COURSE CODE : MTS 211

COURSE TITLE: INTRODUCTION TO ABSTRACT ALGEBRA

NUMBER OF UNITS: 2 UNITS

COURSE DURATION : Two Hours per Week

COURSE COORDINATOR : Dr S.A. Akinleye, B.Sc , M.Sc. Ph.D (Mathematics)

Email: Akinleye@unaab.edu.ng ,or, akinleye_sa@yahoo.com

Office Location: Room B212, COLNAS

Other Lecturers: Mrs Bola Akwu

COURSE CONTENT

Sets: Binary Operations, Mappings, equivalence relations. Cartesian products.

Number theory: Divisibility and Primes. Fundamental theorem of arithmetic, congruencies, linear congruence equations, Euler function.

Group theory: Definition and examples of groups. Subgroup, coset decomposition, Lagrange theorem, cyclic groups, Cayley theorem.

Rings: Definitions and examples. Commutative rings. Integral domain. Division rings. Fields, Construction of the field of fractions of an integral domain and the embedding theorem.

COURSE REQUIREMENTS

This is a compulsory course for all students in Mathematics, Computer Science and Statistics. In view of this , students are required to participate in all the couse activities and have minimum of 75 % attendance to be able to write the final examination.

READING LIST

Kuku A. O. Abstract Algebra, Ibadan University Press, Ibadan (1992 edition)

Battacharya P. B. Basic Abstract Algebra

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 ∪,∩, Δ 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

(ℕ, +), (𝕀, +), (ℚ, .), (ℝ, +, .) (ℂ, +, .) (p(X), ∪) and (P (x), ∪, ∩) are all algebraic systems.

For any binary operation * defined on a set S,

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

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

3. If there is an element e ∈ S such that e*x = x*e = x for all x ∈ 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 ∈ IR, x + 0 = 0 + x = x, x.1 = 1.x = x.

4. if there is an element y ∈ S such that x*y = y*x = e for x ∈ 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 o (y*z) = x o y * x o z for all x,y,z ∈ S and o is right distributive over * if

(x*y) o z = x o z * y o z for all x,y,z ∈ 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 ∈ 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 ϵ $\mathbb{I}_n$

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 $H_1 \underline{c} H_2$ or $H_2 \underline{c} H_1$. 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 $\mathbb{I}$ = {…, -3, -2, -1, 0, 1, 2, …}

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

If a ϵ $\mathbb{I}$, 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 = {{…, -6, -4, -2, 0, 2, 4, …}

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

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

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

Hence the distinct Cosets of ($2\mathbb{I}$, +) in ($\mathbb{I}$, +) are $2\mathbb{I}$ and $2\mathbb{I}$ + 1; obviously $\mathbb{I}$ = $2\mathbb{I}$ U ($2\mathbb{I}$ + 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, …, 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 $H \Delta G$ if for all $g \epsilon G$, $gHg^{-1} = H$.

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

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 ⟶ $G^!$ 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^+ ⟶ 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 ⟶ G/N by

$f(g) = N_g$ for all gϵG

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

$f(g_1.g_2) = N(g_1.g_2)$ 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 = {gϵG: f(g) = $e^!$ where $e^!$ is the identity element of $G^!$ }

1.4.2 ISOMORPHISM AND OTHER HOMOMORPHISMS

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

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

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

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

If f: G ⟶ G is isomorphic and onto then f is called an automorphism.

EXAMPLE 1.4.2.1

Let f: 𝕀 ⟶ ℝ - {o} defined by

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

Then f is clearly a homomorphism, and

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

REMARKS

If f:G ⟶$G^!$ 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 ⟶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) ⟶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) ⟶ 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 $g_1g_2^{-1}\epsilon N \Longrightarrow g_1\epsilon Ng_2$

But $g_1\epsilon Ng_1$ also. And since the right cosets form a partition, hence

$Ng_1 = Ng_2$

$\Longrightarrow \emptyset(f(g_1)) = \emptyset(f(g_2)) \Longrightarrow \emptyset$ 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 $n\epsilon N$.

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

$= f(n) f(g_2) = e^!. f(g_2) = f(g_2)$

(ii) $\emptyset$ is a homomorphism for

$\emptyset (f(g_1) f(g_2)) = \emptyset(f(g_1g_2))$ [Homomorphism] of f]

$= Ng_1g_2$ [Definition of $\emptyset$]

$= Ng_1g_2$ [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, $\mathbb{I}$/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 f^{-} (induced mapping) which establishes the isomorphism is given by

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

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

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

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: $G \longrightarrow G$ such that

$f_a(x) = a^{-1}\, x^a$ for all $x\epsilon G$.

Hence let $x\epsilon G$, 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 ($\mathbb{I}$, +) of integers under addition '+', this forms an abelian group. Also ($\mathbb{I}$, o) is a semi-group with identity 1. Thus the system ($\mathbb{I}$, +, o) form a ring since 'o' is distributive over '+'. It is called the ring integers.

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

2.1.1 COMMUTATIVE RING WITH IDENTITY

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

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

Then ($\mathbb{R}$, +) is called a ring with unity or (identity) element.

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

$$M_4: a.b = b.a$$

Then ($\mathbb{R}$, +, o) is called a commutative ring. A ring ($\mathbb{R}$, +, 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 $\cap$ (inetersection) on P(x) the (P(x), Δ, $\cap$) forms a commutative ring under these operations.

EXAMPLE 2.1.1.2

Let $S = \mathbb{I}\,[\sqrt{2}]$ be the set of all real numbers of the form $x + y\sqrt{2}$ where $x,y\epsilon\, \mathbb{I}$. It is easily verifiable that ($\mathbb{S}$, +, 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 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 ℝ ≠ {0} and (ℝ, +, o) is a ring with identity then the elements o and 1 are distinct because ℝ ≠ {0} implies that there must be a non-zero element a in 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 (ℝ, +, o) is said to have zero divisor (or divisors of zero) if there exists non-zero elements a,b ϵℝ 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

$$2.4 = 4.6 = 0 \text{ (mod 8)}$$

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 ≠ o, then a.b = a.o

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

$$ab - ac = 0 \Longrightarrow a\,(b - c) = 0 \text{ or}$$

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

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

$$= o.b \Longrightarrow a - c = o \text{ (by R.C.L)} \Longrightarrow a = c.$$

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 ≠ 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,bϵA**.**

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

PROOF:

If the ring (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 (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.

⟹ 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 ϵ $\mathbb{I}$}, then ($\mathbb{S}$, +, o) is a subring of ($\mathbb{R}$, +, o) since for a,b,c,d$\epsilon\mathbb{I}$ (a+b$\sqrt{3}$).(c+d$\sqrt{3}$) = (ac + 3bd) + (bc + ad) $\sqrt{3}$ ϵ $\mathbb{I}$ 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 ϵ $\mathbb{R}$: o.x = x.o for all x $\epsilon\mathbb{R}$ } 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 $\epsilon\mathbb{S}$, a-b $\epsilon\mathbb{S}$ and a.b $\epsilon\mathbb{S}$.

