(b) Note that $(f*g)'(n) = (f*g)(n)logn$
$= \sum_{d|n} f(d)g(\frac{n}{d})logn$
$= \sum_{d|n} f(d)g(\frac{n}{d})log(d\frac{n}{d})$
$= \sum_{d|n} f(d)g(\frac{n}{d})logd + \sum_{d|n} f(d)g(\frac{n}{d})log(\frac{n}{d})$
$= \sum_{d|n} f(d)logdg(\frac{n}{d}) + \sum_{d|n} f(d)g(\frac{n}{d})log(\frac{n}{d})$
$= \sum_{n|d} f'(d)g(\frac{n}{d}) + \sum_{d|n} f(d)g'(\frac{n}{d})$
$= (f'*g)(n) + (f*g')(n)$

(c) Note that $I' = 0$. This implies that $(f*(f^{-1}))' = 0$
Then by part (b) we have
$0 = f'*f^{-1} + f*(f^{-1})'$
This implies that $f*(f^{-1})' = -(f'*f^{-1})$
$\Rightarrow f^{-1}*(f*(f^{-1})') = -f^{-1}*(f'*f^{-1})$
$\Rightarrow (f^{-1}*f)*(f^{-1})' = -f'*(f^{-1}*f^{-1})$
$\Rightarrow I*(f^{-1})' = -f'*(f*f)^{-1}$
$\Rightarrow (f^{-1})' = -f'*(f*f)^{-1}.$
This completes the proof.

3.2 Pointwise Sum of Arithmetical Function

3.2.1 Definition

Let S be a non-empty set.
Let F be one of the standard number sets: $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ or $\mathbf{C}$.
Let F^S be the set of all mappings $f : S \longrightarrow F$.
The (binary) operation of pointwise addition is defined on F^S as:
$+ : F^S * F^S \longrightarrow F^S : \forall f, g\ \epsilon F^S$: $\forall s \epsilon S : (f+g)(s) := f(s) + g(s)$ where the $+$ on the right hand side is conventional arithmetic addition.

3.2.2 Properties of pointwise addition

Theorem 1:

Let S be a non-empty set.
Let F be one of the standard number sets: $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ or $\mathbf{C}$.
Let $f, g, h : S \to F$ be functions.
Let $f + g : S \to F$ denote the pointwise sum of f and g.
Then:
$(f + g) + h = f + (g + h)$.
That is, pointwise addition is associative.

Proof:

From the definition of pointwise addition we get,
$\forall\ x \epsilon S : ((f + g) + h)(x) = (f(x) + g(x)) + h(x)$
$= f(x) + (g(x) + h(x))$
$= (f + (g + h))(x)$
Hence proved.

Theorem 2:

Let S be a non-empty set.
Let F be one of the standard number sets: $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ or $\mathbf{C}$.
Let $f, g, h : S \to F$ be functions.
Let $f + g : S \to F$ denote the pointwise sum of f and g.
Then:
$f + g = g + f$
That is, pointwise addition is commutative.

Proof:

From the definition of pointwise addition we get,
$\forall x \epsilon S : (f + g)(x) = f(x) + g(x)$
$= g(x) + f(x)$
$= (g + f)(x)$
Hence proved.

3.3 The M$\ddot{o}$bius Inversion Formula

3.3.1 Definition:

The Möbius function $\mu(n)$ (named after A.F. M$\ddot{o}$bius,1790-1868) is the Dirichlet inverse of the function ϵ defined by

$\epsilon(n) = 1$ for every $n \in N$.

μ is multiplicative because ϵ is multiplicative. Moreover

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{when } n = 1 \\ 0 & \text{when } n > 1 \end{cases}$$

because , by definition $\mu * \epsilon = \iota$, and the L.H.S. is equal to

$\sum_{d|n} \mu(d)\epsilon(\frac{n}{d}) = (\mu * \epsilon)(n)$.

3.3.2 Properties of M$\ddot{o}$bius Inversion Formula

Theorem 1

$\mu(n)$ is determined by the formula

$$\mu(n) = \begin{cases} 1 & \text{when } n = 1, \\ (-1)^r & \text{when n is the product of r distinct primes,} \\ 0 & \text{when } p^2/n \text{ for some prime p.} \end{cases}$$

Proof:

The fundamental theorem of arithmetic ensures that this formula indeed gives us a well-defined arithmetical function. Our task is to derive this formula from our definition μ as the Dirichlet inverse of ϵ. Being multiplicative, $\mu(1) = 1$. For any prime p, we have

$0 = \iota(p) = \sum_{d|p} \mu(d)\epsilon(\frac{p}{d}) = \mu(1) + \mu(p)$

$\Rightarrow \mu(p) = -1$.

Hence, if $n = p_1 p_2 ... p_r$ is the product of r distinct primes, then by the multiplicativity of μ, we have

$\mu(n) = \mu(p_1)\mu(p_2)...\mu(p_r) = (-1)^r$.

Now we show that $\mu(p^k) = 0$ for every prime p and $k \geq 2$.

We have

$0 = \iota(p^2) = \mu(1) + \mu(p) + \mu(p^2) = \mu(p^2)$ because $\mu(p) = -1$.

By induction on k, the claim follows.

Suppose now n is divisible by the square (or some higher power) of a prime number p. Then $n = p^k m$, where $k = v_p(n) \geq 2$ and $p \dagger m$. So $(p^k, m) = 1$; hence

$\mu(n) = \mu(p^k)\mu(m) = 0$.

Theorem 2

The M$\ddot{o}$bius function μ is multiplicative.
That is, $\mu(mn) = \mu(m)\mu(n)$ if $(m, n) = 1$.

Proof:

(i) Let $m = n = 1$. Then $(m, n) = 1$.
$\mu(1.1) = \mu(1) = 1$ and $\mu(1)\mu(1) = 1.1 = 1$.
Thus $\mu(mn) = \mu(m)\mu(n)$.
(ii) Let $m, n \in \mathbf{N}$ with $(m, n) = 1$ and we are done.
(iii) Let $m = p_1p_2...p_r$ and $n = q_1q_2...q_s$ where $p_1, p_2, ...p_r$ and $q_1, q_2, ..., q_s$ are distinct primes such that $m(\neq 1)$ and $n(\neq 1)$ are both square free with $(m, n) = 1$. Then $mn = p_1p_2...p_rq_1q_2...q_s$.
By definition , $\mu(m) = (-1)^r, \mu(n) = (-1)^s, \mu(mn) = (-1)^{r+s}$.
Now $\mu(mn) = (-1)^{r+s} = (-1)^r.(-1)^s = \mu(m)\mu(n)$.
Thus $\mu(mn) = \mu(m)\mu(n)$ if $(m, n) = 1$.
Hence the M$\ddot{o}$bius function μ is multiplicative.

