MA 222: Elementary Number Theory and Algebra
End Semester Examination: **PART A**

---

1. **No partial marking for any question except question 6 and 7.**
2. **In question no. 6 and 7, if only one option is written which is correct then 1 mark will be awarded. No mark will be given if incorrect option is written with or without the correct options.**

---

1. Number of elements of order 4 in the groups $U(\mathbb{Z}_{250})$ and $U(\mathbb{Z}_{16})$ are, respectively [1]

   Answer: 2 and 4.
   Solution: Since $250 = 2 \times 5^3$, there is a primitive root modulo 250 and hence $U(\mathbb{Z}_{250})$ is a cyclic group. Therefore, the number of 4-order elements in it is $\phi(4) = 2$.
   The group $U(\mathbb{Z}_{16}) = \{1, 3, 5, 7, 9, 11, 13, 15\}$ has 4 elements of order 4 namely, 3, 5, 11, and 13. $\square$

2. Let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ be the circle group under multiplication. Let $f : S_3 \to S^1$ be a non-trivial non-injective group homomorphism. Then, what is the order of $\ker(f)$? [1]

   Answer: 3.
   Solution: Since $\ker(f)$ is a normal subgroup of S_3, it has three possibilities (1), A_3, and S_3. Also, f is a non-trivial and non-injective group homomorphism, therefore $\ker(f)$ cannot be (1) or S_3. Hence $\ker(f)$=A_3 and the order of $\ker(f) = |A_3| = 3$. $\square$

3. Consider the following two statements: [1]
   I: A field F is finite if and only if char(F) is a prime number.
   II: A field F is infinite if and only if char(F) is zero.
   Which of the following statement(s) is(are) TRUE?
   (A) **I** is TRUE (B) **I** is FALSE (C) **II** is TRUE (D) **II** is FALSE

   Answer: (B) and (D).
   Solution: For a prime p, $\mathbb{F}_p(x) := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0 \right\}$, the field of fractions of $\mathbb{Z}_p[x]$, is an infinite field with characteristic p. Thus, both the statements are false. $\square$

4. The number of elements in the set $\{x \in A_5 : x^4 = (1)\}$ is equal to [1]

   Answer: 16.
   Solution: The set contains the even permutations from S_5 of order 1, 2, and 4. In S_5, elements of order 4 are 4-cycles only, which are not even permutations. Whereas, 2-cycles and product of two 2-cycles are of order 2. Also, 2-cycles are not even permutations.
   For counting elements which are product of two 2-cycles, notice that after choosing first 2-cycle in $({}^5C_2 =)\,10$ ways, we need to choose 2 symbols from remaining 3 symbols in $({}^3C_2 =)\,3$ ways. Since elements like (1 2)(3 4) and (3 4)(1 2) are same, we divide by 2, to get the total number of elements which are product of two 2-cycles equal to $\frac{10\times 3}{2} = 15$. The identity is the only element of order 1 in any group, therefore, we get the total number of elements in the set equal to $15 + 1 = 16$. $\square$

5. How many primitive roots modulo 162 are there? [1]

Answer: 18.
Solution: Since $162 = 2 \times 3^4$, we have a primitive root modulo 162 and there are $\phi(\phi(162)) = 18$ primitive roots modulo 162. $\square$

6. Which of the following is(are) field(s)? [2]
(A) $\mathbb{Z}_2[x]/(x^4 + x + 1)$ (B) $\mathbb{Z}[x]/(5, x)$ (C) $\mathbb{R}[x]/(x^3 + 2)$ (D) $\mathbb{Z}_4[x]/(x^3 + 1)$

