NUMBER THEORY & 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) If the cyclic group G contains 12 distinct elements then the number of possible generators of the group is
(a) 1 (b) 2 (c) 3 (d) 4

(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 number of generators of an infinite cyclic group is
(a) 1 (b) 2 (c) 0 (d) infinite.

(v) Index of a subgroup is 5 and its order is 3. The order of the group is
(a) 8 (b) 10 (c) 15 (d) none.

(vi) 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]

(vii) 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]

(viii) The remainder in the division of 1!+2!+3!+......+100! by 5 is
(a) 1 (b) 2 (c) 3 (d) 4.

(ix) 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.

(x) 30! is congruent modulo 31 to
(a) 20 (b) 15 (c) 10 (d) 30.

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) State the definition of a partially ordered set. Let *S={1,2,3,4,8,9,16,27}* and let *'a/b'* mean that *a* is a divisor of b. Check that *(S,/)* is a partially ordered set. Draw its Hasse diagram.

(b) Let N be the set of all positive integers. $\wedge$ and $\vee$ are defined as $a \wedge b$= HCF of *a* and *b*, $a \vee b$=LCM of *a* and *b*. Prove that (N, $\wedge, \vee$) is a lattice.

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) Prove that a group is abelian if and only if $(ab)^{-1}=a^{-1}b^{-1}$, for all *a,b* in *G*.

(b) Prove that the number of even permutations on a finite set (containing at least two elements) is equal to the number of odd permutations on it.

6 + 6 = 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) Prove that every group of prime order is cyclic.

(b) Prove that the intersection of any two normal subgroups of a group is a normal subgroup. Is the same true for the union? Justify.

6 + (4 + 2) = 12

Group – E

8. (a) Let $Z[\sqrt{5}]=\{a+b\sqrt{5}:a,b\in Z\}$. Prove that $Z[\sqrt{5}]$ is a ring under the ordinary addition and multiplication of real numbers.

(b) Prove that for every prime p, Z_p, the ring of integers modulo p, is a field. State any theorem that you use.

6 + 6 = 12

9. (a) State the definitions of a ring homomorphism and a ring isomorphism. Prove that $(Z,+,\times)$ 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

Note:

1. **Students having backlog in MATH2201 (old syllabus) and if not joined in any Google classroom for this paper code yet, are advised to follow both Step-I and Step-II as mentioned below in order to submit the answer-scripts properly.**
2. **Students who have already joined any Google Classroom for MATH2201 (old syllabus) can directly go to Step-II as mentioned below.**

Department & Section	Steps	Link
CSE- A,B,C (Backlog)	Step-I : Join Google Classroom using institutional email account	https://classroom.google.com/c/Mzc1OTE3NDg3ODI0?cjc=eebzmyp
	Step-II: Submit the answer script.	https://classroom.google.com/c/Mzc1OTE3NDg3ODI0/a/Mzc1OTE4MjU1NDE5/details