1. Record Nr. UNISA996418203603316

Autore	Hachenberger Dirk
Titolo	Topics in Galois fields / / Dirk Hachenberger and Dieter Jungnickel
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] ©2020
ISBN	3-030-60806-9
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XIV, 785 p. 11 illus.)
Collana	Algorithms and Computation in Mathematics, , 1431-1550 ; ; 29
Disciplina	512.3
Soggetti	Finite fields (Algebra) Galois theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Basic Algebraic Structures and Elementary Number Theory -- Basics on Polynomials- Field Extensions and the Basic Theory of Galois Fields -- The Algebraic Closure of a Galois Field -- Irreducible Polynomials over Finite Fields -- Factorization of Univariate Polynomials over Finite Fields -- Matrices over Finite Fields -- Basis Representations and Arithmetics -- Shift Register Sequences -- Characters, Gauss Sums, and the DFT -- Normal Bases and Cyclotomic Modules -- Complete Normal Bases and Generalized Cyclotomic Modules -- Primitive Normal Bases -- Primitive Elements in Affin Hyperplanes -- List of Symbols -- References -- Index.
Sommario/riassunto	This monograph provides a self-contained presentation of the foundations of finite fields, including a detailed treatment of their algebraic closures. It also covers important advanced topics which are not yet found in textbooks: the primitive normal basis theorem, the existence of primitive elements in affine hyperplanes, and the Niederreiter method for factoring polynomials over finite fields. We give streamlined and/or clearer proofs for many fundamental results and treat some classical material in an innovative manner. In particular, we emphasize the interplay between arithmetical and structural results, and we introduce Berlekamp algebras in a novel way which provides a deeper understanding of Berlekamp's celebrated factorization algorithm. The book provides a thorough grounding in finite field

theory for graduate students and researchers in mathematics. In view of its emphasis on applicable and computational aspects, it is also useful for readers working in information and communication engineering, for instance, in signal processing, coding theory, cryptography or computer science.