Lecture Notes in Mathematics

1534

Cornelius Greither

Cyclic Galois Extensions of Commutative Rings

Springer-Verlag

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 $\mathrm{H}(R, G)$ 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* $\mathrm{NB}(R, C_{p^n})$ of $\mathrm{H}(R, C_{p^n})$. In Chap. I we prove rather precise results on the structure of $\mathrm{NB}(R, C_{p^n})$, and of $\mathrm{H}(R, C_{p^n})/\mathrm{NB}(R, C_{p^n})$. In the field case, the latter group is trivial, but not in general. Kersten and Michaliček (1988) were the first to prove results for $\mathrm{NB}(R, C_{p^n})$. Our result says that $\mathrm{NB}(R, C_{p^n})$ is "almost" isomorphic to an explicitly given subgroup of $S_n^*/(p^n$-th powers), and $\mathrm{H}(R, C_{p^n})/\mathrm{NB}(R, C_{p^n})$ is isomorphic to an explicitly given subgroup of the Picard group of S_n. The description of $\mathrm{NB}(R, C_{p^n})$ 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 $\mathrm{NB}(R, C_{p^n})$, this time as a *factor* group of $S_n^*/(p^n$-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 $S \cong T/IT$, $T \in \mathrm{NB}(R, C_{p^n})$.

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 $\text{const}\cdot p^{(1+r_2)n}$, 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: $\mathrm{NB}(R, \mathbb{Z}_p) \cong \mathbb{Z}_p^{1+r_2}$. This was previously proved in a special case by Kersten and Michaliček (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.

CONTENTS

Introduction *vii*

Chapter 0: Galois theory of commutative rings

§1 Definitions and basic properties 1
§2 The main theorem of Galois theory 6
§3 Functoriality and the Harrison product 8
§4 Ramification 17
§5 Kummer theory and Artin-Schreier theory 19
§6 Normal bases and Galois module structure 25
§7 Galois descent 28
§8 $\mathbb{Z}_p$-extensions 30

Chapter I: Cyclotomic descent

§1 Cyclotomic extensions 32
§2 Descent of normal bases 38
§3 Cyclotomic descent: the main theorems 45

Chapter II: Corestriction and "Hilbert's Theorem 90"

§1 Corestriction 55
§2 Lemmas on group cohomology 60
§3 "Hilbert 90": the kernel and image of the corestriction 62
§4 Lifting theorems 64

Chapter III: Calculations with units

§1 Results on twisted Galois modules 67
§2 Finite fields and ℓ-adic fields 70
§3 Number fields 73

Chapter IV: Cyclic p-extensions and $\mathbb{Z}_p$-extensions of number fields

§1 C_{p^n}-extensions and ramification 77
§2 $\mathbb{Z}_p$-extensions 79
§3 The asymptotic order of $\mathrm{P}(R, C_{p^n})$ 83
§4 Calculation of q_K: examples 88
§5 Torsion points on abelian varieties with complex multiplication 91
§6 Further results: a short survey 95

Chapter V: Geometric theory: Cyclic extensions of finitely generated fields

§1 Geometric prerequisites 97

§2 $\mathbb{Z}_p$-extensions of absolutely finitely generated fields 101

§3 A finiteness result 106

Chapter VI: Cyclic Galois theory without the condition "$p^{-1} \in R$"

§1 Witt rings and Artin-Schreier theory for rings of characteristic p 109

§2 Patching results 113

§3 Kummer theory without the condition "$p^{-1} \in R$" 116

§4 The main result and Artin-Hasse exponentials 120

§5 Proofs and examples 126

§6 Application: Generic Galois extensions 135

References 140

Index 144

CHAPTER 0

Galois theory of commutative rings

§1 Definitions and basic properties

The study of Galois extensions of commutative rings was initiated by Auslander and Goldman (1960) and developed by Chase, Harrison, and Rosenberg (1965). In this section we shall try to present the basics of this theory. Occasionally we refer to the paper of Chase, Harrison, and Rosenberg for a proof. Almost everything we say in this section is can be found there, or in the companion paper Harrison (1965), sometimes with proofs which differ from ours.

Let G be a finite group, $K \subset L$ a field extension. Then, as everybody agrees, L/K is a Galois extension with group G if and only if:

G is a subgroup of $\mathrm{Aut}(L/K)$, the group of automorphisms of L which fix all elements of K; and

$K = L^G$, the field of all elements of L which are fixed by every automorphism in G.

