D 73257 (Pages : 3) Name.......................................

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2014

(CCSS)

Mathematics

MAT 1 C 05 NUMBER THEORY

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1 If $d(n)$ denotes the number of positive divisors of n, prove that $d(n)$ is odd if n is a square.

2 Define the Möbius function $\mu(n)$ and prove that for $n \geq 1$, $\sum_{d/n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$.

3 Prove that $[2x] - 2[x]$ is either 0 or 1.

4 For $x \geq 2$, prove that $\pi(x) = \frac{I(x)}{\log x} + \int_2^x \frac{I(t)}{t \log^2 t} dt$.

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

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

7. Let p be an odd prime. Prove that every reduced residue system mod p contains exactly $\frac{(p-1)}{2}$ quadratic residues mod p.

8 For every odd prime p, prove that $(2/p) = (-1)^{(p^2-1)/8}$.

9 Evaluate the Jacobi symbol $(-68/665)$.

10 What do you mean by crypt analysis. Explain with an example.

11 Find the inverse of the matrix $\begin{pmatrix} 40 & 0 \\ 0 & 21 \end{pmatrix}$ mod 841.

12 Define Hash function. Give an example.

($12 \times 4 = 48$ marks)

Turn over

Part B

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

II. A (a) If f is an arithmetical function with $f(1) \neq 0$, show that there is a unique arithmetical function f^{-1} such that $f * f^{-1} = f^{-1} * f = I$. Also determine f^{-1} using recursion formulas.

(b) State and prove the Selberg identity.

B (a) If $x \geq 1$, prove that $\sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + G(s) + O(x^{-s})$ if $s > 0$, $s \neq 1$.

(b) For $x \geq 1$, prove that

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right] = 1 \text{ and } \sum_{n \leq x} \wedge(n) \left[\frac{x}{n}\right] = log[x]!$$

III. A (a) State and prove Abel's identity.

(b) For every integer $n \geq 2$, prove that

$$\pi(n) < 6 \frac{n}{\log n}.$$

B (a) Let $\{a_n\}$ be a non-negative sequence such that

$$\sum_{n \leq x} a(n) \left[\frac{x}{n}\right] x \log x + O(x) \quad \text{for all} \quad x \geq 1.$$

Prove that there is a constant $A > 0$ and an $x_0 > 0$ such that $\sum_{n \leq x} a(n) \geq Ax$ for all $x \geq x_0$.

(b) If $A(x) = \sum_{n \leq x} \frac{\mu(n)}{n}$, prove that the relation $A(x) = 0(1)$ as $x \to \infty$ implies the prime number theorem.

IV. A (a) Prove that the legendre symbol (n/p) is a completely multiplicative function of n.

(b) State and prove Gauss lemma.

B (a) Prove that the Diophantine equation $y^2 = x^3 + k$ has no solutions if k has the form $k = (4n-1)^3 - 4m^2$ where m and n are integers. Such that no prime $p \equiv -1 \pmod 4$ divides m.

(b) Let p be an odd prime. Prove that $\sum_{r=1}^{p-1} r\,(r/p) = 0$ if $p \equiv 1 \pmod 4$.

A (a) Write a short note on offline enciphering transformations.

(b) The message " KVW ? TA ! KJB ? FVR ". Is intercepted and the first six letters of the plain text are " C.I.A". (The blanks after ? and R of the message are part of the message but the final. is not a part of the message). It is known that for sending the message a linear enciphering transformation is used with a 30 letter alphabet, in which A – Z have numerical equivalents 0 – 25, blank = 26, ? = 27, ! = 28, . = 29. Find the deciphering matrix A^{-1} and the full plain text message.

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

(b) What do you mean by RSA cryptosystem.

(4 × 8 = 32 marks)

D 73256 **(Pages : 3)** **Name....................................**

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2014

(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 Prove that the sequence d = (7, 6, 3, 3, 2, 1, 1, 1) is not graphical.

2 Let V (D) be the vertex set and let m (D) be the number of edges in a digraph D. Prove that :

$$\sum_{v \in V(D)} d^+(v) = \sum_{v \in V(D)} d^-(v) = m(D).$$

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

4 Show that a connected k-regular bipartite graph is 2-connected.

5 Define Hamiltonian graphs. Give an example of a non-Hamiltonian traceable graph.

6 Prove that for a simple planar graph G, $\delta(G) \leq 5$.

7 Let u and v be strings. Prove that $|uv| = |u| + |v|$.

8 Let $L \subseteq \{a, b\}^*$ be a regular language. Is $\{a, b\}^* - L$ is regular ? Justify your answer.

9 Let $G = (\{S\}, \{a, b\}, S, P)$ be a grammar with productions P given by $S \to a\,Sb \mid \lambda$. Find the language generated by the grammar.

10 Let X be a finite set and let P (X) be its power set. Prove that inclusion is a partial order on P (X). Is it a total order ? Justify your answer.

11 Define a lattice. Give an example of a lattice and draw its lattice diagram.

12 Let $(X, +, ., ')$ be a finite Boolean algebra. Prove that ever non-zero element of X contains atleast one atom.

(12 × 4 = 48 marks)

Part B

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

II. A (a) Let G_1 and G_2 be graphs. Prove that $n(G_1 \times G_2) = n(G_1)\, n(G_2)$ and $m(G_1 \times G_2) = n(G_1)\, m(G_2) + m(G_1)\, n(G_2)$, where $n(G)$ and $m(G)$ denote the number of vertices and edges in G.

