Pt. Ravishankar Shukla University, Raipur
M.Phil. (Mathematics) Course 2009-10

Scheme of Examination

There shall be three theory papers and one dissertation in M.Phil.(Mathematics). All are compulsory. Each paper will have 100 marks. The course content of each paper has been divided into five units. However, there will be internal choice in each Unit. Dissertation will be of

S.No.	Particulars			Max. Marks	
1	Theory Papers	Paper-I	Nonlinear Functional Analysis	100	300
		Paper-II	Cryptography	100	
		Paper-III	Topological Structures with Applications	100	
2	Dissertation		Script	100	200
			Viva Voce	100	
3	Seminar		On dissertation	50	100
			On Theory Papers	50	
Grand Total					600

Guidelines of activities/academic calendar for M.Phil. Students:

1. In order to pass the M.Phil. Examination a student required to obtain a minimum of 25% marks in each theory paper and minimum of 50% marks in aggregate to the theory papers, dissertation and seminars separately.
2. The subject of dissertation will be provided by supervisor in the first week of September.
3. The dissertation has to be submitted by the end of first week of March. Thereafter supervisor will take no responsibility for delay in the submission of the dissertation.
4. Students are requested to complete the typing work (preferably in AMS-Tex/Latex) of their dissertation by the last week of February.
5. Every week on student will present his/her seminar using OHP/LCD based on the theory papers/on the subject assigned in the dissertation.

Paper I

Nonlinear Functional Analysis

M.M. 100

Unit I Calculus in Banach spaces : Various forms of continuity, geometry in normed spaces and duality mapping, Nemytskii, hammerstein and Uryshon operators, Gateaux and Frechet derivatives , properties of the derivative, Taylor's theorem, inverse function theorem and implicit function theorem.

Unit II Monotone operators and its applications : Monotone operators, surjectivity theorems, constructive solutions of operator equations, subdifferential and monotonocity, generalizations of monotone operators.

Unit III Fixed point theorems : Banach contraction principle and its generalizations, nonexpansive mappings, asymptotically nonexpansive mappings, fixed point theorems of Brouwer and Schauder,

Unit IV Common Fixed point theorems : Fixed point theorems for multifunctions, common fixed point theorems, sequence of contractions, generalized contractions and fixed points, fixed point theorems in ordered Banach spaces.

Unit V Probabilistic Functional Analysis : Probabilistic concepts, random operators, random fixed point theorems, random operator equations involving monotone operators.

Books recommended:

1. M. C. Joshi and R. K. Bose, Some topics in nonlinear functional analysis, Wiley Eastern Limited, New Delhi 1985.
2. E. Zeidler, Nonlinear functional analysis and its applications I: Fixed Point Theorems, Springer, Heidelberg 1986.
3. K. Deimling, Nonlinear functional analysis and its applications I: Fixed Point Theorems, Springer, Heidelberg 1985.
4. R. Akerkar, Nonlinear functional analysis, Narosa Publishing House, New Delhi.

Paper -II

CRYPTOGRAPHY

Note: Each unit will be given wight-age of 20 marks. Student will attempt one question from each unit. There will be internal choice in each unit.

M.M. 100

UNIT 1:Fundamental concepts:

Elements of number theory: Greatest Common Divisor, divisibility and Euclidean algorithm, Congruences, Semi-Groups, Groups, Residue Class Rings, Fields, Analysis of Operation in the Residue Class Rings, Fermat's Little Theorem, Fast Exponentiation, The Chinese Remainder Theorem ,Time estimates for doing arithmetic, Polynomial time. Factoring concept.

Unit 2 – **Encryption process** :

Encryption, decryption and key generation. Symmetric and Asymmetric Crypto systems, Cryptanalysis, Alphabets and Words, Permutations, Block Ciphers, Multiple Encryption, Use of Block Ciphers, Stream Ciphers, Affine Ciphers, Matrices and Linear Maps, Affine Linear Block Ciphers, Vigenere, Hill and Permutation Ciphers, Cryptanalysis of Affine Linear Block Ciphers

Unit 3- **Public key cryptosystems** :

Enciphering matrices, the idea of public key cryptography, design of RSA, some important properties of RSA, Discrete logarithm problem, public key cryptosystem based on Knapsack problem , the concept of zero knowledge transfer.

