Department of Mathematics, University of Delhi
M.A./M.Sc. Mathematics Final Examinations, 2021, Part II Semester IV
MMATH18 401(i): ADVANCED GROUP THEORY
Unique Papercode: 223502401

Time: 3 hours Maximum Marks: 70

Instructions: • Attempt any five questions in all. • Question 1 is compulsory and answer any four questions from Q.2 to Q.7. • All questions carry equal marks.• All symbols have usual meaning.

(1) (a) Let G be a p-group, then G is an elementary Abelian if and only if $\phi(G) = 1$. (5)
(b) A finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups. (5)
(c) Does the additive group of rationals Q have ACC or DCC or both. If yes, then give a proof. If no, then provide a counterexample. (4)

(2) (a) Let H, K and L be three subgroups of G where $H \leq L$. Then prove that $HK \cap L = H(K \cap L)$. (6)
(b) Recall the map β defined for $r = 1$ case in Krull-Schmidt theorem. Prove that the map β is a normal endomorphism. (8)

(3) Let G be a nilpotent group of order $lcm(a, b)/gcd(a, b)$, where a,b are two postive integers. Does there exist a subgroup of G whose order divides b? If yes, then justify you answer and also find out the order of that subgroup. State all the theorems that you are using in this proof.

(4) (a) If G is a finite group, then G is nilpotent if and only if $G' \leq \phi(G)$. (7)
(b) Prove that if G has either chain condition then G is a direct product of a finite number of indecomposable groups. (7)

(5) (i) If a nilpotent group has an element of order p, then so does its centre. (7)
(ii) A nontrivial finitely generated group cannot equal to its Frattini subgroup. (7)

(6) Let G have both chain conditions. If $G \cong A \times B$ and $G \cong A \times C$, then $B \cong C$.

(7) (a) A finite p-group G is extra-special if $Z(G)$ is cyclic and $\phi(G) = Z(G) = G'$. Now, show that every non-abelian group G of order p^3 is extra special. What goes wrong when G is abelian? (9)
(b) If H be a normal subgroup of G and both H and G/H are nilpotent, then is G nilpotent. If yes, give a proof otherwise provide a counterexample. (5)

M.A./M.Sc. Mathematics, Part II, Semester IV
Examination (OBE) June 2021

Paper: MMATH18 - 401(ii) Algebraic Number Theory
Unique Paper Code: 223502402

Maximum Marks: 70 Time allowed: 3 Hours

• Attempt five questions in all • Question 1 is compulsory • All questions carry equal marks

1. (a) Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. Does $1, \theta, \ldots, \theta^{n-1}$ and $1, \alpha, \ldots, \alpha^{n-1}$ have the same discriminant, where $\alpha = m + \theta$ for some integer m? Justify. (3)

   (b) Find discriminant and integral basis of the number field $K = \mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive 5-th root of unity. (3)

   (c) Let $d \equiv 1 \pmod 4$ be a square-free integer different from 1. Show that $\mathbb{Z}[\sqrt{d}]$ is never a unique factorization domain. (3)

   (d) Let K be number field of degree n. For a prime number p, let $p\mathcal{O}_K$ factors into prime ideals of $\mathcal{O}_K$ as $\prod_{i=1}^{r} \mathcal{P}_i^{e_i}, e_i \geq 1$. Prove that $N_K(\mathcal{P}_i) = p^{f_i}$, for some integer $f_i \geq 1$ and $\sum_{i=1}^{r} e_i f_i = n$. (3)

   (e) Is the set $L = \{m + \pi n \mid n, m \in \mathbb{Z}\}$ a lattice in $\mathbb{R}$? Justify. (2)

2. (a) Let K be a number field of degree n. Prove that the ring of algebraic integers $\mathcal{O}_K$ is a free abelian group of rank n. (10)

   (b) Find norm and trace of $\sqrt{p}$ over $\mathbb{Q}$ for the number field $\mathbb{Q}\left(\sqrt[4]{p}\right)$, where p is a prime number.(4)

3. (a) Find the integral basis and discriminant of the number field $K = \mathbb{Q}(\theta)$, where $\theta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ and p is an odd prime number. (9)

   (b) Find integral basis and discriminant of the number field $K = \mathbb{Q}(\theta)$, where θ is a complex root of the polynomial $p(t) = t^3 - t^2 - t - 2$. (5)

4. (a) Is the ring of algebraic integers of the number field $\mathbb{Q}(\sqrt{-13})$ a Euclidean domain? Justify. (9)

   (b) Find all possible integer solutions of the equation $X^2 + 1 = 2Y^3$. (5)

5. (a) Prove that every non-zero prime ideal of the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$ is invertible for every square-free integer d. (10)

   (b) Let R be an integral domain with fraction field K such that every non-zero fractional ideal of R is invertible. Prove that R is Noetherian. (4)

6. (a) Let K be number field of degree $n = s + 2t$, where s is the number of real monomorphisms and $2t$ the number of complex monomorphisms of K into $\mathbb{C}$. Prove that there exists an embedding of K into the $\mathbb{R}$-vector space $\mathbb{R}^s \times \mathbb{C}^t$ and show that under this embedding the ideals of $\mathcal{O}_K$ are mapped to n-dimensional lattices in $\mathbb{R}^s \times \mathbb{C}^t$. (10)

   (b) Let L be an n-dimensional lattice in $\mathbb{R}^n$ with bases $\{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_n\}$. Prove that $\det(a_{ij}) = \pm\det(b_{ij})$, where $(a_{i1}, a_{i2}, \ldots, a_{in})$ and $(b_{i1}, b_{i2}, \ldots, b_{in})$ denote respectively the co-ordinates of the basis elements v_i, w_i $1 \leq i \leq n$. (4).

7. (a) State and prove Dedekind's Theorem. (10)

   (b) Prove that the class number of the number field $\mathbb{Q}(\sqrt{-10})$ cannot be 1. (4)

Your Roll Number: .....

Department of Mathematics, University of Delhi
M.A./M.Sc. Mathematics Examinations, June 2021
Part II Semester IV

MMATH18-401(iii): Simplicial Homology Theory
Unique Paper Code 223502403

Time: **4 hours** (This includes **one hour** time for downloading the paper, scanning your answer sheets and uploading back in the email for the final submission.)
Maximum Marks: **70**

Instructions: • All notations used are standard • **Question no.** 1 is **compulsory** • Attempt any **four** questions from the remaining six questions.