(b) Prove that, for any loopless connected graph G, $k(G) \leq \lambda(G) \leq \delta(G)$.

B (a) Let G be a simple graph. If G is not connected, then prove that G^c is connected.

(b) Show that the automorphism group of K_n is isomorphic to the symmetric group S_n of degree n.

(c) Let D be a digraph with no directed cycles. Prove that there exists a vertex whose indegree is zero.

III. A (a) Prove that a simple graph is a tree if and only if any two distinct vertices are connected by a unique path.

(b) Prove that the following are equivalent for a conneted graph G :

(i) G is Eulerian.

(ii) The degree of each vertex of G is an even positive integer.

(iii) G is an edge-disjoint union of cycles.

B (a) Prove that, for a connected plane graph G, $n - m + f = 2$, where f denotes the number of faces of G.

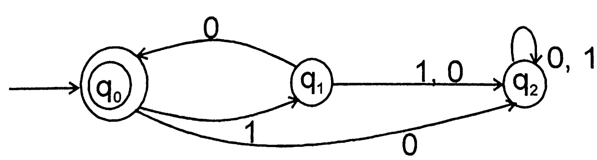
(b) Prove that $K_{3,\,3}$ is non-planar.

IV. A (a) Let $G = (\{S\}, \{a, b\}, S, P)$ be a grammar with production P given by $S \to SS \mid \lambda \mid a\,Sb \mid b\,Sb$. Find the language generated by G.

(b) Give a grammar that generates all reals in $\mathbb{C}$.

B (a) Let $M = (Q, \Sigma, \delta, q_0, F)$ be a deterministic finite accepter and let G_m be its associated transition graph. Prove that for every $q_i, q_j \in Q$ and $w \in \Sigma^+$, $\delta^*(q_i, w) = q_j$ if and only if there is in G_M a walk with label w from q_i to q_j.

(b) Find the language accepted by the following non-deterministic finite acceptor :



V. A (a) Let $(X, \leq)$ be a partially ordered set and A be a non-empty finite subset of X. Prove that A has atleast one maximal element.

(b) Let $d_1, d_2, \ldots, d_n$ be integers such that for all $i = 1, 2, \ldots, n$, $0 \leq d_i \leq n - i$. Prove that there exists a unique permutation $x = x_1 x_2 \ldots x_n$ of $\{1, 2, \ldots, n\}$ whose inversion table is $(d_1, d_2, \ldots, d_n)$.

B (a) Let $(X, +, ., ')$ be a finite Boolean algebra. Prove that every element of X can be uniquely expressed as a sum of atoms.

(b) Prove that the set of all symmetric Boolean functions of n variables $x_1, x_2, \ldots x_n$ is a subalgebra of all Boolean functions of these variables.

(4 × 8 = 32 marks)

D 73255 (Pages : 3) Name.....................................

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2014

(CCSS)

Mathematics

MAT IC 03—LINEAR ALGEBRA

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1 For any two real numbers x and y, let $S = \{(x,y) : x^2 + y^2 = a^2 (a \neq 0)\}$. Is the set S a subspace of the two dimensional Euclidean space ? Justify your claim.

2 Show that the vectors $\alpha_1 = (1,0,-1), \alpha_2 = (1,2,1), \alpha_3 = (0,-3,2)$ form a basis for $\mathbb{R}^3$.

3 Define $T : R^2 \to R^2$ by the rule $T(x, y) = (x, \sin y)$. Is T a linear transformation ? Justify your claim.

4 Let V be a finite dimensional vector space. What is the minimal polynomial for the identity operator on V.

5 Let T be the linear operator on R^2 defined by $T(x_1, x_2) = (-x_2, x_1)$. What is the matrix of T in the standard basis for R^2 ?

6 Prove that every matrix A such that $A^2 = A$ is similar to a diagonal matrix.

7 Let V and W be finite dimensional vector spaces over the field F. Prove that V and W are isomorphic only if dim V = dim W.

8 Define dual space of a vector space. What is the relation connecting the dimensions of a finite dimensional vector space and its dual space.

9 If T and U are linear operators on $\mathbb{R}^2$ defined by $T(x_1, x_2) = (x_2, x_1)$ and $U(x_1, x_2) = (x_1, 0)$, define the operator UT + TU.

10 Prove that similar matrices have the same characteristic polynomial.

11 For any operator T, prove that every T-conductor divides the minimal polynomial for T.

12 Let V be a finite dimensional vector space and W_1 be any subspace of V. Prove that there is a subspace W_2 of V such that $V = W_1 \oplus W_2$.

($12 \times 4 = 48$ marks)

Turn over

Part B

Answer **either** *A* **or** *B of each question.*

Each question carries 8 *marks.*

II. A (a) Show that any linearly independent subset of a finite dimensional vector space is the part of a basis.

(b) Find a basis for vector space of all polynomials of degree n.

B (a) Let V be a finite dimensional vector space over F and let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an ordered basis for V. Let W be a vector space over the same field F and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be any vectors in W. Prove that there is precisely one linear transformation T from V into W such that $T_{\alpha_j} = \beta_j$; $j = 1, 2, \ldots, n$.

(b) Is there exists a linear transformation T from $\mathbb{R}^3$ into $\mathbb{R}^2$ such that :

$T(1,-1,1) = (1,0), T(1,1,1) = (0,1)$? If exists, find the rank and nullity of T.