Theorem 3

Let f and g be two arithmetical function such that f is the summatory function of g. Then
$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} \mu(d)f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})f(d)$.

Proof:

By definition, μ is the Dirichlet inverse of ϵ and $\iota(iota)$ is the identity function. Then
$\epsilon * \mu = \mu * \epsilon = \iota(iota)$ [inverse property] ...(1)
and $f * \iota = \iota * f = f$. [identity property] ...(2)
Also $\epsilon(n) = 1 \ \forall n \in \mathbf{N}$. [definition of unit function] ...(3)
First we suppose that
$f(n) = \sum_{d|n} g(d)$.
Then $f(n) = \sum_{d|n} g(d)\epsilon(\frac{n}{d})$
$= (g * \epsilon)(n)$
$\Rightarrow f = g * \epsilon$
$\Rightarrow f * \mu = (g * \epsilon) * \mu$
$\Rightarrow g * (\epsilon * \mu)$
$= g * \iota = g$.
$\Rightarrow (f * \mu)(n) = g(n) \ \forall n \in \mathbf{N}$

$\Rightarrow \sum_{d|n} f(d)\mu(\frac{n}{d})\mu(d) = g(n)$.
Thus $g(n) = \sum_{d|n} \mu(d)f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})f(d)$.
Conversely, we suppose
$g(n) = \sum_{d|n} \mu(d)f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})f(d)$.
$\Rightarrow g(n) = (\mu * f)(n)$ [definition of Dirichlet product]
$\Rightarrow g = \mu * f$
$\Rightarrow \epsilon * g = \epsilon * (\mu * f) = (\epsilon * \mu) * f$
$\Rightarrow \epsilon * g = \iota * f$
$\Rightarrow \epsilon * g = f$
$\Rightarrow (\epsilon * g)(n) = f(n)\ \forall n \in \mathbf{N}$
$\Rightarrow \sum_{d|n} \epsilon(d)g(\frac{n}{d}) = \sum_{d|n} \epsilon(\frac{n}{d})g(d) = f(n)$
$\Rightarrow \sum_{d|n} g(\frac{n}{d}) = \sum_{d|n} g(d) = f(n)$
Therefore $f(n) = \sum_{d|n} g(d)$.
Hence $f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} \mu(d)f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})f(d)$.

Theorem 4

$\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$, where $\omega(n)$ denotes the number of distinct prime factors of n.

Proof:

We have, $\omega(1) = 0$ and $\omega(mn) = \omega(m)+\omega(n)$, whenever $(m, n) = 1$. Therefore $2^{\omega(n)}$ is a multiplicative function. Also, $\sum_{d|n} \mu(d)$ is a multiplicative function,

because $\mu(n)$ is multiplicative. Both sides of the claimed identity being multiplicative it is enough to prove it for $n = p^k$.

For $n = p^k$ the L.H.S. is $|\mu(1)| + |\mu(p)| = 1 + 1 = 2$, because $\mu(p^l) = 0$ for every $l \geq 2$; and the R.H.S. is $2^1 = 2$, because $\omega(p^k) = 1$. Therefore the claim is proved.

Chapter 4

Dirichlet Product and it's Properties

4.1 Dirichlet Product

4.1.1 Definiton

If $f, g : \mathbf{N} \to \mathbf{C}$ are two arithmetic functions from the positive integers to the complex numbers,the Dirichlet product $f * g$ is a new arithmetic function defined by:

$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$

where the sum extends over all positive divisors d of n, or equivalently over all distinct pairs (a, b) of positive integers whose product is n.

4.1.2 Examples of Dirichlet product

(i) Let $g(n) = n$ for all $n \in \mathbf{N}$. Then h(n)=sum of divisors of n.

(ii) Let $I(n) = [\frac{1}{n}]$ then $h(n) = (f * I)(n) = f(n)$

(iii) Let $u(n) = 1$ for all $n \in \mathbf{N}$. Then $h(n) = (\mu * u)(n) = \sum_{d|n} \mu(d)u(\frac{n}{d}) = \sum_{d|n} \mu(d) = I(n)$.

4.1.3 Properties of Dirichlet product

Theorem 1:

Dirichlet product is commutative and associative. That is, for any arithmetical functions f, g, k

$f * g = g * f$

$(f * g) * k = f * (g * k)$

Proof:

$(f * g)(n) = \sum_{d|n} g(d)f(\frac{n}{d})$
$= \sum_{d|n} f(d)g(n/d)$
$= \sum_{dd'=n} f(d)g(d')$
$= \sum_{g(d')} f(d)$
$= (g * f)(n)$.
Similarly,
$((f * g) * k)(n)$
$= \sum_{abc=n} f(a)g(b)k(c)$
$= (f * (g * k))(n)$.
Hence proved.

Theorem 2

If f is an arithmetical function with $f(1) \neq 0$, then $\exists$ arithmetical function h such that $f * h = h * f = \iota$, the identity function.

Proof:

The identity function $\iota(iota)$ is defined by

$$\iota(\text{n}) = \begin{cases} 1 & \text{when } n = 1 \\ 0 & \text{when } n > 1 \end{cases}$$

Let f be an arithmetical function such that $f(1) \neq 0$.
For n=1,we have
$(f * h)(1) = (h * f)(1) = \iota(1)$
$\Rightarrow \sum_{d|l} f(d)h(\frac{l}{d}) = 1$
$\Rightarrow f(1)h(1) = 1$
$\Rightarrow h(1) = \frac{1}{f(1)} = f^{-1}(1)$
$\Rightarrow h(1)$ is the unique inverse of $f(1)$.
Now let $n > 1$ and we suppose that $h(m) = f^{-1}(m)$ has been uniquely determined for every $m < n$. Then
$(f * h)(n) = (h * f)(n) = \iota(n)$
$\Rightarrow \sum_{d|n, 1 \leq d \leq n} h(d)f(\frac{n}{d}) = 0$
$\Rightarrow h(n)f(\frac{n}{n}) + \sum_{d|n, 1 \leq d \leq n} h(d)f(\frac{n}{d}) = 0$
$\Rightarrow h(n)f(1) = -\sum_{d|n, 1 \leq d \leq n} h(d)f(\frac{n}{d})$
$\Rightarrow h(n) = -\frac{1}{f(1)} \sum_{d|n, 1 \leq d \leq n} h(d)f(\frac{n}{d})$
Hence h is an arithmetical function if $f(1) \neq 0$, where

$f * h = h * f = \iota(iota)$, the identity function.

