141980

D 12294 (Pages : 3) Name.......................................

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 05—NUMBER THEORY

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

1. Prove that the Dirichlet multiplication is associative.
2. Evaluate the Legendre's symbol (73 | 383).
3. If $F(x) = \sum_{n \le x} f(n)$, then prove that $\sum_{n \le x} \sum_{d \mid n} f(d) = \sum_{n \le x} F\left(\frac{x}{n}\right)$.
4. Define the Chebyshev's functions $\psi(x)$ and $\mathcal{J}(x)$.
5. What is meant by a Cryptosystem ?
6. Describe a method to send a signature in RSA cryptosystem.

(6 × 2 = 12 marks)

Part B

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

7. If $n \ge 1$, prove that $\sum_{d \mid n} \phi(d) = n$.
8. For the Euler totient function, prove that $\phi^{-1}(n) = \pi_{p \mid n} (1 - p)$.
9. Prove that the Legendre symbol $(n \mid p)$ is a completely multiplicative function of n.
10. For $x \ge 1$, prove that :

$$\sum_{n > x} \frac{1}{n^s} = O\left(x^{1-s}\right) \text{ if } s > 1.$$

Turn over

141980

11. If $a > 0$ and $b > 0$, then prove that $\pi(ax)/\pi(bx) \sim a/b$ as $x \to \infty$.

12. For $n \geq 1$, prove that the n^{th} prime p_n satisfies the inequality :

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

13. The ciphertext " OF JDFOHFXOL" was intercepted. The ciphertext was enciphered using an affine transformation of single-letter plaintext units in the 27 letter alphabet (with blank = 26). It is known that the first word is "I". ("I" followed by blank). Determine the enciphering key and read the message.

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

(5 × 4 = 20 marks)

Part C

Answer **either** A **or** B *of each question.*
Each question carries 16 *marks.*

15. A (a) If f and g are multiplicative, prove that their Dirichlet product $f * g$ is also multiplicative.

(b) State and prove the Selberg identity.

B (a) Let p be an odd prime. Prove that $(n \mid p) \equiv n^{(p-1)/2} \pmod{p}$ for all integers n.

(b) 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.

16. A (a) Using Euler's summation formula, prove that, for $x \geq 2$,

$$\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2} \log^2 x + \text{A} + \text{O}\left(\frac{\log x}{x}\right),$$ where A is a constant.

(b) For $x \geq 2$, prove that :

$$\sum_{p \leq x} \left[\frac{x}{p}\right] \log p = x \log x + \text{O}(x),$$

where the sum is extended overall primes $\leq x$.

B (a) Prove that the following relations are logically equivalent :

(i) $\lim_{x \to \infty} \frac{\pi(x)\log x}{x} = 1.$

(ii) $\lim_{x \to \infty} \frac{\mathscr{J}(x)}{x} = 1.$

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

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

17. A (a) Briefly describe about digraph transformation.

(b) The ciphertext message "PWULPZTQAWHF" was intercepted. The message was encrypted using an affine map on digraphs in the 26-letter alphabet where a digraph whose two letters have numerical equivalents x and y corresponds to the integer $26x + y$. An extensive statistical analysis of earlier ciphertexts which had been coded by the same enciphering map shows that the most frequently occurring digraphs in all of that ciphertext are "I X" and " T Q", in that order. It is known that the most common digraphs in the English language are "TH" and "HE" in that order. Find the deciphering key, and read the message.

B (a) The message "ZRIXXYVBMNPO" which was resulted from a linear enciphering transformation of digraph-vectors in a 27-letter alphabet,in which A-Z have numerical equivalents 0 – 25, and blank = 26 was intercepted. It was found that the most frequently occurring ciphertext digraphs are "PK" and "RZ", and they correspond to the most frequently occurring plaintext digraphs in the 27-letter alphabet namely "E" (E followed by blank) and "S". Find the deciphering matrix and read the message.

(b) Briefly describe about RSA cryptosystem.