III. A (a) Let T be a linear transformation from V into W. Prove that T is non-singular if and only if T carries each linearly independent subset of V onto a linearly independent subset of W.

(b) Let T be a linear operator on $\mathbb{R}^3$ defined by $T(x_1, x_2, x_3) = (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3)$. Is T invertible ?

B (a) If T is a linear transformation from a finite dimensional vector space V to itself and $\mathcal{B}$ is an ordered basis of V, prove that if T is invertible then $[\,T\,]_{\mathcal{B}}$ is invertible and $[\,T^{-1}]_{\mathcal{B}} = [\,T\,]_{\mathcal{B}}^{-1}$.

(b) Let T be a linear operator on $\mathbb{R}^3$ defined by :

$T(x_1, x_2, x_3) = (3x_1 + x_3, -2x_1 + x_2, -x_1 + 2x_2 + 4x_3)$. What is the matrix of T in the standard ordered basis for $\mathbb{R}^3$?

IV. A (a) If T is a linear transformation form a finite dimensional vector space V to a finite dimensional vector space W, prove that rank (T^t) = rank (T).

(b) Let T be a linear operator on a finite dimensional vector space V. Let $c_1, c_2, \ldots, c_k$ be the distinct characteristic values of T and let $W_i = N(T - c_i I)$. Prove that T is diagonalizable if and only if $\dim W_1 + \dim W_2 + \ldots + \dim W_k = \dim V$.

B (a) Prove that if A is a companion matrix of a monic polynomial p, then p is both the minimal and characteristic polynomial of A.

(b) Let F be a field and let B be an $n \times n$ matrix over F. Then prove that B is similar over the field F to one and only one matrix which is in the rational form.

V. A State and prove the Cayley - Hamilton theorem.

B State and prove the Primary Decomposition theorem.

($4 \times 8 = 32$ marks)

D 73254 (Pages : 3) Name..................................

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2014

(CCSS)

Mathematics

MAT IC 02—REAL ANALYSIS

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1 Prove that a finite point set has no limit points.

2 Let E be a nonempty set of real numbers which is bounded above and let $y = \sup E$. Prove that $y = \in \bar{E}$.

3 Define connected sets. Is interior of a connected set connected ? Justify your answer.

4 Let f be a continuous real function on a metric space Y and let $Z(f) = \{p \in Y : f(p) = 0\}$. Prove that Z (p) is a closed subset of Y.

5 Let f be a differentiable function on $[a, b]$. Prove that f' cannot have any simple discontinuity on $[a, b]$.

6 Show by an example that mean value theorem for real valued functions need not be true for vector valued functions.

7 Let f, g be bounded functions and α be monotonic increasing function on $[a, b]$. If f and g be Riemann-Steiltjes integrable with respect to α on $[a, b]$, then prove that $f + g$ is Reimann-Steiltjes integrable with respect to α and

$$\int_a^b (f+g)\, d\alpha = \int_a^b f\, d\alpha + \int_a^b g\, d\alpha.$$

8 For $1 < s < \infty$, define $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Prove that

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{\infty} \frac{x - [x]}{x^{s+1}}\, dx,$$

where $[x]$ denote the greatest integer less than or equal to x.

9 Give an example of a convergent series of continuous functions with discontinous sum.

Turn over

10 Prove that uniformly convergent sequence of bounded functions is uniformly bounded.

11 Let $f(x)=\sum_{n=1}^{\infty} \frac{1}{1+n^2x}$. For what values of x ndoes the series converge absolutely ?

12 Does a uniformly bounded sequence has a uniformly convergent subsequence ? Justify your answer.

Part B

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

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

(b) Prove that compact subsets of a metric space are closed.

B. (a) Let $\{I_n\}$ be a sequence of intervals in $\mathbb{R}^1$ such that $I_n \supset I_{n+1}$ for each n = 1, 2, . . . Prove that $\bigcap_{n=1}^{\infty} I_n$ is not empty.

(b) Let P be a nonempty perfect set in $\mathbb{R}^1$. Prove that P is uncountable.

III. A. (a) Let Y and Z be metric spaces, $E \subset Y$, $p \in E$ and f maps E into Z. Prove that f is continuous at p if an only if $\lim_{x \to p} f(x) = f(p)$.

(b) Let E be a noncompact bounded set in $\mathbb{R}^1$. Prove that there exists a continuous function on E which is not uniformly continuous.

B. (a) Let f be a continuous mapping of a compact metric space Y into a metric space Z. Prove that f is uniformly continuous on Y.

(b) Let f be monotonic on (a, b). Prove that the set of points on (a, b) at which f is discontinuous is atmost countable.

IV. A. (a) Let f be continuous and α be monotonic and continuous on $[a, b]$. Prove that f is Riemann-Stieltjes integrable with respect to α on $[a, b]$.

(b) Let F and G be differentiable functions on $[a, b]$. If $F' = f$ and $G' = g$ are Riemann integrable, then prove that

$$\int_a^b F(x)\, g(x)\, dx = F(b)\; G(b) - F(a)\, G(a) - \int_a^b f(x)\, G(x)\, dx.$$

B. (a) Let α be monotonically increasing and α' be Riemann integrable on $[a, b]$. If f is a bounded real function on $[a, b]$, then prove that f is Riemann-Stieltjes integrable with respect to α if and only if $f\,\alpha'$ is Riemann integrable. Also prove that

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

(b) Let $\{f_n\}$ be a sequence of functions defined on E and let $|f_n(x)| \leq M_n$ for all $x \in E$ and for each $n = 1, 2, \ldots\ldots$ If $\sum M_n$ converges, then prove that $\sum f_n$ converges uniformly.

