Spring 2014

On Galois theories

Dimitrios Economou
University of Colorado Boulder

University of Colorado Boulder

On Galois theories

Author: Dimitrios Economou
Advisor: Jonathan Wise, Dept. of Mathematics
Honors council representative: Nathaniel Thiem, Dept. of Mathematics
Non-departmental representative: Minhyea Lee, Dept. of Physics

Abstract

The classical Galois theory of fields and the classification of covering spaces of a path-connected, locally path-connected, and semi-locally simply connected space (which will be referred to as the Galois theory of covering spaces) appear very similar. We study the connection of these two Galois theories by generalizing them in categorical language as equivalences of certain categories. This is commonly known as Grothendieck's formulation of Galois theory. These equivalences of categories can then be related to each other by considering covers of Riemann surfaces, providing a link between the Galois theory of fields and the Galois theory of covering spaces. In particular, we find a link between the Galois group in field theory and the fundamental group in topology. We contextualize this link by considering a topological proof of the Abel-Ruffini theorem (the insolvability of quintics).

April 8, 2014

Contents

Introduction

Since antiquity, we have been able to solve for the roots of degree 1 or 2 polynomials. In the 16th century, we worked out how to solve the roots of degree 3 or 4 polynomials using the arithmetic operations and extracting radicals of positive degree as well. It took about three more centuries for us to prove that general degree 5 or higher polynomials could not be solved in such a way. This led to the study of groups and their maps, which are extremely interesting to study in their own right. Proving the unsolvability of degree 5 or higher polynomials (called the Abel-Ruffini theorem) was accomplished by translating properties that encode the solvability of polynomials by radicals into properties of groups, which are easier to work with. This led to classical Galois theory, which connects field theory and group theory.

One can generalize the classical fundamental theorem of Galois theory (the correspondence between subgroups of the Galois group and intermediate fields of a Galois extension) by framing it as an equivalence of categories between algebras and objects that are much easier to work with: sets equipped with a group action. This formulation of Galois theory is typically referred to as Grothendieck's Galois theory (as such, this paper does not give an original formulation but presents it and proves it as we understand it). Further, there is an analogous theory in topology that classifies covering spaces of a base space by (conjugacy classes of) subgroups of the fundamental group of that base space. The classification of covering spaces can also be written in categorical language. These two theories actually share a deep connection. Historically, Grothendieck's Galois theory was formulated in order to define an equivalence of categories for schemes analogous to the one between covering spaces of a locally path-connected and semi-locally simply connected space B and $\pi_1(B)$-sets [**13**]. We can begin to understand that connection by considering branched covers of Riemann surfaces. By connecting these two theories, one can find a topological proof of the Abel-Ruffini theorem, completely analogous to the standard algebraic proof given in most textbooks on abstract algebra (e.g. [**1**]).

The first chapter contains some basic algebraic preliminaries that we use in the categorical Galois theory of field extensions (chapter 5). The second chapter discusses and contains some results about group actions and the category of sets equipped with a group action (and morphisms that respect it). This is the category that we want to translate field extensions (and covering spaces into) because it contains objects and morphisms that are easy to understand. The third chapter is a brief treatment of category theory, the language of which the rest of the paper will be mostly based on. In chapter 4, we generalize field extensions to algebras and begin to rewrite the classical Galois theory of fields in our new language. In chapter 5, we state and prove the categorical Galois theory of fields in the case of finite Galois extensions (there is also a brief discussion of the case of infinite Galois extensions). In chapter 6, we state and prove the categorical Galois theory of covering spaces. We then summarize the treatment of Riemann surfaces and holomorphic maps found in [**8**] (emitting most of the proofs), which gives a connection between the algebraic and topological Galois theories. To conclude, we outline a topological proof of the Abel-Ruffini theorem given in [**11**] as a demonstration of the conceptual power of this connection.

CHAPTER 1

Preliminaries

We expect the reader to be familiar with linear algebra, group theory, and ring theory. We give some of the essentials in this chapter. But first, a few words on notation.

A subset X of a set Y, improper or proper, will be denoted with the symbol $\subset$, as in $X \subset Y$. To distinguish a proper subset P of Y, we will use the symbol $\subsetneq$ as in $P \subsetneq Y$.

1.1. Group Theory

We will always denote any arbitrary group with the letter G.

DEFINITION 1.1. Let G be a group and let H be a subgroup of G. A *left coset* of H by $g \in G$ is the set $gH = \{y \in G \mid \exists h \in H \text{ where } y = gh\} = \{gh \mid h \in H\}$. Similarly a *right coset* of H by $g \in G$ is the set $Hg = \{y \in G \mid \exists h \in H \text{ where } y = hg\} = \{hg \mid h \in H\}$. We will denote the set of all left cosets as G/H and the set of all right cosets as $G\backslash H$. The *index* $[G : H]$ of H in G is defined to be the number of left or right cosets in G/H or $G\backslash H$, respectively. If the number is not finite, the index is infinite.

THEOREM 1.2. Let H be a subgroup of the group G and let $x, y \in G$. Then $xH = yH$ if and only if $x^{-1}y \in H$.

PROOF. ($\Rightarrow$) Suppose $xH = yH$. Then there exists and $h \in H$ such that $y = xh$. Solving for h, we see that $h = x^{-1}y \in H$.
($\Leftarrow$) Suppose that $x^{-1}y \in H$. We need to show that $xH = yH$. Consider $yh \in yH$ for some $h \in H$. Now $yh = xx^{-1}yh = x(x^{-1}y)h \in xH$, because $x^{-1}y \in H$. Thus $yH \subset xH$. On the other hand, consider $xh \in xH$ for some $h \in H$. Now $xh = y(x^{-1}y)^{-1}h \in yH$, so $xH \subset yH$. Therefore $xH = yH$. □

THEOREM 1.3. (Lagrange) Let G be a group and let H be a subgroup of G. Then $\#G = [G : H]\#H = \#G/H\#H$, i.e. the size of a subgroup of a group divides the size of the group by the number of left cosets of H on G.

PROOF. First note that G/H is a partition of G (because congruence modulo a subgroup is an equivalence relation and equivalence relations partition the set...I will add this proof in later) with m left cosets of size n, so that the size of G is mn. Now if $gH \in G/H$, then $\#gH = \#H$. Thus $n = \#H$. Since G/H is a partition of G, $m = \#G/H$. □

Recall that an *automorphism* is an isomorphism from an object to itself. It will be useful to define a set

$$\text{Aut}(X) = \{f : X \to X \mid f \text{ is an automorphism}\}$$

of all automorphisms of an object X.

THEOREM 1.4. Let X be an object. Then $\mathrm{Aut}(X)$ forms a group under composition.

PROOF. We will show that this construction satisfies the group axioms. Let $f, g, h \in \mathrm{Aut}(X)$ and let $x, y \in X$.
(Well-defined) Since the composition of two bijections is a bijection itself, $fg : X \to X$ is a bijection from X to itself. Now we just need to show that is is a homomorphism: $fg(xy) = f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y)) = fg(x)fg(y)$.
(Associativity) The composition of morphisms is associative.
(Identity) The identity morphism is $\mathrm{id}_X : X \to X$ defined by $f(x) = x$ for all $x \in X$, which is clearly an automorphism. The nature of id_X tells us that $f\mathrm{id}_X = \mathrm{id}_X f = f$.
(Inverses) For f, the two-sided inverse is f^{-1}, which exists and is a bijection because f is a bijection by definition. Moreover, f^{-1} is a homomorphism: there are unique elements $a, b \in X$ such that $a = f^{-1}(x)$ and $b = f^{-1}(y)$. Therefore $f(a) = x$ and $f(b) = y$, so $f(ab) = f(a)f(b) = xy$ implies $f^{-1}(x)f^{-1}(y) = ab = f^{-1}(xy)$. □

1.2. Rings and Ideals

In this paper, we will assume that all rings have an additive identity $1 \neq 0$*, unless otherwise noted. We will also assume that ring homomorphisms are* unital*, i.e., if* $\varphi : R \to S$ *is a ring homomorphism, then* $\varphi(1) = 1$*. In this section we will assume that all sums are finite, unless otherwise noted.*

THEOREM 1.5. (Subring Test) Let R be a ring and let $S \subset R$ be a subset of R. Then S is a subring of R if and only if all of these hold:

(1) $S \neq \emptyset$
(2) $\forall x, y \in S : x + (-y) \in S$
(3) $\forall x, y \in S : xy \in S$

There is a natural way to define *direct products* of rings such that the direct product itself is a ring. For two rings R and S, their direct product $R \times S$ is simply the set of all ordered pairs (r, s) such that $r \in R$ and $s \in S$. It is easy to see that we can make $R \times S$ a ring by defining addition and multiplication of elements in it componentwise, and that a map from some ring A to $R \times S$ is a ring homomorphism if and only if $A \to R$ and $A \to S$ are both independently ring homomorphisms.

There is a type of ring element that is invariant under the operation of multiplication in the ring. These elements are useful in describing structures built from rings (such as modules, which we will discuss shortly).

DEFINITION 1.6. An *idempotent* in a ring R is an element[1] $r \in R$ such that $r^2 = r$. An idempotent $r \in R$ is *indecomposable* if $r \neq a + b$ for every nonzero idempotent $a, b \in R$. ←1

DEFINITION 1.7. Let R be a ring. A subring I of R is a *left ideal* of R if I is closed under left multiplication by elements in R. If I is instead closed under right multiplication by elements in R, then I is a *right ideal* of R. If the subring I happens to be closed under both left and right multiplication by elements in R, we say that I is an *ideal* of R.

[1] we will typically care only about the nonzero ones

Ideals can be roughly thought of as generalizing particular subsets of the integers. For example, if we consider the even integers, we might notice that multiplication from any direction by any other integers yields another integer, so that the subring $2\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$. Ideals are important because they come out of ring homomorphisms and they allow us to build quotient rings. So ideals are analogous to normal subgroups.

There are many different types of ideals. Ones we will often see are those which are generated by a certain subset X of R. By this we mean the intersection of a certain collection ideals such that it contains X itself, i.e. the smallest ideal of R containing the subset X. We denote this by (X) and call it the *ideal generated by X*. Of particular importance are those ideals which are generated by a single element:

DEFINITION 1.8. Let R be a ring and let a be an element of R. Then the set

$$aR = \{ar \mid r \in R\}$$

generated by the element $a \in R$ is called the *left principal ideal generated by a*. Similarly,

$$Ra = \{ra \mid r \in R\}$$

is the *right principal ideal generated by a*, and the set of finite sums

$$RaR = \left\{ \sum_i r_i a s_i \mid r_i, s_i \in R \right\}$$

is the *principal ideal generated by a*. We will denote these smallest ideals of R generated by a single element, e.g. by $a \in R$, by (a).

There is a type of ideal that will be useful in our discussion of field theory, which we will now define.

DEFINITION 1.9. Let R be a ring. A proper ideal M of R such that there is no proper ideal N of R where $M \subset N$ is a *maximal ideal*.

There is a certain type of relationship between two ideals that we will use in proving the Chinese Remainder Theorem.

DEFINITION 1.10. Let I and J be ideals of the ring R. The ideals I and J are said to be *comaximal* if $I + J = R$.

LEMMA 1.11. Let I and J be comaximal ideals of a commutative ring R. Define IJ to be the set of all finite sums of elements in I and J, i.e.

$$IJ = \left\{ \sum_i a_i b_i \mid a_i \in I, b_i \in J \right\}.$$

Then IJ is an ideal in $I \cap J$ and $IJ = I \cap J$.

PROOF. To show that IJ is an ideal, we need to check that it is not empty, that it is closed under subtraction, and that it is closed under right and left multiplication by elements in R. Clearly $IJ \neq \emptyset$, because I and J are both not empty. Now for $a_i, c_j \in I$ and $b_i, d_j \in J$,

$$\sum_i a_i b_i - \sum_j c_j d_j = \sum_i a_i b_i + \sum_j (-c_j) d_j \in IJ,$$

so IJ is closed under subtraction. Furthermore, for $a_i \in I$, $b_i \in J$, and $r \in R$, we have both

$$r\left(\sum_i a_i b_i\right) = \sum (r a_i) b_i \in IJ$$

and

$$\left(\sum_i a_i b_i\right) r = \left(\sum_i a_i (r b_i)\right) \in IJ$$

because I and J are ideals of R. Thus IJ is an ideal.

Note that $I \cap J = \{s \mid s \in I \text{ and } s \in J\}$. Consider an arbitrary element $\sum_i a_i b_i \in IJ$. Since $a_i \in I$ and $b_i \in J$, we know that $a_i b_i \in I$ and $a_i b_i \in J$ for all i. In light of the definition of $I \cap J$ defined just above, we can conclude that $\sum_i a_i b_i \in I \cap J$, so that $IJ \subset I \cap J$.

For the reverse inclusion, pick an arbitrary $x \in I \cap J$. Then x is in both I and J. Notice that because I and J are comaximal ideals in R, because $I \cap J$ is an ideal of R, and because R has identity $1 \neq 0$,

$$(I \cap J)(I + J) = (I \cap J)R = I \cap J.$$

Thus we can express any arbitrary element in $I \cap J$ as $x(a + b)$, where $x \in I \cap J$, $a \in I$, and $b \in J$. But $x(a+b) = xa + xb$, which is a finite sum of the form $\sum_i \alpha_i \beta_i$, because I and J are ideals of R. Therefore $x(a + b) \in IJ$, and we deduce that $IJ = I \cap J$. □

LEMMA 1.12. If R is a commutative ring and the k ideals $I_1, ..., I_k$ of R are pairwise comaximal for some integer $k \geq 2$, then $I_1 + I_2 \cdots I_k = R$.

PROOF. The case $k = 2$ is true by assumption. Now suppose that $I_1 + I_2 \cdots I_{k-1} = R$. Then there exists an $a_1 \in I_1$ and an $a \in I_2 \cdots I_{k-1}$ such that $a_1 + a = 1$. If we pick some $b \in I_k$, then we can write $b = (a_1 + a)b = a_1 b + ab \in I_1 + I_2 \cdots I_k$, so $I_1 + I_2 \cdots I_k$ contains both I_1 and I_k, i.e. $R = I_1 + I_k \subset I_1 + I_2 \cdots I_k$. But $I_1 + I_2 \cdots I_k \subset R$, so $I_1 + I_2 \cdots I_k = R$. □

There is a general statement about a given ring and its decomposition into a direct product of its quotient rings with comaximal ideals that will be useful in Galois theory. It is known as the Chinese Remainder Theorem.

