Quiz-II: MA 222: Elementary Number Theory and Algebra
Model Solutions

---

1. Let x be the 100-cycle $(1\ 2\ 3\ \cdots\ 100)$ and let y be the 2-cycle $(49\ 50)$ in the permutation group S_{100}. What is the order of xy? [1]

   Answer: 99.
   Solution: Clearly, $xy = (1\ 2\ \cdots\ 49\ 51\ \cdots\ 100)$ is a 99-cycle. Therefore, the order of xy is 99. □

2. The number of elements in $\mathbb{Z}_{1000001}$ of orders 101 and 1001 are, respectively [1]

   Answer: 100 and 0.
   Solution: The group $\mathbb{Z}_{1000001}$ is cyclic and 101 divides its order, i.e., 1000001. Hence the number of elements of order 101 in $\mathbb{Z}_{1000001}$ is $\phi(101) = 100$. Since 1001 does not divide 1000001, there is no element of order 1001 in $\mathbb{Z}_{1000001}$. □

3. The number of cyclic subgroups of order 4 in S_4 is equal to [1]

   Answer: 3.
   Solution: Any cyclic subgroup of order 4 is generated by an element of order 4 and only elements of order 4 in S_4 are 4-cycles. There are six 4-cycles in S_4, namely, $(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 3\ 2\ 4)$, $(1\ 3\ 4\ 2)$, $(1\ 4\ 3\ 2)$, and $(1\ 4\ 2\ 3)$. Subgroups generated by these six 4-cycles are:
   $\langle(1\ 2\ 3\ 4)\rangle = \{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\} = H_1$,
   $\langle(1\ 2\ 4\ 3)\rangle = \{(1), (1\ 2\ 4\ 3), (1\ 4)(3\ 2), (1\ 3\ 4\ 2)\} = H_2$,
   $\langle(1\ 3\ 2\ 4)\rangle = \{(1), (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\} = H_3$,
   $\langle(1\ 3\ 4\ 2)\rangle = H_2$,
   $\langle(1\ 4\ 3\ 2)\rangle = H_1$,
   $\langle(1\ 4\ 2\ 3)\rangle = H_3$.
   Therefore, S_4 has three distinct cyclic subgroups of order 4. □

4. The number of elements of order 12 in S_7 is equal to [2]

   Answer: 420.
   Solution: The only possible way to write a 12-order element in S_7 is a product of 4- and 3-cycle. The total number of 4-cycles in S_7 is $\frac{^7P_4}{4} = 210$. The remaining three symbols can form 2 possible 3-cycles. Thus, we have $210 \times 2 = 420$ elements of order 12 in S_7. □

5. The number of elements in the set $\{x \in S_5 : x^4 = (1)\}$ is equal to [2]

   Answer: 56.
   Solution: The set contains the elements from S_5 of order 1, 2, and 4. In S_5, elements of order 4 are 4-cycles only, and there are $\frac{^5P_4}{4} = 30$ number of 4-cycles. Whereas, 2-cycles and product of two distinct 2-cycles are of order 2. The number of 2-cycles in S_5 is $\frac{^5P_2}{2} = 10$.
   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 distinct 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 $30 + 10 + 15 + 1 = 56$. □

6. Which of the following is(are) field(s)? [2]
(A) $\mathbb{C}[x]/(x^2+2)$ (B) $\mathbb{Z}[x]/(x^2+2)$ (C) $\mathbb{Q}[x]/(x^2-2)$ (D) $\mathbb{R}[x]/(x^2-2)$