V. A. (a) Let f_n be a sequence of continuous functions on E and let $f_n \to f$ uniformly on E. Prove that f is continuous on E.

(b) Prove that there exists a real continuous function on the real line which is nowhere differentiable.

B. State and prove Stone Weierstrass theorem.

(4 × 15 = 60 marks)

D 73253 **(Pages : 3)** Name..................................

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2014

(CCSS)

Mathematics

MAT IC 01—ALGEBRA – I

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1 Find the order of the element $(3, 6, 12, 16)$ in $Z_4 \times Z_{12} \times Z_{20} \times Z_{24}$.

2 Let H and K be subgroups of a group G. Give an example showing that $H \simeq K$ while G/H is not isomorphic to G/K.

3 Find all composition series of $S_3 \times Z_2$.

4 Let X be a G-set. Show that $G_x : \{g \in G \mid gx = x\}$ is a subgroup of G for each $x \in X$.

5 Show that a subgroup K of a solvable group G is solvable.

6 Let G be a free group on $A = \{a_i : i \in I\}$ and let G' be any group. Show that if α_i' for $i \in I$ are any elements in G', not necessarily distinct, then there is exactly 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 Find the class equation of S_3.

9 Describe the field F of quotients of the integral subdomain :

$D = \{n + m\sqrt{2} : n, m \in Z\}$ of R.

10 Show that an element a in a field F is a zero of $F = [x]$ iff $(x - a)$ is a factor of $f(x)$ in $F = [x]$.

11 Factorize the polynomial $x^3 + 2x^2 + 2x + 1$ into linear factors in $Z_7[x]$.

12 Let F be a field. Show that an ideal $\langle p(x) \rangle \neq \{0\}$ of $F(x)$ is maximal iff $p(x)$ is irreducible over F.

(12 × 4 = 48 marks)

Turn over

Part B

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

II. A (a) Let be a subgroup of a group G. Show that the following are equivalent :

(i) $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

(ii) $gHg^{-1} = H$ for all $g \in G$.

(iii) $gH = H_g$ for all $g \in G$.

(b) Show that A_n is a normal subgroup of S_n and compute $\frac{S_n}{A_n}$.

B (a) Show that the converse of the theorem of Lagrange is false.

(b) Show that the finite indecomposable Abelian groups are exactly the cyclic groups with order a power of a prime.

III. A (a) State and prove second isomorphism theorem.

(b) 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.

B (a) Let X be a G-set. Show that for each $g \in G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Further show that the map of $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

(b) Find the number of distinguishable ways the edges of a square cardboard can be pointed if six colors of paint are available, no color is used more than once and the same color can be used on any number of edges.

IV. A (a) State and prove Third Sylow theorem.

(b) Show that every group of prime-power order is solvable.

B (a) Show that if H and K are finite subgroups of a group G, then $|HK| = \frac{(|H|)\cdot(|K|)}{|H \cap K|}$.

(b) Show that no group of order 36 is simple.

A (a) Show that if F is a field, then every non-constant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit factors in F.

(b) Show that the cyclotomic polynomial :

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over Q for any prime p.

B (a) Show that the multiplicative group of all non-zero elements of a finite field is cyclic.

(b) Find all generators of the cyclic multiplicative group of units of the field Z_{17}.

($4 \times 8 = 32$ marks)

D 53277 **(Pages : 3)** Name.................................

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2014

(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 Find all integers n such that $\phi(n) = \frac{n}{2}$.

2 Define the Mangoldt's function $\wedge(n)$ and prove that for $n \geq 1$,

$$\sum_{d/n} \wedge(d) = \log n.$$

3 Prove that for $x \geq 2$,

$$\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2}\log^2 x + A + O\left(\frac{\log x}{x}\right),$$

where A is a constant.

4 For $x \geq 2$, prove that

$$\vartheta(x)\ \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,dt.$$

5 For a positive integer n, prove that $2^n \leq \binom{2n}{n} < 4^n$.

6 Prove that for every $n > 1$, there exists n consecutive composite numbers.

7 Prove that the Legendre's symbol (n/p) is a completely multiplicative function of n.

8 If P is an odd positive integer, prove that $(2/P) = (-1)P^2 - 1/8$.

9 Determine whether -104 is a quadratic residue or non-residue of the prime 997.

10 In the 27 letter (with blank = 26) use affine enciphering transformation with $a = 13$, $b = 9$ to encipher the message "GIVE ME".

Turn over

11 Working in 26 letter alphabet and using the matrix $\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$ decipher the ciphertex "QVNAYQSHI".

12 How will you authenticate a message in electronic communication ?

(12 × 4 = 48 marks)

Part B

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

II. (A) (a) If $n \geq 1$, prove that

$$\phi(n) = \sum_{d/n} \mu(d) \cdot \frac{n}{d}.$$

(b) Prove that the set of all arithmetical functions f with $f(1) \neq 0$ is a group under Dirichlet multiplication.

(B) (a) Using Euler's Summation formula deduce that $\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2} \log^2 x + A + O\left(\frac{\log x}{x}\right)$ where A is a constant and $x \geq 2$.

(b) For $x \geq 2$, prove that $\sum_{p \leq x} \left[\frac{x}{P}\right] \log p = x \log x + O(x)$

where the sum is extended over all primes $\leq x$.

