D 22833 (Pages : 3) Name..

Reg. No.......................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2012

(CCSS)

Mathematics

MAT IC 05—NUMBER THEORY

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1. Prove that $\sum_{d^2|n} \mu(d) = \mu^2(n)$.

2. Assume f is multiplicative. Prove that f is completely multiplicative iff $f^{-1}(p^a) = 0$ for all primes p and all integers $a \geq 2$.

3. Prove that $\sum_{n \leq x} \lambda(n)\left[\frac{x}{n}\right] = \left[\sqrt{x}\right]$.

4. If $0 < a < b$, prove that there exists an x_0 such that $\pi(ax) < \pi(bx)$ if $x \geq x_0$.

5. Prove that $\lim_{x \to \infty}\left(\frac{M(x)}{x} - \frac{H(x)}{x \log x}\right) = 0$.

6. For $x \geq 1$, prove that $\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1)$.

7. Let p be an odd prime and let $p \equiv 1 \pmod 4$ prove that $\sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r = \frac{p(p-1)}{4}$.

8. Prove that the Legendre's symbol $(n|p)$ is a completely multiplicative function of n.

9. Determine whether 888 is a quadratic residue or non-residue of the prime 1999.

Turn over

10. Explain briefly the term 'Hash function' used in a public key cryptosystem.

11. Write a brief not on affine enciphering transformation.

12. Find the inverse of the matrix $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix}$ mod 5.

(12 × 4 = 48 marks)

Part B

Answer either A or B of each question.
Each question carries 8 marks.

II. A. (a) For $n \geq 1$, prove that $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

(b) Define Dirichlet multiplication. Show that Dirichlet multiplication is associative.

B. (a) State and prove Euler's summation formula.

(b) If $x \geq 2$, prove that $\log[x]! = x \log x - x + O(\log x)$.

III. A. (a) For $x \geq 2$, prove that $\mathcal{J}(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt$ and $\pi(x) = \frac{\mathcal{J}(x)}{\log x} + \int_2^x \frac{\mathcal{J}(t)}{t \log^2 t} dt.$

(b) Prove that the n^{th} prime p_n satisfies the inequalities.

$$\frac{1}{6} n \log n < p_n < 12\left(n \log n + n \log \frac{12}{e}\right).$$

B. Prove that the relation

$$M(x) = 0(x) \text{ as } x \to \infty$$

implies $\psi(x) \sim x$ as $x \to \infty$.

IV. A. (a) State and prove Euler's criterion.

(b) Determine those odd primes p for which 3 is a quadratic residue and those for which it is a non-residue.

B. State and prove Quadratic reciprocity law.

V. A. (a) Write a short note on digraph transformations.

(b) In the 26-letter alphabet, use the matrix $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ to encipher the plain text 'NO ANSWER'.

B. (a) Give a comparison between private key cryptosystem and public key cryptosystem.

(b) Suppose that the following 40-letter alphabet is used for all plain texts and ciphertexts : A – Z with numerical equivalents 0 – 25, black = 26, ! = 27, ? = 28, \$ = 29, the numerals 0 – 9 with numerical equivalents 30 – 39. Suppose that plaintex message units are digraphs and ciphertext message units are trigraphs. (i.e, $k = 2$, $l = 3$, $40^2 < n_A < 40^3$ for all n_A). Send the message "SEND \$7500" to a user whose enciphering key is $(n_A, e_A) = (2047, 179)$.

(4 × 8 = 32 marks)

D 22832 (Pages : 3) Name..................................

Reg. No..................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2012

(CCSS)

Mathematics

MAT 1C 04—DISCRETE MATHEMATICS

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 Let G be a simple graph and let $\delta(G) \geq \frac{n-1}{2}$. Prove that G is connected.

2 Find the automorphism group of K_3.

3 Let G be a simple graph with n vertices and $n \geq 2$. Prove that G is complete if and only if $k(G) = n - 1$.

4 Prove that every tree is a bipartite graph.

5 Give an example of Eulerian graph which is not Hamiltonian.

6 Show that the complement of a simple planar graph with 11 vertices is non-planar.

7 Prove that the intersection of any two sub-lattices of X is also a sublattice of X. Prove that this need not hold for their union.

8 Let $(X, +, \cdot, ')$ be a Boolean algebra. Prove that

(a) $x + x \cdot y = x$.

(b) $(x + y)' = x' \cdot y'$.

