# GALOIS THEORY OF COMMUTATIVE RINGS: A HISTORICAL PERSPECTIVE

SHARON ZHOU

Abstract. This paper is intended as an introduction to the Galois theory of commutative rings. Building on the framework provided by Rognes [9], we explain a generalization of the notion of Galois extension from fields to commutative rings and summarize some important properties of such extensions. Analogous to the Fundamental Theorem of Galois Theory for fields, given a $G$-Galois extension $T/R$ of commutative rings, there is a bijection between separable $R$-subalgebras of $T$ and subgroups $H \leq G$. Applying this theory to number field extensions $L/K$ lets us understand the structure of the number ring extension $\mathcal{O}_L \,/\, \mathcal{O}_K$ in terms of how $L$ ramifies over $K$.

## Contents



## 1. Introduction

Classically, given a field $K$, Galois theory arises from studying the relation between the permutation group of the roots of a polynomial $f(x) \in K[x]$ and the algebraic structure of its splitting field. We say that a finite extension $L/K$ is *Galois* if $|\operatorname{Aut}(L/K)| = [L : K]$, or, equivalently, if $L$ is normal and separable over $K$. In this case, $G = \operatorname{Aut}(L/K)$ is called the Galois group of $f(x)$, and we say that $L/K$ is a *$G$-Galois extension*.

Since fields are rings with certain special properties, it is natural to ask whether the classical Galois theory can be generalized to (commutative) rings. In 1960, Auslander and Goldman [2] introduced the notion of a Galois extension of commutative rings, which they used to generalize the theory of a *twisted group ring* (also called the *crossed product* in early literature) and Galois cohomology. In 1965, Chase, Harrison and Rosenberg [3] generalized the Fundamental Theorem of Galois Theory to commutative rings and exhibited a seven-term exact sequence of Brauer groups which improved Auslander and Goldman's results on Galois cohomology. Based on Auslander and Goldman's work, Chase, Harrison and Rosenberg

*Date*: August 28, 2021.

formulated six equivalent definitions of a Galois extension of commutative rings and studied homomorphisms of Galois extensions.

In his 1992 paper, Greither [6] revisited the results obtained in [2] and [3], supplementing an application of this theory to number fields. Using the theory of ramification in noetherian rings developed by Auslander and Buchsbaum in [1], Greither pointed out a crucial relation between the ramification behavior of an algebraic number field over the base field and the extension structure of the two rings of integers. Specifically, given a $G$-Galois extension $L/K$ of algebraic number fields, a set $S$ of prime ideals in $\mathcal{O}_K$ and $S'$ the set of prime ideals in $\mathcal{O}_L$ lying above those in $S$, the ring $\mathcal{O}_{L,S'}$ of $S'$-integers is $G$-Galois over $\mathcal{O}_{K,S}$ if and only if all the primes that ramify in $L/K$ are contained in $S$.

Just slightly more than a decade later, in 2005, Rognes [9] used these results to introduce the notion of a Galois extension and a Hopf–Galois extension of commutative algebras, establishing the main theorem of Galois Theory in this setting. This is the motivating starting point for Rognes' analogous development of Galois extensions of structured ring spectra [9]. Inspired by the introductory part of Rognes's work, this paper summarizes some key results in the aforementioned literature in modern language. We start with a suitable definition of Galois extensions of fields which can be naturally generalized to commutative rings, present some interesting properties of such extensions, establish the Fundamental Theorem of Galois Theory in this setting, and apply the theory to the study of rings of integers in number fields.

## 2. Revisiting Galois extension of fields

The development of Galois theory was first motivated by the study of roots of polynomials. Given a field $K$ and a polynomial $f(x) \in K[x]$, we can adjoin the roots of $f(x)$ to $K$ to obtain a field extension $L/K$ such that $f(x)$ splits completely over $L$. In general, we have $|\operatorname{Aut}(L/K)| \leq [L : K]$, where $\operatorname{Aut}(L/K)$ is the set of automorphisms on $L$ which fix the base field $K$. When $f(x)$ is separable (has distinct roots), we have $|\operatorname{Aut}(L/K)| = [L : K]$, in which case we write $\operatorname{Gal}(L/K) = \operatorname{Aut}(L/K)$ and call it the *Galois group* of $L/K$.

Although we obtained the Galois group initially by considering its action on the roots of $f(x)$, the Galois group not only encodes all the information about the roots of the particular polynomial $f(x)$ but describes even more structure of the field extension. As a result, it is often more enlightening to focus on the Galois group itself and "forget" the specific polynomials from which it arises. From this perspective, given a finite group $G$ acting effectively[1] from the left by automorphisms on a field $L$, we say that $L/K$ is a $G$-Galois extension of fields if $G$ is a subgroup of $\operatorname{Aut}(L/K)$ and $K = L^G$ is the fixed subfield.

As intuitive as this definition is, however, its word-for-word translation into the world of (commutative) rings results in too weak a definition. Therefore, we need an alternative definition that admits a more natural generalization to rings. To do so, we first define a *twisted group ring*.

**Definition 2.1.** Let $K$ be a field and $L/K$ a finite extension. Let $G$ be a finite group acting effectively from the left by automorphisms on $L$. The *twisted group*

[1]A group action is *effective* if only the unit element acts as the identity.

*ring* of $G$ over $L$ is the $L$-vector space $L\langle G\rangle = \bigoplus_{g\in G} Lu_g$, with multiplication given by the twisted product defined as follows: for $g, h \in G, u_g, u_h \in L$, we define

$$u_g g \cdot u_h h = u_g g(u_h) gh,$$

using the left $G$-action $(g, u_h) \mapsto g(u_h)$ on $L$.

The ring $L\langle G\rangle$ has $u_1$ as its identity. To lighten the notation, let $x \in L$. Then the map $x \mapsto xu_1$ embeds $L$ as a subring of $L\langle G\rangle$. Moreover, consider the map

$$j : L\langle G\rangle \to \mathrm{Hom}_K(L, L)$$

which maps $xg$ to the homomorphism $y \mapsto x \cdot g(y)$. When $L/K$ is a $G$-Galois extension (in the sense that $G$ embeds into $\mathrm{Aut}(L/K)$ and $K = L^G$ is the fixed subfield), we have the following

**Proposition 2.2.** *The map $j$ is a $K$-algebra isomomorphism.*

The proof of the injectivity of $j$ involves Dedekind's lemma, which we now recall.

**Lemma 2.3** (Dedekind's Lemma)**.** *Let $G$ be a group, $F$ a field, and let $\sigma_1, \ldots, \sigma_n : G \to F^\times$ be distinct homomorphisms. Then the $\sigma_i$ are linearly independent over $F$, that is, if there exist $u_1, \ldots, u_n \in F$ such that $\sum_{i=1}^n u_i\sigma_i(g) = 0$ for all $g \in G$, then $u_i = 0$ for all $i$.*

*Proof of lemma.* Assume for contradiction that the $\sigma_i$ are linearly dependent, and let $\sum_i u_i\sigma_i = 0$ be a relation of linear dependence with a minimum number $k$ of nonzero $u_i \in F$. Renumbering if necessary, we may suppose that

$$u_1\sigma_1(g) + \cdots + u_k\sigma_k(g) = 0$$

for all $g \in G$ and that $u_i \neq 0$ for all $1 \leq i \leq k$. Since the $\sigma_i$ are nonzero, it follows that $k \geq 2$. For any $g, h \in G$, we have

$$u_1\sigma_1(gh) + \cdots + u_k\sigma_k(gh) = u_1\sigma_1(g)\sigma_1(h) + \cdots + u_k\sigma_k(g)\sigma_k(h) = 0$$

Multiplying across by $\sigma_1(h)$ and subtracting the previous equality, we obtain

$$u_2\sigma_2(g)\left(\sigma_1(h) - \sigma_2(h)\right) + \cdots + u_k\sigma_k(g)\left(\sigma_1(h) - \sigma_k(h)\right) = 0$$

Since $k$ is as small as possible by assumption, the coefficients of the $\sigma_i$ are necessarily all zero, i.e., we must have $u_i\left(\sigma_1(h) - \sigma_i(h)\right) = 0$ for all $2 \leq i \leq k$. Now $u_i \neq 0$ implies that $\sigma_1(h) = \sigma_i(h)$ for all $h \in G$ and $2 \leq i \leq k$, which contradicts the assumption that the $\sigma_i$ are distinct. □

Dedekind's lemma has many applications. In the following proof of Proposition 2.2, we will use it to bound the number of $K$-endomomorphisms of $L$ by the dimension of $\mathrm{Hom}_K(L, L)$.