III. (A) (a) For $x > 0$, prove that

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x} \log 2}.$$

(b) If $x \geq 2$, let Li $(x) = \int_2^x \frac{dt}{\log t}$.

Prove that

$$L_i(x) = \frac{x}{\log x}\left(1 + \sum_{K=1}^{n-1} \frac{k!}{\log^k x}\right) + n! \int_2^x \frac{dt}{\log^{n+1} t} + C_n$$

where C_n is independent of x.

(B) Prove that the prime number theorem implies $\lim_{x \to \infty} \frac{M(x)}{x} = 0$.

IV. (A) (a) Let p be an odd prime. Prove that every reduced residue system mod p contains exactly $\left(\frac{p-1}{2}\right)$ quadratic residues.

(b) State and prove the Quadratic reciprocity law.

(B) (a) Define the Jacobi symbol (n/p). If P and Q are odd positive integers, prove that

(i) $(n/p)\,(n/Q) = (n/PQ)$.

(ii) $(m/p) = (n/p)$ = whenever $m \equiv n \pmod{P}$.

(b) Let P be an odd prime. Prove that $\sum_{r=1}^{p-1} r^3 (r/p) = \frac{3}{2} p \sum_{r=1}^{p-1} r^2 (r/p)$ if $p \equiv 1 \pmod{4}$.

V. (A) (a) Write a brief note on enciphering matrix.

(b) The message " ! IWGVIEX ! ZRADRYD" send using a linear enciphering transformation of di-graph vectors in a 29-letter alphabet in which A-Z have numerical equivalents 0–25, blank = 26, ? = 27, ! = 28 was intercepted and the last five letters of plain text are the sender's signature "MARIA". Find the deciphering matrix and read the message.

(B) (a) Write a short note on Public Key cryptosystem.

(b) Explain the RSA cryptosystem, illustrating with an example.

(4 × 8 = 32 marks)

D 53276 (Pages : 3) Name..................................

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2014

(CCSS)

Mathematics

MAT IC 04—DISCRETE MATHEMATICS

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1 Define self-complementary graphs. If G be a self-complementary graph of order n, then prove that $n \equiv 0$ or $1 \pmod 4$.

2 Let G be a graph with n vertices and $\delta \geq \frac{n-1}{2}$. Prove that G is connected.

3 Show that no vertex v of a simple graph can be a cut vertex of both G and G^C.

4 Construct a graph with $k = 3, \lambda = 4$ and $\delta = 5$.

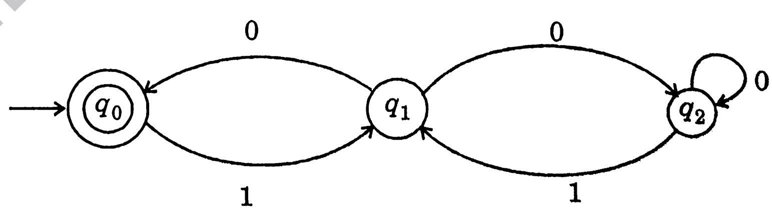
5 Is every graph with n vertices and $n-1$ edges a tree ? Justify your answer.

6 Prove that a graph is planar if and only if it is embeddable on a sphere.

7 Let $G = (\{S\}, \{a, b\}, S, P)$ be a grammar with productions P Given by $S \to aS \mid b \} \lambda$. Find the language generated by the grammar G.

8 Show that the language $L = \{awa : w \in \{a, b\}^*\}$ is regular.

9 Find the language accepted by the following nondeterministic finite accepter.



Turn over

10. Define strict partial order and give an example of it. If S is a strict partial order on a set X, then prove that $S \cup \{(x, x) : x \in\}$ is a partial order on X.

11. Prove that intersection of two chains is a chain. Is union of chains a chain ? Justify your answer.

12. Let $(X, +, ., ')$ be a Boolean algebra. Prove that $(x')' = x$ for all $x \in X$.

(12 × 4 = 48 marks)

Part B

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

II. (A) (a) Prove that the number of odd degree vertices in a given graph G is even.

(b) Prove that, in a connected graph G with atleast three vertices, any two longest paths have a vertex in common.

(B) (a) Let G_1 and G_2 be vertex disjoint graphs. Prove that

$n(G_1 \vee G_2) = n(G_1) + n(G_2)$ and $m(G_1 \vee G_2) = m(G_1) + m(G_2)$, where $n(G)$ and $m(G)$ denote the number of vertices and edges in G.

(b) Prove that a connected graph G with atleast two vertices contains atleast two vertices that are not cut vertices.

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

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

(c) If G is Hamiltonian, then prove that for every nonempty proper subset S of the vertex set V, $w(G - S) \leq |S|$.

(B) (a) Let G be a plane graph and f be a face of G. Prove that there exists a plane embedding of G in which f is the exterior face.

(b) Prove that K_5 is nonplanar.

IV. (A) (a) Find a grammar for the language $L = \{a^n a^m : n \geq 0, m > n\}$ on $\sum = \{a, b\}$.

(b) Find a deterministic finite accepter that recognizes the set of all strings on $\sum = \{a, b\}$ starting with a prefix ab.

(B) Establish the equivalence of deterministic and nondeterministic acceptors.

(A) (a) Let $(X, \leq)$ be a poset and let A be non-empty finite subset of X. prove that A has atleast one maximal element.

