GIAN-CARLO ROTA, *Editor*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume 22

Section: Algebra

P. M. Cohn and Roger Lyndon, *Section Editors*

Field Extensions and Galois Theory

Julio R. Bastida

GIAN-CARLO ROTA, *Editor*
ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS
Volume 22

Section: Algebra
P. M. Cohn and Roger Lyndon, *Section Editors*

Field Extensions and Galois Theory

Julio R. Bastida
Department of Mathematics
Florida Atlantic University
Boca Raton, Florida

With a Foreword by

Roger Lyndon
The University of Michigan
Ann Arbor, Michigan

1984
Addison-Wesley Publishing Company
Advanced Book Program
Menlo Park, California

Reading, Massachusetts · London · Amsterdam · Don Mills, Ontario · Sydney · Tokyo

Library of Congress Cataloging in Publication Data

Bastida, Julio R.
Field extensions and Galois theory.

(Encyclopedia of mathematics and its applications; v. 22)
Bibliography: p.
Includes index.
1. Field extensions (Mathematics). 2. Galois theory.
I. Title. II. Series.
QA247.B37 1984 512′.32 83-7160
ISBN 0-201-13521-3

American Mathematical Society (MOS) Subject Classification Scheme (1980):
12FXX, 12F05, 12F10, 12F15, 12F20

ABCDEFGHIJ-MA-89876543

Manufactured in the United States of America

GIAN-CARLO ROTA, *Editor*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume		Section
1	LUIS A. SANTALÓ **Integral Geometry and Geometric Probability,** 1976 (2nd printing, with revisions, 1979)	Probability
2	GEORGE E. ANDREWS **The Theory of Partitions,** 1976 (2nd printing, 1981)	Number Theory
3	ROBERT J. McELIECE **The Theory of Information and Coding** A Mathematical Framework for Communication, 1977 (2nd printing, with revisions, 1979)	Probability
4	WILLARD MILLER, Jr. **Symmetry and Separation of Variables,** 1977	Special Functions
5	DAVID RUELLE **Thermodynamic Formalism** The Mathematical Structures of Classical Equilibrium Statistical Mechanics, 1978	Statistical Mechanics
6	HENRYK MINC **Permanents,** 1978	Linear Algebra
7	FRED S. ROBERTS **Measurement Theory** with Applications to Decisionmaking, Utility, and the Social Sciences, 1979	Mathematics and the Social Sciences
8	L. C. BIEDENHARN and J. D. LOUCK **Angular Momentum in Quantum Physics:** Theory and Application, 1981	Mathematics of Physics
9	L. C. BIEDENHARN and J. D. LOUCK **The Racah-Wigner Algebra in Quantum Theory,** 1981	Mathematics of Physics

GIAN-CARLO ROTA, *Editor*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume		Section
10	JOHN D. DOLLARD and CHARLES N. FRIEDMAN **Product Integration** with Application to Differential Equations, 1979	Analysis
11	WILLIAM B. JONES and W. J. THRON **Continued Fractions:** Analytic Theory and Applications, 1980	Analysis
12	NATHANIEL F. G. MARTIN and JAMES W. ENGLAND **Mathematical Theory of Entropy,** 1981	Real Variables
13	GEORGE A. BAKER, Jr. and PETER R. GRAVES-MORRIS **Padé Approximants, Part I** **Basic Theory,** 1981	Mathematics of Physics
14	GEORGE A. BAKER, Jr. and PETER R. GRAVES-MORRIS **Padé Approximants, Part II:** **Extensions and Applications,** 1981	Mathematics of Physics
15	E. C. BELTRAMETTI and G. CASSINELLI **The Logic of Quantum Mechanics,** 1981	Mathematics of Physics
16	G. D. JAMES and A. KERBER **The Representation Theory of the Symmetric Group,** 1981	Algebra
17	M. LOTHAIRE **Combinatorics on Words,** 1982	Algebra

GIAN-CARLO ROTA, *Editor*
ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume		Section
18	H. O. FATTORINI **The Cauchy Problem,** 1983	Analysis
19	G. G. LORENTZ, K. JETTER, and S. D. RIEMENSCHNEIDER **Birkhoff Interpolation,** 1983	Interpolation and Approximation
20	RUDOLF LIDL and HARALD NIEDERREITER **Finite Fields,** 1983	Algebra
21	WILLIAM T. TUTTE **Graph Theory,** 1984	Combinatorics
22	JULIO R. BASTIDA **Field Extensions and Galois Theory,** 1984	Algebra
23	JOHN R. CANNON **The One-Dimensional Heat Equation,** 1984	Analysis

Other volumes in preparation

Editor's Statement

A large body of mathematics consists of facts that can be presented and described much like any other natural phenomenon. These facts, at times explicitly brought out as theorems, at other times concealed within a proof, make up most of the applications of mathematics, and are the most likely to survive change of style and of interest.