Also if the values of $h(d) = f^{-1}(d)$ are known for all divisors d with $1 \leq d < n$, there is a uniquely determined value for $h(n) = f^{-1}(n)$ as $f(1) \neq 0$.

Thus by induction on n, the arithmetical function f has a unique Dirichlet inverse $h(= f^{-1})$, where $f(1) \neq 0$.

Conversely, let the Dirichlet inverse $h(n) = f^{-1}$ of $f(n)$ exist.

Then for $n = 1, h(1) = f^{-1}(1) = \frac{1}{f(1)} \Rightarrow f(1) \neq 0$.

and for $n > 1, h(n) = f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n, 1 \leq d \leq n} h(d) f(\frac{n}{d}) \Rightarrow f(1) \neq 0$.

Thus there exists arithmetical function h such that $f*h = h*f = \iota$.

Theorem 3

The Dirichlet inverse of a multiplicative function is multiplicative.

Proof:

We know that every multiplicative function f with $f(1) \neq 0$ has unique Dirichlet inverse h. Then

$(f * h)(n) = (h * f)(n) = \iota(n)$ where the identity function ι is defined by

ι(n)= $\begin{cases} 1 & \text{when } n = 1 \\ 0 & \text{when } n > 1 \end{cases}$

Thus for $n = 1$ we have

$f(1)h(1) = \iota(1) = 1$

$\Rightarrow h(1) = \frac{1}{f(1)} = f^{-1}(1)$.

By induction on mn, we shall prove

$h(mn) = h(m)h(n)$ whenever $(m, n) = 1$.

$h(mn) = h(1) = \frac{1}{f(1)} = \frac{1}{1} = 1$

and $h(m)h(n) = h(1)h(1) = \frac{1}{1}.\frac{1}{1} = 1$

Thus $h(mn)h(m)h(n)$ is true for $mn = 1$.

Next let $mn > 1$ with $(m, n) = 1$. Then either $m > 1$ or $n > 1$.

We assume that

$h(lk) = h(l)h(k)$

holds where $lk < mn$ with $(l, k) = 1$ such that $lk|mn$.

Then we have

$(f * h)(mn) = (h * f)(mn) = \iota(mn)$

$\Rightarrow \sum_{lk|n,1\leq lk\leq mn} h(lk)f(\frac{mn}{lk}) = 0$
$\Rightarrow h(mn)f(\frac{mn}{mn}) + \sum_{lk|n,1\leq lk\leq mn} h(lk)f(\frac{mn}{lk}) = 0$
$\Rightarrow h(mn)f(1) = -\sum_{lk|n,1\leq lk\leq mn} h(lk)f(\frac{m}{l})f(\frac{n}{k})$
$\Rightarrow h(mn) = -\sum_{l|m,k|n}\sum_{lk|n,1\leq lk\leq mn} h(l)h(k)f(\frac{m}{l})f(\frac{n}{k})$
$\Rightarrow h(mn) = -\sum_{l|m,k|n}\sum_{lk|n,1\leq lk\leq mn} h(l)h(k)f(\frac{m}{l})f(\frac{n}{k})+(h(m)f(\frac{m}{m})(h(n)f(\frac{n}{n}))$
$\Rightarrow h(mn) = -\sum_{l|m} h(l)f(\frac{m}{l})\sum_{k|n} f(\frac{n}{k}) + (h(m)f(1))(h(n)f(1))$
$\Rightarrow h(mn) = -((h*f)(m))((h*f)(n)) + h(m)h(n)$
$\Rightarrow h(mn) = -\iota(m)\iota(n) + h(m)h(n)$
$\Rightarrow h(mn) = 0 + h(m)h(n)$
$\Rightarrow h(mn) = h(m)h(n).$

Thus if $h(lk) = h(l)h(k)$, where $lk < mn$ with $(l,k) = 1$ such that $lk|mn$, then

$h(mn) = h(m)h(n)$.

Hence by induction , the Dirichlet inverse of h of a multiplicative function is multiplicative.

4.1.4 Some Problems on Dirichlet product

Problem 1:

The Dirichlet inverse of λ is $|\mu|$.

Solution:

Both λ and $|\mu|$ are multiplicative, so their Dirichlet convolution $\lambda * |\mu|$ is multiplicative. Therefore, e is also multiplicative, so it suffices to show that the two functions agree on prime powers.

Now,
$(\lambda|\mu|)(pk) = \sum_{d|p^k} \lambda(\frac{p^k}{d}|\mu(d)|$
$=\lambda(p^k) + \lambda(p^k - 1)$
$= (-1)^k + (-1)^k - 1$
$= 0$

Since $e(p^k) = 0$, the functions agree on prime powers and hence are the same.

Problem 2:

$d * \Phi = \sigma$.

Solution:

Staring with $1 * \phi = I$ and convolve both sides with 1:
$1 * (1 * \phi) = 1 * I$
$(1 * 1) * \phi = \sigma$
$d * \phi = \sigma$
Hence showed.

Problem 3:

$\sum_{a|n} \sigma(\frac{n}{a}\Phi(a)) = nd(n)$.

Solution:

The left side is
$\sigma * \phi = (1 * I) * (\mu * I)$,
where $\phi = \mu * I$ comes from from Mobius inversion of $\phi * 1 = I$.
Rearranging and moving parentheses around gives
$\sigma * \phi = (1 * I) * (\mu * I) = (I * I) * e = I$
and
$(I * I)(n) = \sum_{a|n} a\frac{n}{a}$
$= \sum_{a|n} n$
$= nd(n)$.
Hence Showed.

4.1.5 Dirichlet Inverse

Definition:

Let f be an arithmetical function with $f(1) \neq 0$. If there exists a unique arithmetical h such that
$f * h = h * f = \iota$
where $\iota(iota)$ is the identity function defined by
$\iota(\text{n}) = \begin{cases} 1 & \text{when } n = 1 \\ 0 & \text{when } n > 1 \end{cases}$
then h is called the Dirichlet inverse of f and is denoted by f^{-1}.

4.2 Multiplicative Functions

4.2.1 Definition

An arithmetical function f is called multiplicative if and only if $f(mn) = f(m)f(n)$ holds whenever $(m, n) = 1$.

