Lecture Notes in Mathematics 1534

Cornelius Greither

Cyclic Galois Extensions of Commutative Rings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Author

Cornelius Greither
Mathematisches Institut
der Universität München
Theresienstr. 39
W-8000 München 2, Germany

Mathematics Subject Classification (1991): 11R18, 11R23, 11R33, 11S15, 13B05, 13B15, 14E20

ISBN 3-540-56350-4 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56350-4 Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author
46/3140-543210 - Printed on acid-free paper

CONTENTS

Für Liane und für Margarete.

INTRODUCTION

The subject of these notes is a part of commutative algebra, and is also closely related to certain topics in algebraic number theory and algebraic geometry. The basic problems in Galois theory of commutative rings are the following: What is the correct definition of a Galois extension? What are their general properties (in particular, in comparison with the field case)? And the most fruitful question in our opinion: Given a commutative ring R and a finite abelian group G, is there any possibility of describing *all* Galois extensions of R with group G?

These questions will be dealt with in considerable generality. In later chapters, we shall then apply the results in number-theoretical and geometrical situations, which means that we consider more special commutative rings: rings of integers and rings of functions. Now algebraic number theory as well as algebraic geometry have their own refined methods to deal with Galois extensions: in number theory one should name class field theory for instance. Thus, the methods of the general theory for Galois extensions of rings are always in competition with the more special methods of the discipline where they are applied. It is hoped the reader will get a feeling that the general methods sometimes also lead to new results and provide an interesting approach to old ones.

Let us briefly review the development of the subject. Hasse (1949) seems to have been the first to consider the totality of G-Galois extensions L of a given number field K. He realized that for finite abelian G this set admits a natural abelian group structure, *if* one also admits certain "degenerate" extensions L/K which are not fields. For example, the neutral element of this group is the direct product of copies of K, with index set G. This constitutes the first fundamental idea. The second idea, initiated by Auslander and Goldman (1960) and then brought to perfection by Chase, Harrison, and Rosenberg (1965), is to admit base rings R instead of fields. It is not so obvious what the definition of a G-Galois extension S/R of commutative rings should be, but once one has a good definition (by the way, all good definitions turn out to be equivalent), then one also obtains nice functoriality properties, stability under base change for instance, and the theory runs almost as smoothly as for fields. Harrison (1965) put the two ideas together and defined, for G finite abelian, the *group* of all G-Galois extensions of a given commutative ring R modulo G-isomorphism. This group is now called the *Harrison group*, and we denote it by $\mathrm{H}(R,G)$. Building on the general theory of Chase, Harrison, and Rosenberg, and developing some new tools, we calculate in these notes the group $\mathrm{H}(R,G)$ in a fairly general setting.

The principal link between this theory and number theory is the study of ramification. Suppose L is a G-Galois extension of the number field K, Σ a set of finite places of K, and $R = \mathcal{O}_{K,\Sigma}$ the ring of Σ-integers in K. Then the integral closure S of R in L is with the given G-action a G-Galois extension of R if and only if L/K is at most ramified in places which belong to Σ. In most applications, Σ will be the set of places over p. The reason for this choice will become apparent when we discuss $\mathbb{Z}_p$-extensions below.

We now discuss the contents of these notes in a little more detail.

After a summary of Galois theory of rings in Chap. 0, which also explains the connection with number theory, and $\mathbb{Z}_p$-extensions, we develop in Chap. I a *structure theory* for Galois extensions with cyclic group $G = C_{p^n}$ of order p^n, under the hypothesis that $p^{-1} \in R$ and p is an odd prime number. For technical reasons, we also suppose that R has no nontrivial idempotents. Since the Harrison group $H(R, G)$ is functorial in both arguments, and preserves products in the right argument, this also gives a structure theory for the case G finite abelian, $|G|^{-1} \in R$.