A literal translation of this definition would result in a too weak definition in the framework of commutative rings, for many reasons. Let us not pursue this, but rather point out two alternative definitions of "Galois extension" in the field case which turn out to generalize well, and which indeed give equivalent generalizations. Thus, we will have found the "correct" notion of a Galois extension of commutative rings. Suppose that G is a finite group which acts on L by automorphisms which fix all elements of K. We thus have a group homomorphism $G \to \mathrm{Aut}(L/K)$.

Definition 1.1. The K-algebra $L * G$ is the L-vectorspace $\bigoplus_{\sigma \in G} L u_\sigma$ (the u_σ are just formal symbols), with multiplication given by $(\lambda u_\sigma)(\mu u_\tau) = \lambda \cdot \sigma(\mu) \cdot u_{\sigma\tau}$ $(\lambda, \mu \in L)$. The map j: $L * G \to \mathrm{End}_K(L)$ is given by

$$j(\lambda u_\sigma) = (\mu \longmapsto \lambda \cdot \sigma(\mu)) \in \mathrm{End}_K(L).$$

Proposition 1.2. *j is a well-defined K-algebra homomorphism, which is bijective iff G is embedded in* $\mathrm{Aut}(L/K)$ *and L/K is a G-Galois extension.*

Proof. The first statement is easy to check. Assume $G \subset \mathrm{Aut}(L/K)$ and L/K is G-Galois. Then by Dedekind's Lemma the elements σ of G are L-left linearly independent in $\mathrm{End}_K(L)$, hence j is a monomorphism. Since $\dim_K(L * G) = [L:K]^2 = \dim_K \mathrm{End}_K(L)$, j is bijective.

If $G \to \mathrm{Aut}(L/K)$ is not injective, then there exist $\sigma \neq \tau$ in G with $j(\sigma) = j(\tau)$, i.e. j cannot be monic. If G embeds into $\mathrm{Aut}(L/K)$ but L/K fails to be G-Galois, then there exists $x \in L \setminus K$ fixed under G. A short calculation shows then that l_x = (left multiplication by x) commutes with $\mathrm{Im}(j) \subset \mathrm{End}_K(L)$. If j were surjective, we would have l_x in the center of $\mathrm{End}_K(L)$, i.e. $x \in K$, contradiction.

Definition 1.3. The K-algebra $L^{(G)}$ is defined to be the set of all maps $G \to L$, endowed with the obvious addition and multiplication. (Note that L^G, without brackets, denotes a fixed field.) Let h: $L \otimes_K L \longrightarrow L^{(G)}$ be defined by $h(x \otimes y) = (x \cdot \sigma(y))_{\sigma \in G}$.

Proposition 1.4. *The map h is a L-algebra homomorphism (here L operates on the left factor of $L \otimes_K L$), and h is bijective iff G embeds into* $\mathrm{End}_K(L)$ *and L/K is G-Galois.*

Proof. The first statement is obvious. Pick a K-basis $y_1, \ldots, y_n$ of L. Then $1 \otimes y_1, \ldots, 1 \otimes y_n$ is an L-basis of $L \otimes_K L$. Thus we see that h is bijective iff the matrix $(\sigma(y_i))_{\sigma \in G, 1 \leq i \leq n}$ has full rank (note that this is indeed a square matrix). The latter condition says that the images of all $\sigma \in G$ are L-left linearly independent in $\mathrm{End}_K(L)$, or (what is the same) that the map j of 1.1 is injective. Hence 1.4 follows from 1.2.

Motivated by these descriptions of Galois field extensions, we define for any finite group G:

Definition 1.5. An extension $R \subset S$ of commutative rings is a G-*Galois extension*, if G is a subgroup of $\mathrm{Aut}(S/R) = \{\varphi: S \to S \mid \varphi\ R\text{-algebra automorphism}\}$, such that $R = S^G$ (fixed ring under G), and the map h: $S \otimes_R S \longrightarrow S^{(G)}$, $h(x \otimes y) = (x\sigma(y))_{\sigma \in G}$ exactly as in 1.3, is bijective, or (what is the same) an S-algebra isomorphism.

Examples: a) Galois extensions of fields are obviously a special case.

b) For any commutative ring R we have the *trivial G-extension* $S = R^{(G)}$ which is defined as follows: The algebra $R^{(G)}$ is again just $\mathrm{Map}(G, R)$ with the canonical R-algebra structure, and the action of G is given by index shift:

$$\sigma\big((x_\tau)_{\tau \in G}\big) = (x_{\tau\sigma})_{\tau \in G} \quad \text{for } \sigma \in G,\ (x_\tau)_{\tau \in G} \in R^{(G)}.$$

It is an easy exercise to prove that in this case indeed $S^G = R$ and h is bijective. We shall see more examples below.