THEOREM 1.13. (Chinese Remainder Theorem) Let R be a commutative ring and let $I_1, I_2, ..., I_k$ be ideals of R which are pairwise comaximal ($I_i + I_j = R$ for $i \neq j$). Then the product of the ideals I equals their intersection, i.e. $I = I_1 I_2 \cdots I_k = I_1 \cap \cdots \cap I_k$, and the quotient ring $R/(I)$ is isomorphic to the direct product ring $R/I_1 \times R/I_2 \times \cdots \times R/I_k$.

PROOF. We prove this statement via induction on k. For the base case, $k = 2$, let $I_1 = A$ and $I_2 = B$. Consider the map

$$\varphi : R \to R/A \times R/B$$

defined by $\varphi(r) = (r + A, r + B)$. The maps $\eta : R \to R/A$ and $\zeta : R \to R/B$ are both homomorphisms of rings: for the former, we check that

$$\eta(rs) = rs + A = (r + A)(s + A) = \eta(r)\eta(s),$$

and

$$\eta(r+s) = (r+s) + A = r + s + A + A = (r + A) + (s + A) = \eta(r) + \eta(s).$$

Showing that ζ is a ring homomorphism is similar. So φ itself is a ring homomorphism by the discussion of direct products of rings above. We now show that φ is a surjection. This map must be a surjection due to the fact that the ideals A and B are comaximal, which allows us to find generators of the direct product ring as follows. Since $A + B = R$ and $1 \in R$, there exists elements $a \in A$ and $b \in B$ such that $a + b = 1$. Therefore, since φ is a ring homomorphism,

$$(1, 1) = \varphi(1) = \varphi(a + b) = \varphi(a) + \varphi(b).$$

So we can set $\varphi(a) = (1, 0)$ and $\varphi(b) = (0, 1)$. Now consider an arbitrary element $(r + A, s + B)$ in $R/A \times R/B$. Well

$$\begin{aligned}\varphi(ra + sb) &= \varphi(r)\varphi(a) + \varphi(s)\varphi(b)\\ &= (r + A, r + B)(1, 0) + (s + A, s + B)(0, 1)\\ &= (r + A, 0) + (0, s + B)\\ &= (r + A, s + B),\end{aligned}$$

so φ is surjective.

The kernel of φ is computed to be

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = (r + A, r + B) = (A, B)\} = A \cap B,$$

because the elements r of R which satisfy the system of equations $r + A = A$ and $r + B = B$ are those which are elements of both A and B. But by lemma 1.11, $A \cap B = AB = I$, so we induce an isomorphism

$$R/(I) \cong R/A \times R/B.$$

For the induction step, we just need to show that I_1 and $I_2 \cdots I_k$ are comaximal, which was shown in lemma 1.12. □

1.3. Modules and Tensor Products

A *module* over a ring is the generalization of a vector space, and they generalize the notion of abelian groups. This motivates the following definition:

Definition 1.14. Let R be a ring. A *left R-module* us a set M together with

(1) addition, under which M forms an abelian group
(2) an action of R on M denoted by $r.m$ for all $r \in R$ and $m \in M$, which satisfies
   (a) $(r + s).m = r.m + s.m$
   (b) $r.(m + n) = r.m + r.n$
   (c) $(rs).m = r.(s.m)$
   (d) $1.m = 1$

   for $r, s \in R$ and $m \in M$.

We define a *right R-module* in a similar fashion, except we have the ring R elements appear on the right instead of the left. Note that an R-module is just the generalized structure of a vector space, as a vector space is an R-module such that R is a field. Indeed there are special kinds of modules called *free modules* which are simply

modules with a basis (a linearly independent set that generates the module). Thus every vector space is a free module where the underlying ring is a field.

Also notice that a homomorphism of two left R-modules M and N is a map $f : M \to N$ that preserves addition and left multiplication by R.

The universal way to take a product of two modules to attain a new module (or two vector spaces to yield a new vector space) is by means of the tensor product. The tensor product allows us to go back and forth between bilinear maps and linear maps.

DEFINITION 1.15. Let R be a ring, M be a right R-module, and N be a left R-module. The *tensor product* of M and N over R is an abelian group, denoted $M \otimes_R N$, together with a bilinear map $\otimes : M \times N \to M \otimes_R N$ which satisfies the following universal property: for every abelian group Z and every bilinear map $\varphi : M \times N \to Z$, there is a unique group homomorphism $\psi : M \otimes_R N \to Z$ such that the diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_R N \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\psi} & \\ & Z & \end{array}$$

commutes.

The existence and uniqueness of the tensor product is found in, e.g., [**1**].

Elements in $M \otimes_R N$ are finite sums of objects of the form $m \otimes n$, where $m \in M$ and $n \in N$, which we call *simple tensors*. In light of this, we will often define additive maps out of tensor products by where they take simple tensors. This uniquely defines additive maps because the tensor products are additively spanned by simple tensors. Note that the tensor product is associative[**1**], so we will often omit parentheses. For example, $A \otimes_R (B \otimes_R C) \cong (A \otimes_R B) \otimes_R C$ could just be written as $A \otimes_R B \otimes_R C$.

Given some module over a ring R, we may wish to produce a module over a ring S given some ring homomorphism $R \to S$. Doing so allows us to multiply the new module by more scalars than in the prior one constructed over the ring R. This procedure is termed *extension of scalars*, or *base extension*. An example of such a procedure follows.

EXAMPLE 1.16. For the sake of simplicity, suppose $R \to S$ is a homomorphism of commutative rings. Let M be an R-module. We can attain a bigger module, an S-module, by means of the tensor product. The multiplication rule $S \times (S \otimes_R M) \to S \otimes_R M$ given by

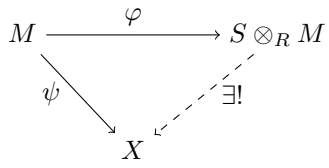
$$(s, \sum_i s_i \otimes m_i) \mapsto \sum_i (ss_i) \otimes m_i$$

gives $S \otimes_R M$ the structure of an S-module. To see that this is well-defined, i.e. independent of the choice of representing elements of $S \otimes_R M$ as sums of simple tensors, notice that the map $S \otimes_R M \to S \otimes_R M$ defined by $a \otimes b \mapsto (sa) \otimes b$ is R-bilinear. By the universal property of bilinear maps, there exists a unique

homomorphism φ_s from $S \otimes_R M$ to itself, sending the simple tensor $a \otimes b$ to $(sb) \otimes b$. Thus $\varphi_s(\sum_i s_i \otimes m_i) = \sum_i \varphi_s(s_i \otimes m_i) = \sum_i (ss_i) \otimes m_i$, and we conclude that the multiplication rule is well-defined. Of course, we also require that this multiplication rule makes $S \otimes_R M$ an S-module, but that is a straightforward check. We will call this module structure on $S \otimes_R M$ the *standard S-module structure*.

Base extension can be characterized with the following universal property that we will make abundant use of.

LEMMA 1.17. (The universal property of base extension.) Let $R \subset S$ be a subring of the ring S. Let M be an R-module. The map $\varphi : M \to S \otimes_R M$ defined by $m \mapsto 1 \otimes m$ is initial among R-linear maps into S-modules. That is, if X is an S-module and $\psi : M \to X$ is R-linear, then there exists a unique (up to isomorphism) S-linear map $S \otimes_R M \to X$ such that the diagram



commutes.

We use the standard S-module structure on $S \otimes_R M$.

PROOF. The map $S \times M \to X$ defined by $(s, m) \mapsto s\psi(m)$ is clearly R-bilinear. By the universal property of bilinear maps, there exists an S-linear map $\gamma : S \otimes_R M \to X$ defined by $s \otimes m \mapsto s\psi(m)$. But γ commutes with φ and ψ because, for an arbitrary $m \in M$, $\varphi \circ \gamma : m \mapsto 1 \otimes m \mapsto 1\psi(m) = \psi(m)$. Thus, the map γ exists, and it is unique in the diagram above because

$$\gamma(s \otimes m) = \gamma(s(1 \otimes m)) = s\gamma(1 \otimes m) = s\psi(m).$$

□

Now let M be a module over the ring R. Note that S is a right R-module through the homomorphism $R \to S$. We have just seen in example 1.16 that the tensor product $S \otimes_R M$ can be considered a left S-module because it admits left multiplication by elements in S (S is a left module over itself and left multiplication by R commutes with left multiplication by S). This brings us to the following statement involving base extension of free modules.

PROPOSITION 1.18. Let R and S be rings. Consider the free R-module R^n and the free S-module S^n. The tensor product $S \otimes_R R^n$ is isomorphic to S^n as left S-modules.

PROOF. See corollary 18 of section 10.4 in [**1**]. □

The remainder of this section consists of lemmas that will come in handy throughout this paper.

LEMMA 1.19. Let F be a nonzero field. If $F^n \cong F^m$ as F-vector spaces, then $n = m$.

PROOF. Suppose $f : F^n \to F^m$ is an isomorphism. Since $\dim_F(\ker f) + \dim_F(\mathrm{im} f) = \dim_F F^n$, we get $m = n$ because f is bijective. □

LEMMA 1.20. Let F be a field and E/F be a field extension. Let V and W be finite dimensional F-vector spaces. Suppose the bases of V and W are the standard bases $\{e_i\}$ and $\{e'_j\}$, respectively. Let $\varphi : V \to W$ be a homomorphism of F-vector spaces. The matrix representing the E-vector space map $E \otimes \varphi : E \otimes_F V \to E \otimes_F W$ in the bases $\{1 \otimes e_i\}$ and $\{1 \otimes e'_j\}$ is equivalent to the matrix representing φ in the bases $\{e_i\}$ and $\{e'_j\}$.

PROOF. Without loss of generality, suppose that $\varphi(e_i) = \sum_j a_{ji} e'_j$, so that the matrix representation of φ is given by (a_{ji}). Now

$$(E \otimes \varphi)(1 \otimes e_i) = 1 \otimes \varphi(e_i) = 1 \otimes \sum_j a_{ji} e'_j = \sum_j a_{ji}(1 \otimes e'_j),$$

so the matrix representing $E \otimes \varphi$ is equals (a_{ji}), the matrix representing φ. □

COROLLARY 1.21. If we have a homomorphism of F-vector spaces $\varphi : V \to W$ and the map $E \otimes \varphi$ as defined in the previous lemma is an isomorphism of F-vector spaces, then φ is an isomorphism of F-vector spaces.

PROOF. This follows from the previous lemma because the matrices of both relevant maps (using the same bases) are the same, together with the fact that if $E \otimes \varphi$ is an isomorphism, its determinant is nonzero, so that that matrix of φ also has a nonzero determinant. Since the determinant of the matrix representing φ is nonzero, the map φ is an isomorphism of F-vector spaces. □

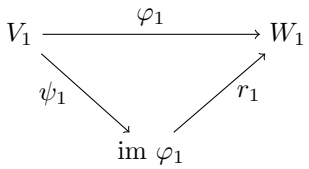
LEMMA 1.22. Let V be a free F-module of rank n. Then $V \to E \otimes V$ given by $v \mapsto 1 \otimes v$ is injective.

PROOF. Choose an F-basis $\{v_i\}$ for V. Then we know that $V \cong F^n$ as F-modules via the map $V \to F^n$ defined by $\sum_i c_i v_i \mapsto (c_i)_i$. By the universal property of bilinear maps, we attain an isomorphism of E-modules $E \otimes V \cong E \otimes F^n$. But $E \otimes F^n \cong E^n$ by theorem 1.18. In particular, the map $E^n \to E \otimes_F V$ defined by $(c_i)_i$ is an isomorphism of E-modules. Furthermore, the map $F^n \to E^n$ defined by $(c_i)_i \mapsto (c_i)_i$ is an injection, because it is injective in each component. Now consider the map $\varphi : V \to E \otimes_F V$ defined by $x \mapsto 1 \otimes x$. With all of the maps defined above, we obtain the commutative diagram

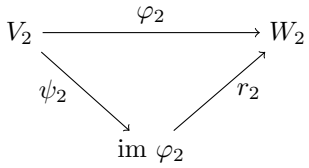
$$\begin{array}{ccc} V & \xrightarrow{\sim} & F^n \\ \varphi \downarrow & & \downarrow \\ E \otimes_F V & \xrightarrow[\sim]{} & E^n \end{array}$$

which forces φ to be injective. □

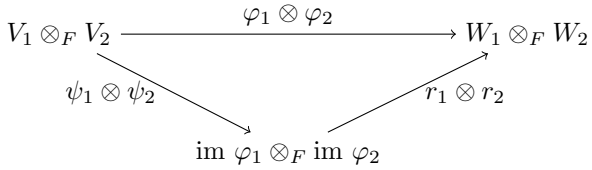
LEMMA 1.23. Let F be a ring, let V_i and W_i be free F-modules, let φ_i be homomorphisms of F-modules, let ψ_i be the natural surjections given by $a \mapsto \varphi_i(a)$, and let r_i be the natural injective maps $a \mapsto a$. If



and



commute, then so does

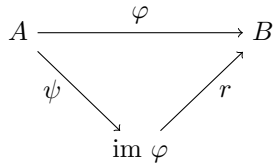


PROOF. This is trivial. □

LEMMA 1.24. Using the same setup as in the previous lemma, we have that $r_1 \otimes r_2$ is injective.

PROOF. If $(r_1 \otimes r_2)(v_1 \otimes v_2) = (r_1 \otimes r_2)(v_1' \otimes v_2')$ then $r_1(v_1) \otimes r_2(v_2) = r_1(v_1') \otimes r_2(v_2')$, which means $v_1 \otimes v_2 = v_1' \otimes v_2'$ be definition of r_1 and r_2. □

LEMMA 1.25. Let A and B be free F-modules and suppose that $\varphi : A \to B$ is F-linear. If (using the same maps as in previous two lemmas)



commutes, then $\ker \varphi = \ker \psi$.