PROOF

Suppose that whenever a,b $\epsilon\mathbb{S}$, we have a-b $\epsilon\mathbb{S}$ and a.b $\epsilon\mathbb{S}$ 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 $f(a) = \overline{a}$,

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

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

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 1ϵ $\mathbb{R}$ 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) ≅ ($\mathbb{R}^!$, $+^!$, $o^!$).

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

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

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 ($\mathbb{R}$/ Ker(f), +, o) ≅ $(\mathbb{R}!, +!, o!)$.

PROOF

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

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

$$\mathbb{R} \text{ x } \mathbb{I} = \{(a,b): a \epsilon\mathbb{R}, b \epsilon\mathbb{I}\}$$

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

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

$$(a,m)\mathbf{.}(b,n) = (ab + mb + na, mn).$$

Under these operations $\mathbb{R}$ x $\mathbb{I}$ 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 $\mathbb{R}$ x $\mathbb{I}$ is a ring with identity.

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

$$\mathbb{R}\text{x } \{0\} = \{(a,0) \mathbf{:} a\epsilon\mathbb{R}\}$$

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

$$(a,0)+(b,0) = (a+b,0) \epsilon \mathbb{R}\text{x}\{0\}$$

$$(a,0).(b,0) = (a.b, 0) \epsilon \mathbb{R}\text{x } \{0\}$$

To show that $\mathbb{R}$x {0} is isomorphic to $\mathbb{R}$, define f: $\mathbb{R} \rightarrow \mathbb{R}$x {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 $\mathbb{R} \cong \mathbb{R}$x {0} and so $\mathbb{R}$ is imbedded in $\mathbb{R}$ x . 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 $a.a_1$, $a.a_2$, …, $a.a_n$ 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, $S = \{(a,b): a\epsilon D, b\epsilon D_o\}$

Define a relation ~ as follows:

$(a,b) \sim (c,d)$ iff $ad = bc$ for all $(a,b),(c,d)\ \epsilon S$.

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

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

Also, if $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

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)

$(a,b) \sim (e,f) \Longrightarrow \sim$ 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. ${}^{a}/_{b} = \{(c,d): (c,d) \sim (a,b)\}$ of course, if $(a,b) \sim (c,d) \Longrightarrow \frac{a}{b} = \frac{c}{d} \Longrightarrow ad = bc$.

Now let us form a set F where

$F = \{\frac{a}{b}: a\epsilon D, b\epsilon D_o\}$ 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) $\frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1} \Longrightarrow \frac{ad + bc}{bd} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1}$

$\Longrightarrow$(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_1bcd_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 ≠ 0

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

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

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

Now Let D’ $\underline{c}$ F where

$$D' = \left\{\frac{ax}{x} : a\epsilon \mathrm{D}, \mathrm{x}\epsilon \mathrm{D}_0\right\}$$

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

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

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

Now we define a mapping f: D →D’ by

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

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

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

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 $\mathbb{I}$ $\underline{c}$ field F, then all the ab^{-1} (or a/b) where a ϵ $\mathbb{I}$, b $\epsilon\mathbb{I}$ 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 $(\mathbb{Q}\left[\sqrt{2}\right], +, o)$ and ($\mathbb{Q}[\sqrt{3}]$, +, o) while ($\mathbb{C}$, +, o) is the quotient field of ($\mathbb{I}$[i], +, o).

COURSE CODE: MTS 211

COURSE TITLE:Abstract Algebra

NUMBER OF UNITS: 2

COURSE DURATION: Two hours per week

COURSE DETAILS:

Course Coordinator: Dr. S. A. Akinleye

Other Lecturer: Miss. A. D. Akinola

COURSE CONTENT:

Set: Binary operations,mappings,equivalence relations,Cartesian products.

Number theory: Divisibility and primes,Fundamental theorem of arithmetic,congruencies,linear congruence equations, Euler's function.

COURSE REQUIREMENTS:

This is a compulsory course for students in the department of Mathematics,Statistics and Computer science.

Sets

Definition

A set is a collection of objects which can be distinguished from each other.We shall said that a set is defined if whenever any object is given, it is possible to decide whether or not it belongs to the set.The objects comprising the set are generally called the elements of the set and they may be finite or infinite in number.

Example:

1. A school constitutes a set and each student or teacher is an element of the set.

2. The whole number $1, 2, 3, ...$ constitutes a set and each whole number is an element of this set.

Capital letters are use to denote sets and small letters $a, b, c, d, ...$ to denote elements.The symbol needed for enclosing the elements of a set is a pair of braces,so that when a set A is specified by listing the elements a, b, c, d and e contained in A,we will write

$$A = \{a, b, c, d, e\}$$

The symbol : or | is used for 'such that'. Example
$N = \{n : n \quad is \quad a \quad whole \quad number\}$ indicates that N is the set of all elements n such that N is a whole number .That is N is the set of all whole number.

Membership of a set :

The element that make up a set are usually called member of that set.We use the symbol $\in$ to stand for 'is a member (element) of' while the symbol $\notin$ stand for 'is not a member (element) of' e.g
If $A = \{a, b, c\}$ then $a \in A, d \notin A$

Finite and Infinite set:

A finite set is one whose members are countable.e.g

1. Consider a set $A = \{n : n \quad is \quad a \quad whole \quad number, 0 < n < 20\}$.

2. Member of a football team.

An infinite set is one whose elements are uncountable,as they are infinitely numerous. e.g

The set N of all whole numbers is an infinite set and we could write it thus:

$N = \{1, 2, 3, ...\}$ with ..., to show it goes on forever.

The set consisting of a single object is called a singleton set.

Subsets:

A set T is called a subset of a set S if every element of T ia also an element of S.We write $T \subseteq S$ or $S \supseteq T$. Observe that this definition implies that every set is a subset of itself.However,if T is a subset of S and $T \neq S$,we say that T is a proper subset of S and then write $T \subset S$ or $S \supset T$.Thus T is a proper subset of S if T is a subset of S and there exist at least one element of S that is not in T.

Two sets S, T are equal if and only if $S \subseteq T$ and $T \subseteq S$

Example:

Kano state,Lagos state,Oyo state is a proper subset of states in Nigeria

Empty set:

A set is said to be empty or null if it contains no elements.If a set S is empty,we write $S = \phi$ or $\{\}$. e.g

$S = \{x|x \in R \quad and \quad x^2 + 1 = 0\} = \phi$ since $x^2 + 1 = 0$ has no real roots.

Empty set ϕ is a subset of every set.