There exist plenty of other definitions, or rather characterizations, of G-Galois extensions of commutative rings. Some of them are listed in the next theorem:

Theorem 1.6. [Chase-Harrison-Rosenberg (1965), Thm. 1.3]: *Let $R \subset S$ be commutative rings, $G \subset$* $\mathrm{Aut}(S/R)$ *a finite subgroup such that $S^G = R$. Then the following conditions are equivalent*:

(*i*) *S/R is G-Galois (i.e. per def.: h: $S \otimes_R S \longrightarrow S^{(G)}$ is bijective)*;

(*ii*) *h: $S \otimes_R S \longrightarrow S^{(G)}$ is surjective*;

(iii) S is a finitely generated projective R-module, and the map j: $S * G \to \mathrm{End}_R(S)$ (defined as in 1.1) is bijective;

(iv) For any $\sigma \in G\backslash\{e_G\}$ and any maximal ideal $M \subset S$, there exists $y \in S$ with $\sigma(y) - y$ not in M.

Proof. Let us first reformulate condition *(ii)*. One sees easily that h is compatible with the G-action, where G acts naturally on the second factor of $S \otimes_R S$, and by index shift on $S^{(G)}$, exactly as in example b) above. Therefore h is surjective iff the element $(1, 0, \ldots, 0)$ is in $\mathrm{Im}(h)$ (the 1 is at position e_G). Letting $\sum x_i \otimes y_i$ be a preimage of $(1, 0, \ldots, 0)$ under h, we get the following reformulation of *(ii)*:

(ii') There exist $n \in \mathbb{N}$ and $x_1,\ldots,x_n$, $y_1,\ldots,y_n \in S$ such that $\sum_{i=1}^n x_i\sigma(y_i)$ is 1 or 0, according to whether $\sigma = e_G$ or $\sigma \neq e_G$. (We may write $\sum_{i=1}^n x_i\sigma(y_i) = \delta_{\sigma,e}$.)

(i) $\Rightarrow$ *(ii)*: This is trivial.

(ii') $\Rightarrow$ *(iii)*: We first show that ${}_RS$ is finitely generated projective. Define the *trace* tr: $S \to R$ by $tr(y) = \sum_{\sigma \in G} \sigma(y)$. ($tr$ is well-defined since $S^G = R$, and R-linear since all $\sigma \in G$ are R-linear.) Let φ_i: $S \to R$ be defined by $\varphi_i(z) = tr(zy_i)$, $z \in S$. Then the formula of *(ii')* implies by direct calculation: $z = \sum_i \varphi_i(z)\cdot y_i$ for all $z \in S$, i.e. the pairs (x_i, φ_i) are a dual basis for ${}_RS$, which is hence finitely generated projective.

Now we may, by localization, assume hat S is even finitely generated free over R, with basis $x_1',\ldots,x_n'$, say. We may then assume that the x_i in condition *(ii')* are just the x_i', because every element of $S \otimes S$ can be written in the form $\sum x_i' \otimes y_i'$, and it does not matter just how we write a preimage of $(1,0,\ldots0)$ under h. Let us therefore omit the ' again. From the calculation just performed we get $x_j = \sum_i \varphi_i(x_j)\cdot x_i$, hence by definition of φ_i, and since the x_i are a basis, $tr(x_jy_i) = \delta_{ij}$. As in the field case, bijectivity of j is equivalent to invertibility of the matrix $A = (\sigma(x_i))_{\sigma,i}$. One calculates as follows: Let $B = (\tau(y_j))_{j,\tau}$. Then $AB = (\delta_{\sigma,\tau}) =$ unit matrix (use *(ii')*), and $BA = (tr(x_jy_i))_{ji} =$ unit matrix. Hence A is invertible, and j is bijective.

(iii) $\Rightarrow$ *(i)*: Since S is finitely generated projective over R, we may again assume that S is free over R, with basis $x_1,\ldots,x_n$. As in the last paragraph, j is bijective iff the matrix $A = (\sigma(x_i))_{\sigma,i}$ is invertible. As in the field case, this is again equivalent to the bijectivity of h.

(ii') $\Rightarrow$ *(iv)*: Just suppose $\sigma \neq e_G$ ($= id$), and $\sigma(y) - y \in M$ for all $y \in S$. Then $1 = \sum_i x_i(y_i - \sigma(y_i)) \in M$, contradiction.