4.2.2 Examples of Multiplicative Functions

$\tau(n)$: the number of divisors of n.
$\sigma(n)$: the sum of the divisors of n.
$\epsilon(n)$: the function defined by setting $\epsilon(n)$ =1 for every $n \in \mathbf{N}$.
$\phi(n)$: the numbers of natural numbers not exceeding n and coprime to n.

4.2.3 Properties of Multiplicative Functions

Theorem 1

The Dirichlet product of two multiplicative functions is multiplicative.

Proof:

We need an observation which follows from the fundamental theorems of arithmetic. Suppose $(m, n) = 1, d$ runs through the divisors of m and k runs through the divisors of n. Then $l = dk$ runs through the divisors of mn just once. Therefore
$\sum_{d|m} \cdot \sum_{k|n}=\sum_{l|mn}$
Suppose f, g are multiplicative functions and $(m, n) = 1$.Then
$(f * g)(m)(f * g)(n) = (\sum_{d|m} f(d)g(\frac{m}{d}))(\sum_{k|n} f(k)g(\frac{n}{k}))$
$= \sum_{d|m} \sum_{k|n} f(d)f(k)g(\frac{m}{d})(\frac{n}{k})$
$= \sum_{d|m} \sum_{k|n} f(dk)g(\frac{mn}{dk})$
$= \sum_{l|mn} f(l)g(\frac{mn}{l})$
$= (f * g)(mn)$.

Theorem 2

(a) If f is multiplicative,then
(1) $f(n) = \prod_{p|n} f(p^{\alpha_p})$, where $n = \prod_{p|n} p^{\alpha_p}$
($\sum_{p|n}$ denotes a product taken over all distinct prime factors of n)

(b) Two multiplicative arithmetical functions f, g are equal if and only if

$(3) f(p^k) = (p^k)$ holds for every prime p and $k \in \mathbf{N}$.

Proof:

(a) Suppose $n > 1$ has the prime factorization

$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ $(r \geq 1, \alpha_i \geq 1)$

where $p_1, p_2, ..., p_r$ are the distinct prime factors of n. Then the numbers $p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ are coprime in pairs ; because f is multiplicative, we have

$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) ... f(p_r^{\alpha_r}) = \prod_{p/n} f(p_p^{\alpha})$

$(b) f(n) = g(n)$ for all $n \in \mathbf{N}$ implies

$f(p^k) = g(p^k)$ for every prime p and $k \in \mathbf{N}$.

Conversely, if $f(p^k) = g(p^k)$ holds for every prime p and every $k \in \mathbf{N}$ and if $n = \prod_{p|n} p^{\alpha_p}$, then

$f(n) = \prod_{p|n} f(p^{\alpha_p})$ [because f is multiplicative]

$= \prod_{p|n} g(p^{\alpha_p})$ [by hypothesis]

$=g(n)$. [because g is multiplicative]

If we know that f is multiplicative and if we know $f(p^k)$, then the theorem at once yields an explicit formula for $f(n)$.

Theorem 3

If f is a multiplicative function and g is defined by $g(n) = \sum_{d|n} f(d)$, then g is also multiplicative.

Proof:

Given $g(n) = \sum_{d|n} f(d)$.

Let $(n_1, n_2) = 1$. If $d_1 | n_1$ and $d_2 | n_2$, then $(d_1, d_2) = 1$ and $c = d_1 d_2$ runs over all divisors of $n_1 n_2$. It implies that $c | n_1 n_2$.

$g(n_1 n_2) = \sum_{c|n_1 n_2} f(c)$

$=\sum_{d_1|n_1, d_2|n_2, (d_1,d_2)=1} f(d_1 d_2)$

$=\sum_{d_1|n_1, d_2|n_2, (d_1,d_2)=1} f(d_1) f(d_2)$ [f is multiplicative]

$=\sum_{d_1|n_1} f(d_1) \sum_{d_2|n_2} f(d_2)$

$=g(n_1) g(n_2)$.

Hence g is multiplicative.

Problem 1

$\sum_{d|n}(\tau(d))^3 = (\sum_{d|n} \tau(d))^2$.

Proof:

$\tau(n)$ is multiplicative; so $\sum_{d|n} \tau(d), (\tau(d))^3, \sum_{d|n}(\tau(d))^3, (\sum_{d|n} \tau(d))^2$ are all multiplicative. Each side of the claimed identity $\sum_{d|n} \tau(d), (\tau(d))^3, \sum_{d|n}(\tau(d))^3, (\sum_{d|n}$ being multiplicative, it suffices to prove it for $n = p^k$.

For $n = p^k$, the L.H.S is
$=(\tau(1))^3 + (\tau(p))^3 + (\tau(p^2))^3 + ... + (\tau(p^k))^3$
$= 1^3 + 2^3 + 3^3 + ... + (k+1)^3$
$=(\frac{(k+1)(k+2)}{2})^2$;
and the R.H.S is
$=(\tau(1)) + (\tau(p)) + (\tau(p^2)) + ... + (\tau(p^k))^2$
$= (1 + 2 + 3 + ... + (k+1))^2$
$=(\frac{(k+1)(k+2)}{2})^2$
Hence the claimed identity is established.

Problem 2

$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$.

Proof:

$\sum_{d|n} \frac{\mu^2(n)}{\phi(n)}$ is multiplicative, because $\mu^2(n) = (\mu(n))^2$ and $\phi(n)$ are multiplicative.

Therefore $\sum_{d|n} \frac{\mu^2(d)}{\phi(d)}$ is multiplicative. Also, $\frac{n}{\phi(n)}$ is multiplicative. Both sides of the claimed identity being multiplicative, it is enough to prove it when $n = p^k$.

For $n = p^k$, the L.H.S is equal to
$\frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} = 1 + \frac{1}{p-1} = \frac{p}{p-1}$
because $\mu(p^l) = 0$ for $l \geq 2$; and the R.H.S is equal to
$\frac{p^k}{p^{k-1}(p-1)} = \frac{p}{p-1}$
Hence the claim is proved.

4.3 Complete Multiplicative Functions

4.3.1 Definition

An arithmetical function f is called completely multiplicative if
(i) f is not identically zero.
(ii) $f(mn) = f(m)(n)$, for all $m, n \in \mathbf{N}$.

4.3.2 Examples of complete multiplicative function:

(1) The arithmetical function $N^\alpha(n) = n^\alpha\ \forall n \in \mathbf{N}$ is completely multiplicative.

(2) The unit function $u(n) = 1$ for all $n \in \mathbf{N}$ is completely multiplicative.

(3) The identity function is completely multiplicative.

