Reg. No. : ....

Name : ....

III Semester M.Sc. Degree (C.B.C.S.S. – OBE – Regular)
Examination, October 2024
(2023 Admission)
Mathematics/Mathematics (Multivariate Calculus and Mathematical Analysis, Modelling Simulation, Financial Risk Management)
Elective Course
MSMAT03E01/MSMAF03E01 – NUMBER THEORY

Time : 3 Hours   Max. Marks : 80

PART – A

Answer **any five** questions. **Each** question carries **4** marks.

1. Prove or disprove :
   a) If $(m,n) = 1$, then $(\Phi(m), \Phi(n)) = 1$.
   b) If n is composite then $(n, \Phi(n)) > 1$.
2. Prove : m is a prime if and only if $\exp_m(a) = m - 1$ for some a.
3. Prove that 5 is a quadratic residue of an odd prime p if $p = \pm 1 \pmod{10}$ and 5 is a non residue if $p = \pm 3 \pmod{10}$.
4. Express the following polynomials in terms of elementary symmetric polynomials if possible
   i) $t_1^3 + t_2^3, (n = 2)$
   ii) $t_1 t_2^2 + t_2 t_3^2 + t_3 t_1^2, (n = 3)$.
5. Prove that the coefficients of the field polynomials are rational integers.
6. Prove that the quadratic fields are precisely those of the form $Q(\sqrt{d})$ for a square free rational integer d. **(5×4=20)**

P.T.O.

PART – B

Answer **any three** questions. **Each** question carries **7** marks.

7. If $n \geq 1$, prove that $\sum_{d/n} \Phi(d) = n$.
8. Let x be an odd integer. If $\alpha \geq 3$, prove that $x^{\frac{\Phi(2^\alpha)}{2}} \equiv 1 \left(\bmod\ 2^\alpha\right)$.
9. Let G be a free abelian group of rank n with basis $\{x_1, x_2, ..., x_n\}$ and (a_{ij}) is an $n \times n$ matrix of integer entries. Prove that the elements $y_i = \sum_j a_{ij} x_j$ form a basis of G if and only if the matrix (a_{ij}) is unimodular.
10. Prove that every number field K possess an integral basis and the additive group Θ is free abelian of rank n equal to the degree of K.
11. If $\zeta = e^{\frac{2\pi i}{5}}$, for $k = \Phi(\zeta)$, Find
    i) $N_k(\zeta + 4)$ and, $N_k(\zeta - 3)$, by using the formula $N_k(a + b - \zeta) = \dfrac{a^5 + b^5}{a + b}$.
    ii) Prove that $\zeta + 2$ has no proper factor in $Z(\zeta)$. **(3×7=21)**

PART – C

Answer **any three** questions. **Each** question carries **13** marks.

12. i) State and prove Mobius inversion formula.
    ii) Prove that the Mobius function is multiplicative but not completely multiplicative.
13. i) State and prove Gauss Lemma.
    ii) For every odd prime p, evaluate the Legendre symbol (2/p).
    iii) Prove that the Legendre symbol (n/p) is completely multiplicative.

14. i) Prove that every subgroup H of a free abelian group G of rank n is free of rank $r \leq n$.
    ii) Define R-module where R is a ring and find all submodules of Z.
15. i) Let $K = Q(\theta)$ be a number field where θ has minimum polynomial p of degree n. Prove that the Q-basis $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$ has discriminant $\Delta\left[1, \theta, \theta^2, ..., \theta^{n-1}\right] = (-1)^{\frac{n(n-1)}{2}} N\left(D\left(p(\theta)\right)\right)$.
    ii) Let $K = Q\left(\sqrt{7}\right)$. Find the norm and the trace of $a + b\sqrt{7}$ where $a, b \in Q$.
16. i) Prove that the ring of integers of $Q(\zeta)$ is $Z[\zeta]$.
    ii) If $\omega = \exp\left(\dfrac{2\pi i}{p}\right)$, find $N(1 - \omega)$, where p is an odd prime. **(3×13=39)**