LOYOLA COLLEGE (AUTONOMOUS) CHENNAI – 600 034

B.Sc. DEGREE EXAMINATION – **MATHEMATICS**

THIRD SEMESTER – **APRIL 2025**

UMT 3501 – ABSTRACT ALGEBRA

Date: 25-04-2025 Dept. No. Max. : 100 Marks

Time: 01:00 PM - 04:00 PM

	SECTION A - K1 (CO1)	
	Answer ALL the Questions	**(10 x 1 = 10)**
1.	**Answer the following**	
a)	When group G is said to be abelian?	
b)	Define index of a subgroup H in a group G.	
c)	Find the inverse of $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 4 & 5 & 2 & 1\end{pmatrix}$.	
d)	When two rings are said to be isomorphic to each other?	
e)	What is a principal ideal ring?	
2.	**Fill in the blanks**	
a)	The set of elements (a, a) in $A \times A$ is called the _____ of $A \times A$.	
b)	If G has no non-trivial subgroups, then G must be finite of _____order.	
c)	An automorphism of a group G is an _____ of G onto itself.	
d)	If m objects are distributed over n places and if $n < m$, then some place receives atleast _____ objects.	
e)	A Euclidean ring possess a _____ element.	
	SECTION A - K2 (CO1)	
	Answer ALL the Questions	**(10 x 1 = 10)**
3.	**Choose the best answer**	
a)	Let G consists of all integers 0, ±1, ±2, … where the binary operation '.' (dot) is the usual sum of integers. Then G is an _____ group. (a) finite (b) infinite abelian (c) symmetric (d) cyclic	
b)	N is a normal subgroup of G if and only if _____ for every $g \in G$. (a) $gNg^{-1} = N$ (b) $gg^{-1} = N$ (c) $gNg^{-1} = e$ (d) $gN = N$	
c)	If φ is a homomorphism of G into $\bar{G}$, then $\varphi(e) =$ _____. (a) e^{-1} (b) $\bar{e}$ (c) e (d) 0	
d)	If U is an ideal of R and $1 \in U$, then _____. (a) $U > R$ (b) $U < R$ (c) $U \neq R$ (d) $U = R$	
e)	Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a _____. (a) Ideal (b) quotient ring (c) field (d) Euclidean ring	
4.	**True or False**	
a)	If a is relatively prime to b and $a \mid bc$ then $a \mid c$.	
b)	If p is a prime number and a is any integer, then $a^p \equiv a \bmod p$.	
c)	The permutation (1 7) (7 6 8) is an even permutation.	
d)	The set of all rational numbers Q under usual addition and multiplication is a commutative ring with unit element.	
e)	One of the first and most famous private key cryptosystems was the shift code used by Julius Caesar.	

SECTION B - K3 (CO2)		
Answer any TWO of the following in 100 words each.		**(2 x 10 = 20)**
5.	If G is a group, then prove the following: (a) the identity of G is unique (b) every $a \in G$ has a unique inverse (c) For every $a \in G$, $(a^{-1})^{-1} = a$ (d) For all $a, b \in G$, $(a.b)^{-1} = b^{-1}a^{-1}$	
6.	(i) Show that the kernel of any homomorphism is a normal subgroup of G.	**(5 marks)**
	(ii) Find the orbits and cycles of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$.	**(5 marks)**
7.	Define an ideal. If R is a ring and U is an ideal of R, then show that R/U is a ring and also that it is a homomorphic image of R.	
8.	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 if and only if R/M is a field.	
SECTION C – K4 (CO3)		
Answer any TWO of the following in 100 words each.		**(2 x 10 = 20)**
9.	If H and K are finite subgroups of a group G, then prove that $o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$.	
10.	Define normal subgroup of a group G. Prove that the subgroup N of G is a normal subgroup of G if and only if every right coset of N in G is a left coset of N in G.	
11.	Is the finite integral domain a field? If so, justify.	
12.	Describe the private key cryptosystem and illustrate with an example.	
SECTION D – K5 (CO4)		
Answer any ONE of the following in 250 words		**(1 x 20 = 20)**
13.	State and prove Lagrange's theorem.	
14.	(i) Prove that every group is isomorphic to a subgroup of $A(S)$ for some appropriate S.	**(12 marks)**
	(ii) How is the set of integers *mod 7* a field under addition and multiplication mod 7?	**(8 marks)**
SECTION E – K6 (CO5)		
Answer any ONE of the following in 250 words		**(1 x 20 = 20)**
15.	Prove the following: (i)The relation congruence modulo n defines an equivalence relation on the set of all integers. (ii) This equivalence relation has n distinct equivalence classes. (iii) If $a \equiv b \ mod \ n$ and $c \equiv d \ mod \ n$, then $a + c \equiv b + d \ mod \ n$ and $ac \equiv bd \ mod \ n$. (iv) If $ab \equiv ac \ mod \ n$ and a is relatively prime to n, then $b \equiv c \ mod \ n$.	
16.	Prove that every non-zero element in a Euclidean ring R can be uniquely written (up to associates) as a product of prime elements or as a unit in R (prove the necessary results).	

$$$$$$$$$$$$