Chapter 5

Groups under Dirichlet Composition

Problem 1

For a multiplicative function f
$\sum_{d|n}\mu(d)f(d)=\prod_{p|n}(1-f(p))$
Also
(i) $\sum_{d|n}\mu(d)\tau(d)=(-1)^{\omega(n)}$
(ii) $\sum_{d|n}\mu(d)\phi(d)=\prod_{p|n}(2-p)$
(iii) $\sum_{d|n}\mu(d)\sigma(d)=(-1)^{\omega(n)}\prod_{p|n}p$.

Proof:

Let $f(n)$ be a multiplicative function and $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$, where $p_1,p_2,...,p_r$ are distinct primes and $\alpha_i\in\mathbf{N}$ for $i=1,2,...,r$.
Then we have
$f(n)=f(n.1)=f(n)f(1)\Rightarrow f(1)=1$.
Let $F(n)=\mu(n)f(n)$.................(1)
For any prime p and $k\geq 2$, we have
$F(1)=\mu(1)f(1)=1.f(1)=f(1)=1$..............(2)
$F(p)=\mu(p)f(p)=(-1)f(p)=-f(p)$..............(3)
and $F(p^k)=\mu(p^k)f(p^k)=0$................(4)
Now since f and μ are multiplicative , so F is also multiplicative.
If $d|n$,then $d=p_1^{\delta_1}p_2^{\delta_2}...p_r^{\delta_r}$ where $0\leq\delta_i\leq\alpha_i$ for $i=1,2,...,r$.
For each value of i , the divisors of $p_i^{\alpha_i}$ are $1,p_i,p_i^2,...p_r^{\alpha_i}$.
Using $(1),(2),(3),(4)$ we get
$\sum_{d|n}\mu(d)f(d)=\sum_{d|n}F(d)=\sum_{d|n}F(p_1^{\delta_1}p_2^{\delta_2}...p_r^{\delta_r})$

$= \sum_{d|n}\{F(p_1^{\delta_1})F(p_2^{\delta_2})...F(p_r^{\delta_r})\}$
$= \{F(1)+F(p_1)+F(p_1^2)+...+F(p_1^{\alpha_1})\}\times\{F(1)+F(p_2)+F(p_2^2)+ ... + F(p_2^{\alpha_2})\} \times ... \times \{F(1) + F(p_r) + F(p_r^2) + ... + F(p_r^{\alpha_r})\}$
$= \{1 - f(p_1)\}\{1 - f(p_2)\}...\{1 - f(p_r)\}$
$= \prod_{i=1}^r (1 - f(p_i)) = \prod_{p|n}(1 - f(p))$............(5)
Hence $\sum_{d|n} \mu(d)f(d) = \prod_{i=1}^r (1 - f(p_i)) = \prod_{p|n}(1 - f(p))$.

(i)

Since $\tau(n)$ is multiplicative, so putting $f(d) = \tau(d)$ in (5), we get
$\sum_{d|n} \mu(d)\tau(d) = \prod_i^r = 1(1-\tau(p_1)) = \{1-\tau(p_i)\}\{1-\tau(p_2)\}...\{1-\tau(p_r)\}$
$= (1 - 2)(1 - 2)...(1 - 2)$
$= (-1)(-1)...(-1) = (-1)^r = (-1)^{\omega(n)}$.

(ii)

Since $\phi(n)$ is multiplicative, so putting $f(d) = \phi(d)$ in (5), we get,
$\sum_{d|n} \mu(d)\phi(d) = \prod_{i=1}^r (1 - \phi(p_i)) = \{1 - \phi(p_1)\}\{1 - \phi(p_2)\}...\{1 - \phi(p_r)\}$
$= \{1 - (p_1 - 1)\}\{1 - (p_2 - 1)\}...\{1 - (p_r - 1)\}$
$= (2 - p_1)(2 - p_2)...(2 - p_r) = \prod_{i=1}^r (2 - p_i) = \prod_{p|n}(2 - p)$
Hence $\sum_{d|n} \mu(d)\phi(d) = \prod_{i=1}^r (2 - p_i) = \prod_{p|n}(2 - p)$.

(iii)

Since $\sigma(n)$ is multiplicative, so putting $f(d) = \sigma(d)$ in (5), we get
$\sum_{d|n} \mu(d)\sigma(d) = \prod_{i=1}^r (1 - \sigma(p_i)) = \{1 - \sigma(p_1)\}\{1 - \sigma(p_2)\}...\{1 - \sigma(p_r)\}$
$= \{1 - (1 + p_1)\}\{1 - (1 + p_2)\}...\{1 - (1 + p_r)\}$
$= (-p_1)(-p_2)...(-p_r) = (-1)^r p_1p_2...p_r = (-1)^r \prod_{p|n} p$.
Hence $\sum_{d|n} \mu(d)\sigma(d) = (-1)^{\omega(n)} \prod_{p|n} p$.

Problem 2

If f is multiplicative and $f(n)$ is never zero, then
$\sum_{d|n} \frac{\mu(d)}{f(d)} = \prod_{p|n}(1 - \frac{1}{f(p)})$.
Also expressions for $\sum_{d|n} \frac{\mu(d)}{\tau(d)}, \sum_{d|n} \frac{\mu(d)}{\phi(d)}, \sum_{d|n} \frac{\mu(d)}{\sigma(d)}$.

Proof:

Here $f(n)$ is given to be multiplicative and $\mu(n)$ is multiplicative , so $\sum_{d|n} \frac{\mu(d)}{f(d)}$ is also multiplicative.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ where $p_1, p_2, ..., p_r$ are distinct primes and $\alpha_i \in \mathbf{N}$ for $i = 1, 2, ...r$. Then we have

$f(n) = f(n.1) = f(n)f(1) \Rightarrow f(1) = 1$.

Let $F(n) = \frac{\mu(n)}{f(n)}$.

Now for any prime p and $k \geq 2$, we have

$F(1) = \frac{\mu(1)}{f(1)} = \frac{1}{1} = 1$

$F(p) = \frac{\mu(p)}{f(p)} = \frac{-1}{f(p)}$

and $F(p^k) = \frac{\mu(p^k)}{f(p^k)} = 0$.

