MTS 211 ABSTRACT ALGEBRA

LECTURE NOTE 2 FOR 2011/2012 FIRST SEMESTER

1.0 ALGEBRAIC STRUCTURE

Let A be a non-empty set, a binary operation on A is a function $*$ such that $A * A \rightarrow A$. That is ,$*$ is A rule by which every pair of elements $x, y \epsilon A$ yield a third element z in A, viz $x * y = z$. Such a set is said to be closed under $*$.

EXAMPLE 1.1.0

The usual arithmetic operations +, - ,x ,÷ are binary operations on the Real set. Similarly, the operations $\cup, \cap, \Delta$ are binary operations on the power set P(A) .

By an algebraic structure (or algebraic system) we mean a non-empty set S, equipped with one or more binary operations. We denote an algebraic structure consisting of set S and a binary operation $*$ by the ordered pair (S, $*$). Similarly, an algebraic system consisting of set S and two operations $*$ and o shall be denoted by the ordered triple (S, $*$, o).

EXAMPLE: 1.1.1

($\mathbb{N}$, +), ($\mathbb{I}$, +), ($\mathbb{Q}$, .), ($\mathbb{R}$, +, .) ($\mathbb{C}$, +, .) (p(X), $\cup$) and (P (x), $\cup$, $\cap$) are all algebraic systems.

For any binary operation * defined on a set S,

1. If x * y = y * x for all x,y $\in$ X, then * is said to be communicative.

2. If x * (y*z) = (x*y)*z for all x,y,z $\in$ S then * is said to be associative.

3. If there is an element e $\in$ S such that e*x = x*e = x for all x $\in$ S then e is called the identity element (or unity element) of S. In particular e*e = e. e.g. 0 and 1 are the identity elements of IR with respect to + and . operations respectively since for any x $\in$ IR, x + 0 = 0 + x = x, x.1 = 1.x = x.

4. if there is an element y $\in$ S such that x*y = y*x = e for x $\in$ S**,** then y is called the inverse of x in S w.r.t*, where e is the identity element of S.

5. If * and o are operations defined on S we say that o is left distributive over * if

$x \circ (y*z) = x \circ y * x \circ z$ for all $x,y,z \in S$

and o is right distributive over * if

$(x*y) \circ z = x \circ z * y \circ z$ for all $x,y,z \in S$.

If o is both left and right distributive over * we simply say o is distributive over *.

1.2 THE STRUCTURE OF GROUPS

1.2.1 DEFINITION AND EXAMPLES OF GROUPS

An algebraic structure (G,*) is called a group if it satisfies the following properties

1. * is closed in G
2. * is associative
3. the identity element exists
4. the inverse of each element of G exists.

A system satisfying only properties 1 and 2 is called a semi group.

A semi-group in which the identity element exists is called a monoid.

Now, if in addition to properties 1 – 4, we also have

5. * is commutative, then (G, *) is called an abelian or commutative group.

EXAMPLE 1.2.1.0

It can easily be verified that $(\mathbb{I}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ and $(\mathbb{R}^*, .)$ are all abelian groups. $(\mathbb{N}, +)$ is not a group since it has no inverse for its elements.

EXAMPLE 1.2.1.1

Let G = { $f_1, f_2, \ldots, F_6$} and $x \in R - \{0.1\}$ where $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$

$f_4(x) = \frac{x-1}{x}$, $f_5(x) = \frac{x}{x-1}$, $f_6(x) = \frac{1}{1-x}$

If we define the binary operation o to be that of functional composition, then (G,o) is a non-abelian group as can be deduced from the composition table below.

0	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_4	f_1	f_2	f_3

(G, 0) is not abelian since for example

$(f_2 \text{ o } f_6)\, x = f_2\,(f_6(x)) = f_2\left(\frac{1}{1-x}\right) = \frac{1}{1/(1-x)} = 1 - x = f_3(x)$

But $(f_6 \text{ o } f_2)(x) = f_6(f_2(x) = f_6\left(\frac{1}{x}\right) = \frac{1}{1-\frac{1}{x}} = \frac{1}{x-1} = f_5(x)$

Which implies $f_2 \text{ o } f_6 \neq f_6 \text{ o } f_2$

EXAMPLE 1.2.1.2

If we define addition modulo n (i.e. $+_n$) on the set $\mathbb{I}_n$ as $\bar{a} + \bar{b} = \overline{b + a} = \bar{c}$ for all $a,b \in \mathbb{I}_n$

Then $(\mathbb{I}_n, +_n)$ forms a group called the group of residue classes modulo n.

Similarly, it can be shown that the set of residues (or representatives) { 0,1,2,…,n-1} under addition modulo n defined by $a +_n b = c$ for all a,b in the set (where c is the remainder when a + b is divided by n) is also a group. It is called the "group of integers modulo n."

1.2.2 ELEMENTARY PROPERTIES OF A GROUP

For any group (G, *) the following properties are satisfied:

1. The identity element of the group is unique

2. Each element in the group has a unique inverse

3. The inverse of the inverse of an element is the element itself i.e. if a ϵG, then $(a^{-1})^{-1} = a$

4. If a,b ϵ G then $(ab)^{-1} = b^{-1}a^{-1}$. This is called the reversal law.

5. If a,b,c are elements of a group (G, *) then the cancellation laws hold. That is

   i. a*c = b*c implies a = b (Right cancellation law)

   ii. c*a = c*b implies a = b (Left cancellation law)

6. If a,b ϵ G, then there exists unique elements x and y in G such that ax = b and ya =b have unique solutions in (G, *).

1.2.3 FINITE AND INFINITE GROUPS

If a group consists of a finite number of elements, it is called a finite group, otherwise the group is infinite. E.g. (G, .) in example 1.2.1.1 is finite while ($\mathbb{I}$, +) is infinite.

1.2.4 ORDER OF A GROUP AND OF ITS ELEMENTS

If a group (G, .) is finite, the number of elements in the group is called the order of the group denoted |G| or o(G).

If x is an element of (G, o) finite or infinite then the order of x is the least positive integer n such that $x^n = e$. e.g. the order of the group $(\{1,a,a^2,\ldots,a^5\},.)$

1.3 SUBGROUPS AND COSETS

A non-empty subset H of a group (G, .) is called a subgroup of (G, o) if (H, o) is itself a group. We call H a complex.

EXAMPLE 1.3.0

($\mathbb{I}$, +) is a subgroup of ($\mathbb{Q}$, +) and ($\mathbb{Q}$, +) is a subgroup of ($\mathbb{R}$, +).

Obviously, any group (G, *) has at least two subgroups viz (G, *) and ({e}, *) where e is the identity element in G. These two subgroups are called trivial subgroups of (G,*). Any other subgroup of (G,*) is non-trivial.