*Proof.* That $j$ is a $K$-algebra homomorphism can be verified directly: for $x, y \in L, g, h \in G, k \in K$, one has

$$j(k \cdot xg) = (z \mapsto kxg(z)) = k \cdot (z \mapsto xg(z))$$

and

$$\begin{aligned} j(xg \cdot yh) &= j(xg(y)gh) \\ &= (z \mapsto xg(y)gh(z)) \\ &= (z \mapsto xg(z)) \circ (z \mapsto yh(z)) \\ &= j(xg) \circ j(yh). \end{aligned}$$

The fact that $j$ respects addition follows from the construction of $L\langle G\rangle$ as an $L$-vector space.

To see that $j$ is bijective, first note that by Dedekind's lemma, the elements $g \in G$ are $L$-linearly independent in $\mathrm{Hom}_K(L, L)$, so $j$ is an injection. In addition, since $[L : K] = |G|$, we have

$$\dim_K L\langle G\rangle = [L : K] \cdot |G| = [L : K]^2 = \dim_K \mathrm{Hom}_K(L, L),$$

so $j$ is surjective, and thus an isomorphism, by dimension considerations. □

We now consider a second map

$$h : L \otimes_K L \to \prod_G L,$$

defined as the canonical ring homomorphism from the tensor product of two copies of $L$ over $K$ to the product of $G$ copies of $L$ (or, equivalently, the set maps from $G$ to $L$), taking $x \otimes y$ to the list $\{g \mapsto x \cdot g(y)\}_{g\in G}$. We give $\prod_G L$ the pointwise product $(l)_g \cdot (l')_g = (ll')_g$. If $L/K$ is a $G$-Galois extension, we have the following observation.

**Proposition 2.4.** *The map $h$ is an $L$-algebra isomomorphism.*

*Proof.* To see that $h$ is an $L$-algebra homomorphism, let $y_1, \ldots, y_n$ be a $K$-basis of $L$. Then $1 \otimes y_1, \ldots, 1 \otimes y_n$ is an $L$-basis of $L \otimes_K L$. One can compute that, for $1 \le i, j \le n$ and any $l \in L$,

$$\begin{aligned} h(1 \otimes y_i + 1 \otimes y_j) &= h(1 \otimes (y_i + y_j)) = \{g \mapsto g(y_i + y_j)\}_g \\ &= \{g \mapsto g(y_i) + g(y_j)\}_g = \{g \mapsto g(y_j)\}_g + \{g \mapsto g(y_j)\}_g \\ &= h(1 \otimes y_i) + h(1 \otimes y_j), \\ h(l \cdot 1 \otimes y_i) &= h(l \otimes y_i) = \{g \mapsto l \cdot g(y_i)\}_g = l \cdot \{g \mapsto g(y_i)\}_g = l \cdot h(1 \otimes y_i) \end{aligned}$$

and

$$\begin{aligned} h((1 \otimes y_i) \otimes (1 \otimes y_j)) &= h(y_i \otimes (1 \otimes y_j)) \\ &= \{g \mapsto g(y_i)g(y_j)\}_g = \{g \mapsto g(y_i)\}_g \cdot \{g \mapsto g(y_j)\}_g \\ &= h(1 \otimes y_i) \cdot h(1 \otimes y_j). \end{aligned}$$

To see that $h$ is bijective, it suffices to show that for any $\sigma \in G$, the matrix $(\sigma(y_i))_{1\le i\le n}$ is invertible (this is an $n \times n$ matrix by construction). Indeed, since the map $j$ is injective by Proposition 2.2, the images of all $\sigma \in G$ are $L$-left linearly independent in $\mathrm{Hom}_K(L, L)$. This completes the proof. □

What we just explained in matrix language is really that $h$ is the $L$-module dual of $j$, which one can make precise via the identifications

$$\mathrm{Hom}_L(L \otimes_K L, L) \cong \mathrm{Hom}_K(L, L), \quad \mathrm{Hom}_L\left(\prod_G L, L\right) \cong L\langle G\rangle.$$

Propositions 2.3 and 2.4 turn out to be the "correct" ways to characterize Galois extensions of fields in the sense that they admit a natural generalization to the world of commutative rings. This will be the focus of the next section.

## 3. Galois extension of commutative rings

Motivated by the observations in the preceding section, Auslander and Goldman [2] introduced the definition of a $G$-Galois extension of commutative rings in 1960 as part of their study of separable algebras over such rings. In 1965, Chase, Harrison and Rosenberg [3] gave five other definitions and proved that they are all equivalent. In his 1992 paper, Greither [6] adopted one of the five alternative definitions from Theorem 1.3 in [3]. Here we follow Greither and summarize the work by these authors.

Let $R, T$ be commutative rings with a ring homomorphism $R \to T$ which makes $T$ a commutative $R$-algebra. Let $G$ be a finite group acting on $T$ from the left via $R$-algebra homomorphisms. Let

$$i : R \to T^G$$

denote the inclusion into the fixed subring, let

$$h : T \otimes_R T \to \prod_G T$$

be the commutative ring homomorphism which maps $x \otimes y$ to the list $\{g \mapsto x \cdot g(y)\}_{g \in G}$, and let

$$j : T\langle G \rangle \to \mathrm{Hom}_R(T, T)$$

be the associative ring homomorphism which maps $xg$ to the $R$-module homomorphism $y \mapsto x \cdot g(y)$. As above, the space $\prod_G T$ is endowed with the pointwise product $(t)_g \cdot (t')_g = (tt')_g$, and $T\langle G \rangle$ the twisted product $t_1 g_1 \cdot t_2 g_2 = t_1 g_1(t_2) g_1 g_2$ given by the left $G$-action $(g_1, t_2) \mapsto g_1(t_2)$ on $T$.

**Definition 3.1.** We say that $R \to T$ is a *$G$-Galois extension* of commutative rings if both $i : R \to T^G$ and $h : T \otimes_R T \to \prod_G T$ are isomorphisms.

Heuristically, the requirement that $i$ be an isomorphism mimics the condition that $R$ is the fixed ring of $T$. The homomorphism $h$, on the other hand, measures the extent to which the extension $R \to T$ is ramified, and Galois extensions are required to be unramified. We will make this more precise by developing a theory of ramification of commutative rings in the last section. Before that, let us first consider some examples to make this definition more concrete.

**Example 3.2.**

(1) If $R, T$ are in fact fields, then Definition 3.1 is the familiar Galois extension of fields.

(2) (Trivial extension) Given a commutative ring $R$, we have the trivial $G$-extension $T = \prod_G R = \mathrm{Map}(G, R)$ equipped with pointwise addition and multiplication, with $G$ acting on it via index shift: for $g \in G, (x_h)_{h \in G} \in \prod_G R$, the action is given by

$$g\left((x_h)_{h \in G}\right) = (x_{hg})_{h \in G}\,.$$

To see that $T^G = R$, first note that if $|G| = n$, then any $x \in R$ can be identified with $(x, \ldots, x) \in T$ which has $n$ identical coordinates. Such an element is of course invariant under any index shift since all the coordinates

are the same, which shows that $R \subset T^G$. Conversely, if $t = (x_1, \dots x_n) \in T$ (where, by an abuse of notation, we are thinking of elements of $G$ as numbers in their role as indices) is fixed under any index shift, then the only possibility is that $x_1 = \ldots = x_n$ for all $n$, which implies that $t \in R$.