PROOF. Let $a \in \ker \varphi$. Then $0 = \varphi(a) = r(\psi(a))$. But r is injective, so $\psi(a) = 0$, i.e. $a \in \ker \psi$. On the other hand, if $x \in \ker \psi$, then $\psi(x) = 0$. But $\varphi(x) = r(\psi(x)) = r(0) = 0$, so $x \in \ker \varphi$. □

LEMMA 1.26. Suppose R is a commutative ring. Let $N \cong R^n$ be a free R-module of rank n with R-module basis $\{e_i\}$. For any nonzero R-module M, any element of $M \otimes_R N$ can be written uniquely as $\sum_i m_i \otimes e_i$ where $m_i \in M$. In particular, if $\sim_i m_i \otimes e_i = 0$ in $M \otimes_R N$, then $m_i = 0$ for all i.

PROOF. We have an R-bilinear map (easy to check) $M \times N \to M^n$ defined by $(m, \sum r_i e_i) \mapsto (mr_i)_i$, where $(mr_i)_i$ is the n-tuple $(mr_1, \ldots, mr_n)$ and $r_i \in R$. By the universal property of bilinear maps, there exists a unique R-linear map

$\phi : M \otimes_R N \to M^n$ defined by $m \otimes \sum r_i e_i \mapsto (mr_i)_i$. This map has an inverse $\phi^{-1} : M^n \to M \otimes_R N$ defined by $(m_i)_i \mapsto \sum_i m_i \otimes e_i$ (this is easy to check). Therefore $M \otimes_R N \cong M^n$ as R-modules, so that any element in $M \otimes_R N$ can be written as the linear combination of simple tensor described in the lemma statement via the surjectivity of ϕ^{-1}.

If $\sum_i m_i \otimes e_i = 0$, then ϕ sends $\sum_i m_i \otimes e_i$ in $M \otimes N$ to the n-tuple $(m_i)_i = (0, \ldots, 0)$. This equation tells us that $m_i = 0$ for all i. □

LEMMA 1.27. Let V and W be (finite dimensional) F-vector spaces, let s and t be two F-vector space morphisms in $\mathrm{Hom}_F(V, W)$, and let E/F be an extension field. Then

$$E \otimes_F \mathrm{Hom}_F(V, W) \cong \mathrm{Hom}_E(E \otimes_F V, E \otimes_F W).$$

PROOF. Note that the map $\otimes : E \times \mathrm{Hom}_F(V, W) \to E \otimes_F \mathrm{Hom}_F(V, W)$ defined by $(e, f) \mapsto e \otimes f$ for all $e \in E$ and $f \in \mathrm{Hom}_F(V, W)$ is F-bilinear. The set $\mathrm{Hom}_F(V, W)$ together with addition, multiplication, and scaling by F respectively defined by $(f+h)(v) = f(v)+h(v)$, $(fh)(v) = f(v)h(v)$, and $(\lambda f)(v) = \lambda f(v)$ for all $f, h \in \mathrm{Hom}_F(V, W)$ is an F-vector space. In the same way, $\mathrm{Hom}_E(E \otimes_F V, E \otimes_F W)$ is an F-vector space. Now, the map

$$\Psi : E \times \mathrm{Hom}_F(V, W) \to \mathrm{Hom}_E(E \otimes_F V, E \otimes_F W)$$

defined by $(e, \varphi) \mapsto e(E \otimes_F \varphi)$ is F-bilinear. It is straightforward to show this fact, but let's examine the map $e(E \otimes_F \varphi)$ more closely by observing where it takes simple tensors in $E \otimes_F V$. Computing

$$\begin{aligned} e(E \otimes_F \varphi)(e' \otimes v) &= e(e' \otimes \varphi(v)) \\ &= (ee') \otimes \varphi(v) \\ &= (E \otimes \varphi)(ee' \otimes v) \\ &= (E \otimes \varphi)(e(e' \otimes v)), \end{aligned}$$

we see that tensoring allows us to attain an E-linear map (because in addition to the above, both sides respect addition) of E-vector spaces from an F-linear map if F-vector spaces by extending the scalars of both F-vector spaces V and W.

Since Ψ is F-bilinear, by the universal property of bilinear maps, there exists a unique F-vector space homomorphism

$$\Xi : E \otimes_F \mathrm{Hom}_F(V, W) \to \mathrm{Hom}_E(E \otimes_F V, E \otimes_F W)$$

defined by $e \otimes \varphi \mapsto e(E \otimes_F \varphi)$ for all $e \in E$ and $\varphi \in \mathrm{Hom}_F(V, W)$. Choose bases (over F) of V and W to be $\{v_i\}$ and $\{w_j\}$, respectively. Then $E \otimes_F V$ has basis $\{1 \otimes v_i\}$ and $E \otimes_F W$ has basis $\{1 \otimes w_i\}$, each over E. What is an F-basis of $\mathrm{Hom}_F(V, W)$? A possible one is $\{\chi_{ij} : V \to W\}$ where χ_{ij} is defined by $v_i \mapsto w_j$ for a fixed $i \in \{1, \ldots, n\}$ and a fixed $j \in \{1, \ldots, m\}$ and $v_k \mapsto 0$ for all $k \neq i$. Then an E-basis of $E \otimes_F \mathrm{Hom}_F(V, W)$ is $\{1 \otimes \chi_{ij}\}$. Similarly, an E-basis of $\mathrm{Hom}_E(E \otimes_F V, E \otimes_F W)$ is $\{E \otimes \chi_{ij}\}$. Now

$$\begin{aligned} \Xi(1 \otimes \chi_{ij})(1 \otimes v_i) &= (E \otimes_F \chi_{ij})(1 \otimes v_i) \\ &= 1 \otimes \chi_{ij}(v_i) \\ &= 1 \otimes w_j, \end{aligned}$$

and for $k \neq i$ we have

$$\begin{aligned}\Xi(1 \otimes \chi_{ij})(1 \otimes v_k) &= (E \otimes_F \chi_{ij})(1 \otimes v_k) \\ &= 1 \otimes \chi_{ij}(v_k) \\ &= 1 \otimes 0 \\ &= 0.\end{aligned}$$

Therefore, Ξ sends a basis to a basis. It follows that Ξ is an isomorphism. □

COROLLARY 1.28. Let V and W be (finite dimensional) F-vector spaces, let s and t be two F-vector space morphisms in $\mathrm{Hom}_F(V, W)$, and let E/F be an extension field. Suppose that the map

$$E \otimes_F s : E \otimes_F V \to E \otimes_F W$$

defined by $e \otimes v \mapsto e \otimes s(v)$ for all $e \in E$ and $v \in V$, and the map

$$E \otimes_F t : E \otimes_F V \to E \otimes_F W$$

defined by $e \otimes v \mapsto e \otimes t(v)$ for all $e \in E$ and $v \in V$, are equal, i.e. $E \otimes_F s = E \otimes_F t$. Then $s = t$.

PROOF. We will prove this assertion by showing that

$$\mathrm{Hom}_F(V, W) \to \mathrm{Hom}_E(E \otimes_F V, E \otimes_F W),$$

defined by $\varphi \mapsto E \otimes \varphi$, is injective. We will do this by making use of lemma 1.27.

Without loss of generality, we can say that $\dim_F V = n$ and $\dim_F W = m$. Note that $\mathrm{Hom}_F(V, W)$ is an F-vector space of dimension mn, so we have an injection from $\mathrm{Hom}_F(V, W)$ to $E \otimes_F \mathrm{Hom}_F(V, W)$ by lemma 1.22 (let's call it r). Since the composition of injections is an injection itself, the map

$$\Xi \circ r : \mathrm{Hom}_F(V, W) \to \mathrm{Hom}_E(E \otimes_F V, E \otimes_F W)$$

defined by $\varphi \mapsto E \otimes_F \varphi$ is injective, and the corollary statement follows. □

The tensor product of a surjective homomorphism of modules is a surjection, but this is not always the case with injective homomorphisms. Only a certain class of modules respect injections under this operation.

EXAMPLE 1.29. Let p be a prime number. The $\mathbb{Z}$-linear map $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ defined by $n \mapsto q$ is an injection. Consider the $\mathbb{Z}$-module $\mathbb{Z}/p\mathbb{Z}$. If we tensor φ up to $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Z}$, we don't get an injective map. The tensor product in the domain is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, but the codomain collapses to zero. Indeed, if $n \in \mathbb{Z}/p\mathbb{Z}$ and $a \in \mathbb{Q}$, then

$$n \otimes q = n \otimes p(qp/p) = (np) \otimes (q/p) = 0 \otimes (q/p) = 0.$$

This gives an example of an injective map whose tensor product over a module fails to be injective.

This motivates us to consider those modules which, when we take the tensor product of injections with them, give back injections.

DEFINITION 1.30. Let A and B be R-modules, where R is a ring. An R-module M is *flat* if whenever $\varphi : A \to B$ is an injective homomorphism of modules, $M \otimes \varphi : M \otimes_R A \to M \otimes_R B$ is injective.[2] ←2

It turns out that all free modules (hence vector spaces) are flat[3]. ←3

LEMMA 1.31. Every free module is flat.

PROOF. Choose F-basis $\{e_i\}$ for E. By lemma 1.26, we can write any element in $E \otimes_F V$ in the form $\sum_i e_i \otimes v_i$ with $v_i \in V$. Similarly, we can write any element in $E \otimes_F W$ in the form $\sum_i e_i \otimes w_i$ with $w_i \in W$. Let $k \in \ker(E \otimes \varphi)$. Then

$$0 = (E \otimes \varphi)(k) = \sum_i e_i \otimes \varphi(v_i),$$

where we have uniquely written $k = \sum_i e_i \otimes v_i$. Thus each $\varphi(v_i) = 0$ by lemma 1.26. So $v_i = 0$ for all i because φ is assumed to be injective. Therefore $k = 0$, which means that the kernel of $E \otimes \varphi$ contains only zero, i.e. $E \otimes \varphi$ is injective. □

[2]This is typically framed more generally in terms of exact sequences (a flat module over R is an R-module M such that taking the tensor product over R with M preserves exact sequences), but this is equivalent.

[3]More generally, all *projective* modules are flat

CHAPTER 2

Group Actions

2.1. Group Actions

A group is a mathematical structure that can be used to describe symmetries of objects. To formalize this notion, the concept of a group bringing about changes on a set is explored in this chapter. We call this a *group action* on a set and it can be used to reveal the structure of groups by observing how their action adds structure to what they act on. The concept of group actions can also extend beyond actions on sets; we can have actions on general objects. This makes group actions a powerful tool, as we will see when we progress towards Galois theory.

DEFINITION 2.1. Let G be a group and let X be a finite nonempty set. A left *group action* on X is a mapping $\alpha : G \times X \to X$ such that for all $g, h \in G$ and $x \in X$, the following are satisfied:

(1) $\alpha(gh, x) = \alpha(g, \alpha(h, x))$
(2) $\alpha(\mathrm{id}_G, x) = x$

where id_G is the identity element in G. We will denote the G-set above as (X, α). Sometimes the action $\alpha(g, x)$ is written in a simpler fashion as $g.x$ and we say that g acts on x from the left. We can then rewrite the above axioms in the simpler notation as

(1) $(gh).x = g.(h.x)$
(2) $\mathrm{id}_G.x = x$.

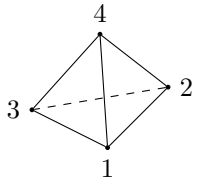
Similarly, a right action of G on X is a mapping $\beta : X \times G \to X$ such that for all $g, h \in G$ and $x \in X$ (using the cleaner notation),

(1) $x.(gh) = (x.g).h$
(2) $x.\mathrm{id}_G = x$.

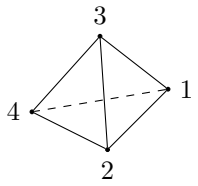
Note that we will use both of these notations throughout this paper.

This definition is a bit abstract, so let's look at an example of a group action with the goal of making them more tangible.

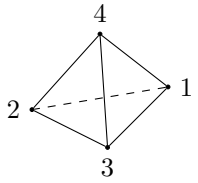
EXAMPLE 2.2. Let $G = A_4$ be the alternating group of four elements and let X be a regular tetrahedron. Label each of the vertices of the tetrahedron with distinct numbers $1, 2, 3$, and 4, as shown below.



Now take a permutation $\sigma \in G$. Then the action of σ on X permutes the vertices while preserving the orientation of the tetrahedron by rotating the tetrahedron around an axis by a certain amount of degrees. For example, the permutation $(12)(34) \in G$ acting on X transforms the tetrahedron so that the vertex 1 and vertex 2 are swapped and the same with 3 and 4:



This is accomplished by rotating the tetrahedron counter-clockwise around the axis that joins the midpoint between 1 and 2 and the midpoint between 3 and 4 by π. As another example, the permutation $(123) \in G$ acting on X rotates the tetrahedron counter-clockwise about the axis joining vertex 4 and the center of the opposing face by $\pi/3$:



The above example reveals that a group action on an object is a description of symmetries of that object, where the information of the object is within a set, and the symmetries are described by the symmetry group of that set. Formally this means that given a group G and a set X, we can get a homomorphism $\varphi : G \to S_X$ where S_X is the symmetric group of set X, and a group action can be thought of as this homomorphism.

Let G be a group and X be a set that G acts on X via α. For all $g \in G$ and $x \in X$, define a mapping $\sigma(g) : X \to X$ where $\sigma(g)(x) = \alpha(g, x)$.

Claim 2.3. We claim that $\sigma(g)$ is in S_X.