(iv) $\Rightarrow$ *(ii')*: We first construct a solution of the formula in *(ii')* for a single $\sigma \neq e_G$ By *(iv)*, the ideal of S generated by all $y - \sigma(y)$ is contained in no maximal ideal, hence is equal to S. One finds hence $n_\sigma \in \mathbb{N}$ and $x_1^{(\sigma)}, \ldots, x_{n_\sigma}^{(\sigma)}$, $y_1^{(\sigma)}, \ldots, y_{n_\sigma}^{(\sigma)} \in S$ with $\sum_i x_i^{(\sigma)}\cdot\left(y_i^{(\sigma)} - \sigma(y_i^{(\sigma)})\right) = 1$. Now one lets $x_0 = \sum_{i=1}^{n_\sigma} x_i^{(\sigma)}\cdot\sigma(y^{(\sigma)})$ and $y_0 = -1$.

We then get (summation from 0 to n_σ): $\sum x_\iota^{(\sigma)}\cdot y_\iota^{(\sigma)} = 1$ and $\sum\, x_\iota^{(\sigma)}\cdot\sigma(y_\iota^{(\sigma)}) = 0$. Now one shuffles together these solutions for individual σ to a solution for all σ as follows: Let I be the index set $\prod_{\sigma\in G\setminus e}\{0,\dots,n_\sigma\}$; for each $\boldsymbol{i}\in I$, let $x_{\boldsymbol{i}}$ be the product of all $x^{(\sigma)}_{\boldsymbol{i}(\sigma)}$ with $\sigma \neq e$, and $y_{\boldsymbol{i}}$ similarly. One can then check that indeed for all $\sigma\in G$: $\sum_{\boldsymbol{i}\in I} x_{\boldsymbol{i}}\cdot\sigma(y_{\boldsymbol{i}})$ is equal to $\delta_{\sigma,e}$, q.e.d.

In our opinion, it is instructive to use the theory of faithfully flat descent already at this early stage of Galois theory of rings. To this end, recall that an R-module M is *faithfully flat* if M is flat, and $M/PM \neq 0$ for each maximal ideal P of R. It is another characterization of faithful flatness that the functor $M\otimes_R -$ preserves and detects short exact sequences of R-modules. One has the following easy results:

Proposition 1.7. [Knus-Ojanguren (1974), Bourbaki Alg. comm. I §3] *Let M be a faithfully flat R-module, and φ: $A\to B$ a homomorphism of R-modules. Then φ is an isomorphism iff $M\otimes_R\varphi$: $M\otimes_R A\to M\otimes_R B$ is an isomorphism. The statement remains correct, if the word "isomorphism" is replaced by "monomorphism", or by "epimorphism".*

This simple result already has applications. Suppose T is an R-algebra which is a faithfully flat R-module, and suppose S is a ring extension of R such that the finite group G acts on S by R-automorphisms. One can then state

Proposition 1.8. *Under these hypotheses, S/R is a G-Galois extension if $T\otimes_R S$ is a G-Galois extension over T.*

Proof. We may consider $T = T\otimes_R R$ as a subalgebra of $T\otimes_R S$, since T is flat. We use the defining property of "G-Galois" and check that the map

$$h_T\colon\ (T\otimes_R S)\otimes_T(T\otimes_R S)\longrightarrow(T\otimes_R S)^{(G)}$$

associated in Def. 1.5. with the extension $T\subset T\otimes_R S$ is, up to canonical isomorphism, just $T\otimes h$ (where $h\colon S\otimes_R S\longrightarrow S^{(G)}$ is the map of Def. 1.5. for the extension $R\subset S$). By 1.7, if $T\otimes h$ is an isomorphism, then so is h. We still have to show that $S^G = R$, i.e. the canonical map ι: $R\to S^G$ is onto. But it follows from the flatness of T that $(T\otimes_R S)^G \cong T\otimes_R S^G$, hence $T\otimes\iota$ is onto. By 1.7, we are done.

The converse of 1.8 is "more than true", in the sense that base change always preserves G-Galois extensions (not only faithfully flat base change). We will see this a little later.

Lemma 1.9. *Any G-Galois extension S/R is faithfully flat over R.*

Proof. Flatness is clear since S/R is projective by Thm. 1.6 (*iii*). Pick a maximal ideal P of R; we need $S/PS\neq 0$. By Nakayama, it suffices to see $S_P\neq 0$. But $R\subset S$, and localization preserves monomorphisms, so we are done.

This lemma suggest to try out S in the role of T; the result is strikingly simple, but we first need to define morphisms of G-Galois extensions:

Definition. If S and S' are two G-Galois extensions, then a *morphism* $\varphi: S \to S'$ is a G-equivariant R-algebra homomorphism from S to S'. (G-equivariance means of course: $\varphi(\sigma x) = \sigma\varphi(x)$ for all $\sigma \in G$, $x \in S$.) The G-Galois extension S/R is called *trivial*, if it is isomorphic to the trivial extension $R^{(G)}/R$.

