

1. Record Nr.	UNINA9910816414903321
Autore	Reilly Norman R.
Titolo	Introduction to applied algebraic systems // Norman R. Reilly
Pubbl/distr/stampa	New York, New York : , : Oxford University Press, , 2009 ©2009
ISBN	0-19-772720-4 0-19-970992-0
Descrizione fisica	1 online resource (xiii, 509 p.) : ill
Disciplina	512/.482
Soggetti	Algebra
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Formerly CIP.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	CONTENTS ; 1. Modular Arithmetic; 1.1 Sets, functions, numbers; 1.2 Induction; 1.3 Divisibility; 1.4 Prime Numbers; 1.5 Relations and Partitions; 1.6 Modular Arithmetic; 1.7 Equations in \mathbb{Z}_n ; 1.8 Bar codes; 1.9 The Chinese Remainder Theorem; 1.10 Euler's ϕ -function; 1.11 Theorems of Euler and Fermat; 1.12 Public Key Cryptosystems ; 2. Rings and Fields; 2.1 Basic Properties; 2.2 Subrings and Subfields; 2.3 Review of Vector Spaces; 2.4 Polynomials; 2.5 Polynomial Evaluation and Interpolation; 2.6 Irreducible Polynomials; 2.7 Construction of Finite Fields; 2.8 Extension Fields; 2.9 Multiplicative Structure of Finite Fields; 2.10 Primitive Elements; 2.11 Subfield Structure of Finite Fields; 2.12 Minimal Polynomials; 2.13 Isomorphisms Between Fields; 2.14 Error Correcting Codes ; 3. Groups and Permutations; 3.1 Basic Properties; 3.2 Subgroups; 3.3 Permutation Groups; 3.4 Matrix Groups; 3.5 Even and Odd Permutations; 3.6 Cayley's Theorem; 3.7 Lagrange's Theorem; 3.8 Orbits; 3.9 Orbit/Stabilizer Theorem; 3.10 Burnside's Theorem; 3.11 K-Colourings; 3.12; 4. Groups; Homomorphisms and Subgroups; 4.1 Homomorphisms; 4.2 The Isomorphism Theorems; 4.3 Direct Products; 4.4 Finite Abelian Groups; 4.5 Conjugacy and the Class Equation; 4.6 The Sylow Theorems 1 and 2; 4.7 Sylow's Third Theorem; 4.8 Solvable Groups; 4.9 Nilpotent Groups ; 5. Rings and Polynomials; 5.1 Homomorphisms and Ideals; 5.2 Polynomial Rings; 5.3 Division Algorithm in $F[x_1, x_2, \dots, x_n]$; Single Divisor; 5.4 Multiple Divisors;

Groebner Bases; 5.5 Ideals and Affine Varieties; 5.6 Complex Numbers; 5.7 Decomposition of Affine Varieties; 5.8 Cubic Equations in One Variable; 5.9 Parameters; 5.10 Singular and Nonsingular Points ; 6. Elliptic Curves; 6.1 Elliptic Curves; 6.2 Homogeneous Polynomials; 6.3 Projective Space; 6.4 Intersection of Lines and Curves; 6.5 Defining Curves by Points; 6.6 Classification of Conics; 6.7 Reducible Conics and Cubics; 6.8 The Nine Point Theorem; 6.9 Groups on Elliptic Curves; 6.10 The Arithmetic on an Elliptic Curve; 6.11 Results Concerning the Structure of Groups on Elliptic Curves ; 7. Further Topics Relating to Elliptic Curves 418; 7.1 Elliptic Curve Cryptosystems; 7.2 Fermat's Last Theorem; 7.3 Elliptic Curve Factoring Algorithm; 7.4 Singular Curves of Form $y^2 = x^3 + ax + b$; 7.5 Birational Equivalence; 7.6 The Genus of a Curve; 7.7 Pell's Equation

Sommario/riassunto

This resource provides a rigorous and extensive undergraduate introduction to algebraic systems covering basic number theory, rings, fields, polynomial theory, groups, algebraic geometry and elliptic curves.