9 Write the following Boolean function in its disjunctive normal form.

$$f(a, b, c) = a + b + c'.$$

10 Describe the language generated by the grammar with productions

$$S \to aAb, S \to \lambda, A \to aAb, A \to \lambda.$$

Turn over

11 Find a grammar that generates the language $L = \{a^n b^m : n \geq 0, m > n\}$.

12 For $\sum = \{a, b\}$, construct a dfa that accept the set consisting of all strings that start with a 'b'.

(12 × 4 = 48 marks)

Part B

Answer A **or** B *of each question.*
Each question carries 8 *marks.*

II. A (a) Prove that the number of edges of a simple graph with w components can't exceed $\frac{(n-w)(n-w+1)}{2}$.

(b) Prove that a vertex v of a connected graph G with atleast three vertices is a cut vertex if and only if there exist vertices u and w, distinct from v, such that v is in every $u - w$ path in G.

B (a) Let δ and Δ be the minimum and maximum of the degrees of a graph. Prove that $\delta \leq \frac{2m}{n} \leq \Delta$.

(b) Let G_1, G_2 be simple graphs. Prove that $n(G_1 \times G_2) = n(G_1)\,n(G_2)$ and $m(G_1 \times G_2) = n(G_1)\,m(G_2) + m(G_1)\,n(G_2)$.

III. A (a) Prove that every connected graph contains a spanning tree.

(b) Prove that a graph is planar if and only if it is embeddable on a sphere.

B (a) Prove that a connected graph G is a tree if and only if every edge of G is a cut edge of G.

(b) Prove that $K_{3,3}$ is non-planar.

IV. A (a) Define Boolean algebra. Give an example of a distributive Boolean algebra.

(b) Discuss the natural correspondence between Boolean algebras and Boolean lattices.

B (a) Let $(X, +, ., ')$ be a finite Boolean algebra. Prove that every two distinct atoms of X are mutually disjoint.

(b) Prove that the characteristic numbers of a symmetric Boolean function completely determine it.

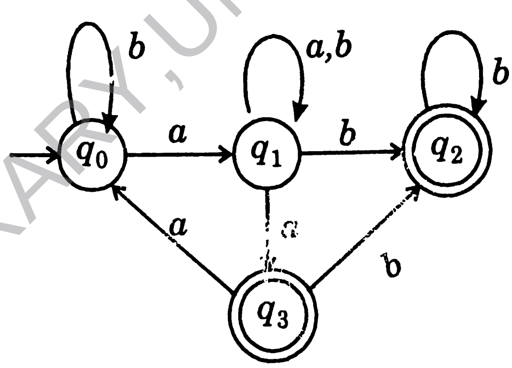
V. A (a) Let $M = (Q, \Sigma, \delta, q_0, F)$ be a dfa accepting the language L. Prove that $M' = (Q, \Sigma, \delta, q_0, Q - F)$ is a dfa accepting Σ^* / L (complement of L).

(b) Find a grammar for the language $L = \{w : |w| \bmod 3 = 0\}$ on $\sum = \{a\}$.

(c) Find an nfa with 4 states accepting the language $L = \{a^n : n \geq 0\} \cup \{b^n a : n \geq 1\}$.

B (a) Find a dfa accepting the language $L = \{ab^5 wb^4 : w \in \{a, b\}^*\}$.

(b) Convert the following dfa into an equivalent dfa.



(4 × 8 = 32 marks)

D 22831

(Pages : 3)

Name.......................................

Reg. No...................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2012

(CCSS)

Mathematics

MAT IC 03—LINEAR ALGEBRA

Time : Three Hours | Maximum : 80 Marks

Answer **all** *questions from Part A.*
Each questions carries 4 marks.
From Part B answer **either** *A or B of each questions.*
Each question carries 8 marks.

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 Verify whether $(1,2,1) \in \mathbb{R}^3$ lies in the linear span of $\{(1,0,1),(1,1,0)\}$.

2 Verify whether the set of all solutions of the system of equations :

$2x + 4y = 2$

$3x + 6y = 3$

is a subspace of $\mathbb{R}^2$.

3 Verify whether $\{(1,2,0),(1,0,2),(1,1,1)\}$ is a basis of $\mathbb{R}^3$.

4 Find the co-ordinate vector of $(1,2,3) \in \mathbb{R}^3$ w.r.t. the ordered basis. $\mathcal{B} = \{(1,1,0),(1,0,1),(0,1,1)\}$.

5 Let $T: V \to W$ be a linear transformation. Prove that T is one to-one if and only if the null space of T is zero.

6 Is it true that every one-to-one linear transformation from $\mathbb{R}^2$ to $\mathbb{R}^2$ is on to. Justify your answer.

