Discrete Mathematics

Question Paper

May 1, 2025

Contents

1 Class Test on 24 April 2025

Name: **R. No.:** ....

Class Test on 24 April 2025

Max Marks: 15 **Max Time: 60 Min**

Answer all the following questions. The use of mobile devices and calculators is prohibited during the class test. Each and every step of your calculation should be shown on the answer sheet with justification.

1. Let g be an element of a group with $ord(g) = 18$. Find the smallest positive integer k s/t $g^{-5} = g^k$. Justify your answer. 1

2. Consider the element 4 in the additive group $\mathbb{Z}_{30}$.

   (a) Find the elements of the cyclic subgroup $\langle 4 \rangle$.

   (b) Find all $m \in \mathbb{Z}_{30}$ s/t $\langle m \rangle = \langle 4 \rangle$. Justify your answer.

   2 + 2

3. Determine whether the two cosets $(5x + 2) + \langle x^2 + 6 \rangle$ and $(2x + 4) + \langle x^2 + 6 \rangle$ are equal in $\mathbb{Z}_7[x]/\langle x^2 + 6 \rangle$. Justify your answer. 1.5

4. Determine whether the polynomial $f(x) = x^5 + x^4 + 1$ is irreducible over $\mathbb{Z}_2[x]$. Justify your answer. 3.5

5. Find the multiplicative inverse of $x^3 + x + 2$ in $GF(3^5) = GF(3)[x]/\langle x^5 + 2x + 1 \rangle$. 5

1.1 Answer Key

1. Let g be an element of a group with $ord(g) = 18$. Find the smallest positive integer k s/t $g^{-5} = g^k$. Justify your answer. 1

   Solution 1.1. *Since* $ord(g) = 18 \Rightarrow g^{18} = 1$.

   $g^{-5} = 1.g^{-5} = g^{18} \times g^{-5} = g^{13}$.

   Thus, we have

   $$g^{-5} = g^{13} \Rightarrow k = 13$$

2. Consider the element 4 in the additive group $\mathbb{Z}_{30}$.

   (a) Find the elements of the cyclic subgroup $\langle 4 \rangle$.

   (b) Find all $m \in \mathbb{Z}_{30}$ s/t $\langle m \rangle = \langle 4 \rangle$. Justify your answer. 2 + 2

   Solution 1.2. *(a) The elements of the cyclic subgroup generated by 4 is given below:*

   $$\begin{array}{lllll} 4^1 = 4, & 4^2 = (4+4) = 8, & 4^3 = 12, & 4^4 = 16, & 4^5 = 20, \\ 4^6 = 24, & 4^7 = 28, & 4^8 = 32 \equiv 2, & 4^9 = 6, & 4^{10} = 10, \\ 4^{11} = 14, & 4^{12} = 18, & 4^{13} = 22, & 4^{14} = 26, & 4^{15} = 30 \equiv 0 \end{array}$$

   Thus,

   $$\langle 4 \rangle = \{4, 8, 12, 16, 20, 24, 28, 2, 6, 10, 14, 18, 22, 26, 0\}$$

   (b) To find all the generators of the cyclic subgroup $\langle 4 \rangle$ of order 15, first we compute the total number of generators we can have of a cyclic subgroup of order 15

   $$= \phi(15) = \phi(3 \times 5) = \phi(3) \times \phi(5) = (3-1)(5-1) = 8$$

   Now, to find all the generators of $\langle 4 \rangle$, we have to find 4^k where $\gcd(k, 15) = 1$.
   So, we can find the value of $k = 1, 2, 4, 7, 8, 11, 13, 14$.
   Thus,

   $$m \in \{4^1 = 4, 4^2 = 8, 4^4 = 16, 4^7 = 28, 4^8 = 2, 4^{11} = 14, 4^{13} = 22, 4^{14} = 26\}$$

   $$m = 4, 8, 16, 28, 2, 14, 22, \ \mathit{or}\ 26$$

3. Determine whether the two cosets $(5x+2)+\langle x^2+6\rangle$ and $(2x+4)+\langle x^2+6\rangle$ are equal in $\mathbb{Z}_7[x]/\langle x^2+6\rangle$. Justify your answer. 1.5

   Solution 1.3. *We know that two cosets $a+I$ and $b+I$ in a quotient ring R/I are equal iff $a-b \in I$.*

   Now, we can see that $a-b=(5x+2)-(2x+4)=3x+5$.

   If $3x+5 \in x^2+6$, then $(x^2+6) \mid (3x+5)$.
   That is not possible; because the degree of $(x^2+6)=2$ and that of $(3x+5)=1$. A lower-degree polynomial cannot be divisible by a higher-degree polynomial unless it is the zero polynomial.

4. Determine whether the polynomial $f(x)=x^5+x^4+1$ is irreducible over $\mathbb{Z}_2[x]$. Justify your answer. 3.5

   Solution 1.4. *The given polynomial $f(x)$ is not divisible by x or $(x+1)$ in $\mathbb{Z}_2[x]$; because it has no root in $\mathbb{Z}_2$. Therefore, it cannot be divided by any linear polynomial.*

   Now, we try to divide $f(x)$ by the 2 degree irreducible polynomial x^2+x+1 in $\mathbb{Z}_2[x]$.

   We find that

   $$x^5+x^4+1=(x^2+x+1)(x^3+x+1)$$

   Thus, the given polynomial $f(x)$ is reducible.

5. Find the multiplicative inverse of x^3+x+2 in $GF(3^5)=GF(3)[x]/\langle x^5+2x+1\rangle$. 5

   Solution 1.5. *To find the inverse of x^3+x+2 in $GF(3^5)$, we have to find the $\gcd(x^3+x+2, x^5+2x+1)$. To find $\gcd$, we apply the following method:*

   $$\begin{aligned}
   x^5+2x+1 &= (x^2+2)(x^3+x+2)+x^2,\\
   x^3+x+2 &= x.x^2+(x+2), \text{ and}\\
   x^2 &= (x+1)(x+2)+1\\
   \\
   \Rightarrow 1 &= x^2+2(x+1)(x+2)\\
   &= x^2+2(x+1)[(x^3+x+2)+2.x.x^2]\\
   &= 2(x+1)(x^3+x+2)+x^2(x^2+x+1)\\
   &= 2(x+1)(x^3+x+2)+(x^2+x+1)[(x^5+2x+1)+2(x^2+2)(x^3+x+2)]\\
   &= (x^2+x+1)(x^5+2x+1)+(x^3+x+2)[2x+2+2(x^4+x^3+x^2+2x^2+2x+2)]\\
   &= (x^2+x+1)(x^5+2x+1)+(x^3+x+2)(2x^4+2x^3)
   \end{aligned}$$

$$\Rightarrow 1 \quad = \quad (x^3 + x + 2)(2x^4 + 2x^3) \mod (x^5 + 2x + 1)$$

$$(x^3 + x + 2)^{-1} = (2x^4 + 2x^3) \in GF(3^5) = GF(3)[x]/\langle x^5 + 2x + 1 \rangle$$