2016

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 alternatives for the following: **10 × 1=10**

(i) The notation * defined by a*b=$\dfrac{a+b}{5}$ is a binary relation on the
(a) set of all integers (b) set of positive integers
(c) set of negative integers (d) set of rationals.

(ii) In $\mathbb{Z}_7$,
(a) $\overline{7} = \overline{15}$ (b) $\overline{7} = \overline{48}$ (c) $\overline{7} = \overline{70}$ (d) $\overline{7} = \overline{1}$

(iii) In the additive group (Z,+), 2^{-3} is
(a) 1/8 (b) -8 (c) -6 (d) 8

(iv) A group G is a simple group if the order of G is
(a) 6 (b) 8 (c) 10 (d) 13.

(v) If the cyclic group G contains 11 distinct elements then the number of its generators are
(a) 2 (b) 7 (c) 9 (d) 10.

(vi) If a is prime to b and a is prime to c, then a is prime to
(a) $b^2 + c^2$ (b) $b^3 + c^3$ (c) ab (d) $a^2 - b^2$

(vii) A connected planar graph with the same number of vertioces and edges determines
(a) 1 region (b) 2 regions
(c) 3 regions (d) 4 regions.

(viii) In the field $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, the multiplicative inverse of $\overline{6}$ is
(a) $\overline{2}$ (b) $\overline{3}$ (c) $\overline{5}$ (d) none of the others.

(ix) A divisor of zero in Z_8, the ring of integers modulo 8, is
(a) [7] (b) [3] (c) [5] (d) [4].

(x) The number of subrings of $2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots.\}$ is
(a) 1 (b) 2 (c) 4 (d) infinite.

Group – B

2. (a) If p is a prime and is not a divisor of a, then prove that $a^{p-1} \equiv 1 (\text{mod } p)$
(b) Find the greatest common divisor of 624 and 441by using the Eucledian algorithm and express it as 624x+441y, where x and y are integers.

6 + 6 = 12

3. (a) State the Chinese Remainder Theorem. Use it to solve the following set of simultaneous congruences : $x \equiv 1\ (mod\ 3), x \equiv 2\ (mod\ 5), x \equiv 3\ (mod\ 3)$.
(b) Prove that there is an infinite number of prime numbers.

7 + 5 = 12

Group – C

4. (a) (i) Determine whether $*$ defined as $a * b = ab + 3$ is a binary operation.
(ii) Determine whether $(\mathbb{R}^+, *)$, $*$ given by $a * b = \sqrt{ab}$ is a group.
(b) Let G be a group and $a, b \in G$. Show that $(aba^{-1})^n = aba^{-1}$ iff $b = b^n$.

(3 + 3) + 6 = 12

5. (a) Show that all the roots of $x^4=1$ forms a commutative group under the operation multiplication.
(b) Prove that the order of a permutation on a finite set is the lcm of length of its disjoint cycles.

6 + 6 = 12

Group – D

6. (a) Prove that *intersection* of any two subgroups of a group (G,*) is a subgroup of G. Is a similar result true for *union*? Justify.
(b) Show that every proper subgroup of a group of order 6 is cyclic.

4 + 2 + 6 = 12

7. (a) Let $H$and K be subgroups of a finite group G. Then prove that $|HK| = \frac{|H||K|}{|H \cap K|}$.
(b) Show that the 8-th roots of unity form a cyclic group. Find all generators of this group.

6 + 6 = 12

Group – E

8. (a) Prove that every field is an integral domain.
(b) If in a ring K with unity, $(xy)^2 = x^2y^2$ for all $x, y \in K$, then prove that K is commutative.

4 + 8 = 12

9. (a) Prove that, for any positive n, the ring Z_n of all integers modulo n, is an integral domain if and only if n is a prime integer.
(b) If a,b be two elements of a field F where b≠0 and $(ab)^2=ab^2+bab-b^2$, then prove that a=1.

6 + 6 = 12