Also, the intersection of two subgroups of (G,*) is also a subgroup. However if (H_1, *) and (H_2, *) are subgroups of (G,*) then ($H_1 U H_2$,*) is a subgroup of (G,*) iff $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. Also if (H_1, *) is an arbitrary indexed collection of subgroups of (G, *) then ($\cap H_1$, *) is also a subgroup.

THEOREM 1.3

The necessary and sufficient conditions that a complex H is a subgroup of a group (G, *) are:

(i) $H \neq \emptyset$

(ii) for every a,b in H, ab^{-1} is also in H.

1.3.1 CENTRE OF A SUBGROUP

The centre of a subgroup (G,*) denoted c(G) is the subset of G containing those elements which commute with all elements of G i.e. $c(G) = \{x \in G: xg = gx \text{ for all } g \in G\}$.

1.3.2 COSETS OF A SUBGROUP

If (G, *) is a group and (H, *) is its subgroup, then the collection

$H*a = \{ h*a: a \in G, h \in H\}$ is called the right Coset of H in G, and

$a*H = \{a*h: a \in G, h \in H\}$ is called the left Coset of H in G.

If e is the identity element in (G, *), then since He = eH, H is itself a Coset.

For any Cosets aH and bH where $a,b \in G$

$aH = bH$ iff $a \in bH$. If $a \notin bH$ then $aH \neq bH$.

Hence, two left (or right) Cosets are either identical or disjoint; and so the left (or right) Cosets of a subgroup H of G forms a partition of G.

The number of left (or right) Cosets of H in G is called the index of H in G, denoted (G:H).

EXAMPLE 1.3.2.1

Find the Cosets of the additive subgroup ($2\mathbb{I}$, +) of the additive group ($\mathbb{I}$, +).

Solution:

The set $\mathbb{I} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$

$2\mathbb{I} = \{\ldots, -6, -4, -2, 0, 2, 4, \ldots\}$

If $a \epsilon \mathbb{I}$, then the Cosets of $2\mathbb{I}$ in $\mathbb{I}$ corresponding to a is $2\mathbb{I} + a$. Since the group is abelian $\mathbb{I} + a = a + \mathbb{I}$, therefore

$2\mathbb{I} + 0 = \{\{\ldots, -6, -4, -2, 0, 2, 4, \ldots\}$

$= 2\mathbb{I} = 2\mathbb{I} + 2 = 2\mathbb{I} + 4 \ldots$ etc.

$2\mathbb{I} + 1 = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$

$= 2\mathbb{I} + 3 = 2\mathbb{I} + 5 = \ldots$ etc

Hence the distinct Cosets of ($2\mathbb{I}$, +) in ($\mathbb{I}$, +) are $2\mathbb{I}$ and $2\mathbb{I} + 1$; obviously $\mathbb{I} = 2\mathbb{I} \cup (2\mathbb{I} + 1)$

THEOREM 1.3.1

The order of every subgroup (H, *) of a finite group (G, *) is a divisor of the order of the group.

PROOF 1.3

Suppose the order of (G, *) is n and the order of the subgroyup (H, *) is m, then by considering the set of all right cosets of H in G where $H = \{ h_1, h_2, \ldots, h_m\}$, since G is finite, the number of right cosets of H in G is finite. Let the number of (distinct) right cosets be k.

Since the right cosets form a partition of G, the number of elements in G (i.e. n) will be equal to the number of elements in all the k right cosets having m elements each. Therefore,

$N = m.k \Longrightarrow k = {}^{n}/_{m}$

1.3.3 NORMAL SUBGROUP

If (H, *) is a subgroup of (G, *) we say H is normal in G denoted H Δ G if for all g ϵ G, gHg^{-1} = H.

From this definition we can verify that the subgroup of every abelian group is normal. Also, H is normal (invariant) if every left cosets of H is also a right coset of H in G. subgroup H, we can easily talk of cosets of H in G without specifying whether right or left.

The trivial subgroups are obviously normal, and so any group having no normal subgroup except the trivial ones is called a simple group.

EXAMPLE 1.3.3.1

If in example 1.2.1.1, we define a subset H = $\{f_1,f_4,f_6\}$ then (H, o) is a normal subgroup of (G,o) since f_k oH = $\{f_1,f_4,f_6\}$ = Hof_k for Thus in a normal

k = 1,4,6.

Similarly, the subgroup (2$\mathbb{I}$, +) Δ ($\mathbb{I}$, +), and the subgroup (R, +) Δ ($\mathbb{C}$, +).

1.3.4 FACTORS OF QUOTIENT GROUP

If (H, *) is a normal subgroup of (G, *) and we define multiplication of cosets as:

$$H_a \circledast H_b = Ha \circledast b$$

then the set of all cosets of H denoted G/H forms a group under this composition, and is called the factor group (or quotient group) relative to H, viz (G/H, $\circledast$).

Similarly, if we define addition of cosets as $H_a + H_b = H_{a+b}$ then (G/H, +) is quotient group.

EXAMPLE 1.3.4.1

The set of cosets R/ $\mathbb{I}$ is a quotient group w.r.t. multiplication.

1.4 GROUP HOMOMORPHISMS

A mapping f:G $\longrightarrow$ $G^{!}$ from a group (G, $\circledast$) into another group ($G^{!}$, *) is called a homomorphism if for all x,y ϵG.

$$F(x \circledast y) = f(x)*f(y)$$

where $\circledast$ and * are the binary operations in G and $G^{!}$ respectively.

Thus, we see that homomorphism is an operation preserving mapping.

EXAMPLE 1.4.1

Let $(R^{+},^{*})$ be the group of all positive real numbers under multiplication and let (R, +) be the group of all real numbers under addition.

If we define f: $R^{+} \longrightarrow$ R by

$$f(x) = \log_{10}{}^{x}$$

then f is a homomorphism since for any x,yϵ R^{+}

$$f(x,y) = \log (x,y)$$

$$= \log (x) + \log (y) = f(x) + f(y)$$

EXAMPLE 1.4.2

Suppose G is a group and N Δ G and we define the mapping f: G $\longrightarrow$ G/N by

$$f(g) = N_g \text{ for all } g\epsilon G$$

then f is a homomorphism of G onto G/N since

$$f(g_1.g_2) = N(g_1.g_2) \text{ for } g_1,g_2\epsilon G$$

$$= Ng_1\ Ng_2 = f(g_1)f(g_2).$$

1.4.1 KERNEL OF HOMOMORPHISM

If f is a homomorphism of G into $G^!$ then Kernel of f (denoted Ker. (f)) is a subset of G containing those elements which are mapped by f to the identity element of $G^!$. i.e. Ker = $\{g \epsilon G: f(g) = e^!$ where $e^!$ is the identity element of $G^!\}$

1.4.2 ISOMORPHISM AND OTHER HOMOMORPHISMS

A homomorphism $f:G \longrightarrow G^!$ is called an epimorphism if f is onto i.e. if $f(G) = G^!$

If $f: G \longrightarrow G^!$ is one-to-one then f is called a monomorphism.

