MA 222: Elementary Number Theory and Algebra
End semester examination: **PART-B**

---

1. Find the order of the element $(1\ 2\ 3)(2\ 4\ 5)(4\ 5\ 6)$ in the group S_8. [1]

   Solution: Clearly, $\alpha := (1\ 2\ 3)(2\ 4\ 5)(4\ 5\ 6) = (1\ 2\ 4\ 3)(5\ 6)(7)(8)$. Then, the order of α is $lcm(2, 4) = 4$. $\square$

2. Let $f \in S_n$ be such that the order of f is odd. Prove that f is an even permutation. [2]

   Solution: Let $f = f_1 f_2 \cdots f_k$ be the decomposition of f into disjoint cycles. Then, $o(f) = lcm(o(f_1), o(f_2), \ldots, o(f_k))$. Since $o(f)$ is odd, $o(f_i)$ is odd for all $i \in \{1, 2, \ldots, k\}$. [1]
   This implies that for each $i \in \{1, 2, \ldots, k\}$, f_i, being an odd cycle is an even permutation. Also, a product of even permutations is an even permutation, therefore f is an even permutation. [1] $\square$

3. Let H be a subgroup of S_n. Show that either every member of H is an even permutation or exactly half of them are even. [2]

   Solution: If every element of H is an even permutation then we are done. Consider H has at least one odd permutation say it is α. Then we have to prove that exactly half of the members are even. Let n_1 and n_2 be the number of odd and even permutations, respectively, in H. Then αH is a subgroup of H and $|H| = |\alpha H|$, therefore $\alpha H = H$. [1]
   We know that the product of an even and an odd permutation is an odd permutation. And the product of two odd permutations is an even permutation. Therefore, the number of odd and even permutations in $\alpha H (= H)$ are given by n_2 and n_1, respectively. Hence $n_1 = n_2$. Also, $|H| = n_1 + n_2$, which gives $n_1 = n_2 = \frac{|H|}{2}$. [1] $\square$

4. Let R be a finite commutative ring with unity. Prove that every prime ideal of R is a maximal ideal of R. [2]

   Solution: Let P be a prime ideal of R. Then R/P is an integral domain. [1]
   Thus, R/P is a finite integral domain and hence it is a field. Therefore, P is a maximal ideal of R. [1] $\square$

5. Let $f(x) \in \mathbb{R}[x]$ be irreducible. Prove that either $\deg(f) = 1$ or $f(x) = ax^2 + bx + c$ such that $b^2 - 4ac < 0$. [2]

   Solution: Let $f(x)$ be any polynomial in $\mathbb{R}[x]$ of degree greater than two. If $f(x)$ has a real root then it is reducible. If all the roots of $f(x)$ are complex numbers then using the fundamental theorem of algebra, we can write $f(x)$ as a product of linear factors in $\mathbb{C}[x]$. Also, if $z_1 \in \mathbb{C}$ is a root of $f(x)$ then $\overline{z_1}$(conjugate of z_1) is also a root of $f(x)$ as the coefficients of the polynomial are real numbers. Hence $g(x) = (x - z_1)(x - \overline{z_1})$ is a quadratic factor of $f(x)$ in $\mathbb{R}[x]$ and $f(x)$ is reducible. Therefore, any polynomial of degree greater than two can be written as a product of linear or quadratic polynomials in $\mathbb{R}[x]$. [1]
   If deg(f)=2, then $f(x) = ax^2 + bx + c$ can be written as product of two linear factors if

$b^2 - 4ac \geq 0$. Therefore, if $f(x) = ax^2 + bx + c$ is irreducible then $b^2 - 4ac < 0$. Also, all the polynomials of degree 1 are irreducible. Thus, if $f(x) \in \mathbb{R}[x]$ be irreducible then either $\deg(f) = 1$ or $f(x) = ax^2 + bx + c$ such that $b^2 - 4ac < 0$. [1] $\square$

6. Let p be a prime. Prove that $\{f(x) \in \mathbb{Z}[x] : f(0) \in p\mathbb{Z}\}$ is a maximal ideal in $\mathbb{Z}[x]$. [2]