(b) Prove that in the lexicographic ordering for the set of all permuations of n symbols, the permutation whose inversion table is $(d_1, d_2, \ldots d_n)$ has index (or rank)

$$1 + d_1 (n-1)! + d_2 (n-2)! + \ldots + d_i (n-i)! + \ldots + d_{n-1} 1! + d_n 0!.$$

(B) (a) Prove that every finite Boolean algebra is isomorphic to a power set Boolean algebra.

(b) Write the following Boolean function in their disjunctive normal form

$$f(x_1, x_2, x_3) = (x_1 + x_2')x_3' + x_2 x_1' (x_2 + x_1' x_3).$$

(4 × 8 = 32 marks)

D 53274 **(Pages : 4)** **Name....................................**

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2014

(CCSS)

Mathematics

MAT IC 02—REAL ANALYSIS

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*

Each question carries 4 *marks.*

I. 1 Let X be a metric space, $E \subset X$ and let E° denote the set of interior points of E. Prove that E is open if and only if $E^{\circ} = E$.

2 Prove that closed subsets of a compact set are compact.

3 For $x, y \in \mathbb{R}^1$, let $d(x, y) = \dfrac{|x-y|}{1+|x-y|}$. Is d a metric on $\mathbb{R}^1$? Justify your answer.

4 Let f be a continuous mapping of a compact metric space Y into a metric space Z. Prove that $f(Y)$ is compact.

5 Let f be a real valued uniformly continuous function on the bounded set E in $\mathbb{R}^1$. Prove that f is bounded on E.

6 Let f be differentiable in (a, b). If $f'(x) \geq 0$ for all $x \in (a, b)$, then prove that f is monotonically increasing.

7 Let $f \geq 0$, f be continuous and $\int_a^b f(x)\,dx = 0$. Prove that $f(x) = 0$ for all $x \in [a, b]$.

8 Let f be a bounded function and α be a monotonic increasing function on $[a, b]$. If f Riemann-Stieltjes integrable with respect to α, then prove that $|f|$ is Riemann-Stieltjes integrable with respect to α on $[a, b]$ and $\left|\int_a^b f\,d\alpha\right| \leq \int_a^b |f|\,d\alpha$.

9 Is the curve $\gamma : [-2, 2] \to \mathbb{R}^2$ defined by $\gamma(x) = \left(x, 2\sqrt{x}\right)$ rectifiable ? Justify your answer.

Turn over

10 Prove that the series $\sum_{n=1}^{\infty} (-1)^n \frac{x^2+n}{n^2}$ converges uniformly in every bounded interval.

11 Define equicontinuous family of functions and give an example of it.

12 Prove that the uniform closure of an algebra of bounded functions is a uniformly closed algebra.

(12 × 4 = 48 marks)

Part B

Answer A **or** *B of each question.*

Each question carries 8 marks.

II. A. (i) Prove that countable union of countable sets is countable.

(ii) Let Y be a metric space and $E \subset Y$. Prove that the following are equivalent.

(a) $\bar{E}$ is closed.

(b) $E = \bar{E}$ if and only if E is closed.

(c) $\bar{E} \subset F$ for every closed set $F \subset Y$ such that $E \subset F$.

B. (i) Let $E \subset \mathbb{R}^k$. Prove that the following are equivalent.

(a) E is closed and bounded.

(b) E is compact.

(c) Every infinite subset of E has a limit point in E.

(ii) Prove that Cantor set is perfect.

III. A. (i) If f is a continuous map from a metric space X into a metric space Y. Prove that $f(\bar{E}) \subset \overline{f(E)}$.

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

$$f(x) = (f_1(x), f_2(x), \ldots, f_k(x)),$$

where $x \in X$. Prove that f is continuous if and only if each of the functions $f_1, f_2, \ldots, f_k$ is continuous.

(iii) Let f be a bijective continuous mapping of a compact metric space X onto a metric space Y. Prove that the inverse of f is a continuous map from Y onto X.

B. (i) Describe discontinuities of first and second kinds with the help of examples.

(ii) Let f be a continuous mapping of $[a, b]$ into $\mathbb{R}^k$ and f be differentiable in (a, b). Prove that there exists $x \in (a, b)$ such that $|f(b) - f(a)| \leq (b - a) |f'(x)|$.

IV. A. (i) Let f be continuous and α be monotonic increasing on $[a, b]$. Prove that f is Riemann-Stieltjes integrable with respect to α on $[a, b]$.

(ii) Let f be Riemann integrable and for $a \leq x \leq b$, let

$$F(x) = \int_a^t f(t)\,dt.$$

Prove that F is continuous on $[a, b]$.

B. (i) Let f be a bounded function and let α_1, α_2 be monotonic increasing on $[a, b]$. If f is Riemann-Stieltjes integrable with respect to α_1 and α_2, then prove that f is Riemann-Stieltjes integrable with respect to $\alpha_1 + \alpha_2$ and

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

(ii) Let γ be a curve in $\mathbb{R}^1$, defined on $[a, b]$. If γ' is continuous, then prove that γ is rectifiable and

$$\wedge(\gamma) = \int_a^b |\gamma'(t)|\,dt.$$

V. A. (i) Let α be monotonically increasing on $[a, b]$. Let f_n be Riemann-Stieltjes integrable with respect to α on $[a, b]$, for $n = 1, 2, 3, \ldots$ and let $f_n \to f$ uniformly on $[a, b]$. Prove that f is Riemann-Stieltjes integrable with respect to α on $[a, b]$ and

$$\int_a^b f\,d\alpha = \lim_{n\to\infty} \int_a^b f_n\,d\alpha.$$

(ii) Let K be compact and let $f_n \in C(K)$ for each $n = 1, 2, \ldots$. If $\{f_n\}$ is pointwise bounded and equicontinuous, then prove that $\{f_n\}$ is uniformly bounded on K.

