KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

LECTURE PLAN
DEPARTMENT OF MATHEMATICS

STAFF NAME: Dr.M.M.SHANMUGAPRIYA
SUBJECT NAME: MODERN ALGEBRA SUB.CODE:15MMU603
SEMESTER: VI CLASS: III B.Sc (MATHEMATICS)

S.No	Lecture Duration Period	Topics to be Covered	Support Material/Page Nos
		UNIT – I	
1.	1	Introduction about set theory	T1: 3-5
2.	1	Basic concepts on sets with examples	T1: 5-7
3.	1	Some general properties on sets	T1: 8-12
4.	1	Mappings- Definition and Types of mappings with example	T1: 19-23
5.	1	Theorems on mapping	T1: 25-29
6.	1	Binary operations-Types of binary operations	T1: 33-35
7.	1	Relations	T1: 37-38
8.	1	Properties of relation in a set	T1: 38-40
9.	1	Equivalence Relation	T1: 40-41
10.	1	Basic concepts on groups	T1: 48-50
11.	1	Some examples on groups	T1: 50-53
12.	1	Definition of abelian and symmetric group with example	R5: 3.6-3.7, 3.12-3.13
13.	1	General properties of groups	T1: 55-57
14.	1	Continuation of general properties on groups	T1: 57-59
15.	1	Examples on groups	T1: 59-61
16.	1	Continuation of examples on groups	T1: 61-65
17.	1	Examples on finite groups	T1: 70-72
18.	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit I =18		
		UNIT – II	
1.	1	Subgroups: Definition and some examples of subgroups	T1: 137-138
2.	1	Theorems on subgroups	T1: 139-143

3.	1	Intersection of subgroups	T1: 145-146
4.	1	Order of an element with example	T1: 113-118
5.	1	Cosets- Theorems on cosets	T1: 152-155
6.	1	Index of a subgroup in a group	T1: 157-159
7.	1	Fermat theorem	T1: 159-162
8.	1	A counting principle- Theorems	R1: 44-46
9.	1	Cyclic group	T1: 170-177
10.	1	Normal subgroup	T1: 188-191
11.	1	Quotient groups	R2: 66-69
12.	1	Theorems on normal subgroups and quotient groups	R5: 3.33-3.36
13.	1	Some examples on normal subgroup.	T1: 191-193
14.		Continuation of examples on normal subgroup	T1: 193-196
15.	1	Some examples on Quotient groups	T1: 205-208
16.	1	Recapitulation and discussion of possible questions .	
	Total No of Hours Planned For Unit II =16		
UNIT –III			
1.	1	Basic concepts on homomorphisms	R2: 51-52
2.	1	Examples of homomorphisms	T1: 211-213
3.	1	Theorems on homomorphisms	T1: 213-216
4.	1	Isomomorphism	R3: 307-308
5.	1	Automorphisms	T1: 221-224
6.	1	Inner automorphisms, Theorems on automorphism	T1: 224-226
7.	1	Cauchy’s theorem for abelian groups	T1: 249-250
8.	1	Cauchy’s theorem	T1: 251
9.	1	Sylow’s theorem for abelian groups	T1: 251-253
10.	1	Examples of Sylow’s theorem	T1: 253
11.	1	Permutation groups	T1: 93-95
12.	1	Some examples of permutation groups	T1: 95-96
13.	1	Theorems on permutation groups	R5: 3.15-3.17
14.	1	Recapitulation and discussion of possible questions .	
	Total No of Hours Planned For Unit III =14		
UNIT-IV			
1.	1	Basic concepts on ring theory	T1: 254
2.	1	Elementary properties of a ring	T1: 255-256
3.	1	Examples of rings	T1: 257-258
4.	1	Some special classes of rings	T1: 259-261
5.	1	Integral domain-Definition and examples	T1: 261-262
6.	1	Fields and Skew Fields	R4: 1-3
7.	1	Theorems on Integral domain and fields	T1: 263-265
8.	1	Homomorphisms of rings- Lemma	T1: 354-356

9.	1	Theorems on Homomorphisms of rings	T1: 356-358
10.	1	Continuation of theorems on Homomorphisms of rings	T1: 358-360
11.	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit IV =11		
UNIT – V			
1.	1	Ideal-Definition and examples	R5: 4.18-4.19
2.	1	Theorems on ideals	R5: 4.19-4.20
3.	1	Quotient rings	R5: 4.20-4.21
4.	1	Maximal ideal	T1: 361-362
5.	1	Theorems on maximal ideals	T1: 364-366
6.	1	Fields of quotients of an integral domain	R5: 4.27-4.28
7.	1	Continuation of fields of quotients of an integral domain	R5: 4.28-4.29
8.	1	Euclidean Rings: Definition and examples	T1: 370-373
9.	1	Properties of Euclidean rings	T1: 373-374
10.	1	Theorems on Euclidean rings	T1: 374-375
11.	1	Continuation of theorems on Euclidean rings	T1: 375-377
12.	1	Unique Factorization theorem	T1: 377-378
13.	1	Recapitulation and discussion of possible questions	
14.	1	Discussion of previous ESE question papers.	
15.	1	Discussion of previous ESE question papers.	
16.	1	Discussion of previous ESE question papers.	
	Total No of Hours Planned For Unit V=16		
	Total No of Hours Planned = 75		

TEXT BOOK:

T1: Vasistha A.R., 2005. Modern Algebra, Krishna Prakasan Mandir, Meerut.

REFERENCES:

R1. Herstein.I.N.,2010. Topics in Algebra, John Wiley &sons, New York.

R2. Artin. M., 2009. Algebra, Prentice-Hall of India, New Delhi.

R3. Fraleigh. J.B., 2004. A First Course in Abstract Algebra, Seventh edition, Pearson Education Ltd, Singapore.

R4. Kenneth Hoffman., 2003. Linear Algebra, Second edition, Prentice Hall of India Pvt Ltd, New Delhi.

R5: Dr.Arumugam.S., and Thangapandi Isaac.,2007. Modern Algebra, SCITECH Publication Pvt. Ltd.

Name of the Faculty Handled: Dr.M.M.Shanmugapriya

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

Semester – VI

		L T P C
15MMU603	**MODERN ALGEBRA**	**5 0 0 5**

Scope: After completing this course, the student will be enriched with the knowledge of concepts of groups, rings and fields etc which are very useful for their future study in accordance with research.

Objectives: To enable the students to understand the concepts of sets,groups ,rings and various properties of those structures.

UNIT I

Sets – Mappings – Binary operations and Relations. Groups – Abelian group, Symmetric Group – Definitions and Examples – Basic properties.

UNIT II

Subgroups – Cyclic subgroup – Index of a group – Order of an element – Fermat theorem –A Counting Principle - Normal Subgroups and Quotient Groups.

UNIT III

Homomorphisms – Cauchy's theorem for Abelian groups – Sylow's theorem for Abeliangroups Automorphisms – Inner automorphism – Cayley's theorem, permutation groups.

UNIT IV

Rings: Definition and Examples –Some Special Classes of Rings – Commutative ring – Field – Integral domain - Homomorphisms of Rings.

UNIT V

Ideals and Quotient Rings – More Ideals and Quotient Rings – Maximal ideal - The field of Quotients of an Integral Domain – Euclidean rings.

TEXT BOOK

1. Vasishtha.A.R., 2005. Modern Algebra, Krishna Prakasam Mandir , Meerut .

REFERENCES

1. Herstein. I.N. 2010.Topics in Algebra, John Wiley & Sons, New York.
2. Artin.M., 2008. Algebra, Pearson Prentice-Hall of India, New Delhi.
3. Fraleigh.J.B., 2004. A First Course in Abstract Algebra , Seventh edition , Pearson Education Ltd, Singapore.
4. Kenneth Hoffman., Ray Kunze., 2003. Linear Algebra, Second edition, Pearson Prentice Hall of India Pvt Ltd, New Delhi.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Class : III B.Sc Mathematics **Semester : VI**

Subject: Modern Algebra **Subject Code: 15MMU603**

Unit I

Part A (20x1=20 Marks)

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
A ------is a collection of well defined objects.	set	function	relation	group	set
The sum of two natural number is also --------- number	real	odd	natural	even	natural
A set consisting of one element is called a ------- set.	singleton	null	equal	sub	singleton
The set which contains no element at all is called the ------ set.	singleton	null	equal	sub	null
The number of power set in S= {a,b,c} is ------------	4	7	9	8	8
If $A\subseteq B$ and $B\subseteq A$ then ----------	A=B	A^1B	A=0	B=0	A=B
If $B\subset A$ then $A\cup B$= --------	A	A'	B		A
If A and B are two sets then $(A\cap B)^1$ = ---------	$A\cap B$	$A'\cap B'$	$A'\cup B'$	$A\cup B$	$A'\cup B'$
If A,B and C are three sets then $A\cap(B\cup C)$ = ---------	$(A\cap B)\cup(A\cap C)$	$(A\cup B)\cap(A\cup C)$	$(A\cap B)\cap(A\cap C)$	$(A\cap B)\cup(A\cup C)$	$(A\cap B)\cup(A\cap C)$

If A,B and C are three sets then A∪ (B∩C) = ---------	(A∩B)∪(A∩C)	(A∪B) ∩ (A∪C)	(A∩B)∩(A∩C)	(A∩B)∪(A∪C)	(A∪B) ∩ (A∪C)
If A,B and C are three sets then A∪ (B∪C) = ---------	(A∩ B)∪C	A∩ (B ∩ C)	A∩(B ∪ C)	(A∪ B)∪C	(A∪ B)∪C
If A,B and C are three sets then (A∩ B) ∩ C = ---------	(A∩ B)∪C	A∩ (B∩C)	(A∪ B)∪C	(A∩ B) ∪ C	A∩ (B∩C)
If B⊂A then A∩B= --------	A	A'	B	φ	B
If a finite set S has n elements, then the power set has ---- elements.	2^n	2^{n+1}	2^{n-1}	2^{n-2}	2^n
If A and B are two sets then $(A∪B)^1$ = ---------	A∩B	A'∩B'	A'∪B'	A∪B	A'∩B'
The symmetric difference of two set A & B is defined by ---------	(A-B)∪(B-A)	(A-B)∩(B-A)	(B-A)∪(A-B)	(B-A)∩(A-B)	(A-B)∪(B-A)
If A and B are two sets, B ⊂A then A∩B =---------------	A	{}	1	B	singleton
One to one mapping is also known as -------------	injective	bijective	surjective	1-1 onto	injective
On to mapping is also known as -------------	injective	bijective	surjective	1-1 onto	surjective
Two sets are said to be ------------- if their intersection is empty.	union	disjoint	difference	superset	disjoint
Two sets A and B are said to ---------- set, if every element of A is an element of B.	equal	infinite	null	singleton	equal
A set consisting of a number of sets is called --------- set.	union	disjoint	power	superset	power
If the range of the function has one element , then the function is ------	onto	one -one	constant	identity	onto

Composition of mapping is not ----------	commutative	equal	well defined	set	commutative
The function f : Z→Z defined by f(x) = 3x is ------	bijection	1-1 and onto	not 1-1 but onto	neither 1-1 nor onto	bijection
The set of natural number is a -------------- group with respect to the operation addition	semi	normal	symmetric	abelian	semi
An infinite group is said to be ---------------order	identity	finite	infinite	symmetric	infinite
If G is a group, then the identity element of G is ----------	zero	two	unique	one	unique
If G is a group, then every a∈G has a --------- inverse in G	zero	two	unique	one	unique
The equivalence relation has -------- distinct equivalence classes.	one	n	n!	no	n
If every element of the group G is its own inverse, then G is --------	abelian	finite	infinite	subgroup	abelian
Two integers a and b are said to be relatively prime , if (a,b) = --------	0	1	2	3	1
A Group G is said to be ---------------- if for every a,b in G ,a.b =b.a	Non-abelian	abelian	unity	inverse	abelian
The number of elements in a finite group is called ------------ of the group	order	infinite	abelian	Non-abelian	order
If G is a group, then the identity element of G is ----------	zero	two	unique	one	unique
For every $a \in G$ $(a^{-1})^{-1}$ = -------	a^{-1}	a	1	0	a
The --------- identity element is also right identity	left	normal	right	coset	left

If s is a set with n elements then A(S) has ------- elements.	one	n	n!	zero	n!
The number of elements in a group is called the -------- of the group	finite	order	semi	symmetric	order
The identity element in a group is ---------	unique	disjoint	symmetric	not equal	unique
The inverse of each element of a group is --------.	symmetric	disjoint	unique	not equal	unique
The --------- element of a group has its own inverse	single	identity	two	no	identity
The left identity element is also ------------ identity	left	normal	right	same	right
The right inverse of an element is ----------- inverse.	left	normal	right	same	left
If a, b $\in$G, then $(a^{-1})^{-1}$----------	a^{-1}	a	1	0	a
If a, b$\in$G, then$(a.b)^{-1}$=-----------	a^{-1}	a^{-1} b^{-1}	$b^{-1}a^{-1}$	b^{-1}	$b^{-1}a^{-1}$
------------- is the binary operation on the set N of natural numbers	Subtraction	Division	Cartesian product	Addition	Addition
The properties of an equivalence relation are ------------.	reflexive, symmetry and transitive	reflexive and transitive	reflexive, anti symmetry and transitive	symmetry and anti transitive	reflexive, symmetry and transitive
One to one on to mapping is also known as -------------	bijective	injective	surjective	transitive	injective
If different elements in A have different f-images in B, then the function is said to be ------	one-one	onto	one-one on to	inverse	one-one
The identity mapping f : A→A is defined by ---------	f(x') = x	f(x) = f(x')	f(x) = x'	f(x)= x	f(x)= x

The relation is said to be a partial order relation if it satisfies ------------.	reflexive, symmetry and transitive	reflexive and transitive	reflexive, anti symmetry and transitive	symmetry and anti transitive	reflexive, anti symmetry and transitive
-----------is a binary operation on the set of natural numbers.	Addition	Subtraction	Division	equation	Addition
If ab = ba , ∀a,b ∈G, then G is said to be ---------group.	symmetric	abelian	sub	semi	abelian
The number of elements in a ---------- group is called the order of the group.	sub	infinite	finite	semi	finite

UNIT-I

SYLLABUS

Sets – Mappings – Binary operations and Relations. Groups – Abelian group, SymmetricGroup – Definitions and Examples – Basic properties.

Introduction to set theory

The algebra of sets defines the properties and laws of sets, the set-theoretic operations of union, intersection, and complementation and the relations of set equality and set inclusion. It also provides systematic procedures for evaluating expressions, and performing calculations, involving these operations and relations.