---

(1) Prove or disprove the following statements:
   (a) Every simplicial complex is locally path connected.
   (b) Number of faces of an n-simplex σ^n is $2^{2n+1} - 1$.
   (c) Let σ^n be an n-simplex, $n \geq 1$. Then $diam(\sigma^n) = \|v - w\|$, for some vertices v and w in σ.
   (d) Composite of simplicial approximations to continuous maps is a simplicial approximations to the composite of maps.
   (e) Let $K = Cl(\sigma^2)$, where $\sigma^2 = \langle (0,1), (-1,0), (1,0) \rangle$ with ordering on vertices $(0,1) < (-1,0) < (1,0)$. Then $[\sigma^2, \langle (0,1), (1,0) \rangle] = [\langle (0,1), (-1,0) \rangle, \langle (-1,0) \rangle]$.
   (f) Let K be a simplicial complex such that $|K|$ is homeomorphic to $\mathbb{S}^n$, where $n \in \mathbb{N}$. Then the Euler characteristic of K is 2 if n is an even natural number and 0, otherwise.
   (g) There exists a 2-pseudomanifold with exactly three vertices. (2×7)

(2) (a) For a given geometrically independent set $X = \{v_0, v_1, \cdots, v_k\}$ in $\mathbb{R}^n$, show that there is a unique k-dimensional hyperplane H^k which passes through all the points of X. Use this to define barycentric coordinates for any $h \in H^k$. Establish uniqueness of these barycentric coordinates. (6)
   (b) If $\sigma^k = \langle v_0, v_2, \cdots, v_k \rangle$ is a k-simplex in $\mathbb{R}^n$, $k \leq n$, then show that σ^k equals union of all the line segments joining v_0 to the points of the simplex generated by $\{v_1, v_2, \cdots, v_k\}$. Further, establish that any two such line segments will intersect only at the point v_0. (5)
   (c) Can a polyhedron have more than one triangulation? Justify your claim. (3)

(3) (a) Define mesh of a positive dimensional simplicial complex K and show that $\lim_{n \to \infty} mesh(K^{(n)}) = 0$. (5)
   (b) Carefully state simplicial approximation theorem explaining every term. (3)
   (c) For an oriented simplicial complex K, if σ^{p-2} is a $(p-2)$ face of a simplex σ^p of K, then show that $\sum [\sigma^p, \sigma^{p-1}][\sigma^{p-1}, \sigma^{p-2}] = 0$, where the summation is over all $(p-1)$ simplexes σ^{p-1} of K. (6)

(4) (a) Define chain complex $C_*(K)$ associated to an n-dimensional oriented simplicial complex K and write $C_*(K)$ for $K = Cl(\langle a_0, a_1, a_2 \rangle)$. Further, find boundary of 1-chain $1.\sigma^1$ and boundary of 2-chain $1.\sigma^2$.

(b) Compute $H_p(\mathbb{S}^2)$, for all $p \geq 0$ using 2-skeleton of $Cl(\sigma^3)$. $(5+9)$

(5) (a) Let $\Phi : K \to L$ be a simplicial map between two simplicial complexes K and L. Then carefully define homomorphisms $\Phi_p : C_p(K) \to C_p(L)$, $p \geq 0$ and show that for $p \geq 1$, $\partial \circ \Phi_p = \Phi_{p-1} \circ \partial$. Use this to define homomorphisms $\Phi_p^* : H_p(K) \to H_p(L)\ \forall\ p \geq 0$. (7)

(b) Use functorial properties to establish that if K and L are triangulations of a polyhedron X, then $H_p(K) \cong H_p(L)\ \forall p \geq 0$. (7)

(6) (a) Let $m, n \in \mathbb{N} \cup \{0\}$ be distinct. Then show that
(i) $\mathbb{S}^m$ is not homeomorphic to $\mathbb{S}^n$.
(ii) $\mathbb{R}^m$ is not homeomorphic to $\mathbb{R}^n$. $(4+3)$

(b) Define retract of a topological space. Show that
(i) $\mathbb{D}^n$ is retract of $\mathbb{R}^n$, $n \geq 1$.
(ii) $\mathbb{S}^{n-1}$ is not a retract of $\mathbb{D}^n$, $n \geq 1$. $(2+5)$

(7) (a) Carefully state Brouwer's fixed point theorem and prove it.

(b) If two continuous self-maps f and g over $\mathbb{S}^n$, $n \geq 1$ are homotopic, then show that $deg\ f = deg\ g$. Who proved this result? What you know about converse of this result. $(6+8)$

DEPARTMENT OF MATHEMATICS
M. A./M. SC. MATHEMATICS PART (II) -SEMESTER IV
FINAL EXAMINATION JUNE 2021
MMATH18- 402(I) ABSTRACT HARMONIC ANALYSIS, UPC: 223502405

Time: 3 HOURS Maximum Marks: 70

• Write your **Name, University Roll No., College and Course on the first page and your Roll No. on each subsequent answer sheet**. • Attempt **five** questions in all. • **Question No. 1 is compulsory**. Attempt any four from the remaining six questions. • All the questions carry equal marks. • All the symbols have their usual meanings.

(1) (a) For $f, g \in L^1(\mathbb{R})$, prove that $\widehat{f * g}(\chi) = \hat{f}(\chi)\hat{g}(\chi), \forall \chi \in \hat{\mathbb{R}}$. (3)

(b) Prove or disprove: Every bounded function is positive definite. (3)

(c) Prove of disprove: The space $C_0(X)$ is unital, X being a locally compact group. (3)

(d) For a finite group G, determine the number of its conjugacy classes in terms of the number of elements in its dual space. (3)

(e) Give example of a symmetric and a non-symmetric subset of $\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$. (2)

(2) (a) Prove that every one dimensional unitary representation is irreducible. Is every irreducible unitary representation one dimensional? Justify your answer. (7)

(b) Let G be a locally compact group and $M(G)$ be the Banach algebra of complex regular Borel measures on G. Prove that $M(G)$ is unital. Is $M(G)$ a commutative Banach algebra ? Justify your answer. (7)

(3) (a) Discuss an example of a function of positive type on the locally compact group $\mathbb{R}$ with justification. (7)

(b) Prove that $\mathbb{R}/\mathbb{Z}$ is a topological group and is locally compact. (7)

(4) (a) Let G be a compact group, π be a unitary representation of G and L be the span of the coordinate functions of π. Prove that L is a two sided ideal of $L^1(G)$ which is invariant under left and right translations. (7)

(b) Let G be a locally compact abelian group and $\mathcal{T}$ denote the collection of all continuous homomorphisms from G into $\mathbb{T}$. Prove that there is a one to one correspondence between $\mathbb{T}$ and the dual group of G. (7)

(5) (a) Let G be a locally compact group and $x \in G$. Prove that there exists a positive real number $\Delta(x)$ such that for every right Haar measure λ on G, $\lambda(E) = \Delta(x^{-1})\lambda(xE)$, E being a Borel set. (7)