This ENCYCLOPEDIA will attempt to present the factual body of all mathematics. Clarity of exposition, accessibility to the non-specialist, and a thorough bibliography are required of each author. Volumes will appear in no particular order, but will be organized into sections, each one comprising a recognizable branch of present-day mathematics. Numbers of volumes and sections will be reconsidered as times and needs change.

It is hoped that this enterprise will make mathematics more widely used where it is needed, and more accessible in fields in which it can be applied but where it has not yet penetrated because of insufficient information.

GIAN-CARLO ROTA

Foreword

Galois theory is often cited as the beginning of modern "abstract" algebra. The ancient problem of the algebraic solution of polynomial equations culminated, through the work of Ruffini, Abel, and others, in the ideas of Galois, who set forth systematically the connection between polynomial equations and their associated groups. This was the beginning of the systematic study of group theory, nurtured by Cauchy and Jordan to its flowering at the end of the last century. It can also be viewed as the beginning of algebraic number theory (although here other forces were also clearly at work), developed later in the century by Dedekind, Kronecker, Kummer, and others. It is primarily this number-theoretic line of development that is pursued in this book, where the emphasis is on fields, and only secondarily on their groups.

In addition to these two specific outgrowths of Galois's ideas, there came something much broader, perhaps the essence of Galois theory: the systematically developed connection between two seemingly unrelated subjects, here the theory of fields and that of groups. More specifically, but in the same line, is the idea of studying a mathematical object by its group of automorphisms, an idea emphasized especially in Klein's Erlanger Program, which has since been accepted as a powerful tool in a great variety of mathematical disciplines.

Apart from the historical importance of the Galois theory of fields, its intrinsic interest and beauty, and its more or less direct applications to number theory, these many generalizations and their important applications give further compelling reasons for seeking an understanding of the theory in its classical form, as presented in this volume. The Galois theory of field extensions combines the esthetic appeal of a theory of nearly perfect beauty with the technical development and difficulty that reveal the depth of the theory and that make possible its great usefulness, primarily in algebraic number theory and related parts of algebraic geometry.

In this book Professor Bastida has set forth this classical theory, of field extensions and their Galois groups, with meticulous care and clarity. The treatment is self-contained, at a level accessible to a sufficiently well-motivated beginning graduate student, starting with the most elementary facts about fields and polynomials and proceeding painstakingly, never omitting precise definitions and illustrative examples and problems. The qualified reader will be able to progress rapidly, while securing a firm grasp of the fundamental concepts and of the important phenomena that arise in the theory of fields. Ultimately, the study of this book will provide an intuitively clear and logically exact familiarity with the basic facts of a comprehensive area in the theory of fields. The author has judiciously stopped short (except in exercises) of developing specialized topics important to the various applications of the theory, but we believe he has realized his aim of providing the reader with a sound foundation from which to embark on the study of these more specialized subjects.

This book, then, should serve first as an easily accessible and fully detailed exposition of the classical Galois theory of field extensions in its simplest and purest form; and second, as a solid foundation for and introduction to the study of more advanced topics involving the same concepts, especially in algebraic number theory and algebraic geometry.

We believe that Professor Bastida has offered the reader, for a minimum of effort, a direct path into an enchantingly beautiful and exceptionally useful subject.

ROGER LYNDON

Preface

Since its inception at the beginning of the nineteenth century, the theory of field extensions has been a very active area of algebra. Its vitality stems not only from the interesting problems generated by the theory itself, but also from its connections with number theory and algebraic geometry. In writing this book, our principal objective has been to make the general theory of field extensions accessible to any reader with a modest background in groups, rings, and vector spaces.