Remark. It is obvious that we obtain a *category* GAL(R,G) of G-Galois extensions of a given ring R.

Now we can see that "base-extending any Galois extension with itself gives a trivial extension". More precisely: Let S/R be a G-Galois extension, let $T = S$, and consider the ring extension $T \otimes_R S/T$. Since $T = S$, it is now easy to check that the isomorphism h: $S \otimes_R S \to S^{(G)}$ gives an isomorphism of G-Galois extensions h: $T \otimes_R S \to T^{(G)}$. Recall that G operates naturally on the second factor S, and by index shift on $S^{(G)}$. We now can prove a result on the trace:

Lemma 1.10. *Let S/R be G-Galois, and tr: $S \longrightarrow R$ the trace (see proof (ii') $\Rightarrow$ (iii) of* 1.6). *Then*:

a) tr: $S \to R$ is surjective

b) The R-submodule R of S is a direct summand of S.

Proof. a) By the previous remarks, $S\otimes S/S\otimes R$ ($= S$) is isomorphic to the trivial extension of S. One has a commutative diagram

$$\begin{tikzcd}
S \otimes_R S \arrow[r, "\cong"] \arrow[d, "S\otimes tr"'] & S^{(G)} \arrow[d, "tr_S"] \\
S \otimes_R R \arrow[r, "\cong"] & S
\end{tikzcd},$$

where tr_S is the trace associated to the extension $S^{(G)}/S$. S is embedded diagonally in $S^{(G)}$, and one sees from the way G acts on $S^{(G)}$ that $tr_S(x,0,...,0) = (x,x,...,x) =$ diag(x) for all $x \in S$. Hence tr_S is onto; by 1.7, tr is onto.

b) Pick $c \in S$ with $tr(c) = 1$, and let f: $S \to R$ be defined by $f(x) = tr(cx)$. Then f is an R-linear section of the inclusion $R \subset S$, so R is a direct summand of S.

Now we can show:

Lemma 1.11. *Let S/R be G-Galois, and T any R-algebra. Then $T \otimes_R S/S$ is again a G-Galois extension.*

Proof. Write S_T for $T \otimes_R$ S.We want three things: T embeds in S_T, $S_T{}^G = T$, and h_T: $S_T \otimes_T S_T \longrightarrow S_T{}^{(G)}$ is an isomorphism. The last condition is the easiest to see, since we know already that h_T is (up to canonical isomorphism) just $T\otimes h$, and h is an isomorphism by hypothesis. Since R splits of in S, the map $T \to S_T$ also splits, in particular T is a subring of S_T. To see the second condition, we argue as in

Chase–Harrison–Rosenberg (1965): Pick $c \in S$ with $tr(c) = 1$ (Lemma 1.10). and let $y \in S_T$ be fixed under G. Then $y = (T \otimes tr)(1 \otimes c) \cdot y = \sum_\sigma (1 \otimes \sigma(c)) \cdot y = \sum_\sigma (T \otimes \sigma)((1 \otimes c) \cdot y) = (T \otimes tr)((1 \otimes c) \cdot y) \in \mathrm{Im}(T \otimes tr) = T \otimes R = T$, q.e.d.

As another example of this descent technique, we show the following important fact:

Proposition 1.12. *Let S/R and S'/R be G–Galois. Then every morphism φ: $S \to S'$ of G–Galois extensions is an isomorphism.*

Proof. There exists a faithfully flat R–algebra T such that both S_T $(= T \otimes_R S)$ and S'_T are trivial G–extensions of T. (Trivial G–extensions are obviously preserved by arbitrary base change. Hence one can for example take $T = S \otimes_R S'$, since base extension with S (resp. S') trivializes S/R (resp. S'/R).) It is obvious that $T \otimes \varphi$ is a morphism from S_T to S'_T. We may now suppose, by virtue of 1.7, that $T = R$ (fresh notation), $S = S' = R^{(G)}$. Moreover it is harmless to suppose R local. Let now $e^\sigma \in R^{(G)}$ be the element with 1 in position σ and 0 elsewhere ($\sigma \in G$). These e^σ, $\sigma \in G$, are a complete set of irreducible idempotents of $R^{(G)}$, and they are permuted by G in an obvious fashion. In particular, G permutes the e^σ transitively. Getting back to our morphism φ, we now see that the $\varphi(e^\sigma)$ are pairwise orthogonal idempotents with sum 1. If any of them is zero, then all are zero since φ is G–equivariant, so no $\varphi(e^\sigma)$ is zero. Therefore φ must simply permute the e^σ, which implies immediately that φ is an isomorphism.