Preliminary notations:

Set theory:

1. A set is any well defined class or collection of objects.
2. A set 'A' is said to be a subset of s. if every element in A is an element of s. if $a\varepsilon A = a\varepsilon s$.
3. A set is said to be a finite if it consists of a specific number of different elements, otherwise it is called as an infinite set.
4. Two sets A and B are said to be equal if and only if every element of A is an element of B, and also every element of B is an element of A.

   If the two sets A and B are equal then we write it as A=B.

   If the two sets A and B are not equal then we write it as $A \neq B$.
5. A set which contains no element is called as null set or an empty set.
6. A set consisting of a single element is called singleton set.
7. Given a set S we use the notations as,

   $A=\{a\varepsilon s/p(a)\}$ means that A is the set of all the elements in s for which the property p holds

8. The union of the two sets A and B is denoted as AUB the set is {x/xεA or xεB}.
9. The intersection of the two sets A and B is denoted as A∩B is the set {x/xεA and xεB}.
10. The two sets A and B have no elements is then we say that A and B are disjoint or mutually exclusive.

Prepositions:

1. For any 3 sets A,B,C we have

   A∩(BUC)=(A∩B)U(A∩C)

   First we try to prove that

   (A∩B)U(A∩C)ς A∩(BUC)

   Now B ς BUC

   A∩B ς A∩(BUC) ⟶ 1

   c ς BUC

   A∩C ς A∩(BUC) ⟶ 2

   1 and 2 (A∩B)U(A∩C) ς A∩(BUC) ⟶ 3

   Next we try to prove

   A∩(BUC) ς(A∩B)U(A∩C)

   xεA A∩(BUC) ⟶ 4

   Let xεA and (xεB or xεC)

   xεA and xεB or xεA and xεC

   xε A∩B or xε A∩C

$x\varepsilon(A\cap B)U(A\cap C) \longrightarrow 5$

from 4 and 5 $A\cap(BUC) \varsigma (A\cap B)U(A\cap C) \longrightarrow 6$

Definitions:

1. Given a set T we say that T serves as an index set for the family f.f={A_α} of sets if for every $\alpha\varepsilon T$, there is a set of A_α is the family of F.The index set T can be any finite set or infinite.

2. By the union of sets A_α where α is in T, we mean the set {x/xε A_α for atleast one α in T} we denote it by U A_α $\alpha\varepsilon T$.

3. By the intersection of he sets A_α where α is in T we mean that the set { x/xε A_α for every α εT } we denote it by $\cap$ $\alpha\varepsilon T$ A_α.

4. The sets A_α are mutually disjoint if $\alpha\neq\beta$ $A_\alpha\cap A_\beta$ is the null set.

5. Given the two sets A and B then the difdferenc set A-B is the set {xεA/xεB} then B is a subset of A in this case we call A-B is the complement of B in A.

6. Let A and B be any two given sets then their Cartesian product A*B is defined as the set of all ordered pairs(a,b) where aεA and bεB.

Note:

i) $(a_1,b_1)=(a_2,b_2)$ iff $a_1=a_2$ and $b_1=b_2$ given any index set T we can define the Cartesian product of the sets A_α as α varies over T.

ii) If the set A is a finite set having elements then the set A*A is also a finite set but has n^2 elements.

iii) The set of all elements (a,a) is A*A is called the diaponal of A*A.

Definition:

The binary relation ~ on A is said to be a equivalence relation if for all a,b,c is A.

i) a~a reflexing
ii) a~b=b~a symmetry
iii) a~b and b~c=a~c transistivity

Example:

Let s be the set of all integers given a,bεs defines a~b if a-b is even integer.

Solution:

i) since 0=a-a is even a~a

ii) if a~b then a-b is even –(b-a) is also even=b~a.

iii)if a~b then a-b is even and b~c then (b-c) is even.

a-c=(a-b)+(b-c) is also even=a~c.

The given relation is equivalence relation.

Definition:

If A is a set and if ~ is an equivalence relation on A then the equivalence class of aεA is the set {xεA/a~x} we write it as cl(a).

Fundamental theorem on equivalence relation:

Theorem 1.1.1

The distinct equivalence classes of an equivalence relation A provide us with a decomposition of A as a union of mutually disjoint subsets. Conversely given a decomposition of A as union of mutually disjoint, non empty subsets we can define an equivalence relation on A for which these subsets are the distinct equivalence classes.

Proof:

Let the equivalence relation on A be denoted by '~' since for any aεA, a~a.

A must be in cl(a).

Hence the union of the cl(a) is all of A we now try to prove that given two equivalence classes they are either equal or disjoint.

Now we suppose that cl(a) and cl(b) are not disjoint then f an element.

$x\varepsilon cl(a)\cap cl(b)$

Since $x\varepsilon cl(a)$ $a\sim x$

Since $x\varepsilon cl(b)$ $b\sim x$

But by the symmetry of relation we have $x\sim b$.

$a\sim x$ and $x\sim b=a\sim b \longrightarrow 1$

Now we suppose that $y\varepsilon cl(b)$

$b\sim y \longrightarrow 2$

1 and 2 $a\sim y=y\varepsilon cl(a)$.

Every element in cl(b) is in cl(a) $cl(b)\varsigma cl(a) \longrightarrow 3$

In a similar way we can prove that

$Cl(a)\varsigma cl(b) \longrightarrow 4$

3 and 4 cl(a)=cl(b)

Thus we have shown that the distinct cl(a) are either they are equal or disjoint.

Let us suppose that $A=uA_\alpha$ where A_α mutually disjoint non empty set[α is in the some index set]. Given an element a is A is exactly in one A_α.

We define for $a,b\varepsilon A, a\sim b$ if a and b are in the same A_α.

We now prove that this is an equivalence relations on a and that the distinct equivalence classes on the A_α.ˈ.

Now a and a are in the same A_α. $a\sim a$.

Now assume that $a\sim b$, then by definition a and b are in the same A_α.

$b\sim a$ hence if $a\sim b=b\sim a$ then it follows that a and b are in the same A_α.

B and c are in the same A_β.

Now suppose that $A_\alpha \neq A_\beta$ since bε A_β.= $A_\alpha \cap A_\beta \neq 0$

Which is a contradiction. Since A_α and A_β. Are distinct $A_\alpha = A_\beta$. Hence a and c are in the same A_α.

a~c thus a~b and b~c=a~c. thus the relation defined above satisfies reflexity symmetry and transitivity. Hence the above relation is an equivalence relation.

Lat aεA let A_α be the unique no of the partition such that aε A_α then by definition of ~ we get cl(a)= A_α.

Thus distinct equivalence classes are A_α.

State And Prove Demorgan's Theorem:

Statement:

For a subset c of s let $c^{|}$ denotes the complement of c in s. for any two subsets A,B of s we have,

i) $(A\cap B)^{|} = A^{|} \cup B^{|}$ ii) $(A\cup B)^{|} = A^{|} \cap B^{|}$

Proof:

i)let $x\varepsilon(A\cap B)^{|} \longrightarrow 1$

$x\not\varepsilon(A\cap B)$

$x\not\varepsilon A$ and $x\not\varepsilon B$

$x\varepsilon A^{|}$ and $x\varepsilon B^{|}$

$x\varepsilon A^{|} \cup B^{|} \longrightarrow 2$

from 1 and 2 we get $(A\cap B^{|}) \subseteq A^{|} \cup B^{|} \longrightarrow 3$

now let $x\varepsilon A^{|} \cup B^{|} \longrightarrow 4$

$x\varepsilon A^{|}$ or $x\varepsilon B^{|}$

$x \notin A$ or $x \notin B$

$x \notin (A \cap B)$

$x \in (A \cap B)' \longrightarrow 5$

from 4 and 5we get $(A' \cup B') \subseteq (A \cap B)' \longrightarrow 6$

from 3 and 6 we get $(A \cap B)' = (A' \cup B')$

ii)$(A \cup B)' = A' \cap B'$

let $x \in (A \cup B)' \longrightarrow 1$

$x \notin (A \cup B)$

$x \notin A$ and $x \notin B$

$x \in A'$ and $x \in B'$

$x \in A' \cap B' \longrightarrow 2$

from 1 and 2 we get $(A \cup B)' \subseteq A' \cap B' \longrightarrow 3$

now let $x \in A' \cap B' \longrightarrow 4$

$x \in A'$ and $x \in B'$

$x \notin A$ and $x \notin B$

$x \notin A \cup B$

$x \in (A \cup B)' \longrightarrow 5$

from 4 and 5 we get $A' \cap B' \subseteq (A \cup B)' \longrightarrow 6$

from 3 and 6 we get $(A \cup B)' = A' \cap B'$.

Problem:

1. If A is a finite set having n elements then prove that A has exactly 2^n distinct subsets.

Solution:

Given that A is a finite set with n elements

Thus A contains obviously the empty set also that it contains the following subsets.

nc_1=number of 1 element subsets.

nc_2=number of 2 element subsets.

nc_n=number of n element subsets.

The total number of subsets$=nc_0+nc_1+nc_2+\ldots\ldots+nc_n$

$=1+nc_1+nc_2+\ldots\ldots\ldots+1$

From binomial theorem we know that

$(1+x)^n=1+nx+\frac{n(n-1)}{2!}x^2+\ldots\ldots\ldots..+x^n$

When x=1 we have,

$2^n=1+n+\frac{n(n-1)}{2!}+\ldots\ldots\ldots\ldots.+1$

From these both we have the total no of subsets$=2^n$.

Introduction to Mappings

In mathematics, the term mapping, usually shortened to map, refers to either

A function, often with some sort of special structure, or

A morphism in category theory, which generalizes the idea of a function.

Mappings:

A mapping from a set S is a rule that associates with each element s in s a unique element t in T.

Note:

In the above case way that t is the unique of s under the mapping.

Definition:

If S and T are non empty sets then a mapping from s to T is a subset of M of s*t such that for every sεS there is a unique tεT such that the ordered pairs(s, t) is in M.

Note:

Let σ be a mapping from S to T we denote this by σ : ST or T=Sσ.

Examples:

1. Let S be any set. Define i:S $\Longrightarrow$S by s=si for any sets sεs. This mapping I is called the identity mapping.

2. Let S and T be any two sets and let t_0 be an element of T. define ψ:S $\Longrightarrow$T by an ψ(s)=t_0 for every sεs then ψ is a mapping.

3. Let S and T be any two sets. Define τ by (a, b)τ = a for any (a, b)εS*T. this τ is called as the projection of S*T on S. in a similarity we can define the projection of S * T on T.

Note: .

Let S be any set we construct a new set s^*, the set whose elements are the subsets of S then we call S^* the set of subsets of S.

Example:

1. If S={x_1, x_2}

Then s^*= {{}, {x_1}, {x_2}, S}

2.Given a mapping τ: T, we define for tεT, the inverse of t w.r.to τ to be the

set {sεS/t=ST}.

Definition:

1.The mapping τ of S into T is said to be onto T if given tεT, F an element sεS such that t=st.
2. The mapping τ of s into T is said to be a one to one mapping. If whenever $s_1 \neq s_2$ then $s_1\tau \neq s_2\tau$.
3. The two mappings σ and τ of s into T are said to be equal is sσ=sτ for every sεs.
4. If σ:S $\Longrightarrow$ T and τ:T $\Longrightarrow$ U then the composition (or product) of τ andσ is the mapping $\sigma_0\tau$: S$\Longrightarrow$ U.
5. Defined by s($\sigma_0\tau$) =(sσ)τ fro every s ε S
=tτ for every tεT
=u for every uεU.

Example:
Let S = {x_1, x_2, x_3} and T=S.

Let σ : S$\Longrightarrow$S be defined by $x_1\sigma = x_2$, $x_2\sigma = x_3$, $x_3\sigma = x$ and τ : S$\Longrightarrow$S be defined by

$x_1\tau = x_1$, $x_2\tau = x_3$, $x_3\tau = x_2$

thus $x_1(\sigma_0\tau)=(x_1\sigma)\tau$

$= x_2\tau = =x_3$

$X_2(\sigma_0\tau)=(x_2\sigma)\tau$

$= x_3\tau = =x_2$

$X_3(\sigma_0\tau)=(x_3\sigma)\tau$

$= x_1\tau = =x_1$

$x_1(\tau_0\sigma)=(x_1\tau)\sigma$

$= x_2\sigma = =x_2$

$X_2(\tau_0\sigma)=(x_2\tau)\sigma$

$= x_3\sigma = =x_1$

$X_3(\tau_0\sigma)=(x_3\tau)\sigma$

$= x_2\sigma = =x_3$

So from above resets we conclude that is general $\sigma_0\tau \neq \tau_0\sigma$.

Lemma 1.2.1: Associative law:

If σ: S $\Longrightarrow$t, τ : T $\Longrightarrow$U and u: U $\Longrightarrow$V then

$(\sigma_0\tau)_0\mu =\sigma_0(\tau_0\mu)$

Proof:

We know that $\sigma_0\tau$ makes sense and takes S into U.

Thus $(\sigma_0\tau)\,_0\mu$ also makes sense and takes S into V.

Now let us prove for any sεS,

$S[(\sigma_0\tau)_0\mu]=s[\sigma_0(\tau_0\mu)]$

l.h.s $=s[(\sigma_0\tau)_0\mu]$

$=s(\sigma_0\tau)\mu$

$=((s\sigma)\tau)\mu$
$=s\sigma(\tau_0\mu)$

$= s[\sigma_0(\tau_0\mu)]$=r.h.s.= associative property.

Lemma 1.2.2:

Let $\sigma:S \Longrightarrow T$ and $\tau:T \Longrightarrow U$ then

i) $\sigma_0\tau$ is onto if each of σ and τ is onto.

ii) $\sigma_0\tau$ is one to one if each of σ and τ is one to one.

Proof:

Since $\tau: T \Longrightarrow U$ is onto for a given $u \varepsilon U$, F a $t\varepsilon T$ such that

$t\tau=u \longrightarrow 1$

since $\sigma:S \Longrightarrow T$ is onto

for given $t\varepsilon T$ F a $s\varepsilon S$ such that

$s\sigma=t \longrightarrow 2$

now $s(\sigma_0\tau)=(s\sigma)\tau$

$=t\tau$ by 2

$=u$ by 1

Thus for every $u\varepsilon U$ F a $s\varepsilon S$ such that $s(\sigma_0\tau)=u$

Then by definition $\sigma_0\tau$ is onto

Let $s_1, s_2 \varepsilon s$ and $s_1 \neq s_2$

Since σ is one to one $s_1\sigma \neq s_2\sigma$

$s_1\sigma \& s_2\sigma$ are distinct elements in T.

since τ is one to one $s_1\tau \neq s_2\tau$

$= s_1(\sigma_0\tau)=(s_1\sigma)\tau \neq (s_2\sigma)\tau=s_2(\sigma_0\tau)$

$= s_1(\sigma_0\tau) \neq s_2(\sigma_0\tau)$

$=(\sigma_0\tau)$ is one to one by definition.