The book is divided into four chapters. In order to give a precise idea of the background that the reader is expected to possess, we have preceded the text by a section on prerequisites. Except for the initial remarks, in which we indicate the restrictions that will be imposed on the rings considered throughout our presentation, the reader should not be concerned with the contents of this section until explicit reference is made to them. The first chapter is devoted to the general facts on fields and polynomials required in the study of field extensions. Although most of these facts can be found in one or another of the references given in the section on prerequisites, we have attempted to facilitate the reader's task by having them collected and stated in a manner suitably adapted to our purposes.

The theory of field extensions is presented in the subsequent three chapters, which deal, respectively, with algebraic extensions, Galois theory, and transcendental extensions. The chapter on algebraic extensions is of basic importance for the entire theory, and has to be thoroughly understood before proceeding further. The last two chapters, on the other hand, can be read independently of each other.

Chapters are divided into sections, and each section ends with a set of problems. The problems include routine exercises, suggest alternative proofs of various results, or develop topics not discussed in the text. We have refrained from identifying the more difficult, and as a rule, no hints are given for the solutions. A result stated in a problem is not used in the text, but it may be required for the solution of a later problem.

The choice of material was dictated by the dual objective of providing thorough coverage of each topic treated and of keeping the length of the book within reasonable bounds. We decided to include in the text the results that constitute the core of the general theory of field extensions. Those parts of the theory sufficiently developed to merit a book of their own have been left out entirely, and several specialized topics of considerable interest have been relegated to the problems. We have not attempted to discuss any serious applications of our subject to number theory or algebraic geometry, since doing this would have required the introduction of additional background material. However, as the reader cannot fail to notice, connections with number theory manifest themselves occasionally in the presentation.

We have included bibliographical notes at the end of each chapter. These will provide the reader with references to the works in which important contributions were first published, with easily available references on topics presented as problems and on alternative treatments of topics covered in the text, and with suggestions for further reading.

The reference list at the end of the book comprises mainly the works cited in the text and notes. The vast literature on field extensions and Galois theory and on their applications to number theory and algebraic geometry cannot be surveyed, even superficially, within the confines of a few pages. To get a good idea of the present state of the literature, the reader may consult the pertinent sections of *Mathematical Reviews*, the review journal of the American Mathematical Society.

It is with the deepest gratitude and respect that we acknowledge the help given to us by Professor Harley Flanders, without which this book could not have been written. He read the manuscript and made very substantive suggestions on both content and style; offered us unrestricted access to his notes on field extensions; discussed proofs, examples, and problems with us; and never betrayed the slightest impatience in dealing with us during the four-year period that we worked on this book.

We would also like to express our sincere appreciation to Professor Gian-Carlo Rota, for his kind invitation to write a volume for the *Encyclo-*

pedia; to Professors Paul M. Cohn and Roger C. Lyndon, for their valuable suggestions; to Professors Tomás P. Schonbek and Scott H. Demsky, for their help with the bibliographical material; to my students Lynn Garrett and Jaleh Owliaei, for their comments; to Ruth Ebel and especially Rita Pelava, for their efficient typing; and to my colleagues at Florida Atlantic University, for their constant encouragement.

JULIO R. BASTIDA
Boca Raton, Florida

Historical Introduction

Problems of geometric construction appeared early in the history of mathematics. They were first considered by the Greek mathematicians of the fifth century B.C. Only two instruments—an unmarked ruler and a compass—were permitted in these constructions. Although many such constructions could be performed, others eluded the efforts of these mathematicians. Four famous problems from the period that remained unsolved for a long time are the following: doubling the cube, which consists of constructing a cube whose volume is twice that of a given cube; trisecting the angle; squaring the circle, which consists of constructing a square whose area is that of a given circle; and constructing regular polygons.

At the end of the eighteenth century, when it was observed that questions on geometric constructions can be translated into questions on fields, a breakthrough finally occurred. The 19-year-old Gauss [2: art. 365] proved in 1796 that the regular 17-sided polygon is constructible. A few years later, Gauss [2: art. 365, 366] stated necessary and sufficient conditions for the constructibility of the regular n-sided polygon. He gave a proof only of the sufficiency, and claimed to have a proof of the necessity; the latter was first given by Wantzel [1] in 1837. In his investigations, Gauss introduced and used a number of concepts that became of central importance in subsequent developments. A by-product of the works of Gauss and Wantzel on regular polygons was a proof that an arbitrary angle cannot be trisected. The proof of the impossibility of doubling the cube is more elementary, but its discovery is difficult to trace. As to the remaining problem, it was realized that the proof of the impossibility of squaring the circle depended on knowing that the number π is transcendental; this missing ingredient was supplied in 1882 by Lindemann [1], who used analytic techniques to settle one of the more fascinating questions in this area of mathematics.