Answer: (A) and (B).
Solution: **(A)** Let $f(x) = x^4 + x + 1$. Clearly, $f(x)$ has no linear factor as it has no root in $\mathbb{Z}_2$. The remaining possibility for factorization of $f(x)$ is a product of two quadratic polynomials, say $f(x) = (ax^2 + bx + c)(dx^2 + ex + f)$. But this factorization is not possible for any a, b, c, d, e, and f in $\mathbb{Z}_2$. Therefore, $f(x)$ is irreducible over $\mathbb{Z}_2[x]$. Since $\mathbb{Z}_2[x]$ is a PID and $x^4 + x + 1$ is irreducible over $\mathbb{Z}_2[x]$, hence $\mathbb{Z}_2[x]/(x^4 + x + 1)$ is a field.
(B) Since $(5, x)$ is a maximal ideal in integral domain $\mathbb{Z}[x]$, therefore $\mathbb{Z}[x]/(5, x)$ is a field.
(C) The polynomial $x^3 + 2$ has a real root, therefore it is reducible over $\mathbb{R}[x]$. Since $\mathbb{R}[x]$ is PID, $(x^3 + 2)$ is not a maximal ideal. Hence, $\mathbb{R}[x]/(x^3 + 2)$ is not a field.
(D) In $\mathbb{Z}_4[x]/(x^3+1)$, $2+(x^3+1)$ is a zero divisor as $(2+(x^3+1))(2+(x^3+1)) = 0+(x^3+1)$. Therefore, $\mathbb{Z}_4[x]/(x^3 + 1)$ is not a field. $\square$

7. Consider the following two statements: [2]
I: There is NO injective (one-one) group homomorphism from $U(\mathbb{Z}_8)$ to $\mathbb{Z}_8$.
II: There is NO surjective (onto) group homomorphism from $\mathbb{Z}_8$ to $U(\mathbb{Z}_8)$.
Which of the following statement(s) is(are) TRUE?
(A) **I** is TRUE (B) **I** is FALSE (C) **II** is TRUE (D) **II** is FALSE

Answer: (A) and (C).
Solution: **Statement I**: Suppose there is an injective group homomorphism Φ from $U(\mathbb{Z}_8)$ to $\mathbb{Z}_8$. Then $\Phi(U(\mathbb{Z}_8))$ will be isomorphic to $U(\mathbb{Z}_8)$. Since, $\mathbb{Z}_8$ is cyclic and $\Phi(U(\mathbb{Z}_8))$ is a subgroup of $\mathbb{Z}_8$, so $\Phi(U(\mathbb{Z}_8))$ is also cyclic. But $\Phi(U(\mathbb{Z}_8))$ can't be cyclic as $U(\mathbb{Z}_8)$ is not cyclic. Therefore, there is no injective group homomorphism from $U(\mathbb{Z}_8)$ to $\mathbb{Z}_8$.
Statement II: Let Ψ be a surjective group homomorphism from $\mathbb{Z}_8$ to $U(\mathbb{Z}_8)$. Then, the quotient group $\mathbb{Z}_8/ker(\Psi)$ is isomorphic to $U(\mathbb{Z}_8)$. Since $\mathbb{Z}_8$ is cyclic, so $\mathbb{Z}_8/ker(\Psi)$ is also cyclic. But $\mathbb{Z}_8/ker(\Psi)$ can't be cyclic as $U(\mathbb{Z}_8)$ is not cyclic. Thus, there is no surjective group homomorphism from $\mathbb{Z}_8$ to $U(\mathbb{Z}_8)$. $\square$

8. Write down the last two digits of 3^{1492}. [2]

Answer: 41
Solution: Since $\gcd(3, 100) = 1$, $3^{\phi(100)} \equiv 1 \pmod{100}$. We know that $\phi(100) = 40$, then $3^{40} \equiv 1 \pmod{100}$. Consider

$$\begin{aligned} 3^{1492} = 3^{1480+12} &\equiv 3^{12} \pmod{100} \\ &\equiv (-19)(-19)(-19) \equiv -59 \equiv 41 \pmod{100}. \end{aligned}$$