Proof. Since $\sigma(g)$ maps X to itself, it suffices to show that $\sigma(g)$ is a bijection. Now, $\sigma(g^{-1})$ is the inverse of $\sigma(g)$ because on one hand $(\sigma(g^{-1})\sigma(g))(x) = \sigma(g^{-1})(\sigma(g)(x)) = \sigma(g^{-1})\alpha(g, x) = \alpha(g^{-1}, \alpha(g, x)) = \alpha(g^{-1}g, x) = \alpha(\mathrm{id}_G, x) = x$ and on the other hand $(\sigma(g)\sigma(g^{-1}))(x) = \sigma(g)(\sigma(g^{-1})(x)) = \sigma(g)\alpha(g^{-1}, x) = \alpha(g, \alpha(g^{-1}, x)) = \alpha(gg^{-1}, x) = \alpha(\mathrm{id}_G, x) = x$. □

We can construct a homomorphism using this that tells us that actions of a group G on X are the same as group homomorphisms from G to S_X.

LEMMA 2.4. Let α be a group action of G on the set X. For $g \in G$, the map $\varphi : G \to S_X$ given by $\varphi(g) = \sigma(g)$ is a homomorphism of groups.

PROOF. Let $g, h \in G$ and consider some $x \in X$. Consider $\varphi(gh) = \sigma(gh)$ and $\varphi(g)\varphi(h) = \sigma(g)\sigma(h)$. Now $\sigma(gh)(x) = \alpha(gh, x) = \alpha(g, \alpha(h, x)) = (\sigma(g)\sigma(h))(x)$, proving the theorem. □

This homomorphism really does provide us with an action α of G on X defined by $\alpha(g, x) = \varphi(g)(x) = \varphi_g(x)$ for all $g \in G$ and all $x \in X$ because $\alpha(g, \alpha(h, x)) = \alpha(g, \varphi_h(x)) = \varphi_g(\varphi_h(x)) = (\varphi_g\varphi_h)(x) = \varphi_{gh}(x) = \alpha(gh, x)$ and $\alpha(e, x) = \varphi_e(x) = \varphi(e)(x) = ex = x$. It will be helpful to think about group actions as permuting elements in a set X, and we have shown that we can get this permutation homomorphism from G to the symmetries of X from some action of G on X and conversely that we can get an action of G on X from some permutation homomorphism from G to the symmetries of X.

Since groups act on sets, they can also act on subsets of themselves.

PROPOSITION 2.5. Let G be a group. Let S be the set of all subsets of G. For any subset $X \in S$ define $g.X = gX = \{gx \mid x \in X\}$ for all $g \in G$. Then this gives a group action $\alpha : G \times S \to S$.

PROOF. We just need to show that the conditions for a group action are satisfied.
(1) $\mathrm{id}_G.X = \mathrm{id}_G X = \{\mathrm{id}_G x \mid x \in X\} = \{x \mid x \in X\} = X$.
(2) $(gh).X = \{(gh)x \mid x \in X\} = \{g(hx) \mid x \in X\} = g.\{(hx) \mid x \in X\} = g.(hX) = g.(h.X)$. □

We can also define a group action on any set of cosets.

EXAMPLE 2.6. Let G be a group and let H be a subgroup of G. Then the mapping $\alpha : G \times G/H \to H$ defined by $\alpha(G, xH) = g.(xH) = (gx)H$ for all $g \in G$ is an action of G on the left cosets of H by x.

PROOF. This result follows directly from proposition 2.5 because xH is a subset of G for all x in G (since G is a group, its operation well-defined). □

Group actions partition sets:

EXAMPLE 2.7. Let G be a group that acts on the nonempty finite set X. Define a relation on X by

$$x \sim y \text{ iff } x = g.y \text{ for some } g \in G.$$

The relation $\sim$ is an equivalence relation.

PROOF. Let $x, y \in X$.
(Reflexive) $x \sim x$ because $1.x = x$.
(Symmetric) Let $x \sim y$. Then there exists a g in G such that $x = g.y$. But $x = g.y \Rightarrow g^{-1}.x = g^{-1}.(g.y) = (g^{-1}g).y = e.y = y$, so $y \sim x$.
(Transitive) Let $x \sim y$ and $y \sim z$. Then $x = g.y$ and $y = h.z$ for some $g, h \in G$. But $x = g.(h.z) = (gh).z$, so $x \sim z$.

□

Example 2.7 tells us that the action of a group on a set partitions the set into disjoint equivalence classes under the action of the group. We call these equivalence classes a certain name:

DEFINITION 2.8. Let G be a group and x be an element in the set X. The *orbit* of x is the set of all elements in X such that there is a $g \in G$ where g acting on x gives the elements. We write it as $\text{Orb}(x) = \{y \in X \mid \exists g \in G \text{ where } g.x = y\}$. This orbit is the equivalence class of x under the action of G on X.

DEFINITION 2.9. Let G be a group and x be an element in the set X. The *stabilizer* of x is the set of all elements in G that fix x when they act on it. We write it as $\text{Stab}(x) = \{g \in G \mid g.x = x\}$.

THEOREM 2.10. Let G be a group and let $x \in X$ be an element in the set X. Then $\text{Stab}(x)$ is a subgroup of G.

PROOF. Since $e.x = x$, $e \in \text{Stab}(x)$, so $\text{Stab}(x) \neq \emptyset$. Let $g, h \in \text{Stab}(x)$. Then $g.x = x$ and $h.x = x$. Thus $x = g.(h.x) = (gh).x$, so $gh \in \text{Stab}(x)$. Finally let $g \in \text{Stab}(x)$. Then $x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.x$, so $g^{-1} \in \text{Stab}(x)$. □

2.2. G-sets

If we have a set together with a group action on it, we attain a work-space in which the group action is important. We give these structures a name:

DEFINITION 2.11. Let G be a group and X be a set. (Note: we will sometimes denote X as X_n where n is the cardinality of the set.) Then the pair (X, α), where α is an action of G on X, is a *G-set*.

DEFINITION 2.12. A G-set is *irreducible* if its group action $\alpha : G \times X \to X$ has exactly one orbit, i.e. for any pair of elements $x, y \in X$ there is a $g \in G$ such that $\alpha(g, x) = y$. If the action satisfies this property, we say that it is *transitive* and that G acts transitively on X.

EXAMPLE 2.13. The action of the group S_n on the set $S = \{1, ..., n\}$ is transitive because given any two elements in S, we can find a permutation in S_n that takes one of the elements to the other. We can find this permutation because the permutations in S_n are bijective maps from S onto itself by definition.

EXAMPLE 2.14. A group G can act on itself by left multiplication, i.e. $g.x = gx$ for all $g \in G$ and $x \in G$. This action is transitive because every element is in the orbit of $g.e$.

We can relate any two G-sets with a mapping between them that respects the action of G. These special kinds of maps are given a name in the following definition and we will see them again and again.

DEFINITION 2.15. Let (X, α) and (Y, β) be two G-sets. A morphism of G-sets from X to Y is a mapping $f : X \to Y$ such that $f(\alpha(g, x)) = \beta(g, f(x))$ for all $g \in G$ and all $x \in X$, i.e. f respects the action on both sides. We will call these morphisms of G-sets *G-equivariant maps*. This can be seen in the following commutative diagram.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ X & \xrightarrow[f]{} & Y \end{array}$$

A G-equivariant map is an *isomorphism of G-sets* if it is bijective.

We will often want to show that a given map is G-equivariant (it respects the G-action. If it so happens that the map under consideration is a bijection, we can choose which direction of the map to show as being G-equivariant, and doing so implies that the other direction is G-equivariant as well. This can come in handy if one direction of the map is difficult to work with.

LEMMA 2.16. A bijection $\varphi : X \to Y$ of G-sets is G-equivariant if and only if its inverse $\varphi^{-1} : Y \to X$ is.

PROOF. ($\Rightarrow$) We simply exploit the fact that φ is bijective, so that it has an inverse φ^{-1} and any $y \in Y$ is $y = \varphi(x)$ for some $x \in X$, to see that $g.\varphi(x) = \varphi(g.x)$ implies $\varphi^{-1}(g.\varphi(x)) = g.x = g.\varphi^{-1}(\varphi(x))$ for all $g \in G$. The other direction is similar. □

Every G-set X is a disjoint union of transitive G-sets (which were the orbits). This is a direct consequence of example 2.7. Let's find some more features. Notice that there is a relationship between the orbits and the stabilizers of different elements, which is described in the following theorem.

THEOREM 2.17. (Orbit-Stabilizer) Let G be a group that acts on a finite set X. Then $\#G = \#\mathrm{Orb}(x)\#\mathrm{Stab}(x)$.

PROOF. Let $x \in X$. Consider the mapping

$$\varphi : G \to \mathrm{Orb}(x)$$

defined by

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

Let $y \in \mathrm{Orb}(x)$. Then there exists a $g \in G$ such that $y = g.x$. Thus $\varphi(g) = g.x = y$, so φ is surjective. We can induce a bijection from this mapping by forcing it to be injective. Let $\varphi(g) = \varphi(h)$. Then $g.x = h.x \Rightarrow g^{-1}.(g.x) = g^{-1}.(h.x) \Rightarrow (g^{-1}g).x = (g^{-1}h).x \Rightarrow e.x = (g^{-1}h).x \Rightarrow (g^{-1}h).x = x \Rightarrow g^{-1}h \in \mathrm{Stab}(x)$. Therefore $g \equiv h (\mathrm{mod}\ \mathrm{Stab}(x))$. It follows that the mapping

$$\varphi : G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)$$

is a bijection. Thus $\#\mathrm{Orb}(x) = \#G/\mathrm{Stab}(x) = [G : \mathrm{Stab}(x)]$. But by theorem 1.3,

$$[G : \mathrm{Stab}(x)] = \frac{\#G}{\#\mathrm{Stab}(x)},$$

which is what we were looking for. □

There is also a precise relationship between the sizes of irreducible G-sets and the sizes of the corresponding groups, as is seen in the next theorem.

THEOREM 2.18. Let (X, α) be an irreducible G-set. Then $\#X$ divides $\#G$.

PROOF. Let $x \in X$. Since (X, α) is an irreducible G-set, G acts transitively on X. By definition 2.12 (transitive action), we know that the orbit of x is the entire set X. It then follows from theorem 2.17 that $\#X\#\mathrm{Stab}(x) = \#G$, i.e. $\#X$ divides $\#G$. □

Consider a group G acting transitively on a set X. If we list out the set of all left cosets of the subgroup $\mathrm{Stab}(x)$ of G for some $x \in X$, we will find that the action of G on X is the same as the action of G on the left cosets of the stabilizer of x, $G/\mathrm{Stab}(x)$, by left multiplication. This allows us to translate transitive actions to actions of G on some left coset space of a subgroup of G in G.

THEOREM 2.19. Let (X, α) be an irreducible G-set, i.e. the action α is transitive. Then the action of G on X is isomorphic to the action of G on $G/\mathrm{Stab}(x)$ by left multiplication for some $x \in X$.

PROOF. Let G act transitively on X. We want to show that this action is the same as the action of G on $G/\mathrm{Stab}(x)$ by left multiplication. To this end, we will find a bijection between X and $G/\mathrm{Stab}(x)$ that respects the actions on both sides. Let $H = \mathrm{Stab}(x)$ for some $x \in X$. Every element in X can be written as gx for some $g \in G$ because G acts transitively on X. Thus the mapping $\varphi : G \to X$ defined by $\varphi(g) = gx$ is surjective. We can induce a bijection from this mapping by considering $\psi : G/H \to X$ defined by $\psi(gH) = gx$. This mapping is well defined because for $g, g' \in G$, we have

$$gH = g'H \Leftrightarrow g^{-1}g \in H \Leftrightarrow gx = g'x.$$

The mapping ψ is still surjective by the above reasoning, so we just need to show that this mapping is injective to show that it is a bijection. Let $\psi(gH) = \psi(g'H)$. Then $gx = g'x \Rightarrow g^{-1}g'x = x \Rightarrow g^{-1}g' \in \mathrm{Stab}(x) \Rightarrow gH = g'H$. Thus ψ is a bijection. ψ respects the action because $\alpha(g', \psi(gH)) = g'\psi(gH) = g'gx$ and on the other hand $\psi(\alpha(g', gH)) = \psi(g'gH) = g'gx$. □

THEOREM 2.20. Let G act on X. Then $\mathrm{Stab}(gx) = g\mathrm{Stab}(x)g^{-1}$ for all $x, y \in X$ and $g \in G$.

PROOF. Let x and $y = g.x$ be two elements in the set X. Suppose $h \in \mathrm{Stab}(y)$. Then by definition $h.y = y$. So $h.(g.x) = g.x \Leftrightarrow g^{-1}(h.(g.x)) = g^{-1}.(g.x) \Leftrightarrow (g^{-1}.((hg).x) = (g^{-1}g).x \Leftrightarrow (g^{-1}hg).x = e.x = x \Leftrightarrow g^{-1}hg \in \mathrm{Stab}(x)$. Therefore $\mathrm{Stab}(gx) \subset g\mathrm{Stab}(x)g^{-1}$. For the other inclusion, suppose that $h \in g\mathrm{Stab}(x)g^{-1}$. Then $(g^{-1}hg).x = x \Leftrightarrow (hg).x = g.x \Leftrightarrow h.(g.x) = g.x \Leftrightarrow h \in \mathrm{Stab}(gx)$. Therefore $g\mathrm{Stab}(x)g^{-1} \subset \mathrm{Stab}(gx)$, and we conclude that $\mathrm{Stab}(gx) = g\mathrm{Stab}(x)g^{-1}$. □

THEOREM 2.21. Let $f : X \to Y$ be a G-equivariant map such that $f(x) = y$. Then $\mathrm{Stab}(x) \subset \mathrm{Stab}(y)$. If f is a bijection, then $\mathrm{Stab}(x) = \mathrm{Stab}(y)$.

PROOF. Let $h \in \mathrm{Stab}(x)$. Then $h.x = x$. Now on one hand $f(h.x) = h.f(x) = h.y$ and on the other hand $f(h.x) = f(x) = y$, so $h.y = y$, i.e. $h \in \mathrm{Stab}(y)$. Thus $\mathrm{Stab}(x) \subset \mathrm{Stab}(y)$.