Equality of sets:

Two sets are equal if they have the same elements e.g

$\{a, e, i, o, u\} = \{e, o, u, i, a\}$.

Also we introduce two new symbols namely $\Longrightarrow$ and $\Longleftrightarrow$. e.g

$x \in \{x, y, z\} \Longrightarrow \{x\} \subset \{x, y, z\}$.

This means that the statement on the right hand side must follow from the statement on the left but the statement on the left does not necessarily follow from that on the right.

$\Longrightarrow$ stands for implies and $\Longleftrightarrow$ stands for 'implies and implied by' or 'if and only if'

For any two sets A and B,

If $x \in B \Longrightarrow x \in A$, then $B \subset A$.

$A \subset B$ and $B \subset A \Longrightarrow A = B$.

Universal set :

The set containing all elements under discussion in a particular problem is called the universal set and is denoted by symbol Σ

Complement:

Given a set A,then the set which contains all the elements of the universal set,which are not elements of A is called the complement of A and is denoted by A' or A^c.Thus

$A' = \{x : x \in \Sigma \quad and \quad x \notin A\}$ e.g

$\Sigma = \{1, ..., 8\}$,$A = \{2, 4, 6, 8\}$, $A' = \{1, 3, 5, 7\}$.

Equivalent set:

If to each elements of a set A there corresponds an element of another set B and to each element of B there corresponds an element of A,the element of the two sets are said to be in one-to-one correspondence.The sets are then said to be equivalent.The symbol which expresses this relationship is $\sim$ and $A \sim B$ means that A is equivalent to B.e.g

The sets $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$ are equivalent because we could make the first element of A correspond to the first element of B and so on.

The sets $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4, 5\}$ are not equivalent because even through we can pair all the elements of A with some of the elements of B,the reverse procedure leaves one element without any pair.

Power set:

The family β of all subsets of S is called the power set of S and is denoted by 2^s.

For example

Is $S = \{1, 2, 3\}$,$\beta = \{\phi, S, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{3, 1\}\} = 2^3$.

Definition:

Let Ω be any set .The family or collection of sets S_ω written $\{S_\omega\}_{\omega \in \Omega}$ is said to be indexed by Ω and Ω is called an indexing set for this family.

For example

1. Let $\Omega = N =$ set of all natural number and $S_n = 1 + \frac{1}{2} + ... + \frac{1}{2^n}$.Then the family $\{S_n | n \in N\}$ is indexed by $\Omega = N$.

2. (*) Let $\Omega = \{1, 2, 3, 4, 5\}$ and S_ω=all integral multiples of ω.Thus $S_1 = Z$

   $S_2 = 2Z = \{..., -4, -2, 0, 2, 4, ...\}$

   $S_3 = 3Z = \{..., -6, -3, 0, 3, 6, ...\}$

   $S_\omega = \{..., -2\omega, -\omega, 0, \omega, 2\omega, ...\}\omega \in \Omega$

3. Let $\Omega =$ the set of all English words and $S_\omega = \{x | x \quad is \ a \quad letter \quad in \quad \omega \in \Omega\}$

   Suppose ω is the word 'fence' then $S_\omega = \{e, f, n, c\}$

4. let $\Omega = \{a, b, c\}$

   $S_a = \{all \quad even \quad integers\}$

   $S_b = \{x \in Z | -10 \leq x \leq 5\}$

   $S_c = \{all \quad integers \quad \geq -5\}$

The last example shows that indexing set may have no direct bearing on the sets being indexed. Ω may just provide a way of distinguishing the set concerned.

Intersection:

Suppose we have two sets S, T.The intersection of S and T is the set of all elements common to both S and T and is denoted by $S \cap T$. Thus $S \cap T = \{x | x \in S \quad and \quad x \in T\}$.Observe that if $T \subset S$, then $S \cap T = T$.Also if $S \cap T = \phi$,we say S and T are disjoint.

If $\Omega = \{\omega\}$ is any indexing set for a family $\{S_\omega\}_{\omega \in \Omega}$ we define the intersection $\cap_{\omega \in \Omega} S_\omega$ of members of this family as the set of all elements common to all the $S_\omega, \omega \in \Omega$.Thus $\cap_{\omega \in \Omega} S_\omega = \{x | x \in S_\omega \quad for \quad each \quad \omega \in \Omega\}$.

For example

Let $S = \{1, 3, 5, 7, 9\}$,$T = \{x \in Z | x^3 - 6x^2 + 11x - 6 = 0\}$.Then $S \cap T = \{1, 3\}$.

Union:

Let S, T be two sets.We define the union of S and T ,written $S \cup T$, as the set of elements which are either in S or T.Thus $S \cup T = \{x | x \in S \quad or \quad x \in T\}$.It follows that $S \cup T = T \cup S$.If Ω is an indexing set for a family $\{S_\omega\}_{\omega \in \Omega}$,then the union $\cup_{\omega \in \Omega} S_\omega$ of the sets S_ω is defined as $\cup_{\omega \in \Omega} S_\omega = \{x | x \quad is \quad in \quad at \quad least \quad one \quad S_\omega$.

For example

In example (*),$\cup_{\omega \in \Omega} S_\omega = Z$.

Theorem: If S, T are two sets,then

1. $S \cap (T \cap V) = (S \cap T) \cap V$
2. $(S \cup T) \cup V = S \cup (T \cup V)$
3. $S \cap (T \cup V) = (S \cap T) \cup (S \cap V)$
4. $S \cup (T \cap V) = (S \cup T) \cap (S \cup V)$

Proof: (1)-(2) (exercise)

3. Let $x \in L.H.S$,then $x \in S$ and $x \in T \cup V$. This implies that $x \in S$ and $x \in (T \quad or \quad V)$.

i.e $x \in (S \quad and \quad T)$ or $x \in (S \quad and \quad V)$.

i.e $x \in S \cap T$ or $x \in S \cap V$,

i.e $x \in S \cap T \cup x \in S \cap V$

Hence $x \in R.H.S$.

Therefore $S \cap (T \cup V) \subseteq (S \cap T) \cup (S \cap V)$.

Let $x \in R.H.S$,then $x \in S \cap T$ or $x \in S \cap V$.

i.e $x \in (S \quad and \quad T)$ or $x \in (S \quad and \quad V)$

$\Longrightarrow \quad that \quad x \in S \quad and \quad x \in T \quad or \quad V$

i.e $x \in S \cap (T \cup V)$

Hence $(S \cap T) \cup (S \cap V) \subseteq S \cap (T \cup V)$

Therefore $(S \cap (T \cup) = (S \cap T)n \cup (S \cap V)$

Definition:

A family $\{S_\omega\}_{\omega \in \Omega}$ of subset S_ω of a set S is said to form a partition if

1. $S = \cup_{\omega \in \Omega} S_\omega$ and

2. For any $S_\omega, S_{\omega'}$,either $S_\omega = S_{\omega'}$ or $S_\omega \cap S_{\omega'} = \phi$

i.e $\omega \neq \omega' \Longrightarrow S_\omega \cap S_{\omega'} = \phi$

Definition:

Let S, T be two sets,we define $S - T$,the difference of S and T (sometimes read 'S minus T) as the set of elements which are in S but not in T.