$\square$

9. Consider the group $(\mathbb{Q}, +)$ and its subgroup $(\mathbb{Z}, +)$. Consider the following statements: [2]
I: For every positive integer n, $\mathbb{Q}/\mathbb{Z}$ has a unique subgroup of order n.
II: There is exactly one group homomorphism from $\mathbb{Q}/\mathbb{Z}$ to $(\mathbb{Q}, +)$.
Which of the following is TRUE?
(A) Both **I** and **II** are TRUE (B) Both **I** and **II** are FALSE
(C) **I** is TRUE but **II** is FALSE (D) **I** is FALSE but **II** is TRUE

Answer: (A).
Solution: Statement I: Let n be any positive integer. Then $\mathbb{H}_n := \left\{\frac{m}{n} + \mathbb{Z} : 0 \le m < n\right\}$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$ of order n. Let S_n be any subgroup of $\mathbb{Q}/\mathbb{Z}$ of order n. Then for any $\frac{a}{b} + \mathbb{Z} \in S_n$ $(a \in \mathbb{Z}, b \in \mathbb{N})$, $n\left(\frac{a}{b} + \mathbb{Z}\right) = 0 + \mathbb{Z}$, i.e., $b \mid n$. Now, by division algorithm, there exist $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, b-1\}$ such that $a = bq + r$. Then $\frac{a}{b} + \mathbb{Z} = \frac{r}{b} + \mathbb{Z}$, where $b \mid n$ and $0 \le r < n$. This implies that $\frac{a}{b} + \mathbb{Z} \in \mathbb{H}_n$, which in turn implies that $S_n \subset \mathbb{H}_n$. But since S_n and $\mathbb{H}_n$ are of same order, we get the unique subgroup of order n, i.e., $S_n = \mathbb{H}_n$.
Statement II: Let f be a group homomorphism from $\mathbb{Q}/\mathbb{Z}$ to $(\mathbb{Q}, +)$. Then $o(f(a)) \mid o(a)$, for all $a \in \mathbb{Q}/\mathbb{Z}$, since all the elements of $\mathbb{Q}/\mathbb{Z}$ are of finite order. This implies that $o(f(a))$ is finite, for all $a \in \mathbb{Q}/\mathbb{Z}$. But $(\mathbb{Q}, +)$ has only one finite-order element, i.e., 0. Thus, $f(a) = 0$, for all $a \in \mathbb{Q}/\mathbb{Z}$. This gives exactly one group homomorphism from $\mathbb{Q}/\mathbb{Z}$ to $(\mathbb{Q}, +)$.

□

10. What is the multiplicative inverse of $1 + x^2 + (x^3 + 2x + 1)$ in $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$? [2]

Answer: $2x^2 + x + 2 + (x^3 + 2x + 1)$.
Solution: Let $I = (x^3 + 2x + 1)$. Then

$$\mathbb{Z}_3[x]/I = \{ax^2 + bx + c + I : a, b, c \in \mathbb{Z}_3\}.$$

Let $ax^2 + bx + c + I$ be the multiplicative inverse of $1 + x^2 + I$ in $\mathbb{Z}_3[x]/I$. Then $(x^2 + 1 + I)(ax^2 + bx + c + I) = 1 + I$. We get $ax^4 + bx^3 + (a + c)x^2 + bx + c + I = 1 + I$. Also, $x^3 + I = -2x - 1 + I$ and substituting this in the above expression, we get

$$(c - a)x^2 - (a + b)x + (c - b) + I = 1 + I.$$

This implies $(c - a)x^2 - (a + b)x + (c - b) - 1 \in I$. Therefore, $(c - a)x^2 - (a + b)x + (c - b) - 1 = f(x)(x^3 + 2x + 1)$, for some $f(x) \in \mathbb{Z}_3[x]$. We have $f(x) = 0$, otherwise the degree of right-hand side will be greater than the degree of left-hand side. Therefore, $(c - a)x^2 - (a + b)x + (c - b) - 1 = 0$. Equating the coefficients on both side, we get $a = 2,\ b = 1$, and $c = 2$ and hence the multiplicative inverse of $1 + x^2 + I$ is $2x^2 + x + 2 + I$. □

•••