Using $(1), (2), (3)$ and (4), we get

$\sum_{d|n} \frac{\mu(d)}{f(d)} = \sum_{d|n} F(d) = \{F(1) + F(p_1) + F(p_1^2) + ... + F(p_1^{\alpha_1})\} \times \{F(1) + F(p_2) + F(p_2^2) + ... + F(p_2^{\alpha_2})\} \times \{F(1) + F(p_r) + F(p_r^2) + ... + F(p_r^{\alpha_r})\}$

$= \{1 - \frac{1}{f(p_1)}\}\{1 - \frac{1}{f(p_2)}\}...\{1 - \frac{1}{f(p_r)}\} = \prod_{i=1}^{r}\{1 - \frac{1}{f(p_i)}\}$

$\Rightarrow \sum_{d|n} \frac{\mu(d)}{f(d)} = \prod_{i=1}^{r}\{1 - \frac{1}{f(p_i)}\} = \prod_{p|n}(1 - \frac{1}{f(p)})$.

Hence $\sum_{d|n} \frac{\mu(d)}{f(d)} = \prod_{p|n}(1 - \frac{1}{f(p)})$.

(i)

Since $\tau(n)$ is multiplicative and $\tau(n) \neq 0 \ \forall n \in \mathbf{N}$, so putting $f(d) = \tau(d)$ in (5) and using $\tau(p) = 1 + 1 = 2$, we get

$\sum_{d|n} \frac{\mu(d)}{\tau(d)} = \prod_{i=1}^{r}\{1 - \frac{1}{\tau(p_i)}\} = \{1 - \frac{1}{\tau(p_1)}\}\{1 - \frac{1}{\tau(p_2)}\}...\{1 - \frac{1}{\tau(p_r)}\}$

$= (1 - \frac{1}{2})(1 - \frac{1}{2})...(1 - \frac{1}{2}) = \frac{1}{2}.\frac{1}{2}...\frac{1}{2}$

$= \frac{1}{2^r} = 2^{-r} = 2^{-\omega(n)}$

where $\omega(n)$ is the number of distinct prime factors of n.

(ii)

Since $\phi(n)$ is multiplicative and $\phi(n) \neq 0 \ \forall n \in \mathbf{N}$, so putting $f(d) = \phi(d)$ in (5) and using $\phi(p) = p - 1$, we get

$\sum_{d|n} \frac{\mu(d)}{\phi(d)} = \prod_{i=1}^{r}\{1 - \frac{1}{\phi(p_i)}\} = \{1 - \frac{1}{\phi(p_1)}\}\{1 - \frac{1}{\phi(p_2)}\}...\{1 - \frac{1}{\phi(p_r)}\}$

$= (1 - \frac{1}{p_1-1})(1 - \frac{1}{p_2-1})...(1 - \frac{1}{p_r-1})$

$= (\frac{p_1-2}{p_1-1}).(\frac{p_1-2}{p_1-1})...(\frac{p_1-2}{p_1-1}) = \prod_{i=1}^{r}(\frac{p_i-2}{p_i-1})$

Hence $\sum_{d|n} \frac{\mu(d)}{\phi(d)} = \prod_{p|n}(\frac{p-2}{p-1})$.

(iii)

Since $\sigma(n)$ is multiplicative and $\sigma(n) \neq 0 \; \forall n \in \mathbf{N}$, so putting $f(d) = \sigma(d)$ in (5) and using $\sigma(p) = p + 1$, we get

$\sum_{d|n} \frac{\mu(d)}{\sigma(d)} = \prod_{i=1}^{r}\{1 - \frac{1}{\sigma(p_i)}\} = \{1 - \frac{1}{\sigma(p_1)}\}\{1 - \frac{1}{\sigma(p_2)}\}...\{1 - \frac{1}{\sigma(p_r)}\}$

$= (1 - \frac{1}{p_1+1})(1 - \frac{1}{p_2+1})...(1 - \frac{1}{p_r+1})$

$= (\frac{p_1}{p_1+1}).(\frac{p_1}{p_1+1})...(\frac{p_r}{p_r+1})$

$= \prod_{i=1}^{r}(\frac{p_i}{p_i+1}) = \prod_{p|n}(\frac{p}{p+1})$.

Hence $\sum_{d|n} \frac{\mu(d)}{\sigma(d)} = \prod_{p|n}(\frac{p}{p+1})$.

Problem 3

f is called completely multiplicative if $f(mn) = f(m)(n)$ holds for all $m, n \in \mathbf{N}$. For a completely multiplicative function f

(i) $f(g * h) = (fg) * (fh)$

(ii) μf is the Dirichlet inverse of f.

Proof:

(i) If f is completely multiplicative, we will show that f distributes multiplication over Dirichlet composition. Let n be a positive integer, then

$f(g * h)(n) = f(n)(g * h)(n)$

$= f(n) \sum_{d|n} g(d)h(\frac{n}{d})$

$= \sum_{d|n} f(d)g(d)f(\frac{n}{d})g(\frac{n}{d})$

$= (fg * fh)(n)$

So we have,

$f(g * h) = (fg) * (fh)$

Then (i) is proved.

(ii) If f is completely multiplicative and let n be a positive integer then

$(\mu f * f)(n) = \sum_{d|n}(\mu f)(d)f(\frac{n}{d})$

$= \sum_{d|n} \mu(d)f(d)f(\frac{n}{d})$

$f(n) \sum_{d|n} \mu(d) = f(n)\iota(n) = \begin{cases} f(1) = 1 & \text{when } n = 1 \\ 0 & \text{when } n > 1 \end{cases} = \iota(n)$

therefore $\mu f * f = \iota$ which implies that $f^{-1} = \mu f$.
So, μf is the Dirichlet inverse of f.
Then (ii) is proved.

Problem 4

The set of all arithmetical functions which satisfy the condition $f(1) \neq 0$ forms an(infinite) abelian group under Dirichlet composition, whose identity element is the function ι .

Proof:

Let S=$\{f(n) : \forall n \in \mathbf{N}$ and $f(1) \neq 0\}$. Then $\forall f, g \in S$, the Dirichlet product(composition) is defined by
$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

1. Closure Property: Let $f, g \in S$. Then $f(1) \neq 0$ and $g(1) \neq 0$. Also $f * g$ is an arithmetical function.
Now $(f * g)(1) = f(1)g(1) \neq 0$.
Hence $f * g \in S$.
Also $\forall$ $f, g \in S$, $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) \in S$.
So, $f * g \in S$ is also an arithmetical function.