It remains to show that $h$ is bijective. Indeed, if $h$ maps $x \otimes y \in T \otimes_R T$ to the trivial element $(e, \dots, e) \in \prod_G T = \prod_G \mathrm{Map}(G, R)$, then we must have $x = y = e$ since the product runs over all $g \in G$. Thus, $h$ is injective. On the other hand, to get any $(x_g)_{g\in G} \in \prod_G T$, consider the element $(x_g)_{g\in G} \otimes (e_g)_{g\in G} \in T \otimes_R T$. After applying an index shift to the second component, this element is mapped to the desired image. Hence $h$ is also surjective.

Definition 3.1 is not the definition first offered by Auslander and Goldman, who instead took the conditions on $i, j$, and $T$ in the following proposition as their definition. Informally, the injectivity of $j$ captures Dedekind's lemma and ensures that the action of $G$ on $T$ is effective.

**Proposition 3.3.** *Let $G$ act on rings $T$ and $R$ as above. Then the extension $R \to T$ is $G$-Galois if and only if the following conditions are satisfied:*

*(1) $T$ is a finitely generated projective $R$-module;*
*(2) The maps $i : R \to T^G$ and $j : T\langle G\rangle \to \mathrm{Hom}_R(T, T)$ are isomorphisms.*

To prove this result, we first review some basic terminology from the theory of localization, which will play a key role in many of the upcoming proofs by allowing one to piece together global information about a ring from local data.

Let $R$ be a commutative ring and $K$ its field of fractions, and let $S \subset R$ be a multiplicative set ($S$ contains 1 and is closed under multiplication). The set

$$S^{-1}R := \{r/s \in K \mid r \in R, s \in S\} \subset K$$

is called the *localization of $R$ at $S$*. Note that $K$ is the localization of $R$ at its unit group $R^\times = R - \{0\}$.

Perhaps the most important sets at which we perform localization are prime ideals: if $\mathfrak{p} \subset R$ is a prime ideal, we frequently take $S = R - \mathfrak{p}$ to obtain the localization at $\mathfrak{p}$, which is given by

$$R_\mathfrak{p} := S^{-1}R = \{r/s \in K \mid r \in R, s \notin \mathfrak{p}\}.$$

Every element of $R$ which does not lie in $\mathfrak{p}$ becomes a unit in $R_\mathfrak{p}$. A ring like $R_\mathfrak{p}$ is called a *local ring*, and it has a unique maximal ideal

$$\mathfrak{p}\, R_\mathfrak{p} = \{r/s \in K \mid r \in \mathfrak{p}, s \notin \mathfrak{p}\},$$

consisting of the complement of the unit group $R_\mathfrak{p}^\times = \{r/s \in K \mid r, s \notin \mathfrak{p}\}$, which is the set of elements invertible modulo $\mathfrak{p}$. In general, localizing at $S$ maps every ideal disjoint from $S$ to the corresponding ideal in the local ring and every ideal which intersects $S$ nontrivially to the unit ideal in the local ring. More precisely, we have the following result, which follows easily from the observation that $S^{-1}I$ contains 1 if and only if there is some $s \in I \cap S$.

**Proposition 3.4.** *Let $R$ be a domain and $I \subset R$ be an ideal. The image of $I$ under the localization map $R \to S^{-1}R$ generates an ideal $S^{-1}I = \{i/s \mid i \in I, s \in S\} \subset S^{-1}R$, with $S^{-1}I \neq S^{-1}R$ if and only if $I \cap S \neq \varnothing$.*

We are now in a position to prove Proposition 3.3 (for the original proof, see Theorem 1.6 of [6] and Theorem 1.3 of [3]).

*Proof.* First, suppose that $T/R$ is a $G$-Galois extension (both $i : R \to T^G$ and $h : T \otimes_R T \to \prod_G T$ are isomorphisms). In particular, $h$ is surjective. Since $h$ is compatible with the $G$-action, where $G$ acts naturally on the second factor of $T \otimes_R T$ and via index shift on $\prod_G T$ as in the case of the trivial extension (see Example 3.2), it is surjective if and only if the element $(1, 0, \ldots, 0)$ lies in the image of $h$ (with 1 in the coordinate indexed by $e$). Writing $(1, 0, \ldots, 0) = h(\sum x_i \otimes y_i)$, we can reformulate the surjectivity of $h$ as the following condition:

For some $n \in \mathbb{N}$ there exist $x_1, \ldots, x_n, y_1, \ldots, y_n \in T$ such that

$$\sum_{i=1}^{n} x_i g(y_i) = \begin{cases} 1 & \text{if } g = e, \\ 0 & \text{if } g \neq e \end{cases} \tag{3.5}$$

which we can denote by $\sum_{i=1}^{n} x_i g(y_i) = \delta_{g,e}$.

First, we show that $T$ is finitely generated projective as an $R$-module. Recall the *trace map* $\mathrm{tr} : T \to R$ defined by

$$\mathrm{tr}(t) = \sum_{g \in G} g(t), \quad t \in T.$$

This map is well defined since applying any $g \in G$ to $\sum_{g \in G} g(t)$ permutes the sum, so $\mathrm{tr}(t)$ lies in the fixed ring $T^G = R$. It is also $R$-linear since any $g \in G$ is $R$-linear.

Define $\varphi_i : T \to R$ by $\varphi_i(t) = \mathrm{tr}(ty_i)$. For any $t \in T$, the summation formula in (3.5) implies that

$$t = \sum_{i=1}^{n} \varphi_i(t) \cdot x_i,$$

so the pairs $(x_i, \varphi_i)$ form a dual basis for $S$ as an $R$-module, which is therefore finitely generated projective.[2]

Localizing if necessary, we may assume without loss of generality that $S$ is finitely generated free over $R$, with basis $v_1, \ldots, v_n$. Further, we may take the $x_i$ in (3.5) to be the $v_i$, since any element of $T \otimes_R T$ takes the form of $\sum v_i \otimes u_i$, so we are free to express the preimage of $(1, 0, \ldots, 0)$ under $h$ in any suitable basis. Thus we will assume that $x_i = v_i$ and $y_i = u_i$. This gives us

$$x_j = \sum_{i=1}^{n} \varphi_i(x_j) \cdot x_i,$$

and so $\mathrm{tr}(x_j y_i) = \delta_{i,j}$ by the definition of the $\varphi_i$. As in the proof of Proposition 2.4, $j$ is bijective if and only if the matrix $M = (g(x_i))_{g,i}$ is invertible. Letting $N = (h(y_j))_{j,h}$, we see that

$$MN = (\delta_{g,h}) = I_n, \quad NM = (\mathrm{tr}(x_j y_i))_{j,i} = I_n$$

by (3.5), where $I_n$ denote the $n \times n$ identity matrix. Thus $M$ is invertible, which shows that $j$ is bijective.

Conversely, suppose that $T$ is a finitely generated projective $R$-module and that $j : T\langle G \rangle \to \mathrm{Hom}_R(T, T)$ is an isomorphism. Localizing once again if necessary, we may assume that $T$ is free over $R$ with basis $x_1, \ldots, x_n$. As before, the bijectivity

[2]There is a typo in [6] regarding the previous display (the $x_i$ was mistakenly put as $y_i$).

of $j$ is equivalent to the invertibility of the matrix $M = (g(x_i))_{g,i}$, which is in turn equivalent to the bijectivity of $h$. This completes the proof. □

*Remark* 3.6. Throughout this proof, we really only made use of the surjectivity of $h$ (although the definition of a $G$-Galois extension requires that $h$ be bijective). Indeed, surjectivity of $h$ alone suffices to show that $T/R$ is a $G$-Galois extension, and is therefore equivalent to bijectivity in this context. This is part of the content of Theorem 1.6 in [6].