§ 2 The main theorem of Galois theory

We fix a finite group G and a G–Galois extension S/R of (commutative) rings. Can one find a bijection between subgroups $H \subset G$ and R–subalgebras $U \subset S$? Certainly this problem is not well posed if we admit *all* subalgebras. (Already for $R = \mathbb{Z}$ and $|G| = 2$, the trivial G–extension $S = \mathbb{Z} \times \mathbb{Z}$ has infinitely many subalgebras.) The correct condition to impose on subalgebras is *separability*, an important concept in itself. One may found the whole theory on this concept, which we avoided for the sake of simplicity; we shall use separable algebras practically only in Chapter 0, and as little as possible. Let us just recall the definition and refer the interested reader to DeMeyer–Ingraham (1971). We remind the reader that all rings are supposed commutative.

Definition. An R-algebra S is called *separable* if S is projective as a module over $S\otimes_R S$ (the structure is $(s\otimes t)y = syt$ for $y \in S$, $s\otimes t \in S\otimes S$). If one admits non-commutative algebras S, one has to take $S\otimes S^{opp}$ in the place of $S\otimes S$.

Example. If $R \subset S$ is a field extension of finite degree, then S is a separable R-algebra iff the extension S/R is separable in the usual sense.

Galois extensions are always separable; more precisely, there is the following extension to Theorem 1.6:

Theorem 2.1. *Let S/R be an extension of rings, G a finite subgroup of* Aut(S/R) *such that $S^G = R$. Then the following are equivalent:*

(i) S/R is G-Galois

(ii) S is separable over R, and for each nonzero idempotent $e \in S$ and any σ, $\tau \in G$ with $\sigma \neq \tau$, there exists $y \in S$ with $e\cdot\sigma(y) \neq e\cdot\tau(y)$. (Note that the last condition is vacuously true if S has no idempotents beside 0 *and* 1.)

Proof. See Chase-Harrison-Rosenberg (1965), Thm. 1.3. The last condition in (*ii*) is abbreviated to "if $\sigma \neq \tau$, then σ and τ are *strongly distinct*" in loc.cit.

To keep matters simple, let us assume from now on that S is *connected*, i.e. S has no idempotents besides 0 and 1. The first part of the Main Theorem runs as follows:

Theorem 2.2. [Chase-Harrison-Rosenberg (1965)] *Let S/R be a G-Galois extension, $H \subset G$ a subgroup, and let $U = S^H$ be the subalgebra of H-invariant elements. Then:*

(i) U is separable over R

(ii) S is, in the canonical way, an H-Galois extension of U

(iii) H is the group of all $\sigma \in G$ which leave U pointwise fixed

(iv) If H is a normal subgroup of G, then U is, in the canonical way, a G/H-Galois extension of R.

Proof. We include most of the proof, in order to give the reader a better feeling for the theory. Our argument is mainly the original one (loc.cit.); the changes reflect personal tastes and do not claim to be simplifications. Parts of the proof can be understood without any knowledge about separable algebras.

(*ii*): Choose $x_1,\dots,x_n$, $y_1,\dots,y_n \in S$ as in (*ii'*) (proof of 1.6). Then, a fortiori, $\sum_i x_i\sigma(y_i) = \delta_{\sigma,id}$ for all $\sigma \in H$. The formula $S^H = U$ holds by definition. Hence S/U is H-Galois by Thm. 1.6.

(*i*): By (*ii*) and Thm. 1.6 (*iii*), S is projective over U, hence $S\otimes_R S$ is projective over $U\otimes_R U$. Recalling the definition of separable algebras, we see from Thm. 2.1 that S is projective over $S\otimes_R S$. Hence, by an easy argument, S is projective over $U\otimes_R U$. But U is a direct summand of S (as a U-module, and hence as a $U\otimes U$-module), by (*ii*) and Lemma 1.10 c). Hence U is projective over $U\otimes_R U$, q.e.d.

(iii): We reproduce the direct argument of Chase, Harrison, and Rosenberg. Let $H' = \{\sigma \in G | \sigma \text{ fixes } U \text{ pointwise}\}$. Then $H \subset H'$ and $S^{H'} = S^H = U$. Applying *(ii)* and the definition of Galois extension to U and both of H, H', we obtain that $S \otimes_R S$ is simultaneously isomorphic to $S^{(H)}$ and to $S^{(H')}$, which forces $|H| = |H'|$, and hence $H = H'$.

(iv): See loc.cit. p.23. Another approach: Reduce by faithfully flat descent to the case $S = R^{(G)}$ and check directly that S^H is canonically isomorphic to $S^{(G/H)}$. By the way: It is not difficult to prove also *(ii)* by this method.

