Course Type	Course Code	Name of Course	L	T	P	Credit
DE	NMCD536	Finite Field Theory	3	0	0	3

Course Objective
The theory of finite fields plays an important role in Computer science, Electrical Communications and as well as in Mathematics because of its diverse applications in coding theory, combinatorics, cryptography, and the mathematical study of switching circuits. The objective of this course is to study the theoretical properties of finite fields, the theory of polynomials over finite fields, and their applications.
Learning Outcomes
Students will learn the basic properties of finite fields, properties of polynomials over finite fields and their importance in the area of coding theory, cryptography and shift register sequences.

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1	Review of Groups, Rings, Integral domains, Polynomial Rings, Division Algorithm and field extensions.	7	Students will learn the basics of field extension and finite fields.
2	Characterization of finite fields, Roots of irreducible polynomials, Traces, Norms and Bases, Roots of unity, Cyclotomic polynomials, Representation of elements of finite fields.	11	Students will be able to understand the concepts of traces, norms, different types of bases, cyclotomic polynomials and different ways of representing the elements of a finite field.
3	Polynomial over finite fields, Order of polynomials, Primitive polynomials, Irreducible polynomials, Construction of Irreducible polynomials.	8	Students will learn the different kind of polynomials such as irreducible and primitive polynomials over finite fields.
4	Linearized polynomials, Binomials and Trinomials, Permutation Polynomials.	8	Students will be able to understand the construction of Irreducible polynomials, and properties of different types of polynomials over finite fields.
5	Irreducibility tests : Rabin Test and Berlekemp Test, Factorization of polynomials over finite fields: Berlekemp algorithm and Zassenhaus algorithm, Calculation of roots of polynomials, the number of solutions of the polynomial equation.	8	Students will learn the Irreducibility tests, factorization algorithms of polynomials and techniques to find roots of polynomials over finite fields.
	Total	42	

Text Books:

1. R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 2009.
2. G. L. Mullen and and D. Panario, Handbook of Finite Fields, Chapman and Hall/CRC, 2013.

Reference Books:

1. A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone,T. Yaghoobian, Applications of Finite Fields, Springer, 1993.
2. D. Jungnickel, Finite Fields: Structure and Arithmetics, Spektrum Akademischer Verlag, 1993.