2. Commutative Property: Let $f, g \in S$ and $n \in \mathbf{N}$
$(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$
$= \sum_{d_1 d_2 = n} g(d_2)f(d_1)$
$= (g * f)(n)$

3. Associative Property: Let $f, g, h \in S$ and $n \in \mathbf{N}$
$((f * g) * h)(n) = \sum_{dd_3 = n}(f * g)(d)h(d_3)$
$= \sum_{dd_3 = n}(\sum_{d_1 d_2 = d} f(d_1)g(d_2))h(d_3))$
$= \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)$
$= \sum_{d_1 d = n} f(d_1)(\sum_{d_2 d_3 = d} g(d_2)h(d_3))$
$= \sum_{d_1 d = n} f(d_1)(g * h)(d)$
$= (f * (g * h))(n)$

4. Identity element: Let $n \in \mathbf{N}$ and

ι(n)= $\begin{cases} 1 & \text{when } n = 1 \\ 0 & \text{when } n > 1 \end{cases}$

$(\iota * f)(n) = \sum_{d|n}(\iota(d)f(\frac{n}{d})$
$= \iota(1)f(n) + \sum_{d|n,d>1} \iota(d)f(\frac{n}{d})$
$= 1.f(n) + 0$
$= f(n)$
Similarly, $(f * i)(n) = f(n)$, $\forall f(n) \in S$.

5. Existence of inverse element: Let $f, h \in S$ and $n \in \mathbf{N}$

$(f * h)(1) = (h * f)(1) = \iota(1)$
$\Rightarrow \sum_{d|l} f(d)h(\frac{l}{d}) = 1$
$\Rightarrow f(1)h(1) = 1$
$\Rightarrow h(1) = \frac{1}{f(1)} = f^{-1}(1)$
$\Rightarrow h(1)$ is the unique inverse of $f(1)$.

Now let $n > 1$ and we suppose that $h(m) = f^{-1}(m)$ has been uniquely determined for every $m < n$. Then

$(f * h)(n) = (h * f)(n) = \iota(n)$
$\Rightarrow \sum_{d|n,1 \leq d \leq n} h(d)f(\frac{n}{d}) = 0$
$\Rightarrow h(n)f(\frac{n}{n}) + \sum_{d|n,1 \leq d \leq n} h(d)f(\frac{n}{d}) = 0$
$\Rightarrow h(n)f(1) = -\sum_{d|n,1 \leq d \leq n} h(d)f(\frac{n}{d})$
$\Rightarrow h(n) = -\frac{1}{f(1)} \sum_{d|n,1 \leq d \leq n} h(d)f(\frac{n}{d})$
Hence h is an arithmetical function if $f(1) \neq 0$, where
$f * h = h * f = \iota$, the identity function.

Hence S is an infinite abelian group under Dirichlet composition for arithmetical functions.

Chapter 6

Rings under Pointwise Addition and Dirichlet Composition

Problem 1

The set of all arithmetical functions forms a commutative ring (with zero divisors) under the operations of pointwise addition and Dirichlet composition.

Proof:

Let S=$\{f(n) : \forall n \in \mathbf{N}$ and $f(1) = 0\}$. Then $\forall f, g \in S$, the pointwise addition and Dirichlet composition (product) is defined by,

$(f + g)(n) = f(n) + g(n)$

$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

First let us show that, f together with Dirichlet product forms an abelian monoid.

• **Closure property of addition:** Let $f, g \in S$. Then $f(1) = 0$ and $g(1) = 0$. Also $f + g$ is an arithmetical function.

Now $(f + g)(n) = f(n) + g(n) \in S$ since $f(n)$ and $g(n)$ both $\in S$.

Hence closure property for addition satisfies.

• **Associative property of addition:** Let $f, g, h \in S$ and $n \in \mathbf{N}$

$((f + g) + h)(n) = (f + g)(n) + h(n)$

$= (f(n) + g(n)) + h(n)$
$= f(n) + g(n) + h(n)$.............(1)
Again, $(f + (g + h))(n) = f(n) + (g + h)(n)$
$= f(n) + (g(n) + h(n))$
$= f(n) + g(n) + h(n)$............(2)
From (1) and (2) we can write,
$((f + g) + h)(n) = (f + (g + h))(n)$

• **Existence of additive identity :** $0(n) = 0$ for every $n \in \mathbf{N}$ if $f \in S$ and $n \in \mathbf{N}$ then
$(f + 0)(n) = f(n) + 0(n)$
$= f(n) + 0$
$= f(n), \forall f(n) \in S.$

• **Existence of additive inverse:** $(-f)(n) = -f(n)$ for any $n \in \mathbf{N}$ we have
$(f + (-f))(n) = f(n) + (-f)(n)$
$= f(n) + (-f(n))$
$= 0$
$= 0(n)$

• **Commutative law of addition:** Let $f, g \in S$ and $n \in \mathbf{N}$
$(f + g)(n) = f(n) + g(n)$
$= g(n) + f(n)$
$= (g + f)(n)$

• **Closure property of multiplication:** Let $f, g \in S$. Then $f(1) = 0$ and $g(1) = 0$. Also $f * g$ is an arithmetical function.
Now $(f * g)(1) = f(1).g(1) = 0.0 = 0$.
Hence $f * g \in S$.

- **Associative law of multiplication:** Let $f, g, h \in S$ and $n \in \mathbf{N}$
$((f*g)*h)(n) = \sum_{dd_3=n}(f*g)(d)h(d_3)$ $[d_3 = \frac{n}{d}]$
$= \sum_{dd_3=n}(\sum_{d_1d_2=d} f(d_1)g(d_2))h(d_3))$
$= \sum_{d_1d_2d_3=n} f(d_1)g(d_2)h(d_3)$
$= \sum_{d_1d=n} f(d_1)(\sum_{d_2d_3=d} g(d_2)h(d_3))$
$= \sum_{d_1d=n} f(d_1)(g*h)(d)$
$= (f*(g*h))(n)$

- **Distributive law of multiplication:** Now let us show that Dirichlet convolution distributes over addition in S. Let f, g, h be arithmetic functions and $n \in \mathbf{N}$
(i) Left Distributive:
$(f*(g+h))(n) = \sum_{d|n} f(d)(g+h)(\frac{n}{d})$
$= \sum_{d|n} f(d)(g(\frac{n}{d}) + h(\frac{n}{d}))$
$= \sum_{d|n}(f(d)g(\frac{n}{d}) + f(d)h(\frac{n}{d}))$
$= \sum_{d|n} f(d)g(\frac{n}{d}) + \sum_{d|n} f(d)h(\frac{n}{d})$
$= (f*g)(n) + (f*h)(n)$
(ii) Right Distributive: $((f+g)*h)(n) = \sum_{d|n}(f+g)(d)h(\frac{n}{d})$
$= \sum d|n(f(d) + g(d))h(\frac{n}{d})$
$= \sum_{d|n}(f(d)h(\frac{n}{d}) + g(d)h(\frac{n}{d}))$
$= \sum_{d|n} f(d)h(\frac{n}{d}) + \sum_{d|n} g(d)h(\frac{n}{d})$
$= (f*h)(n) + (g*h)(n)$
Hence the set of all arithmetical functions forms a commutative ring.