7 Give a linear functional f on $\mathbb{R}^2$ such that $f(1, 0) = 0$ and $f(0, 1) = 1$. Find its null space.

8 Prove that similar matrices have the same characteristic polynomial.

9 Find a characteristic value of the matrix $A = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$.

Turn over

10 Let T be a linear operator with characteristic polynomial $(x-1)^3 (x-2)^2$. Describe the possible minimal polynomials of T.

11 Express $\mathbb{R}^3$ as a direct sum of a 1-dimensional subspace and a 2- dimensional subspace.

12 Let α be characteristic vector of a linear operator T. Find the dimension of the T-cycle subspace Z (α, T).

($12 \times 4 = 48$ marks)

Part B

Answer **either** *A or B of each questions.*
Each question carries 8 marks.

II. A. Let V be a vector space over a field F and W be a subset of V. Prove that the following are equivalent.

(i) For $\alpha, \beta \in W$ and $c \in F$, $\alpha + \beta \in W$ and $c\alpha \in W$.

(ii) For $\alpha, \beta \in W$ and $c \in F$, $\alpha + c\beta \in W$.

(iii) For $\alpha, \beta \in W$ and $c, d \in F$, $c\alpha + d\beta \in W$.

B. (a) Let V be a vector space spanned by $\{\beta_1, \beta_2, \ldots, \beta_m\}$. Show that any set of linearly independent vectors of V contains at most m elements.

(b) Prove that if V is a finite dimensional vector space then any two bases of V have the same number of elements.

III. A. Let V, W be vector space over a field F and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of V and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis of W. Let E_{pq} be linear transformations from V to W such that

$$E_{pq}(\alpha_i) = \begin{cases} 0 & \text{if } i \neq p \\ \beta q & \text{if } i = p \end{cases}$$

Prove that $\{E_{pq}\ p = 1, 2, \ldots, n, q = 1, 2, \ldots, m\}$ is a basis for the space L (V, W) of an linear transformations from V to W.

B. (a) Prove that every n-dimensional vector space over a field F is isomorphism to F^n.

(b) Let V be the vector space of complex number over the field R of reals. Give an isomorphism of V with $\mathbb{R}^2$.

IV. A (a) Let c be a characteristic value of a linear operator T. Prove that for every polynomial f, $f(c)$ is a characteristic value of f(T).

(b) Let $c_1, c_2, \ldots, c_k$ be distinct characteristic values of a linear operator T and W_i be the characteristics space associated with c_i. Let $W = W_1 + W_2 + \ldots + W_k$. Prove that dim $W = \dim W_1 + \dim W_2 + \ldots + \dim W_k$.

B (a) Let T be a linear operator on a finite dimensional space. Prove that the characteristic polynomial and the minimal polynomial and the minimal polynomial of T have the same roots

(b) Find the minimal polynomial of the matrix $A = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$.

V. A. Let $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$. Prove that there exist projections $E_1, E_2, \ldots, E_k$ satisfying the following :

(i) $E_i E_j = 0$ for $i \neq j$

(ii) $E_1 + E_2 + \ldots + E_k = I$.

(iii) Range of $E_i = W_i$ for every i.

B. Let T be a linear operator on a finite dimensional space V and $p = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ be the minimal polynomial of T where p_i same irreducible and $p_i \neq p_j$ for $i \neq j$. Prove that there are polynomials $h_1, h_2 \ldots, h_k$ such that

(i) $E_i = h_i(T)$ is a projection.

(ii) $E_1 + E_2 + \ldots + E_k = I$.

(iii) $E_i E_j = 0$ for $i \neq j$.

(4 × 8 = 32 marks)

D 22830 (Pages : 3)

Name..

Reg. No.....................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2012

(CCSS)

Mathematics

MAT 1C 02—REAL ANALYSIS

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 *marks.*

I. 1. Prove that every neighbourhood is an open set.

2. Let E be a nonempty subset of real numbers which is bounded above. If $y = \sup E$, then prove that $y \in \overline{E}$.

3. Construct a bounded set of real numbers with exactly three limit points.

4. Prove that compact subsets of metric spaces are closed sets.

5. Prove that continuous image of connected spaces are connected.

6. Prove that the set of discontinuities of a monotonic function on an open interval is atmost countable.

7. Let $f_1, f_2, ..., f_k$ be real functions on a metric space X and let f be the mapping of X into $\mathbb{R}^k$ defined by $f(x) = (f_1(x), f_2(x), ..., f_k(x))$.

   Prove that f is continuous if and only if each of the functions $f_1, f_2, ..., f_k$ is continuous.