(b) Prove that the algebra of continuous central functions on $SU(2)$ is isomorphic to $C([0, 2\pi])$ (7)

(6) (a) For $f \in C_c(G)$, prove that f is left uniformaly continuous. (7)

(b) Prove that the dual group of $\mathbb{Z}^n$ is isomorphic to $\mathbb{T}^n$. (7)

(7) (a) Consider the general linear group $GL_3(\mathbb{R})$ and let A be a 3×3 diagonal matrix with diagonal entries as $1, 2, -5$. Prove that there exists a unitary representation π of $GL_3(\mathbb{R})$ such that $\pi(A)$ is not the identity operator. (7)

(b) Prove that every unitary representation of a locally compact group is a direct sum of cyclic representations. (7)

No. of Printed Pages **2**

M.A./M.Sc. Mathematics Examinations (June 2021)
Part II Semester IV
MMATH18-402(ii): Frames and Wavelets
Unique Paper Code: 223502406

Time: 3 hr Maximum Marks: 70

Instructions: • Question No. 1 is **COMPULSORY** • Answer any **FOUR** questions from Question No. 2 to Question No. 7 • All questions carry equal marks • Symbols have their usual meaning.

Question No. 1 is **COMPULSORY**.

(1) (a) Find the optimal frame bounds of the Mercedes-Benz frame. [2 Marks]

(b) Give an example, with justification, of an exact frame of $\ell^2(\mathbb{N})$ which is not orthonormal. [3 Marks]

(c) Give an example, with justification, of a Riesz sequence in an infinite dimensional Hilbert space $\mathcal{H}$ which is not a frame for $\mathcal{H}$. [3 Marks]

(d) Show that if $\{f_k\}_{k=1}^{\infty}$ is a frame for an infinite dimensional Hilbert space $\mathcal{H}$ with frame operator S, then $\|S^{\frac{-1}{2}} f_k\|^2 \in [0,1]$ for every $k \in \mathbb{N}$. [3 Marks]

(e) Give an example, with justification, of two frames for an infinite dimensional Hilbert space $\mathcal{H}$ which are not dual frames. [3 Marks]

(Answer any **FOUR** questions from Question No. 2 to Question No. 7.)

(2) (a) Discuss the lower and upper frame conditions of $\{e_k + e_{k+1}\}_{k=1}^{\infty} \subset \ell^2(\mathbb{N})$, where $\{e_k\}_{k=1}^{\infty}$ is an orthonormal basis of $\ell(\mathbb{N})$. [4 Marks]

(b) Give an example, with justification, of an infinite collection of vectors $\mathbb{C}^2$ which constitutes a Parseval frame for $\mathbb{C}^2$. [4 Marks]

(c) Show that a finite collection of vectors $\{f_k\}_{k=1}^{m}$ in $\mathbb{C}^n$ is a frame for $\text{span}\{f_k\}_{k=1}^{m}$. [6 Marks]

(3) (a) How do you use the frame algorithm in approximation of signals? Explain. [4 Marks]

(b) Show that if T is the pre-frame operator of a frame sequence $\{f_k\}_{k=1}^{\infty}$ in an infinite dimensional Hilbert space $\mathcal{H}$, then $\{f_k\}_{k=1}^{\infty}$ is a frame for $\mathcal{H}$ if and only if T^* is injective. [4 Marks]

(c) Under what condition(s) a complete Bessel sequence $\{f_k\}_{k=1}^{\infty}$ in an infinite dimensional Hilbert space $\mathcal{H}$ constitutes a Riesz basis for $\mathcal{H}$? Explain. [6 Marks]

(4) (a) Give an example, with justification, of a Schauder basis for an infinite dimensional Hilbert space $\mathcal{H}$ which is not a frame for $\mathcal{H}$. [4 Marks]

(b) Show that if $\{f_k\}_{k=1}^{\infty}$ is a Schauder basis for the Banach space X with associated coefficient functionals $\{\varphi_k\}_{k=1}^{\infty}$, then $\{\varphi_k\}_{k=1}^{\infty}$ is a basis for its closed span in the dual space X^*. Also find its associated biorthogonal system. [7+3= 10 Marks]

(5) (a) Find scaling relations of the Haar multiresolution analysis. [4 Marks]

(b) Show that if ϕ is the Haar scaling function and for each $j \in \mathbb{Z}$, [5 Marks]

$$\mathcal{V}_j = \Big\{ f \in L^2(\mathbb{R}) : \text{f is constant on} \Big[\frac{n}{2^j}, \frac{(n+1)}{2^j}\Big), n \in \mathbb{Z} \Big\},$$

then $(\mathcal{V}_j, \phi)_{j\in\mathbb{Z}}$ is a multiresolution analysis.

(c) Show that if $\{f_k\}_{k=1}^{\infty} \subset \mathcal{H}$ and $\sum_{k=1}^{\infty} |\langle f, f_k\rangle|^2 < \infty$, then the pre-frame operator of $\{f_k\}_{k=1}^{\infty}$ is bounded. [5 Marks]

(6) (a) How do you express a frame for an infinite dimensional Hilbert space $\mathcal{H}$ in terms of orthonormal bases of $\mathcal{H}$? Explain. [7 Marks]

(b) Show that if $\{f_k\}_{k=1}^{\infty}$ is a frame for an infinite dimensional Hilbert space $\mathcal{H}$ with frame operator S and $\langle f_j, S^{-1} f_j\rangle \neq 1$ for some $j \in \mathbb{N}$, then $\{f_k\}_{\substack{k=1 \\ k\neq j}}^{\infty}$ is a frame for $\mathcal{H}$. [7 Marks]

(7) (a) Give an example, with justification, of a tight Gabor frame for $L^2(\mathbb{R})$ which is not exact. [4 Marks]

(b) Let ϕ be the Haar scaling function and for each non-negative integer j, let $\mathcal{V}_j$ be the space spanned by the set $\{\phi(2^j x - k) : k \in \mathbb{Z}\}$. How do you reconstruct a function $f \in V_j$ from the Haar reconstruction formula? Explain. [5 Marks]

(c) Under what condition(s) a pair of Bessel sequences in an infinite dimensional Hilbert space $\mathcal{H}$ constitute a dual frame pair? Justify your answer. [5 Marks]

✠

Your Roll Number: .....

Department of Mathematics, University of Delhi
M.A./M.Sc. Mathematics Examinations, June 2021
Part II Semester IV

MMATH18-402(iii): Operators on Hardy Hilbert Spaces
Unique Paper Code 223502407

Time: **4 hours** (This includes **one hour** time for downloading the paper, scanning your answer sheets and uploading back in the email for the final submission.)
Maximum Marks: **70**

Instructions: • All symbols carry their usual meaning. • **Question no.** 1 is **compulsory** • Attempt any **four** questions from the remaining six questions .