B. (i) Let $\{f_n\}$ be a sequence of functions, differentiable on $[a, b]$ such that $\{f_n(x_0)\}$ converges for some point x_0 on $[a, b]$. 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 $[a, b]$.

(ii) Let K be compact and let $f_n \in C(K)$ (set of all complex valued continuous functions of K) for each $n = 1, 2, \ldots$ If $\{f_n\}$ converges uniformly on K, then prove that $\{f_n\}$ is equicontinuous on K.

(4 × 8 = 32 marks)

D 53273 (Pages : 3) Name..............................

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

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, JANUARY 2014

(CCSS)

Mathematics

MAT IC 01—ALGEBRA—I

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1 Find the order of the element $(3,3)+\langle(1,2)\rangle$ in the factor group $Z_4 \times Z_8 / \langle(1,2)\rangle$.

2 Show that M is a maximal normal subgroup of a group G iff G/M is simple.

3 Find the center of $S_3 \times Z_4$.

4 Let X be a G-set and let $Y \subseteq X$. Show that $G_Y = \{g \in G : gy = y \text{ for all } y \in Y\}$ is a subgroup of G.

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

6 Let K and L be normal subgroups of a group G with $K \vee L = G$ and $K \cap L = \{e\}$. Show that $G/K \simeq L$ and $G/L \simeq K$.

7 Show that any two sylow p-subgroups of a finite group G are conjugate.

8 Show that for a prime number p, every group G of order p^2 is abelian.

9 Show that any two fields of quotients of an integral domain D are isomorphic.

10 Let F be a field. Show that a non-zero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in the field F.

11 Show that a factor ring of a field is either the trivial ring of one-element or is isomorphic to the field.

12 Show that if R is a ring with unity 1, then the map $\phi : Z \to R$ given by $\phi(n) = n \cdot 1$ for $n \in Z$ is a homomorphism of Z into R.

(12 × 4 = 48 marks)

Turn over

Part B

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

II. A (a) Let H be a subgroup of a group G. Show that the left coset multiplication is well defined by the equation :

$(aH)(bH) = (ab)H$

iff left and right cosets coincide.

(b) Let H be a normal subgroup of a group G, and let $m = (G : H)$. Show that $a^m \varepsilon H$ for every $a \varepsilon G$.

B (a) Show that if a group G has a composition series, and if N is a proper normal subgroup of G, then there exists a composition series containing N.

(b) Give isomorphic refinements of the two series :

$\{0\} < \langle 18 \rangle < \langle 3 \rangle < Z_{72}$

and $\{0\} < \langle 24 \rangle < \langle 12 \rangle < Z_{72}$.

III. A (a) Let X be a G-set and let $x \varepsilon X$. Show that $|G_x| = (G : G_x)$.

(b) Find the number of distinguishable ways the edges of an equilateral triangle can be painted if four different colours of paint are available, assuming only one colour is used X on each edge, and the same colour may be used on different edges.

B (a) Let a group G be generated by $A = \{a_i : i \varepsilon I\}$ and G' be any group. Show that if a_i' for $i \varepsilon I$ are any elements in G', not necessarily district, then there is at most one homomorphism $\phi : G \to G'$ such that $\phi(a_i) = a_i'$. Show further that if G is free on A, then there is exactly one such homomorphism.

(b) How many different homomorphisms are there for a free group of rank 2 into S_3 ?

IV. A (a) State and prove first Sylow theorem.

(b) Show that every group of order $(35)^3$ has a normal subgroup of order 125.

B (a) Let p be a prime and let G be a group of order p^n. Show that if X is a finite G-set, then $|X| \equiv |X_G| \pmod{p}$.

(b) Show that if p and q are distinct primes with $p < q$ and if q is not congruent to 1 modulo p, then every group G of order pq is abelian and cyclic.

V. A (a) State and prove Einstein criteria for irreducibility.

(b) Demonstrate that $x^3 + 3x^2 - 8$ is irreducible over Q.

B (a) Let R be a commutative ring with unity. Show M is a maximal ideal of R iff R/M is a field.

(b) Find all prime ideals and all maximal ideals of Z_{12}.

(4 × 8 = 32 marks)

First Semester M.Sc Degree Examination
Mathematics
Model Question Paper 2014 Admissions
MAT1C02: Linear Algebra

Time: 3hrs. Max.Mark:60

Part A
Answer four questions form this part
Each questions carries 3 marks

1. Does there exists a linear transformation T: $R^3 \rightarrow R^3$ such that T(1,0,1)=(1,1), T(-1,-1,0)= (1,2) and T(0,1,1)=(2,1) ? Why?

2. Let T: $R^3 \rightarrow R^3$ be defined by T(x,y)=(x+y, 2x). Find the matrix of T with respect to the usual basis of R^2.

