© 2019 FIZ Karlsruhe

ZMATH 2011c.00606

Carstensen, Celine; Fine, Benjamin; Rosenberger, Gerhard

Abstract algebra. Applications to Galois theory, algebraic geometry and cryptography.

Sigma Series in Pure Mathematics 11; De Gruyter Graduate. Berlin: Walter de Gruyter; Lemgo: Heldermann Verlag (ISBN 978-3-11-025008-4/pbk). xi, 366 p. (2011).

This book is an introductory text on abstract algebra and the authors assume that the readers are familiar with Calculus and with some linear algebra, primarily matrix algebra and the basic concepts of vector spaces, bases and dimensions. All other necessary material is introduced and explained in the book. The material is presented sequentially so that the polynomials and field extensions precede an in-depth look at group theory. The centerpiece of these notes is the development of Galois theory and its important applications, especially the insolvability of the quintic. The basic algebraic structures (group, rings and fields) are introduced in the first three chapters. The first notion is briefly exposed but the last two notions are presented here in detail, so that we can find enough information regarding factor rings and ring homomorphisms, quotient fields, subrings and ideals (prime, maximal or principal), integral domains or principal ideal domains. In Chapter 3, the fundamental theorem of arithmetic is revised (its proof and several other ideas from classical number theory) and it is proved that there are many other integral domains where this also holds (called unique factorization domains). Then the authors begin the theory of polynomials and polynomial equations over rings and fields (including the fundamental theorem of algebra or of symmetric polynomials), develop the main ideas of field extensions and adjoining elements to fields. Regarding these, they translate three problems of constructions using a straightedge and compass into the language of field extensions and prove that each of these problems is insolvable in general and give the complete solution to the construction of the regular n-gons. The authors finish the first part of the book with splitting fields and normal extensions, presenting another proof for the fundamental theorem of algebra. The concept of a splitting field is essential to the Galois theory of equations. After this, the necessary material from group theory needed to complete both the insolvability of the quintic and solvability by radicals in general is presented. Hence the middle part of the book, Chapters 9 through 14, are concerned with group theory, including permutation groups, solvable groups, abelian groups and group actions. Chapter 14 is somewhat off to the side of the main theme of the book. Here the authors give a brief introduction to free groups, group presentations and combinatorial group theory. Finally, after all of these presentations, the last but most important part of the book begins. They study general normal and separable extensions and the fundamental theorem of Galois theory. Using this, the authors present several major applications of the theory, including solvability by radicals and the insolvability of the quintic, the fundamental theorem of algebra, the constructions of regular n-gons and the famous impossibilities: squaring the circle, doubling the cube and trisecting an angle. Some aspects from the theory of modules follow (vector spaces being crucial in the study of fields and Galois theory since every field extension is a vector space over any subfield), finitely generated abelian groups, integral and transcendental extensions (including the transcendence of e and π) and algebraic geometry (this involving the study of algebraic curves which roughly are the sets of zeros of a polynomial or of a set of polynomials in several variables over a field). The book is finished in a slightly different direction giving an introduction to algebraic and group based cryptography. *Florentina Chirteş (Craiova)*

Classification: H45 H75 P20
Keywords: groups; rings; fields; subgroups; ideals; polynomials; fields extensions; solvability; modules; cryptography
doi:10.1515/9783110250091