C 33204 (Pages : 4) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 05—NUMBER THEORY

(2017 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 marks.

1. Prove that the Dirichlet multiplication is commutative and associative.
2. If $x \geq 2$, prove that :

   $\log [x]! = x \log x - x + O(\log x)$.
3. For $x \geq 2$, prove that :

   $$I(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t}\, dt.$$
4. Prove that $\lim_{x \to \infty} \left(\frac{M(x)}{x} - \frac{H(x)}{x \log x} \right) = 0$.
5. Prove that every reduced residue mod p contains exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic non-residues mod p where p is an odd prime.
6. Evaluate the Legendre's symbol $(13/31)$.
7. What is meant by cryptosystem ?
8. Explain how to authenticate a message in public key cryptography.

(8 × 2 = 16 marks)

Turn over

Part B

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

9. If $n \geq 1$, prove that :

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

10. State and prove Euler's summation formula.

11. For $n \geq 1$, prove that the n^{th} prime P_n satisfies the inequalities :

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

12. For every odd prime p, prove that :

$$(2/p) = (-1)^{p^2-1/8}.$$

13. Determine whether 219 is a quadratic residue or non-residue mod 383.

14. Find the inverse of the matrix $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix} \bmod 29$.

(4 × 4 = 16 marks)

Part C

Answer **either** *A* **or** *B of each question.*
Each question carries 12 marks.

15. A (a) Let f be multiplicative. Prove that f is completely multiplicative if and only if $f^{-1}(n) = \mu(n) f(n)$ for all $n \geq 1$.

(b) Define the divisor functions $\sigma_\alpha(n)$. If $n \geq 1$, prove that :

$$\sigma_\alpha^{-1}(n) = \sum_{d \mid n} d^\alpha \cdot \mu(d) \cdot \mu\left(\frac{n}{d}\right).$$

B If $n \geq 1$, prove that :

(a) $$\sum_{n \leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right).$$

(b) $$\sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} G(s) + O\left(x^{-s}\right) \text{ if } s > 0, s \neq 1.$$

16. A For every integer $n \geq 2$, prove that :

$$\frac{1}{6}\frac{n}{\log n} < \pi(n) < 6 \cdot \frac{n}{\log n}.$$

B (a) Prove that there is a constant A such that :

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + A + O\left(\frac{1}{\log x}\right) \text{ for all } x \geq 2.$$

(b) If $a > 0$ and $b > 0$, then prove that :

$\pi(ax)/\pi(bx) \sim a/b$ as $x \to \infty$.

17. A (a) State and prove Gauss Lemma.

(b) Determine those odd primes p for which $(-3/p) = 1$ and those for which $(-3/p) = -1$.

B (a) If p and q are distinct odd primes, then prove that :

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

(b) Prove that the Diophantine equation $y^2 = x^3 + k$ has no solution 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.

18. A (a) Explain briefly about affine enciphering transformations.

(b) The message "SONAFQCHMWPTVEVY", resulted from a linear enciphering transformation of digraph vectors, where the sender used the usual 26-letter alphabet A – Z with numerical equivalents 0 – 25 respectively, was intercepted. It was found that the most frequently occurring ciphertext digraphs were "KH" and "XW" and suppose that those digraphs correspond to "TH" and "HE" respectively. Find the deciphering matrix and read the message.

B (a) Describe briefly about public key cryptosystem.

(b) Suppose that the following 40-letter alphabet is used for all plaintexts and ciphertexts : A – Z with numerical equivalents 0 – 25, blank = 26, · = 27, ? = 28, $ = 29, the numerals 0 – 9 with numerical equivalents 30 – 39. Suppose that plaintext 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 × 12 = 48 marks)

C 33203 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 04—DISCRETE MATHEMATICS

(2017 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 *marks.*

1. Define automorphism of a simple graph. Illustrate it using an example.
2. Let G be a simple connected graph. Prove *or* disprove : If G has a cut edge then G has a cut vertex.
3. Prove that every connected graph contains a spanning tree.
4. Define (a) plannar graph ; (b) plane graph ; (c) plane embedding and explain with example.
5. Give an example of a partial order relation which is not total.
6. Define a Boolean Algebra. Give an example.
7. Define a grammar and the language generated by this grammar. Illustrate.
8. Define a regular language. Give an example.

(8 × 2 = 16 marks)

Part B

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

9. Define vertex connectivity and connectivity. Also prove that a simple graph G with n vertices is complete if and only if $K(G) = n - 1$.
10. Define isomorphism of graphs. Illustrate. If G and H are simple graphs and $\varphi : V(G) \to V(H)$ is a bijection such that $uv \in E(G) \Rightarrow \varphi(u)\,\varphi(v) \in E(H)$ then show that φ need not be an isomorphism.
11. Prove the following :
    (a) A tree with at least two vertices contains at least two pendant vertices.
    (b) Every tree is a bipartite graph.