Note:

The converse of above lemma is false.

i) If$(\sigma_0\tau)$ is onto then σ and τ is need not be onto.

ii) $\sigma_0\tau$ is one to one if each of σ and τ is need not be one to one.

Definition:

Let σ:S T if σ is both one to one and on to then we say the mapping σ is one to one correspondence between S and T.

Lemma 1.2.3:

Statement:

The mapping σ: S $\Longrightarrow$ T is one to one correspondence between S and T iff there exists a mapping μ:T $\Longrightarrow$ S such that $\sigma_0\mu$ and $\mu_0\sigma$ are the identity mappings on S and T respectively.

Proof:

First let us assume that the mapping σ: S $\Longrightarrow$ T is a one to one correspondence between S and T.

Since σ is onto, for given tεT, F an element sεS such that sσ=t $\longrightarrow$ 1

Since σ is one to one this s in must be unique now we define the mapping

σ^{-1}:T $\Longrightarrow$ S by s= t σ^{-1} iff t=sσ the mapping σ^{-1} is the inverse of σ.

Let $\sigma_0\,\sigma^{-1}$: s $\Longrightarrow$ S

Now for any sεS, s ($\sigma_0\,\sigma^{-1}$) = (sσ) σ^{-1}

=t σ^{-1} by 1

= s

=si

$\sigma_0\,\sigma^{-1}$ is the identity mapping on s.

if we take μ= σ^{-1} then

$\sigma_0\mu$ is the identity mapping on s.

Now $\sigma^{-1}{}_0\sigma$: T $\Longrightarrow$ T then for any tεT.

t($\sigma^{-1}{}_0\sigma$)=(tσ^{-1})σ

=sσ

=t

=ti

$\sigma^{-1}{}_0\sigma$ is the identity mapping on T.

Conversely if σ: S $\Longrightarrow$ T is such that F a mapping on μ: T $\Longrightarrow$ S with the property that $\sigma_0\mu$ and $\mu_0\sigma$ are the identity mapping on S and T respectively. Then we have to show that σ is a one to one correspondence between S and T. we have to show σ is both one to one and onto.

Let $t \varepsilon T$ then $t=ti$

$=t\,(\mu_0\sigma)=(t\mu)\sigma$

Now $t\mu$ is an element of S. so t is the image under σ of the element $t\mu$ in s. for a given $t\varepsilon T$ F a $t\mu\varepsilon S$ such that $(t\mu)\,\sigma=t$ by definition σ is onto.

Let $s_1, s_2 \varepsilon S$ assume that $s_1\sigma=s_2\sigma$

Now consider $s_1=s_1(\sigma_0\mu)$

$= (s_1\sigma)\,\mu$

$= (s_2\sigma)\,\mu$

$=s_2\,(\sigma_0\mu)$

$=s_2$ ($\sigma_0\mu$ is the identity on s)

Whenever $s_1\sigma=s_2\sigma=s_1=s_2$

Then by definition σ is one to one.

Definition:

A binary operation 0 on a non empty set A is a mapping which associates each pair (a, b) of elements of A an uniquely defined element $C\varepsilon A$ thus 0 is a mapping of product of the set A*A to A symbolically a map $0: A*A \Longrightarrow A$ is called a binary operation on the set A.

Example:
Addition and multiplication on binary operation on N.
If S is non empty set then A(s) is the set of all one to one mappings of s onto itself.
Theorem: 1.2.1:
If σ, τ, μ are elements of A(S) then i) $\sigma_0\tau$ is in A(S)
ii) $(\sigma_0\tau)\,0\mu=\sigma_0\,(\tau_0\mu)$
iii) F an element I the identity map in A(S) such that $\sigma_0 i=i_0\sigma$
iv)F an element $\sigma^{-1}\varepsilon A(S)$ such that $\sigma_0\sigma^{-1}=\sigma^{-1}0\sigma = i$
Proof:

1.Lemma 1.2.2

2.Lemma 1.2.1

3.Clearly the identity map ‘i’ is both one to and on to $i\varepsilon A(S)$ let $s\varepsilon S$

Now consider $s(\sigma_0 i)=(s\sigma)i$

$=s\sigma$ ¥ $s\varepsilon S=\sigma_0 i=\sigma$

Lemma 1.2.3(write the first part only).

Lemma: 1.2.4:

If s has more than two elements we can find two elements $\sigma*\tau$ in A(S) such that $\sigma_0\tau\neq\tau_0\sigma$.

Proof:

Let us assume that S has more than two elements let x_1, x_2, and x3 be three distinct elements in s.

Now we define $\sigma: S \Longrightarrow S$

By $x_1\sigma=x_2$

$X_2\sigma=x_3$

$X_3\sigma=x_1$

$S\sigma=s$ for only $s\varepsilon S$ different from x_1, x_2, x_3

Define $\tau: S \Longrightarrow S$

By $x_2\tau=x_3$

$x_3\tau=x_2$

and $s\tau=s$ for any $s\varepsilon S$ different from x_2, and x3 clearly both σ and τ are one to one and on to and hence in A(S)

now $x_1(\sigma_0\tau)=(x_1\sigma)\tau$

$=x_2\tau$

$=x_3 \longrightarrow 1$

And $x_1(\tau_0\sigma)=(x_1\tau)\sigma$

$=x_1\sigma$

$=x_2 \longrightarrow 2$

Comparing 1 and 2 we observe that $\sigma_0\tau\neq\tau_0\sigma$.

Problem1:

If the set S has n elements then prove that A(S) has n! Elements.

Solution:

When $S=\{x_1, x_2, x_3...x_n\}$

Any one to one mapping on S onto itself is given by specifying the image of each elements.

The image of x_1 can be chosen is different ways. Since the image of x_2 is different from image of x_1 it can be chosen in n – 1 different ways and so on. Hence the total no of one to one mapping of s onto itself is n(n-1)(n-2)……3.2.1=n!.

Problem2:

If f: $A \Longrightarrow B$ is a map and E_1, E_2 are any two subsets of A then show that

i) $f(E_1UE_2)=f(E_1)Uf(E_2)$

ii) $f(E_1\cap E_2)\varsigma\ f(E_1)\cap f(E_2)$

Solution:

i) Let $b\varepsilon f(E_1UE_2)$

$b=f(a)$ for some $a\varepsilon\ E_1UE_2 \longrightarrow 1$

$b=f(a)$ for some $a\varepsilon E_1$ or $a\varepsilon E_2$

$b=f(a)$ and $f(a)\varepsilon f(E_1)$or $f(a)\varepsilon f(E_2)$

$b=f(a)$ and $f(a)\varepsilon\ f(E_1)U\ f(E_2) \longrightarrow 2$

from 1 and 2 we get $f(E_1UE_2)\varsigma\ f(E_1)Uf(E_2) \longrightarrow 3$

now let $b^{|}\varepsilon f(E_1)Uf(E_2) \longrightarrow 4$

$b^{|}\varepsilon f(E_1)$ or $b^{|}\varepsilon f(E_2)$

$b^{|}=f(a^{|})$ for some $a^{|}\varepsilon E_1$ or E_2

$b^{|}=f(a^{|})$ for some $a^{|}\varepsilon(E_1UE_2)$

$b^{|}=f(a^{|})$ for some $f(a^{|})\varepsilon f(E_1UE_2) \longrightarrow 5$

from 4 and 5 we get $f(E_1)Uf(E_2)\varsigma\ f(E_1UE_2) \longrightarrow 6$

from 3 and 6 we get $f(E_1UE_2)=\ f(E_1)Uf(E_2)$

ii) Let bε $f(E_1 \cap E_2)$ ⟶ 7

bεf(a) for some aε$E_1 \cap E_2$

b=f(a) for some aε E_1 and aε E_2

b=f(a) and f(a)ε$f(E_1)$ and f(a)ε$f(E_2)$

b=f(a) and f(a)ε$f(E_1) \cap f(E_2)$ ⟶ 8

from 7 and 8 we get $f(E_1 \cap E_2)$ς $f(E_1) \cap f(E_2)$

Introduction to Group Theory

In mathematics, a **group** is a set of elements together with an operation that combines any two of its elements to form a third element satisfying four conditions called the group axioms, namely closure, associativity, identity and invertibility. One of the most familiar examples of a group is the set of integers together with the addition operation; the addition of any two integers forms another integer. The abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way, while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics.

Group theory:

Definition of a group:

A non empty set G is called a group if in G there is defined a binary operation called a product and denoted by '.' Such that

i) For a, bεG a.bεG $^{-1}$(closure property)

ii) a,b,cεG a.(b.c)=(a.b).c(associative property)

iii) F an element eεG such that a.e=e.a ¥ aεG e is called the identity of the element in G.

iv) For every aεG F an element a^{-1}εG such that $a.a^{-1}=a^{-1}.a=e$ eixtence of inverse.

The algebra structure of the group is given by (G,.).

Definition:

i) A group G is said to be an abelian group or commutative if for every a,bεG a.b=b.a

ii) A group which is not abelian is called a non abelian group.

iii) The order of a group G, denoted by o(G) is the no of elements in G.

iv) If G contains finite no of elements we say that G is a finite group otherwise it is called as an infinite group.

v) We know that if a set S contains 'n' elements then A(S) contains n! elements amd A(S) is a group. This group is called as the symmetric group of degree n denoted by s_n.

Some examples of groups.

Let G consists of the integers 0, ±1, ±2,…… where we means by a.b foe a,bεG the usually sum of integers that is a.b=a+b.

Solution:

Closure property:

Let a, b εG then a+bεG, since the sum of two integers is also an integer in G.

Associative property:

Let a,b,cεG then (a+b)+c=a+(b+c) since the associative property is true in the case of integers.

Existence of identity elements:

OεG, now a+o=a ¥aεG o is the additive identity element in G.

Existence of inverse element:

For any aεG we can find an element –a in G such that a+(-a)=0

-a acts as the inverse for a in G (G, +) is a group.

Examples:

1. The set of all 2*2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a,b,c,dεR is a group under matrix addition.
2. Q,R,C groups are all under usual addition.
3. Let G consists of real nos (1, -1) under the binary operation multiplication then G is an abelian group of order 2.

4. Since sum of two integers is commutative for any a,bεG a+b=b+a G is an abelian group. Also G contains infinite number of elements. G is an infinite abelian group to the binary operation addition.

Some preliminary lemmas:

Lemma 2.3.1:

If G is a group then

1. The identity element of G is unique.
2. Every aεG has an unique inverse in G.
3. Left and right cancellation laws hold

   a.b=a.c b=c

   b.a=c.a b=c

4. for every aεG $(a^{-1})^{-1}=a$

5. for all aεG$(a.b)^{-1}=b^{-1}.a^{-1}$

Proof:

If possible let there be two I denoted elements e, f in G.

Let aεG since e is the identity. Consider f as an ordinary elements in G. then by the definition,

a.e=e.a=a

f.e=e.f=f

since f is the identity consider e as an ordinary element in G. then by definition

a.f=f.a=a

e.f=f.e=e

we know that e.f=f and e.f=e f=e hence the identity element is unique.

2. let aεG

If possible let there be two inverses $a^{|}$ and $a^{||}$ for a in G. then by definition we know that
$a.a^{|}=a^{|}.a=e$

$a.a^{||}=a^{||}.a=e$

Since e is the identity element we can wriye

$a^{|} = a^{|}.e$

$= a^{|}.(a.a^{|})$

$= (a^{|}.a).a^{||}$

$= e.a^{||}$

$= a^{||}$

$a^{|} = a^{||}$ hence every element in G has a unique inverse.

3.. let a,b,cεG let us suppose that a.b=a.c

Since aεG a^{-1}εG

Now premultiplying by a^{-1} we get

$a^{-1}.(a.b)= a^{-1}.(a.c)$

$(a^{-1}.a).b=(a^{-1}.a).c$

e.b=e.c

b=c

left cancellation law is true.

Since aεG a^{-1}εG now post multiplying by a^{-1} we get

$(b.a). a^{-1}=(c.a). a^{-1}$

$b.(a^{-1}.a)=c.(a^{-1}.a)$

b.e=c.e

right cancellation law is true.

4. let aεG let a^{-1} be the inverse of a in G then $(a^{-1})^{-1}$ will be the inverse of a^{-1} in G.

Since G is a group we have

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

we have $a^{-1}.a= a^{-1}.(a^{-1})^{-1}$

using left cancellation law we have $a=(a^{-1})^{-1}$.

5.. let $a,b \varepsilon G$ let a^{-1}, b^{-1} be the inverse of a and b in G.

Then a.b and $b^{-1}. a^{-1}$ exists in G by closure property

Now we consider

$(a.b).(b^{-1}. a^{-1})=a.(b.b^{-1}). a^{-1}$

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

$=a. a^{-1}$

$=e$

$(a.b)^{-1}=b^{-1}. a^{-1}$

Lemma 2.3.2:
Given a,b in the group G then the equations a.x=b and y.a=b have unique solutions for x and y in G.

Proof:

Given that $a,b \varepsilon G$

Since $a,b \varepsilon G$, $a^{-1} \varepsilon G$

. $x=a^{-1}.b \varepsilon G$

Now consider

$a.x=a.(a^{-1}.b)$

$=(a. a^{-1}).b$

$=e.b$

$=b$

X satisfies the given equation and hence $x=a^{-1}.b$ is a solution.

To establish the uniqueness of the solution, let there be two solution x_1 and x_2 for the equation a.x=b

We have $a.x_1=a.x_2$

$x_1=x_2$

henc $x=a^{-1}.b$ is a unique solution for a.x=b. in a similar way we can prove that $y=b.a^{-1}$ is a unique solution for y.a=b.

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. i) Prove that $A\cap(B\cup C) = (A\cap B) \cup (A\cap C)$

ii) If a finite set S has n elements, then prove that the power set S has 2^n elements.

2. Write about the types of binary operations.

3. If G is a group ,then prove that
i)the identity element of G is unique
ii)every $a\in G$ has a unique inverse in G
iii)for every $a\in G$, $(a^{-1})^{-1} = a$
iv)for all $a,b\in G$, $(a.b)^{-1} = b^{-1}.a^{-1}$

4. If a,b are any two elements of a group G, then prove that the equations $ax = b$ and $ya = b$ have unique solutions in G.

5. Show that the set $G =\{ a+b\sqrt{2}: a,b\in Q\}$ is a group with respect to addition.

6. i) Prove that the inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order.
ii)Show that if every element of the group G is its own inverse , then G is abelian.

7. Let G be a group. Then prove that i) identity element of G is unique
ii) for any $a\in G$, the inverse of a is unique.