A homomophism $f: G \longrightarrow G^!$ is called an isomorphism if f is one-to-one and onto, thus we say G is isomorphic (denoted $\cong$) to $G^!$.

A homomorphism $f: G \longrightarrow G$ (i.e. G into itself) is called an endomorphism.

If $f: G \longrightarrow G$ is isomorphic and onto then f is called an automorphism.

EXAMPLE 1.4.2.1

Let $f: \mathbb{I} \longrightarrow \mathbb{R} - \{o\}$ defined by

$$F(n) = \begin{cases} 1 \; if \; n \; is \; an \; even \; integer \\ -1 \; if \; n \; is \; an \; odd \; integer \end{cases}$$

Then f is clearly a homomorphism, and

Ker.(f) = $\{n \epsilon \mathbb{I} : f(n) = 1\} = \mathbb{I}_e$ (even integers) while the direct image $f(\mathbb{I}) = \{1, -1\}$

REMARKS

If $f:G \longrightarrow G^!$ is a homomorphism with kernel K then k ΔG. Also if e and $e^!$ are the identity elements of G and $G^!$ then

(i) $f(e) = e^!$

(ii) $f(a^{-1}) = [f(a)]^{-1}$ for all a ϵ G

(iii) if the order of a ϵG is finite and divides the order of a.

THEOREM 1.4.2.1 (Fundamental Homomorphism)

If f: G $\longrightarrow$H is a homomorphism of group G into group H then:

i. The Ker. (f) = N is a normal subgroup of G

ii. the mapping $\emptyset$: f(G) $\longrightarrow$G/N defined by $\emptyset$ (f(g)) = N_g is an isomorphism.

PROOF

We first show that N (i.e. Ker (f)) is a normal subgroup of G. N $\neq \emptyset$ since it contains e the identity of G. Let $n_1, n_2 \epsilon N$, then

$f(n_1) = f(n_2) = e^!$

Also since f is a homomorphism

$f(n_1 n_2^{-1}) = f(n_1)f(n_2^{-1}) = f(n_1)\,[f(n_2)]^{-1}$

$= e^1 e^{-1} = e^1$

$\Longrightarrow n_1 n_2^{-1} \epsilon N$. Hence N is a subgroup.

Now take $n \epsilon N$, and any $g \epsilon G$, then

$f(gng^{-1}) = f(g)\, f(n)\, f(g^{-1})$

$= f(g)\, e^!\, [f(g)]^{-1}$

$= f(g)\, [f(g)]^{-1} = e^{-!}$

$\Longrightarrow gng^{-1} \epsilon N$, thus N Δ G

Now the homomorphism f induces map $\emptyset$ on G/N.

Next, we prove that $\emptyset$: f(G) $\longrightarrow$ G/N is a mapping.

It is conceivable that for $g_1 \neq g_2$

$F(g_1) = f(g_2)$. Thus, consider

$f(g_1 g_2^{-1}) = f(g_1)\, f(g_2^{-1})$

$= f(g_1)\,[f(g_2)]^{-1}$

$= f(g_2)\,[f(g_2)]^{-1} = e^{!}$

Hence $g_1 g_2^{-1} \epsilon N \implies g_1 \epsilon N g_2$

But $g_1 \epsilon N g_1$ also. And since the right cosets form a partition, hence

$Ng_1 = Ng_2$

$\implies \emptyset(f(g_1)) = \emptyset(f(g_2)) \implies \emptyset$ is a mapping

We now show that $\emptyset$ is isomorphic

(i) $\emptyset$ is one-to-one, for if $\emptyset\,(f(g_1)) = \emptyset(f(g_2))$ then $g_1 = ng_2$ for some $n \epsilon N$.

$\implies f(g_1) = f(ng_2)$

$= f(n)\, f(g_2) = e^{!}.\, f(g_2) = f(g_2)$

(ii) $\emptyset$ is a homomorphism for

$\emptyset\,(f(g_1)\, f(g_2)) = \emptyset(f(g_1 g_2))$ [Homomorphism] of f]

$= Ng_1 g_2$ [Definition of $\emptyset$]

$= Ng_1 g_2$ [G/N is quotient]

$= \emptyset(f(g_1))\ \emptyset(f(g_2))$

Thus (i) and (ii) show that $\emptyset$ is an isomorphism since $\emptyset$ is onto by the definition of factor group (proof completed).

EXAMPLE 1.4.2.2

From example 1.4.2.1 above, we have $f: (\mathbb{I}, +) \longrightarrow (\mathbb{R}^{+}, .)$, Ker. (f) = $\mathbb{I}e$, $f(\mathbb{I}, +) = (\{-1,1\}, .)$.

Hence, $\mathbb{I}/\text{Ker}\,(f) = \mathbb{I}/\mathbb{I}_e = \{\mathbb{I}_e, \mathbb{I}_o\}$

Theorem 1.4.2.1 guarantees that $(\{\mathbb{I}_e, \mathbb{I}_o\}, *) \cong (\{1, -1\}, .)$ as can be seen in the tables

*	$\mathbb{I}_e$	$\mathbb{I}_o$
$\mathbb{I}_e$	$\mathbb{I}_e$	$\mathbb{I}_o$
$\mathbb{I}_o$	$\mathbb{I}_o$	$\mathbb{I}_e$

*	1	−1
1	1	−1
−1	−1	1

The mapping $\bar{f}$ (induced mapping) which establishes the isomorphism is given by

$\bar{f}$: ({-1,1}, .) ⟶ ({ $\mathbb{I}_e$, $\mathbb{I}_o$},*)

$\bar{f}$ ($\mathbb{I}_e$) = f(0 + $\mathbb{I}_e$) = f (o) = 1

$\bar{f}$ ($\mathbb{I}_o$) = f(1 + $\mathbb{I}_e$) = f (1) = -1

THEOREM 1.4.2.2

In an abelian group the only inner automorphism is the identity mapping on G., but in a non-abelian group there is always a non-trivial inner automorphism.

f(-1) = $\mathbb{I}_e$* $\mathbb{I}_e$ = $\mathbb{I}_o$

f(1) = $\mathbb{I}_e$* $\mathbb{I}_e$ = $\mathbb{I}_e$

PROOF

We first note that an inner automorphism is an automorphism f_a: G⟶ G such that

$f_a(x) = a^{-1} x^a$ for all xϵG.