---

(1) Prove or disprove the following statements:
   (a) Let $\lambda \in \mathbb{C}$ be fixed and set $\phi(z) = \lambda z$. Then $\{1, \phi, \phi^2, \phi^3, \ldots\}$ is an orthonormal basis for $H^2(\mathbb{D})$.
   (b) Let $f(z) = z^2 + \frac{z}{2} - \frac{1}{2}, z \in \mathbb{D}$. Then f is an outer function.
   (c) Let p be given by $p(z) = a_0 + a_1 z + \ldots a_m z^m$ where m is fixed. Then T given by $(Tf)(z) = p(z)f(z)$ defines a bounded linear operator on $H^2(\mathbb{D})$.
   (d) The orthogonal projection P from $L^2(S^1)$ onto $\widetilde{H}^2(S^1)$ has a Toeplitz matrix wrt the standard basis on $L^2(S^1)$.
   (e) The operator PJP restricted to the space $\widetilde{H}^2(S^1)$ where J is the usual flip operator and P is the orthogonal projection from $L^2(S^1)$ onto $\widetilde{H}^2(S^1)$ is a Hankel operator.
   (f) Let $\phi_n(e^{i\theta}) = e^{in\theta}, e^{i\theta} \in \mathbb{T}, n \in \mathbb{N}$. Then T_{ϕ_n} is compact for each $n \in \mathbb{N}$.
   (g) If $\phi(e^{i\theta}) = 1 + e^{-i\theta}$ and $\psi(e^{i\theta}) = 2e^{-i\theta} + e^{-2i\theta}$, then the Hankel operators H_ϕ, H_ψ commute.

(2×7)

(2) (a) Show that the operator M_z on $H^2(\mathbb{D})$ given by $(M_z f)(z) = zf(z)$ is unitarily equivalent to the unilateral shift on l^2. Give an operator on $\widetilde{H}^2(S^1)$ to which M_z is also unitarily equivalent.
   (b) Find the adjoint M_z^* of the operator M_z given in (2a) above. Show further that k_w is an eigen vector for the operator M_z^* for each $w \in \mathbb{D}$, where $k_w(z) = \frac{1}{(1-\overline{w}z)}, z \in \mathbb{D}$.

(6+8)

(3) (a) Let $z_1, z_2, \ldots z_n \in \mathbb{D}$. Show that the function $\phi(z) = \Pi_{k=1}^n \frac{z_k - z}{(1-\overline{z_k}z)}$ is an inner function. Further, let

$$\mathcal{M} = \{f \in H^2(\mathbb{D}) : f(z_1) = f(z_2) = \ldots = f(z_n) = 0\}.$$

   Show that $\mathcal{M}$ is closed.
   (b) With $\mathcal{M}$ and ϕ as in (3a) above, show that $\mathcal{M} = \phi H^2(\mathbb{D})$.
   (c) Let $z_n = 1 + \frac{1}{n^2}, n \in \mathbb{N}$. Show that there exists an inner function f whose non-zero zeros are exactly the $\{z_n\}$ and which has a zero of multiplicity 2 at 0.

(4+6+4)

(4) (a) Show that the mapping $\phi \mapsto T_\phi$ is an injective, bounded, linear, adjoint preserving mapping from $L^\infty(S^1)$ into the algebra of bounded linear operators on $\widetilde{H}^2(S^1)$. Find its range space.
(b) Let $\phi, \psi \in L^\infty(S^1)$, and P be the orthogonal projection from $L^2(S^1)$ onto $\widetilde{H}^2(S^1)$. Show that if $P(e^{-i\theta}\psi) \otimes P(e^{-i\theta}\overline{\phi}) = 0$, then either T_ψ is co-analytic or T_ϕ is analytic.
(c) Compute $UU^* + e_n \otimes e_n$, for $n \in \mathbb{N} \cup \{0\}$, where U is the unilateral shift and $\{e_n\}_n$ is the standard orthonormal basis or $\widetilde{H}^2(S^1)$.
$(7 + 4 + 3)$

(5) (a) Find the commutant of the unilateral shift acting on $\widetilde{H}^2(S^1)$.
(b) Determine whether the operators T_ϕ and T_ψ acting on $\widetilde{H}^2(S^1)$ are (i) normal (ii) self adjoint, where $\phi(e^{i\theta}) = -2 + e^{i\theta} + e^{-i\theta}$ and $\psi(e^{i\theta}) = 2i(e^{i\theta} + e^{-i\theta}) + 1$. Do T_ϕ and T_ψ commute? Justify. (8+6)

(6) (a) For $\phi \in L^\infty(S^1)$, determine the adjoint of the Hankel operator H_ϕ. If $\phi(e^{i\theta}) = 1 + e^{i\theta} + e^{-i\theta}$ and $\psi(e^{i\theta}) = i + e^{i\theta} - e^{-i\theta}$ are the operators H_ϕ, H_ψ, self-adjoint? Further, does $H_\psi H_\phi$ define a Hankel operator? Justify your answers.
(b) Let $w_1, w_2 \in \mathbb{D}$ be fixed. Find the matrix of the operator $T = k_{\overline{w_1}} \otimes k_{w_1} + 2k_{\overline{w_2}} \otimes k_{w_2}$. Hence or otherwise show that T is a Hankel operator and find a $\phi \in L^\infty$ such that $T = H_\phi$. Here, for any $w \in \mathbb{D}, k_w(z) = \frac{1}{(1-\overline{w}z)}, z \in \mathbb{D}$.
$(8 + 6)$

(7) (a) Let $\phi, \psi \in L^\infty(S^1)$ and suppose $H_\psi \neq 0$ and $H_\phi H_\psi = H_\psi H_\phi$. Show that there exists a complex number c such that $H_\phi = cH_\psi$.
(b) Show that an operator A has a Hankel matrix with respect to the standard basis of $\widetilde{H}^2(S^1)$ if and only if it satisfies the equation $U^*A = AU$, where U is the unilateral shift. Hence or otherwise show that the kernel of every Hankel operator H is invariant under the unilateral shift.
(c) Show that $JPJ = M_{e^{i\theta}}(I - P)M_{e^{-i\theta}}$, where J is the flip operator, and P is the orthogonal projection from $L^2(S^1)$ onto $\widetilde{H}^2(S^1)$.
(5+6+3)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DELHI
M.A./M.Sc. Mathematics Examinations, June 2021
Part II, Semester IV
MMATH18-403(i): CALCULUS ON $\mathbb{R}^n$
(Unique Paper Code 223502409)

Time: 3 hours Maximum Marks: 70

Instructions: • Write your Name, University Roll No., College, Course and Title of the Paper with Unique Paper Code on the first page and your Roll No. and page No. on each subsequent answer sheet. •Attempt **five** questions in all. **Question 1 is compulsory**. All questions carry equal marks.• The symbols used have their usual meanings.

