KATHMANDU UNIVERSITY
End Semester Examination
January, 2025

Marks Scored:

Level : B.Sc.
Year : IV

Course : MATH 402
Semester : I

Exam Roll No. :

Time: 30 mins.

F. M. : 10

Registration No.:

Date 31 JAN 2025

SECTION "A"

[10Q. × 0.5 = 5 marks]

Fill in the blank space(s) by writing the most appropriate word(s) or symbol(s).

1. The subgroup $3\mathbb{Z}$ of a group $\mathbb{Z}$ is cyclic with generator _____.
2. A subgroup H of a group G is normal if it's left and right cosets _____.
3. Let G be a group and N and H be normal subgroups of G with $N \subset H$. Then $G/N \cong$_____.
4. A homomorphism of $f: \mathbb{R} \to \mathbb{R}$ is called _____.
5. Since $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$, $\mathbb{Z}_2/< x^2 + x + 1 >$ is an _____ of $\mathbb{Z}_2$.
6. Let P, Q, R are any three points on elliptic curve $E(a, b)$. If $Q = -P$ then $R =$_____
7. Any irreducible polynomial of degree n yields the same field up to _____
8. After shift rows transformation in AES the state matrix $\begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & F2 & 69 & 26 \\ A3 & C9 & 7D & 4E \\ 3A & 11 & 91 & B2 \end{bmatrix}$ will be transformed into _____.
9. An ideal $N \neq R$ in a commutative ring R is a prime ideal if _____
10. A round constant in key expansion of AES is a word where three rightmost bytes are _____.

SECTION "B"

[10 Q.× 0.5 = 5 marks]

Fill in the blank space(s), **DO NOT TICK**, by selecting the most appropriate answers from among the given ones.

11. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ then $\sigma\tau =$ _____

[$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$]

12. Define $\phi: \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ by $\phi(x) = 4x$, then Ker(ϕ)= _____

[{0,4,8}; {0.2.4.6.8.10}; {0,6}; {0,3,6,9}]

13. The order of $(4,48) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$ is _____

[15; 10; 24; 12]

14. AES uses _____ rounds for 192 bit keys.

[10; 12; 14; 16]

15. An ideal N of R is prime iff R/N is _____

[Group; Ring; Integral domain; Field]

16. The order of $\mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right)$ over $\mathbb{Q}$ is _____

[1; 2; 3; 4]

17. The polynomial $x^2 + 1$ is _____ over $\mathbb{Z}_2$

[Reducible; Irreducible; Cyclotomic; Coset]

18. The number of primitive polynomials of degree 4 on $\mathbb{Z}_2$ is _____

[1; 2; 3; 4]

19. The degree of codeword in Reed Solomon code having length n is less than _____

[2^n; 2^{n-1}; $2^n - 1$; $2^n - 2$]

20. AddRoundKey transformation of [4C] and [A7] in AES is _____

[51; 2A; 75; EB]

KATHMANDU UNIVERSITY
End Semester Examination
January, 2025

Level : B.Sc.
Year : IV
Time : 2 hrs. 30mins.

31 JAN 2025

Course : MATH 402
Semester : I
F. M. : 40

SECTION "C"
[2Q × 8 = 16 marks]

Attempt *ANY TWO* questions.

1.
   a. Define elliptic curve. [1]
   b. Identify every point on an elliptic curve $E_{11}(1,1)$. [3]
   c. For $P = (1,5) \in E_{11}(1,1)$ compute $5P$. [4]

2.
   a. Define an ideal of a ring. [1]
   b. Show that $\mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} | \, a, b \in \mathbb{Q}\}$ is a ring. [3]
   c. Define $f: \mathbb{Q}\sqrt{2} \to \mathbb{Q}\sqrt{2}$ by $f(a + b\sqrt{2}) = a - b\sqrt{2}, \forall \, a + b\sqrt{2} \in \mathbb{Q}\sqrt{2}$. Show that f is an automorphism. [4]

3.
   a. Define algebraic and transcendental elements of an extension field. [2]
   b. Find the basis and dimension of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. [3]
   c. Let E be a finite extension of degree n over finite field F. Prove that if F has q elements then E has q^n elements. [3]

SECTION "D"
[8Q × 3 = 24 marks]

Attempt *ANY EIGHT* questions.

4. Let $H = \{(1), (123), (132)\}$ be the subgroup of S_3. Find all cosets of H.

5. Let G be a group and H be a non empty subset of G. Prove that H is a subgroup of G iff $ab^{-1} \in H, \forall \, a, b \in H$.

6. Let $\phi: G \to \bar{G}$ is a group homomorphism and let H be a subgroup of G. Show that if H is normal in G then $\phi(H)$ is normal in $\bar{G}$.

7. Show that every field F is and integral domain.

8. Prove that every ED is a PID.

9. Find the multiplicative inverse of $(x^2 + 1)$ modulo $x^4 + x + 1$ in $GF(2^4)$.

P.T.O.

10. Multiply $[3 \quad 1 \quad 1 \quad 2]\begin{bmatrix} FE \\ 65 \\ 7D \\ 91 \end{bmatrix}$ for mix column operation in AES using modulus polynomial $x^8 + x^4 + x^3 + x + 1$ in $GF(2^8)$.

11. Find the generator polynomial for 2 error correcting Reed-Solomon (RS) code using primitive polynomial $x^3 + x + 1$ in $\mathbb{Z}_2[x]$.

12. Define $E: \mathbb{Z}_2^2 \to \mathbb{Z}_2^5$ such that $E(w) = wG$, where $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ be generator matrix. Decode the received word 11110 using Hamming code coset Leader table.