For example

Let $S = \{1, 2, 3, 4, 7, 10\}$

$T = \{2, 7, 5, 8, 11\}$

$S - T = \{1, 3, 10\}$

Theorem:

1. $A - B \subset A$

2. $(A - B) \cap B = \phi$

Proof:

1. Let $x \in (A - B)$. By definition $x \in A$ and $x \notin B$. In any case $x \in A$,so $(A - B) \subset A$

2. Let $x \in (A - B) \cap B$

Then $x \in A - B$ and $x \in B$ (1)

Now $x \in A - B$ implies that $x \in A$ and $x \notin B$. This contradicts (1).Hence there does not exist any element in $(A - B) \cap B$.

Therefore $(A - B) \cap B = \phi$.

Theorem:

1. $\Sigma' = \phi, \phi' = \Sigma$

2. $(S')' = S$

3. $(S \cup T)' = S' \cap T'$

4. $(S \cap T)' = S' \cup T'$

(3) and (4) are known as De Morgan's law.

Proof.

3. Let $x \in (S \cup T)'$ then $x \notin (S \cup T)$. i.e $x \notin (S \quad or \quad T)$.Then clearly $x \in S'$ and $x \in T'$ which means that $x \in S' \cap T'$ i.e $(S \cup T)' \subseteq S' \cap T'$. Similarly let $x \in S' \cap T'$,then $x \in S'$ and $x \in T'$. i.e $x \notin S$ and $x \notin T$. Hence x cannot be in $S \cup T$,since it is neither in S nor in T. i.e $x \in (S \cup T)'$.

Therefore $S' \cap T' \subseteq (S \cup T)'$.

Therefore $(S \cup T)' = S' \cap T'$.

Definition: Let S, T be two sets.The symmetric difference of S and T is defined as $(S \cup T) - (S \cap T)$ and written as $S \triangle T$.

Definition: Let $\{S_\omega\}_{\omega \in \Omega}$ be a family of sets indexed by Ω. The disjoint union or set sum of S_ω is define as $\cup_{\omega \in \Omega}\{S_\omega \times \{\omega\}\}$ and written as $\vee_{\omega \in \Omega} S_\omega$. If sets S_ω are disjoint then $\vee_{\omega \in \Omega} S_\omega$ and $\cup_{\omega \in \Omega} S_\omega$ have the same number of elements.

For example.

1. Let $\Omega = \{1, 2\}, S_1 = \{a, b\}, S_2 = \{c, d\}$

Then $S_1 \vee S_2 = \{(a, 1), (b, 1), (c, 2), (d, 2)\}$

2. Let $\Omega = \{a, b, c\}$

$S_a = \{1, 2, 3, 6, 8, 10\}, S_b = \{2, 4, 6, 7, 9\}, S_c = \{4, 11, 6, 1, 3, 18\}$

Then $S_a \vee S_b \vee S_c = (S_a \times \{a\}) \cup (S_b \times \{b\}) \cup (S_c \times \{c\})$. Note that $S_a \cup S_b \cup S_c$ has 11 elements but $S_a \vee S_b \vee S_c$ has 17 elements.

Definition: The cartesian product (or product set) of S and T written as $S \times T$ is the set of all ordered pair (a, b) such that $a \in S$ and $b \in T$.

If S or T is a null set,then so is $S \times T$.If S has s elements and T has t

elements,$S \times T$ has st elements. If either S or T is infinite and the other is non-empty,then $S \times T$ is infinite.

For example

Let $S = \{c, d\}, T = \{4, 7, 9\}$ then $S \times T = \{(c, 4), (c, 7), (c, 9), (d, 4), (d, 7), (d, 9)\}$.

Hence $S \times T$ has 6 elements.

Definition: The cartesian product $S_1 \times ... \times S_n$ of n sets $S_1, ...S_n$ as the set of all n-tuples $(\alpha_1, ..., \alpha_n)$ where $\alpha_i \in S_i, i = 1, 2, ..., n$ with the understanding that $(\alpha_1, ..., \alpha_n) = (\alpha'_1, ..., \alpha'_n)$ if and only if $\alpha_i = \alpha'_i$.

For example

The Euclidean 3-space $=R \times R \times R = \{(a, b, c) | a, b, c \in R\}$.

Definition: An open sentence in a single variable x is an expression of the form $p(x)$ such that when x is replaced by a specific value like a,then $p(aP$ is either true or false.

An open sentence in two variables x, y is an expression of the form $p(x, y)$ such that whenever x, y are given specific values a, b say,then $p(a, b)$ is either true or false.

For example

1. x divides y is an open sentence in x and y $p(2, 4)$ is rue but $p(3, 5)$ is false.
2. $x - y = 4$ is an open sentence in two variables $p(12, 8)$ is true but $p(9, 6)$ is false.

Definition: Let S and T be two sets. A propositional function defined on $S \times T$ is an open sentence $p(x, y)$ where x takes in S and y in T.

Definition: Let S, T be two sets.A relation $\sim$ from S to T is given by a triple $(S, T, p(x, y))$ where $p(x, y)$ is a propositional function on $S \times T$.

If $p(a, b)$ is true,write $a \sim b$ (to be read a is in relation to b). Otherwise write $a \sim b$. If $\sim$ is a relation from S to T,we may write it as $\sim: S \longrightarrow T$ and $b =\sim (a)$ where $a \in S, b \in T$ and $p(a, b)$ is true. If $\sim= (S, S, p(x, y))$ we say that $\sim$ is a relation on S.

Definition: Let $\sim$ be a relation from a set S to a set T.The domain D of $\sim$ is the subset of S consisting of first co-ordinate elements of $\sim^*$. i.e

$D = \{a|(a, b) \in\sim^*\}$.

The range F of $\sim$ is the subset of T consisting of second co-ordinate elements of $\sim^*$ i.e

$F = \{b|(a, b) \in\sim^*\}$.

For example

$S = \{1, 3, 4, 7, 8\}$,$T = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Let $\sim= (S, T, p(x, y))$ where $p(x, y)$ means $y = 2x$.

Then $\sim * = \{(1, 2), (3, 6), (4, 8)\}$.

$D = \{1, 3, 4\}, F = \{2, 6, 8\}$.

Definition: A relation $\sim$ on a set S is said to be reflexive if $a \sim a$ for all $a \in S$ i.e $(a, a) \in\sim^*$ for all $a \in S$.