The basic idea is simple. If R contains a primitive p^n-th root of unity ζ_n (this notion has to be defined, of course), and $p^{-1} \in R$, then Kummer theory is available for C_{p^n}-extensions of R. The statements of Kummer theory are, however, more complicated than in the field case: it is no longer true that every C_{p^n}-extension S/R can be gotten by "extracting the p^n-th root of a unit of R", but the obstruction is under control. The procedure is now to adjoin ζ_n to R somehow (it is a lot of work to make this precise), use Kummer theory for the ring S_n obtained in this way, and descend again. Here a very important concept makes its appearance. A G-Galois extension S/R is defined to have *normal basis*, if S has an R-basis of the form $\{\gamma(x) \mid \gamma \in G\}$ for some $x \in S$. Fo $G = C_{p^n}$, the extensions with normal basis make up a *subgroup* $NB(R, C_{p^n})$ of $H(R, C_{p^n})$. In Chap. I we prove rather precise results on the structure of $NB(R, C_{p^n})$, and of $H(R, C_{p^n})/NB(R, C_{p^n})$. In the field case, the latter group is trivial, but not in general. Kersten and Michaličk (1988) were the first to prove results for $NB(R, C_{p^n})$. Our result says that $NB(R, C_{p^n})$ is "almost" isomorphic to an explicitly given subgroup of $S_n^*/(p^n\text{-th powers})$, and $H(R, C_{p^n})/NB(R, C_{p^n})$ is isomorphic to an explicitly given subgroup of the Picard group of S_n. The description of $NB(R, C_{p^n})$ is basic for the calculations in Chap. III and V.

In Chap. II we treat corestriction and a result of type "Hilbert 90". This amounts to the following: We get another description of $NB(R, C_{p^n})$, this time as a *factor* group of $S_n^*/(p^n\text{-th powers})$. This is sometimes more practical, as witnessed by the *lifting theorems* which conclude Chap. II: If I is an ideal of R, contained in the Jacobson radical of R, then every C_{p^n}-extension S of R/I with normal basis is of the form $S = T/IT$, $T \in NB(R, C_{p^n})$.

In Chap. III we set out to calculate the order of $\mathrm{NB}(R, C_{p^n})$, where now $R = \mathcal{O}_K[p^{-1}]$, K a number field. Although one almost never knows the groups S_n^* explicitly, which are closely related to the group of units in the ring of integers of $K(\zeta_n)$, one can nevertheless do the calculation one wants, by dint of some tricks involving a little cohomology of groups. All this is presented in a quite elementary way. We demonstrate the strength of the method by deducing the Galois theory of finite fields, and a piece of local class field theory. The main result for number fields K is that with R as above, and n not "too small", the order of $\mathrm{NB}(R, C_{p^n})$ equals $\mathrm{const} \cdot p^{(1+r_2)n}$, where r_2 is half the number of nonreal embeddings $K \to \mathbb{C}$ as usual.

The goal of Chap. IV is to get an understanding, how far the subgroup $\mathrm{NB}(R, C_{p^n})$ differs from $\mathrm{H}(R, C_{p^n})$, and a similar question for $\mathbb{Z}_p$ in the place of C_{p^n}. Here $\mathrm{H}(R, \mathbb{Z}_p)$ is the group of $\mathbb{Z}_p$-extensions of R. A $\mathbb{Z}_p$-extension is basically a tower of C_{p^n}-extensions, $n \to \infty$. It is known that all $\mathbb{Z}_p$-extensions of K are unramified outside p, and hence already a $\mathbb{Z}_p$-extensions of R, which justifies the choice of the ring R.