Turn over

12. For any simple plannar graph, prove that $\delta(G) \leq 5$.

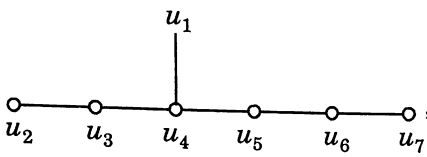
13. Let S be a set of statements. Define $p \leq q$ to mean ϕ implies q. Verify whether $\leq$ is reflexive, symmetric and transitive. Is it anti-symmetric. Justify your claim.

14. Find the dfa for the language $L = \{w : | w | \bmod 3 = 0\}$ on $\sum = \{a, b\}$.

(4 × 4 = 16 marks)

Part C

Answer **either** *A* **or** *B of each of the following* **four** *questions.*
Each question carries 12 *marks.*

15. A (a) If G : 

, find Aut (G).

(b) Show by an example that $G_1[G_2]$ need not be isomorphic to $G_2[G_1]$, where G_1 and G_2 are two simple graphs.

B (a) Prove that a graph is bipartite if and only if it contains no odd cycles.

(b) Prove that a connected graph G with at least 2 vertices contains at least 2 vertices that are not cut vertices.

16. A If G is a simple graph, prove that the following are equivalent :

(i) G is a tree.

(ii) $m = n - 1$ and G is connected.

(iii) Any two distinct vertices are connected by a unique path.

B For a non-trivial connected graph G, prove the following are equivalent.

(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.

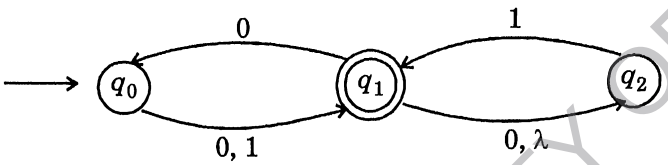
17. A (a) Define a Boolean Algebra. Give an example.

(b) State and prove any five properties of a Boolean Algebra.

B (a) If $(X, \leq)$ is a partially ordered set and A is a non-empty finite subset of X, prove that A has a maximum element if and only if it has a maximal element.

(b) Define symmetric Boolean functions with respect to a pair of variables x_i and x_j. Give an example.

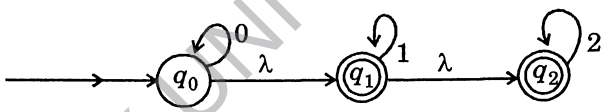
A (a) Convert the *nfa* given by the transition graph into an equivalent *dfa* :



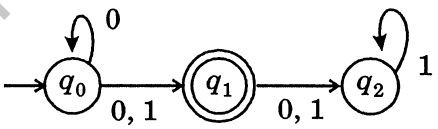
(b) Construct one grammar for :

$$L = \{w \in \{a, b\}^* : w = w^*\}, \sum = \{a, b\}.$$

(c) Determine the *dfa* equivalent to the *nfa* given by the transition graph :



B (a) Convert the following *nfa* into an equivalent *dfa* :



(b) Define regular languages. Illustrate with an example.

(4 × 12 = 48 marks)

C 33202 (Pages : 4) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 03—REAL ANALYSIS—I

(2017 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 *marks.*

1. Prove that balls in $\mathbb{R}^k$ are convex sets.
2. Give an example of a bounded set of real numbers with exactly *two* limit points.
3. Let $f : \mathbb{R} \to \mathbb{R}$ be a function defined by $f(x) = [x]$, where $[x]$ denote the largest integer less than or equal to x. What discontinuities does the function f have ?
4. Let f be differentiable and $f'(x) \leq 0$ for all $x \in (a, b)$. Prove that f is monotonically decreasing on (a, b).
5. Let α be a monotonically increasing function on $[a, b]$ and let f_1, f_2 be a real bounded functions on $[a, b]$. If f_1 and f_2 are Riemann-Stieltjes integral with respect to α $(f \in \mathcal{R}(\alpha))$ on $[a, b)$, then prove that $f_1 + f_2$ is Riemann–Stieltjes integral with respect to α on $[a, b]$.
6. Let α be a monotonically increasing function on $[a, b]$ and let f be a real bounded function on $[a, b]$. If f is Riemann-Stieltjes integral with respect to α on $[a, b]$, then prove that $|f|$ is Riemann-Stieltjes integral with respect to α on $[a, b]$.
7. Give an example of a convergent sequence of continuous functions whose limit is not continuous.
8. Prove that every uniformly convergent sequence of bounded functions is uniformly bounded.

$(8 \times 2 = 16$ marks)

Part B

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

9. Prove that a subset E of a metric space X is open if and only if its complement E^c is closed.
10. Prove that every closed subset of a compact set is compact.

Turn over

11. Let f be a continuous map from a metric space X into a metric space Y. If E is a connected subset of X, then prove that $f(E)$ is a connected subset of Y.

12. Let a and c be real numbers, $c > 0$ and f be defined on $[-1, 1]$ by :

$$f(x) = \begin{cases} x^a \sin\left(x^{-c}\right) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}.$$

Prove that $f'(0)$ exists if and only if $a > 1$.