8. Prove that if G is an abelian group, then for all $a,b\in G$ and all integers n, $(a.b)^n=a^n.b^n$.

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

10. If a.b.c are any elements of G, then prove that $ab =ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Class : III B.Sc Mathematics **Semester : VI**

Subject: Modern Algebra **Subject Code:**

Unit II

Part A (20x1=20 Marks)

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
Every subgroup of an abelian group is -----------	cyclic	normal	ring	field	normal
Every subgroup of an ---------- group is normal	cyclic	abelian	non- abelian	order	abelian
Every subgroup of a ---------- group is normal	abelian	cyclic	ring	field	cyclic
An infinite group is said to be ---------------order	identity	finite	infinite	symmetric	infinite
If G is a group, then the identity element of G is ----------	zero	two	unique	none	unique
Let H and K be subgroups of a group G, then--------	$H\cup K$ is a subgroup of G	$H\cap K$ is a subgroup of G	H X K is a subgroup of G	HK is a subgroup of G	$H\cap K$ is a subgroup of G
If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)

N(a) is a ------------- of G	coset	subset	normal-subgroup	subgroup	normal-subgroup
If H is a subgroup of G, the -------- of H in G is the number of distinct right cosets of H in G.	ideal	index	coset	congruent	index
If G is a finite group and a∈G the order of 'a' is least positive integer m such that a^m =-------	1	0	e	a	e
If a∈G, then N(a)={x∈G: ax = xa} is called the ---------- of a in G.	normalizer	centralizer	either a or b	none	either a or b
If o(G) = P where p is a prime number then G is -----------	cyclic	abelian	non- abelian	order	cyclic
If H_1 and H_2 are two subgroups of a group G,then ------------ that is also a subgroup of G	$H_1 \cap H_2$	$H_1 \cup H_2$	$H_1 \subset H_2$	$H_1 \supset H_2$	$H_1 \cap H_2$
The ------ of a group G is defined by Z = {z∈G: zx = xz, all x∈G}.	normal subgroup	center	ideal	ring	center
If 'n' is a positive integer and 'a' is relatively prime to 'n' then aφ(n)≡1 mod n.This is called -------theorem	Euler's	Fermat	Lagrange	sylow	Euler's
Any two ------- in a group is either identical (or) disjoint.	left coset	center coset	subgroup	right coset	right coset
Every group is a --------- group of itself.	semi	sub	finite	abelian	sub
Every complex is not always a -------- group.	normal	semi	sub	abelian	sub
Every --------is a subset of itself.	function	relation	group	set	set

The identity of a subgroup is the -------- as that of the group	different	inverse	same	not equal	same
A subgroup other than group G and an element e is called -------- subgroup.	proper	improper	normal	trivial	proper
Improper subgroup is also called--------- subgroup.	proper	quotient	trivial	normal	trivial
The inverse of an element of a subgroup is the --------- as an element of the group.	different	identity	same	not equal	same
The relation of congruency in a group G is an --------- relation.	symmetric	equivalence	partial order	anti symmetric	equivalence
If H is a subgroup of G, a∈G, then Ha={ha: h ϵ H} is called --------- of H in G	left coset	right cancellation	left cancellation	right coset	right coset
If H is a subgroup of G, a∈G then aH={ah: h∈H}is called -------- of H in G.	left coset	right cancellation	left cancellation	right coset	left coset
A nonempty subset H of a group G is said to be ------------- of G H itself forms a group	coset	subset	normal-subgroup	subgroup	subgroup
Any two right cosets are -----------	common	identical	unity	zero	identical
Any two left cosets are -----------	disjoint	equal	unity	zero	disjoint
If H is a subgroup of G, there is a --------- correspondence between any two right cosets of H in G	onto	one-one	one-one onto	one-one into	one-one
The number of distinct right cosets of H in G is -----------	equal	zero	finite	infinite	finite

The number of distinct right cosets of H in G is called----------- of H in G	index	order	cardinal number	finite	index
The order of each subgroup of a -------- group is a divisor of the order of the group.	infinite	finite	normal	semi	finite
If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)
If G is a finite group and $a \in G$ the --------- of 'a' is least positive integer m such that $a^m = e$	coset	subset	order	infinite-order	order
The---------- of each subgroup of a finite group is a divisor of the order of the group	index	order	cardinal number	infinite-order	index
If H is a subgroup of a finite group G, then the index of H in G = --------	o(H)|o(G)	o(G)|o(H)	o(G)	o(H)	o(G)|o(H)
If p is a prime number, then φ(p)= -------	p-1	p+1	p+2	p+3	p-1
The Euler φ function, φ(n) is defined by --------	0	1	2	3	1
A non empty subset H of a group G is said to be a subgroup, if $a \in H, b \in H \Rightarrow$ -------	$ab \in H$	$ba \in H$	$ab^{-1} \in H$	$b^{-1} a \in H$	$ab^{-1} \in H$
If G is a finite group and $a \in G$ the order of a is least positive integer m such that $a^m =$ ------	e	1	0	2	e
If a is congruent to b mod H , then------	$ab \in H$	$ba \in H$	$ab^{-1} \in H$	$b^{-1} a \in H$	$ab^{-1} \in H$
The relation $a \equiv b$ mod H is an ------------- relation.	binary	equivalence	partial order	symmetric	equivalence

If H is any subgroup of G and h∈H, then Hh= ----------	G	h	H	h'	H
If H is any subgroup of G and h∈H, then hH= ----------	G	h	H	h'	H
If a,b are any two elements of a group G and H is any subgroup of G then,Ha=Hb ⇔-------	ab∈H	ba∈H	ab^{-1}∈H	$b^{-1}a$∈H	ab^{-1}∈H
If a,b are any two elements of a group G and H is any subgroup of G then,aH=bH ⇔-------	ab∈H	ba∈H	ab^{-1}∈H	a^{-1} b∈H	a^{-1} b∈H
If G is a finite group of order n and a∈G, then an = -------	1	0	e	a	e
If H, K are subgroup of the abelian group G, then HK is a ---------group of G.	sub	semi	normal	isomorphic	sub
A subgroup N of a group G is said to be ------------- of G if gng^{-1} ∈N	coset	subset	normal-subgroup	subgroup	normal-subgroup
A subgroup N of a group G is said to be normal subgroup of G if--------	gng^{-1}∈G	gng^{-1}∈N	gn∈N	) ng^{-1}∈N	gng^{-1}∈N
If G is a group, N normal subgroup of G then G/N is called -------	quotient group	ring	normal-subgroup	subgroup	quotient group
N(a) is a ------------- of G	coset	subset	normal-subgroup	subgroup	normal-subgroup
A normal subgroup is ---------- with every complex	commutative	equal	unity	zero	commutative
If N is a normal subgroup of G and H is any subgroup of G , then NH is a -------group of G.	normal	sub	semi	abelian	normal

If N is a normal subgroup of G iff gNg^{-1} = -------	g	g^{-1}	N	n	N
The ------------- of any two normal subgroups of a group is a normal subgroup.	intersection	union	addition	subtraction	intersection
The subgroup N of G is a normal subgroup of G iff left coset of N in G is a ------- of N in G	left coset	right coset	normal subgroup	subgroup	right coset

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Class : III B.Sc Mathematics **Semester : VI**

Subject: Modern Algebra **Subject Code:**

Unit II

Part A (20x1=20 Marks)

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
Every subgroup of an abelian group is -----------	cyclic	normal	ring	field	normal
Every subgroup of an ---------- group is normal	cyclic	abelian	non- abelian	order	abelian
Every subgroup of a ---------- group is normal	abelian	cyclic	ring	field	cyclic
An infinite group is said to be ---------------order	identity	finite	infinite	symmetric	infinite
If G is a group, then the identity element of G is ----------	zero	two	unique	none	unique
Let H and K be subgroups of a group G, then--------	$H\cup K$ is a subgroup of G	$H\cap K$ is a subgroup of G	H X K is a subgroup of G	HK is a subgroup of G	$H\cap K$ is a subgroup of G
If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)

N(a) is a ------------- of G	coset	subset	normal-subgroup	subgroup	normal-subgroup
If H is a subgroup of G, the -------- of H in G is the number of distinct right cosets of H in G.	ideal	index	coset	congruent	index
If G is a finite group and $a \in G$ the order of 'a' is least positive integer m such that a^m =-------	1	0	e	a	e
If $a \in G$, then $N(a)=\{x \in G: ax = xa\}$ is called the ---------- of a in G.	normalizer	centralizer	either a or b	none	either a or b
If o(G) = P where p is a prime number then G is -----------	cyclic	abelian	non- abelian	order	cyclic
If H_1 and H_2 are two subgroups of a group G,then ------------ that is also a subgroup of G	$H_1 \cap H_2$	$H_1 \cup H_2$	$H_1 \subset H_2$	$H_1 \supset H_2$	$H_1 \cap H_2$
The ------ of a group G is defined by $Z = \{z \in G: zx = xz$, all $x \in G\}$.	normal subgroup	center	ideal	ring	center
If 'n' is a positive integer and 'a' is relatively prime to 'n' then $a\varphi(n) \equiv 1$ mod n.This is called -------theorem	Euler's	Fermat	Lagrange	sylow	Euler's
Any two ------- in a group is either identical (or) disjoint.	left coset	center coset	subgroup	right coset	right coset
Every group is a --------- group of itself.	semi	sub	finite	abelian	sub
Every complex is not always a -------- group.	normal	semi	sub	abelian	sub
Every --------is a subset of itself.	function	relation	group	set	set

The identity of a subgroup is the -------- as that of the group	different	inverse	same	not equal	same
A subgroup other than group G and an element e is called -------- subgroup.	proper	improper	normal	trivial	proper
Improper subgroup is also called--------- subgroup.	proper	quotient	trivial	normal	trivial
The inverse of an element of a subgroup is the --------- as an element of the group.	different	identity	same	not equal	same
The relation of congruency in a group G is an --------- relation.	symmetric	equivalence	partial order	anti symmetric	equivalence
If H is a subgroup of G, a∈G, then Ha={ha: h ϵ H} is called --------- of H in G	left coset	right cancellation	left cancellation	right coset	right coset
If H is a subgroup of G, a∈G then aH={ah: h∈H}is called -------- of H in G.	left coset	right cancellation	left cancellation	right coset	left coset
A nonempty subset H of a group G is said to be ------------- of G H itself forms a group	coset	subset	normal-subgroup	subgroup	subgroup
Any two right cosets are -----------	common	identical	unity	zero	identical
Any two left cosets are -----------	disjoint	equal	unity	zero	disjoint
If H is a subgroup of G, there is a --------- correspondence between any two right cosets of H in G	onto	one-one	one-one onto	one-one into	one-one
The number of distinct right cosets of H in G is -----------	equal	zero	finite	infinite	finite

The number of distinct right cosets of H in G is called----------- of H in G	index	order	cardinal number	finite	index
The order of each subgroup of a -------- group is a divisor of the order of the group.	infinite	finite	normal	semi	finite
If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)
If G is a finite group and a∈G the --------- of 'a' is least positive integer m such that a^m =e	coset	subset	order	infinite-order	order
The---------- of each subgroup of a finite group is a divisor of the order of the group	index	order	cardinal number	infinite-order	index
If H is a subgroup of a finite group G, then the index of H in G = --------	o(H)|o(G)	o(G)|o(H)	o(G)	o(H)	o(G)|o(H)
If p is a prime number, then φ(p)= -------	p-1	p+1	p+2	p+3	p-1
The Euler φ function, φ(n) is defined by --------	0	1	2	3	1
A non empty subset H of a group G is said to be a subgroup, if a∈H, b∈H⇒ -------	ab∈H	ba∈H	ab^{-1}∈H	b^{-1} a∈H	ab^{-1}∈H
If G is a finite group and a∈G the order of a is least positive integer m such that a^m = ------	e	1	0	2	e
If a is congruent to b mod H , then------	ab∈H	ba∈H	ab^{-1}∈H	b^{-1} a∈H	ab^{-1}∈H
The relation a ≡ b mod H is an ------------- relation.	binary	equivalence	partial order	symmetric	equivalence

If H is any subgroup of G and h∈H, then Hh= ----------	G	h	H	h'	H
If H is any subgroup of G and h∈H, then hH= ----------	G	h	H	h'	H
If a,b are any two elements of a group G and H is any subgroup of G then,Ha=Hb ⇔-------	ab∈H	ba∈H	ab^{-1}∈H	$b^{-1}a$∈H	ab^{-1}∈H
If a,b are any two elements of a group G and H is any subgroup of G then,aH=bH ⇔-------	ab∈H	ba∈H	ab^{-1}∈H	a^{-1} b∈H	a^{-1} b∈H
If G is a finite group of order n and a∈G, then an = -------	1	0	e	a	e
If H, K are subgroup of the abelian group G, then HK is a ---------group of G.	sub	semi	normal	isomorphic	sub
A subgroup N of a group G is said to be ------------- of G if gng^{-1} ∈N	coset	subset	normal-subgroup	subgroup	normal-subgroup
A subgroup N of a group G is said to be normal subgroup of G if--------	gng^{-1}∈G	gng^{-1}∈N	gn∈N	) ng^{-1}∈N	gng^{-1}∈N
If G is a group, N normal subgroup of G then G/N is called -------	quotient group	ring	normal-subgroup	subgroup	quotient group
N(a) is a ------------- of G	coset	subset	normal-subgroup	subgroup	normal-subgroup
A normal subgroup is ---------- with every complex	commutative	equal	unity	zero	commutative
If N is a normal subgroup of G and H is any subgroup of G , then NH is a -------group of G.	normal	sub	semi	abelian	normal

If N is a normal subgroup of G iff gNg^{-1} = -------	g	g^{-1}	N	n	N
The ------------- of any two normal subgroups of a group is a normal subgroup.	intersection	union	addition	subtraction	intersection
The subgroup N of G is a normal subgroup of G iff left coset of N in G is a ------- of N in G	left coset	right coset	normal subgroup	subgroup	right coset

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Class : III B.Sc Mathematics **Semester : VI**

Subject: Modern Algebra **Subject Code: 15MMU603**

Unit III

Part A (20x1=20 Marks)

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
Every permutation can be uniquely expressed as a product of --------- cycles.	disjoint	2	3	m	disjoint
Every permutation is a product of --------- cycles.	disjoint	2	3	m	2
A group is said to be --------- if it has trivial normal subgroup	finite	infinite	simple	subgroup	simple
The product of two disjoint cycles is --------	2 cycles	m cycles	commutative	equal	commutative
A cycle of length --------- is called a transposition.	3	2	1	0	2
Two cycles are said to -------- if they have no symbols in common	disjoint	transposition	2 cycles	m cycles	disjoint
Every transposition is an --------- permutation	even	odd	zero	unit	odd