Problem 2

The set of all arithmetical functions with $f(1) = 0$ is not an integral domain under the operations of pointwise addition and Dirichlet composition.

Proof:

Let S=$\{f(n) : \forall n \in \mathbf{N}$ and $f(1) = 0\}$. Then $\forall f, g \in S$, the pointwise addition and Dirichlet composition (product) is defined by,
$(f+g)(n) = f(n) + g(n)$
$(f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

For a function to be an integral domain it has to satisfy the three following properties:

(i) S has to be a commutative ring.

(ii) S has to be a ring with unity.

(iii) S has to be a ring without zero divisors.

• **Closure property of addition:** Let $f, g \in S$. Then $f(1) = 0$ and $g(1) = 0$. Also $f + g$ is an arithmetical function.

Now $(f+g)(n) = f(n)+g(n) \in S$ since $f(n)$ and $g(n)$ both $\in S$.

Hence closure property for addition satisfies.

• **Associative property of addition:** Let $f, g, h \in S$ and $n \in \mathbf{N}$

$((f+g)+h)(n) = (f+g)(n) + h(n)$

$= (f(n) + g(n)) + h(n)$

$= f(n) + g(n) + h(n)$.............(1)

Again, $(f + (g+h))(n) = f(n) + (g+h)(n)$

$= f(n) + (g(n) + h(n))$

$= f(n) + g(n) + h(n)$............(2)

From (1) and (2) we can write,

$((f+g)+h)(n) = (f + (g+h))(n)$

• **Existence of additive identity :** $0(n) = 0$ for every $n \in \mathbf{N}$ if $f \in S$ and $n \in \mathbf{N}$ then

$(f+0)(n) = f(n) + 0(n)$

$= f(n) + 0$

$= f(n), \forall f(n) \in S.$

• **Existence of additive inverse:** $(-f)(n) = -f(n)$ for any $n \in \mathbf{N}$ we have

$(f + (-f))(n) = f(n) + (-f)(n)$

$= f(n) + (-f(n))$

$= 0$

$= 0(n)$

- **Commutative law of addition:** Let $f, g \in S$ and $n \in \mathbf{N}$
  $(f+g)(n) = f(n) + g(n)$
  $= g(n) + f(n)$
  $= (g+f)(n)$

- **Closure property of multiplication:** Let $f, g \in S$. Then $f(1) = 0$ and $g(1) = 0$. Also $f * g$ is an arithmetical function.
  Now $(f * g)(n) = f(d)g(\frac{n}{d})$ is also $\in S$ since $f(d)$ and $g(\frac{n}{d})$ both are arithmetical functions.
  Hence closure property for multiplication satisfies.

- **Associative law of multiplication:** Let $f, g, h \in S$ and $n \in \mathbf{N}$
  $((f * g) * h)(n) = \sum_{dd_3=n}(f * g)(d)h(d_3)$ $[d_3 = \frac{n}{d}]$
  $= \sum_{dd_3=n}(\sum_{d_1d_2=d} f(d_1)g(d_2))h(d_3))$
  $= \sum_{d_1d_2d_3=n} f(d_1)g(d_2)h(d_3)$
  $= \sum_{d_1d=n} f(d_1)(\sum_{d_2d_3=d} g(d_2)h(d_3))$
  $= \sum_{d_1d=n} f(d_1)(g * h)(d)$
  $= (f * (g * h))(n)$

- **Distributive law of multiplication:** Now let us show that Dirichlet convolution distributes over addition in S. Let f, g, h be arithmetic functions and $n \in \mathbf{N}$
  Left Distributive:
  $(f * (g+h))(n) = \sum_{d|n} f(d)(g+h)(\frac{n}{d})$
  $= \sum_{d|n} f(d)(g(\frac{n}{d}) + h(\frac{n}{d}))$
  $= \sum_{d|n}(f(d)g(\frac{n}{d}) + f(d)h(\frac{n}{d}))$
  $= \sum_{d|n} f(d)g(\frac{n}{d}) + \sum_{d|n} f(d)h(\frac{n}{d})$
  $= (f * g)(n) + (f * h)(n)$
  Right Distributive: $((f+g) * h)(n) = \sum_{d|n}(f+g)(d)h(\frac{n}{d})$
  $= \sum_{d|n}(f(d) + g(d))h(\frac{n}{d})$
  $= \sum_{d|n}(f(d)h(\frac{n}{d}) + g(d)h(\frac{n}{d}))$
  $= \sum_{d|n} f(d)h(\frac{n}{d}) + \sum_{d|n} g(d)h(\frac{n}{d})$
  $= (f * h)(n) + (g * h)(n)$

Hence the set of all arithmetical functions with $f(1) = 0$ forms a commutative ring.

(ii) Now we will check if S is ring with unity. Let $n \in \mathbf{N}$ and

ι(n)= $\begin{cases} 1 & \text{when } n = 1 \\ 0 & \text{when } n > 1 \end{cases}$

$(\iota * f)(n) = \sum_{d|n}(\iota(d)f(\frac{n}{d})$

$= \iota(1)f(n) + \sum_{d|n,d>1} \iota(d)f(\frac{n}{d})$

$= 1.f(n) + 0$

$= f(n)$

Similarly, $(f * \iota)(n) = f(n)$, $\forall f(n) \in S$.

(iii) At last we will check if S is a ring without zero divisors.

Let $f, g \in S$ such that $f = 0$ and $g = 0$. Then there exists $m, n \in \mathbf{N}$ such that $f(n) = 0$ and $f(m) = 0$. Now,

$(f * g)(mn) = \sum_{d|nm} f(d)g(\frac{nm}{d})$

$= \sum_{d|nm,d<n} f(d)g(\frac{nm}{d}) + f(n)g(m) + \sum_{d|nm,d>n} f(d)g(\frac{nm}{d}) = f(n)g(m) = 0.0 = 0.$

Since $d < n$ implies that $f(d) = 0$ and $d > n$ implies that $\frac{nm}{d} < m$ which indicates $g(\frac{nm}{d}) = 0$.

Therefore it follows that $f * g = 0$ and S has zero divisors.

Which doesn't satisfy the property of integral domain.

Hence S is not an integral domain.

Index