(3 × 16 = 48 marks)

D 12292 **(Pages : 4)** **Name.......................................**

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 03—REAL ANALYSIS – I

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

1. Prove that every neighborhood is an open set.
2. Let E be a non-empty set of real numbers which is bounded above. If $y = \sup \mathrm{E}$, then prove that $y \in \bar{\mathrm{E}}$.
3. Identify the discontinuities of the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = [x]$, where $[x]$ denote the largest integer less than or equal to x.
4. Give an example of a continuous real function defined on [–4, 5] which is not differentiable at –1.
5. Let f be a bounded real function and α be a monotonic increasing real function on $[a, b]$. If f is Riemann-Stieltjes integrable with respect to α on $[a, b]$, then prove that $|f|$ is Riemann-Stieltjes integrable with respect to α on $[a, b]$.
6. Let γ be a curve in the complex plane, defined on $[0, 2\pi]$ by $\gamma(t) = e^{2it}$. Prove that γ is rectifiable.
7. Prove that every uniformly convergent sequence of bounded functions is uniformly bounded.
8. Prove that every member of an equicontinuous family is uniformly continuous.

(8 × 2 = 16 marks)

Part B

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

9. Is arbitrary intersection of open sets in a metric space open ? Justify your answer.
10. Prove that closed subsets of a compact set are compact.

Turn over

11. Let f be a continuous mapping of a compact metric space X into $\mathbb{R}^k$. Prove that $f(X)$ is closed and bounded.

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

13. Let f be a bounded function and α be a monotonic increasing function on $[a, b]$. If f is Riemann-Stieltjes integrable with respect to α on $[a, b]$ and if $a < c < b$, then prove that f is Riemann-Stieltjes integrable with respect to α on $[a, c]$ and on $[c, b]$ and

$$\int_a^c f\,d\alpha + \int_c^b f\,d\alpha = \int_a^b f\,d\alpha.$$

14. For n = 1, 2, 3, ... and x real, let

$$f_n(x) = \frac{x}{1+nx^2}.$$

Show that $\{f_n\}$ converges uniformly.

(4 × 4 = 16 marks)

Part C

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

Unit I

15. A (a) Prove that a subset E of a metric space X is open if and only if its complement E^c is closed.

(b) Let E be a subset of $\mathbb{R}^k$. Prove that the following are equivalent :

(i) E is closed and bounded.

(ii) E is compact.

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

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

(b) Prove that a subset E of the real line $\mathbb{R}^1$ is connected if and only if E is an interval.

Unit II

16. A (a) Prove that a mapping f of a metric space X into a metric space Y is continuous 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 function on E which is not bounded.

B (a) Let f be continuous on $[a, b]$ and $f'(x)$ exists at some point $x \in (a,b)$. If g is defined on an interval I which contains the range of f and g is differentiable at the point $f(x)$, then prove that the function h defined on $[a, b]$ by :

$h(t) = g(f(t))$ is differentiable at x and $h'(x) = g'(f(x))f'(x)$.

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

Unit III

17. A (a) Let f be a bounded function and α be a monotonic increasing function on $[a, b]$. If P_1 is a refinement of P, then prove that :

$U(P_1, f, \alpha) \leq U(P, f, \alpha)$.

(b) Let f be a bounded real function and α be a monotonic increasing real function on $[a, b]$. If f is continuous on $[a, b]$, then prove that f is Riemann-Stieltjes integrable with respect to α on $[a, b]$.

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

(b) If f is Riemann integrable on $[a, b]$ and if there is a differentiable function F on $[a, b]$ such that $F' = f$, then prove that :

$$\int_a^b f\, dx = F(b) - F(a).$$

Turn over

Unit IV

18. A (a) If $\{ f_n \}$ is a sequence of continuous functions on E and if $f_n \to f$ uniformly on E, then prove that f is continuous on E.

(b) Let $\mathscr{C}(X)$ denote the set of all complex valued, continuous, bounded functions defined on a metric space X. Prove that $\mathscr{C}(X)$ is a complete metric space under the metric $d(f,g) = \sup_{x \in X} | f(x) - g(x) |$, where $f, g \in \mathscr{C}(X)$.

B If f is a continuous complex function on $[a, b]$, then prove that there exists a sequence of polynomials P_n such that lim $\lim_{n \to \infty} P_n(x) = f(x)$ uniformly on $[a, b]$.