13. Let α be a monotonically increasing function on $[a, b]$ and let f be a real bounded function on $[a, b]$. If f is continuous on $[a, b]$, then prove that f is Riemann–Stieltjes integral with respect to α $(f \in \mathcal{R}(\alpha))$ on $[a, b]$.

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

$(4 \times 4 = 16$ marks)

Part C

Answer A *or* B *of the following questions.*
Each question carries 12 *marks*

Unit I

15. (A) (a) Let $\{G_\alpha\}$ be a collection of open sets in a metric space X. Prove that the $\bigcup_\alpha G_\alpha$ is open in X.

(b) If E is an infinite subset of a compact space K, then prove that E has a limit point in K.

(c) Prove that nonempty perfect sets in $\mathbb{R}^k$ is uncountable.

(B) (a) Prove that finite point set has no limit points.

(b) Let X be a metric space and $E \subset Y \subset X$. Prove that E is closed if and only if $E = \overline{E}$.

(c) Let X be a metric space and $K \subset Y \subset X$. Prove that K is compact relative to X if and only if K is compact relative to Y.

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

UNIT II

16. (A) (a) Let X and Y be metric spaces and $f : X \to Y$ be a function. Prove that f is continuous if and only if $f^{-1}(V)$ is open in X for every open set V in Y.

(b) Prove that continuous image of a compact space is compact.

(c) Prove that monotonic functions have no discontinuities of the second kind.

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

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

UNIT III

17. (A) (a) Let α be a monotonically increasing function on $[a, b]$ and let f be a real bounded functions on $[a, b]$. Prove that $f \in \mathcal{R}(\alpha)$ on $[a, b]$ if and only if for every $\in > 0$ there exists a partition P of $[a, b]$ such that :

$$U(P, f, \alpha) - L(P, f, \alpha) < \in.$$

(b) Let γ be a curve on $[a, b]$. if γ' is continuous on $[a, b]$, then prove that γ is rectifiable and

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

(c) State and prove fundamental theorem of integral calculus.

(B) (a) 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 $U(P', f, \alpha) \leq U(P, f, \alpha)$.

(b) Let α be monotonically increasing and α' is Riemann integrable $(\alpha' \in \mathcal{R})$ 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

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

UNIT IV

18. (A) (a) Let X be a metric space and let $C(X)$ be the set of all complex valued, continuous, bounded functions with domain X. Prove that $C(X)$ is a complete metric space under the metric d given by :

$$d(f, g) = \sup_{x \in x} |f(x) - g(x)|.$$

(b) Let $\{f_n\}$ be a sequence of functions differentiable on $[a, b]$ and such that $\{f_n(x_0)\}$ converges forsome 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 $x \in [a, b]$.

(c) Let K be a compact metric space and let $f_n \in C(K)$ 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 be a continuous complex function on $[a, b]$. Prove that there exists a sequence of polynomials P_n such that

$$\lim_{n \to \infty} P_n(x) = f(x)$$

uniformly on $[a, b]$.

(b) Prove that the uniform closure of the set of all polynomials on $[a, b)$ is the set of all continuous functions on $[a, b]$.

$(4 \times 12 = 48$ marks)

C 33201 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 02—LINEAR ALGEBRA

(2017 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 2 *marks.*

1. Define linearly dependent subset of a vector space and show that if two vectors are linearly dependent then one of them is a scalar multiple of the other.
2. Show that if V is a finite-dimensional vector space, then any two bases of V have the same number of elements.
3. Define trace of a square matrix A of order n and show that the trace function is a linear functional on the matrix space $F^{n \times n}$.
4. Show that if S is any subset of a finite-dimensional vector space V, then $(S^o)^o$ is the subspace spanned by S.
5. Prove that similar matrices have the same characteristic polynomial.
6. Define minimal polynomial for a linear operator on a vector space and find a 3×3 matrix over R for which the minimal polynomial is $(x - 1)$.
7. Prove that if E is the projection on R along N of a vector space V, then $(I - E)$ is the projection on N along R.
8. Write any vector α in the inner product space R^2 as a linear combination of the vectors (1, 0) and (0, 1).

$(8 \times 2 = 16$ marks)

Part B

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

9. Let V be a vector space over the field F. Show that the intersection of any collection of subspaces of V is a subspace of V.
10. Find the co-ordinate matrix of the vector (1, 0, 1) in the basis of C^3 consisting of the vectors $(2i, 1, 0)$, $(2, -1, 1)$, $(0, 1 + i, 1 - i)$, in that order.

Turn over

11. Let V and W be vector spaces over the field F and let T be a linear transformation from V into W. Show that if T is invertible, then the inverse function T^{-1} is a linear transformation from W onto V.

12. Let T be a linear operator on the n-dimensional vector space V, and suppose that T has n-distinct characteristic values. Prove that T is diagonalizable.

13. Let E be a projection of a vector space V and let T be a linear operator on V. Prove that the range of E is invariant under T iff E T E = T E.

14. Apply the Gram–Schmidt process to the vectors $\beta_1 = (1, 0, 1), \beta_2 = (1, 0, -1), \beta = (0, 3, 4)$, to obtain an orthonormal basis for R^3 with the standard inner product.