The converse of this theorem reads as follows for connected ground rings R. Warning: for nonconnected R the statement is more involved, see Chase, Harrison, and Rosenberg (1965).

Theorem 2.3. *Let R, S, and G be as in 2.2; let $U \subset S$ be a separable R-subalgebra. Then there is a subgroup H of G with $U = S^H$, and H is of necessity the group of all $\sigma \in G$ fixing U pointwise.*

For the *proof*, we refer to loc.cit. (The theory of separability is used in an essential way.)

§3 Functoriality, and the Harrison product

In this section we summarize the paper of Harrison (1965). Several proofs are omitted.

We have already seen in §1 that any homomorphism f: $R \to T$ of commutative rings induces a functor "base extension" from the category GAL(R,G) of G-Galois extensions of R to the category GAL(S,G). We now consider the second argument with the aim of establishing functoriality in G, too. For motivation, consider a finite group G and a factor group G/N. Then in the classical case there is just one way to associate a G/N-Galois extension with a given G-Galois extension L/K: just take L^N/K. This works for rings just as well, by Thm. 2.2. It is important, however, to allow general group homomorphisms π: $G \to H$. Before giving the construction, let us briefly mention the case where π is the inclusion of G in H. This case has no counterpart in classical Galois theory; it will turn out that in this case the map π^*: GAL(R,G) → GAL(R,H) is given by a sort of induction process, as in representation theory, and even if S/R is a G-Galois field extension, $\pi^*(S/R)$ is never a field unless $G = H$. Extreme example: $G = e$, and S is the(!) G-Galois extension R of R. Then π^*R will turn out to be the trivial H-extension of R. Now we present the general result.

Theorem 3.1. *a) Let R be a commutative ring R, $\pi\colon G \to H$ a homomorphism of finite groups. Then there is a canonical functor π^*: $\mathrm{GAL}(R,G) \to \mathrm{GAL}(R,H)$. If π happens to be a canonical surjection $G \to G/N$, then $\pi^*(S) = S^N$ as in the above discussion. (For the construction of π^*, see the proof of this theorem.)*

b) The prescription "$\pi \longmapsto \pi^*$" preserves composition up to canonical isomorphism. In other words: If we let $\mathrm{H}(R,G)$ be the set of isomorphism classes of G-Galois extensions of R, then $\mathrm{H}(R,G)$ is again functorial in G, and the prescription "$\pi \longmapsto \mathrm{H}(R,\pi)$" now preserves composition.

Definition. The set $\mathrm{H}(R,G)$ just defined is also called the *Harrison set* of R and G.

Proof of Thm. 3.1. We do a) and b) simultaneously. First we define π^*. Let $S \in \mathrm{GAL}(R,G)$. We set

$$\pi^*S = \mathrm{Map}_\pi(H,S) \Big(= \{x\colon H \to S \,\big|\, \forall g \in G,\ h \in H\colon x(\pi(g)h) = g(x(h))\}.\Big)$$

The H-action on π^*S is given by $(h'{*}x)(h) = x(h{\cdot}h')$ for $x \in \mathrm{Map}_\pi(H,S)$, $h,h' \in H$. The R-algebra structure is defined "component-wise", i.e. by the inclusion of $\mathrm{Map}_\pi(H,S)$ in $\mathrm{Map}(H,S) = S^{(H)}$. (It is immediate that $\mathrm{Map}_\pi(H,S)$ is indeed a subalgebra.)

One sees easily that π^* is a functor from $\mathrm{GAL}(R,G)$ in the category of R-algebras with action of H. It remains to establish:

(*i*) If $\psi\colon H \to J$ is another group homomorphism, then we have a natural isomorphism $\psi^*\big(\pi^*S\big) \cong (\psi\pi)^*S$;

(*ii*) π^*S/R is, with the given H-action, indeed an H-Galois extension.

We do (*i*) first, by exhibiting natural bijections

$$\mathrm{Map}_\psi(J,\ \mathrm{Map}_\pi(H,S)) \overset{\alpha,\beta}{\rightleftarrows} \mathrm{Map}_{\psi\pi}(J,\ S).$$

(It is left to the reader to verify that α and β are J-equivariant R-algebra homomorphisms.) Let $\alpha(y) = y(-)(e_H)$ for y in the left hand side, i.e. $\alpha(y)(j) = y(j)(e_H)$ for $j \in J$. Let $\beta(z)(j)(h) = z(\psi(h)j)$ for z in the right hand side, $h \in H$, $j \in J$.