The inverse of even permutation is ---------- permutation.	odd	even	zero	either odd or even	even
The inverse of odd permutation is ---------- permutation	odd	even	zero	either odd or even	odd
The group Sn has ------ elements.	n!/2	n!/3	n!	(n+1)!	n!/2
A mapping φ from a group G into a group $\overline{G}$ is said to be -------- if for all a , b ϵG, φ(ab)=φ(a)φ(b)	automorphism	isomorphism	homomorphism	endomorphism	homomorphism
A mapping φ from a group G into a group $\overline{G}$ is said to be homoorphism if for all a , bϵG, then φ (ab)= --------	φ(a) φ (b)	φ(a)- φ (b)	φ(a)+ φ(b)	φ(a)/ φ(b)	φ(a) φ (b)
A homomorphism of a group into itself is called --------	automorphism	isomorphism	homomorphism	endomorphism	endomorphism
The Product of two even permutation is ------	odd	even	zero	either odd or even	even
The Product of two odd permutation is ------	odd	even	zero	either odd or even	even
The product of even permutation and odd permutation is ------ permutation.	odd	even	zero	either odd or even	odd
The product of odd permutation and even permutation is ------ permutation	odd	even	zero	either odd or even	odd
If φ(x) = x for every x∈G is a ------------	automorphism	isomorphism	homomorphism	endomorphism	homomorphism
If φ is a homomorphismof G into $\overline{G}$ with kernal K, then K is a -------- group of G.	sub	semi	normal sub	quotient	normal sub

A homomorphism φ from G into $\overline{G}$ is said to be isomorphism if φ is ----	one-to-one	onto	into	one-one onto	one-to-one
Every ------- group having more than two elements has a nontrivial automorphism	infinite	finite	normal	sub	finite
. Every finite group G is --------- to a permutation group.	homomorphic	automorphic	isomorphic	endomorphic	isomorphic
The number of elements in the finite set S is known as the -------- of permutation.	degree	equality	symmetric	product	degree
A ------------ of a group into itself is called endomorphism	automorphism	isomorphism	homomorphism	endomorphism	homomorphism
If φ is a homomorphismof G into $\overline{G}$with ------- K, then K is a normal subgroup of G.	kernal	isomorphism	homomorphism	endomorphism	kernal
Every permutation is the product of its --------.	ring	kernal	group	cycle	cycle
Every ------------- is an odd permutation	cycle	transposition	even permutation	odd permutation	transposition
A --------- of length 2 is called a transposition.	ring	kernal	group	cycle	cycle
A homomorphism φ from G into $\overline{G}$is said to be --------- if φ is one-to-one	automorphism	isomorphism	homomorphism	endomorphism	isomorphism
If φ is a homomorphism of G into $\overline{G}$ then φ(e) =--------	$\overline{e}$	0	1	e	$\overline{e}$
If φ is a homomorphism of G into $\overline{G}$ then φ (x^{-1}) = -------	$(\varphi(x))^{-1}$	φ (x)	x^{-1}	x	$(\varphi(x))^{-1}$

The mapping f : G→G/N is called a ------- mapping.	one-one	onto	natural	into	natural
Every homomorphic image of a group G is ----------- to some quotient group of G.	automorphism	isomorphism	homomorphism	endomorphism	isomorphism
Every homomorphic image of an abelian group is ---------	finite	infinite	normal	abelian	abelian
An isomorphic mapping of a group G onto itself is called ---------	automorphism	isomorphism	homomorphism	endomorphism	automorphism
If G is a group, then A(G), the set of automorphism of G is also a --------	subgroup	group	normal group	semi group	group
Every group is ------------ to a subgroup of A(S) for some appropriate S	isomorphism	automorphic	homomorphic	endomorphic	isomorphism
Every --------- is the product of its cycles.	cyclic group	sub group	semi group	permutation	permutation

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Class : III B.Sc Mathematics Semester : VI

Subject: Modern Algebra Subject Code: 15MMU603

Unit III

Part A (20x1=20 Marks)

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
Every permutation can be uniquely expressed as a product of ---------- cycles.	disjoint	2	3	m	disjoint
Every permutation is a product of --------- cycles.	disjoint	2	3	m	2
A group is said to be --------- if it has trivial normal subgroup	finite	infinite	simple	subgroup	simple
The product of two disjoint cycles is --------	2 cycles	m cycles	commutative	equal	commutative
A cycle of length --------- is called a transposition.	3	2	1	0	2
Two cycles are said to -------- if they have no symbols in common	disjoint	transposition	2 cycles	m cycles	disjoint
Every transposition is an --------- permutation	even	odd	zero	unit	odd

The inverse of even permutation is ---------- permutation.	odd	even	zero	either odd or even	even
The inverse of odd permutation is ---------- permutation	odd	even	zero	either odd or even	odd
The group Sn has ------ elements.	n!/2	n!/3	n!	(n+1)!	n!/2
A mapping φ from a group G into a group $\bar{G}$ is said to be -------- if for all a , b ϵG, φ(ab)=φ(a)φ(b)	automorphism	isomorphism	homomorphism	endomorphism	homomorphism
A mapping φ from a group G into a group $\bar{G}$ is said to be homoorphism if for all a , bϵG, then φ (ab)= --------	φ(a) φ (b)	φ(a)- φ (b)	φ(a)+ φ(b)	φ(a)/ φ(b)	φ(a) φ (b)
A homomorphism of a group into itself is called --------	automorphism	isomorphism	homomorphism	endomorphism	endomorphism
The Product of two even permutation is ------	odd	even	zero	either odd or even	even
The Product of two odd permutation is ------	odd	even	zero	either odd or even	even
The product of even permutation and odd permutation is ------ permutation.	odd	even	zero	either odd or even	odd
The product of odd permutation and even permutation is ------ permutation	odd	even	zero	either odd or even	odd
If φ(x) = x for every x∈G is a ------------	automorphism	isomorphism	homomorphism	endomorphism	homomorphism
If φ is a homomorphismof G into $\bar{G}$ with kernal K, then K is a -------- group of G.	sub	semi	normal sub	quotient	normal sub

A homomorphism φ from G into $\bar{G}$ is said to be isomorphism if φ is ----	one-to-one	onto	into	one-one onto	one-to-one
Every ------- group having more than two elements has a nontrivial automorphism	infinite	finite	normal	sub	finite
. Every finite group G is --------- to a permutation group.	homomorphic	automorphic	isomorphic	endomorphic	isomorphic
The number of elements in the finite set S is known as the -------- of permutation.	degree	equality	symmetric	product	degree
A ------------ of a group into itself is called endomorphism	automorphism	isomorphism	homomorphism	endomorphism	homomorphism
If φ is a homomorphismof G into $\bar{G}$with ------- K, then K is a normal subgroup of G.	kernal	isomorphism	homomorphism	endomorphism	kernal
Every permutation is the product of its --------.	ring	kernal	group	cycle	cycle
Every ------------- is an odd permutation	cycle	transposition	even permutation	odd permutation	transposition
A --------- of length 2 is called a transposition.	ring	kernal	group	cycle	cycle
A homomorphism φ from G into $\bar{G}$is said to be --------- if φ is one-to-one	automorphism	isomorphism	homomorphism	endomorphism	isomorphism
If φ is a homomorphism of G into $\bar{G}$ then φ(e) =--------	$\bar{e}$	0	1	e	$\bar{e}$
If φ is a homomorphism of G into $\bar{G}$ then φ (x^{-1}) = -------	$(\varphi(x))^{-1}$	φ (x)	x^{-1}	x	$(\varphi(x))^{-1}$

The mapping f : G→G/N is called a ------- mapping.	one-one	onto	natural	into	natural
Every homomorphic image of a group G is ----------- to some quotient group of G.	automorphism	isomorphism	homomorphism	endomorphism	isomorphism
Every homomorphic image of an abelian group is ---------	finite	infinite	normal	abelian	abelian
An isomorphic mapping of a group G onto itself is called ---------	automorphism	isomorphism	homomorphism	endomorphism	automorphism
If G is a group, then A(G), the set of automorphism of G is also a --------	subgroup	group	normal group	semi group	group
Every group is ------------ to a subgroup of A(S) for some appropriate S	isomorphism	automorphic	homomorphic	endomorphic	isomorphism
Every --------- is the product of its cycles.	cyclic group	sub group	semi group	permutation	permutation

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Class : III B.Sc Mathematics **Semester : VI**

Subject: Modern Algebra **Subject Code: 15MMU603**

Unit IV

Part A (20x1=20 Marks)

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
A field which has only a finite number of elements is called ------ .	finite field	sub field	skew field	integral domain	finite field
Right distributive law is defined by (b+c).a = -------------	(a.b) -(a.c)	(b.a) + (b.c)	(a.b) / (a.c)	(a.b) *(a.c)	(b.a) + (b.c)
The ring of integers is a ring --------- divisor.	with	equal to	without	not equal to	without
. If R is a ring, for all a, b, c ϵR then a(b-c) = ---------	-ab+bc	ab-bc	ab+bc	ac-bc	ab-bc
. If R is a ring, for all a, b, c ϵ R then a(0) = ---------	a	1	0	∞	0
A ring is called a Boolean ring if -------.	a^2 =e for all a ϵ R, where e is the multiplicative	a^2 =a for all a ϵ R	a^2 =0 for all a ϵ R	a^n =0 for all a ϵ R	a2 =a for all a ϵ R
A ring is called ------ if it is commutative, unit element and without zero divisors.	finite field	sub field	skew field	integral domain	integral domain

The set R consisting of a single element ------ with two binary operations is called zero ring.	1	2	0	∞	0
If φ is a ------------- of R into R' then φ(0)= 0	automorphism	isomorphism	automorphism	homomorphism	homomorphism
If R is a ---------- ring, a≠0∈ R is said to be zero divisor , such that ab= 0	zero	commutative	division	Euclidean ring	commutative
Every ------------- ring of a ring is a homomorphic image of the ring.	quotient	euclidean ring	division	proper	quotient
The ------------- is also known as skew field.	division ring	euclidean ring	sub ring	simple ring	division ring
The product of two non zero element is equal to the ----------- element of the ring.	equal	unit	zero	finite	zero
The product of two non zero integers cannot equal to the ----------- integers.	zero	unit	equal	finite	zero
If R is a commutative ring, a≠0∈ R is said to be zero divisor , such that ab= ---------	1	2	0	∞	0
A commutative ring with unity ------------ is called integral domain	without zero divisors	without zero divisors	zero	identity	without zero divisors
A commutative ring is an ---------- if it has no zero divisors	division ring	field	integral domain	eucledian ring	integral domain
A finite integral domain is a ----------	division ring	field	integral domain	Eucledian ring	field
A --------- is a commutative division ring	division ring	field	integral domain	Eucledian ring	field

A finite commutative ring without zero divisor is a---------.	field	division ring	integral domain	Eucledian ring	field
A ring R is called a --------------ring if all its elements are idempotent	division	boolean	commutative	Eucledian	boolean
Every field is also a ---------- ring.	division	boolean	commutative	Eucledian	division
If in a ring R there is an element 1 in R such that a.1=1.a=a then R is --------	ring with unit element	commutative ring	zero	division ring	ring with unit element
If the multiplication of R such that a.b=b.a then R is --------	ring with unit element	commutative ring	zero	division ring	commutative ring
A ring in which the non zero elements form a group is called a --------	ring with unit element	commutative ring	zero	division ring	division ring
The set R consisting of a single element 0 with two binary operations is called------- ring.	skew field	commutative ring	zero ring	division ring	zero ring
The set I of all integers with two binary operations is called the ring of -------	skew field	commutative	integers	division ring	integers
The product of two integers is also an --------	skew field	commutative	integers	division ring	integers
An element a of a ring R is said to be idempotent if -------	a=1	$a^2=1$	$a^2=a$	$a^2=0$	$a^2=a$
An element a of a ring R is said to be ------------- if $a^2=a$	idempotent	nilpotent	identity	unity	idempotent
A ring is said to be ------------------ if its nonzero elements form a group under multiplication	division ring	field	integral domain	Euclidian ring	division ring

A ring is an algebraic structure with --------- binary operations.	one	two	three	no	two
Left distributive law is defined by a.(b+c) = -------------	(a.b) + (a.c)	(a.b) - (a.c)	(a.b) / (a.c)	(a.b) *(a.c)	(a.b) + (a.c)
If φ is a homomorphism of R into R' then φ(0)= ------	1	2	0	∞	∞
A homomorphism of R into R' is said to be an --------- if it is a one-one mapping	automorphism	isomorphism	endomorphism	kernal	isomorphism
A homomorphism of R into R' is an isomorphism iff I(φ) = -------	1	2	0	∞	0
If φ is a homomorphism of R into R' then φ(-a)= ------	φ(a)	- φ(a)	0	∞	- φ(a)
Every quotient ring of a ring is a --------- image of the ring.	automorphic	isomorphic	automorphic	homomorphic	homomorphic
In a group, the identity element is ------.	unique	different	zero	one	unique
. If R is a ring, for all a, b, c ϵ R then (-a)(-b) = ---------	-ab	ab	a+b	a-b	ab
Division ring is also known as --------	finite field	sub field	skew field	integral domain	skew field

UNIT-IV

SYLLABUS

Rings: Definition and Examples –Some Special Classes of Rings – Commutative ring – Field – Integral domain - Homomorphisms of Rings.

INTRODUCTION TO RING THEORY

In algebra, ring theory is the study of rings—algebraic structures in which addition and multiplication are defined and have similar properties to those operations defined for the integers. Ring theory studies the structure of rings, their representations, or, in different language, modules, special classes of rings (group rings, division rings, universal enveloping algebras), as well as an array of properties that proved to be of interest both within the theory itself and for its applications, such as homological properties and polynomial identities **.**

Definition

A non empty set R is said to be an associative ring if in R these are defined two operations denoted by '+' and '.' Called addition and multiplication respectively such that for all a,b,c ϵR

i. a +b ϵ R
ii. a +b=b+a
iii. a+(b+c)=(a+b)+c
iv. There is an element 0 in R such that a+0=0+a=a ∀ a ϵ R
v. There exist an element –a in R such that a+(-a)=0=(-a)+a
vi. a.b ϵ R
vii. (a.b).c=a.(b.c)
viii. (i) Left Distributive law:

a.(b+c)=a.b+a.c

(ii) Right distributive law:

(b=c).a=b.a=c.a

Definition

A nonempty set R is called a ring, if it has two binary operations called addition denoted by a + b and multiplication denoted by ab for a, b ∈ R satisfying the following axioms: Multiplication is associative, i.e. a(bc) = (ab)c for all a, b, c ∈ R.

Distributive laws hold: a(b + c) = ab + ac and (b + c)a = ba + ca for all a, b, c ∈ R.

Definition

. Let R be a ring.

(1) If multiplication in R is commutative, it is called a commutative ring.

(2) If there is an identity for multiplication, then R is said to have identity.

(3) A nonzero element a ∈ R is said to have a left (resp. right) inverse b if ba = 1 (resp. ab = 1) We say that a is invertible or a unit in R if it has a left and a right inverse.

(4)A commutative division ring is called a field.