(4 × 4 = 16 marks)

Part C

Answer **either** (A) **or** (B) *of each of the* **four** *questions.*
Each question carries 12 *marks.*

15. (A) Show that if W_1 and W_2 are finite-dimensional subspaces of a vector space V, then $W_1 + W_2$ is finite-dimensional and $\dim W_1 + \dim W_2 = \dim(W_1 \cap W_2) + \dim(W_1 + W_2)$.

(B) Let V and W be vector spaces over the field F and let T be a linear transformation from V into W. If V is finite-dimensional, then show that :

rank (T) + nullity (T) = dimV.

16. (A) Let V and W be finite-dimensional vector spaces over the field F such that dim V = dim W. Show that if T is a linear transformation from V into W, then the following are equivalent :

(i) T is invertible.

(ii) T is non-singular.

(iii) T is onto.

(iv) If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis for V, then $\{T\alpha_1, T\alpha_2, \ldots, T\alpha_n\}$ is a basis for W.

(B) Let W be the subspace of R^5 spanned by the vectors :

$\alpha_1 = (2, -2, 3, 4, -1), \alpha_2 = (-1, 1, 2, 5, 2), \alpha_3 = (0, 0, -1, -2, 3), \alpha_4 = (1, -1, 2, 3, 0)$. Describe W^o and find a basis for W^o.

17. (A) Let A be the 4×4 real matrix $A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ -2 & -2 & 2 & 1 \\ 1 & 1 & -1 & 0 \end{bmatrix}$. Show that the characteristic polynomial for A is $x^2 (x-1)^2$ and that it is also the minimal polynomial.

(B) Let V be a finite-dimensional vector space over the field F and let T be a linear operator on V. Show that T is diagonalizable iff the minimal polynomial for T has the form $p = (x-c_1)\ldots(x-c_k)$ where $c_1, c_2, \ldots, c_k$ are distinct elements of F.

18. (A) (a) Let W be a finite-dimensional subspace of an inner product space V and let E be the orthogonal projection of V on W. Show that E is an idempotent linear transformation of V onto W, $W^{\perp}$ is the null space of E, and $V = W \oplus W^{\perp}$.

(b) Illustrate the result in Part (a) by a example.

(B) Show that if $V = W_1 \oplus \ldots \oplus W_k$ then there exist k linear operators $E_1, E_2, \ldots, E_k$ on V such that :

(i) Each E_i is a projection.

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

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

(iv) The range of E_i is W_i.

Conversely, show that If $E_1, \ldots, E_k$ are k linear operators on V satisfying conditions (i), (ii) and (iii), and if we let W_i be the range of E_i, then $V = W_1 \oplus \ldots \oplus W_k$.

($4 \times 12 = 48$ marks)

C 33200 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 01—ALGEBRA–I

(2017 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question is of 2 *marks.*

1. Verify whether (1, 1) is a generator of the group $\mathbb{Z}_2 \times \mathbb{Z}_4$.
2. Verify whether $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ definedby $\phi(x, y) = (x, y + 1)$ is an isometry of the plane.
3. Describe the factor group $\mathbb{Z}/2\mathbb{Z}$.
4. Find all zeros of the polynomial $x^2 - 2$ in $\mathbb{Z}_7$.
5. Verify whether $x^2 — 2$ is irreducible in $\mathbb{Z}_5[x]$.
6. Verify whether $N = \{f(x) \in \mathbb{Q}[x] : f(2) = 0\}$ is an ideal in $\mathbb{Q}[x]$.
7. Find the irreducible polynomial for y $\sqrt{1+\sqrt{3}}$ over $\mathbb{Q}$.
8. Find a generator of the multiplicative group of the field $\mathbb{Z}_7$.

(8 × 2 = 16 marks)

Part B

Answer any **four** *questions.*
Each question is of 4 *marks.*

9. Find the order of (8, 4) in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{60}$.
10. Show that the composition of two isometries of the plane is again an isometry.
11. Let H, K be groups and $\pi : H \times K \to H$ be defined by $(h, k) \mapsto h$. Show that (H × K) / ker π is isomorphic to H.

Turn over

12. Prove that the field of quotients of the integral domain $\mathbb{Z}$ is isomorphic to $\mathbb{Q}$.

13. Let $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Prove that if $f(x)$ is reducible then $f(x)$ has a zero in F.

14. Verify whether the field $\mathbb{R}$ of reals is an algebraic extension of the field $\mathbb{Q}$ of rationals.

(4 × 4 = 16 marks)

Part C

Answer either part A **or** *part B of each of the* **four** *questions.*
Each question is of 12 *marks.*

15 A (a) Describe the direct product H × K of two groups H and K. Verify the group axioms on H × K.

(b) Show that $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime.

Or

B Let G, G' be groups and $\phi : G \to G'$ be a homomorphism with ker $\phi = H$:

(a) Prove that product in G / H defined by $Ha\ Hb = Hab$ is well defined.