We prove in IV §2: $\mathrm{NB}(R, \mathbb{Z}_p) \simeq \mathbb{Z}_p^{1+r_2}$. This was previously proved in a special case by Kersten and Michaličeк (1989). The result is what one expects from the formula for $|\mathrm{NB}(R, C_{p^n})|$, but the passage to the limit presents some subtleties. The index $q_n = [\mathrm{H}(R, C_{p^n}) : \mathrm{NB}(R, C_{p^n})]$ is studied in some detail, and we show that q_n either goes to infinity or is eventually constant for $n \to \infty$. The first case conjecturally never happens: we prove that this case obtains if and only the famous Leopoldt conjecture fails for K and p. Another way of saying this is as follows: $\mathrm{NB}(R, \mathbb{Z}_p)$ has finite index in $\mathrm{H}(R, \mathbb{Z}_p)$ if and only if the Leopoldt conjecture is true for K and p. We give results about the actual value of that index; in particular, it can be different from 1.

Apart from adjoining roots of unity, there is so far only other explicit way of generating large abelian extensions of a number field K, namely, adjoining torsion points on abelian varieties with complex multiplication. We show in IV §5 that $\mathbb{Z}_p$-extensions obtained in that way tend to have normal bases over $R = \mathcal{O}_K[p^{-1}]$, and a weak converse to this statement. These results are in tune with the much more explicit results of Cassou-Noguès and Taylor (1986) for elliptic curves.

There is a change of scenario in Chap. V. There we consider function fields of varieties over number fields. Such function fields are also called *absolutely finitely generated fields over* $\mathbb{Q}$. After some prerequisites from algebraic geometry, we show a relative finiteness result on C_{p^n}-Galois coverings of such varieties, which is similar to results of Katz and Lang (1981), and we prove that *all* $\mathbb{Z}_p$-extensions of an absolutely finitely generated field K already come from the greatest number field k contained in K. In other words: for number fields k one does not know how

many independent $\mathbb{Z}_p$-extensions k has, unless Leopoldt's conjecture is known to be true for K and p, but in a geometric situation, no new $\mathbb{Z}_p$-extensions arise.

The last chapter (Chap. VI) proposes a structure theory for Galois extensions with group C_{p^n}, in case the ground ring R contains a primitive p^n-th root of unity ζ_n but not necessarily $p^{-1} \in R$. It is assumed, however, that p does not divide zero in R. Even though Kummer theory fails for R, we may still associate to many C_{p^n}-extensions S/R a class $\varphi_n(S) = [u]$ in R^* mod p^n-th powers. If R is normal, S will be the integral closure of R in $R[p^{-1}, \sqrt[p^n]{u}]$. The main question is: Which units $u \in R^*$ may occur here? In §2 we essentially perform a reduction to the case R p-adically complete. Taking up a paper of Hasse (1936), we then answer our question by using so-called Artin-Hasse exponentials. It turns out that the admissible values u are precisely the values of certain universal polynomials, with parameters running over R. Reduction mod p also plays an essential role, and for this reason we have to review Galois theory in characteristic p in §1. In the final §6 the descent technique of Chap. I comes back into play. In §4-5 a "generic" C_{p^n}-extension of a certain universal p-complete ring containing ζ_n (but not p^{-1}) was constructed, and we are now able to see in detail how this extension descends down to a similar ground ring without ζ_n, to wit: the p-adic completion of $\mathbb{Z}[X]$. This extension is, roughly speaking, a prototype of C_{p^n}-extensions of p-adically complete rings. All this is in principle calculable.

Most chapters begin with a short overview of their contents. Cross references are indicated in the usual style: the chapters are numbered **0**, I, II, ..., VI, and a reference number not containing **0** or a Roman numeral means a reference within the same chapter. *All rings are supposed commutative* (except, occasionally, an endomorphism ring), and with unity. Other conventions are stated where needed.

Earlier versions of certain parts of these notes are contained in the journal articles Greither (1989), (1991).

It is my pleasurable duty to thank my colleagues who have helped to improve the contents of these notes. Ina Kersten has influenced the presentation of earlier versions in many ways and provided valuable information. Also, the helpful and detailed remarks of several referees are appreciated; I like to think that their suggestions have resulted in a better organization of the notes. Finally, I am grateful for written and oral communications to S. Ullom, G. Malle, G. Janelidze, and T. Nguyen Quang Do.