Answer: (C).
Solution: Since $\mathbb{Q}$ is a field and x^2-2 is irreducible in $\mathbb{Q}[x]$, hence $\frac{\mathbb{Q}[x]}{(x^2-2)}$ is a field. Clearly, x^2+2 and x^2-2 have roots in $\mathbb{C}$ and $\mathbb{R}$, respectively. Therefore, $\frac{\mathbb{C}[x]}{(x^2+2)}$ and $\frac{\mathbb{R}[x]}{(x^2-2)}$ are not fields. We have

$$R := \frac{\mathbb{Z}[x]}{(x^2+2)} = \left\{ax + b + (x^2+2) : a, b \in \mathbb{Z}\right\},$$

with unity $1{+}(x^2+2)$. Consider $z = 2 + (x^2+2) \in R$, then z has no inverse in R. Hence, R is not a field. □

7. Write down all the irreducible polynomials of degree 2 in $\mathbb{Z}_2[x]$. [1]

Answer: $x^2 + x + 1$.
Solution: All possible polynomials of degree 2 in $\mathbb{Z}_2[x]$ are x^2, x^2+x, x^2+x+1, and x^2+1. Substituting $x = 0$ and $x = 1$, we observe that the polynomials x^2, x^2+x, and x^2+1 have roots in $\mathbb{Z}_2$. But $f(x) = x^2+x+1$ has no root in $\mathbb{Z}_2$, hence $f(x)$ is the only irreducible polynomial of degree 2. □

8. For rings R and S, consider the ring $R \times S = \{(r, s) : r \in R, s \in S\}$ with respect to componentwise addition and multiplication. Then, which of the following statement(s) is(are) TRUE? [1]
(A) The characteristic of the ring $6\mathbb{Z}$ is 6
(B) The ring $6\mathbb{Z}$ has no zero divisor
(C) The characteristic of the ring $(\mathbb{Z}/6\mathbb{Z}) \times 6\mathbb{Z}$ is zero
(D) The ring $6\mathbb{Z} \times 6\mathbb{Z}$ is an integral domain

Answer: (B) and (C).
Solution: Characteristic of the ring $6\mathbb{Z}$ is 0.
The ring $6\mathbb{Z}$ has no zero divisors as it is a subring of an integral domain $\mathbb{Z}$.
Since characteristic of $6\mathbb{Z}$ is 0, therefore characteristic of $(\mathbb{Z}/6\mathbb{Z}) \times 6\mathbb{Z}$ is also 0.
For any $0 \neq a \in 6\mathbb{Z}$, we have $(a, 0)\cdot(0, a) = (0, 0)$. Therefore, $6\mathbb{Z}\times 6\mathbb{Z}$ has zero divisors and it is not an integral domain. □

9. The number of units f in the ring $\mathbb{Z}_{12}[x]$ such that $\deg(f) \leq 2$ is equal to [2]

Answer: 16.
Solution: Nilpotent elements in $\mathbb{Z}_{12}$ are 0 and 6. Units in $\mathbb{Z}_{12}$ are 1, 5, 7, and 11.
We know that $f(x) = ax^2 + bx + c$ is a unit if a and b are nilpotent elements, and c is a unit. Hence, we have $2 \times 2 \times 4 = 16$ polynomials which are units in $\mathbb{Z}_{12}[x]$. □

10. Let $I = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$ and $J = \{f(x) \in \mathbb{Z}[x] : f(0) \in 2\mathbb{Z}\}$. Which of the following statement is TRUE? [2]

(A) Both I and J are maximal ideals (B) I is maximal but J is not maximal

(C) J is maximal but I is not maximal (D) Both I and J are not maximal ideals

Answer: (C).

Solution: Clearly $I \subsetneq J \subsetneq \mathbb{Z}[x]$, therefore I is not a maximal ideal.

Let J_1 be an ideal of $\mathbb{Z}[x]$ such that $J \subsetneq J_1$. Then J_1 contains a polynomial $g(x)$ whose constant term is an odd number. Also, $h(x) = g(x) + 1 \in J \subset J_1$, therefore $1 = h(x) - g(x) \in J_1$ which gives $J_1 = \mathbb{Z}[x]$. Hence, J is a maximal ideal. $\square$

•••