

Springer Monographs in Mathematics

Helmut Koch

Galois Theory of p -Extensions



Springer

Helmut Koch

Humboldt-Universität Berlin
Institut für Mathematik
Unter den Linden 6
10117 Berlin
Germany

Translator

Franz Lemmermeyer
California State University San Marcos
Department of Mathematics
333 South Twin Oaks Valley Rd.
92096-0001 San Marcos, CA
USA
e-mail: franzl@csusm.edu

Catalog-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Koch, Helmut: Galois theory of p -extensions / Helmut Koch.
ISBN 978-3-642-07817-0 ISBN 978-3-662-04967-9 (eBook)
DOI 10.1007/978-3-662-04967-9

Mathematics Subject Classification (2000): 11R34, 11-02

ISBN 978-3-642-07817-0

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag Berlin Heidelberg GmbH.
Violations are liable for prosecution under the German Copyright Law.

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Originally published by Springer-Verlag Berlin Heidelberg New York in 2002
Softcover reprint of the hardcover 1st edition 2002

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typeset in \TeX by the Translator
Cover production: Erich Kirchner, Heidelberg

SPIN 10868507 44/3142db - 5 4 3 2 1 0 - Printed on acid-free paper

Foreword

This book deals with a quite young area of algebraic number theory: the algebraic theory of p -extensions, which was developed in the last 25 years and has now reached a degree of completion that makes a systematic presentation highly desirable.

This area of arithmetic deals with the theory of finite extensions of fields of arithmetic type. These are p -adic number fields, fields of formal power series with finite fields of constants, algebraic number fields and algebraic function fields of one variable with finite fields of constants. The main goal is obtaining information beyond what is provided by classical class field theory, which – as is well known – describes the extensions with commutative Galois group. The commutativity of the Galois group is very essential here. Class field theory is thereby closely connected with a wide circle of mathematical ideas ranging from the theory of radical extensions (nowadays called Kummer theory) to topological duality theorems, the theory of abelian and harmonic integrals and Picard varieties. The group-theoretical foundation of all these questions is the Pontryagin duality of abelian groups and their character groups. It is this part of mathematics that A. Weil has called “abelian mathematics”.

As is well known, when Hilbert started building class field theory, he was led by the analogy between algebraic number fields and function fields, i.e., the field of meromorphic functions on compact Riemann surfaces. From this point of view, any “nonabelian” generalization of class field theory has to correspond to the investigation of the fundamental group of Riemann surfaces.

It has turned out that building a theory extending beyond the frame of class field theory is possible for extensions whose Galois group is nilpotent (or, what amounts to the same, a p -group). As in the study of the fundamental group in topology, it emerged that the groups of interest here have a natural presentation in terms of generators and relations, which clarifies essential parts of their structure. These investigations are contained in this book. Although the theory presented here is far from dealing with the general case of finite groups, it leads to the solution of many number-theoretic problems. For example, the theory says a lot about the structure of *all* extensions of a p -adic number field or of the field of formal power series over a finite field of constants. This theory also leads to the solution of the class field

tower problem and of the problem connected with it, the growth of minimal discriminants of algebraic number fields.

At the same time I would like to stress that we are dealing here with a theory that is not yet complete. On the contrary, several extremely interesting problems remain unsolved. Examples of such questions are the following: a concrete description of the Galois group of the algebraic closure of a p -adic number field (e.g. including the ramification groups), the existence of extension fields of the rational number field with given (nonsolvable) Galois group, and the integrality of L -series for Artin characters different from the trivial character.

I am convinced that this book is of interest to a large circle of mathematicians. On the one hand, it is accessible to nonexperts and leads the reader quickly into a new area of investigation that contains a wealth of problems awaiting solution. On the other hand, the book contains almost all the basic material pertaining to this area as well as many new results by the author that will be of interest to the experts. The author's papers are among the most interesting results in this direction and have contributed essentially to the reputation that this area of mathematics has nowadays.

I hope that this book by H. Koch will stimulate the further development of this direction in algebraic number theory.

Moscow, December 1969

I.R. Shafarevich

Preface for the English Translation

There are a number of reasons why an English translation of this book appears more than 30 years after its publication.

1. It is very hard to find a copy of this book even from used book stores. On the other hand, it is still in demand since the subject has not been included in textbooks.

2. This book demonstrates that the cohomology of groups is very useful for studying Galois theory of number fields; at the same time, it offers a down to earth introduction to the cohomological method. Thus it may be read in parallel to Serre's classical lectures *Cohomologie Galoisienne* first published in the Springer Lecture Notes Series in 1964, and whose English translation appeared in 2000.

3. Another book published in 2000 is the encyclopedic [NSW] by J. Neukirch, A. Schmidt and K. Wingberg, where the results presented in this book are discussed only marginally. For example, the authors refer to the German original of this book for the improved version of the Golod-Shafarevich inequality. On the other hand, [NSW] contains new results on the Galois theory of p -extensions, in particular in connection with maximal p -extensions unramified outside of a set S of primes containing the primes dividing p . The present book, on the other hand, concentrates on extensions in which primes dividing p may be unramified.

Berlin, autumn 2001

H. Koch

Note by the Translator

It is my pleasure to thank Linda Holt for her comments, Farshid Hajir for suggesting the translation in the first place and for his contribution to the postscript, Wayne Aitken for corrections and explanations, Richard Hill, Hendrik Lenstra, Akito Nomura, Peter Pleasant and an unknown referee for lists of typos and errors, and Helmut Koch for his help in preparing this translation.

San Marcos, spring 2002

F. Lemmermeyer

Preface of the German Edition

The main objective of this book is a consistent presentation of results by I.R. Shafarevich, A. Fröhlich, A. Brumer and the author on the Galois theory of p -extensions on the basis of Galois cohomology. In order to make these results accessible to a wider circle of mathematicians with algebraic interests, prerequisites are restricted to knowledge of basic facts from algebra, group theory, and algebraic number theory as they are readily available in standard textbooks.