For the other part of the theorem, suppose that f is a bijection. Then f has an inverse, namely $f^{-1} : Y \to X$ defined by $f^{-1}(y) = x$. This mapping is G-equivariant because on one hand $f^{-1}(f(g.x)) = g.x = g.f^{-1}(y)$ and on the other hand $f^{-1}(f(g.x)) = f^{-1}(g.f(x)) = f^{-1}(g.y)$, so $f^{-1}(g.y) = g.f^{-1}(y)$. Suppose $g \in \mathrm{Stab}(y)$. Then by application of the previous case we get the other inclusion $\mathrm{Stab}(y) \subset \mathrm{Stab}(x)$. Therefore $\mathrm{Stab}(x) = \mathrm{Stab}(y)$. □

LEMMA 2.22. A G-equivariant map is an isomorphism if and only if it is a bijection.

PROOF. This follows directly from the previous theorem and the definition of a G-equivariant map. □

We would like to look at the automorphism group of G-sets. To do so, it will be helpful to characterize when G-equivariant map is an automorphism. In order for a morphism between a left coset space and itself to be an automorphism, the left cosets must coincide with the right cosets.

THEOREM 2.23. Let G be a group and let H be a subgroup of G. Then the mapping $\varphi : G/H \to G/H$ defined by $\varphi(g'H) = g'gH$ is an automorphism if and only if $gHg^{-1} = H$.

PROOF. ($\Rightarrow$) Since φ is a G-equivariant bijection, we know that $\text{Stab}(H) = \text{Stab}(gH) \Leftrightarrow \text{Stab}(H) = g\text{Stab}(H)g^{-1} \Leftrightarrow H = gHg^{-1}$, where we used the fact that $\text{Stab}(H) = H$.
($\Leftarrow$) Suppose that $H = gHg^{-1}$. We need to show that $\varphi : G/H \to G/H$ defined by $\varphi(g'H) = g'gH$ is an automorphism. The mapping φ is well defined, because if we consider two equal cosets $g_1H = g_2H$, we see that on one hand $\varphi(g_1H) = g_1gH = g_1Hg$ and on the other hand $\varphi(g_2H) = g_2gH = g_2Hg = g_1Hg$. It is equivariant because $\varphi(g_0g_1H) = g_0g_1gH = g_0(g_1gH) = g_0\varphi(g_1H)$. The inverse of φ is the mapping $\varphi^{-1} : G/H \to G/H$ defined by $\varphi^{-1}(x) = xg^{-1}$, which can be seen by noting that, for some $g' \in G$, $\varphi^{-1}(g'gH) = g'gHg^{-1} = g'H$. □

Two mappings are the same if they have the same domain and they do the same thing to all elements in the domain. This implies that if we have two automorphisms, one being the mapping $\varphi : G/H \to G/H$ defined by $\varphi(g'H) = g'g_1H$ and the other $\psi : G/H \to G/H$ defined by $\psi(g'H) = g'g_2H$, then $\varphi = \psi$ whenever $g_1^{-1}g_2 \in H$. This requirement follows directly from theorem 1.1. In this case, we want the mappings to take any coset in the domain to the same coset in the codomain, and two cosets gH and $g'H$ are the same whenever $g^{-1}g' \in H$.

Here it will be useful to define a useful set that encapsulates all of the elements which give right and left cosets that coincide.

DEFINITION 2.24. Let H be a subgroup of a group G. The *normalizer* of H in G, written $N(H)$, is the set of all elements in G which commute with H, i.e. $N(H) = \{g \in G \mid gHg^{-1} = H\}$.

THEOREM 2.25. Let G be a group and H be a subgroup of G. Then

$$\text{Aut}_{\text{G-set}}(G/H) \cong N(H)/H.$$

PROOF. Consider the mapping $\Phi : N(H) \to \text{Aut}(G/H)$ defined by $\Phi(g) = \varphi_g$ where $\varphi_g(g'H) = g'Hg^{-1} = g'g^{-1}H$. The mapping Φ is a homomorphism because on one hand $\Phi(gh) = \varphi_{gh}$, where $\varphi_{gh}(g'H) = g'H(gh)^{-1} = g'Hh^{-1}g^{-1}$, and on the other hand $\Phi(g)\Phi(h) = \varphi_g \circ \varphi_h(g'H) = \varphi_g(g'Hh^{-1}) = g'Hh^{-1}g^{-1}$. We also know that Φ is surjective because given some $\varphi_g \in \text{Aut}(G/H)$, we have $\Phi(g) = \varphi_g$ by theorem 2.23. The kernel of Φ is $\text{Ker } \Phi = \{g \in N(H) \mid \Phi(g) = \varphi_e = id\} = \{g \in G \mid gH = H\} = H$. Thus we induce an isomorphism $\tilde{\Phi} : N(H)/H \to \text{Aut}_{\text{G-set}}(G/H)$. □

Groups can act on any kind of mathematical structure, including rings. Here we will provide a natural definition of a group action on a ring, motivated by the fact that we want the group action to respect the ring structure.

DEFINITION 2.26. Let G be a group and let R be a ring. Then the action of G on R acts on the set R in such a way that $\forall g \in G$ and $\forall x, y \in R$,

(1) $g.(x + y) = g.x + g.y$
(2) $g.(xy) = (g.x)(g.y)$
(3) $g.(h.x) = (gh).x$
(4) $g.1 = 1$

THEOREM 2.27. Let G act on a ring R. Then the elements in R that are fixed by the action of G on R, R^G, is a subring of R.

PROOF. $1 \in R^G$ because $g.1 = 1$ for all $g \in G$, so R^G is not empty. Let $x, y \in R^G$. Then there exists a $g \in G$ such that $g.x = x$ and $g.y = y$. Now $g.[x + (-y)] = g.x + g.(-y) = (g.x) + [-(g.y)] = x + (-y)$, so $x + (-y) \in R^G$. Finally $g.(xy) = (g.x)(g.y) = xy$, so $xy \in R^G$. □

An important concept is that of objects which are invariant under a group action:

DEFINITION 2.28. Let G be a group that acts on a set X. Then the subset of elements in X that are fixed by the action of G on X is $X^G \equiv \{x \in X \mid \forall g \in G : g.x = x\}$.

For the following two examples, let $G = \mathrm{Aut}_{\mathbb{R}\text{-algebras}}(\mathbb{C}) = \{\mathrm{id}, \sigma\}$, where $\sigma(a + bi) = a - bi$.

EXAMPLE 2.29. Let G act on the ring of complex numbers $\mathbb{C}$. Then $\mathbb{C}^G = \{z \in \mathbb{C} \mid g.z = z\} = \mathbb{R}$.

CHAPTER 3

Category Theory

Category theory formalizes mathematics as a collection of objects and morphisms (or arrows). It provides a language with which we can use to connect different branches of mathematics.

3.1. Categories

A category is a useful mathematical structure that contains abstract objects and morphisms between them that obey some axioms. We now provide a precise definition below and then provide some examples of categories.

DEFINITION 3.1. A *category* $\mathcal{C}$ is a collection of the following data:

(1) *Objects* $A, B, C, ... \in \text{Ob}(\mathcal{C})$

(2) A class of *morphisms* (or *arrows*) for each ordered pair of objects in $\text{Ob}(\mathcal{C})$. A morphism f from object A to object B is represented by the familiar notation $f : A \to B$ and the class of all morphisms from A to B is written $\text{Hom}_{\mathcal{C}}(A, B)$. *Note*: we will often write the class of morphisms without the subscript of the category when the category is contextually clear.

(3) A rule of composition for any ordered triple of objects in $\text{Ob}(\mathcal{C})$ where if $f \in \text{Hom}_{\mathcal{C}}(A, B)$ and $g \in \text{Hom}_{\mathcal{C}}(B, C)$, then g composed with f is given by $gf : A \to C$. *Note*: we will sometimes use the notation f_{AB} to denote a morphism $f : A \to B$.

(4) For each object $A \in \text{Ob}(\mathcal{C})$ an *identity morphism on* A $\text{id}_A : A \to A$

which are subject to the two axioms listed below:

Axiom 1: Composition of morphisms is associative $(h(gf) = (hg)f)$ if the composites make sense.

Axiom 2: For the identity morphism $\text{id}_B : B \to B$ corresponding to each object B and each of the morphisms $f : A \to B$ and $g : B \to C$, where A and C are also objects, we have (i) $\text{id}_B f = f$ and (ii) $g\ \text{id}_B = g$.

Note: we often won't explicitly write $A \in \text{Ob}(\mathcal{C})$ for objects in $\mathcal{C}$, but rather $A \in \mathcal{C}$ when the meaning is contextually clear.

3.1.1. Examples of Categories. Let's construct some simple categories containing different numbers of objects and morphisms to get an idea of their structure. It is natural to start with a category that contains nothing at all and then add objects and morphisms to it. It is convenient to start constructing these simple categories because the law of composition is always forced.

(1) The empty category contains no objects and no morphisms. The category axioms are trivially satisfied by this category.
(2) The category containing one object and one morphism. The morphism must be the identity morphism for the object. If we call the object A, then the morphism is $\mathrm{id}_A : A \to A$. The composition of morphism $f \in \mathrm{Hom}(A, A)$ with morphism $g \in \mathrm{Hom(A,A)}$ is given by $gf : A \to A$, which is again the identity morphism in the class. It is clear from this that the axioms are satisfied.
(3) The category containing two objects and two morphisms, which are necessarily the identity morphisms corresponding to each object. This is much like the previous example.
(4) The category containing two objects and three morphisms, two of which are the identity morphisms for each object and the third is the morphism from one object to the other. Let A and B be the objects in this category. The classes of morphisms in this category comprise of the identities and the morphism between A and B.

Categories of Familiar Objects and Morphisms.

(1) The category of sets **Set** comprises of all sets in Ob(**Set**) (e.g. $\mathbb{Z}$, $\mathbb{R}$, $\{2, 4, 6, 8, ...\}$, $\emptyset$, etc.) together with a class of morphisms for each ordered pair of sets in Ob(**Set**) which are functions between each ordered pair of sets from a domain to a codomain, a natural rule of composition for any ordered triple of sets where if $f_{AB} \in \mathrm{Hom}(A, B)$ and $g_{BC} \in \mathrm{Hom}(B, C)$, then $gf : A \to C$ is defined by $gf(x) = g(f(x))$ for all $x \in A$, and the identity morphism for a set $A \in \mathrm{Ob}(\mathbf{Set})$ defined by $\mathrm{id}_A(x) = x$ for all $x \in A$.

    To show that the first axiom is satisfied, it is sufficient to show that the composition of functions is associative when it makes sense. Let $A, B, C, D \in \mathrm{Ob}(\mathbf{Set})$. Let $f_{AB} \in \mathrm{Hom}(A, B)$, $g_{BC} \in \mathrm{Hom}(B, C)$, and $h_{CD} \in \mathrm{Hom}(C, D)$ and pick an element $x \in A$. Then $(f(gh))(x) = f((gh)x) = f(g(h(x)))$ and $((fg)h)(x) = (fg)(h(x)) = f(g(h(x)))$, where we see that $f(gh) = (fg)h$. If it turns out that $A = \emptyset$, then this axiom is trivially satisfied. The second axiom will now be shown to be fulfilled by this construction. Let $A, B, C \in \mathrm{Ob}(\mathbf{Set})$ and consider the identity morphism id_B. Consider the functions f_{AB} and g_{BC} in their respective morphism classes. Then by definition of the law of composition for functions in this category, the second axiom is automatically satisfied. An interesting morphism in this category is the *empty function* $\mathrm{id}_\emptyset : \emptyset \to \emptyset$, which is the identity morphism for the empty set $\emptyset$. This morphism is required to exist in order for the category of sets to exist.
(2) The category of groups, **Grp**, comprises of groups as the objects and group homomorphisms as the morphisms. The law of composition of homomorphisms is defined in the usual way as with functions. For any group

$G \in \mathrm{Ob}(\mathbf{Grp})$, there is an identity homomorphism $\mathrm{id}_G : G \to G$ defined by $\mathrm{id}_G(g) = g$. We know this is a homomorphism in $\mathrm{Hom}(G, G)$ because $\mathrm{id}_A(gh) = gh$ while $\mathrm{id}_A(g)\mathrm{id}_A(h) = gh$.

The two axioms are satisfied because composition of functions is associative and there is an identity homomorphism that satisfies the required properties for any group, as shown in the category of sets example.

3.1.2. Types of Morphisms and Objects. If a category had only objects, there would be no interesting structure in it. All of the structure comes from the relationships between the objects, which are the morphisms. As we have seen in the first chapter, there are several different types of morphisms that have distinguishing properties. Perhaps the most natural one is the morphism which allows us to compare the sizes of two collections of objects by defining a one-to-one correspondence between them. Before the concept of counting, we compared sizes of two collections by forming maps between them that have inverses. This type of mapping is called an *isomorphism*.

DEFINITION 3.2. Let $\mathcal{C}$ be a category and let $X, Y \in \mathrm{Ob}(\mathcal{C})$. Then a morphism $f \in \mathrm{Hom}_{\mathcal{C}}$ is an *isomorphism* if there exists a morphism $g : Y \to X$ such that $fg = \mathrm{id}_Y$ and $gf = \mathrm{id}_X$, i.e. g is a two-sided inverse of f.

CLAIM 3.3. Isomorphisms form an equivalence relation on objects.

PROOF. Let X, Y, Z be objects in the category $\mathcal{C}$.
(Reflexive) The morphism $\mathrm{id}_X : X \to X$ is an ismorphism because id_X is its own two-sided inverse. Thus X is isomorphic to X.
(Symmetric) Let $f : X \to Y$ be an isomorphism. Then there is two-sided inverse $g : Y \to X$ of f, which is an isomorphism between Y and X because f is its inverse. Thus if X is isomorphic to Y, then Y is isomorphic to X.
(Transitive) Let $f : X \to Y$ and $g : Y \to Z$ be isomorphisms. Then there are two-sided inverses $f^{-1} : Y \to X$ and $g^{-1} : Z \to Y$. Now $gf : X \to Z$ is an isomorphism because it has a two-sided inverse $f^{-1}g^{-1} : Z \to X$. Thus if X is isomorphic to Y and Y is isomorphic to Z, then X is isomorphic to Z.

□

If $Y = X$, then we say that f is an *automorphism*. Automorphisms are symmetries of their corresponding objects because they map the object to itself while preserving its structure. It will be useful to collect all automorphisms for a given object, which motivates the following definition.