8. Evaluate $\lim_{x \to 0} \frac{x - \sin x}{x^3}$.

9. Let $f \in \mathcal{R}(\alpha_1)$ and $f \in \mathcal{R}(\alpha_2)$. Prove that $f \in \mathcal{R}(\alpha_1 + \alpha_2)$ and

   $\int_a^b f \, d(\alpha_1 + \alpha_2) = \int_a^b f \, d\alpha_1 + \int_a^b f \, d\alpha_2$.

10. Let α be a monotonically increasing function on $[a, b]$ and let f be any real valued function on $[a, b]$. If P' is a refinement of the partition P of $[a, b]$, then prove that $U(P', f, \alpha) \le U(P, f, \alpha)$.

11. Prove that every uniformly convergent sequence of bounded functions is uniformly bounded.

Turn over

12. Let $f_n(x) = \begin{cases} 0 & \text{if } x < \frac{1}{n+1} \\ \sin^2 \frac{\pi}{x} & \text{if } \frac{1}{n+1} \le x \le \frac{1}{n}. \\ 0 & \text{if } x > \frac{1}{n} \end{cases}$

Show that $\{f_n\}$ converges to a continuous function, but not uniformly convergent.

(12 × 4 = 48 marks)

Part B

Answer A **or** *B of each question.*
Each question carries 8 *marks.*

II. A. (a) Prove that the set of rational numbers is countable.

(b) Let X be a metric space and $E \subset X$. Prove that

(i) $\overline{E}$ is closed.

(ii) $E = \overline{E}$ if and only if E is closed.

B. (a) Prove that a set E is open if and only if its complement E^c is closed.

(b) Let E be an infinite subset of a compact set K. Prove that E has a limit point in K.

III. A. (a) Let f be a continuous mapping of a compact metric space X into a metric space Y. Prove that f uniformly continuous on X.

(b) State and prove Taylor's theorem.

B. (a) Let E be a noncompact set in $\mathbb{R}^1$. Prove that there exists a continuous and bounded function on E which has no maximum.

(b) Let f be a real continuous function on a compact metric space X and let $M = \sup_{x \in X} f(x)$, $m = \inf_{x \in X} f(x)$. Prove that there exist points $p, q \in X$ such that $f(p) = M$ and $f(p) = m$.

IV. A. (a) Let α be monotonically increasing and $\alpha' \in \mathcal{R}$ on $[a, b]$. Let f be a bounded real function on $[a, b]$. Prove that $f \in \mathcal{R}(\alpha)$ if and only if $f\alpha' \in \mathcal{R}$. In that case prove that

$$\int_a^b f \, d\alpha = \int_a^b f(x)\, \alpha'(x)\, dx.$$

(b) If f is continuous, then prove that $f \in \mathcal{R}(\alpha)$ on $[a, b]$.

B. (a) Let $f \in \mathcal{R}(\alpha)$ on $[a, b]$. Prove that $|f| \in \mathcal{R}(\alpha)$ on $[a, b]$ and $\left|\int_a^b f d\alpha\right| \leq \int_a^b |f| d\alpha$.

(b) Let $\{f_n\}$ be a sequence of functions defined on E. Let $\lim_{n \to \infty} f_n(x) = f(x)$ for all $x \in X$ and let $M_n = \sup_{x \in E} |f_n(x) - f(x)|$. Prove that $f_n \to f$ uniformly if and only if $M_n \to 0$ as $n \to \infty$.

V. A. (a) Let K be compact metric space and $\{f_n\}$ be a sequence of continuous functions on K such that $f_n(x) \geq f_{n+1}(x)$ for all $x \in K$ and $n = 1, 2, 3, \ldots$ If $\{f_n\}$ converges pointwise to a continuous function f on K, then prove that $f_n \to f$ uniformly on K.

(b) Let K be a compact metric space and let $f_n \in \mathcal{C}(K)$ for $n = 1, 2, 3, \ldots$ and $\{f_n\}$ converges uniformly on K. Prove that $\{f_n\}$ is equicontinuous on K.

B. (a) Let $f_n \to f$ uniformly on a set E in a metric space. Let x be a limit point of E and let $\lim_{t \to x} f_n(t) = A_n$ for $n = 1, 2, 3, \ldots$ Prove that $\{A_n\}$ converges and $\lim_{t \to x} f(t) = \lim_{n \to \infty} A_n$.

(b) Let $\{f_n\}$ be a sequence of functions differentiable on $[a, b]$ and such that $\{f_n(x_0)\}$ converges for some point x_0 in $[a, b]$. If $\{f'_n\}$ converges uniformly on $[a, b]$, then prove that $\{f_n\}$ converges uniformly on $[a, b]$ to a function f and $f'(x) = \lim_{n \to \infty} f'_n(x)$ for all $x \in [a, b]$.