(1) (a) Let $f:\mathbb{R}^n \to \mathbb{R}$ be such that $|f(x)| \le \|x\|^2$, $\forall x \in \mathbb{R}^n$. What can you say about the differentiability of f at $\mathbf{0}$? Justify your answer. [2]

(b) If $W = \{(x,y) \in \mathbb{R}^2 : x \neq y\}$ and $f : W \to \mathbb{R}^3$ is of class C^1 such that $Df(x,y) = \mathbf{0}$, $\forall (x,y) \in W$, can you conclude that f is a constant? Justify your answer. [2]

(c) Show by successive integration that the 1-form

$$\omega = ydx + (x + z\cos(yz))dy + y\cos(yz)dz$$

in $\mathbb{R}^3$ is exact. [4]

(d) Give an example with justification of a 1-form in $\mathbb{R}^2$ which is of class C^1 but not of class C^2. [3]

(e) Let $T(r,\theta,\varphi) = (x,y,z)$, where $x = r\sin\theta\cos\varphi$, $y = r\sin\theta\sin\varphi$, $z = r\cos\theta$. If $\omega = dx \wedge dy \wedge dz$, compute the pull back ω_T. [3]

(2) (a) State and prove the implicit function theorem and illustrate the theorem with an example. [7]

(b) Suppose ω and λ are k- and m-forms $(k,m \ge 1)$, respectively, of class C^1 in the open set $E \in \mathbb{R}^n$. Show that $d(\omega \wedge \lambda) = d\omega \wedge \lambda + (-1)^k \omega \wedge d\lambda$. Verify this formula for the forms ω and λ in $\mathbb{R}^3$, where $\lambda = zdy + xdz$ and [7]
$\omega = 2xy^3z^4dx + (3x^2y^2z^4 - ze^y\sin(ze^y))dy + (4x^2y^3z^3 - e^y\sin(ze^y) + e^z)dz$.

(3) (a) Prove that for every k-chain Γ, $k \ge 2$, $\partial^2\Gamma = 0$. Verify explicitly that $\partial^2\sigma = 0$, where σ is the affine simplex $\sigma = [P_1, P_2, P_3, P_4.P_5]$. [7]

(b) Let H be the parallelogram in $\mathbb{R}^2$ with vertices $(2,2),(4,3),(5,6)$ and $(3,5)$. Find the affine map T which sends $(0,0)$ to $(2,2)$, $(1,0)$ to $(4,3)$ and $(0,1)$ to $(3,5)$. Use T to convert the integral $I = \int_H e^{2u+v}\,du\,dv$ to an integral over the unit square S, and thus compute it. Show also that T maps a convex set to a convex set, and hence conclude that $T(S) = H$. [7]

(4) (a) Suppose for $1 \le j \le n$, $g_j : \mathbb{R} \to \mathbb{R}$ are differentiable. Define $f:\mathbb{R}^n \to \mathbb{R}$ by $f(x_1, x_2, \cdots, x_n) = \sum_{j=1}^n g_j(x_j)$. Show that f is differentiable in $\mathbb{R}^n$ and find Df. [5]

(b) Let E be an open subset of $\mathbb{R}^k$ containing the standard simplex Q^k, $k > 1$ and $\sigma = [0, e_1, e_2, \cdots, e_k]$ be the oriented affine k-simplex in $\mathbb{R}^k$ with parameter domain Q^k. For any $(k-1)$-form λ of class C^1 in E, prove that $\int_\sigma d\lambda = \int_{\partial\sigma} \lambda$. [9]

(5) (a) Let $f : Q^k \to \mathbb{R}$ be continuous, where

$$Q^k = \{x = (x_1, x_2, \ldots, x_k) \in \mathbb{R}^k : x_i \geq 0, \forall\, 1 \leq i \leq k, \sum_{i=1}^{k} x_i \leq 1\}.$$

Define $\int_{Q^k} f$ and show the existence of the integral. Show also that the definition does not depend on the order in which the k single integrals are carried out. [8]

(b) Suppose $\sigma = [P_0, P_1, \cdots, P_k]$ is an oriented affine k-simplex ($k \geq 2$) in an open set $E \in \mathbb{R}^n$, $0 < i < j \leq k$ and $\tilde{\sigma}$ is the affine k-simplex obtained from σ by interchanging P_i and P_j. Show that for any k-form ω in E, $\int_{\tilde{\sigma}} \omega = -\int_{\sigma} \omega$. [6]

(6) (a) Suppose ω is a k-form in an open set $E \subset \mathbb{R}^n$, Φ is a k-surface in E with parameter domain $D \subset \mathbb{R}^k$ and Δ is the k-surface in $\mathbb{R}^k$ with parameter domain D, defined by $\Delta(u) = u$, $u \in D$. Then show that $\int_{\Phi} \omega = \int_{\Delta} (\omega)_{\Phi}$. [6]

(b) Define $f : \mathbb{R}^2 \to \mathbb{R}$ by [8]

$$f(x, y) = \begin{cases} \frac{x^3}{x^2+y^2}, & \text{if } (x.y) \neq (0,0), \\ 0, & \text{if } (x.y) = (0,0). \end{cases}$$

Show that

(i) the directional derivative $f'((0,0),(u,v))$ exists for all unit vectors (u,v) and has absolute value at most 1,

(ii) if $\gamma : \mathbb{R} \to \mathbb{R}^2$ is any differentiable map with $\gamma(0) = (0,0)$ and $\|\gamma'(0)\| > 0$, then $g : \mathbb{R} \to \mathbb{R}$ defined by $g(t) = f(\gamma(t))$ is differentiable at $t = 0$, but

(iii) f is not differentiable at $(0,0)$.

(7) (a) Calculate the second order Taylor polynomial for the function $f(x, y) = \cos^2(x^2 y^3)$. [5]

(b) State and prove the existence theorem for partition of unity of class C^∞. [9]

Your Roll Number: .....

Department of Mathematics, University of Delhi
M.A./M.Sc. Mathematics Examinations, June 2021
Part II Semester IV

MMATH18-403(iii): Topological Dynamics
(Unique Paper Code 223502411)

Time: **4 hours** (This includes **one hour** time for downloading the paper, scanning your answer sheets and uploading back in the email for the final submission.)
Maximum Marks: 70

Instructions: • All notations used are standard • **Question no.** 1 is **compulsory** • Attempt any **four** questions from the remaining six questions .