The general theory of fields evolved during the last half of the nineteenth century, when the algebraists made significant advances in the study of algebraic numbers and algebraic functions. The first systematic exposition of the theory of algebraic numbers was given in 1871 by Dedekind [4]; in this work, Dedekind introduced the basic notions on fields, but restricted the field elements to complex numbers. As regards transcendental numbers, the early contributions were made by analysts. The most notable of these contributions were that by Liouville [1] in 1851, devoted to the construction of classes of transcendental numbers, and those by Hermite [2] in 1873 and Lindemann [1] in 1882, in which proofs are given of the transcendence of the numbers e and π, respectively. But it was not until 1882 that transcendentals made their appearance in the theory of fields, when Kronecker [2] succeeded in using the adjunction of indeterminates as the basis for a formulation of the theory of algebraic numbers. It was also in 1882 that fields of algebraic functions of complex variables were introduced by Dedekind and Weber [1] in order to lay the foundations of the arithmetical theory of algebraic functions. This work, in which a purely algebraic treatment of Riemann surfaces is given, marks the beginning of what was to become a very fruitful interplay between commutative algebra and algebraic geometry. It was next discovered in 1887 by Kronecker [3] that every algebraic number field can be obtained as the quotient of the polynomial domain $\mathbf{Q}[X]$ by the principal ideal generated by an irreducible polynomial, showing in effect that the theory of algebraic numbers does not require the use of complex numbers. Finally, the abstract definition of a field as we know it today was given in 1893 by Weber [1] in an article on the foundations of Galois theory. Weber also observed in this work that Kronecker's construction can be applied to arbitrary fields, and in particular to every field of integers modulo a prime; and that as a result, we recover the theory of higher congruences previously developed by Galois [2], Serret [1: 343–370], and Dedekind [2].

The final step toward the axiomatic foundations of the theory of fields was taken by Steinitz [1] in 1910. Spurred on by both the earlier contributions and the discovery by Hensel [1] of the p-adic fields, Steinitz set out to derive the consequences of Weber's axioms. His work, in which field extensions were first studied in full generality and in which normality, separability, and pure inseparability were introduced in order to give a detailed analysis of the structure of algebraic extensions, became the cornerstone in the development of abstract algebra. In the words of Artin and Schreier [1]: "E. Steinitz hat durch seine 'Algebraische Theorie der Körper' weite Gebiete der Algebra einer abstrakten Behandlungsweise erschlossen; seiner bahnbrechenden Untersuchung ist zum grossen Teil die starke Entwicklung zu danken, die seither die moderne Algebra genommen hat". It is in the closing pages of Steinitz's article that the theory of transcendental extensions was first presented. However, before this theory could be brought to its present state, two significant additions were yet to be made, both partially motivated by questions in algebraic geometry. In 1939, MacLane [1] introduced the notion of separability for transcendental extensions. This was then followed in 1946 by the treatise on the foundations of algebraic geometry by Weil [1], in which the abstract notion of derivation is introduced in the study of separability.

Galois theory is generally regarded as one of the central and most beautiful parts of algebra. Its creation marked the culmination of investigations by generations of mathematicians into one of the oldest problems in algebra, the solvability of polynomial equations by radicals. The familiar formula for the roots of the quadratic equation was essentially known to the Babylonian mathematicians of the twentieth century B.C. No significant progress was made on polynomial equations of higher degree until the sixteenth century, when del Ferro and Ferrari discovered the formulas for the cubic and quartic equations, respectively. These results were first published by Cardano [1] in 1545; it is probably for this reason that Cardano's name has been traditionally associated with the formulas for the cubic equation.