(5)An element a of a commutative ring R is called a zerodivisor if there is a nonzero b ∈ R such that ab = 0. An element a ∈ R that is not a zerodivisor is called a nonzerodivisor. If all nonzero elements of a commutative ring are nonzerodivisors, then R is called an integral domain.

(6) A nonempty subset S of a ring R is called a subring of R if S is a ring with respect to addition and multiplication in R.

Example of rings

The set of integers Z, the set of rational numbers Q, the set of real numbers R and the set of complex numbers C are commutative rings with identity.

NOTE

i. In this case we also say that (R,+,.) is a ring
ii. 0 is called the zero element of the ring and it is the additive identity element
iii. If there is an element 1 in R such that a.1=1.a=a ∀ a ϵ R then R is called a ring with unit element.
iv. If for all a,b ϵ R a.b=b.a then R is called a commutative ring

Some Special Classes Of Rings

Definition

If R is a commutative ring then a≠0 ϵ R is said to be a zero-devisor if there exist a,b ϵ R,b≠ 0 such that ab=0

[Eg : define (a1,b1,c1) (a2,b2,c2)=(a1a2,b1b2,c1c2)

(1,2,0) (0,0,7)=(0,0,0)]

Examples

1.Some M is a ring of 2*2 matrices with their elements as integers, the addition and multiplication of matrices being the two ring composition then M is a ring with zero-devisors

2.The ring of integer is a ring without zero-devisors

Definition

A commutative ring is an integral domain if it has no zero devisors

Example : The ring of integers

Definition

A ring is said to be a division ring if its non-zero element form a group under multiplication

Remark

Sometimes a division ring is called a skew field.

Definition

A field is a commutative division ring

Lemma 4.1

If R is ring, then for all a,b ϵ R

1. a.0 = 0.a = 0
2. a(-b)=(-a)b=-(ab)
3. (-a)(-b)=ab

If in addition,R has a unit element 1 then

4. (-1) a =-a
5. (-1)(-1)=1

1) Let a ϵ R then consider

a.0 = a.(0+0)

=a.0+a.0 (L.D.L)

(i.e) a.0=0 = A. + A.0

=> 0 = a.0 (by L.C.L)

Since R is a group under addition we have

a.0 = 0

Similarly we can prove 0.a = 0

Thus we have a.0 = 0.a = 0

2) We shall first show that a(-b) = -(ab)

(i.e) To P.T a(-b) + ab = 0

Now consider, a(-b) + ab = a(-b + b)

=a(0)

= 0 by 1

(i.e) a(-b) + ab = 0

(i.e) a(-b) = -ab

Similarly we can P.T (-a)b = -ab

⇨ a (-b) = (-a)b = -ab

3)Now consider (-a)(-b)

(-a) (-b) = -(a(-b)) by 2

= -(-ab)

=ab

4)Given that R has a unit element 1

By definition 1.a = a.1 = a ~~v~~ a ϵ R

Now consider (-10a = a = (-a) a + 1.a

= (-1 + 1) a

= 0.a = 0

⇨ (-1) a = -a

5)In a proof of fourth result we have,

(-1) a = -a ~~v~~ a ϵ R

If we take a = -1 then we have (-1)(-1) = -(-1)

(-1) (-1) = 1

The Pigeon Hole Principle

Definition

If n objects are distributed over m places and if n > m then some places receives at least two objects.

Equivalently, if n objects are distributed over n places in such a way that no place receive more than one object, then each place receives exactly one object.

Lemma: 4.2

A finite integral domain is a field.

Proof

An integral domain is a commutative ring such that ab=0 if atleast one of a or b is 0.

A field is a commutative ring with unit element in which every non zero element has a multiplicative inverse in the ring.

Let D be the finite integral domain with n elements

In order to show that D is a field we have to P.T

I. There exist an element $1 \in D$ such that

$a.1 = 1.a = a \ \forall \ a \in D$

II. For every element $a \neq 0 \in D \ \exists \ a \ b \in D$ show that ab=1

Let $x_1, x_2 \ldots x_n$ be the n elements of D

Let $a \neq 0 \in D$

Consider the elements,

$x_1a, x_2a, \ldots x_na$ they are in D

we claim that they are all distinct

if possible let us assume that

$x_ia = x_ja$ for $i \neq j$

then $x_ia - x_ja = 0$

$(xi - xj)a = 0$ (R.D.L)

Since D is an integral domain and $a \neq 0$ (by assumption)

We have $xi - xj = 0 \Rightarrow xi - xj$

This is contradiction since $i \neq j$

Our assumption that $xia = xja$ is false

$xia \neq xja$ for $i \neq j$

x1a,x2a…xna are distinct and these n-distinct elements lie in D.

therefore by the pigeon hole principle these elements are the elements of D

if Y ϵ D then y=xia for some xi

in particular since a ϵ D we must have

a=x a for some xi0 ϵ D

since D is commutative we have

a = xi0 a=axi0

we shall P.T xi0 is a unit element for every element of D

now yxi0 = (xi a)xi0

=xi(axi0)

=xi.a

=y

Xi0 is the unit element of D and we write it as 1

xi0=1

Now 1 ϵ D .. a.1 = a ∀ a ϵ D

1 must be of the form xia for some xi ϵ D

1 = xia

∄ a,b ϵ b such that 1 = ba

Ab = ba = 1 => Innverse exist

Thus we proved two conditions

Hence every finite integral domain is a field

Corollary:

If p is a prime no then jp, the ring of integers mod p is a field.

Proof:

Jp has a finite no of elements $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{(p-1)}$ where $\overline{i}$, is the class of integers which give remainder i on division by p.

Then by the above lemma it is enough to prove that jp is an integral domain but we know that jp is a commutative ring. Let a,b ϵ jp and ab = 0 then p must divide a or b

Either a = 0 mod p or b = 0 mod p

(i.e) a = 0 or b = 0

Jp has no zero divisor

By definition jp is a finite integral domain

Hence by the above lemma, jp is a field

NOTE

Let f be an finite field having m elements like jp, by corollary (ii) of lagranges theorem we have $a^{0(f)}$ =e

Under addition we have

$\underbrace{a + a + \ldots}_{\text{m terms}} = 0$

(i.e) ma = 0

Definition

An integral domain D is said to be of characteristic '0' in the relation ma = 0 where $a \neq 0$ is in D and where m is an integer can hold only if m = 0

Example

i. The ring of integers
ii. The ring of even integers
iii. The ring of rationals

Definition

An integral domain D is said to be of finite characteristic if $\exists$ a +ve integer 'm' such that ma = 0 for all $a \in D$

NOTE

1. If D is of finite characteristic then we define the characteristic of D to be the smallest the integer p, S.T $pa = 0 \ \forall a \in D$
2. If D is of finite characteristic then its characteristics is a prime number
3. An integral domain which has an finite characteristics

Definition

An element 'a' of a ring R is said to be Idompotent if $a^2 = a$

A ring R is called a Boolean ring if all elements are idempotent

Homomorphisms

Definition

A mapping from ring R into the ring R is said to be a homomorphism if

i. $\Phi(a + b) = \Phi(a) + \Phi(b)$

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

Lemma 4.3

If Φ is a homo morphism of R into R then

i. $\Phi(0) = 0$

ii. $\Phi(-a) = -\Phi(a)$ for every $a \in R$

Proof

i. Let $a \in R$ then $\Phi(a) \in R$ now $\Phi(a) + 0 = \Phi(a)$

(i.e) $\Phi(a) + 0 = \Phi(a + 0)$

(i.e) $\Phi(a) + 0 = \Phi(a) + \Phi(0)$

$\Rightarrow \Phi(0) = 0$ by L.C.L

ii. From (i) we have $\Phi(0) = 0$

(i.e) $0 = \Phi(o)$

$= \Phi(a + -a)$

$= \Phi(a) + \Phi(-a)$

⇨ $\Phi(-a) = -\Phi(a)$

Hence the proof

NOTE

If both R and R' have the respective unit element as 1 and 1' for their multiplication, it need not follow that $\Phi(1)=1'$

However if R' is a integral domain (or) R' is arbitrary but Φ is onto then $\Phi(1) = 1'$

Definition

If Φ is a homomorphism of R onto R' then the kernel of Φ, denoted by $I(\Phi)$ is the set of all elements $a \in R$ such that Φ9a)=0 where 0 is the zero element of R'.

(i.e) $I(\Phi) = \{ a \in R \,/\, \Phi(a)=0, \text{the zero element of } R' \}$

Lemma : 4.4

If Φ is a homomorphism of R into R' with kernel I(Φ),then

1. I(Φ) is a subgroup of R under addition
2. If a ϵ I(Φ) and r ϵ R then both ar and ra are in I(Φ)

Proof

1. We know that Φ(0) = 0 by lemma3.3.3

0 ϵ I(Φ)

I(Φ) is a non-empty subset of R

Let a,b ϵ I(Φ)

Φ(a) = 0 and Φ(b) = 0

Since Φ is a homomorphism we have,

Φ(a+b) = Φ(a) + v9b)

= 0 + 0

=0

⇨ a+b ϵ I(Φ)

let a ϵ I(Φ)

Φ(a) = 0

But we know Φ(-a) = - Φ(a)

=0

-a ϵ I(Φ) whenever a ϵ I(Φ) then by a lemma I(Φ) is a subgroup of R under addition.

Since a ϵ I(Φ) by definition Φ(a)=0

Now consider Φ(ar)

Φ(ar)= Φ(a). Φ(r)

=0

⇨ ar ϵ I (Φ)

similarly Φ(ra) = Φ (r). Φ(a)

= Φ(r).0

=0

⇨ ra ϵ I(Φ)

Hence if a ϵ I(Φ) and r ϵ R, then both ar and ra are in I(Φ)

Definition

1. A homomorphism of R into r' is said to be an isomorphism if it is a one to one mapping.
2. Two rings are said to be isomorphic if ther is an isomorphism of one onto the other

Lemma:4.5

The homomorphism Φ of R in R' is an isomorphism iff I(v) = {0}

Proof

Let us assume that Φ is an isomorphism of R into R'. then by definition Φ is one to one.

Let a ϵ I(Φ)

Φ(a) = 0 where 0 is the identity element of R'

Φ(a) = Φ(0) [Φ(0)=0]

⇨ a = 0 [ϕ is one to one]

Conversely,

Assume that I(Φ)={0}

It is enough to prove that Φ is one to one.

Let x,y ϵ R

Then $\Phi(x)$, $\Phi(y)$ ϵ R'

Now $\Phi(x) - \Phi(y) = \Phi(x) + \Phi(-y)$

$= \Phi(x - y)$

If $\Phi(x) = \Phi(y)$ then

$\Phi(x) - \Phi(y)=0$

Thus $\Phi(x - y) = 0$

- ⇨ $x - y \; \epsilon \; I(\Phi) = \{0\}$
- ⇨ $x - y = 0$
- ⇨ $x = y$
- ⇨ Φ is one to one

Hence the homomorphism Φ of R into R' is an isomorphism iff I{ Φ}= 0 .

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. If R is a ring, then foe all a,b ∈ R,

   (i) a0 = 0a = 0.

   (ii) a(-b) = (-a)b = -(ab)

   (iii) (-a)(-b) = ab.

   (iv) a(b-c) = ab - ac

2. i) Define Integral domain with example.

   ii) Prove that every finite integral domain is a field.

3. Prove that every field is an integral domain.

4. i) Define field with example.

   ii) Prove that a skew field has no divisors of zero.

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

6. Prove that a ring R has zero divisors iff cancellation law is valid in R.

7. Prove that a finite commutative ring R without zero divisors is a field.

8. Let R and R' be a rings and f:R→R' be an isomorphism. Then prove that
   i) R is commutative ⇒ R' is commutative
   ii) R is ring with identity ⇒ R' is ring with identity
   iii) R is an integral domain⇒ R' is an integral domain
   iv) R is a field⇒ R' is a field

9. Prove that the homomorphism ϕ of a ring into a ring R' is an isomorphism of R into R' iff $I(\phi) = (0)$, where $I(\phi)$ denotes the kernel of ϕ.

10. State and Prove fundamental theorem on homomorphism of rings.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Class : III B.Sc Mathematics **Semester : VI**

Subject: Modern Algebra **Subject Code: 15MMU603**

Unit V

Part A (20x1=20 Marks)

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
Every field is a ----------	field	commutative ring	integral domain	Euclidean ring	Euclidean ring
Any other ---------- of R are called proper ideals.	right	left	prime	ideal	ideal
Every sub ring is not an ---------.	division ring	ideal	group	boolean	ideal
Every subgroup of a cyclic group is -----------	abelian	normal	ring	field	normal
Every cyclic group is -----------	abelian	normal	ring	field	abelian
The ring of integers is a ring --------- divisor.	with	equal to	without	not equal to	without
The product of two integers is also an --------	skew field	commutative	integers	division ring	integers
If R is a commutative ring, then every left ideal will also ------- ideal.	right	left	prime	proper	right
A non empty subset S of a ring R is said to be -------- ideal of R if sr∈S.	right	left	prime	proper	right

Every ideal of a ring R is also a --------- ring of R.	division	boolean	sub	simple	sub
Every subring is not an ---------.	ideal	division ring	group	boolean	ideal
. A non empty subset S of a ring R is said to be -------- ideal of R if rs∊S.	right	left	prime	proper	left
A ring having no proper ideal is --------ring	division	boolean	commutative	simple	simple
Any other ideal of R are called--------- ideals.	right	left	prime	proper	proper
The intersection of any two left ideals of a ring is again --------- ideal of the ring.	right	left	prime	proper	left
Every ------------ can be embedded in the field.	field	commutative ring	integral domain	Euclidian ring	integral domain
A ring of integers is a ------------ ideal ring.	right	left	prime	principal	principal
Every ------- is a principal ideal ring	field	commutative ring	integral domain	Euclidian ring	field
The quotient field of a --------- integral domain coincides with itself.	infinite	finite	single	zero	finite
Any two isomorphic integral domain have -------- quotient field	automorphic	isomorphic	automorphic	homomorphic	isomorphic
A ---------- ring possesses a unit element.	zero	commutative	division	Euclidean ring	commutative
The ring of integers is a --------	field	commutative ring	integral domain	Euclidean ring	Euclidean ring
Every ------- is a Euclidian ring.	field	commutative ring	integral domain	Euclidean ring	field