---

(1) (a) Construct a generator for the right shift operator on $X = \{\frac{1}{n}, 1 - \frac{1}{n} \mid n \in \mathbb{N}\}$ under the usual metric. (3)
(b) Give an example to justify that continuity of the function is a necessary condition in the hypothesis of Sarkovskii's Theorem. (3)
(c) Prove that the identity map on the Cantor space has pseudo orbit tracing property (POTP). (3)
(d) Can we say that every homeomorphism has a minimal set? Justify your claim. (3)
(e) Find attracting and repelling fixed points of the function $f(\theta) = \theta + \epsilon\ sin2\theta$, $0 < \epsilon < \frac{1}{2}$ and $\theta \in [0, 2\pi)$. (2)

(2) Let A be a $k \times k$ matrix with entries in $\{0, 1\}$.
(a) Prove that X_A is a closed subset of Σ_k. (4)
(b) Prove that A is an irreducible matrix if and only if its associated digraph is strongly connected. (5)
(c) Prove that A is an irreducible matrix if and only if $A \vee (A * A) \ldots\ldots \vee \underbrace{(A * \ldots * A)}_{n-times} = J$, for some $n \in \mathbb{N}$. (5)

(3) (a) Let $f : \mathbb{R} \to \mathbb{R}$ be a C^1 map and p be a hyperbolic fixed point of f. Prove that there exists an open interval U about p such that for every $x \in U$, $x \neq p$, $|f^{'}(p)| > 1$ implies there exists a $k \in \mathbb{N}$ satisfying $f^k(x) \notin U$. (5)
(b) Do the graphical analysis of $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \frac{1}{2}(x^3 + x)$ and draw the phase portrait of the orbit of $x = \frac{1}{2}$. (4)
(c) Find for which values of distinct $a, b \in \mathbb{R}$, $f, g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax$ and $g(x) = bx$ are topologically conjugate. (5)

(4) (a) Can we say that if a continuous function $f : [a, b] \to [a, b]$ has a periodic point of prime period 5 then it has a periodic point of all prime period n, $n \geq 1$? Justify your claim. (5)
(b) Prove that set of periodic points of the doubling map on the unit circle $\mathbb{S}^1$ is dense in $\mathbb{S}^1$. (5)
(c) If X is compact metric space and $f : X \to X$ is continuous, then prove that for every $x \in X$, $\omega(x, f) = \cap_{m \geq 0} \overline{(\cup_{n \geq m} \{f^n(x)\})}$. (4)

(5) (a) Prove that the set of points having converging semiorbits of an expansive self-homeomorphism of a compact metric space X is a countable set. Justify giving an example that result need not be true if X is not compact. (8)

(b) Prove that the usual interval $(\sqrt{2}, \sqrt{3})$ does not admit any expansive homeomoephism. (6)

(6) Consider $\mathbb{R}$ with the usual metric and $f : \mathbb{R} \to \mathbb{R}$.

(a) If f is a contraction map then prove that f has pseudo orbit tracing property (POTP). (8)

(b) If f is an isometry then prove that f does not have POTP. (6)

(7) (a) Let (X, d) be a compact metric space and $f : X \to X$ be a topologically Anosov homeomoephism. Prove that f has canonical coordinates and for $\epsilon > 0$, a number less than an expansive constant for f, we have $W^s(x, d) = \cup_{n \geq 0}(f^{-n}(W^s_\epsilon(f^n(x), d)))$. (9)

(b) Prove that if (X, d) is a compact metric space and $f : X \to X$ is a homeomorphism satisfying that for every $\epsilon > 0$ there exists a $\delta > 0$ such that every finite δ-pseudo orbit $(z_i)_{0 \leq i \leq k}$, $k \in \mathbb{N}$, is ϵ-traced by some point of X, then f has POTP. (6)

Department of Mathematics, University of Delhi
M.A./M.Sc. Mathematics Final Examination, 2021
Part II Semester IV

MMATH18 404(iv): OPTIMIZATION TECHNIQUES AND CONTROL THEORY

Unique Paper Code: 223502415

Time: 3 hours | Maximum Marks: 70

Instructions: • Attempt five questions in all. • Question 1 is compulsory.
• Answer any four questions from Q. 2 to Q. 7. • All questions carry equal marks.

(1) (a) Give an example of a convex function defined on $\mathbb{R}^2$ such that its effective domain $\mathrm{ED}(f) \neq \mathbb{R}^2$, $f(x) = -\infty$ for some x in $\mathbb{R}^2$ and $f(u)$ is finite at another point u in $\mathbb{R}^2$. [2 Marks]

(b) If the primal program (P_ϕ) is consistent then is it strongly consistent, where ϕ is a proper conex function? Justify. [3 Marks]

(c) Find the support function of the set $C = [1,2] \times [3,4] \subseteq \mathbb{R}^2$ defined as $f(x,y) = \sup_{(a,b)\in C}\{ax + by\}$. [3 Marks]

(d) Let $f : \mathbb{R} \to \mathbb{R} \cup \{+\infty\}$ be a convex function and $u, v \in \mathbb{R}, u \neq v$ be such that $f(u), f(v) \in \mathbb{R}$. If $z = \dfrac{u+v}{2}$ and $f(z)$ is finite prove that [3 Marks]

$$D^- f(z;1) \geq \min\{D^+ f(u;1), D^+ f(v;1)\}.$$

(e) Check the stability of the primal program (P_ϕ), if $\phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \cup \{+\infty\}$ is defined as [3 Marks]

$$\phi(x,w) = \begin{cases} x + w, & \text{if } x^2 = w, \\ +\infty, & \text{if } x^2 \neq w. \end{cases}$$

(2) (a) Find a function $f : \mathbb{R} \to \mathbb{R} \cup \{+\infty\}$ and its closure $\mathrm{cl}f$, whose subdifferential at every point in $\mathbb{R}$ is as follows [8 Marks]

$$\partial f(x) = \begin{cases} \emptyset, & \text{if } x < -1, \\ (-\infty, -1], & \text{if } x = -1, \\ \{-1\}, & \text{if } -1 < x < 0, \\ [-1, 0], & \text{if } x = 0, \\ \{x^3\}, & \text{if } 0 < x < 1 \\ \emptyset, & \text{if } x \geq 1. \end{cases}$$

Can you have more than one such function? Justify.