(b) Prove that the map $\mu : G/H \to G'$ defined by $\mu(Ha) = \phi(a)$ for all $Ha \in G/H$ is well defined.

(c) Let $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ be defined by $\phi(k) = 2k$. Show that $\mathbb{Z}_{10} / \ker \phi$ is isomorphic to $\mathbb{Z}_5$.

16 A (a) Define simple groups and maximal normal subgroups.

(b) Show that M is a maximal normal subgroup of a group G if and only if G / M is simple.

(c) Describe the commutator subgroup of the symmetric group S_3.

Or

B Let F be the field of quotients of an integral domain D. With the usual notations prove the following.

(a) the map $i : D \to F$ defined by $i(a) = [a, 1]$ is an isomorphism from D into F.

(b) Let L be any field containing D. Show that there exists an isomorphism $\Psi : F \to L$ such that $\Psi(a) = a$ for all $a \in D$.

17 A (a) State and prove division algorithm in the polynomial ring F [x] where F is a field.

(b) Show that if $a \in F$ is a zero of $f(x) \in F[x]$ then $(x - a)$ is a factor of $f(x)$.

Or

B (a) Define maximal ideal of a ring R.

(b) Find all maximal ideals of the ring $\mathbb{Z}_{10}$.

(c) Let R be a commutative ring with unity and M be an ideal of R. Show that M is a maximal ideal if and only if R/M is a field.

18 A Let F be a field and $p(x)$ be an irreducible polynomial in F $[x]$ of degree $n > 1$. Let I be the ideal generated by $p(x)$. Prove that :

(a) E = F $[x]$ / I is a field.

(b) $p(x)$ has a zero in E.

(c) Degree of E over F is n.

Or

B (a) Prove that every finite extension of a field F is an algebraic extension of F.

(b) Let F, E, K be fields such that E is an extension of F and K is an extension of E. Prove that [K : F] = [K : E] [E : F].

(4 × 12 = 48 marks)

C 33199 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 05—NUMBER THEORY

(2008 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1 If $n \geq 1$, prove that :

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

2 Prove that the equation $f(n) = \sum_{d \mid n} g(d)$ implies $g(n) = \sum_{d \mid n} f(d) \cdot \mu(n/d)$.

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

4 Define the Chebyshev's functions $\psi(x)$ and $\vartheta(x)$ and give a relation connecting them.

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

6 For all $x \geq 1$, prove that :

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + 0(1).$$

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

8 Evaluate the Legendre's symbol $(19 \mid 31)$.

9 If P is an odd positive integer prove that :

$$(2 \mid p) = (-1)^{(p^2-1)/8}.$$

Turn over

10 What is meant by digraph transformations ?

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

12 How will you authenticate a message in electronic communication ?

(12 × 4 = 48 marks)

Part B

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

II. A (a) Prove that $\frac{n}{\phi(n)} = \sum_{d^2 \mid n} \frac{\mu^2(d)}{\phi(d)}$.

(b) If both g and $f * g$ are multiplicative, prove that f is also multiplicative.

B (a) If $x \geq 1$, prove that :

$$\sum_{n \leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right).$$

(b) If $x \geq 1$, prove that :

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right] = 1.$$

(c) State and prove Legendre's identity.

III. A (a) For $x \geq 2$, prove that :

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t \log^2 t}\, dt.$$

(b) Prove that the following two relations are equivalent :

(i) $\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right)$.

(ii) $\vartheta(x) = x + O\left(\frac{x}{\log x}\right)$.

B For every integer $n \geq 2$, prove that :

$$\frac{1}{6} \frac{n}{\log n} < \pi(n) < 6 \frac{n}{\log n}.$$

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

(b) Determine those odd primes p for which $(-3/p) = 1$ and those for which $(-3 \mid p) = -1$.

B (a) Let p be an odd prime. Prove that :

$$\sum_{r=1}^{p-1} r^2 (r \mid p) = p \sum_{r=1}^{p-1} r (r \mid p) \text{ if } p \equiv 3 (\text{mod } 4).$$

(b) State and prove the reciprocity law for Jacobi symbols.

V. A (a) The ciphertext "OFJDFOHFXOL" was intercepted. The ciphertext was enciphered using an affine transformation of single-letter plaintext units in the 27-letter alphabet (with blank = 26) and the first word is "I" ("I followed by blank). Determine the enciphering key and read the message.

(b) Write a brief note on public key cryptosystem.

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

(b) What is meant by RSA cryptosystem ?

(4 × 8 = 32 marks)

C 33198 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 04—DISCRETE MATHEMATICS

(2008 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*

Each question carries 4 *marks.*

I. 1 Prove that the sum of degree of vertices of a simple graph is even. Illustrate it with an example. Use this result to prove the number of vertices of odd degree in any simple graph is even.

2 Let G be a simple graph. Prove that $\Gamma(G) = \Gamma(G^c)$ where $\Gamma(G)$ is the automorphism group of G.

3 Prove that a tree with at least two vertices contains at least two pendent vertices.

4 Define Hamiltonian graphs. If G is Hamiltonian and S is a non-empty proper subset of V(G) then prove that $w(G-S) \leq |S|$.