DEFINITION 3.4. Let $\mathcal{C}$ be a category and let X be on object in it. Then the set of all automorphisms of X is written as

$$\mathrm{Aut}_{\mathcal{C}}(X) = \{f : X \to X \in \mathrm{Hom}_{\mathcal{C}}(X, X) \mid f \text{ is an automorphism}\}$$

If we take this set together with composition, we form a group.

THEOREM 3.5. The set $\mathrm{Aut}_{\mathcal{C}}(X)$ of all automorphisms an object X in the category $\mathcal{C}$ forms a group under composition.

PROOF. (Closure) The set $\mathrm{Aut}_{\mathcal{C}}(X)$ is closed under composition because given two automorphisms $f : X \to X$ and $g : X \to X$, we have $fg : X \to X$. Since f and g are both isomorphisms, there exists morphisms $f^{-1} : X \to X$ and $g^{-1} : X \to X$ such that $ff^{-1} = f^{-1}f = gg^{-1} = g^{-1}g = \mathrm{id}_X$. If we consider the composition

$fg : X \to X$, we can find its own two-sided inverse to be $(fg)^{-1} = g^{-1}f^{-1}$. This is a two-sided inverse for fg because for one side we have $fgg^{-1}f^{-1} = ff^{-1} = \mathrm{id}_X$ and for the other side we have $g^{-1}f^{-1}fg = g^{-1}g = \mathrm{id}_X$, where we used the property of the identity morphism of X as a neural element in the compositions. Since fg is an isomorphism in which its codomain coincides with its domain, $fg \in \mathrm{Aut}_{\mathcal{C}}(X)$.
(Associativity) Consider $f, g, h \in \mathrm{Aut}_{\mathcal{C}}(X)$. Then $(fg)h = f(gh)$ because the composition of functions is associative.
(Identities) Since $\mathcal{C}$ is a category, it has the identity morphism id_X that satisfies the desired properties. This identity morphism is in in $\mathrm{Aut}_{\mathcal{C}}(X)$ because it is an automorphism. It is its own two-sided inverse and had the same codomain as its domain.
(Inverses) By the definition of an isomorphism, we know that each automorphism has an inverse that satisfies the desired properties (gives the identity morphism of X when composed from both directions). □

There are also morphisms which are analogous to injective and surjective functions.

Definition 3.6. An *epimorphism* is a morphism $f : X \twoheadrightarrow Y$ such that for all morphisms $g_1, g_2 : Y \to Z$,

$$g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2.$$

A *monomorphism* is a morphism $f : X \hookrightarrow Y$ such that for all morphisms $g_1, g_2 : Z \to X$,

$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2.$$

Monomorphisms are analogous to injective functions while epimorphisms are analogous to surjective functions.

There are some more special objects and morphisms, many of which are generalizations of concepts central to abstract algebra.

Definition 3.7. Let $\mathcal{C}$ be a category. An object $X \in \mathcal{C}$ is said to be *initial* if $|\mathrm{Hom}(Y, X)| = 1$ for all objects $Y \in \mathcal{C}$, and is said to be *final* if $|\mathrm{Hom}(X, Y)| = 1$ for all objects $Y \in \mathcal{C}$.

Example 3.8. The empty set is the initial object in the category of sets. Furthermore, every singleton is a terminal object in this category.

Example 3.9. Let A be a ring and let M and N be A-modules. Consider the category $\mathcal{C} = \{(B, \beta) \mid B \text{ is an } A\text{-module}, \beta : M \times N \to B \text{ is } A\text{-bilinear}\}$ where morphisms between objects in $\mathcal{C}$ are given by

$$\mathrm{Hom}((B, \beta), (B', \beta')) = \{A\text{-modules homomorphisms } \varphi : B \to B' \mid \beta' = \varphi \circ \beta\}.$$

By the universal property of bilinear maps, the initial object of $\mathcal{C}$ is the tensor product, i.e. the pair $(M \otimes_A N, M \times N \to M \otimes_A N : (m, n) \mapsto m \otimes n)$.

Definition 3.10. Let $\mathcal{C}$ be a category. An object X in $\mathcal{C}$ is a *zero object* if it is both initial and final.

If a category $\mathcal{C}$ has a zero object Z, then for any objects $A, B \in \mathcal{C}$, the unique morphisms $A \to Z$ and $Z \to B$ have a composite $0 : A \to B$ called the *zero morphism* from A to B. One reason we care about zero morphisms is that if a

category has zero morphisms, then we can define the notions of kernel and cokernel for all morphisms in that category as follows [**3**].

DEFINITION 3.11. Let $\mathcal{C}$ be a category with zero morphisms. Let $f : X \to Y$ be an arbitrary morphism in $\mathcal{C}$. A *kernel* of f is an object $\ker f$ together with a morphism $k : \ker f \to X$ such that $f \circ k = 0$ is the zero morphism from $\ker f$ to Y and given any morphism $k' : K' \to X$ such that $f \circ k' = 0$, there is a unique morphism $u : K' \to \ker f$ such that $k \circ u = k'$. We see that $\ker f$ is initial in $\mathcal{C}$.

The definition of cokernels is similar to that of kernel.

DEFINITION 3.12. Let $\mathcal{C}$ be a category with zero morphisms. Let $f : X \to Y$ be an arbitrary morphism in $\mathcal{C}$. A *cokernel* of f is an object $\operatorname{coker} f$ together with a morphism $q : Y \to \operatorname{coker} f$ such that $q \circ f = 0$ and given any morphism $q' : Y \to Q'$ such that $q' \circ f = 0$, there is a unique morphism $u : \operatorname{coker} f \to Q'$ such that $u \circ q = q'$. We see that $\operatorname{coker} f$ is final in $\mathcal{C}$.

If R is a ring, the category of R-modules has a zero object (it is the R-module whose underlying abelian group is the trivial group), so we can consider cokernels and kernels in said category. In fact, the category of R-modules is well-behaved in that every morphism in it has a cokernel and a kernel [**3**]. In fact, given some morphism of R-modules $f : M \to N$, the kernel of f is $\ker f$ (in the usual sense as a set of elements in the domain M which are mapped to zero in N) together with the injection $i : \ker f \to M$. Similarly, the cokernel of f is the quotient $N/(\operatorname{im} f)$ together with the surjection $\pi : N \to N/(\operatorname{im} f)$ defined by $x \mapsto x \bmod (\operatorname{im} f)$. We will use these universal properties of kernels and cokernels in the category of R-modules in proving the fundamental theorem of Galois theory.

3.2. Functors

Much like how we relate objects in a category with morphisms, we can think of relations between categories themselves. In particular, we want to consider the morphisms between categories which preserve their structure. We call these relations *functors*.

DEFINITION 3.13. If $\mathcal{C}$ and $\mathcal{D}$ are categories, then a *functor* F from $\mathcal{C}$ to $\mathcal{D}$ is a function that assigns to each $A \in \operatorname{Ob}(\mathcal{C})$ an object $F(A) \in \operatorname{Ob}(\mathcal{D})$, and to each morphism $f \in \operatorname{Hom}_{\mathcal{C}}(A, B)$ a morphism $F(f) \in \operatorname{Hom}_{\mathcal{D}}(F(A), F(B))$, in such a way that

(1) F preserves composition, i.e. $F(fg) = F(f)F(g)$ whenever fg makes sense, and
(2) F preserves identity morphisms, i.e. $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for all $A \in \operatorname{Ob}(\mathcal{C})$.

The definition of a functor is somewhat mysterious, but the idea of functors is that they allow us to convert diagrams in one category into diagrams of another. The importance of this is that we can often translate definitions and theorems in one category into a different category by means of functors. It would be good to look at some examples of functors, so let's do so now.

EXAMPLE 3.14. Given some category $\mathcal{C}$, we have the identity functor, which takes objects in $\mathcal{C}$ to themselves and morphisms in $\operatorname{Hom}(X, Y)$ to themselves. If we call this functor F, consider morphisms $f \in \operatorname{Hom}(B, C)$ and $g \in \operatorname{Hom}(A, B)$, and take an object A in $\mathcal{C}$, we can verify that F is a functor as follows. Since F takes

morphisms to themselves, we have $F(fg) = fg = F(f)F(g)$. We also see that F preserves identity morphisms because on one hand $F(\mathrm{id}_A) = \mathrm{id}_A$ and on the other hand $\mathrm{id}_{F(A)} = \mathrm{id}_A$.

EXAMPLE 3.15. Consider the mapping $F : \mathbf{Grp} \to \mathbf{Set}$ which takes each group G in $\mathbf{Grp}$ to its underlying set and each group homomorphism in $\mathrm{Hom}(G, H)$ to its corresponding mapping between the sets G and H. The mapping F is a functor because it preserves composition and identity morphisms: Given two group homomorphisms $f : B \to C$ and $g : A \to B$, we have $F(fg) = fg = F(f)F(g)$ because f and g are simply mappings between sets with the additional structure of the homomorphism property. We also have that for some group G, $F(\mathrm{id}_G) = \mathrm{id}_G$ because id_G's underlying map of sets is the identity function, and $\mathrm{id}_{F(G)} = \mathrm{id}_G$ because F takes the group G to its underlying set. We can see that this functor disregards some structure of groups, and is showing us that a group is really just a set with some additional structure. We naturally call this type of functor a *forgetful functor*, because the functor forgets some data in the domain category.

EXAMPLE 3.16. Let R be a subring of the ring S, and let $\mathcal{C}$ be the category of R-modules. The map

$$\Gamma = S \otimes_R — : \mathcal{C} \to \mathcal{C}$$

defined by $M \mapsto S \otimes_R M$ and $\varphi \mapsto S \otimes \varphi$ is a functor from the category of R-modules to itself. It is straightforward to check that this satisfies the definition of a functor. Firstly, given to R-module maps $\varphi : M \to N$ and $\psi : N \to Q$, we have

$$\Gamma(\psi\varphi) = S \otimes (\psi\varphi),$$

which sends $s \otimes m \in S \otimes M$ to $s \otimes \psi\varphi(m) = s \otimes \psi(\varphi(m))$. The map Γ also respects identity morphisms because, given an R-module M, we clearly have $\Gamma(\mathrm{id}_M) = \mathrm{id}_{\Gamma(M)}$.

It was mentioned earlier that functors often allow us to translate theorems between different categories (and hence mathematical structures). If we are to come up with a functor between two categories that tells us that the two categories are essentially the same, we might first want the functor to be an isomorphism.

LEMMA 3.17. Functors respect isomorphisms.

PROOF. Obvious. □

DEFINITION 3.18. Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. The categories $\mathcal{C}$ and $\mathcal{D}$ are said to be *isomorphic* if there are functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that FG gives the identity functor on $\mathcal{D}$ and GF gives the identity functor on $\mathcal{C}$.

Although we know that two isomorphic categories are essentially the same, this notion of sameness with isomorphic categories tells us that certain categories which we would like to say are essentially the same are not. It would be nice if we could come up with a weaker notion of categorical sameness, because isomorphism is too strict. Consider an example of two categories which we would like to consider as being essentially the same.

Recall the category $\mathcal{C}$ that has a single object and its identity morphism. We can draw the object (as a dot) and its morphism (as an arrow) like so:

where the arrow is taken to be the identity morphism on the object $\bullet$. Also consider the category $\mathcal{D}$ with two objects (call them 1 and 2) and two non-identity morphisms. We can draw this as (omitting the identity morphisms)

$$1 \underset{f_{21}}{\overset{f_{12}}{\rightleftarrows}} 2$$

where we have given the two non-identity morphisms labels f_{ab} for an arrow going from a to b (thus we will call the identity morphism for 1 and 2 f_{11} and f_{22}, respectively).

Notice that the two objects 1 and 2 in $\mathcal{D}$ are isomorphic because $f_{12}f_{21} = f_{22}$ and $f_{21}f_{12} = f_{11}$. Thus the category $\mathcal{D}$ is essentially the same as category $\mathcal{C}$, since $\mathcal{D}$ has the same structure as $\mathcal{C}$ (the two objects in $\mathcal{D}$ behave in the same way as one object). But $\mathcal{C}$ and $\mathcal{D}$ are not isomorphic categories, because if we were to suppose that they were, we would have a functor $F : \mathcal{C} \to \mathcal{D}$ and a functor $G : \mathcal{D} \to \mathcal{C}$ such that FG gives the identity functor on $\mathcal{D}$ and GF gives the identity functor on $\mathcal{C}$. Thus $FG(f_{11}) = f_{11}$ and $FG(f_{22}) = f_{22}$. But $FG(f_{11}) = F(G(f_{11})) = F(\mathrm{id}_\bullet)$ and $FG(f_{22}) = F(G(f_{22})) = F(\mathrm{id}_\bullet)$, so we have that $f_{11} = f_{22}$, a contradiction. Therefore the two categories $\mathcal{C}$ and $\mathcal{D}$ can't be isomorphic. Nonetheless it would be nice if we could consider $\mathcal{C}$ and $\mathcal{D}$ to be essentially the same, so how should we say that they are?

If we look carefully at the definition of isomorphic categories, we find that the part of it that makes its notion of sameness too strict is the fact that it doesn't care if the objects in a category are isomorphic. In fact, they must be identical. For example, we require that $FG(X) = X$. But we shouldn't care if this composition gives back the same object, but rather any object that is isomorphic to it. So we just need to require that the functors F and G are inverse up to isomorphism. To make this more rigorous, we will now introduce a new type of relationship between two functors.

Definition 3.19. Let F and G be two functors between categories $\mathcal{C}$ and $\mathcal{D}$. A *natural transformation* η from F to G associates to each object X in $\mathcal{C}$ a morphism $\eta_X : F(X) \to G(X)$ between objects in $\mathcal{D}$ such that for all $f : X \to Y$, the diagram

$$\begin{array}{ccc} F(X) & \xrightarrow{F(f)} & F(Y) \\ \Big\downarrow{\scriptstyle \eta_X} & & \Big\downarrow{\scriptstyle \eta_Y} \\ G(X) & \xrightarrow[G(f)]{} & G(Y) \end{array}$$

commutes, i.e. $\eta_Y \circ F(f) = G(f) \circ \eta_X$. If, for each X in $\mathcal{C}$, the morphism η_X happens to be an isomorphism, we call η a natural isomorphism and say that the two functors F and G are *naturally isomorphic*.