Hence let xϵG, if G is abelian, then

$f_a(x) = a^{-1}$xa (by definition)

$= a^{-1}(a\ g)$ (commutativity)

$= (a^{-1}\ a)\ g = g$ (associativity)

f_a is the identity mapping on G.

If G is not abelian, then for $a,b \epsilon G$

$ab \neq ba \Longrightarrow b \neq a^{-1}\ ba$ (or $a \neq bab^{-1}$)

Now, $f_a(b) = a^{-1}ba \neq b$

i.e. f_a is not equal to the identity

$\therefore f_a$ is not a trivial inner automorphism.

(proof completed).

RINGS AND THEIR ELEMENTARY PROPERTIES

2.0 INTRODUCTION

We have established a survey of all the basic ideas and important results necessary for this project in section one above. We will now introduce the main topic of lesson – the theory of rings – by considering its elementary properties and some useful results derived from these.

2.1 RINGS

An algebraic structure (R, +, .) is called a ring if:

A. (R, +) is an Abelian group. In other words, the following axioms are satisfied.

A_1: Closure: For all $a,b \epsilon R$, $a+b \epsilon R$

A_2: Commutativity: For all $a,b \epsilon R$, $a+b = b+a$

A_3: Associativity: For all $a,b \epsilon R$, $(a+b)+c = a+(b+c)$

A_4: Additive identity: There exists a number 0 in R such that $a + 0 = 0 + a = a$ for all $a \epsilon R$

A_5: Additive Inverses: There exists an element –a in R such that $a+(-a) = 0$ for all $a \epsilon R$

M. (R, .) is a semi-group: That is

M_1: Closure Property: For all $a,b \epsilon R$, $a.b \epsilon R$

M_2: Associativity: For all $a,b,c \epsilon R$, $(a.b).c = a.(b.c)$.

D. Multiplication: '.' Is distractive over additive '+' that is, for all a,b,c in R.

D_1: $a.(b+c) = a.b + a.c$ (left dist. Law)

D_2: $(a+b).c = a.c + b.c$ (right dist. Law)

NOTE:

1. The additive identity is the zero-element of R, and so should not be confused with the number 0.

2. It can be shown that – (- a) = a. Since a + (-a) = 0, let b = -a then a + b = 0, a = -b = -(-a).

EXAMPLE 2.1.1

Consider the system (𝕀, +) of integers under addition '+', this forms an abelian group. Also (𝕀, o) is a semi-group with identity 1. Thus the system (𝕀, +, o) form a ring since 'o' is distributive over '+'. It is called the ring integers.

We can also verify that the algebraic systems (ℝ, +, o), (ℚ, +, o) and (ℂ, +, o) are all examples of rings.

2.1.1 COMMUTATIVE RING WITH IDENTITY

If in addition to the above properties of ring (ℝ, +, o) we have also M_3: an element $1 \epsilon R$ such that for all $a \epsilon R$

$$a.1 = 1.a = a$$

Then (ℝ, +) is called a ring with unity or (identity) element.

If a ring (ℝ , +, o) is such that for all $a,b \epsilon R$

M_4: $a.b = b.a$

Then (ℝ, +, o) is called a commutative ring. A ring (ℝ, +, o) in which the properties M_3 and M_4 are satisfied is called a commutative ring with identity (or unity).

EXAMPLE 2.1.1.1

Consider the power set P(x) discussed in section one, if we define the binary operations Δ (symmetric difference) and ∩ (inetersection) on P(x) the (P(x), Δ, ∩) forms a commutative ring under these operations.

EXAMPLE 2.1.1.2

Let $S = 𝕀 [\sqrt{2}]$ be the set of all real numbers of the form $x + y\sqrt{2}$ where $x,y \epsilon 𝕀$. It is easily verifiable that (𝕊, +, o) is a commutative ring with unity.

EXAMPLE 2.1.1.3

Consider the modulo 5 set $\mathbb{I}_5 = \{0,1,2,3,4\}$. It can easily be established that $(\mathbb{I}_5, +_5, o_5)$ is a commutative ring with unity under these compositions.

Generally, $(\mathbb{I}_n, +_n, o_n)$ is a commutative ring with unity element $\bar{1}$ and is called the ring of integers modulo n.

2.1.2 ELEMENTARY THEOREMS ON RINGS

If $(\mathbb{R}, +, o)$ is a ring, then the following properties hold good:

THEOREM 2.1.2.1

For every element a in $\mathbb{R}$, $a.o = o.a = o$

PROOF

Since o is the additive identity then,

$a.o + a.o = a.(o+o) = a.o = a.o+o$

$\Longrightarrow a.o = o$ by (L.C.L) (i)

Conversely, $o.a = (o+o).a \Longrightarrow o+o.a = o.a+o.a$

$\Longrightarrow o = o.a$ by (R.C.L) (ii)

(i) and (ii) give the result.

THEOREM 2.1.2.2

For all a,b in $\mathbb{R}$ (i) $a.(-b) = -(a.b) = (-a).b$

(ii) $(-a).(-b) = a.b$

PROOF

(i) $a.o = o \Longrightarrow a(-b+b) = o \Longrightarrow a(-b)+a.b = o$

$\Longrightarrow a.(-b) = -(a.b)$ (inverse law) (iii)

Conversely, $o.b = o \Longrightarrow (-a+a).b = o, (-a).b + a.b = o$

$\Longrightarrow$ (-a).b = -(a.b) (iv)

(iii) and (iv) give the result.

(ii) (-a).(-b) = (-a).(-b) = (-a).(-b) + a.o = (-a)(-b)+a(-b+a)

= (-a)(-b) + a(-b) + a.b = (-a+a)(-b) + a.b

= o(-b) + a.b = o + a.b = a.b

THEOREM 2.1.2.3

For all a,b,c in $\mathbb{R}$, (i) a(b – c) = ab – ac and (ii) (b – c)a = ba – ca

PROOF

(i) a(b – c) = a(b + (-c)) = ab + a (-c) = ab + (-ac) = ab - ac

(ii) (b – c)a = (b + (-c))a = ba + (-c)a = ba + (-ca) = ba – ca.

REMARK

Theorem 2.1.2.1 shows that in a ring with identity, the identity and zero elements are never the same (since a.1 = 1.a =a) except if the ring contains only one element o.

We call a ring ({0}, +, o) consisting of only one element, 0, a zero ring.

If $\mathbb{R} \neq \{0\}$ and ($\mathbb{R}$, +, o) is a ring with identity then the elements o and 1 are distinct because $\mathbb{R} \neq \{0\}$ implies that there must be a non-zero element a in $\mathbb{R}$, otherwise, if 1 = 0 then a = a.1 = a.o = o which is a contradiction. Thus we can safely assume that any ring with identity contains more than one element.