The first seven chapters of this book deal with cohomology of profinite groups, in particular of pro- p -groups. It goes without saying that the first chapter of Serre's *Cohomologie Galoisienne* served as a blueprint. Some chapters of this part may be seen as a commentary on Serre's lectures. The rest of the book deals with field theory. The theorems of class field theory that we need are stated explicitly and may be accepted axiomatically by the readers. There exist, by the way, at least two easily accessible presentations of class field theory in the style and extent in which we will need it, namely J.W.S. Cassels and A. Fröhlich [8] as well as J. Neukirch [46].

Some of the results of this book I found during a one-year stay in 1967/68 as a researcher at the Steklov Institute for Mathematics of the Academy of Science of the USSR. I would like to express my heartfelt gratitude to the Steklov Institute and in particular to Prof. I.R. Shafarevich for the invitation. I.R. Shafarevich's influence on this book is much larger, though: it goes back to my first stay in Moscow in 1960/61 as a student, which was followed by numerous inspiring and stimulating conversations.

I would like to thank the editors, in particular Prof. Dr. H. Reichardt, for including this book into the series "Mathematische Monographien". Moreover I thank Prof. Dr. H. Reichardt and the members of the number theory research group of the Institute for Pure Mathematics at the German Academy of Science in Berlin, namely Dr. O. Neumann, W. Thor, H. Pieper, and W. Zink, who have read parts of the manuscript and suggested improvements and corrections. I thank the VEB Deutscher Verlag der Wissenschaften, in particular the copy editors L. Boll and Miss E. Arndt, for their exemplary and expert work on the manuscript, which has contributed essentially to the success of this publication.

Contents

Introduction	1
1. Profinite Groups	3
1.1 Projective Limits of Groups and Rings	3
1.2 Profinite Groups	7
1.3 Subgroups and Quotient Groups	9
1.4 Abelian Profinite Groups, Pontryagin's Duality Theory	10
1.5 Discrete Modules	10
1.6 The Category \mathcal{C}	12
1.7 Inductive Limits in \mathcal{C}	13
2. Galois Theory of Infinite Algebraic Extensions	17
2.1 The Galois Group of Infinite Extensions	17
2.2 The Main Theorem of Galois Theory	19
3. Cohomology of Profinite Groups	21
3.1 Definition of Cohomology Groups	21
3.2 Group Extensions	24
3.3 Dimension Shifting	24
3.4 Shapiro's Lemma	28
3.5 Restriction and Corestriction	28
3.6 The Transfer	29
3.7 Inflation and Transgression	30
3.8 Inductive Limits of Cohomology Groups	35
3.9 Cup Products	37
4. Free pro-p Groups	41
4.1 Construction of Free pro- p Groups	41
4.2 The Magnus Group Algebra	42
4.3 Abelian pro- p Groups	43
4.4 First Characterization of Free pro- p Groups	44
4.5 Second Characterization of Free pro- p Groups	47

5. Cohomological Dimension	49
5.1 Definition of Cohomological Dimension	49
5.2 Euler-Poincaré Characteristic	50
6. Presentation of pro-p Groups	53
6.1 The Generator Rank	53
6.2 Relation Systems	54
7. Group Algebras of pro-p Groups	59
7.1 Complete Group Algebras	59
7.2 Discrete and Compact G -Modules	60
7.3 Pro- p Groups of Dimension ≤ 2	61
7.4 Filtrations	64
7.5 Computing with Commutators and Powers	66
7.6 Group Rings of Free pro- p Groups	68
7.7 The Theorem of Golod-Shafarevich	69
7.8 Relation Structure and Cup Product	72
8. Results from Algebraic Number Theory	77
8.1 Algebraic Number Theory for Infinite Extensions	77
8.2 Normal Extensions	77
8.3 The Frobenius Automorphism	79
8.4 Local and Global Fields	79
8.5 The Multiplicative Group of a Local Field	81
8.6 Finite Class Field Theory	82
8.7 Infinite Class Field Theory	84
8.8 The Principal Ideal Theorem	85
8.9 Cohomology of the Formation Module	87
8.10 Cohomology of the Multiplicative Group	89
8.11 Norm Residue Symbol	90
9. The Maximal p-Extension	93
9.1 Fields of Characteristic p	93
9.2 Fields Containing the p -th Roots of Unity	94
9.3 Fields not Containing the p -th Roots of Unity	96
10. Local Fields of Finite Type	99
10.1 The Case $\chi(\mathfrak{p}) \neq p$	99
10.2 The Case $\chi(\mathfrak{p}) = p, \delta(k) = 0$	101
10.3 The Case $\chi(\mathfrak{p}) = p, \delta(k) = 1$	103
11. Global Fields of Finite Type	111
11.1 The Maximal p -Extension	111
11.2 The Maximal p -Extension with Restricted Ramification	114
11.3 Generator Rank	119

11.4	Explicit Computation of Generators and Relations	122
11.5	The Structure of G_S in Special Cases	129
12.	On p-Class Groups and p-Class Field Towers	133
12.1	A Criterion for Class Number Prime to p	133
12.2	The p -Class Field Tower of Cyclic Extensions of Degree p	136
12.3	A Criterion for Infinite Class Field Towers	144
13.	The Cohomological Dimension of G_S	149
13.1	Cohomology of S -Unit Groups	149
13.2	The Case $\delta(k) = 1$	154
13.3	The Case $\delta(k) = 0$	157
	References	163
	Bibliography	167
	Notation	173
	Postscript	175
	Additional References	181
	Author Index	187
	Subject Index	189