The set of integer is not an ------ of the ring of rational numbers	division ring	ideal	sub ring	simple ring	ideal
If U is an ideal of the ring R, then R/U is a ring and is a ---------- image of R.	automorphic	isomorphic	automorphic	homomorphic	homomorphic
A -------- has no proper ideals.	right	ideal	prime	field	field
A commutaive ring with unity is a field if it has no ---------- ideals	division	boolean	proper	simple	proper
If R is a commutative ring with unit element and M is an ideal of R, then M is------------ of R iff R/M is a field.	maximal ideal	division ring	integral domain	Eucledian ring	maximal ideal
A ring R can be imbedded in a-------R' if there is an isomorphism of R intoR'.	automorphism	ring	automorphism	kernal	ring
Any two ----------- integral domain have isomorphic quotient field.	automorphic	isomorphic	automorphic	homomorphic	isomorphic
A -------- of integers is a principal ideal ring.	right	left	prime	ring	ring
A commutative ring possesses a -------- element.	zero	unit	prime	ideal	unit
The integral domain of Gausian integers is an ------------.	division ring	euclidean ring	sub ring	simple ring	euclidean ring
If R is a commutative ring with unit element, then a and b are said to be associates if ---------.	a=u+b	a=u/b	a=u-b	a=u.b	a=u.b
If U is an ideal of a ring R with unity, then ---------	U=R	U=0	R=0	U≠R	U=R
The set of integers I is only a ---------- ring.	division	boolean	sub	simple	sub
The set Q of rational numbers is only a ----------	division ring	ideal	sub ring	simple ring	sub ring

The set Q of rational numbers is not an --------------- of the ring of real numbers	division ring	ideal	sub ring	simple ring	ideal
The intersection of any two ideals of a ring is again --------- of the ring	right	ideal	prime	proper	ideal
A field has no ---------- ideals.	right	ideal	prime	proper	proper
A ---------- ring with unity is a field if it has no proper ideals	division	boolean	commutative	simple	commutative
If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R iff R/M is a ----------------	field	division ring	integral domain	Eucledian ring	field
A ring R can be imbedded in a ring R' if there is an ----------- of R intoR'.	automorphism	isomorphism	automorphism	kernal	isomorphism
An integral domain R with unit element is a ---------- ideal ring if every ideal A in R is of the form A = (a) , aϵR.	right	left	prime	principal	principal
. A non empty subset S of a --------R is said to be left ideal of R if rsϵS.	ring	ideal	sub ring	simple ring	ring
Every ------------ is not an ideal.	division ring	sub ring	group	boolean	sub ring
A ring having no proper --------- is simple ring	division	boolean	commutative	ideal	ideal
Any other ideal of R are called--------- ideals.	right	left	prime	proper	proper
The -------------- of any two left ideals of a ring is again left ideal of the ring.	union	intersecton	prime	proper	intersecton
If U is an ideal of a ring R with --------, then U=R	Unity	zero	ideal	ring	Unity
The set Q of rational numbers is not an ideal of the ------- of real numbers	division ring	ring	sub ring	simple ring	ring

The------------- of any two ideals of a ring is again ideal of the ring.	right	intersection	prime	proper	intersection
A commutative ring with identity is a field iff it has no ----------- ideals	division	boolean	proper	simple	proper
A ---------- ring with identity is a field iff it has no proper ideals	division	boolean	commutative	simple	commutative

UNIT-V

SYLLABUS

Ideals and Quotient Rings – More Ideals and Quotient Rings – Maximal ideal - The field of Quotients of an Integral Domain – Euclidean rings.

INTRODUCTION TO IDEALS AND QUOTIENT RINGS

In ring theory, an **ideal** is a special subset of a ring. Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. Addition and subtraction of even numbers preserves evenness, and multiplying an even number by any other integer results in another even number; these closure and absorption properties are the defining properties of an ideal.Among the integers, the ideals correspond one-for-one with the non-negative integers: in this ring, every ideal is a principal ideal consisting of the multiples of a single non-negative number. However, in other rings, the ideals may be distinct from the ring elements, and certain properties of integers, when generalized to rings, attach more naturally to the ideals than to the elements of the ring. For instance, the prime ideals of a ring are analogous to prime numbers, and the Chinese remainder theorem can be generalized to ideals. There is a version of unique prime factorization for the ideals of a Dedekind domain (a type of ring important in number theory). An ideal can be used to construct a quotient ring similarly to the way that modular arithmetic can be defined from integer arithmetic, and also similarly to the way that, in group theory, a normal subgroup can be used to construct a quotient group.

IDEALS AND QUOTIENT RINGS

Definition

If R is any ring then a subset L of R is called a left Ideal of R, if

i. L is a subgroup of R under addition
ii. $r \in R, a \in L \Rightarrow ra \in L$

In a similar way we can define a right ideal

Definition

A non empty subset u of R is said to be a (two sided) ideal of R if

i. u is a subgroup of R under addition
ii. For every u ϵU and r ϵ R, both ur and ru ϵ U

NOTE

i. An ideal is thus simultaneously a left ideal and right ideal of R
ii. Since the ring R is an abelian group w.r.to addition it follows that any ideal U is normal subgroup of r (since any subgroup of an abelian group is normal)
iii. If u is an ideal of the ring R then $\frac{R}{U}$ is a ring and is homomorphic of R

Lemma:5.1

If U is an ideal of R, U is a normal subgroup of R (by note (i))

w.r.to addition $\frac{R}{U}$ is the set of all distinct cosets of U in R, mearly we say that coset and we donot say left coset or right coset. Since R is an abelian group w.r.to addition,

a + U = U + a

$\frac{R}{U}$ consists of all cosets a+u,a ϵ R

From a theorem 2.6.1 we know that $\frac{R}{U}$ is a group under addition (prove here), where the composition law is (a + u) + (b+ u) = (a + b) + U ∀ a,b ϵ R

$\frac{R}{U}$ is also abelian since R is abelian w.r.t.addition. let us define the multiplication in $\frac{R}{U}$ as follows

(a + u) + (b + u) = ab + u ∀ a,b ϵ R

Now we prove, the above said multiplication is well defined

If a + u = a' + u

And b +u = b' + u

Then by our definition of multiplication ,we have to prove that

(a + u) (b + u) =(a’ + u) (b’ + u)

(i.e) to prove that (ab + u) = (a’b’ + u)

Since a + u =a’ + 0

We have

A= a’ + u1 where u1 ϵ u

Similarly since b + u =b’ + u

We have b= b’+u2 where u2 ϵ u

ab= (a’ + u1) (b’ + u2)

=a’b’ + a’u2 +b’u1 + u1u2

Since u is an ideal of R we have

a’u2 + b’u1 and u1u2 ϵ u

a’u2 + b’u1 + u1u2 ϵ U

ab=a’b’ + u3 where u3=a’u2 + b’u1 + u1u2 ϵ u

ab + u =a’b’ + u3 = u

=a’b’ + u

⇨ ab+u =a’b’ = u

The multiplication defined above is well defined now (a + u) (b + u) =ab+u ϵ $\frac{R}{U}$

As a,b ϵ R by closure property ab ϵ u

$\frac{R}{U}$ is closed with respect is multiplication

Since R is associative w.r.to multiplication,

$\frac{R}{U}$ is also associative w.r.to multiplication

Let x,y,z ϵ $\frac{R}{U}$

Then x = a + u

y=b + u

z=c + u where a,b,c ϵ R

now we P.T x(y + z) =xy + xz

L.H.S = x(y + z)

=(a + u) (b + u + c + u)

=(a + u) [(b + c) + u]

=(a(b + c) + u)

=ab + ac + u

=(ab + u) + (ac + u)

=(a + u) (b + u) + (a + u) 9c + u)

=xy + yz

=R.H.S

Similarly we prove that (y + z) x =yx + zy

If R is commutative then $\frac{R}{U}$ is also commutative as seen below,

Consider (a + u) (b + u) = ab + u

=ba + u (R is commutative ab=ba)

=(b + u) (a + u)

$\frac{R}{U}$ is also commutative, if R is commutative

If R has an unit element 1, then $\frac{R}{U}$ has unit element 1 + u

Define a mapping ϕ:R -> $\frac{R}{U}$

By ϕ(a) = a = u for a ϵ R

Let a,b ϵ R

Then ϕ (a + b) = (a + b) + U

=(a + u) + (b + u)

= ϕ (a) + ϕ((b)

And ϕ (ab) = ab + u

=(a + u) (b + u)

Φ (a). ϕ (b)

⇨ by def ϕ is a homomorphism

let y ϵ $\frac{R}{U}$ then y= a + u for a ϵ R and ϕ (a) = a + u = Y

a is the pre image of Y in $\frac{R}{U}$

ϕ is onto

If u ϵ U then ϕ(u) = u + U = u whih is the identity element of $\frac{R}{U}$

The kernel of ϕ is exactly U

Hence the lemma

Remark :

The ring $\frac{R}{U}$ is known as quotient Ring

Theorem 5.1

let R, R' be ring and ϕ a homomorphism of R onto R' with kernel U. then R' is isomorphic

To $\frac{R}{U}$

Moreover there is a one to one correspondence between the set of ideals of R' and the set of ideals of R which contain U. this correspondence can be achieved by associating with an idel W' in R', the ideal W in R defined by

W = { x ϵ R / ϕ (x) ϵ W so defined $\frac{R}{W}$ -> R' by

Ψ (u + a) = ϕ (a) -------- 1

Where u + a is an arbitrary element of $\frac{R}{U}$ and a ϵ R

Let us prove that the mapping is well defined (i.e) to show that U + a = U + b

⇨ ψ(u + a) = ψ(u + b) ∀ u + a, U +b ϵ $\frac{R}{U}$ where a,b ϵ R

let us prove that the mapping is well defined

(i.e) to show that U + a = U + b

=> ψ (u + a) = ψ(U + b) ∀ u +a, U +b ϵ $\frac{R}{U}$ where a,b ϵ R

Now assume that u + a = u + b

Since a =0 = a ϵ u + a ……(o ϵ u)

a ϵ u + a = u +b by an assumption

a = u + b for some u ϵ U

now ψ (u + a) =ϕ(a)

= ϕ(u + b)

=Φ(u) + ϕ(b)

= 0' + ϕ(b)

=ψ (u + b) by 1

ψ is well defined

ψ[(u + a) = (u + b)] = ψ (u + (a+b))

$= \phi(a + b)$

$=\Phi(a) + \phi(b)$

$=\psi (u + a) + \psi (u + b)$

$\psi[(u + a) = (u + b)] = \psi (u + ab)$

$= \phi(ab)$

$=\Phi(a) . \phi(b)$

$=\psi (u + a) \ \psi (u + b)$

Ψ is a homomorphism

Given that ϕ is onto'.

For every r' ϵ R' ∄ ar ϵ R such that $\phi(r) = r'$

$\Psi(u + r) = r'$

U + r is thepre image of r' under ψ

Ψ is onto

Let us now show that ψ is one to one

Now we prove the result by proving that the kernel of ψ namely U_ψ consist of only one element U which is the identity element of $\frac{R}{U}$

By definition of kernel we have,

$U_\psi= \{ U +a \epsilon \frac{R}{U} / \psi(u + a)^{=0'}$the zero element of R'}

$=\{ u + a \epsilon \frac{R}{U} / \phi(a)^{=0'}\}$ by 1

$=\{u\}$ since $\phi(a) =0'$

- ⇨ $a \epsilon u$
- ⇨ $u + a =U$

ψ is one to one

$\psi : \frac{R}{U} \to R'$ is an onto isomorphism

$\frac{R}{U} \sim R'$

(i.e) $R' \sim \frac{R}{U}$ (isomorphism is an equivalence relation)

(ii) Given that W = { x ϵ R / ϕ(x) W'} and W' is an ideal of R'

To prove

U C W and W is an ideal of R

Let x ϵ U

Φ(x) = 0' ϵ W'

⇨ x ϵ W

x ϵ U => x ϵ W

U C W

Now ϕ(0) = 0' ϵ W' (W' is an ideal of R')

Φ(0) ϵ W'

0 ϵ W… W is an non empty subset of R

Let x,y ϵ W,

Φ(x) ϵ W', Φ(y) ϵ W'

Φ(x + y) = Φ(x) + Φ(y) ϵ W' (W' is closed under addition)

⇨ x + y ϵ W whenever x,y ϵ W

let x ϵ W

Φ(x) ϵ w'

Now Φ(-x) = - Φ(x) ϵ W'

Φ(-x) ϵ W'

⇨ -x ϵ W' whenever x ϵ W

Then by a lemma W is a subgroup of R under addition

Next we prove that W is an ideal of R let r ϵ R and x ϵ W

Φ(r) ϵ R' and Φ(x) ϵ W' …. x ϵ R

Xr and rx ϵ R (R is closed under multiplication)

$\Phi(xr) = \Phi(x).\ \Phi(r) \in W'$ (W' is an ideal of R')

$xr \in W$

similarly we can prove that

$rx \in W$ ~~∀~~ $r \in W$, $x \in W$

W is an ideal of R containing U

(i.e) inverse image of an ideal W' of R' is also an ideal W of R containing U

Conversely assume that w is an ideal of R and we prove that w' is an ideal of R'

Define $W'=\{ x' \in R'/ x'=\phi(y), y \in W\}$

Now $0 \in W$ $\phi(0) =0' \in w'$

W' is a non empty subset of R'

Let $x1',x2' \in w'$

$x1'= \phi(y_1)$

$x2'= \phi(y_2)$

$y_1, y_2 \in W$

$x1' + x2'= \phi(y_1)+ \phi(y2)$

$= \phi(y_1+y_2)$

$\in w'$ since $y_1+y_2 \in w$

thus $x_1' + x_2' \in w'$

then $x'= \phi(y)$, $y \in w$

$- y \in w$

$-x' = -\phi(y)$

$= \phi(-y) \in w'$ …..($-y \in w$)

$-x' \in w'$ whenever $x' \in w'$

Then by lemma w' is a subgroup of R' under addition

Let $x' \in w$, $r' \in R'$

Let $r \in R$, $\phi(r)=r'$

$X' = \phi(y)$, $y \in w$

$\phi(yr) = \phi(y). \phi(x)$

$=x'r'$

$yr \in w$ as w is an ideal of R

$\phi(yr) \in w'$

$x'r' \in w'$

Similarly we can prove that $r'x' \in w'$

w' is an ideal of R'

next we prove that the ideal w of R is unique

let T be another ideal of R

$T = \{ y \in R / \phi(y) \in w'\}$

We have to prove that W= T

Let $y \in w$

$\phi(y) \in w'$ (by def of W)

y ϵ T (by def of T)

W C T

Let t ϵ T

ϕ(t) ϵ w'

t ϵ w

T C W

⇨ W = T

Thus W is unique

Thus there is a one to one correspondence between the ideals of R' and the ideals of R containing U

(iii) Now we define a mapping F : R -> $\frac{R'}{W'}$

By F(a) =W' +ϕ(a), a ϵ R

Since ϕ is onto,for every a' ϵ R' ∄ an element a ϵ R s.t ϕ(a) = a'

Now W' + ϕ(a) = W' + a'

= F9a)

A is the pre image of w' + ϕ(a)

F is onto

Let x,y ϵ R

F(x + y) = W' + ϕ(x + y)