There are several other ways of defining $G$-Galois extensions of commutative rings, which all turn out to be equivalent (see Section 1 of [3] and Section 0 of [6] for the exact statements and proofs). In particular, a characterizing property of a $G$-Galois extension $T/R$ is that, for any non-identity element $g \in G$ and any maximal ideal $\mathfrak{m} \subset T$, there exists $x \in T$ such that $g(x) - x \notin \mathfrak{m}$. This definition is especially useful for checking that we recover the usual notion of a $G$-Galois extension when working with fields (whose only ideals are the trivial ideal and the entire field).

Having seen the notion of Galois extensions of commutative rings, we now discuss some properties enjoyed by such Galois extensions based on Section 0.1 and Section 0.6 of [6]. To that end, we recall some definitions from module theory.

**Definition 3.7.** Let $M$ be an $R$-module. We say that $M$ is *flat* if for every injective linear map $\varphi : K \to L$ of $R$-modules, the map

$$\varphi \otimes_R M : K \otimes_R M \to L \otimes_R M$$

induced by $k \otimes m \mapsto \varphi(k) \otimes m$ is also injective. We say that $M$ is *faithfully flat* if it is flat and $M \otimes_R N \neq 0$ for every nonzero $R$-module $N$.

Another characterization of a faithfully flat module $M$ is that $M$ is flat and $M/\mathfrak{m}M \neq 0$ for any maximal ideal $\mathfrak{m}$. In functorial language, $M$ is faithfully flat if the tensor product functor $- \otimes_R M$ is exact (maps short exact sequences to short exact sequences) and faithful (injective on maps), i.e., $-\otimes_R M$ preserves and detects exact sequences.

A useful fact due to Knus and Ojanguren [8] is that, for any faithfully flat $R$-module $M$ and homomorphism $\varphi : A \to B$ of $R$-modules, $\varphi$ is an isomorphism (or monomorphism or epimorphism) if and only if the induced map $M \otimes_R \varphi : M \otimes_R A \to M \otimes_R B$ is an isomorphism (or monomorphism or epimorphism, respectively). As we shall see below, this result, commonly referred to as the *descent technique*, can be very useful in proving the existence of isomorphisms.

For the rest of this section, let $R \subset T$ be commutative rings. The following proposition illustrates one of the many desirable properties of being faithfully flat.

**Proposition 3.8.** *Let $T$ be faithfully flat as an $R$-module, and let $G$ be a finite group acting on a ring extension $S$ of $R$ via $R$-automorphisms. Then $S/R$ is a $G$-Galois extension if $T \otimes_R S$ is a $G$-Galois extension over $T$.*

*Proof.* Since $T$ is flat over $R$, we may consider $T$ as a subalgebra of $T \otimes_R S$ via the identification $T = T \otimes_R R$. Let $h : S \otimes_R S \to \prod_G S$ denote the map associated with the extension $S/R$ as in Definition 3.1. Then the induced map

$$h' : (T \otimes_R S) \otimes_R (T \otimes_R S) \to \prod_G T \otimes_R S$$

associated with the extension $(T \otimes_R S)/T$ can be seen as $T \otimes h$ up to isomorphism. By descent, if $T \otimes h$ is an isomorphism, then so is $h$. It remains to be shown that $S^G = R$, i.e., the map $i : R \to S^G$ is surjective. Indeed, since $T$ is flat, we have $(T \otimes_R S)^G = T \otimes_R S^G$, which shows that $T \otimes i$, and therefore $i$, is surjective (by faithfully flat descent). □

In fact, all Galois extensions are faithfully flat. To see this, we first recall a lemma due to Nakayama.

**Lemma 3.9** (Nakayama)**.** *Let $M$ be a finitely generated $R$-module, and $I \subset R$ an ideal contained in the intersection of all all maximal ideals of $R$. If $IM = M$, then $M = 0$.*

A proof of this lemma can be found in various standard algebra texts, for example Chapter 16 of [5]. It gives a criterion for determining when a module must be zero, which we shall be employing in the proof of the following proposition.

**Proposition 3.10.** *Let $T/R$ be a $G$-Galois extension. Then $T$ is faithfully flat as an $R$-module.*

*Proof.* By Proposition 3.3, $T$ is a finitely generated projective $R$-module, so it must be flat. It remains to be shown that $T$ is faithful, i.e., $T/\mathfrak{m}T \neq 0$ for all maximal ideals $\mathfrak{m} \subset R$. By Nakayama's lemma, it suffices to prove that $T_\mathfrak{m} \neq 0$: if $T = \mathfrak{m}T$, localization at $\mathfrak{m}$ yields $T_\mathfrak{m} = \mathfrak{m}T_\mathfrak{m}$. Since $\mathfrak{m}T_\mathfrak{m}$ is the unique maximal ideal of $T_\mathfrak{m}$, it follows from Nakayama's lemma that $T_\mathfrak{m} = 0$. Note that the finite generation condition is needed in order to apply this lemma.

Note that the inclusion map $R \to T$ is a monomorphism of $R$-modules. Since localization preserves monomorphisms, the localized map $R_\mathfrak{m} \to T_\mathfrak{m}$ is also a monomorphism. Now $R_\mathfrak{m}$ is nonzero because it has a nonzero quotient $R/\mathfrak{m}R$, so $T_\mathfrak{m}$ is also nonzero. □

Since any Galois extension of commutative rings is faithfully flat, one naturally wonders what will happen if we let $S$ play the role of $T$ in Proposition 3.8, i.e., if we consider $S \otimes_R S$. To explain the consequences of this move, it is beneficial to work in a categorical framework, which we now set up.

**Definition 3.11.** Let $T, T'$ be two $G$-Galois extensions of $R$. Then $\varphi : T \to T'$ is a *morphism* if it is a $G$-equivariant $R$-algebra homomorphism, i.e.,

$$\varphi(gx) = g\varphi(x)$$

for all $g \in G, x \in T$. We say that $T/R$ is a *trivial extension* if it is isomorphic to the trivial extension $(\prod_G R)/R$ (see Example 3.2).

This definition gives us a category $\mathrm{Gal}(R, G)$ where the objects are $G$-Galois extensions of a commutative ring $R$, with an isomosphism $h : T \otimes_R S \to \prod_G T$. By construction and as in Example 3.2, $G$ acts on the second factor of $S$ in the tensor product and by index shift on $\prod_G S$. This leads to the following observation regarding the trace map, which we introduced in the proof of Proposition 3.3.

**Proposition 3.12.** *The trace map is a split surjective $R$-module homomorphism. In particular, $R$ is an $R$-module direct summand of $T$.*

*Proof.* We show two things: first, that the trace map $\mathrm{tr} : S \to R$ is surjective; second, that $R$ is a direct summand of $T$ as an $R$-submodule.

By the remarks on $\mathrm{Gal}(R, G)$, $S \otimes S / S \otimes R$ is isomorphic to the trivial extension $\prod_G S$. Thus we have a commutative diagram

$$\begin{array}{ccc} S \otimes_R S & \xrightarrow{\cong} & \prod_G S \\ \downarrow{\scriptstyle S \otimes \mathrm{tr}} & & \downarrow{\scriptstyle \mathrm{tr}_S} \\ S \otimes_R R & \xrightarrow{\cong} & S \end{array}$$

where $\mathrm{tr}_S$ is the trace map associated with the extension $\left(\prod_G S\right)/S$. Note that $S$ is embedded diagonally in $\prod_G S$. Since $G$ acts by index shift on $\prod_G S$, we have

$$\mathrm{tr}_S(x, 0, \ldots, 0) = (x, x, \ldots, x),$$

which is the diagonal element with $x$ in each coordinate. Thus $\mathrm{tr}_S$ is surjective, and so tr is surjective by descent, which justfies the removal of tensoring with $S$.