We now have a way to weaken our concept of sameness in categories.

DEFINITION 3.20. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. An *equivalence of categories* is a functor $F : \mathcal{C} \to \mathcal{D}$, a functor $G : \mathcal{D} \to \mathcal{C}$, and two natural isomorphisms $\epsilon : FG \to \mathrm{id}_{\mathcal{D}}$ and $\eta : \mathrm{id}_{\mathcal{C}} \to GF$ where we are denoting the identity functors of $\mathcal{C}$ and $\mathcal{C}$ as $\mathrm{id}_{\mathcal{C}}$ and $\mathrm{id}_{\mathcal{D}}$, respectively. Notice that this is like an isomorphism of categories, except we replace the equalities in $GF = \mathrm{id}_{\mathcal{C}}$ and $FG = \mathrm{id}_{\mathcal{D}}$ with the less strict natural isomorphisms $GF \cong \mathrm{id}_{\mathcal{C}}$ and $FG \cong \mathrm{id}_{\mathcal{D}}$, respectively. If the two categories $\mathcal{C}$ and $\mathcal{D}$ have an equivalence of categories, then we say that they are *equivalent*, or "essentially the same", as we have hitherto been calling it.

Let's reconsider the category $\mathcal{C}$ of one object $\bullet$ and its identity morphism $\mathrm{id}_\bullet$ and the category $\mathcal{D}$ of two objects (1 and 2) and its non-identity morphisms f_{12} and f_{21}. We will unpack the definition of an equivalence of categories to see that $\mathcal{C}$ and $\mathcal{D}$ are equivalent.

Consider the two functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that F sends $\bullet$ to 1 and (as an implication of this mapping) $\mathrm{id}_\bullet$ to f_{11}, and G sends every object in $\mathcal{D}$ to $\bullet$ and every morphism in $\mathcal{D}$ to $\mathrm{id}_\bullet$. We need to find two natural isomorphisms $\epsilon : FG \to \mathrm{id}_{\mathcal{D}}$ and $\eta : \mathrm{id}_{\mathcal{C}} \to GF$. To do this, let's begin by writing out the compositions FG and GF explicitly. We begin with the simpler one, GF, which takes $\bullet$ to itself and $\mathrm{id}_\bullet$ to itself, giving the identity functor on $\mathcal{C}$. Thus we can simply use the identity natural isomorphism for η. For ϵ, we need to find both $\epsilon_1 : FG(1) = 1 \to 1$ and $\epsilon_2 : FG(2) = 1 \to 2$ such that both of the non-trivial commutative diagrams commute. It turns out that we must have $\epsilon_1 = f_{11}$ and $\epsilon_2 = f_{12}$, and we quickly see that the two relevant diagrams commute. For the first one we have (evaluating the nodes and arrows)

$$\begin{array}{ccc} 1 & \xrightarrow{f_{11}} & 1 \\ {\scriptstyle f_{11}}\downarrow & & \downarrow{\scriptstyle f_{12}} \\ 1 & \xrightarrow[f_{12}]{} & 2 \end{array}$$

and for the second one we have

$$\begin{array}{ccc} 1 & \xrightarrow{f_{11}} & 1 \\ {\scriptstyle f_{12}}\downarrow & & \downarrow{\scriptstyle f_{11}} \\ 2 & \xrightarrow[f_{21}]{} & 1 \end{array}.$$

We can finally conclude that $\mathcal{C}$ and $\mathcal{D}$ are equivalent.

The problem with the above definition of an equivalence of categories is that in practice, if we have some functor $F : \mathcal{C} \to \mathcal{D}$, it is often a challenge to construct a functor $G : \mathcal{D} \to \mathcal{C}$ such that $GF \cong \mathrm{id}_{\mathcal{C}}$ and $FG \cong \mathrm{id}_{\mathcal{D}}$ (we will call such a functor a *weak inverse*). It is therefore useful to have a more practical characterization of an

equivalence of categories. We will now provide the new characterization and show that it does indeed give an equivalence.

THEOREM 3.21. Let F be a functor $F : \mathcal{C} \to \mathcal{D}$ between two categories. Then F produces an equivalence of categories if and only if it is

(1) *fully faithful*, i.e. given two objects A and B in $\mathcal{C}$, the map $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$ is bijective, and
(2) *essentially surjective*, i.e. each object X in the category $\mathcal{D}$ is isomorphic to an object $F(A)$ for some A in $\mathcal{C}$.

Note that we say the functor is *full* if the map $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$ is surjective, and *faithful* if it is injective.

PROOF. WIP. □

In the discussion of functors, we have assumed that they do not flip morphisms, i.e. for a morphism between two objects A and B, $f : A \to B$, a functor F sends f to $F(f) : F(A) \to F(B)$. But we could just as well have a functor that flips the morphism f so that it gets sent to $F(f) : F(B) \to F(A)$. These types of functors are called *contravariant* functors. To distinguish the functors that flip morphisms from the ones that don't, we call the ones that don't *covariant*. A functor that is not specified as being either covariant or contravariant will be assumed to be covariant. If the functor $F : \mathcal{C} \to \mathcal{D}$ is contravariant, we can always turn it into a covariant functor by reversing all the morphisms in the source category $\mathcal{C}$. This category which is the category $\mathcal{C}$ with all morphisms flipped is called the *opposite category* and we denote it with the symbol $\mathcal{C}^{op}$ (read "C op"). So in this example the functor $F : \mathcal{C}^{op} \to \mathcal{D}$ is covariant. A contravariant equivalence of categories is called an *anti-equivalence*.

EXAMPLE 3.22. Let $\mathcal{C}$ be a category and pick an object $X \in \mathcal{C}$. Then the mapping

$$\mathcal{C}^{op} \to \mathbf{Set}$$

sending the object Y to $\mathrm{Hom}(Y, X)$ and the morphism $A \xrightarrow{\phi} B$ to the morphism $\mathrm{Hom}(B, X) \to \mathrm{Hom}(A, X)$ given by $f \mapsto f \circ \phi$ for each f in $\mathrm{Hom}(B, X)$ is a functor.

Equivalences of categories respect the structures of the categories in question. In particular, equivalences respect monomorphisms:

LEMMA 3.23. Let $F : \mathcal{C} \to \mathcal{D}$ be an equivalence of categories. Then F sends monomorphisms to monomorphisms.

PROOF. Let $f : X \to Y$ be monomorphism in $\mathcal{C}$. We need to show that $F(f) : F(X) \to F(Y)$ is a monomorphism, i.e. for all $g_1, g_2 : D \to F(X)$ in $\mathcal{D}$,

$$F(f) \circ g_1 = F(f) \circ g_2$$

implies $g_1 = g_2$. To this end, let D be an arbitrary object in $\mathcal{D}$ and $g_1, g_2 : D \to F(X)$ be two morphisms in $\mathcal{D}$ such that $F(f) \circ g_1 = F(f) \circ g_2$. Since F is essentially surjective, there exists an object $Z \in \mathcal{C}$ and an isomorphism $\varphi : F(Z) \to D$. Now, F is also full, so there exists morphisms $h_1, h_2 : Z \to X$ such that $F(h_1) = g_1 \circ \varphi$

and $F(h_2) = g_2 \circ \varphi$. Therefore,

$$\begin{aligned} F(f \circ h_1) &= F(f) \circ F(h_1) \quad \because F \text{ is a functor} \\ &= F(f) \circ g_1 \circ \varphi \\ &= F(f) \circ g_2 \circ \varphi \\ &= F(f) \circ F(h_2) \\ &= F(f \circ h_2). \end{aligned}$$

But F is faithful, so $f \circ h_1 = f \circ h_2$, and f is a monomorphism, so $h_1 = h_2$. Hence, $F(h_1) = F(h_2)$, which implies that $g_1 \circ \varphi = g_2 \circ \varphi$. We conclude that $g_1 = g_2$ because φ is an isomorphism. □

A category we will use extensively is the category of G-sets. One can think of the category of G-sets as the category of sets, but with some additional structure added in that must be carried around in the category.

Definition 3.24. Let G be some group. We can construct a category of G-sets G-**set** by taking all of the G-sets together with a class of morphisms for each ordered pair of G-sets (X, α) and (Y, β) defined by $\mathrm{Hom}_{G\text{-}\mathbf{set}} = \{f : X \to Y \mid f(\alpha(g, x)) = \beta(g, f(x))\}$. Recall that these types of morphisms are called G-equivariant maps. We also include a rule of composition for any pair of G-equivariant maps. Say f takes X (having action α) to Y (having action β) and g takes Y to Z (having action γ). Then the rule of composition is defined in the usual way where $gf : X \to Z$ but satisfying $gf(\alpha(h, x)) = \gamma(h, gf(x))$ for some $h \in G$. This follows from the fact that f and g are G-equivariant themselves, so that

$$gf(\alpha(h, x)) = g(f(\alpha(h, x))) = g(\beta(h, f(x))) = \gamma(h, gf(x)).$$

The first axiom is satisfied because the composition of functions is associative when they make sense and the second axiom is also satisfied in the same way as in the example of the category of sets.

If we recall that a transitive left G-set for some group G is isomorphic to the left coset space of G for some subgroup H of G, we may suspect that we can find an equivalence between the category of subgroups of G and the category of transitive left G-sets. It turns out that it this is true if we choose the correct morphisms in the category of subgroups of G. Let $\mathcal{D}$ be the category of transitive left G-sets, where the morphisms are naturally G-equivariant maps, and let $\mathcal{C}$ be the category of subgroups of G. We need to choose the right morphisms between subgroups of G in order for us to find an equivalence between $\mathcal{C}$ and $\mathcal{D}$. It turns out that the class of morphisms we need are

$$\mathrm{Hom}_{\mathcal{C}}(H_1, H_2) = \{\alpha H_2 \in G/H_2 \mid H_1 \alpha H_2 = \alpha H_2\}.$$

We claim that the equivalence of categories F from $\mathcal{C}$ to $\mathcal{D}$ takes any subgroup H to the left coset space G/H and takes any morphism of subgroups $\alpha H_2 : H_1 \to H_2$ to the G-equivariant map φ_α, where $\varphi_\alpha(gH_1) = gH_1\alpha H_2 = g\alpha H_2$.

For this functor to be an equivalence of categories, it must be essentially surjective and fully faithful. We have already proved that this functor is essentially surjective in theorem 2.19, which tells us that for any irreducible G-set X, there exists a

subgroup H of G such that $G/H \cong X$. We just need to check that F is full and faithful. To see that F is full, suppose we have two different left cosets αH_2 and βH_2 such that $F(\alpha H_2) = F(\beta H_2)$. This implies that $\varphi_\alpha = \varphi_\beta \Leftrightarrow \varphi_\alpha(gH_1) = \varphi_\beta(gH_1) \Leftrightarrow gH_1\alpha H_2 = gH_1\beta H_2 \Leftrightarrow g\alpha H_2 = g\beta H_2 \Leftrightarrow \alpha H_2 = \beta H_2$, i.e. the two left cosets have to be the same, and we conclude that F is full. In order for F to be faithful, every $\varphi : G/H_1 \to G/H_2$ must be φ_α for some αH_2. First notice that $\varphi(H_1) = \alpha H_2$ for some $\alpha \in G$. Now on one hand $\varphi(H_1H_1) = H_1\varphi(H_1) = H_1\alpha H_2$ (because φ is G-equivariant) and on the other hand $\varphi(H_1H_1) = \varphi(H_1) = \alpha H_2$, so $H_1\alpha H_2 = \alpha H_2$. We see that $\varphi = \varphi_\alpha$ because for some arbitrary left coset $xH_1 \in G/H_1$, where $x \in G$, we have $\varphi(xH_1) = x\varphi(H_1) = x\alpha H_2 = xH_1\alpha H_2 = \varphi_\alpha(xH_1)$. We have just proved the following statement, which will be used in translating the categorical fundamental theorem of Galois theory to the classical one:

LEMMA 3.25. The category of transitive left G-sets is equivalent to the category of subgroups of G.

There is a useful result about functors that send a fixed object to morphisms from said object in a given category.

LEMMA 3.26. (Yoneda) Let $\mathcal{C}$ be a category, let A be a fixed object in $\mathcal{C}$, and let h_A be the functor $\mathcal{C} \to \mathbf{Set}$ sending objects $B \in \mathcal{C}$ to the set $\mathrm{Hom}_{\mathcal{C}}(A, B)$. Suppose we are given an arbitrary (covariant) functor $F : \mathcal{C} \to \mathbf{Set}$. Then there exists a bijection between the set of natural transformations from h_A to F and $F(A)$, i.e.

$$\mathrm{Nat}(h_A, F) \cong F(A).$$

PROOF. [**3**] □

With Yoneda's lemma, we can learn about a morphism between objects by looking at natural transformations between those objects. This is expressed in the following corollary.

COROLLARY 3.27. In any category, $X \to Y$ is an isomorphism if and only if $\mathrm{Hom}(Y, Z) \to \mathrm{Hom}(X, Z)$ is an isomorphism for every object Z.

CHAPTER 4

Algebras Over Commutative Rings

For this chapter, let R be a commutative ring with identity $1 \neq 0$, unless otherwise noted.

An algebra over a commutative ring is the generalization of an algebra over a field, which is a vector space in which we have a bilinear product, giving the notion of scaling vectors by elements in the field. Therefore one may think of an algebra as a module which also has the structure of a (unital and commutative) ring. Keeping this in mind, we define an algebra over a commutative ring as follows.

DEFINITION 4.1. An *R-algebra* M is an R-module M together with a binary operation $\mu : M \times M \to M$ that is R-bilinear, i.e.

$$r.\mu(m,n) = \mu((r.m),n) = \mu(m,(r.n))$$

for all $r \in R$ and $m, n \in M$, and satisfies the following properties[1]. ←1

The multiplication law is commutative, i.e.

$$\mu(m,n) = \mu(n,m)$$

for all $n, m \in M$.