(**) For example

Let $S = N$,the set of all natural numbers.For $a, b \in N$,let $a \sim b$ means a divides b.Then a divides a for all $a \in N$ and so $\sim$ is reflexive.

Definition: A relation $\sim$ on a set S is said to be symmetric if $a \sim b$ implies that $b \sim a$ for all $a, b \in S$. i.e $(a, b) \in \sim^*$ implies that $(b, a) \in \sim^*$ for all $a, b \in S$.

For example

In the example (**) above,$\sim$ is not symmetric,since a divides b does not necessarily imply that b divides a.

e.g 2|6 but 6 does not divide 2.

Definition: A relation $\sim$ on a set S is said to be transitive if $a \sim b$ and $b \sim c$ imply that $a \sin c$. i.e $(a, b) \in \sim^*, (b, c) \in \sim^*$ imply that $(a, c) \in \sim^*$.

e.g In the example (**) above,$\sim$ is transitive,since a divides b and b divides c imply that a divides c.

Definition: A relation $\sim$ on a set S is called an equivalence relation if $\sim$ is reflexive,symmetric and transitive.

For eaxample

Let $S = Z$. Define $a \sim b$ by 5 divides $(a - b)$. Then $\sim$ is an equivalence relation.

Proof.

5 divides $(a - b)$ implies that $(a - b) = 5k$ for some $k \in Z$ i.e $a = 5k + b$.

So $a \sim a$ since $a = 5k + a$ for some $k = 0 \in Z$ i.e $\sim$ is reflexive.

Now $a \sim b$ implies that $a = 5k + b$. i.e $b = a + 5k'$ where $k' = -k$ also in Z.Hence $a \sim b$ implies $b \sim a$ ie.$\sim$ is symmetric.

Now $a \sim b$,$b \sim c$ all imply that $a = 5k_1 + b, b = 5k_2 + c$ respectively for some

$k_1, k-2 \in Z$ i.e $b = a-5k-1$ and $a-5k-1 = 5k_2+c$ i.e $a = 5(k_1+k_2)+c$. Now $k_1 + k_2 = k \in Z$.Hence $a = 5k + c$ for $k \in Z$.

Thus $a \sim b, b \sim c$ imply $a \sim c$. Hence $\sim$ is transitive.

Therefore $\sim$ is an equivalence relation.

Definition: Let $\sim$ be an equivalence relation on a set S. foe $a \in S$, we define equivalence class of a as the set of all elements b in S such that $a \sim b$ and denote this set by $[a]$.The set of all equivalence classes in S is called the quotient set of $\sim$ and written $s/\sim$.

For example

In the example (**) above,

$[0] = \{b \in Z | b = 5k \quad for \quad all \quad k \in Z\} = \{..., -10, -5, 0, 5, ...\}$

$[1] = \{b \in Z | b = 1 + 5k \quad for \quad all \quad k \in Z\} = \{..., -9, -4, 1, 6, 11, ...\}$

.

.

.

$[4] = \{b \in Z | b = 4 + 5k, \quad for \quad all \quad k \in Z\} = \{..., -6, -1, 4, 9, 14, ...\}$

of course $[5] = [0]$

The equivalence classes above are called residue classes modulo 5.In general case where 5 is replaced by an arbitrary positive integer m,then the equivalence classes are called residue classes modulo m and are given by $[0], [1], ..., [m-1]$.

Theorem: If $\sim$ is an equivalence relation on a set S,then the set of equivalence classes of $\sim$ gives a partition of S.Conversely,given any partition of S,there exists an equivalence relation $\sim$ on S such that the set of equivalence classes of r is the given partition.

Natural Numbers

Let N be a non-empty set.Assume the following axioms on N.

1. There exists an injective map $\alpha : N \longrightarrow N$; the image $\alpha(a)$ of $a \in N$ is denoted by a^* and is called the successor of a.

2. The successors form a proper subset of N.

3. (Axioms of induction): Let S be any subset of N which contains a non-successor and such that $a \in S \Longrightarrow a^* \in S$. Then $S = N$.

The first principle of Mathematical Induction

Let T_n be a statement concerning natural members n.Assuming that T_1 is true and that the truth of T_r implies the truth of T_{r^*},then T_n is true for every $n \in N$.

Proof

Suppose S is the subset of elements $r \in N$ for which T_r is true.Then $1 \in S$ and $t \in S \Longrightarrow t^* \in S$.So by the induction axioms $S = N$.Hence the result.

Definition:

(a). Define $'+' : N \times N \longrightarrow N$ such that for $m, n \in N, m_n$ satisfies

1. $m + 1 = m^*$

2. $m + n^* = (m + n)^*$ (b). $'.' : N \times N \longrightarrow N$ such that for $m, n \in N, m, n$ satisfies

1. $m.1 = n$

2. $m.n^* = m.n + m$

Theorem: The following laws are satisfied by the $^{(}+^{)}$ and $^{(}.^{)}$ defined on N. For all $m, n, q \in N$,we have

1. $m + n = n + m; mn = nm$ (Commutative law)

2. $m + (n + q) = (m + n) + q; m(nq) = (mn)q$ (associative law)

3. $m + q = n + q \Longrightarrow m = n; mq = nq \Longrightarrow m = n$ (cancelation law)

4. $m.(n + p) = m.n + m.p$ (distributive law)

Thus $(N, +), (N, .)$ are commutative semi groups.

proof.

2. Let m, n be fixed natural numbers and T_q the assertion that $m+(n+q) = (m + n) + q$ for all $q \in N$.Now T_1 is true by the definition above,since $m + (n + 1) = m + n^* = (m + n)^* = (m + n) + 1$

We now assume that T_r is true and show that T_{r^*} holds i.e

$m + (n + r)^* = (m + n) + r^*$.Now by the definition above (a-(2))

$m + (n + r^*) = m + (n + r)^* = (m + (n + r))^*$ and also

$(m+n)+r^* = ((m+n)+r)^*$ so that the truth of T_r implies the truth of T_{r^*}

So, T_r is true for all $n \in N$.

Example:

17 divides $(3 \times 5^{2n+1} + 2^{3n+1})$ for any $n \in N$.

proof

let T_n be the statement that 17 divides $3 \times 5^{2n+1} + 2^{3n=1}$. Obviously T_1 holds since

$3 \times 5^3 + 2^4 = 5^2 \times 17 - 2 \times 17 = 23 \times 17$

Now assume T_r holds .We prove that T_{r+1} holds

$3 \times 5^{2(r+1)+1} + 2^{3(r+1)+1}$

$= 5^2(3 \times 5^{2r+1} + 2^{3r+1}) - 2^{2r+1}(5^2 - 8)$

$= 5^2(3 \times 5^{2r+1} + 2^{3r+1}) - 2^{2r+1}) \times 17$

Since T_r holds,$17/(3 \times 5^{2r=1} + 2^{3r+1})$ and so T_{r+1} holds.