Unit 4- **Primality and factoring**:

Trial Division, p-1 Method, pseudo primes, the rho methods, Fermat factorization and factor basis, the continued fraction method, the quadratic sieve method.

Unit 5- **Elliptic curves** :

Basic facts and application of elliptic curve in cryptography, elliptic curve cryptosystem, elliptic curve primality test, elliptic curve factorization. Digital Signatures: RSA Signature, Signature from Public Key Systems, ElGamal Signature.

Books recommended :

1.A course in number theory and cryptography by N. Koblitz. Springer 2002.
2.An introduction to cryptography by J. A. Buchmman. Springer.2001.
3.Introduction to Cryptography by Hans Delfs and H.Knebl. Springer 2001.
4. Modern cryptography by O.Goldrich. Springer. 1999
5. Modern cryptography: theory and practice by Wenbo Mao. HP. 2004.

Paper III

TOPOLOGICAL STRUCTURES WITH APPLICATIONS

M.M. 100

Note: Each unit will be given wight-age of 20 marks. Student will attempt one question from each unit. There will be internal choice in each unit.

Unit-I Fundamental Concepts of Topological Spaces- Topological spaces-Definition and examples, subspace, quotient space. Topological spaces and generalizations (closure spaces, etc.). Continuity and open sets in topological spaces. Metric, product and quotient topologies. Continuous functions and topological equivalence. Surfaces. Separation axioms T_0, T_1, T_2, $T_{3½}$, T_4, Uryshon's lemma, Titze extension theorem.

Unit-II Compactness and Connectedness- Compactness. Basic properties of compactness. Nets and filter. Compactness and nets. Ultra-filters. Ultra-filters and compactness. The role of topology in Chaos and dynamical systems- *History of Chaos, examples, notions of Chaos.* Compact spaces. Identification spaces and compactness. Connectedness and path-connectedness. Cantor sets. Application of compact sets in *population dynamics and Fractals.*

Unit-III Manifolds and Complexes- Manifolds. Triangulations. Classification of surfaces. Euler Characteristics. Topological groups. Group actions and Orbit spaces. Topological Semi-fields. Common fixed point of mappings defined on Banach spaces over topological semi-fields and its application *to solve certain nonlinear functional equations.* Application of manifold in *Robotic coordination and configuration spaces, geometry of manifolds, the topology of the Universe.*

Unit-IV Homotopy, Winding Numbers and Vector Field- Homotopy and paths. The winding number. Degrees of maps. The Brouwer fixed point theorem. The Borsuk-Ulam Theorem.. Vector fields and the Poincare Index Theorem. Applications in *the fundamental theorem of algebra, Sandwiches, Game theory and Nash equilibria, Vector fields, Path integrals and the winding number, Vector fields on surfaces, Index theory for n-symmetry fields.*

Unit-V The Topological Degree Axiomatic Definition of the Brouwer Degree in $\mathbf{R}^n$. Application of the Brouwer Degree. Brouwer Theorem, Perron-Frobenius Theorem, Surjective Maps, Hedgehog Theorem. The Leray-Schauder degree. Borsuk's Antipodal Theorem. Compact Linear Operators. Application of topological degree in *Fixed Point Theory.*

Text Books:

1. K. D. Joshi, Introduction to General Topology, Wiley Eastern Ltd, New Delhi, !983.
2. James R. Munkres, Topology, 2nd Edition, Pearson Education Asia, 2002.
3. William F. Basener, Topology and its applications, Wiley-InterScience, 1973.
4. R. Akerkar, Nonlinear functional analysis, Narosa Publishing House, New Delhi.

Recommended Books:

5. C. Robinson, Dynamical Systems, Stability, Symbolic Dynamics and Chaos, CRC Press, 1995.
6. S. Willord, General Topology, Dover, 2004.
7. R. L. Devancy, An Introduction to Chaotic Dynamical Systems, Persues Publicating Co., 1989.