3. Let V=R^3 and S= {(1,0,0),(1,1,0)}. Find the annihilator S^o?

4. Prove that if T is a linear operator on F^n such that T^2=T, where F is either C or R, then T is diagonalizable.

5. Prove that the T-Cyclic subspace z(∝:T) is one dimensional if and only if ∝ is a characteristic vector for T.

6. Let V be a inner product space and let x ε V prove that if <x,y>=0 for all yεV then x=0.

Part B
Answer any four questions from this part without omitting any unit.
Each question carries 12 marks.
Unit – I

7. a) Let V and W be vector spaces over the field F and let T be a linear transformation from V into W. Prove that if V is finite dimensional, then rank(T) + nullity T = dim V
   b) Find a basis for the space L(R^2, R^3) over R.

8. a) Let B and B' be two ordered bases for an n dimensional vector space V over the field F and T be a linear operator on V. Then prove that there exist an invertible nxn matrix P over F such That $[T]_{B'}= D^{-1}[T]_B P$

   b) Find range an null space of the linear operator T(a,b,c)=(a+b,2c,0) on R^3.

9. a) Let V be a finite dimensional vector space over a field F. Let {e_1,e_2,......., e_n}be a basis of V. Describe the dual basis and show that it is a basis for the dual space V*.
   b) Let V=R^3 over R. Give a basis for V and give the dual basis.

Unit- II

10. a) Prove the Cayley-Hamilton theorem.

b) Let A and B be nxn matrices over a field F. Prove that if I-AB is invertible then I-BA is also invertible. Deduce that AB and BA have the same characteristic values.

11. a) Let T be a linear operator on an n-dimensional vector space V. Then prove that the characteristic and minimal polynomials for T have same roots, except for multiplicities.

b) Fine the minimal polynomial for $A=\begin{bmatrix} 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ -2 & -2 & 2 & 1 \\ 1 & 1 & -1 & 0 \end{bmatrix}$

12. a) State and prove a necessary and sufficient condition for a linear operator on a finite dimensional vector space to be triangularly.

b) Find an invertible matrix P such that $P^{-1}AP$ is a diagonal matrix,

where $A=\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$

Unit III

13. a) State and prove primary decomposition theorem.

b) if $T(x_1,x_2)= (2x_1, x_2, -x_1)$ find a diagonalizable operator D and a nilpotent operator N on R^2 such that T=D+N

14. a) Define a cyclic vector for a linear operator T of a vector space. If a linear operator T of a finite dimensional vector space has a cyclic vector show that dim V is the same as the degree of the minimal polynomial of T.

b) Let T has a diagonalizable operator of n-dimensional vector space. If T has a cyclic vector show that T ahs r distinct characteristic values.

15. a) Define an inner product space. Prove that an orthogonal set of non-zero vector in an inner product space is linearly independent.

b) If W is a finite – Dimensional subspace of an inner product space V then show that $V=W\oplus W^{\perp}$ where is the orthogonal complement of $W^{\perp}$ in V.

First Semester M.Sc Degree Examination
Mathematics
Model Question Paper 2014 Admissions
MAT1C01: Basic Abstract Algebra

Time: Three Hours | Maximum : 60 Marks

Part A

Answer four questions from this part.

Each question carries 3 marks.

1. Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic ? Why or why not ?.
2. Let X be a G-set. Then prove that G_x is a subgroup for each $x \in X$.
3. Prove that no group of order 20 is simple.
4. Is $\{(2,1),(4,1)\}$ a basis for $\mathbb{Z} \times \mathbb{Z}$? Prove your assertion.
5. Factorize $f(x) = x^4 + 3x^3 + 2x + 4$ in $\mathbb{Z}_5[x]$.
6. Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x] / \langle x^2 + c \rangle$ is a field.

Part B

Answer **4** questions from this part without omitting any Unit. Each question carries **12** marks.

UNIT I

7. (*a*) Prove that direct product of abelian groups is abelian.

   (*b*) Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m,n) = 1$.

8. (*a*) Let X be a G-set and let $x \in X$. Then prove the following:

   (i) $|Gx| = (G : G_x)$

   (ii) If $|G|$ is finite then $|Gx|$ is a divisor of $|G|$

   (*b*) Prove Cauchy's theorem for groups.

9. (a) Prove that every group of prime power order is solvable.

(b) Prove that for a prime number p, every group of order p^2 is abelian.

UNIT I I

10. (a) Prove that any two fields of quotients of an integral domain D are isomorphic.

(b) Find the elements of □ that makes up the field of quotient of

$D = \{n + mi : n, m \in □\}$ in □

11. (a) State and prove second isomorphism theorem.

(b) Prove that two subnormal series of a group G have isomorphic refinements.

12. (a) If G is a nonzero free abelian group with a finite basis of r elements, then prove that G is isomorphic to $□ \times □ \times \cdots \times □$ for r factors.

(b) Prove that every finitely generated abelian group is isomorphic to a group of the form $□_{m_1} \times □_{m_2} \times \cdots \times □_{m_r} \times □ \times □ \times \cdots \times □$ where m_i divides m_{i+1} for $i = 1, 2, \cdots, r-1$.

UNIT I I I

13. (*a*) Prove Evaluation homomorphism theorem.

(*b*) Prove that $R[x]$ is a ring if R is a ring.

14. (*a*) Prove Eisenstein criteria.

(*b*) Prove that the cyclotomic polynomial is irreducible over □.

15. (*a*) Prove that R/M is a field if and only if M is a maximal ideal of R.

(*b*) Prove that and ideal $< p(x) > \neq \{0\}$ of $F[x]$ is maximal if and only if p(x) is irreducible over F.