5 Prove that every connected graph contains a spanning tree.

6 If G is a plane graph and f is a face of G then prove that there exists a plane embedding of G in which f is the exterior face.

7 Let $A = \{a, b\}$ and $L = \{a(ab)^n : n \geq 0\}$. Find a grammar that generates L.

8 Define dfa and illustrate it with an example. Find a dfa for $L = \{a^n b : n \geq 0\}$.

9 Find a nfa with four states for $L = \{a^n : n \geq 0\} \cup \{b^n a : n \geq 1\}$.

Turn over

10. Let X a set and $\leq$ a binary relation on X which is reflexive and transitive. Define a binary relation R on X by $xRy \Leftrightarrow x \leq y$ and $y \leq x$. Is R an equivalence relation on X ? Justify your claim.

11. Let $(X, +, \cdot, ')$ be a Boolean Algebra. Prove that $x + x \cdot y = x$ and $x \cdot (x + y) = x$ for all $x, y \in X$.

12. Write the conjunctive normal form of $x_1 x_2' (x_1 + x_2' + x_1 x_2)$.

Part B

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

II A (a) Prove that a graph is bipartite if and only if it contains no odd cycles.

(b) Show that $\delta \geq \frac{n-2}{2}$ need not imply that G is connected.

Or

B (a) Prove that a connected graph with at least two vertices contains at least two vertices that are not cut vertices.

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

III A (a) Prove that $K_{3,3}$ is non-planar.

(b) State and prove the Eulers formula for a simple connected graph.

(c) Prove that a simple graph G is Eulerian if and only if G is the edge-disjoint union of cycles.

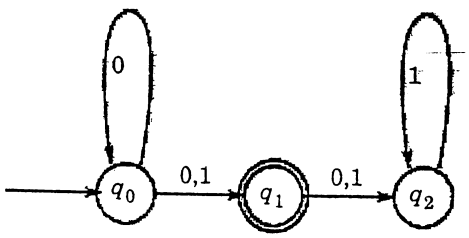
Or

B (a) Prove that K_5 is non-planar.

(b) Prove that a simple graph G is Eulerian if and only if the degree of each vertex of G is a positive even integer.

IV A (a) Define equivalent finite accepters. Illustrate it with an example.

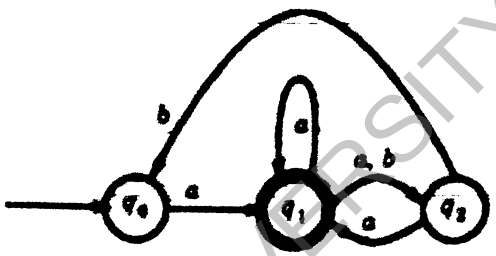
(b) Convert the *nfa* in the following transition graph into an equivalent deterministic machine.



Or

B (a) Show that the language $L = \{ww^R : w, w \in \{a, b\}^*, |w| = 2\}$ is regular.

(b) Convert the *n/fa* in the following transition graph into an equivalent *d/fa*.



V A (a) Let $(X, *, ')$ be a Boolean Algebra. If $x, y \in X$, define $x \leq y$ if $x * y' = 0$. Prove that $(X, \leq)$ is a lattice. Find the minimum and maximum elements of this lattice.

(b) Prove that every finite Boolean Algebra is isomorphic to a power set Boolean Algebra.

Or

B (a) Assuming n mutually independent Boolean variables, prove that there are 2^{2^n} Boolean functions on these n variables. Also prove that these 2^{2^n} Boolean functions form a Boolean Algebra.

(b) Write the disjunctive normal form of $x_1 x_2' (x_1' + x_2 + x_1 x_2)$.

C 33197 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 03—LINEAR ALGEBRA

(2008 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1. Prove that any proper subspace of $\mathbb{R}^2$ consists of all scalar multiples of some fixed vector in $\mathbb{R}^2$. Interpret it geometrically.

2. Is the set of vectors containing the zero vector linearly dependent. Justify your claim.

3. Define $T:\mathbb{R}^2 \to \mathbb{R}^2$ by $T(x, y) = (\sin x, y)$. Explain in detail whether T is a linear transformation.

4. Let V be the vector space of all complex valued functions on the real line. Let f_i be defined by $f_1(x) = 1, f_2(x) = e^{ix}, f_3(x) = e^{-ix}$. Prove that $\{f_1, f_2, f_3\}$ is linearly independent.

5. Let V and W be vector spaces over F and $T: V \to W$ be a linear transformation. If S is a subspace of V, prove that f (S) is a subspace of W.

6. Define rank of a linear transformation. Give an example of a linear transformation and find its rank.

7. Let $T:\mathbb{R}^3 \to \mathbb{R}^3$ be defined by $T(x_1, x_2, x_3) = (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3)$. Is T invertible ? Justify your answer.