(4 × 12 = 48 marks)

D 12290 **(Pages : 3)** **Name..**

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 01—ALGEBRA – I

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

1. Verify whether (1,2) is a generator of the cyclic group $\mathbb{Z}_3 \times \mathbb{Z}_4$.
2. Describe an isometry of the plane that fixes the Y-axis.
3. Let G = S_3 and H be the subgroup generated by (1 2). Define an action of G on G/H and find the isotropy group G_x for x = H.
4. Let $F = \mathbb{Z} \times \mathbb{Z} / \sim$ be the field of quotients of $\mathbb{Z}$ where the notations are the usual ones. Find all elements in $\mathbb{Z} \times \mathbb{Z}$ which are $\sim$ – related to (1,1).
5. Verify whether $x^4 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$.
6. Verify whether the ideal generated by 10 is a maximal ideal in $\mathbb{Z}_{12}$.
7. Verify whether $\frac{\sqrt{3}}{\sqrt{2}}$ is algebraic over $\mathbb{Q}$.
8. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(8 × 2 = 16 marks)

Part B

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

9. Find the order of (1, 2, 3) in $\mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_6$.
10. Let G = H × K. Show that G has a normal subgroup isomorphic to H.

Turn over

11. Let X be a G-set and $g \in G$. Let $\sigma_g : X \to X$ be defined by $x \mapsto gx$. Show that σ_g is onto.

12. Describe the field of quotients of the integral domain $\mathbb{Z}_5$.

13. Prove that $x^5 + 15x^2 + 9x + 3$ is irreducible in $\mathbb{Q}[x]$.

14. Show that if α and β are constructible by straight edge and compass then so is αβ.

(4 × 4 = 16 marks)

Part C

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

15. A (a) Let G be a group and H be a subgroup of G. Show that coset multiplication given by $(aH)(bH) = (ab)H$ is well defined if and only if H is a normal subgroup of G.

(b) Show that if H is a normal subgroup of G then G / H is a group.

B Let $\phi : G \to G'$ be an onto homomorphism of groups. Show that :

(i) if N is a normal subgroup of G then $\phi(N)$ is a normal subgroup of G'.

(ii) if H is a normalsubgroup of G' then $\phi^{-1}(H)$ is a normal subgroup of G.

(iii) if Ker 0 is a maximal normal subgroup of G then G' is simple.

16. A (a) Let G be a finite group and X be a G-set. Let G_x be the isotropy group at x and G_x be the orbit of x for $x \in X$. Show that :

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

(ii) $|Gx|$ is a divisor of $|G|$.

(b) Describe an action of S_3 on the set {1, 2, 3} and find all orbits in this action.

B (a) Let D be an integral domain. For $(a,b),(c,d) \in D \times D$ define $(a,b) \sim (c,d)$ if $ad = bc$. Show that ~ is an equivalence relation on D × D.

(b) Let $[a, b]$ denote the ~- class containing (a, b). Show that $[a,b] + [c,d] = [ad + bc, bd]$ is a well defined addition in D × D/ ~ .

17. A (a) Let F be a field and $f(x) \in F[x]$ be of degree 2 or 3. Show that $f(x)$ is irreducible if and only if $f(x)$ has no zero in F.

(b) Let $f(x) \in \mathbb{Z}[x]$. Show that $f(x)$ factors into a product of two polynomials of degree r and s in $\mathbb{Q}[x]$ if and only if it has a factorization with polynomials of degree r and s in $\mathbb{Z}[x]$.

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

(b) Let R be a commutative ring and N be a prime ideal of R. Show that R / N is an integral domain.

(c) Find all prime ideals of the ring $\mathbb{Z}$ of integers.

18. A (a) Let E be a finite extension of a field F and K be a finite extension of E. Show that $[K:F] = [K:E][E:F]$.

(b) Let α be algebraic over F and let $\beta \in F(\alpha)$. Show that $\deg(\beta\,;F)$ divides deg $(\alpha : F)$.

B (a) Show that for every prime p and every natural number n, there is a field of p^n elements.

(b) Let E and F be finite fields of order p^n. Prove that E is isomorphic to F.

(4 × 12 = 48 marks)

D 12291 **(Pages : 4)** **Name.......................................**

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

FIRST SEMESTER P.G. DEGREE EXAMINATION, NOVEMBER 2021

(CCSS)

Mathematics

MAT 1C 02—LINEAR ALGEBRA

(2019 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

1. Let $S = \{(a_1, a_2, a_3) \varepsilon R^3 : a_1 + 3a_2 = a_3\}$ be the subset of the vector space R^3. Verify whether S is a subspace of R^3.
2. Is there a linear transformation T from R^3 into R^2 such that T (1,–1, 1) = (1, 0) and T (1, 1, 1) = (0, 1) ? Justify your answer.
3. 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 ordered basis $B = \{\alpha_1, \alpha_2\}$, where $\alpha_1 = (1,2)$ and $\alpha_2 = (1,-1)$.
4. If w_1 and w_2 are subspaces of a finite-dimensional vector space, then $w_1 = w_2$ iff $w_1^0 = w_2^0$.
5. Define minimal polynomial for an $n \times n$ matrix over R. Find a 3×3 matrix over R for which the minimal polynomial is x^2.
6. Let T be the linear operator on R^2, the matrix of which in the standard ordered basis is $A = \begin{bmatrix} 1 & -1 \\ 2 & 2 \end{bmatrix}$.