2.2 SUBRINGS AND ZERO DIVISORS

2.2.1 ZERO DIVISORS

A ring ($\mathbb{R}$, +, o) is said to have zero divisor (or divisors of zero) if there exists non-zero elements a,b $\epsilon\mathbb{R}$ such that a.b = o. We call a the " left zero divisor", and, b the "right zero divisor".

EXAMPLE 2.2.1.0

The monoid ($\mathbb{I}_5$, o) discussed in example 2.1.1.3 have no zero divisors since there are no such elements a,b in $\mathbb{I}_5$ such that a,b = o.

However consider the set $\mathbb{I}_8$, = {0,1,2,…,6,7} we see that the ring ($\mathbb{I}_8$, +, o) contains three zero divisor 2,4 and 6 since

$$2.4 = 4.6 = 0 \pmod 8$$

Whereas none of 2,4,6 is zero.

THEOREM 2.2.1.1

A ring is without zero divisors if and only if the two cancellation laws hold for multiplication.

PROOF

Let the cancellation laws hold good in $\mathbb{R}$ and let a.b = 0 where $a \neq o$, then a.b = a.o

$\Longrightarrow$ b = o by (L.C.L). Conversely, suppose $\mathbb{R}$ has no zero divisors and $a \neq o$, if ab = ac then:

$ab - ac = 0 \Longrightarrow a(b - c) = 0$ or

$a(b - c) = a.o \Longrightarrow b - c = o$ (by L.C.L) $\Longrightarrow b = c$

Similarly, we can show that the RCL holds since if $b \neq 0$ and a.b = c.b then (a – c) b = o

= o.b $\Longrightarrow$ a – c = o (by R.C.L) $\Longrightarrow$ a = c.

2.2.2 INTERNAL DOMAIN

A commutative ring with of integers is an integral domain or if a,b are non-zero integers then $a.b \neq o$.

The ring of integers modulo p ($\mathbb{I}_p$, $+_p$, o_p) where p is prime and is also an integral domain.

For instance ($\mathbb{I}_8$, +, o) is not an integral domain since it has zero divisors 2,4 and 6).

2.2.3 IDEMPOTENT AND NILPOTENT ELEMENTS

An element ‘a’ of a ring ($\mathbb{R}$, +, o) such that $a^2 = a$ is called idempotent element.

Also, if any element $a \epsilon \mathbb{R}$ is such that $a^n = o$ where n is a positive integer then a is called nilpotent element.

EXAMPLE 2.2.3.1

In an integral domain D, if e ($\neq$ o) is an idempotent element then it is the identity element of the domain. e.g. in ($\mathbb{I}$, +, o), the only idempotent elements of D are 0 and 1.

Furthermore, the only nilpotent element of an integral domain D is o.

THEOREM 2.2.3.1

If ($\mathbb{R}$, +, o) is a ring with identity having no zero divisors, then the only solutions of the equation $a^2 = a$ are a = 0 and a = 1.

The Proof is very obvious since;

If $a^2 = a$ and $a \neq o$, then $a.s = a.1 \implies a = 1$.

EXAMPLE 2.2.4 (TRIVIAL RING)

Let (A, +) be any abelian group, and let us define o on A by a o b = o for all $a,b \epsilon A$**.**

Then (A, +, o) is a ring; it is called a trivial ring on A. It is obvious that all the elements of (A, +, o) are zero divisors.

2.2.4 CHARACTERISTIC OF A RING

If ($\mathbb{R}$, +, o) is an arbitrary ring and there exists a positive integer n such that

$n . a = o$ for all $a \epsilon \mathbb{R}$

then the least positive integer with this property is called the characteristic of the ring.

If no such positive integer exists (i.e. $na = o \implies n = o$ for all $a \epsilon \mathbb{R}$) then we say ($\mathbb{R}$, +, o) has characteristic zero.

EXAMPLE 2.2.4.1

The rings of integers, rational numbers and real numbers have characteristic zero while the ring $(p(x), \Delta, \cap)$ is of characteristic 2 since $2A = A\Delta A = (A - A) \cup (A - A) = \emptyset$ for all A in P(x).

THEOREM 2.2.4.1

Let $(\mathbb{R}, +, o)$ be a ring with identity, then $(\mathbb{R}, +, o)$ has characteristic $n > 0$ iff n is the least positive integer for which $n.1 = o$.

PROOF:

If the ring $(\mathbb{R}, +, o)$ is of characteristic $n > o$ then it follows trivially that $n.1 = 0$. Suppose $m.1 = 0$ where $0 < m < n$ then

$$Ma = m(1.a) = (m1).a = o.a = o$$

for every element $a \epsilon \mathbb{R}$ implying the characteristic of $(\mathbb{R}, +, o)$ is less than n, a contradiction.

The converse is established the way.

CORROLARY 1

In an integral domain all the non-zero elements have the same additive order, which is the characteristic of the domain.

CORROLARY 2

The characteristic of an integral domain is either zero or a prime number.

2.2.5 DIVISION RING (OR SKEW FIELD)

A division ring is a ring with identity in which every non-zero element has a multiplicative inverse.

$\Longrightarrow$ It is a ring with unity in which the non-zero elements form a group w.r.t multiplication.

FIELD

A commutative dicision ring is called a field. Also by implication, we can say that: A field is an integral domain in which every non-zero element has a multiplicative inverse.

Thus, every field is an integral domain. The converse does not hold however, but, any finite integral domain is a field.

EXAMPLE 2.2.5.1

$(\mathbb{Q}, +, o)$, $(\mathbb{R}, +, o)$ and $(\mathbb{C}, +, o)$ are fields of rational, real and complex numbers respectively.

$(\mathbb{I}, +, o)$ is an integral domain which is not a field.

2.2.6 SUBRING OF A RING

Let $(\mathbb{R}, +, o)$ be a ring abd let $S \underline{C} R$ be a non-empty subset of $\mathbb{R}$. If $(\mathbb{S}, +, o)$ is itself a ring, then $(\mathbb{S}, +, o)$ is called a subring of $(\mathbb{R}, +, o)$.

From our definition of ring, it is evident that $(\mathbb{S}, +, o)$ is a subring of $(\mathbb{R}, +, o)$ if $(\mathbb{S}, +)$ is a subgroup of $(\mathbb{R}, +)$, $(\mathbb{S}, o)$ is a subsemigroup of (R,o) and the two distributive laws hold for all elements of $\mathbb{S}$.

We should note that both distributive and associative laws automatically hold in $\mathbb{S}$ since they are valid in $\mathbb{R}$, thus they are not particularly required when defining a subring. All that is required are:

i. $\mathbb{S}$ is non-empty

ii. $(\mathbb{S}, +)$ is a subgroup of $(\mathbb{R}, +)$ and

iii. $(\mathbb{S}, o)$ is unique.