To show that $R$ is a direct summand of $S$, pick $a \in S$ such that $\mathrm{tr}(a) = 1$. Consider the map $f : S \to R$ defined by $f(x) = \mathrm{tr}(ax)$. Then $f$ is an $R$-linear section of the inclusion map $i : R \hookrightarrow S$, since $f \circ i = \mathrm{id}_S$. Thus $R$ is a direct summand of $S$. □

Another application of the technique of (faithfully flat) descent appears in the proof of the following proposition, which gives us quite a rigid structure on homomorphisms between $G$-Galois extensions of a given ring. The strategy is to first perform a faithfully flat base change to the case of a trivial extension and, assuming without loss of generality that $R$ is local, consider the list of elements $e_g \in \prod_G R$ where each element has 1 in the position labelled by $g$ and 0 otherwise. The set $\{e_g \mid g \in G\}$ is permuted by $G$ transitively. One then checks that the $\varphi(e_g)$ are pairwise orthogonal idempotents which sum to 1. Now $G$-equivariance implies that none of the $\varphi(e_g)$ are 0, so $\varphi$ must also permute the $e_g$, making $\varphi$ an isomorphism. For a detailed proof, see Proposition 1.12 of [6].

**Proposition 3.13.** *Let $T/R$ and $T'/R$ be $G$-Galois extensions. Then every map of $G$-Galois extensions $\varphi : T \to T'$ is an isomorphism.*

We finish this section with a discussion on the structure of the $G$-Galois extension $T/R$ as an $R[G]$-module, where $R[G]$ denotes the group ring. The action of $G$ on $T$ makes $T$ into a left $R[G]$-module, and it is a classical result in Galois theory for fields that, for any $G$-Galois extension $L/K$, $L$ is free cyclic over $K[G]$. That is, $L$ admits a $K$-basis in the form $\{gx \mid g \in G\}$ for some $x \in K$. Such a basis is usually called a *normal basis*.

This result no longer holds, however, in the context of Galois extensions over commutative rings. A more detailed account of this theory can be found in Chapter 0.6 of [6], including reasons for this failure of generalization. Here, we present a weakened version of the above observation on normal bases.

**Proposition 3.14.** *$T$ is invertible as an $R[G]$-module, i.e., a finitely generated projective $R[G]$-module of constant rank 1.*

*Proof.* Since $T$ is finitely presented as an $R$-module, so is it finitely presented as an $R[G]$-module, where we allow new relations of the form $g \cdot x - g(x)$ for $g \in G$ and $x$ running over a finite list of $R$-generators of $T$. By the descent technique, it suffices to show that $T$ (as an $R[G]$-module) is invertible after a faithfully flat extension of

$R[G]$, i.e., after tensoring with faithfully flat $R[G]$-module over $R[G]$. Consider the extension $R[G] \subset T[G]$. Then

$$T[G] \otimes_{R[G]} T \cong T \otimes_R T$$

as an $R[G]$-module, and the right hand side is isomorphic to $\prod_G T$ via the associated map $h$. Since $\prod_G T$ is free cyclic over $T[G]$ on the element $(1, 0, \ldots, 0)$ with 1 in the position labelled by the identity $e$, we see that $T$ is finitely generated over $R[G]$ with rank 1. □

## 4. Fundamental Theorem of Galois theory

Now that we have the notion of a $G$-Galois extension of commutative rings, it is natural to ask whether we can obtain a similar result to the Fundamental Theorem of Galois Theory for fields. As one may recall, the classical Fundamental Theorem of Galois Theory states that, given a Galois extension $L/K$ of fields with $G = \mathrm{Gal}(L/K)$, there is an inclusion-reversing bijection between subfields $E$ of $L$ containing $K$ and subgroups $H$ of $G$ such that $[L : E] = |H|$ and $[E : K] = |G : H|$. Further, $E$ is Galois over $K$ with Galois group $G/H$ if and only if $H$ is a normal subgroup of $G$.

Given a finite group $G$ and a $G$-Galois extension $T/R$ of commutative rings, the question of finding a correspondence between $R$-subalgebras $S$ of $T$ and subgroups $H$ of $G$ was first explored by Chase, Harrison and Rosenberg in [3]. This question is only meaningful when restricted to a specific subset of subalgebras: as a simple example, take $R = \mathbb{Z}, |G| = 2$, then the trivial $G$-extension $T = \mathbb{Z} \times \mathbb{Z}$ has infinitely many $\mathbb{Z}$-subalgebras, while $G$ has no nontrivial subgroups. It turns out that, in this context, the "correct" type of algebras to consider is *separable* algebras, which we now define.

**Definition 4.1.** An $R$-algebra $T$ is called *separable* if $T$ is projective as a module over $T \otimes_R T$ under the structure $(x \otimes y)t = xty$ for $t \in T, x \otimes y \in T \otimes_R T$.

More generally, if $R$ is noncommutative, then one has to replace $T \otimes_R T$ by $T^e = T \otimes_R T^{op}$ in the above definition.

**Example 4.2.** If $L/K$ is a finite dimensional field extension, then Definition 4.1 agrees with the usual definition of separable field extensions, i.e., every element of $L$ is the root of a separable polynomial (with no repeated roots) over $K$.

Surely, we would want Galois extensions to be separable. This is indeed the case, as shown by the next theorem, which also contains a converse to this observation.

**Theorem 4.3.** *Let $T/R$ be an extension of commutative rings and $G$ a finite subgroup of $\mathrm{Aut}(T/R)$ such that $T^G = R$. Then the following are equivalent:*

*(1) $T/R$ is a $G$-Galois extension;*
*(2) $T$ is separable over $R$, and for each nonzero idempotent $e \in T$ and any two distinct elements $\sigma, \tau \in G$, there exists $x \in T$ such that $e \cdot \sigma(x) \neq e \cdot \tau(x)$.*

This theorem is proved as part of Theorem 1.3 in [3]. In the appendix of [2], Auslander and Goldman proved the forward direction, i.e., that Galois extensions are necessarily separable.

If the only idempotents of $T$ are 0 and 1, condition (2) is vacuously satisfied. In this case, we say that $T$ is *connected*. Assuming that $T$ is connected, Chase, Harrison, and Rosenberg proved the following theorem as an analogue to the classical Fundamental Theorem of Galois Theory of fields.

**Theorem 4.4** (Chase-Harrison-Rosenberg 1965)**.** *Let $T/R$ be a $G$-Galois extension, $H \subset G$ a subgroup, and $S = T^H$ the subalgebra of elements fixed by $H$. Then*

*(1) $S$ is separable over $R$;*
*(2) $T$ is the canonical $H$-Galois extension of $S$;*
*(3) $H$ consists precisely of all $\sigma \in G$ which fix $S$ pointwise;*
*(4) If $H$ is a normal subgroup of $G$, then $S$ is the canonical $G/H$-Galois extension of $R$.*

*Proof.* We start by proving claim (2). Since $T/R$ is Galois, we may choose $x_1, \ldots, x_n$, $y_1, \ldots, y_n \in T$ satisfying (3.5). For any $h \in H$, we have

$$\sum_{i=1}^{n} x_i h(y_i) = \delta_{h,\mathrm{id}}.$$

Thus $T/S$ is an $H$-Galois extension by Remark 3.6.

Now we show claim (1). By Proposition 3.3, claim (2) implies that $T$ is finitely generated projective over $S$, so $T \otimes_R T$ is projective over $S \otimes_R S$. Now Theorem 4.3 implies that $T$ is separable over $R$, i.e., $T$ is projective over $T \otimes_R T$. It follows that $T$ is also projective over $S \otimes_R S$. By Proposition 3.12, since $T$ is Galois over $S$, $S$ is a direct summand of $T$ as an $S$-module (and therefore an $S \otimes_R S$-module). Therefore, $S$ is projective over $S \otimes_R S$, which means that $S$ is separable, as desired.

To prove claim (3), let $H' \subset G$ denote the set of elements fixing $S$ pointwise. Then $H$ is a subset of $H'$, and $T^{H'} = T^H = S$. By claim (2), $T$ is a Galois extension of $S$ with Galois groups $H$ and $H'$. By Proposition 3.3, the associated maps

$$h : T \otimes_S T \to \prod_H T,\ h' : T \otimes_S T \to \prod_{H'} T$$

are bijective, so $|H| = |H'|$. Thus $H = H'$.