Second principle of Mathematical induction

Let T_r be a statement about a natural number r,if for each r,the truth of T_q for all $q < r$ implies the truth of T_r,then T_n is true for all n.

proof

Let S be the set of natural numbers,such that T_s is not true.If $S \neq \phi$,then by the well-ordering principle (every non-empty subset of N has a first or least element is known as well-ordering principle of N) for N,S has a least element r,say T_r is not true but T_s is true for all $s < r$,contradicting our induction hypothesis. So $S = \phi$. So T_n is true for all $n \in N$.

Integers

Definition: Consider the set $N \times N$,the cartesian product of N by itself. Define a relation on $N \times N$ by $(a, b) \sim (c, d)$ if and only if $a + d = b + c$

Definition: The set I of equivalence classes $[a, b]$ of relation $\sim$ defined above is called the set of integers.

Positive integers

N can be identified with a subset of I as follows:

Define a mapping $\phi : (N, +) \longrightarrow (I, +)$ by $n \longrightarrow [n^*, 1]$.

ϕ is well=defined since $a = b \Longrightarrow a + 1 = b + 1$ i.e $[a^*, 1] = [b^*, 1]$.

ϕ is injective since $[a^*, 1] = [b^*, 1] \Longrightarrow a = b$. So ϕ is an injective homomorphism $N \longrightarrow I$. The elements in the image of N under ϕ are called positive integers.

The Zero integers

For any $a, b \in N$,$[a, a] = [b, b]$ and $[a, b] = [c, b]$ if and only if $c = a$.Also for any $a, c, d \in N$, $[a, a] + [c, d] = [c, d] + [a, a] = [c, d]$.hence $[a, a]$ for any $n \in N$,the zero integer denoted by 0 i.e $[a, a]$ for any $a \in N$ is the identity element of $(I, +)$.

Negative integers

Let I be the set of all $[a, b] \in I$ such that $a < b$. Now for $a, b \in N, [a, b] + [b, a] = [a + b, b + a] = [r, r] = 0$ for any $r \in N$. Thus $[b, a]$ is the additive inverse of $[a, b]$.We denote this element by $-[a, b]$.

Definition: Let $n \in I$. The absolute values of a written $|a|$ is defined by $|a| = \{^{a \quad if \quad a\geq0}_{a \quad if \quad a<0}$

Thus $|a| = 0$ if and only if $a = 0$ and $|a| \in T_=$ if $a \neq 0$.The following laws holds, for $a, b \in I$.

1. $-|a| \leq a \leq |a|$ any $a \in I$

2. $|ab| = |a||b|$

3. $|a| - |b| \leq |a + b| \leq |a| + |b|$

4. $|a| - |b| \leq |a - b| \leq |a| + |b|$.

Divisibility and Primes

Definition: Let b be an integer.An integral divisor or factor of b is an integer a such that $b = ac$ for some integer c. b is also said to be divisible by a or an integral multiple of a. We write $a|b$ if a divides b.If $a|b$ and $0 < a < b$,then a is called a proper divisor of b.

Examples

$4|12$,

$-5|25$

$1| \quad all \quad (integer)$

Theorem: If

1. $a|b$,then $a|bc$ for any integer c

2. If $a|c$ then $a|bx+cy$ for any integers x, y.

3. If $a|b$ and $b|a$,then $a = \pm b$

4. If $a|b$ and $a > 0, b > 0$ then $a \leq b$.

proof

2. $a|b, a|c \Longrightarrow b = ar$ and $c = as$ for some $r, s \in Z$, $bx + cy = arx + asy = a(rx + ry)$

So $a|(bx + cy)$

Definition: An integer p such that $|p| > 1$ is called a prime or a prime number if the only divisor of p are ± 1 and $\pm p$.

$p > 1$ is a prime if there is no divisor d of p such that $1 < d < p$.An integer a which is not a prime is said to be composite.

Example

1. $5, 7, 13$ are primes

2. $24 = 8 \times 3$ is composite.

Theorem: (Division Algorithm)

For any integers $a, b, b > 0$ there exist unique integers q, r such that $a = bq + r, 0 \leq r \leq b$

Proof.

Consider the set $S = \{a - bx | x \in Z \quad and \quad a - bx \geq 0\}$. $S \neq \phi$ since for instance either $a - b|a| \quad or \quad a + b|a| \in S$. By definition of S,either $0 \in S$, in which case 0 is the least element of S or all elements in S are in N in which case S has to contain a least element by well-ordering principle for N.In any case,S must contain a least element $r \geq 0$. Now,by definition of S, $r = a - bq$ for some $q \in Z$ and so,$a = bq + r$,Since $r \geq 0$,we only have to show $r < b$. Suppose $r \geq b$,then $r - b = a = a - bq - b = a - b(q+1) \geq 0$.However,$a - bq - b < a - bq$,contrary our choice of q such that r is the least element in S. So $0 \leq r < b$.

We now show that q, r are unique.Suppose $a = bq + r = bq' + r'$ where $0 \leq r < b$ and $0 \leq r' < b$.Then $b(q' - q) = r - r'$. So $b|(r - r')$. But $|r - r'| < |b|$. So $r - r' = 0$ i.e $r = r'$.Hence $q = q'$ also.

Definition: In the expression $a = bq = r, q$ is called the quotient and r the remainder.

Definition: Let a, b be two integers.A common divisor of a and b is an integer d such that $d|a$ and $d|b$.Suppose that every common divisor of a and b also divides d,then d is called the greatest common divisor or highest common factor of a and b written (g.c.d) or (h.c.f) respectively.

We also write $d = (a, b)$. observe that if d, d' are two gcd's of a, b,then $d' = \pm d$.Therefore a g.c.d of two integers is a non-negative integer .

If $(a, b) = 1$,we say that a and b are relatively prime.

Examples:

1. $(18, 42) = 6$

2. $(15, 7) = 1$.so that 15 and 7 are relatively prime.

Theorem: If a, b be two non-zero integers,then $d = (a, b)$ exists.Moreover $d = ua + vb$ for some integers u, v.In general if $d = (a_1, ..., a_n)$ is the h.c.f of n non-zero integers $\{a_i\}$,then $d = \sum_{i=1}^{n} x_i a - i$ for some integers $x_i \in Z$.

proof.

