UG Semester III

Paper 5: Linear & Abstract Algebra

Credit: 4 **T:04**

Course Outcomes:

1. The fundamental concept of Rings, Fields, subrings, integral domains and the corresponding morphisms.
2. The concept of linear independence of vectors over a field, the idea of basis and the dimension of a vector space.
3. Basic concepts of linear transformations, the Rank-Nullity Theorem, matrix of a linear transformation and the change of basis.
4. Automorphisms for constructing new groups from the given group.
5. Group actions, Sylow theorems and their applications to check nonsimplicity.
6. Compute inner products and determine orthogonality on vector spaces.

UNIT I

Automorphism, inner automorphism, automorphism groups and their computations, Conjugacy relations, Normaliser, Counting principle and the class equation of a finite group, Center of group of prime power order, simple groups, Group action, Burnside lemma, Sylow theorems and its applications.

UNIT II

Prime and maximal ideals, Euclidean Rings, Principal ideal rings, Polynomial Rings, Polynomial over the Rational Field, The Eisenstein Criterion, Polynomial Rings over Commutative Rings, unique factorization domain.

UNIT III

Vector spaces, Subspaces, Linear independence and dependence of vectors, Basis and dimension, Quotient space, Linear transformations, Direct sums, The Algebra of linear transformations, rank nullity theorem, their representation as matrices, Linear functionals, Dual space, Characteristic values, Cayley Hamilton Theorem.

UNIT IV

Inner product spaces, Cauchy-Schwarz inequality, Orthogonal vectors, Orthonormal sets and bases, Bessel's inequality for finite dimensional spaces, Gram-Schmidt orthogonalization process, Bilinear and Quadratic forms.

References:

Text books:

1. Topics in Algebra by I. N. Herstein.
2. Algebra by V. Sahai and V. Bist
3. Linear Algebra by V. Sahai and V. Bist

Suggested Readings:

1. Linear Algebra by K. Hoffman and R. Kunze.

Web References:

1. Digital platforms web links : NPTEL/SWAYAM/ MOOCS/Openstax.org
2. https://openlearninglibrary.mit/edu/courses
3. http://heecontent.upsdc.gov.in/SearchContent.aspx
4. https://www.lkouniv.ac.in/en/article/e-content-faculty-of-science

Paper 6: Mechanics

Credit: 4 **T:04**

Course Outcomes:

1. The significance of mathematics involved in physical quantities and their uses.
2. To understanding the various concepts of basic mechanics like simple harmonic motion, motion under other laws and forces.
3. To study and to learn the cause-effect related to these.
4. The applications in observing and relating real situations/structures.

UNIT I

Frame of reference, work energy principle, Forces in three dimensions, Poinsot's central axis, Wrenches, Null lines and planes.

UNIT II

Virtual work, Stable and Unstable equilibrium, Catenary, Catenary of uniform strength.

UNIT III

Velocities and accelerations along radial and transverse directions, and along tangential and normal directions, Simple Harmonic motion, Motion under other law of forces. Elastic strings, Motion in resisting medium, Constrained motion, Motion on smooth and rough plane curves.

UNIT IV

Motion of particles of varying mass, Rocket motion, Central orbit, Kepler's laws of motion, Motion of particle in three dimensions, Rotating frame of reference, Rotating Earth, Acceleration in terms of different coordinates systems.

References Text Books:

1. R.C. Hibbeler, Engineering Mechanics-Statistics
2. Nelson, Engineering Mechanics- Dynamics, Tata McGraw Hill

Suggested Readings:

1. J.L. Synge & B.A. Griffith, Principles of Mechanics, Tata McGraw Hill

Web References:

1. Digital platforms web links: NPTEL/SWAYAM/ MOOCS/Openstax.org
2. https://openlearninglibrary.mit/edu/courses
3. http://heecontent.upsdc.gov.in/SearchContent.aspx
4. https://www.lkouniv.ac.in/en/article/e-content-faculty-of-science

(For students with Mathematics as a minor subject)

Paper Q3: Applicable Mathematics– III

Credit: 2 **T:02**

Course Outcomes:

1. To understand the concepts of groups, cyclic groups, and homomorphism of groups.
2. To know the concepts of rings, ideals, quotient rings and homomorphism of rings.
3. To know the concept of vector spaces and linear transformations.

UNIT I

Equivalence relations and partitions, congruence modulo n, groups, subgroups, cyclic groups, coset decomposition, Lagrange's theorem, Fermat's & Euler's theorems.

UNIT II

Normal subgroups, quotient groups, homomorphism and homomorphism theorems, permutation group, even and odd permutations.

UNIT III

Rings, types of rings - commutative rings, rings with unity, division rings, integral domains and fields, subrings, ideals and quotient rings, ring homomorphism, characteristic of a ring, Polynomial rings.

UNIT IV

Vector spaces, subspaces, linear independence and dependence, basis and dimension, quotient space, linear transformations.

References:

Textbooks

1. V. Sahai & V. Bist : Algebra, Narosa.
2. J.A. Gallian : Contemporary Abstract Algebra, Narosa.
3. R.G. Bartle : Introduction to Real Analysis, Wiley.

Suggested books:

1. J.B. Fraleigh : A First course in Abstract Algebra, Pearson.
2. D.S. Dummit & R.M. Foote : Abstract Algebra, Wiley International edition.

Co-Curricular Course in Mathematics

Paper CC-2: Elementary Cryptography
(Pre-requisites: Mathematics in Class 12)

Credit: 2 **T:02**

Course Objectives:

1. To provide deeper understanding of mathematics used in cryptography
2. To familiarize with cryptographic techniques for secure communication of two parties over an insecure channel
3. To provide understanding of modern cryptography
4. To explain modern stream and block ciphers
5. To explain asymmetric key cryptography

Course Outcomes:

At the end of this course students will be able to:.

1. Use modern symmetric key algorithms for cryptography
2. Use modern asymmetric key algorithms for cryptography
3. To examine the issues and structure of modern stream and block ciphers

UNIT I

Overview of Cryptography, What is cipher?, Security Attacks, Security Services and Security Mechanisms, A model for Network Security, Symmetric Cipher Modes, Substitute Techniques, Transposition Techniques, Rotor Machines, Steganography.

UNIT II

Historical encryption schemes, Perfect secrecy and One Time Pad, Cryptanalysis of historical ciphers.

UNIT III

General structure of modern stream and block cipher, RC-4 stream cipher, DES and AES block cipher.

UNIT IV

Principles of Public key crypto system, Cryptography using arithmetic modulo primes, Diffie Hellman Key Exchange, the RSA algorithm, square-and-multiply, Key Management, Elliptic key cryptography.

Recommended Books:

1. Cryptography and Network Security, William Stallings, Prentice Hall.
2. Understanding Cryptography, Christof Paar and Jan Pelzl, Springer.