EXAMPLE 2.2.6.1

Consider the ring of integers $(\mathbb{I}, +, o)$, the ring of even integers $(\mathbb{I}_e, +, o)$ where $\mathbb{I}_e = 2\mathbb{I}$ is a subring of $(\mathbb{I}, +, o)$ but $(\mathbb{I}_o, +, o)$ considering of odd integers is not.

EXAMPLE 2.2.6.2

Let $\mathbb{S} = \{ a + b\sqrt{3} : a,b \in \mathbb{I}\}$, then $(\mathbb{S}, +, o)$ is a subring of $(\mathbb{R}, +, o)$ since for $a,b,c,d \in \mathbb{I}$ $(a+b\sqrt{3}).(c+d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3} \in \mathbb{I}$ and $(\mathbb{S}, +)$ is a subgroup of $(\mathbb{R}, +)$.

Similarly, $(\mathbb{I}[\sqrt{2}] +, o)$ is a subring of $(\mathbb{R}, +, o)$.

EXAMPLE 2.2.6.3

Let $(\mathbb{R}, +, o)$ be any ring then $(\mathbb{R}, +, o)$ and $(\{0\}, +, o)$ are subrings of $(\mathbb{R}, +, o)$ called "trivial subrings". Also, (Cent. $\mathbb{R}, +, o$) is a subring of $(\mathbb{R}, +, o)$ where cent. $\mathbb{R} = \{o \in \mathbb{R}: o.x = x.o$ for all $x \in \mathbb{R} \}$ is called the centre of the ring $(\mathbb{R}, +, o)$.

THEOREM 2.2.6.1

If $\mathbb{S}$ is a non-empty subset of $\mathbb{R}$, then $(\mathbb{S}, +, o)$ is a subring of $(\mathbb{R}, +, o)$ iff for $a,b \in \mathbb{S}$, $a-b \in \mathbb{S}$ and $a.b \in \mathbb{S}$.

PROOF

Suppose that whenever $a,b \in \mathbb{S}$, we have $a-b \in \mathbb{S}$ and $a.b \in \mathbb{S}$ then $\mathbb{S}$ is a subgroup with respect to addition. Moreover, $\mathbb{S}$ is closed under multiplication. Since associativity and distributive laws hold in $\mathbb{R}$, associativity of multiplication and distributivity hold in $\mathbb{S}$. Proof completed.

REMARK

In a ring with identity, a subring need not contain the identity element. Also, some subrings have multiplicative identity whereas the entire ring does not. Also, both the ring and one of its subrings possess distinct identity elements. For instance, consider the ring $(\mathbb{R} *x \mathbb{R}*, +, o)$ of all ordered pairs of non-zero real numbers where $(a,b)+(c,d) = (a+c, b+d)$ and $(a,b).(c,d)=(a.c,b.d)$. We can easily verify that $(\mathbb{R} *x \mathbb{R}*, +, o)$ is a ring with identity element (1,1) whereas $(\mathbb{R}x0, +, o)$ which is its subring has identity element (1,0).

2.3 RING HOMOMORPHISMS AND ISOMORPHISMS

2.3.1 HOMOMORPHISM OF RINGS

Let $(\mathbb{R}, +, o)$ and $(\mathbb{S}, \oplus, \odot)$ be two rings and f: $\mathbb{R} \longrightarrow \mathbb{S}$ be a function, then f is a ring homomorphism if and only if $f(a+b) = f(a) \oplus f(b)$, and, $f(a.b) = f(a) \odot f(b)$ for every pair of elements a,b in $\mathbb{R}$.

EXAMPLE 2.3.1.1

Let $\mathbb{R}$ and $\mathbb{S}$ be arbitrary rings and let f: $\mathbb{R} \longrightarrow \mathbb{S}$ maps each element of $\mathbb{R}$ onto the zero element $0^!$ of $\mathbb{S}$, we find that f is operation preserving

$f(a+b) = 0^! = 0^! \oplus 0^! = f(a) \oplus f(b)$

$f(a.b) = 0^! = 0^! \odot 0^! = f(a) \odot f(b)$

for all $a,b \epsilon \mathbb{R}$.

This mapping, as in groups, is the trivial homomorphism.

EXAMPLE 2.3.1.2

Consider the rings $(\mathbb{I}, +, o)$ and $(\mathbb{I}_n, +_n, x_n)$, and let f: $\mathbb{I} \rightarrow \mathbb{I}_n$ defined by $f(a) = \overline{a}$,

then f(a+b), $\overline{a + b} = \overline{a} +_n \overline{b} = f(a) +_n f(b)$

$f(a.b) = \overline{a.b} = \overline{a}\ o_n\ \overline{b} = f(a)\ o_n\ f(b)$

Hence f is homomorphic.

THEOREM 2.3.1

Let f: $\mathbb{R} \rightarrow \mathbb{R}^!$ be a homomorphism of a ring $\mathbb{R}$ into $\mathbb{R}^!$, then

(i) $f(0) = 0^!$ Where 0 and $0^!$ Are the additive identities of $\mathbb{R}$ and $\mathbb{R}^!$ Respectively.

(ii) $f(-a) = -f(a)$ for all $a \epsilon \mathbb{R}$

(iii) If $\mathbb{R}$ is a commutative ring then $\mathbb{R}^!$ is also a commutative ring.

(iv) If $\mathbb{R}$ is a ring with identity, then $\mathbb{R}^!$ is also a ring with identity.

(v) If $\mathbb{R}$ is a ring without zero divisors, then $\mathbb{R}^!$ is also a ring without zero divisors.

(vi) If $\mathbb{R}$ is a skew field then $\mathbb{R}^!$ is also a skew field.

(vii) If $\mathbb{R}$ is a field then $\mathbb{R}^!$ is also a field.

PROOF

(i) $f(a) + f(o) = f(a+o)$ Definition of homomorphism i.e. $f(a) + f(o) = f(a) = f(a) + o^!$

$\Longrightarrow f(o) = o^!$ by LCL.

(ii) $f(a) + f(-a) = f(a+(-a)$ definition of homomorphism i.e. $f(a) + f(-a) = f(0) = 0^!$

$\Longrightarrow f(-a) = - f(a)$

(iii) Since $\mathbb{R}$ is commutative $f(ab) = f(ba)$

$F(a)\ f(b) = f(b)\ f(a)$ (definition of homomorphism)

Hence $\mathbb{R}^!$ Is also commutative.

(iv) Let $1 \epsilon\ \mathbb{R}$ be the unity of $\mathbb{R}$,

$f(a) = f(a.1) = f(a)\ f(1)$

$\Longrightarrow f(1)$ is the unity element of $\mathbb{R}^!$

Thus $\mathbb{R}^!$ is also a ring with identity.