=W' + ϕ(x)+ ϕ(y)

==W' + ϕ(x)W'+ ϕ(y)

$=F(x) + F(y) \forall x,y \in R$

We shall show that the kernel of F namely K_F is W

Assume that L is the kernel of F and we prove that W = L

Now by def L = { x ϵ R / F(x) = w'}

Let x ϵ L … F(x) = w'

w'+ ϕ(x)=w'

ϕ(x) ϵ w'

x ϵ w

L C W

Let x ϵ W … ϕ(x) ϵ w'

w'+ ϕ(x)=w'

F(x) = w'

x ϵ L

W C L

Hence w = L

The kernel of F is W and is unique

F is a homo of R onto $\frac{R'}{W'}$ with kernel W

Then by a theorem (2.7.1) $\frac{R}{W}$ is isomorphic to $\frac{R'}{W'}$

$\frac{R}{W} \sim \frac{R'}{W'}$

Lemma 5.2

Let R be a commutative ring with unit element whose only ideas are {0} and R itself ,then R is a field

Proof

In order to prove this result, it is enough if we prove that $\forall$ a $\neq$ 0 ϵ R $\exists$ a b $\neq$ 0 ϵ R s.t

ab = 1

Let a $\neq$ 0 ϵ R

Consider the set Ra = { xa / x ϵ R}

We claim that Ra is an ideal of R

Since 0 = 0.a ϵ Ra

Ra is a non empty subset of R

Let u,v ϵ Ra

Then u = x` a and v = x2a for some x1,x2 ϵ R)

Now u – v = x1a –x2a

= (x1-x2)a

ϵ …[x1-x2 ϵ Ra]

Ra is a subgroup of R under addition

Let r ϵ R let u = xa

Then consider ru = r(xa) = (rx) a ϵ Ra (rx ϵ R)

Similarly we can prove that ur ϵ Ra

By deff Ra is an ideal of R

From the given hypothesis it follows that Ra = { 0} or Ra = R

(i.e) every multiply of R is a multiple of a by some element of R

There exist an element $b \neq 0$ s.T ab=1

R is a field

Definition

An ideal $M \neq R$ in a ring R is said to be a maximal ideal of R, if whenever u is an ideal of R such that M C U C R then either R = U or M = U

In otherwords, an ideal of R is a maximal ideal, if it is impossible to sqneeze an ideal between it and full ring.

NOTE

i. An ring need not have a maximal ideal
ii. Ring in the unit element has maximal idea**ls**

Examples

1) Let R be the ring of integers and U be an ideal of R. since U is a subgroup of R under addition from group theory (eg subgroup of even integers$_0$) we know that U consists of all multiples of a fixed integer say n_0 (i.e) u = (n_0) if P is a prime no we claim that p = (p) is a maximal ideal of R

Proof

If U is an ideal of R and U) R then U = (n_0) for some integer n_0

Since p ϵ P C U , p=m n_0 for some integer m

since p is a prime no,

p = m n_0 => n_0 =1 or n_0 = p

if n_0 =1 then u = (p) = p

U = P

If $n_0 = 1$ then $1 \in U$

Let $r \in R$, then $r = 1.r \in U$ for all $r \in R$

[U is an ideal of R]

$R \subseteq U$

Since u is an ideal other than R (or) P itself between them

P is a maximal ideal of R

2) Let R be the ring of all real valued continous functions on the closed unit interval

Let M = { f(x) ϵ R / f (u2)=0} M is certainly an ideal of R. then M is a maximal ideal of R

Proof

If there is an ideal U of R such that m c u and m ≠ u, then there is a function g(x) ϵ u and g(x) $\notin$ m

Since g(x) $\notin$ m ,g($^1/_2$) = α ≠ 0

Let h(x) = g(x) – α

Now h($^1/_2$)= g($^1/_2$) – α

= α – α

= 0

h(x) ϵ m c u (i.e) h(x) ϵ u

α = g(x) – h(x) ϵ u ….[u is an ideal of r so a subgroup of r]

now $1 = \alpha \alpha^{-1} \in u$

since $\alpha^{-1} = {}^{1}/_{\alpha}$

$= \frac{1}{g(x)-h(x)} \in$ R …………… α^{-1} is continuous and u is an ideal of R

Thus for any t(x) ϵ R we have

t(x) = 1.t(x) ϵ u …[u is an ideal of R]

R $\underline{C}$ U

But U $\underline{C}$ R [u is an ideal of R]

U=R

Thus m is a maximal ideal of R

Theorem 5.2

If R is a commutative ring with unit element and m is an ideal of R then m is a maximal ideal of R iff ${}^{R}/_{M}$ is a field

Proof

Given that m is an ideal of R

Assume that ${}^{R}/_{M}$ is a field

We shall P.T m is a maximal field of R

Since ${}^{R}/_{M}$ is a field , its only ideals are {0} and ${}^{R}/_{M}$

Then by theorem 93.4.1) there I a one to one correspondence between the set of ideals of ${}^{R}/_{M}$ and the set of ideals of R which contain m. the ideal M of R corresponds to the ideal {0} of ${}^{R}/_{M}$ whereas the ideal R of R corresponds to the ideal ${}^{R}/_{M}$ of ${}^{R}/_{M}$' in this one to one correspondence. Thus there is no ideal between m and R other than these two

Hence m is a maximal ideal of R

Conversely assume that m is a maximal ideal of R

Then by the correspondence mentioned above $R/_{M}$ has only {0} and itself an ideals. Further since R is a commutative ring with unit element hen by lemma 3.5.1 , $R/_{M}$ is a field.

Definition .

If all ideals of a ring R are finitely generated then R is called a Noetherian ring.

Theroem 5.3

A commutative ring with identity is Noetherian if and only if given any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, there exists an m such that $I_m = I_{m+i}$ for all $i \geq 0$.

Proof.

Let R be Noetherian. Since $\{I_n\}^{\infty}_{n=1}$ is an ascending chain, I =

$\cup^{\infty}_{n=1} I_n$ is an ideal of R. Hence we can find $a_1, a_2, \ldots, a_g \in$ I such that I = $(a_1, a_2, \ldots, a_g)$. It is easy to see that there is an m such that $a_i \in I_m$ for all i = 1, 2, . . . , g. Hence $I \subseteq I_m$ which implies that $I_m = I_{m+i}$ for all $i \geq 0$.

Conversely let every ascending chain of ideals be stationary. Let I be an ideal of R which is not finitely generated. Then I is nonzero and I < R.

Inductively, we can find $a_1, a_2, \ldots \in$ I such that $I_n = (a_1, a_2, \ldots, a_n)$ and the chain I_n, n = 1, 2, . . . is not stationary. This is a contradiction.

Hence I is finitely generated.

THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

Definition

A ring R can be imbedded in a ring R' if there is an isomorphism of R into R'.

If R and R' have unit elements 1 and 1' we insist in addition that this isomorphism takes 1 and 1'

R' is called an over ring or extension of R . if R can be imbedded in r'

Definition

Let R be an integral domain. A nonzero element a ∈ R is called irreducible if it is not a unit and whenever a = bc then either b or c is a unit. We say a is a prime if (a) is a prime ideal.

Theorem 5.4

Every integral domain can be imbedded in a field

Proof

let d be an integral domain

Let m_o be the set of all ordered pairs(a,b) where a,b ϵ D and b ≠ 0 [consider (a,b) as $\frac{a}{b}$]

In m_o we define a relation '~' as follows

(a,b) ~ (c,d) iff ad = bc -------------------------1

We claim that this is an equivalence reletion on m_o

Let (a,b) , (c,d) , (e,f) ϵ m_o

Since ab= ba

We can write (a,b) ~ (a,b)

(i.e) reflexivity is satisfied

Now let us assume that (a,b) ~ (c,d)

Then by the definition ad=bc

Cb=da (the ring is commutative0

⇨ (c,d) ~ (a,b)

Summary is true

Let (a,b) ~ (c,d) and (c,d) ~ (e,f)

(ie) ad= bc and cf = de

a=$\frac{bc}{d}$ and f=$\frac{de}{c}$

now consider af = $\frac{bc}{d} \cdot \frac{de}{c}$

(i.e) af = be

(i.e) (a,b) ~ (e,f)

(i.e) transitivity is true

Hence the relation '~' defined above is an equivalence relation on m_0

Let [a,b] be the equivalence class of (a,b) in M_0

Let F be the set of all such equivalence classes [a,b] where a,b ϵ D and b ≠ 0

We shall prove that F is a field w.r.to two operations addition and multiplication defined below

[a,b] + [c ,d] = [ad + bc + bd]

[a,b] . [c,d] = [ac,bd]

Since D is an integral domain and both d ≠ 0 and b ≠ 0

We have bd ≠ 0

[ad + bc,bd] ϵ F and

[ac ,bd] ϵ F

We now P.T the addition defined above is well defined

(I.e) if [a,b] = [a', b']

[c,d] = [c',d']

Then we have to prove that

[a,b] +[c,d] = [a',b'] +[c',d']

To p.T

[ad + bc, bd] =(a'd' + b'c', b'd']

(i.e) to P.T

(ad +bc)b'd' = (a'd' + b'c'+ bd

Since [a,b] =[a'b']

We have $\frac{a}{b} = \frac{a'}{b'}$ => ab' = a'b

Similarly [c,d] = [c',d'] $\frac{c}{d} = \frac{c'}{d'}$ => cd' = c'd

Now consider

(ad + bc)b'd' = ad b'd + bcb'd'

=ab'dd' + bb'cd'

=ba'dd' + bbb'dc'

=bd(a'd' = b'c')

Addition defined above well defined

[0,b] acts as a zero element for this addition and [-a,b] is the additive inverse of [a,b]. then we can verify that F is an abelian group under the addition defined above.we can also verify that the non-zero elements of F namely the elements [a,b] , a $\neq$ 0 form an abelian group under multiplication

Here [d,d] acts as the unit element and $[c,d]^{-1}$ =[d,e] { $c \neq 0$, [d,c] is in F}

The distributive laws also hold in F

F is a field

We have to s.t D can be imbedded in F for $x \neq 0$, $y \neq 0$ in D, we note that

[ax,x] =[ay,y]

Let us denote [ax,x] by [a,1]

Define $\phi : D \to F$ by $\phi(a) = [a,1]$ $\forall a \in D$

Let $a,b \in D$

Then $\phi(a + b)= [a + b,1]$

$=[a,1] + [b,1]$

$=\phi(a) + \phi(b)$

Φ is homomorphism of D into F

Let $y \in F$ then $Y=[a,1] \in F, a \in D$ and $\phi(a)=[a,1]=y$

A is the pre image of Y under ϕ

Then by def ϕ is onto.

Now $\phi(a) = \phi(b)$

- $\Rightarrow$ [a,1] =[b,1]
- $\Rightarrow$ a= b

ϕ is onto

ϕ is an homomorphism of D into F

F is the homomorphic image of D under ϕ

If 1 is the unit element of D then $\phi(1) \in F$

Let a' be any element of F then

$\phi(a) = a'$ for some $a \in D$

now consider $\phi(1).a' = \phi(1).\ \phi(a)$

$= \phi(1.a)$

$=\phi(a)$

$=a'$

Also $a'.\ \phi(1)= \phi(a).\ \phi(1)$

$= \phi(a.1)$

$= \phi(a)$

$=a'$

$\phi(1)$ is the unit element of F

thus every integral domain can be imbedded in a field

Definition

Let R be a commutative ring. An ideal P of R is said to be a prime ideal of R. If $ab \in P$, $ab \in R$ => $a \in P$ or $b \in P$

Theorem 5.5

Let R be a commutative ring and S an ideal of R then the ring of residue classes $\frac{R}{S}$ is an integral domain iff S is a prime ideal

Proof

Let R be a commutative ring and S an ideal of R.

Then $\frac{R}{S}$ = { S +a / a ϵ R}

Let S + a, s + b be any two elements of $\frac{R}{S}$

Then ab ϵ R

$\frac{R}{S}$ is also a commutative ring

Now let S be a prime ideal of R

Then we have to prove that $\frac{R}{S}$ is an integral domain

The zero element of $\frac{R}{S}$ is the residue class S itself

Let S + a, S + b ϵ $\frac{R}{S}$

Then (s + a) (s + b) = s

- ⇨ s + ab = s
- ⇨ ab ϵ s
- ⇨ either a or b is in s …(s is a prime ideal)
- ⇨ either s = a =s or s + b = s
- ⇨ either s +a or s + b is the zero element of $\frac{R}{S}$

$\frac{R}{S}$ is without zero divisor

Since $\frac{R}{S}$ is a commutative ring without zero divisor, $\frac{R}{S}$ is a integral domain

Conversely , let $\frac{R}{S}$ be an integral domain then we have to P.T S is an prime ideal of R

Let a,b be any two element in r s.t ab ϵ s

We have ab ϵ s

- ⇨ s + ab = s
- ⇨ (s +a) (s + b) = s

$\frac{R}{S}$ is an integral domain it is without zerp divisor

Either s + a =s or s + b=s

Either a ϵ s or b ϵ s

Then by def s is a prime ideal of R

IMPORTANT RESULTS.

Let R be an integral domain and a, b ∈ R. Then

(1) a is a unit in R if and only if (a) = R.

(2) a and b are associates if and only if (a) = (b)

(3) a | b if and only if (b) ⊂ (a)

(4) a is a proper divisor of b if and only if (b) < (a) < R.

(5) a is irreducible if and only if (a) is maximal among proper principal ideals.

Definition

An integral domain R is called a factorization domain, abbreviated as FD, if every non-zero element of R can be expressed as a product of irreducible elements.

Definition

. A ring R is said to satisfy ascending chain condition
(acc) on principal ideals if for any chain $(a_1) \subset (a_2) \subset \ldots$ of principal ideals of R, there exists an n such that $(a_n) = (a_{n+i})$ for all i = 1, 2, 3, ...

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. i) Define an ideal. Prove that the intersection of any two left ideals of a ring is again a left ideal of the ring.

2. Prove that every integral domain can be imbedded into a field.

3. i) If U is an ideal of a ring R with unity and $1 \in U$, prove that U=R.

   ii) If F is a field then prove that its only ideals are (0) and F itself

4. If R is a commutative ring with unit element and M is an ideal of R, then prove that M is a maximal ideal of R iff $R \vert M$ is a field.

5. Prove that a commutative ring without zero divisor can be imbedded in a field

6. Let R be a commutative ring and S an ideal of R. Then prove that the ring of residue classes R/S is an integral domain iff S is a prime ideal.

7. State and prove unique factorization theorem.

8. Prove that the ring of Gaussian integers is a Euclidean ring.

9. i) Prove that a Euclidian ring possesses a unit element
   ii) Prove that every field is a Euclidean ring.

10.Prove that every euclidean ring is a principal ideal ring.