(4 × 8 = 32 marks)

D 22829

(Pages : 3)

Name.......................................

Reg. No...................................

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2012

(CCSS)

Mathematics

MAT 1C 01—ALGEBRA—I

Time : Three Hours

Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 marks.

I. 1 How many abelian groups (upto isomorphism) are there of order 24 ? Of order 25 ? Of order (24) (25) ?

2 Show that if H and N are subgroups of a group G, and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.

3 Show that the converse of the theorem of Lagrange is false.

4 Let X be a G-set, show that for each $g \varepsilon G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \varepsilon X$ is a permutation of X.

5 Show that if N is a normal subgroup of a group G, and if H is any subgroup of G, then HVN = HN = NH.

6 Let G be a group generated by $A = \{a_i : i \varepsilon I\}$ and let G' be any group. Show that of a_i' for $i \varepsilon I$ are any elements in G', not necessarily distinct, then there is atmost one homomorphism $\phi : G \to G'$ such that $\phi(a_i) = a_i'$.

7 Let G be a finite group and let a prime p divide $|G|$. Show that if G has precisely one proper sylow p-subgroup, then G is not simple.

8 Show that a group G of order 48 has a normal subgroup of either order 16 or order 8.

9 Describe the field F of quotients of the integral subdomain $D = \{m + ni : m, n \varepsilon Z\}$ of C.

10 Prove that if D is an integral domain, the D [x] is an integral domain.

11 Factorize the polynomial $x^4 + 4$ in $Z_5[x]$ into linear factors $Z_5[x]$.

12 Show that if F is a field, then every ideal in F [x] is principal.

($12 \times 4 = 48$ marks)

Turn over

Part B

Answer **A** *or* **B** *of each question.*
Each question carries 8 marks.

II. A (a) Show that if a positive integer n is written as a product of powers of two distinct primes, as in $n = (P_1)^{n_1} \cdot (P_2)^{n_2}$, then Z_n is isomorphic to $Z_{(P_1)^{n_1}} \times Z_{(P_2)^{n_2}}$.

(5 marks)

(b) Give the order of the element $(2, 0) + \langle(4,4)\rangle$ in $Z_6 \times Z_8 / \langle(4,4)\rangle$. (3 marks)

B (a) Show that the set of all commutators $aba^{-1}b^{-1}$ of a group G generates a normal subgroup C of G, and that G/C is abelian.

(4 marks)

(b) Find all composition series of $Z_5 \times Z_5$. (4 marks)

III. A (a) Let X be a G-set. For $x_1, x_2 \varepsilon x$, let $x_1 \sim x_2$ if and only if there exists $g \varepsilon G$, such that $gx_1 = x_2$. Show that '$\sim$' is an equivalence relation on X.

(3 marks)

(b) Let G be a finite group and X a finite G-set. Show that if r is the number of orbits in X under G, then $r.|G| = \sum_{g \varepsilon G} |X_g|$.

(5 marks)

B. (a) Let H be a subgroup of a group G and let N be a normal subgroup of G. Show that $\frac{HN}{N} \simeq \frac{H}{H \cap N}$.

(4 marks)

(b) Show that a subgroup K of a solvable group G is solvable. (4 marks)

IV. A (a) Let G be a group of order p^n, where p is a prime, and let X be a finite G-set show that $|X| \equiv |X_G| \pmod{p}$, where $X_G = \{x \varepsilon X : gx = x \text{ for all } g \varepsilon G\}$.

(2 marks)

(b) State and prove first sylow theorem. (2 + 4 = 6 marks)

B (a) Show that for a prime p, every group of order p^2 is abelian. (4 marks)

(b) Let F be a field of quotients of an integral domain D and let L be any field containing D. Show that there exists a map $\psi : F \rightarrow L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for $a \varepsilon D$.

(4 marks)

V. A (a) State and prove Division Algorithm for F [x], F is a field. (2 + 4 = 6 marks)

(b) Is $\dfrac{Q[x]}{\langle 2x^{10} - 25x^3 + 10x^3 - 30\rangle}$ a field, Justify your answer. (2 marks)

B (a) Let R be a commutative ring with unity, and let M $\neq$ R be an ideal in R. Show that M is a maximal ideal of R iff R/M is a field.

(6 marks)

(b) Show that if R is a ring with unity and N is an ideal of R containing a unit, then N = R.

(2 marks)

(4 × 8 = 32 marks)