Lastly, to prove claim (4), let $H$ be a normal subgroup of $G$. Then $G/H$ acts on $S = T^H$ such that $S^{G/H} = T^G = R$. Using the $x_i, y_i$ defined in the proof of claim (2), we define new elements

$$x_i' = \sum_{h \in H} h(a \cdot x_i),\ y_i' = \sum_{h \in H} h(y_i)$$

where $a \in T$ satisfies $\mathrm{tr}(a) = 1$ (such an element is guaranteed to exist by Proposition 3.12). Then $x_i', y_i' \in T^H = S$. For any $g \in G$,

$$\sum_{i=1}^{n} x_i' g(y_i') \begin{cases} 1 & \text{if } g \in H \\ 0 & \text{if } g \notin H \end{cases},$$

which shows that the $R$-algebra $S$ and the quotient group $G/H$ satisfy the criterion in Remark 3.6. Finally, the faithfulness of the action of $G/H$ on $S$ follows from the above observation that $H$ is precisely the set of elements of $G$ which fix $S$ pointwise. Therefore, $S$ is the canonical $G/H$-Galois extension of $R$. □

Greither outlined an alternative approach to proving claim (4): first, use the technique of faithfully flat descent and reduce to the case of $T = \prod_G R$, from where one checks directly that $T^H$ is isomorphic to $\prod_{G/H} T$ (see Section 2 of [6]).

In [3], Chase, Harrison and Rosenberg proved a converse to Theorem 4.4. First, we prove a lemma that gives us a way of constructing Galois extensions from existing ones.

**Lemma 4.5.** *Let $T/R$ be $G$-Galois. Then for any $R$-algebra $S$, the extension $(S \otimes_R T)/T$ is again $G$-Galois, where $G$ acts on $S \otimes_R T$ via $g(s \otimes t) = s \otimes g(t)$.*

*Proof.* To lighten the notation, write $T_S$ for $S \otimes_R T$. We need to show three things: that $S$ embeds into $T_S$, that $T_S^G = S$, and that $h_S : T_S \otimes_S T_S \to \prod_G T_S$ is an isomorphism.

The last claim follows from the identification of $h_S$ with $S \otimes h$ and the assumption that $h : T \otimes_R T \to \prod_G T$ is an isomorphism. Since $R$ is a direct summand of $T$, the map $S \to T_S$ also splits, making $S \cong S \otimes 1$ a subring of $T_S$. This proves the first claim.

Lastly, since $S$ is certainly fixed under the $G$-action on $T_S$, the real content of the second claim is that $T_S^G \subset S$. By Proposition 3.12, we can pick $a \in T$ with $\mathrm{tr}(a) = 1$. For any $x \in T_S^G$, we have, by the definition of the trace map,

$$\begin{aligned} x &= (S \otimes \mathrm{tr})(1 \otimes a) \cdot x \\ &= \sum_{g \in G} (1 \otimes g(a)) \cdot x = \sum_{g \in G} (S \otimes g)((1 \otimes a) \cdot x) \\ &= (S \otimes \mathrm{tr})((1 \otimes a) \cdot x), \end{aligned}$$

so $x$ lies in the image of the map $S \otimes \mathrm{tr}$, which is just $S \otimes R \cong S$. Thus $T_S^G \subset S$, as desired. □

We are now ready to state and prove the converse to Theorem 4.4.

**Theorem 4.6.** *Let $T/R$ be a $G$-Galois extension, and let $S \subset T$ be a separable $R$-algebra. Let $H \subset G$ be the group of elements which fix $S$ pointwise. Then $S = T^H$.*

*Proof.* We need to show that $T^H \subset S$. By Lemma 4.5, $T \otimes T$ is a $G$-Galois extension of $T$. The associated isomorphism $h$ induces a $G$-action on $\prod_G T$ via the formula

$$(gf)(h) = f(gh),$$

which makes $\prod_G T$ also a $G$-Galois extension of $T$. Since $T$ is projective over $R$, we can identify $T \otimes S$ with its image in $T \otimes T$. We first show that $(\prod_G T)^H \subset h(T \otimes S)$.

Since $H$ is a subgroup of $G$, there exist $g_1, \ldots, g_k \in G$ such that $G = \cup_{i=1}^k g_i H$. Then $(\prod_G T)^H$ consists of all maps from $G$ to $T$ whose resrictions to the cosets $g_i H$ are just the identity. Define the maps $\varphi_i : \prod_G T \to T$ by $\varphi_i(f) = f(g_i)$. Since $S$ is separable over $R$, so are $T \otimes S$ and therefore $h(T \otimes S)$. By Lemma 1.2 in [3], there exist pairwise orthogonal idempotents $y_1, \ldots, y_k \in h(T \otimes S)$ such that

$$\varphi_i(x) y_i = x \cdot y_i$$

for all $x \in h(T \otimes S)$, and

$$y_j(g_i) = \varphi_i(y_i) = \delta_{ij}$$

for $i, h \leq n$. This makes $y_1, \ldots, y_k$ a $T$-basis of $(\prod_G T)^H$, and so $(\prod_G T)^H \subset h(T \otimes S)$. Applying $h^{-1}$ to both sides of the inclusion yields

$$T \otimes T^H \subset (T \otimes T)^H \subset T \otimes S.$$

We can now apply the tensored map $\mathrm{tr} \otimes 1$ to this inclusion and deduce that $T^H \subset S$ by Proposition 3.12. □

The theory is more delicate if $T$ is not connected, i.e., contains nontrivial idempotents. A counterexample to Theorem 4.4 for such $T$ is given by Chase, Harrison, and Rosenberg in Section 2 of [3]P: let $T = \bigoplus_{i=1}^{4} Re_i$ (direct sum of four free $R$-modules of rank 1) be a $\mathbb{Z}/4$-extension where the $e_i$ are pairwise orthogonal idempotents such that $\sum e_i = 1$. Suppose that the $e_i$ are cyclically permuted by the generator $\sigma$ (say $\sigma(e_i) = e_{i+1 \pmod 4}$). Setting

$$U = R(e_1 + e_2) \oplus R(e_3 + e_4),$$

we see that $\mathrm{Aut}(T/U)$ is trivial since any $f \in \mathrm{Aut}(T/U)$ is generated by $\sigma$ and therefore cannot swap two pairs of $e_i$, but the intermediate ring fixed by the trivial group is $T$ rather than $U$.

## 5. Application to number fields

An important application of Galois theory of commutative rings lies in the study of number fields. Specifically, the ramification of one number field over another gives us information about the structure of the commutative ring extension of the corresponding rings of integers.

Let $L/K$ be a $G$-Galois extension of number fields, and $\mathcal{O}_K, \mathcal{O}_L$ the rings of algebraic integers in $K$ and $L$, respectively. The main goal of this section is to show that $\mathcal{O}_L/\mathcal{O}_K$ is a $G$-Galois extension of rings if and only if $L/K$ is *unramified*. To that end, we review some basic concepts and results regarding the ramification of rings.

First, if $L/K$ is a $G$-Galois extension of number fields, then $G$ also operates on the ring $\mathcal{O}_L$ with

$$(\mathcal{O}_L)^G = \mathcal{O}_L \cap K = \mathcal{O}_K.$$

That is, $\mathcal{O}_K$ is the fixed subring of $\mathcal{O}_L$ by the action of $G$. This observation leads to a natural question: under what conditions is $\mathcal{O}_L$ a $G$-Galois extension of $\mathcal{O}_K$? The answer is certainly not "always," as illustrated by the following example.

**Example 5.1.** Take $K = \mathbb{Q}, L = \mathbb{Q}[i]$, and let $\sigma$ denote the complex conjugation map. Then $G = \{e, \sigma\}$. $\mathcal{O}_L \,/\, \mathcal{O}_K$ is *not* a $G$-Galois extension.