Let $S = \{xa + yb | x, y \in Z\}$. Then S contains a set T of positive integers and by well-ordering principles T has a least element $d = ua + vb$,say for some belongs to Z. Now $a = qd + r$ for some integers q, r where $0 \leq r < d$. So $r = a - qd = (1 - qu)a + (-qv)b$, so that $r \in S$.Hence $r = 0$ and so $a|a$. Similarly it can be shown that $d|b$.Now suppose any other integer c,say ,divides both a and d. Then $c|ua$ and $c|vb$,so that $c|(ua + vb)$ i.e $c|d$. Therefore $d = ua + vb$ is the h.c.f of a and b.

Example

1. Find $d = (1824, 760)$

Solution

$1824 = 760 \times 2 + 304$

$760 = 304 \times 2 + 152$

$304 = 152 \times 2$

Thus $d = (1824, 760) = 152$

2. Find integers u, v such that $d = ua + vb$ in the example above.

Solution

$152 = 760 - 304 \times 2$

$= 769 - (1824 - 760 \times 2)2$

$= 760 \times 5 - 1824 \times 2$

$= 5b - 2a$

where $a = 1824, b = 760$

So $u = -2, v = 5$

Theorem (**)

1. $(ca, cb) = c(a, b)$ for any positive integer c

2. If $t|a, t|b$ and $t > 0$,then $(\frac{a}{t}, \frac{b}{t}) = \frac{1}{t}(a, b)$

If $d = (a, b)$ then $(\frac{a}{d}, \frac{b}{d}) = 1$

3. $(b, a) = (a, -b) = (a, b + at)$ for any $t \in Z$.

Theorem (***)

If a, b, c are integers and $c|ab, (b, c) = 1$, then $c|a$.

Corollary:

Let p be a prime and $\{a-1, ..., a_n\}$ a set of n integers.If p divides $a_1a_2...a_n$,then p divides at least one of the a_i.

Theorem: Unique factorization theorem or fundamental theorem of Arithmetic:

Every positive integer $n > 1$ can be expressed as a positive prime uniquely,except for the order of prime factors.

proof

We use the second principle of induction.Let T_n be the statement that a given integer $n > 1$ can be expressed as a product of positive primes.

If n is a prime p,then the theorem holds since p is itself a product with only one factor .Otherwise n is composite and therefore has the form $n = ab$ where $a < n, b < n$,Assume that T_r is true for $r < n$,then $a = p_1, ...,_u$, say, and $b = q_1, ..., q_v$ So $n = ab = P_1, ...p_u q_1, ..., q_v$.Thus T_n is true.

We now prove uniqueness. Suppose $n = P_1, ...p_k = q_1, ..., q_j$ are two prime factorizations of n.

Since $P_1|n$,then $P_1|(q_1, ..., q_j)$ and by the corollary above,$P_1|q_j$ for some j.Since both p_1, q_j are primes,we have $P_1 = q_j$.So by cancelation law,we can cancel out P_1, q_j from both sides to have $P_2, ..., p_k = p_1 q_2 ... q_{j-1} q_{j+1} ... q_1$.

If we repeat the process successively with $p_2, p_3, ., .., p_k$ the L.H.S involving the P_i will become 1 and so also with the R.H.S.Hence $l = m$ and every P_i is equal to some q_j.

Corollary: Every integer $n > 1$ can be written in the form $n = P_1^{x_1} ... P_i^{x_i}$ where P_i's are distinct primes and the $\{a_i\}$ are positive integers ≥ 1.

Definition: Let $a_1, ..., a_n$ be non-zero integers.An integer b is called a common multiple of the $\{a_i\}$ if $a_i|b$ for $i = 1, 2, ..., n$. b is called the least common multiple (l.c.m) of the $\{a_i\}$ if b is a common multiple of the $\{a_i\}$ and given any other common multiple c of the $\{a_i\}$,then $b|c$.We denote the l.c.m of the set $\{a_i\}, i = 1, 2, ..., m$ by $[a_1, ..., a_m]$.

For example

l.c.m of 6 and 15 is 30.

Theorem: There are finitely many primes.

Proof.

Suppose there were k of them, say $p_1, ..., p_k$.Consider the integer $1+p_1...p_k = s$.Then $P_i \neq s$ for $i = 1, 2, ..., k$. So if a prime q divides s, q must be distinct from $\{p-i\}$.Now s is either a prime,in which case it is distinct from the p_i,or it is composite, in which case it has a prime factor distinct from the $\}p-i\}$. In either case,we have a prime,different from the $\{p_i\}$,contradicting the fact that there were k of them.So their number must be infinite.

Congruencies

Residue classes: Let m be a fixed integer greater than one, which will be referred to as modulus.Two integers x and y are said to be congruent with regards to the modulus m , or congruent modulo m, if $x - y$ is divisible by m. This is written symbolically as

$$x \equiv y(modm)$$

and is equivalent to the statement that there exists an integer k such that

$$x = y + km$$

For example, $3 \equiv 18(mod5), -2 \equiv 14(mod8), 12 \equiv 0(mod3)$. Any integer whatever is congruent modulo m with precisely one of the integers in the set

$$Z_m = \{0, 1, 2, 3, ..., m-2, m-1\}$$

which is therefore called a complete set of residues modulo m.

Definition: The equivalence classes of R are called the residue classes of R modulo n.If $b \in [a], b$ is called a residue of a modulo n or b is said to be congruent to a modulo n.

A set $T = \{a_1, ..., a_n\}$ of integers is called a complete residue system modulo n if T contains exactly one integer each from the residue classes modulo n. i.e given any $x \in Z$,there exists one and only one a_i such that $x \equiv a_i(modulon)$.

Let m be some fixed positive integer.Let $a, b \in Z$;then we say that a is congruent to b (modulo m) if and only if $a - b$ is divisible by m.i.e for $k \in Z$ we have $a - b = km$.

Example

1. $\{0, 1, 2, 3, ..., n - 1\}$ is a complete residue system $modn$

2. For $n = 7, \{0, 1, 2, 3, 4, 5, 6\}, \{14, 15, 16, ..., 20\}$ are complete residue systems $mod7$.

Theorem: Let a, b, c, d, n be integers.

1. If $a \equiv b(modn)$ and $c \equiv d(modn)$,then $ra + tc \equiv rb + td(modn)$ where r, t are integers.

2. If $a \equiv b(modn)$ and $c \equiv d(modn)$,then $ac \equiv bd(modn)$

3. If $a \equiv b(modn), c/n$ and $c > 0$,then $a \equiv b(modc)$

4. Let $f(x)$ be a polynomial in $Z[x]$,suppose that $a \equiv b(modn)$,then $f(a) \equiv f(b)(modn)$

5. Suppose that $n_1, ..., n_s$ are integers,then $a \equiv b(modn_i)$ for each i,if and

only if $a \equiv b(mod[n_1, ..., n_s])$

Theorem: Let a, c, d, n be integers,$d = (c, n)$.Then $ca \equiv cb(modn)$ if and only if $a \equiv b(mod\frac{n}{d})$.Thus if $d = 1$,then $a \equiv b(modn)$.