8. Let $T: V \to W$ be a linear transformation. Prove that rank T^t = rank T.

9. Prove that similar matrices have the same characteristic polynomial.

Turn over

10. Find the characteristic polynomial of the identity matrix of order three.

11. Find the minimal polynomial for T, the linear operator on $\mathbb{R}^2$ which is represented by the matrix $\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$.

12. Find a 3×3 matrix for which the minimal polynomial is x^3.

$(12 \times 4 = 48$ marks)

Part B

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

II. A. (a) Prove that a non-empty subset W of V is a subspace of V if and only if for each pair of vectors $\alpha, \beta \in W$ and each scalar $c \in F$, the vector $c\alpha + \beta \in W$.

(b) Let V be the vector space of all polynomial functions from $\mathbb{R}$ into $\mathbb{R}$ of degree 2 or less. Let t be a fixed real number. Define $g_1(x) = 1, g_2(x) = x + t, g_3(x) = (x + t)^2$. Prove that $\mathcal{B} = \{g_1, g_2, g_3\}$ is a basis for V. If $f(x) = c_0 + c_1 x + c_2 x^2$, write f as a linear combination of elements of $\mathcal{B}$.

B. (a) Prove that two finite dimensional vector spaces over the same field are isomorphic if and only if they are of the same dimension.

(b) If W_1 and W_2 are finite dimensional subspaces of vector space V then prove that $W_1 + W_2$ is finite dimensional and $\dim W_1 + \dim W_2 = \dim (W_1 + W_2) + \dim (W_1 \cap W_2)$.

III. A. (a) Let W_1 and W_2 be subspaces of a finite dimensional vector space V. Prove that $(W_1 + W_2)^\circ = W_1^\circ \cap W_2^\circ$ and $(W_1 \cap W_2)^\circ = W_1^\circ + W_2^\circ$.

(b) Give an example of a linear functional on $F^{n \times n}$.

B. (a) Let T be the 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 $\mathbb{R}^3$.

(b) Let $\mathcal{B} = \{\alpha_1, \alpha_2, \alpha_3\}$ be the basis of $\mathbb{C}^3$ where $\alpha_1 = (1, 0, -1), \alpha_2 = (1, 1, 1)$ and $\alpha_3 = (2, 2, 0)$. Find the dual basis of $\mathcal{B}$.

IV. A. (a) Let $a, b, c \in \mathbb{R}$ and $A = \begin{bmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}$. Find the characteristic polynomial for A and show that it is the minimal polynomial for A.

(b) Let V be a finite dimensional vector space over F and T be a linear operator on V. Prove that T is triangulable if and only if the minimal polynomial for T is a product of linear polynomials over F.

B. (a) Prove that the matrix of a linear transformation is similar to a diagonal matrix if and only if there is a basis $\mathcal{B} = \{v_1, v_2, ..., v_n\}$ of V made up of the eigen vectors of T.

(b) Find all invariant subspaces of the real linear operator whose matrix in the standard ordered basis is $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

V. A. (a) Let E be a projection of R along N. Then prove that I–E is a projection of N along R.

(b) Let T be a linear operator on a finite dimensional vector space V. If T is diagonalizable and if $c_1, c_2, ..., c_k$ are the distinct eigen values of T then prove that there exist linear operators $E_1, E_2, ..., E_k$ on V such that :

(i) $T = c_1 E_1 + c_2 E_2 + ... + c_k E_k$.

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

(iii) Range of E_i is the characteristic space for T associated with c_i

B. State and prove the primary decomposition theorem.

(4 × 8 = 32 marks)

19/02/18

C 33196 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 02—REAL ANALYSIS—I

(2008 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

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

2 For $x, y \in \mathbb{R}^1$, let :

$$d(x,y) = \begin{cases} 1 \text{ if } x \neq y \\ 0 \text{ if } x = y \end{cases}.$$

Prove that d is a metric on $\mathbb{R}^1$. Which subsets of the resulting metric space are open ?

3 Let X be a metric space and let $E \subset X$. Prove that E is closed in X if and only if $\overline{E} = E$.

4 Is there a non-empty perfect set in $\mathbb{R}^1$ which contains no rational number ? Justify.

5 Define uniform continuity and give an example of it. Let $f : [0,1] \to \mathbb{R}^1$ be a function defined by $f(x) = \frac{x^2}{x+1}$. Is f uniformly continuous ? Justify your answer.

6 Define discontinuities of first and second kind. What type of discontinuities does the following function have ?

$$f(x) = \begin{cases} x & \text{if } -4 \leq x < -1 \\ 2+x & \text{if } -1 \leq x < 0 \\ x & \text{if } 0 \leq x \leq 1 \end{cases}.$$

7 Let f be a differentiable function in (a, b) and let $f'(x) \leq 0$ for all $x \in (a, b)$. Prove that f is monotonic decreasing on (a, b).

8 Let $f : \mathbb{R}^1 \to \mathbb{R}^1$ be a function defined by $f(x) = |x|^3$. Prove that $f^{(3)}(0)$ does not exist.

Turn over

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

10 For $1 < s < \infty$, let :

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s}.$$

Prove that

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

where $[x]$ denotes the largest integer less than or equal to x.