*Proof.* First, we have $\mathcal{O}_L = \mathbb{Z}[i]$ and $\mathcal{O}_K = \mathbb{Z}$. We will show that the map $j : L\langle G\rangle \to \mathrm{Hom}_K(L, L)$ defined in Section 3 fails to be a bijection by showing that it is not surjective. To see this, consider the maximal ideal $\mathfrak{p} = (1 + i) \subset \mathbb{Z}[i]$. Then $2 \in \mathfrak{p}$. It suffices to show that, for each $\varphi \in \mathrm{img}\, j$, we have $\varphi(1) \equiv \varphi(i) \pmod{\mathfrak{p}}$. Indeed, writing $\varphi = f(a \cdot e + b \cdots \sigma)$ for $a, b \in \mathbb{Z}[i]$, we have

$$\varphi(1) = a + b, \varphi(i) = a \cdot i - b \cdot i \equiv a - b \pmod{\mathfrak{p}}.$$

Since $a - b \equiv a + b \pmod 2$, it follows that $a - b \equiv a + b \pmod{\mathfrak{p}}$. On the other hand, we can certainly find $\phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[i], \mathbb{Z}[i])$ such that $\phi(1) = 1, \phi(i) = 0$, which do not lie in the same residue class modulo $\mathfrak{p}$. Thus, $j$ is not surjective, so $\mathcal{O}_L \,/\, \mathcal{O}_K$ is not a $G$-Galois extension. □

The problem that prevents $L/K$ in this example from being a $G$-Galois extension has to do with *ramification*, which we now explain (following Auslander and Buchsbaum [1]).

Given commutative rings $T$ and $R$, we say that $T$ is an $R$-algebra if there is a ring homomorphism $R \to T$ sending 1 to 1. Let $\mathfrak{p} \subset R$ and $\mathfrak{P} \subset T$ be prime ideals in $R$ and $T$, respectively.

**Definition 5.2.** Let $\mathfrak{P} \subset T$ be a prime ideal and $\mathfrak{p} = R \cap \mathfrak{P}$. We say that $\mathfrak{P}$ is *unramified* if

(1) $T_{\mathfrak{P}} = \mathfrak{P} T_{\mathfrak{P}}$;
(2) $T/\mathfrak{P}$ is a separable field extension of $R/\mathfrak{p}$.

If one is working with field extensions, the first condition can be rephrased in the language of the ramification index. Given a prime $\mathfrak{p} \subset R$, the primes *lying over* $\mathfrak{p}$ are those which occur in the prime decomposition

$$\mathfrak{p}\, T = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i},$$

and the exponents $e_i$ are called the *ramification indices*. If $e$ is the exact power of $\mathfrak{P}$ dividing $\mathfrak{p}\, T$, we say that $e$ is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ and denote it by $e(\mathfrak{P}|\,\mathfrak{p})$. Thus, condition (1) means that $e(\mathfrak{P} \mid \mathfrak{p}) = 1$. In other words, we say that $L/K$ is ramified at $\mathfrak{p}$ (or, equivalently, that $\mathfrak{p}$ ramifies in $L$) if $e_i$ is greater than 1 for some $i$. Otherwise, $L/K$ is said to be unramified at $\mathfrak{p}$.

If $R$ is a field, then the $R$-algebra $T$ is *separable* if $T$ is a finite-dimensional $R$-algebra which decomposes as a direct sum of separable field extensions of $R$. Building on Definition 5.2, we have the following

**Definition 5.3.** Let $T$ be an $R$-algebra. We say that $T$ is *unramified* if

(1) every prime ideal in $T$ is unramified;
(2) for each prime $\mathfrak{p} \subset R$, there are only finitely many prime ideals $\mathfrak{P} \subset T$ such that $\mathfrak{p} = \mathfrak{P} \cap R$.

In other words, $T/R$ is an unramified extension if and only if given any prime $\mathfrak{p}$ which lies below some $\mathfrak{P} \subset T$, the quotient $T_{\mathfrak{p}}/\,\mathfrak{p}\, T_{\mathfrak{p}}$ is a separable $R_{\mathfrak{p}}/\,\mathfrak{p}\, R_{\mathfrak{p}}$-algebra. We have the following result due to Auslander and Buchsbaum [1].

**Theorem 5.4.** *Let $L/K$ be a $G$-Galois extension of number fields. Then the corresponding extension $T/R = \mathcal{O}_L\,/\,\mathcal{O}_K$ of rings of integers is a $G$-Galois extension of commutative rings if and only if $L/K$ is unramified as an extension of number fields.*

To prove this theorem, we need to first characterize which prime ideals in $\mathcal{O}_K$ ramify in $L/K$.

**Definitions 5.5.** Let $T/R$ be a ring extension such that $T$ is a free $R$-module with basis $\{e_1, \ldots, e_n\}$. Given $\varphi \in \mathrm{End}_R(T)$, let $(a_{ij})_{ij}$ be the matrix representation of $\varphi$ on the basis $\{e_1, \ldots, e_n\}$. The *trace* of $\varphi$ is defined as

$$\mathrm{tr}(\varphi) = \sum_{i=1}^{n} a_{ii}.$$

For each $x \in T$, let $M_x$ denote the $R$-endomorphism of $T$ given as multiplication by $x$. The *trace* of $x$ relative to $T$ and $R$ is

$$\mathrm{tr}_{T/R}(x) = \mathrm{tr}(M_x).$$

Given any set $x_1, \ldots, x_k \in T$, the *discriminant* of this set is

$$\operatorname{disc}(x_1, \ldots, x_n) = \det(\operatorname{tr}_{T/R}(x_i x_j))_{ij}.$$

The *discriminant* of $T$ over $R$ is the principal ideal of $R$ generated by the discriminant of any basis of $T$ over $R$. We denote this ideal by $D_{T/R}$.

The next proposition gives us a quick way of computing the discriminant.

**Proposition 5.6.** *Let $L/K$ be a finite separable field extension of degree $n$, and let $C/K$ be an algebraically closed field extension with distinct embeddings $\sigma_1, \ldots, \sigma_n$ of $L$ into $C$. Then for any $K$-basis $e_1, \ldots, e_n$ of $L$,*

$$\operatorname{disc}(e_1, \ldots, e_n) = (\det(\sigma_i(e_j))_{ij})^2.$$

*Proof.* This can be verified by computing that

$$\begin{aligned}
\operatorname{disc}(e_1, \ldots, e_n) &= \det(\operatorname{tr}_{T/R}(e_i e_j))_{ij} \\
&= \det\left((\sum_{k=1}^{n} \sigma_k(e_i e_j))_{ij}\right) \\
&= \det\left((\sum_{k=1}^{n} \sigma_k(e_i)\sigma(e_j))_{ij}\right) \\
&= \det((\sigma_k(x_i))_{ik}) \det((\sigma_k(x_j))_{jk}) \\
&= (\det(\sigma_i(e_j))_{ij})^2,
\end{aligned}$$

making use of the multiplicity of the determinant. □

It is a standard result in algebraic number theory that the discriminant ideal $D_{T/R}$ is well defined, i.e., that it does not depend on which $R$-basis of $T$ we choose (if we compute the discriminants of two different bases, they will only differ by a unit in $R$). The following lemma tells us that the prime ideals which ramify in $\mathcal{O}_K$ are exactly the prime factors of the discriminant (a proof can be found in, for example, Theorem 1 in Section 5.3 of [10]).

**Lemma 5.7.** *The prime ideals in $\mathcal{O}_K$ that ramify in $L/K$ are exactly those that divide, i.e., contain, the discriminant of $T/R$.*

In the following proof of Theorem 5.5, we first treat the case where $T$ is a free $R$-module of finite rank. This need not, however, always be the case: if we take $K = \mathbb{Q}[\sqrt{-5}]$ and $L = \mathbb{Q}[\sqrt{-5}, \sqrt{10}]$, then $\mathcal{O}_L$ is not free over $\mathcal{O}_K$.