These formulas express the roots of the equations in terms of the coefficients, using exclusively the field operations and the extraction of roots. Attempts to find such formulas for polynomial equations of higher degree were unsuccessful; and partly as a consequence of the work of Lagrange [2; 3] in 1770–1772, the algebraists of the period came to believe that it was impossible to derive them. This was proved to be the case at the beginning of the nineteenth century. Several proofs were published by Ruffini [1] between 1799 and 1813, but they were incomplete. The first satisfactory proof was given by Abel [2] in 1826, three years before his tragic death before the age of 27; between 1826 and 1829 he obtained further results on the solvability of polynomial equations by radicals, which were published in Abel [3; 1: II, 217–243, 269–270, 271–279].

The contributions of Ruffini and Abel were followed by the decisive results of Galois [1: 25–61] in 1832. Galois proved that the solvability of a polynomial equation by radicals is equivalent to a special property of a group naturally associated with the equation. Galois made this discovery before the age of 20, at a time when abstract algebra virtually did not exist!

Although Galois's result on the solvability of polynomial equations by radicals settled a problem that had eluded the efforts of some of the greatest mathematicians of earlier generations, later developments have shown that the ideas introduced by Galois in his solution surpass by far the importance of the problem that he originally set out to solve. First, Galois defined and used the group-theoretical properties of normality, simplicity, and solvability, which play a significant role in the theory of groups. Moreover, he solved a problem of fields by translating it into a more tractable problem on groups; in so doing, he probably made the earliest application of a method that has become pervasive in algebra, namely, that of studying a mathematical object by suitably relating it to a mathematical object with a simpler structure. Nor is it an exaggeration to say that Galois theory is a prerequisite for much current research in number theory and algebraic geometry.

The story of Galois's life is a topic of considerable controversy. A gifted mathematician who is killed in a duel at the age of 20 presents unlimited opportunities for the creation of a myth. Unfortunately, this is precisely what several well-known authors have done in their writings on Galois. By means of intentional or unintentional omissions and distortions, legends have been created in which Galois is portrayed as a struggling genius unappreciated not only by the general public, but also by some of the leading mathematicians of his time. The recent article by Rothman [1] offers a lively account of such theories, as well as a careful attempt to unravel them.

Galois's ideas were expressed originally within the context of the theory of equations: To each polynomial equation is assigned a group of permutations of its roots. The progress made toward the axiomatic foundations of algebra in the last part of the nineteenth century had a considerable impact on Galois theory. Dedekind [4] observed that a more natural setting for Galois theory is obtained by regarding the groups associated with polynomial equations as groups of automorphisms of the corresponding splitting fields. Furthermore, he pioneered the systematic use of linear algebra in Galois theory. Since the abstract theory of field extensions was not developed until the first decade of the present century, Dedekind had to restrict his considerations to special types of fields. That his formulation of Galois theory remains meaningful for arbitrary fields was shown subsequently by the works of Weber [1] in 1893, of Steinitz [1] in 1910, and of Artin [3] in 1942. It is to these algebraists, and especially to Artin, that we owe what is now considered to be the definitive exposition of the Galois theory of finite groups of field automorphisms. A further contribution that must be mentioned is the generalization of the principal results of this theory to a special type of infinite groups of field automorphisms, discovered by Krull [1] in 1928.

Prerequisites

We shall assume that the reader possesses a certain familiarity with the rudiments of abstract algebra. More specifically, in addition to the basic properties of integers, sets, and mappings, the reader is expected to know the elementary parts of the theory of groups and the theory of rings, and to possess a reasonable background in linear algebra. Suggested references on these prerequisites are the following.

1. Adamson, I. T. *Elementary Rings and Modules*. New York: Harper & Row, 1972.
2. Godement, R. *Cours d'Algèbre*. Paris: Hermann, 1963. (English translation: *Algebra*. New York: Houghton Mifflin, 1968.)
3. Halmos, P. R. *Naive Set Theory*. New York: Springer-Verlag, 1974.
4. Hoffman, K., and Kunze, R. *Linear Algebra*. Englewood Cliffs, NJ: Prentice-Hall, 1971.
5. Ledermann, W. *Introduction to Group Theory*. Edinburgh: Oliver & Boyd, 1973.
6. Rotman, J. J. *The Theory of Groups, an Introduction*. Boston: Allyn & Bacon, 1973.

This list is not intended as an exhaustive bibliography on the basic concepts of algebra. We have simply selected six easily accessible books that, for our purposes, are particularly suitable as references. The books [1] and [2] seem the most convenient: In the first place, we shall adhere almost