(b) Find the function $\phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \cup \{+\infty\}$ if the Lagrangain function $L(x,\lambda)$ is given as [6 Marks]

$$L(x,\lambda) = \begin{cases} x^2 - (1+\lambda)x, & \text{if } \lambda \geq -1, \\ -\infty, & \text{if } \lambda < -1. \end{cases}$$

Is the function ϕ closed? Justify.

(3) (a) Let f be a convex function defined on $\mathbb{R}^n$ such that $\text{cl}f \neq f$. Do they have the same conjugate? Justify. [4 Marks]

(b) Find the value of k such that the conjugate of the function $f(x) = kx^2$ defined on $\mathbb{R}$, is twice the given function? [3 Marks]

(c) Derive the dual of the problem using conjugate duality [7 Marks]

$$\begin{aligned} \text{Min } z &= c^T x \\ \text{subject to } Ax &\geq b, x \geq e \end{aligned}$$

where A is an $m \times n$ matrix, $e = (1, 1, ..., 1)$ and c are n vectors and b is an m vector.

(4) (a) If $f : \mathbb{R}^n \to \mathbb{R} \cup \{+\infty\}$ is a convex function and $x_1, x_2 \in \mathbb{R}^n$ are such that $f(x_1), f(x_2)$ are finite then prove that [7 Marks]

$$(\xi_1 - \xi_2)^T (x_1 - x_2) \geq 0, \forall \xi_1 \in \partial f(x_1), \xi_2 \in \partial f(x_2).$$

How can you write the above inequality in terms of directional derivative? What happens if the function f is differentiable at x_1 and x_2?

(b) Consider the primal problem (P_ϕ), where $\phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \cup \{+\infty\}$ is defined as [7 Marks]

$$\phi(x, w) = \begin{cases} x + w^2, & \text{if } x \geq -w, \\ +\infty, & \text{if } x < -w. \end{cases}$$

Find the primal and dual perturbation functions Φ and Ψ, respectively. Also, find the dual problem (D_{ϕ^*}).

(5) (a) What is an Euler−Poisson equation? Use it to find the solution of the following control problem [7 Marks]

$$\begin{aligned} \text{Max } J(x) &= \int_0^1 (x\ddot{x} - x^2 - 2x\dot{x})dt \\ \text{subject to } x(0) &= 0, x(1) = \tfrac{e^2-1}{e}. \end{aligned}$$

(b) Solve the following control problem [7 Marks]

$$\begin{aligned} \text{Max } J(x) &= \int_0^1 2x(t)dt + x(1) \\ \text{subject to } \dot{x}(t) &= x(t) + 2u^3(t) \\ x(0) = 0, x(1) &\text{ is free, } -1 \leq u(t) \leq 1. \end{aligned}$$

(6) (a) A vessel is to be loaded with stocks of three items. Each unit of item i has a weight w_i and value v_i. Use the dynamic programming approach to find the most valuable cargo load, if the maximum cargo weight the vessel can take is 5, if the details are as follows [7 Marks]

i	w_i	v_i
1	1	45
2	3	125
3	2	80

(b) Use the dynamic programming approach to solve the linear programming problem [7 Marks]

$$\text{Max } z = 3x_1 + x_2$$
$$\text{subject to } x_1 \leq 4, x_2 \leq 2, x_1 + 2x_2 \leq 6,$$
$$x_1 \geq 0, x_2 \geq 0.$$

(7) (a) Use the preliminary version of the conjugate gradient method, to find the critical points of [7 Marks]

$$q(x_1, x_2) = 2x_1^2 + 2x_1x_2 + x_2^2 + 2x_1 + x_2$$

starting from the point $(0, 0)$.

(b) Use the Newton's method to find the next two iterates starting from the point $(0, 0)$ to solve the problem [7 Marks]

$$\text{Min } f(x, y) = x^2 + 2x^4 + y^2 - 2y$$
$$\text{subject to } x > -1, y > -1.$$

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DELHI
M.A./M.Sc. Mathematics Examinations, June 2021
Part II, Semester IV

MMATH18-405(i): CRYPTOGRAPHY

Time: 3 Hours M.M. - 35

Instruction: Attempt five questions in all. Question no. one is compulsary. All the questions carry equal marks.

1. (a) An obvious approach to increase the security of a symmetric cipher is to apply the same cipher twice i.e., $y = e_{k_2}(e_{k_1}(x))$ where e is encryption algorithm and k_1, k_2 are keys. Now, assume vignere cipher on the following ciphertext twice with the keyword `TRICKY`. What will be the plaintext for the ciphertext `QFFILEYMDX`?
(The correspondance of english text and alphabetic characters is according to the following rule;$A \leftrightarrow 0, B \leftrightarrow 1, C \leftrightarrow 2, \cdots Z \leftrightarrow 25$.) (02)

(b) Let n be a positive integer and let $K = \{0,1\}^n$ be the key space. Given a key $K = (k_1, k_2, \cdots, k_n) \in \{0,1\}^n$, the keystream generator sets

$$s_i = k_i, \quad 1 \leq i \leq n$$

and

$$s_i = \sum_{j=1}^{n} c_j s_{i-j} \mod 2, i > n$$

where $c_1, c_2, \cdots, c_n$ are fixed coefficients. Suppose $n = 4$, the key stream is generated by recursion $s_{i+4} = s_i + s_{i+1}$, so we have chosen $c_1 = c_2 = 0, c_3 = c_4 = 1$. Let $k = (1,0,0,0)$ be the key. Then what will be the key stream and period of the key stream? (01)

(c) What is the condition for a system to be perfectly secret in terms of probability distributions? Give an example of a perfectly secure cryptosystem. (01)

(d) Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 83$ and a primitive root $\alpha = 5$. The secret key of Alice is $X_A = 6$ and secret key of Bob is $X_B = 10$. What will be the shared secret key? (01)

(e) In a public-key system, using RSA, suppose you intercepted the ciphertext $C = 8$, sent to a user whose public key is $e = 13, n = 33$. What is the plaintext x? (01)

(f) In DES, how many bits are given as input and taken as output in S-box? (01)

2. Suppose that we have the following 128-bit AES key, given in hexadecimal notation:

$$2B7E151628AED2A6ABF7158809CF4F3C$$

Construct two more keys from this key, explaining each step of the construction. (07)

3. Decrypt the ciphertext 101010101010, using ECB mode and OFB mode explaining each step. Use the permutation cipher with block length 3 and the key, $k = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. The IV is 000. For OFB mode use $r = 2$. (07)

4. Suppose we encrypt the plaintext $p =$ `0123456789ABCDEF`, its binary expansion is

0	0	0	0	0	0	0	1
0	0	1	0	0	0	1	1
0	1	0	0	0	1	0	1
0	1	1	0	0	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	0	1	1	0	1
1	1	1	0	1	1	1	1