(v) From (1) we have $f(o) = o^!$. Since the mapping f is one-one then 0 is the only element of $\mathbb{R}$ which has the f- image $o^!$.

Let $f(a) \neq 0^! \Longrightarrow a \neq 0$

Similarly if $f(b) \neq 0^! \Longrightarrow b \neq 0$

Now, $ab \neq 0$ since $\mathbb{R}$ has no zero divisors

$\Longrightarrow f(ab) \neq f(0) = 0^!$

Hence $\mathbb{R}^!$ Has no zero divisors.

(vi) If $\mathbb{R}$ is a skew field this means it is a ring with unity element and without zero divisors. Thus in view of (iv) and (v), $\mathbb{R}^!$ Will also be a ring with unity element and without zero divisors. Hence $\mathbb{R}^!$ Is a skew-field also.

(vii). If $\mathbb{R}$ is a field , then it is a commutative ring with unity element and without zero-divisors. Hence in view of (iii), (iv) and (v) $\mathbb{R}^!$ Will also be a commutative ring with unity element and without zero divisors. i.e. $\mathbb{R}^!$ Is also a field.

2.3.2 ISOMORPHISM OF RING

Two rings $(\mathbb{R}, +, o)$ and $(\mathbb{R}^!, +^!, o^!)$ are said to be isomorphism if there exists a one-to-one homomorphism f from $\mathbb{R}$ onto $\mathbb{R}^!$, and we write $(\mathbb{R}, +, o) \cong (\mathbb{R}^!, +^!, o^!)$.

2.3.3 KERNEL OF HOMOMORPHISM

If f is a homomorphism from ring $(\mathbb{R}, +, o)$ into ring $(\mathbb{R}^!, +^!, o^!)$ the kernel of f is

$$\text{Ker. } (f) = \{a \in \mathbb{R}: f(a) = 0^!\}$$

Where $0^!$ Is the zero element of $(\mathbb{R}^!, +^!, o^!)$.

THEOREM 2.3.3.1

If f is a homomorphism from $(\mathbb{R}, +, o)$ onto $(\mathbb{R}^!, +^!, o^!)$ then $(\mathbb{R}/\text{ Ker}(f), +, o) \cong (\mathbb{R}!, +!, o!)$.

PROOF

Define $\bar{f}$: $\mathbb{R}/\text{ Ker}(f) \rightarrow \mathbb{R}^!$ The induced mapping by taking $\bar{f}(a + \text{Ker } (f)) = f(a)$.

From the proof of theorem earlier $(\mathbb{R}/\text{ Ker}(f), +, o) \cong (\mathbb{R}!, +!, o!)$ by $\bar{f}$. Thus we only need to show that $\bar{f}$ preserves the multiplication operation $(\mathbb{R}/\text{ Ker}(f), +, o)$. How $\bar{f}(a + \text{Ker } (f))$**.**$(b + \text{Ker } (f)) = \bar{f}(a.b + \text{Ker } (f)) = \bar{f}(a.b) = f(a)^{-2}f(b) = \bar{f}(a + \text{Ker } (f))^{1}$**.** $(b + \text{Ker } (f))$. Proved.

2.3.4 IMBEDDING OF A RING INTO ANOTHER

A ring $\mathbb{R}$ is imbedded in another ring $\mathbb{R}^!$ If there exists some subrings $\mathbb{S}$ or $\mathbb{R}^!$ Such that $\mathbb{R} \cong \mathbb{S}$.

THEOREM 2.3.4.1

Any ring can be imbedded in a ring with identity.

PROOF

Let $\mathbb{R}$ be an arbitrary ring and $\mathbb{I}$ the ring of integers. Construct the cross product

$$\mathbb{R} \times \mathbb{I} = \{(a,b): a \in \mathbb{R}, b \in \mathbb{I}\}$$

and define the following operations on $\mathbb{R} \times \mathbb{I}$

$$(a,m) + (b,n) = (a+b, m+n)$$

$$(a,m).(b,n) = (ab + mb + na, mn).$$

Under these operations $\mathbb{R} \times \mathbb{I}$ becomes a ring. Its additive and multiplicative identities are (0,0) and (0,1) respectively, since (0,0)+(a,b) = (a,b) and, (0,1).(a,b) = (a,b) and the additive inverse of any element (a,m) is (-a, -n). Hence $\mathbb{R} \times \mathbb{I}$ is a ring with identity.

Now, consider the subset $\mathbb{R} \times \{0\}$ of $\mathbb{R} \times \mathbb{I}$

$$\mathbb{R} \times \{0\} = \{(a,0) : a \in \mathbb{R}\}$$

This is a subring of $\mathbb{R} \times \mathbb{I}$ since if (a,0), (b,0) $\in \mathbb{R} \times \{0\}$ then

$$(a,0)+(b,0) = (a+b,0) \in \mathbb{R} \times \{0\}$$

$$(a,0).(b,0) = (a.b, 0) \in \mathbb{R} \times \{0\}$$

To show that $\mathbb{R} \times \{0\}$ is isomorphic to $\mathbb{R}$, define $f: \mathbb{R} \rightarrow \mathbb{R} \times \{0\}$ by

$$f(a) = (a,0)$$

Evidently, f is one-to-one, and is also operations preserving for

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

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

Hence $\mathbb{R} \cong \mathbb{R} \times \{0\}$ and so $\mathbb{R}$ is imbedded in $\mathbb{R} \times$. This complete the proof.

NOTE:

Since it is possible to embed any ring without identity in a ring with identity, there is no loss of generality in assuming that every ring has an identity element.

EXAMPLE 2.3.4.1

($\mathbb{I}$, +, o) is embedded in ($\mathbb{Q}$, +, o) by the embedding f: m → m/1 while ($\mathbb{I}$, +, o) is embedded in ($\mathbb{C}$, +, o) by the embedding f: a → a + o,i.

THEOREM 2.3.4.2

Any finite integral domain is a field.

PROOF

Suppose $a_1, a_2, \ldots, a_n$ are elements of ring ($\mathbb{R}$, +, o). For a fixed non-zero element $a \epsilon \mathbb{R}$, consider $a.\{a_1, a_2, \ldots, a_n\}$. The products $a.a_1, a.a_2, \ldots, a.a_n$ are all distinct, for if $a.a_1 = a.a_j$, then $a_1 = a_j$, by the leftcancellation law. It follows that each element of $\mathbb{R}$ is of the form $a.a_1$.

In particular, there exists some $a_1 \epsilon \mathbb{R}$ such that $a.a_1 = 1$. Since multiplication is commutative we have $a_1 = a^{-1}$ which shows that every non-zero element of $\mathbb{R}$ is invertible.

Hence, ($\mathbb{R}$, +, o) is a field.