We check α is well-defined, i.e. $\alpha(y) \in \mathrm{Map}_{\psi\pi}(J,S)$: Let $j \in J$, $g \in G$. We calculate:

$$\begin{aligned} \alpha(y)(\psi\pi(g)\cdot j) &= y(\psi\pi(g)\cdot j)(e_H) \\ &= \big(\pi(g) * y(j)\big)(e_H) \quad (\text{since } y \in \mathrm{Map}_\psi \ldots) \\ &= y(j)(e_H\pi(g)\,) \quad (\text{def. of } H\text{-action on } \mathrm{Map}_\pi(H,S)) \\ &= g\,(y(j)(e_H)) \quad (\text{since } y(j) \in \mathrm{Map}_\pi \ldots) \end{aligned}$$

$$= g\,(\alpha(y)(j)), \text{ q.e.d.}$$

$\beta\alpha$ is the identity: Let $y \in \mathrm{Map}_{\psi}(J, \mathrm{Map}_{\pi}(H,S))$, $j \in J$, $h \in H$. Then $(\beta\alpha(y))(j)(h) = \alpha(y)(\psi(h)j) = y(\psi(h)\,j)(e_H) = (h * y(j))(e_H)$ (since $y \in \mathrm{Map}_{\psi}\ldots$), and the last expression equals $y(j)(h)$, q.e.d.

$\alpha\beta$ is the identity: Let $z \in \mathrm{Map}_{\psi\pi}(J,S)$, $j \in J$. Then $(\alpha\beta(z))(j) = \beta(z)(j)(e_H) = z(\psi(e_H)j) = z(j)$, q.e.d. This completes the proof of (*i*).

(*ii*): We will give one argument for the general case, and another for the special case that H is abelian.

Note first that π^* commutes with faithfully flat base change, i.e. for any faithfully flat R-algebra T and any S in GAL(R,G), there is a canonical H-equivariant isomorphism $\pi^*(T \otimes S) \cong T \otimes \pi^* S$. By faithfully flat descent, it thus suffices to find such a T with $\pi^*(T \otimes S)$ an H-Galois extension of T. Taking $T = S$ and changing notation, we are reduced to proving: π^* of the trivial G-extension $R^{(G)}$ is an H-Galois extension of R. Let $\iota\colon \{e\} \to G$, $\iota'\colon \{e\} \to H$ be the obvious maps. One checks quite easily: $\iota^* R$ is the trivial G-extension $R^{(G)}$. Since $\pi\iota = \iota'$, we obtain:

$$\begin{aligned} \pi^*(R^{(G)}) \cong \pi^*\iota^* R &\cong (\iota')^* R \qquad \text{(by } (i)) \\ &\cong R^{(H)}, \end{aligned}$$

and we already know that this is indeed an H-Galois extension, q.e.d.

The following nice argument for H abelian is due to Harrison. We factor π as $\pi = \delta\gamma$, with $\gamma = (\mathrm{id}_G, e_H)\colon G \to G \times H$, and $\delta = (\pi, \mathrm{id}_H)\colon G \times H \to H$. Then γ is a split monomorphism, and δ is onto. It is sufficient to show (*ii*) for γ, and for δ, taking into account (*i*). For $\pi = \gamma$, one sees directly that $\pi^* S \cong S \otimes_R R^{(H)}$, with the obvious action of $G \times H$, and one can check that this is a $G \times H$-Galois extension. For $\pi = \delta$, i.e. π onto, one calculates from the definition that $\delta^* S = S^{\mathrm{Ker}(\delta)}$, which is indeed a Galois extension with group $\mathrm{Im}(\delta)$ by Thm. 2.2.

We now present Harrison's construction which makes the set H(R,G) into an abelian group if G is a finite *abelian* group. This will then be called the Harrison group of R and G. (Recall that H(R,G) = GAL(R,G)/$\cong$). We use without further comment the following easy fact: If S, $T \in$ GAL(R,G), then $S \otimes_R T$ with the natural action of $G \times G$, is a $G \times G$-Galois extension of R. Let G be finite abelian, $\iota\colon \{e\} \to G$ be the inclusion of the trivial group in G, $\mu\colon G \times G \to G$ the multiplication (a homomorphism!), and $j\colon G \to G$ the map $g \longmapsto g^{-1}$ (again, a homomorphism).

Definition. The Harrison product $S{\cdot}T$ of S, $T \in$ GAL(R,G) is defined to be

$$S{\cdot}T \;=\; \mu^*(S \otimes_R T) \in \mathrm{GAL}(R,G).$$

By functoriality, the Harrison product $[S{\cdot}T]$ of two isomorphism classes $[S]$, $[T]$ $\in$ H(R,G) is a well-defined element of H(R,G). We shall often abuse notation and write $S \in$ H(R,G) etc.