9. (a) State the definitions of a ring homomorphism and a ring isomorphism . Prove that (Z, +, ×) is homomorphic to Z_7 under addition and multiplication modulo 7 by defining an appropriate function from Z onto Z_7 and showing that it is a homomorphism.

(b) Let R be a ring. The centre of R is the set $\{x \in R : ax = xa\}$ for all $a \in R$. Prove that the centre of a ring is a subring.

6 + 6 = 12

B.TECH/CSE/4TH SEM/MATH 2201/2017

NUMBER THEORY AND ALGEBRAIC STRUCTURES (MATH 2201)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) Let G be a group and $a \in G$. If $o(a) = 17$, then $o(a^8)$ is
(a) 17 (b) 16 (c) 8 (d) none of the others.

(ii) In the additive group *(R, +)*, where *R* denotes the set of reals, $(2.5)^0$ =
(a) 1 (b) 0 (c) -1 (d) 2.5.

(iii) In the additive group Z_6 = {[0], [1], [2], [3], [4], [5]} under addition, the order of the element [4] is
(a) 0 (b) 2 (c) 3 (d) 6.

(iv) The remainder in the division of $1! + 2! + 3! + 4! + \cdots + 100!$ by 4 is
(a) 0 (b) 1 (c) 2 (d) 3.

(v) In the field Z_{11} = {[0], [1], [2], ..., [10]}, under addition and multiplication modulo 11, the multiplicative inverse of [8] is
(a) [3] (b) [9] (c) [7] (d) [5].

(vi) A divisor of zero in Z_9 = {[0], [1], ..., [8]} under addition and multiplication modulo 9 is
(a) [3] (b) [7] (c) [2] (d) [5].

(vii) Which of the following permutations is cyclic?
(a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
(c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

(viii) In a lattice (L, $\wedge$, $\vee$), the dual of the statement $(a \wedge b) \vee a = a \wedge (b \vee a)$ is
(a) $(a \wedge b) \wedge a = a \wedge (b \wedge a)$ (b) $(a \vee b) \vee a = a \vee (b \vee a)$
(c) $(a \wedge b) \vee a = a \vee (b \vee a)$ (d) none of these.

(ix) $H = \{1, -1\}$ is a multiplicative subgroup of $G = \{1, -1, i, -1\}$. Then the index of H in G is
(a) 1 (b) 2 (c) 3 (d) 4.

(x) In the set $S = \{1, 2, 3, 4, 6, 9\}$, R is defined as follows : $a\,R\,b$ if b is a multiple of a. Then
(a) 3 and 4 are comparable (b) 9 succeeds 3
(c) 3 succeeds 9 (d) 4 and 6 are comparable.

Group – B

2. (a) Solve the following set of simultaneous congruences by using the Chinese Remainder Theorem

$$x \equiv 5 \pmod{11}$$
$$x \equiv 14 \pmod{29}$$
$$x \equiv 15 \pmod{31}$$

(b) State the definition of a primitive root of a prime number p. Find all the primitive roots of p = 11 and p = 17. Show your calculations in detail.

6 + 6 = 12

3. (a) Use the Euclidean algorithm to find the greatest common divisor of 522 and 332 and express it as $522x + 332y$, where x and y are integers.

(b) Let S be a set and $P(S)$ be its power set, i.e., set of all subsets of S. Prove that $P(S)$ is a lattice with respect to the operations $\cap$ (intersection) and $\cup$ (union).

6 + 6 = 12

Group – C

4. (a) Show that the set $G = \{a + b\sqrt{2} : a, b \in Q\}$ is a group with respect to addition, where Q denotes the set of rationals.

(b) Either prove the following statements or give counter-examples:
(i) Every binary operation on a set consisting of a single element is both commutative and associative.
(ii) Every commutative binary operation on a set having just two elements is associative.

(c) Prove that in a group G, for all a, b in G, the equation $ax = b$ has a unique solution in G.

4 + (2 + 2) + 4 = 12

5. (a) Show that the set S_3 of all permutations on three symbols 1, 2, 3 forms a finite non-abelian group of order 6 with respect to the usual 'composition' operation.

(b) Find a solution of the equation $ax = b$ in S_3, where $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

(c) Let G be a group with finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.

6 + 3 + 3 = 12

Group – D

6. (a) State and prove Lagrange's Theorem regarding the order of a subgroup of a finite group.

(b) If in a group G, $a^5 = e$ and $aba^{-1} = b^2$ for all a, b in G, find the order of b.

6 + 6 = 12

7. (a) Let G be a finite group and $a \in G$. Prove that $a^{o(G)} = e$. Hence prove Fermat's Little Theorem.

(b) Let H be a subgroup of a group G such that $[G : H] = 2$. Then prove that H is a normal subgroup of G.

6 + 6 = 12

Group – E

8. (a) Prove that $\mathbb{Z}_{11}$, the ring of all integers modulo 11, is a field. State any theorem that you use. Find the multiplicative inverses of all the non-zero elements of $\mathbb{Z}_{11}$. Show your calculations.

(b) State the definition of the characteristic of a ring. Prove that the characteristic of an integral domain is 0 or a prime number.

6 + 6 = 12