2.3.5 FIELD OF QUOTIENTS

Let D be an integral domain and F be a field containing a subset D' such that D ≅D', then F is called the field or quotients of D (or the quotient field of D).

We now extend the ideas of the above theorem into constructing the embedding field itself, that is, the field of quotient.

THEOREM 2.3.5.1

Any integral domain can be embedded in a field. That is, from the elements of an integral domain D, it is possible to construct a field F which contains a subset D' isomorphic to D.

PROOF

Let D be an integral domain and let D_o denote the set of all non-zero elements of D.

Form a set D x D_o, say, S = {(a,b): aϵD, bϵD_o}

Define a relation ~ as follows:

(a,b) ~(c,d) iff ad = bc for all (a,b),(c,d) ϵS.

This is an equivalence relation, because (a,b) ~ (a,b) since ab = ba $\Longrightarrow$ ~ is reflexive.

Also, if (a,b) ~(c,d), then ad = bc or cd = da $\Longrightarrow$(c,d) ~ (a,b). That is ~is symmetric.

Also, if (a,b) ~ (c,d) and (c,d) ~ (e,f)

Then, ad = bc and cf = de

i.e. (ad)f = (bc)f $\Longrightarrow$ (ad)f = b(cf)

$\Longrightarrow$ a(df) = b(de)

i.e. a(fd) = b(ed) $\Longrightarrow$(af)d = (be)d

$\Longrightarrow$af = be (by R.C.L)

(a,b) ~ (e,f) $\Longrightarrow$ ~ is transitive.

Hence, the relation partitions the product set S into disjoint equivalence classes.

Let us denote the equivalence class containing

(a,b) by a/b (oe [a,b] or $(\overline{a, b})$

i.e. a/b = {(c,d): (c,d) ~ (a,b)} of course, if (a,b) ~ (c,d) $\Longrightarrow \frac{a}{b} = \frac{c}{d} \Longrightarrow$ad = bc.

Now let us form a set F where

F = {$\frac{a}{b}$: aϵD, bϵD_o} is the set of equivalence classes

And define the following operations of F:

Addition: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ for all $\frac{a}{b}, \frac{c}{d} \epsilon F$

Multiplication: $\frac{a}{b} . \frac{c}{d} = \frac{ac}{bd}$ for all $\frac{a}{b}, \frac{c}{d} \epsilon F$

We claim that these operations are well-defined and illustrated as follows:

If $\frac{a}{b} = \frac{a_1}{b_1}$ *and* $\frac{c}{d} = \frac{c_1}{d_1}$, then

(i) $\frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1} \Longrightarrow \frac{ad+bc}{bd} = \frac{a_1d_1+b_1c_1}{b_1d_1}$

$\Longrightarrow$(ad + bc) b_1d_1 = bd(a_1d_1 + b_1c_1)

From L.H.S, (ad + bc)b_1d_1 = adb_1d_1 + bcb_1d_1

= ab_1dd_1 + bb_1cd_1

= ba_1dd_1 + bb_1dc_1

= bda_1d_1 + bdb_1c_1

= bd(a_1d_1 + b_1c_1) = RHS

Hence, addition is well defined.

(ii) $\frac{a}{b} . \frac{c}{d} = \frac{a_1.c_1}{b_1.d_1} \Longrightarrow$ acb_1d_1 = bda_1c_1 = bda_1c_1

From L.H.S, acb_1d_1 = $a_1$bcd_1

= ba_1dc_1 = bda_1c_1 = R.H.S

Hence multiplication is also well defined.

Now we can verify that under these operations F forms a field.

The additive identity is $\frac{0}{a}$ where a $\neq$ 0

And the multiplicative identity is $\frac{a}{a}$, a $\neq$ 0

The additive inverse of $\frac{a}{b} = -\frac{a}{b}$ and the multiplicative inverse of $\frac{a}{b}$ is $\frac{b}{a}$ (a $\neq$ 0)

Associativity, commutativity and distributivity can also be easily established. Hence (F, +, o) is a field.

Now Let D' $\underline{c}$ F where

$$D' = \left\{\frac{ax}{x} : a \epsilon D, x \epsilon D_0\right\}$$

Since if $x \neq 0$, $y \neq 0$, then $\frac{ax}{x} = \frac{ay}{y}$ for axy = xay

Hence, we can write D' for any non-zero x as

$$D' = \left\{\frac{ax}{x} : a \epsilon D\right\}$$

Now we define a mapping f: D →D' by

$$f(a) = \frac{ax}{x} \text{ for all } a \epsilon D$$

f is one-to-one because if f(a) = f(b) then

$$\frac{ax}{x} = \frac{bx}{x} \Longrightarrow ax^2 = bx^2 \Longrightarrow (a-b)x^2 = 0$$

Or $a - b = 0 \Longrightarrow a = b$

f is onto, since for any $\frac{ax}{x} \epsilon D'$ there is $a \epsilon D$ such that $f(a) = \frac{ax}{x}$

Finally f preserves operations because

$$f(a+b) = \frac{(a+b)x}{x} = \frac{(a+b)x^2}{x^2} = \frac{ax^2 + bx^2}{x^2}$$

$$= \frac{ax^2}{x^2} + \frac{bx^2}{x^2} = \frac{ax}{x} + \frac{bx}{x} = f(a) + f(b)$$

And $f(ab) = \frac{(ab)x}{x} = \frac{abx^2}{x^2} = \frac{ax.bx}{x.x}$

$$= \frac{ax}{x} \cdot \frac{bx}{x} = f(a).f(b)$$

Hence, f is isomorphic, that is, D ≅ D'.

We see that the elements of D' can be identified with the elements of D in a one-to-one basis, and so D $\underline{c}$ F.

EXAMPLE 2.3.5.1

We see that $(\mathbb{Q}, +, o)$ is the quotient field of $(\mathbb{I}, +, o)$ since if $\mathbb{I} \subseteq$ field F, then all the ab^{-1} (or a/b) where $a \in \mathbb{I}$, $b \in \mathbb{I}$ must also be in F. Thus $(\mathbb{Q}, +, o)$ must be a subring of F and $(\mathbb{Q}, +, o)$ is thus the smallest field containing $(\mathbb{I}, +, o)$.

Similarly, we can construct the field of quotients $(\mathbb{R}, +, o)$ from $(\mathbb{Q}, +, o)$; and the field $(\mathbb{C}, +, o)$ from $(\mathbb{R}, +, o)$.

EXAMPLE 2.3.5.2

$(\mathbb{R}, +, o)$ is the quotient field of both $(\mathbb{Q}[\sqrt{2}], +, o)$ and $(\mathbb{Q}[\sqrt{3}], +, o)$ while $(\mathbb{C}, +, o)$ is the quotient field of $(\mathbb{I}[i], +, o)$.