Solution: It is easy to check that $I := \{f(x) \in \mathbb{Z}[x] : f(0) \in p\mathbb{Z}\}$ is an ideal of $\mathbb{Z}[x]$. Suppose there is an ideal J of $\mathbb{Z}[x]$ such that $I \subsetneq J \subseteq \mathbb{Z}[x]$. Take $g(x) \in J \setminus I$. Then, $g(x) = xh(x) + t$, for some $h(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z} \setminus p\mathbb{Z}$. [1]
Since t is co-prime to p, there exist the integers α and β such that $t\alpha + p\beta = 1$. Consider a polynomial in I, $p(x) := \alpha x h(x) - p\beta$. Then $1 = \alpha g(x) - p(x) \in J$. Thus, $J = \mathbb{Z}[x]$. Therefore, I is a maximal ideal in $\mathbb{Z}[x]$. [1] $\square$

7. Let R be a commutative ring with unity. For an ideal I of R, consider

$$I[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in I, n \geq 0 \right\}.$$

Note that $I[x]$ is an ideal of $R[x]$. Let R_1 denote the quotient ring R/I.

(a) Prove that the rings $R[x]/I[x]$ and $R_1[x]$ are isomorphic. [2]

(b) If I is a prime ideal in R, is $I[x]$ a prime ideal in $R[x]$? [1]

(c) If I is a maximal ideal in R, is $I[x]$ a maximal ideal in $R[x]$? [1]

Solution: (a) Let $\phi : R[x] \to R_1[x]$ be a map defined by $\phi(f(x)) = \overline{f(x)}$, where $\overline{f(x)}$ is polynomial in $R_1[x]$ whose coefficients are reduced modulo I. Clearly, $\phi(f_1(x) + f_2(x)) = \phi(f_1(x)) + \phi(f_2(x))$ and $\phi(f_1(x) \cdot f_2(x)) = \phi(f_1(x)) \cdot \phi(f_2(x))$. Thus, ϕ is a ring homomorphism. [1]
Let $g(x) = (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n \in R_1[x]$. Then $h(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ such that $\phi(h(x)) = g(x)$. Therefore, ϕ is an onto homomorphism. Kernel of ϕ is the collection of all polynomials whose coefficients are from ideal I that is equal to $I[x]$. Then, by the first isomorphism theorem for rings, we have $R[x]/I[x] \cong R_1[x]$. [1]

(b) If I is a prime ideal in R, then $R_1 = R/I$ is an integral domain and so is $R_1[x]$. By part (a), we have $R[x]/I[x]$ is an integral domain. Hence, $I[x]$ is a prime ideal in $R[x]$.

(c) No, this need not be true. For example, $R = \mathbb{Z}$ and $I = (2)$, then I is a maximal ideal in R. But $I[x] = 2\mathbb{Z}[x]$ is not a maximal ideal in $\mathbb{Z}[x]$, as $I[x] \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

$\square$

8. Find the multiplicative inverse of $5 + 6x + 12x^2$ in $\mathbb{Z}_{36}[x]$, if exists. [3]

Solution: Clearly, 5 is a unit, and 6 and 12 are nilpotent elements in $\mathbb{Z}_{36}$. Therefore, $5 + 6x + 12x^2$ is a unit and inverse exists. [1]
Let $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ be the multiplicative inverse of $5 + 6x + 12x^2$. Then

$$(5 + 6x + 12x^2)(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) \equiv 1 \pmod{36}.$$

Comparing constant terms on both sides of the above congruence we get $5a_0 \equiv 1 \pmod{36}$. This gives $a_0 \equiv 29 \pmod{36}$. Similarly, comparing the coefficients of x, we get $6a_0+5a_1 \equiv 0 \pmod{36}$. Substituting the value of a_0, we get $a_1 \equiv 30 \pmod{36}$. [1]
By comparing coefficients of x^2, we get $5a_2 + 6a_1 + 12a_0 \equiv 0 \pmod{36}$, which gives $a_2 \equiv 24 \pmod{36}$. Similarly, coefficients of x^3: $5a_3 + 6a_2 + 12a_1 \equiv 0 \pmod{36}$ gives $a_3 \equiv 0 \pmod{36}$ and coefficients of x^4: $5a_4 + 6a_3 + 12a_2 \equiv 0 \pmod{36}$ gives $a_4 \equiv 0 \pmod{36}$. It is clear that $a_5 \equiv a_6 \equiv \cdots \equiv a_n \equiv 0 \pmod{36}$. Therefore, the multiplicative inverse of $5 + 6x + 12x^2$ in $\mathbb{Z}_{36}[x]$ is $29 + 30x + 24x^2$. [1] □