The application of IP yields

1	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0
1	1	1	1	1	1	1	1
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0

so we obtain

$$L_0 = 11001100000000000110011001111111$$
$$R_0 = 11110000101010101111000010101010$$

The DES key we used is

$$133457799BBCDFF1$$

whose binary expansion is

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

We compute the first round key,

$$K_1 = 000110110000001011101111111111000111000001110010.$$

Using this key we obtain

$$\begin{aligned} E(R_\circ) \oplus K_1 &= 011000010001011110111010100001100110010100100111 \\ f(R_{circ}, K) &= 00000011010010111010100110111011 \end{aligned}$$

and finally

$$R_1 = 11001111010010110110010101000100.$$

Now, compute the second round using above given information. (07)

5. (a) What is whitening? (01)

   (b) Suppose an SPN network in which the key is,

$$K = 00111010100101001101011000111111$$

and the round keys are,

$$K_1 = 0011101010010100$$
$$K_2 = 1010100101001101$$
$$K_3 = 1001010011010110$$
$$K_4 = 0100110101100011$$
$$K_5 = 1101011000111111$$

Suppose the plaintext is, $x = 1100010000001101$. Then what will be the output of first round of SPN? That is, find out u', v' and w' using following permutation and substitution:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Table 1: Substitution Table

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Table 2: Permutation Table

(03)

(c) Show that the stream cipher that is constructed with a linear shift register can also be viewed as a block cipher in OFB mode if the length of the plaintext is a multiple of block length. (03)

6. (a) For $k = 21$ and $m = 247$, find s for which $k^s \mod m = 60$. (02)

   (b) For $k = 21$ and $m = 247$, find s for which $k^s \mod m = 64$. (02)

   (c) Suppose two parties perform a Diffie-Hellman key exchange, and you intercept their values of $k = 21, m = 247$, $k^r \mod m = 34$, and $k^s \mod m = 64$. Use your answer to part (b) to determine the candidate RSA encryption exponent $e = k^{r \cdot s} \mod m$. (03)

7. We give an example of the ElGamal cryptosystem implemented in $\mathbb{F}_{3^3}$. The polynomial $x^3 + 2x^2 + 1$ is irreducible over $\mathbb{Z}_3[x]$ and hence $\mathbb{Z}_3[x]/(x^3 + 2x^2 + 1)$ is the field $\mathbb{F}_{3^3}$. The correspondance is given in following table. We can associate the 26 letters of the alphabet with the 26 nonzero field elements, and thus encrypt ordinary text in a convenient way. We will use a lexicographic ordering of the (nonzero) polynomials to set up the correspondance. Suppose Bob

A	$\leftrightarrow$	1	B	$\leftrightarrow$	2	C	$\leftrightarrow$	x
D	$\leftrightarrow$	$x+1$	E	$\leftrightarrow$	$x+2$	F	$\leftrightarrow$	$2x$
G	$\leftrightarrow$	$2x+1$	H	$\leftrightarrow$	$2x+2$	I	$\leftrightarrow$	x^2
J	$\leftrightarrow$	x^2+1	K	$\leftrightarrow$	x^2+2	L	$\leftrightarrow$	x^2+x
M	$\leftrightarrow$	x^2+x+1	N	$\leftrightarrow$	x^2+x+2	O	$\leftrightarrow$	x^2+2x
P	$\leftrightarrow$	x^2+2x+1	Q	$\leftrightarrow$	x^2+2x+2	R	$\leftrightarrow$	$2x^2$
S	$\leftrightarrow$	$2x^2+1$	T	$\leftrightarrow$	$2x^2+2$	U	$\leftrightarrow$	$2x^2+x$
V	$\leftrightarrow$	$2x^2+x+1$	W	$\leftrightarrow$	$2x^2+x+2$	X	$\leftrightarrow$	$2x^2+2x$
Y	$\leftrightarrow$	$2x^2+2x+1$	Z	$\leftrightarrow$	$2x^2+2x+2$			

Table 3: Correspondance of alphabets and field elements

uses $\alpha = x$ and $a = 11$ in an ElGamal cryptosystem; then $\beta = x + 2$. Show how Bob will decrypt the following string of ciphertext;

$$(K, H)(P, X)(N, K)(H, R)(T, F)(V, Y)(E, H).$$

(07)

Department of Mathematics
University of Delhi, Delhi
M.A./M.Sc., Part II Semester IV, June 2021
MMATH18-405(ii) Support Vector Machine

Time: 3 hours Max Marks: 35

Instruction: Attempt five questions in all. Question 1 is compulsory. All questions carry equal marks.

1. (a) What are the constraint in dual optimization problem solved to obtain the hard margin optimal separating hyperplane? **(1)**

   (b) What is hinge loss for $f(x) = w^T x_i + b$? **(1)**

   (c) Is support vector regression subset of support vector machine? **(1)**

   (d) Should we use the primal or the dual form of the SVM problem to train a model on a training set with millions of instances and hundreds of features?? **(1)**

   (e) What is the role of C in Linear C-Support Vector Classification? **(1)**

   (f) A function is convex if its Hessian is negative semidefinite.(T/F) **(1)**

   (g) If you remove one of the support vectors does the size of the optimal margin decrease, stay the same, or increase? **(1)**

2. Write algorithm of Linear ϵ-support vector regression.What ϵ signify in this algorithm?

   (7)

3. Consider the optimization problem

$$\begin{aligned} \underset{w,b}{\text{minimize}} \quad & < w.w > + C_1 \sum_{i=1}^{l} \Omega_i + C_2 \sum_{i=1}^{l} \Omega_i^2 \\ \text{subject to} \quad & y_i(< w.x_i > + b) \geq 1 - \Omega_i, \ i = 1, \ldots, l. \\ & \Omega_i \geq 0, \ i = 1, \ldots, l \end{aligned}$$

   Discuss the effect of varying the parameters C_1 and C_2. Derive the dual Optimization problem.

   (7)

4. Prove that the number of linear separators of two classes is either infinite or zero.

(7)

5. What are the objectives of flatness of support vector machines.Explain.

(7)

6. Prove.There exist solutions to the primal problem

$$\begin{aligned} \min_{w,b} \quad & \frac{1}{2} w^t w + C \sum_{i=1}^{l} \Omega_i \\ \text{subject to} \quad & y_i((w.x_i) + b) \geq 1 - \Omega_i, \ i = 1, \ldots, l. \\ & \Omega_i \geq 0, \ i = 1, \ldots, l \end{aligned}$$

w.r.t. (w, b).

(7)

7. State the Duality Theorem of linear programming and use it to prove the Theorem of Complementary Slackness.

(7)