Definition: A reduced residue modulo n is a set $V = \{a_1, ...a_s\}$ of integers such that $(a_i, n) = 1$ for each i, a_i does not congruent to $a_j(modn)$ for $i \neq j$ and such that every integer y with $(y, n) = 1$ is congruent modulo n to some members a_i of set V.

Note that if $a \equiv b(modn)$,then $(a, n) \equiv (b, n)$.

Binary operation

The rule by which we combine any two elements of a set to produce a third element is what is we shall call a law of composition or an operation.If any law of composition (*) is such that for all $a, b \in S, a * b$ defines a unique element $c \in S$, we say that the law of composition (*) is closed and (*) is an operation.Clearly $\cap, \cup, \times, +$ are all binary operations which we are familiar with.

Rules of binary operation

1. Closure:

   Let S be a set.An operation * on S is a binary operation if for every pair of elements $a, b \in S.a * b$ is in S.Then S is closed with respect to the binary operation *.

2. Commutative property:

   Let $(S, *)$ be a set S together with a binary operation * on S. The binary operation * on S is said to satisfy the commutative law or property if for every pair a, b in S,$a * b = b * a$

3. Associative property:

   Let $(S, *)$ be a set S together with a binary operation * on S.The binary operation * on S is said to satisfy the associative law or property if for every triple $a, b, c \in S$, $(a * b) * c = a * (b * c)$

   Example:

   1. (a) i $(N, +), (Z, +), (R, +)$ is closed with respect to addition

   ii Addition on N, Z, R is commutative

   iii Addition on N, Z, R is associative

   (b) i $(N, \times), (Z, \times), (R, \times)$ is closed with respect to multiplication

   ii Multiplication on N is commutative

   iii Multiplication on N is associative

   (c) $(N, -), (Z, -), (R, -)$

   (i) N is not closed with respect to subtraction

   e.g $2, 3 \in N$ but $2 - 3 = -1 \notin N$

   Z is closed with respect to subtraction

   R is closed with respect to subtraction

   ii Subtraction on N is not commutative

   e.g $2, 3 \in N$ but $1 = 3 - 2 \neq 2 - 3 = -1$

Likewise subtraction on Z, R is not commutative.

iii Subtraction on N, Z, R is not associative

(d) $(Z^*, \div), Z^* - Z\ \{0\}, (R^*, \div), R^* = R\ \{0\}$

i Z^*, R^* is not closed with respect to division.

ii Division on Z^*, R^* is not commutative.

e.g $2, 3 \in Z^*, R^*$ but $2 \div 3 \neq 3 \div 2$

iii Division on Z^*, R^* is not associative

e.g $2, 3, 5 \in Z^*, R^*$ but $\frac{2}{15} = (2 \div 3) \div 5 \neq 2 \div (3 \div 5) = \frac{10}{3}$

Example 2:

A binary operation $\otimes$ on the set R of real numbers is defined as

$$a \bigotimes b = a + b - 3ab$$

for every pair $a, b \in R$,show that

(a) the operation $\otimes$ on R is commutative

(b) the operation $\otimes$ on R is associative. Solution

(a) Show that $a \bigotimes b = b \bigotimes a$ for every pair $a, b \in R$

$L.H.S = a \bigotimes b = a + b - 3ab = b + a - 3ba = b \bigotimes a = R.H.S$

Hence $\otimes$ on R is commutative.

(b) Show that $(a \bigotimes b) \bigotimes c = a \bigotimes (b \bigotimes c)$ for every $a, b, c \in R$.

$L.H.S = (a + b - 3ab) \bigotimes c$

$= (a + b - 3ab) + c - 3(a + b - 3ab)c$

$= a + b + c - 3ab - 3ac - 3bc + 9abc$

$R.H.S = a \bigotimes (b + c - 3bc)$

$= a + (b + c - 3bc) - 3a(b + c - 3bc)$

$= a + b + c - 3ab - 3ac - 3bc + 9abc$

$= L.H.S$

Hence $\bigotimes$ on R is associative.

4. Identity:

   Let $(S, *)$ be a set S together with a binary operation * on S.If there is an element $e \in S$ such that

   $$e * a = a * e = a$$

   ,for all $a \in S$,then e is called an identity on set S with respect to the binary operation *

5. Inverses:

   Let $(S, *)$ be a set S together with a binary operation * on S,having an identity e.If a and b are elements in S such that

   $$a * b = b * a = e$$

   then a is called the inverse of b and b is called the inverse of a in $(S, *)$.Denote the inverse of a by a^{-1}.Thus $b = a^{-1}$ and $a = b^{-1}$.

   Example:

In $(R, \bigotimes)$ where $a \bigotimes b = a + b - 3ab$ for all $a, b \in R$ determine:

(a) an identity if it exists,

(b) numbers which have an inverses.

Solution

(a) Solve for e,the equation $a \bigotimes e = a$

$\Longrightarrow a + e - 3ae = a$

$\Longrightarrow (1 - 3a)e = 0 \Longrightarrow e = 0$

Hence 0 is the identity in $(R, \bigotimes)$

(b) Given a,solve for b,the equation $a \bigotimes b = 0$

$\Longrightarrow a + b - 3ab = 0$

$\Longrightarrow b(1 - 3a) = -a \Longrightarrow b(3a - 1) = a$

$\Longrightarrow b = \frac{a}{3a-1}$,if $a \neq \frac{1}{3}$

$\Longrightarrow a^{-1} = \frac{a}{3a-1}$,if $a \neq \frac{1}{3}$

Hence all numbers,except $\frac{1}{3}$,have inverses in $(R, \bigotimes)$

6. Distributive law:

Let $(S, *, o)$ be a set S together with two binary operations * and o on S.If for every $a, b, c \in S$,

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

then we say that $*$ is left distributive over o.

If $(aob) * c = (a * c)o(b * c)$ then we say that $*$ is a right distributive over o.

If $*$ is both left distributive and right distributive over o,then $*$ is distributive over o.

Example:

Consider $(R.*, \bigotimes)$ where $a * b = ab$ and $a \bigotimes b = a + b + ab$ for all $a, b \in R$.

(a) Is * distributive over $\bigotimes$?

(b) Is $\bigotimes$ distributive over *?

Solution

(Excersise)

READING LIST:

1. A. O. Kuku Abstract Algebra,1976.

2. W. Ledermann, A. J. Weir, Introduction to group theory,second edition,longman mathematics seried 1996.

3. J. J. Rotman, The theory of groups,Allyn and Bacon series Advanced Mathematics, University of Illinois (consulting editor: Kaplansky I, University of Chicago). 4. J. B. Fraleigh, A first course in Abstract Algebra, 5th edition,University of Rhode Island,Addison-Wesley Publishing company 1993.