*Proof.* Let $T = R(t_1, \ldots, t_n)$ be a free $R$-module of rank $n$. Then $T \otimes_R T$ is a free $T$-module on the generators $1 \otimes t_1, \ldots, 1 \otimes t_n$ (with operation on the first factor), and the associated map $h : T \otimes_R T \to \prod_G T$ sending $t_1 \otimes t_2$ to $g \mapsto t_1 \cdot g(t_2)$ is represented as a $T$-module homomorphism by the $n \times n$ matrix

$$M = (g(t_i))_{g,i}$$

for $g \in G$ and $i = 1, \ldots, n$. By Proposition 5.6, $D_{T/R}$ is the ideal generated by $d = (\det M)^2$. By Lemma 5.7, the prime ideals in $\mathcal{O}_K$ which ramify in $L$ are exactly those dividing the discriminant, so $h$ is an isomorphism if and only if $d$, and therefore $\det M$, are units in $R$, that is, if there are no ramified primes. □

To prove the theorem in its generality, we will again make use of localization. Specifically, we need the notion of $S$-integers.

**Definition 5.8.** Let $S$ be a set of nonzero prime ideals of $\mathcal{O}_K$. Then the ring of *S-integers* of $K$ is the set $\mathcal{O}_{K,S} = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}$.

By convention, we allow $v_{\mathfrak{p}}(x) = \infty$ so that 0 lies in $\mathcal{O}_{K,S}$. If $S$ is empty, we take $\mathcal{O}_{K,S} = \mathcal{O}_K$.

The following theorem was proven by Greither in [6].

**Theorem 5.9.** *Let $S$ be a set of prime ideals in $\mathcal{O}_K$ and $S'$ the set of primes in $\mathcal{O}_L$ lying above those in $S$. Then the extension $\mathcal{O}_{L,S'} / \mathcal{O}_{K,S}$ of rings of $S$-integers is $G$-Galois if and only if $S$ contains all the primes that ramify in $L/K$.*

*Proof.* We begin with a more general situation and then adapt it to this particular proof. Let $T$ be an $R$-algebra which is finitely presented as an $R$-module, with a finite group $G$ acting faithfully on $T$ via $R$-algebra automorphisms. Let $\varphi : R \to T$ denote the ring extension map. Localizing at maximal ideals of $R$, we see that $T/R$ is $G$-Galois if and only if $T_{\mathfrak{m}}/R_{\mathfrak{m}}$ is $G$-Galois for all maximal ideals $\mathfrak{m} \subset R$.

We now apply this observation to Theorem 5.9 by letting $R = \mathcal{O}_{K,S}, T = \mathcal{O}_{L,S'}$. There is a one-to-one correspondence between maximal ideals $\mathfrak{m} \subset R$ and maximal ideals $\mathfrak{m} \subset (\mathcal{O}_K) - S$.[3] Note that the localization of $R$ at $\mathfrak{m}$ is just $(\mathcal{O}_K)_{\mathfrak{m}}$. Thus, it suffices to prove that, for all maximal ideals $\mathfrak{m} \subset \mathcal{O}_K$,

$$(\mathcal{O}_L)_{\mathfrak{m}}/(\mathcal{O}_K)_{\mathfrak{m}} \text{ is } G\text{-Galois} \iff \mathfrak{m} \text{ does not ramify in } L/K.$$

From now on, let $R = (\mathcal{O}_K)_{\mathfrak{m}}, T = (\mathcal{O}_L)_{\mathfrak{m}}$. Note that $R$ is local. Let $x_1, \ldots, x_n$ be an $R$-basis of $T$ (this implies that $|G| = [L : K] = n$). Consider the associated map $h : T \otimes_R T \to \prod_G T$. As in the proof of Proposition 3.4, $h$ is represented by the matrix

$$M = (g(x_i))_{g \in G, 1 \leq i \leq n},$$

and $h$ is an isomorphism (that is, $T/R$ is $G$-Galois) if and only if $M$ is invertible. Recalling the trace map $\mathrm{tr} : L \to K, \mathrm{tr}(x) = \sum_{g \in G} g(x)$, we have

$$M^T M = (\mathrm{tr}(x_i x_j))_{ij}.$$

Now the local discriminant $D_{\mathfrak{m},T/R}$ is the $R$-ideal generated by $\det(M^T M)$, which equals the unit ideal if and only if $L/K$ is unramified at $\mathfrak{m}$ (as a consequence of Lemma 5.7, since the only ideal containing the unit ideal is itself). Therefore, the invertibility of $M$ is equivalent to $L/K$ being unramified, so $T/R$ is $G$-Galois if and only if $L$ is unramified over $K$. □

For the interested reader, Rognes also provides a topological account of Galois extensions in [9] based on the theory of regular covering spaces. Without going into detail, the key parallel runs as follows: given a finite discrete group $G$ acting from the right on a compact Hausdorff space $Y$ with the quotient space $X = Y/G$, there is a canonical map

$$\xi : Y \times G \to Y \times_X Y$$

taking $(y, g)$ to $(y, y \cdot g)$, where $Y \times_X Y$ denotes the fiber product of $Y$ with itself. This map is always surjective, and it is a homeomophism if and only if $p : Y \to X$ is a regular covering space, with deck transformation group $G$ acting freely and transitively on each fiber. There is also a parallel notion of $Y$ being *ramified* as a cover of $X$, which is measured by the extent to which $\xi$ fails to be injective.

[3] This is a standard result in localization theory; for a proof, see Chapter 16 of [5].

If we let $R = C(X)$ and $T = C(Y)$ be the rings of continuous (real or complex) functions on $X$ and $Y$, respectively, we obtain a $G$-action on $T$ and a map $R \to T$ which is dual to the orbit projection map $p : Y \to X$. It follows from the isomorphism $C(Y)^G \cong C(Y/G)$ that the map $\xi$ is dual to the homomorphism

$$h : T \otimes_R T \to \prod_G T,$$

so that $\xi$ is an isomorphism if and only if $h$ is an isomorphism. This is the very first step toward constructing the notion of Hopf-Galois extensions.

## Acknowledgments

I would like to thank Peter May for suggesting the topic for this paper and Iris Li for introducing me to the various tools needed for developing a Galois theory of commutative rings. I would not have been able to appreciate the fascinating implications of this idea without their help. I'm also very grateful to Peter May for organizing the REU program in this unusual time, and to all the guest speakers for their engaging lectures.

## References

[1] M. Auslander and D. A. Buchsbaum. On ramification theory in noetherian rings. *Amer. J. Math.*, 81:749–765, 1959.

[2] M. Auslander and O. Goldman. The brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1961.

[3] S. U. Chase, D. K. Harrison, and A. Rosenberg. *Galois theory and Galois cohomology of commutative rings*, volume 52. Mem. Amer. Math. Soc., 1965.

[4] A. W. M. Dress. One more shortcut to galois theory. *Adv. Math.*, 110:129–140, 1995.

[5] D. Dummit and R. Foote. *Abstract Algebra*. John Wiley and Sons, Inc., 2004.

[6] C. Greither. *Cyclic Galois extensions of commutative rings, Lecture Notes in Mathematics*, volume 1534. Berlin: Springer–Verlag, 1992.

[7] N. Johnson. Galois notes, 2010. Online; accessed 12-August-2021. Available at `https://nilesjohnson.net/research/UGA-Galois-notes.pdf`.

[8] M. Knus and M. Ojanguren. *Théorie de la descente et algebres d'Azuyama, Springer Lecture Notes in Mathematics*, volume 389. Springer–Verlag, Heidelberg, 1974.

[9] J. Rognes. Galois extensions of structured ring spectra, 2005. Online; accessed 28-July-2021. Available at `https://arxiv.org/abs/math/0502183v2`.

[10] P. Samuel. *Algebraic theory of numbers*. Hermann ; Kershaw Pub. Co., Paris : London, 1971. Translation of: Théorie algébrique des nombres.