11 Is the sum of a convergent series of continuous functions continuous? Justify your answer.

12 Prove that the series :

$$\sum_{n=1}^{\infty} (-1)^n \frac{x^2 + n}{n^2}$$

converges uniformly in every bounded interval.

(12 × 4 = 48 marks)

Part B

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

II. A (a) Prove that a finite set has no limit points.

(b) Prove that arbitrary union of open sets is open. Is arbitrary intersection of open sets open ? Justify your answer.

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

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

III. A (a) Prove that a mapping of a metric space X into a metric space Y is continuous on X if and only if $f^{-1}(V)$ is open in X for every open set V in Y.

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

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

(b) If f is differentiable on $[a,b]$, then prove that f' cannot have any simple discontinuities on $[a,b]$.

A (a) Let f be a bounded real function on $[a, b]$ and α be monotonically increasing on $[a, b]$. If f is continuous, then prove that f Riemann-Stieltjes integrable with respect to α on $[a, b]$ $\left(f \in \mathrm{R}(\alpha) \text{ on } [a, b]\right)$.

(b) State and prove fundamental theorem of integral calculus.

B (a) Let f be Riemann integrable on $[a, b]$ and for $a \le x \le b$, let :

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

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

(b) Let γ be a curve on $[a, b]$. If γ' is continuous on $[a, b]$, then prove that γ is rectifiable and

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

A (a) Let X be a metric space and let C (X) be the set of all complex valued, continuous, bounded functions on X. Prove that C (X) is a complete metric space with respect to the metric :

$$d(f, g) = \|f - g\|,$$

where $f, g \in \mathrm{C}(\mathrm{X})$ and $\|f\| = \sup\{|f(x)| : x \in \mathrm{X}\}$.

(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 × 8 = 32 marks)

16/102/Kg

C 33195 (Pages : 2) Name.....

Reg. No.....

FIRST SEMESTER P.G. DEGREE EXAMINATION, DECEMBER 2017

(CCSS)

Mathematics

MAT 1C 01—ALGEBRA–I

(2008 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

I. 1. Find the order of the element (2, 5) in the group $\mathbb{Z}_4 \times \mathbb{Z}_{20}$.

2. Let G be a group and H be a subgroup of G.Suppose that $(aH)\ (bH) = abH$ gives a well defined binary operation on the set K (G) of all left cosets of H in G. Show that H is a normal subgroup of G.

3. Give a composition series of the group $\mathbb{Z}_{24}$.

4. Let X be a G - set. Show that for each $g \in G$, $\sigma_g : X \to X$ defined by $x \mapsto gx$ is a permutation of X.

5. Let $G = \mathbb{Z}_4$ and $X = \{1, 2, 3, 4\}$. Give an action of G on X so that X becomes a G – set with two orbits.

6. Let $G = \mathbb{Z} \times \mathbb{Z}_2$ and $H = \{0\} \times \mathbb{Z}_2$. Show that G/H is isomorphic to $\mathbb{Z}$.

7. Give two subgroups of order 3 in $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

8. Find all Sylow 5 – subgroups of $\mathbb{Z}_{10} \times \mathbb{Z}_{20}$.

9. Let D denote the integral domain $\mathbb{Z}_5$. Show that the field of quotients of D is isomorphic to the field $\mathbb{Z}_5$.

10. Show that $x^2 = 3$ has no solutions in the field of rationals.

11. Verify whether $x^5 + 4x^4 + 6x^2 + 2$ is irreducible in $\mathbb{Q}[x]$.

12. Let R be a ring with unity and N be an ideal containing a unit. Show that N = R.

(12 × 4 = 48 marks)

Turn over

Part B

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

II. A (a) Prove that if M is a maximal normal subgroup of a group G then G/M is a simple group.

(b) Give a maximal normal subgroup of S_3.

B (b) Define the commutator subgroup C of a group G.

Prove that

(i) C is normal in G.

(ii) G/C is abelian.

III. A (a) Let X be a G – set and for $x \in X$, let $G_x = \{g \in G : gx = x\}$. Show that G_x is a subgroup of G.

(b) Let G_x denote the orbit of x. Show that $|G_x| = (G : G_x)$.

B Let N be a normal subgroup of a group G and H be a subgroup of G. Show that

(i) HN/N is isomorphic to H/ (H ∩ N).

(ii) If H is also normal in G then HN is a normal subgroup of G.

IV. A (a) Define Sylow p – subgroup of a group G.

(b) Prove that the number of Sylow p – subgroups of G is congruent to 1 mod p.

B Describe the elements of the field of quotients of an integral domain. Define addition and multiplication in it. Prove that these are well defined.

V. A (a) Let F be a field. Show that an element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.

(b) Show that a non-zero polynomial $f(x) \in F[x]$ can have atmost n zeros in F.

B (a) Define prime ideal of a ring. Sow that every maximal ideal in a commutative ring with unity is a prime ideal.

(b) Let F be a field of characteristic p. Show that F contains a subfield isomorphic to the field $\mathbb{Z}_p$.

(4 × 8 = 32 marks)