   Determine the subspaces of R^2 invariant under T.
7. Find a projection E which projects R^2 onto the subspace spanned by (1, –1) along the subspace spanned by (1, 2).
8. Describe explicitly all inner products on R.

(8 × 2 = 16 marks)

Turn over

Part B

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

9. Show that a non-empty subset W of a vector space V is a subspace of V iff for each pair of vectors α, β in W and each scalar in c in F the vector $c\,\alpha + \beta$ is in W.

10. Let T be the linear operator on 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? If so, find a rule for T^{-1}.

11. Let V be a finite-dimensional vector space over the field F, and let $B = \{\alpha_1, \ldots, \alpha_n\}$ be a basis for V. Show that there is a unique dual basis $B^* = \{f_1, \ldots, f_n\}$ for V* such that $f_i(\alpha_j) = \delta_{ij}$, where $\delta_{ij} = \begin{Bmatrix} 1 \ \ if\ i = j \\ 0\ if\ i \neq j \end{Bmatrix}$.

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

13. Let $w_1, w_2, \ldots, w_k$ be subspaces of a vector space V such that $V = w_1 \oplus \ldots \oplus w_k$. Show that there exists k linear operators $E_1, E_2, \ldots, E_k$ on V such that :

    (i) $E_i E_j = \begin{cases} E_i & \text{if } \hat{j} = i \\ 0 & \text{if } j \neq i \end{cases}$.

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

    (iii) the range of E_i is W_i.

14. Apply the Gram–Schmidt process to obtain an orthonormal basis for the subspace spanned by the vectors $\beta_1 = (1, 0, i)$ and $\beta_2 = (2, 1, 1 + i)$ in the inner product space C^3, with the standard inner product.

(4 × 4 = 16 marks)

Part C

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

15. A (a) Is the vector $(3,-1,0,-1)$ in the subspace of R^4 spanned by the vectors $(2,-1,3,2)$, $(-1,1,1,-3)$ and $(1,1,9,-5)$? Justify your answer.

(b) Let V be a vector space which is spanned by a finite set of vectors $\beta_1, \beta_2, \ldots, \beta_m$. Show that any independent set of vectors in V is finite and contains no more than m elements.

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

16. A Let V be an n-dimensional vector space over the field F and let W be an m-dimensional vector space over F. Show that the vector space L (V, W) is infinite dimensional and has dimension mn.

B (a) Let $g, f_1, \ldots, f_r$ be linear functionals on a vector space V with respective null spaces $N, N_1, \ldots, N_r$. Show that g is a linear combination of $f_1, \ldots, f_r$ iff N contains the intersection $N_1 \cap \ldots \cap N_r$.

(b) If W is a subspace of a finite dimensional vector space V and if $\{g_1, \ldots, g_r\}$ is any basis for w^0, then $W = \bigcap_{i=1}^{r} N_{g_i}$, where N_{g_i} is the null space of g_i.

17. A Let T be a linear operator on a finite-dimensional vector space V. Let $c_1, \ldots, c_k$ be the distinct characteristic values of T and let w_i be the null space of $(T - c_i I)$. Show that T is diagonalizable iff $\dim w_1 + \ldots + \dim w_k = \dim V$.

B (a) 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 triangulable iff the minimal polynomial for T is a product of linear polynomials over F.

(b) Show that every matrix A such that $A^2 = A$ is similar to a diagonal matrix.

Turn over

18. A Let T be a linear operator on a finite-dimensional vector space V. Suppose that there exist k distinct scalars $c_1 c_2, \ldots, c_k$ an k non-zero linear operators $E_1, \ldots, E_k$. such that :

(i) $T = c_1 E_1 + \ldots, c_k E_k$.

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

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

Show that T is diagonalizable and $c_1, \ldots, c_k$ are the distinct characteristic values of T with the characteristic space for T associated with c_i is the range of E_i.

B (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) Let S be a subset of a finite-dimensional inner product space V. Show that $\left(S^{\perp}\right)^{\perp}$ is the subspace spanned by S.

(4 × 12 = 48 marks)