9. Give an example of a field F with 125 elements. Also, find all the subfields of F. [3]

Solution: Let $f(x) = x^3+x+1$. Clearly, $f(x)$ is an irreducible polynomial over the PID $\mathbb{Z}_5[x]$, as it has no root in $\mathbb{Z}_5$. [1]
Therefore, $\mathbb{Z}_5[x]/(x^3 + x + 1)$ is a field of order $5^{deg(f)} = 5^3 = 125$. [1]
We know that if the order of a field is p^n then it has a subfield of order p^r where r is a divisor of n. The only divisors of 3 are 1 and 3. Therefore, subfields of $\mathbb{Z}_5[x]/(x^3+x+1)$ are of order 5 and 125. The subfield of order 125 is $\mathbb{Z}_5[x]/(x^3 + x + 1)$ itself and the subfield of order 5 is isomorphic to $\mathbb{Z}_5$. [1] □

10. Let $p = 4n + 1$ be a prime.

    (a) Prove that n is a quadratic residue modulo p. [2]

    (b) Find the remainder of n^n when divided by p. [2]

Solution: **(a):** Clearly, 4 is a quadratic residue modulo p. Then

$$\left(\frac{n}{p}\right) = \left(\frac{4n}{p}\right) = \left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right).$$

[1]
Also, -1 is quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$. Hence, n is a quadratic residue modulo p. [1]

(b): From part (a), $n \equiv k^2 \pmod p$ for some positive integer k. Consider

$$\begin{aligned} 4k &\equiv 4k + p \pmod p \\ &\equiv 4k + 4n + 1 \equiv 4k + 4k^2 + 1 \equiv (2k + 1)^2 \pmod p. \end{aligned}$$

Therefore, $k \equiv k_1^2 \pmod p$, where $k_1 = (2k + 1)2^{-1}$. Hence $n \equiv k_1^4 \pmod p$. [1]
Then

$$n^n \equiv k_1^{4(\frac{p-1}{4})} \equiv k_1^{p-1} \equiv 1 \pmod p,$$

i.e., $n^n \equiv 1 \pmod p$. Therefore, the remainder of n^n when divided by p is 1. [1] □

11. Let $\sigma(n) = \sum_{d|n} d$, sum of all the positive divisors of n. Let $f(n) = \sum_{d|n} \mu(d)\sigma(n/d)$, where μ is the Möbius function. Calculate the value of $f(2022^{2022})$. [3]

Solution: Consider $g : \mathbb{N} \to \mathbb{C}$ such that $g(n) = n$, for all $n \in \mathbb{N}$. Then

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} g(d).$$

[1]

By the Möbius inversion formula, we have

$$\begin{aligned} g(n) = \sum_{d|n} \sigma(d)\mu(n/d) &= \sum_{d|n} \mu(d)\sigma(n/d) \\ &= f(n). \end{aligned}$$

Therefore, $f(2022^{2022}) = g(2022^{2022}) = 2022^{2022}$. [2] □

12. Let p be an odd prime. If g_1 and g_2 are primitive roots modulo p, then prove that $g_1 g_2$ can't be a primitive root modulo p. [2]

Solution: Note that $\frac{p-1}{2}$ is a positive integer for any odd prime p. Since g_1 is primitive root modulo p and $g_1^{p-1} \equiv 1 \pmod{p}$, $g_1^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Similarly, $g_2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. [1]
Then

$$\begin{aligned} (g_1 g_2)^{\frac{p-1}{2}} &= g_1^{\frac{p-1}{2}} g_1^{\frac{p-1}{2}} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

Therefore, the order of $g_1 g_2$ is strictly less than $p - 1$ and hence it cannot be a primitive root modulo p. [1] □

• • •