The multiplication law is also associative, i.e.

$$\mu(\mu(m,n),k) = \mu(m,\mu(n,k))$$

for all $m, n, k \in M$.

The R-module M must also have a unit (identity element), 1, such that

$$\mu(m,1) = \mu(1,m) = m$$

for all $m \in M$.

We will often drop the map μ when it is clear from context. An instance of this notation is seen in the following definition of maps between algebras.

DEFINITION 4.2. Let A and B be R-algebras. A *map of R-algebras* from A to B is a homomorphism of rings

$$\varphi : A \to B$$

such that φ commutes with the R-action, i.e.,

$$\varphi(r.a) = r.\varphi(a)$$

for all $a \in A$ and $r \in R$, φ respects the multiplication law, i.e.,

$$\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$$

[1]Note that one might see these three conditions as respectively making M a *commutative, associative, and unital* R-algebra, but in this paper, when we say R-algebra we really mean an R-module with this particular structure.

for all $a_i \in A$, and φ takes respects the identity in A, i.e. $\varphi(1) = 1$.

EXAMPLE 4.3. Every commutative ring R is an R-algebra. Before we check the conditions, let's think about it intuitively. Since R is a commutative ring, elements in it can be added and subtracted from each other, and we can multiply any element $x \in R$ by any ring element $\lambda \in R$, so an R-action is allowed. This admits an R-bilinear multiplication map when we consider the commutative and associative structure of R.

So if we define the R-action to be left multiplication, i.e. for $r, s \in R$ define $r.s = rs$, we give R an R-module structure, which can be checked as follows. By virtue of the fact that R is a ring, we immediately recover that R is an abelian group under addition, and that for $r_i, s_i \in R$,

(1) $(r_1 + r_2).s = (r_1 + r_2)s = r_1 s + r_2 s$,
(2) $(r_1 r_2).s = (r_1 r_2)s = r_1(r_2 s)$,
(3) $r.(s_1 + s_2) = r(s_1 + s_2) = rs_1 + rs_2$, and
(4) $1.s = 1s = s1 = s$.

All that remains to be shown is that the action is R-bilinear. For $r, s, t \in R$, we have

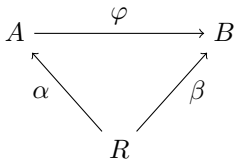
$$r.(st) = r(st) = (rs)t = (r.s)t$$

and since A is commutative,

$$r.(st) = r(st) = (rs)t = (sr)t = s(rt) = s(r.t).$$

There is a more compact description of an R-algebra (and their maps) that is equivalent to definitions 4.1 (and 4.2).

PROPOSITION 4.4. An *R-algebra* is a pair (A, α) where A is a commutative ring and $\alpha : R \to A$ is a homomorphism of commutative rings. A map between R-algebras (A, α) and (B, β) is a ring homomorphism $\varphi : A \to B$ such that the diagram



commutes.

We may consider proposition 4.4 an equivalent definition of R-algebras. We will now show this to be the case, beginning with some lemmas, and build some more intuition for what an R-algebra is along the way.

LEMMA 4.5. If A is an R-algebra (in the sense of definition 4.1), then there exists a unique map of R-algebras $i : R \to A$ defined by $i(r) = r.1$.

PROOF. Let A be an R-algebra. In example 4.3, we saw that R is an R-algebra if we definition the multiplication rule as multiplication in the ring. We will first show that the map i given in the lemma statement is a map of R-algebras.

The map i preserves the multiplication laws in R and A because for any $r, s \in R$,

$$\begin{aligned} i(r)i(s) &= (r.1)(s.1) \\ &= r.(1(s.1)) \\ &= 1(r.(s.1)) \\ &= (rs).1 \\ &= i(rs). \end{aligned}$$

The map φ is a homomorphism of rings because the above holds and for any $r, s \in R$,

$$\begin{aligned} i(r) + i(s) &= r.1 + s.1 \\ &= r + s \\ &= (r + s).1 \\ &= i(r + s). \end{aligned}$$

The map also commutes with the R-action: for any $r, s \in R$, we have

$$\begin{aligned} i(r.s) &= i(rs) \\ &= i(r)i(s) \\ &= (r.1)(s.1) \\ &= r.(1(s.1)) \\ &= r.(s.1) \\ &= r.i(s). \end{aligned}$$

Finally, i takes identity to identity because

$$i(1_R) = 1_R.1_A = 1_A.$$

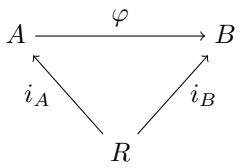
Thus the map i is a map of R-algebras. This map is unique because for any arbitrary $r \in R$, we have

$$i(r) = i(r.1_R) = r.i(1_R) = r.1_A.$$

□

Since the map i in lemma 4.5 is unique and we will use it in the next lemma, let's label it with the respective R-algebra A by i_A.

LEMMA 4.6. Let $\varphi : A \to B$ be a homomorphism of commutative rings where A and B are R-algebras. The map φ is a map of R-algebras in the sense of definition 4.2 if and only if



commutes.

PROOF. ($\Rightarrow$) Pick some element $r \in R$. Then on one hand,

$$\varphi \circ i_A(r) = \varphi(i_A(r)) = \varphi(r.1) = r.\varphi(1) = r.1,$$

and on the other hand, $\varphi_B(r) = r.1$, by lemma 4.5. Thus $\varphi \circ i_A = i_B$.
($\Leftarrow$) Suppose that $\varphi \circ i_A = i_B$. We first show that for all $r \in R$ and $a \in A$, $\varphi(r.a) = r.\varphi(a)$. Well for an arbitrary $r \in R$ and $a \in A$,

$$\begin{aligned}
\varphi(r.a) &= \varphi(r.(1a)) \\
&= \varphi((r.1)a) \\
&= \varphi(r.1)\varphi(a) \\
&= \varphi(i_A(r))\varphi(a) \\
&= i_B(r)\varphi(a) \\
&= (r.1)\varphi(a) \\
&= r.(1\varphi(a)) \\
&= r.\varphi(a).
\end{aligned}$$

Since φ is a homomorphism of rings, we automatically recover the relations

$$\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2),$$

for all $a_i \in A$, and

$$\varphi(1) = 1.$$

Therefore φ is a map of R-algebras. □

LEMMA 4.7. If $p : R \to A$ is a homomorphism of commutative rings, then $r.s = p(r)s$ defines an R-algebra structure on A, in the sense of definition 4.1.

PROOF. Assuming that p is a homomorphism of rings, we need to show that the additional datum of the action distributes from the left and right over addition, is commutative, is associative, is R-bilinear, and that there is an identity $1 \in A$ such that $1a = a1 = a$ for all $a \in A$.

We show these in the order listed:

(1) $r.(a_1 + a_2) = p(r)(a_1 + a_2) = p(r)a_1 + p(r)a_2 = r.a_1 + r.a_2$
(2) $(r_1 + r_2).a = p(r_1 + r_2)a = p(r_1)a + p(r_2)a = r_1.a + r_2.a$
(3) $r.a = p(r)a = ap(r)$
(4) $(r_1 r_2).a = p(r_1 r_2)a = p(r_1)p(r_2)a = r_1.(p(r_2)a) = r_1.(r_2.a)$
(5) $r.(a_1 a_2) = p(r)(a_1 a_2) = (p(r)a_1)a_2 = (r.a_1)a_2$
(6) $p(r)a_1 a_2 = a_1 p(r)a_2 = a_1(r.a_2)$
(7) $1.a = p(1)a = 1a = a = a1 = ap(1)$

□

We are now prepared to prove that proposition 4.4 is an equivalent definition of algebras.

THEOREM 4.8. Proposition 4.4 gives in equivalent characterization of algebras and maps between them as given in definitions 4.1 and 4.2.

We frame this claim as an equivalence of categories as follows. Define the category $\mathcal{C}$ to have pairs (A, i_A) such that A is a commutative ring and $i_A : R \to A$

is a homomorphism of commutative rings, and a morphism class between any two objects in $\mathcal{C}$:

$$\mathrm{Hom}_{\mathcal{C}}((A, i_A), (B, i_B)) = \{\varphi : A \to B \mid \varphi \circ i_A = i_B\}.$$

To encapsulate the default definitions of an R-algebra, we define the category R-alg to be R-modules together with the R-bilinear binary operation given in the definition satisfying the definition's conditions. The morphisms between these R-algebras are the ones given in definition 4.2. We will prove that the map $F : R\text{-alg} \to \mathcal{C}$, which sends the R-algebra B to (B, φ_B), and sends the morphism φ to itself, is an equivalence of categories.

Proof. Let's first check that F is a functor. Consider the morphisms $\varphi \in \mathrm{Hom}_{R\text{-alg}}(A, B)$ and $\psi \in \mathrm{Hom}_{R\text{-alg}}(B, C)$. It is straightforward that

$$F(\psi\varphi) = \psi\varphi = F(\psi)F(\varphi),$$

so F preserves composition. Pick out some R-algebra B. The identity morphism from B to itself is easily seen to be $\mathrm{id}_B : B \to B$ sending $b \in B$ to itself. Note that $F(\mathrm{id}_B) = \mathrm{id}_B$ by definition, so we just need to check that $\mathrm{id}_{F(B)} = \mathrm{id}_B$ to verify F preserves identity morphisms. Well $\mathrm{id}_{F(B)}$ must be a morphism in the class

$$\mathrm{Hom}_{\mathcal{C}}((B, i_B), (B, i_B)) = \{\varphi : B \to B \mid \varphi \circ i_B = \varphi_B\} = \{\mathrm{id}_B\},$$

so that $\mathrm{id}_{F(B)}$ has no choice but to be id_B, and we see that $F(\mathrm{id}_B) = \mathrm{id}_{F(B)}$. We have verified that F is a functor, so we are now free to show that it is an equivalence.

(Full) Let A and B be R-algebras in R-alg. We need to check that the map

$$F : \mathrm{Hom}_{R\text{-alg}}(A, B) \to \mathrm{Hom}_{\mathcal{C}}(F(A), F(B))$$

sending φ to itself is surjective. Let $(\varphi : A \to B) \in \mathrm{Hom}_{\mathcal{C}}((A, i_A), (B, i_B))$. Then $\varphi \circ i_A = i_B$. Therefore φ is an R-algebra map by lemma 4.6, and we have $F(\varphi) = \varphi$.

(Faithful) We need to show that the map F is injective. To this end, suppose that $F(\varphi) = F(\psi)$ for two arbitrary R-algebra maps φ and ψ. Then immediately we have $\varphi = \psi$.

(Essentially surjective) Let $(A, p) \in \mathcal{C}$, where A is a commutative ring and $p : R \to A$ is a homomorphism of commutative rings. We need to find an R-algebra X and an isomorphism in $\mathcal{C}$ such that $F(X) \cong (A, p)$, i.e. $(X, i_X) \cong (A, p)$. Choose $X = A$. Then we are only left with showing that i_A is isomorphic to p. It turns out that they are equal: $r.a = p(r)a$ gives A an R-algebra structure by lemma 4.7, so $i_A(r) = r.1 = p(r)1 = p(r)$, i.e. $i_A = p$. □

In light of the theorem we just proved, we see immediately that there can be many ways to give a commutative ring T an R-algebra structure, depending on what homomorphisms of commutative rings $\{R \to T\}$ we have at our disposal. In particular, if $T = R$, then we can select an R-algebra structure on T from the collection of R-automorphisms.

Example 4.9. As an example of endowing certain objects with an R-algebra structure, consider the polynomial ring $R[x]$. We can give $R[x]$ a natural R-algebra structure via the ring homomorphism $R \to R[x]$ defined by $r \mapsto r.1 = r$, where $r.1$ is the constant polynomial r.

The above example allows us to find a natural bijection between R-algebra homomorphisms from the quotient of a polynomial ring with a polynomial and an arbitrary R-algebra B and the set of roots of that polynomial in said R-algebra B. To see this we will first prove some lemmas. For the remainder of this section, B and C will be R-algebras. Note that for this discussion, R need not be commutative.

LEMMA 4.10. Let $z \in R$ be an element in the the ring R. Then there exists a unique homomorphism of R-algebras, $e_b : R[x] \to B$ defined by $p(x) \mapsto p(b)$. In particular, there is a bijection between B and the R-algebra homomorphisms from $R[x]$ to B.

The homomorphism e_b is suggestively labeled to stand for "evaluation at b".

PROOF. Let $\varphi : R[x] \to B$ be an arbitrary homomorphism of R-algebras sending x to b. We will show that this map has to be e_b. Since φ is a homomorphism of R-algebras, we have (supposing without loss of generality that $p(x)$ is an arbitrary polynomial of degree n with coefficients in R)

$$\begin{aligned}\varphi(p(x)) &= \varphi(r_n x^n + \cdots + r_0) \\ &= \varphi(r_n)\varphi(x)^n + \cdots + \varphi(r_0) \\ &= \varphi(r_n)b^n + \cdots + \varphi(r_0) \\ &= \varphi_B(r_n)b^n + \ldots \varphi_B(r_0) \\ &= e_b(p(x)),\end{aligned}$$

where we used the R-algebra structure on $R[x]$ given above and the respective commutative diagram to find that φ must take the coefficients of p to where $\varphi : R \to B$ in the relevant commutative diagram must take them. It follows that $B \to \mathrm{Hom}_{R\text{-alg}}(R[x], B)$ sending b to e_b is a bijection. □

Notice that if $\pi : B \to B'$ is a homomorphism of R-algebras, then we can attain a map (understanding the homomorphism classes as those belonging to the category of R-algebras)

$$\tilde{\pi} : \mathrm{Hom}(B', C) \to \mathrm{Hom}(B, C)$$

defined by $\theta \mapsto \theta \circ \pi$, for any R-algebra C. It turns out that we can learn about properties of the map $\tilde{\pi}$ be knowing properties of π, which can be easier to know. In particular interest to us is the following lemma.

LEMMA 4.11. If π is surjective, then $\tilde{\pi}$ is injective.

PROOF. Assuming π is surjective, for any $b' \in B'$, there exists a $b \in B$ such that $\pi(b) = b'$. Consider two arbitrary homomorphisms from R-algebra B' to R-algebra C, θ and θ' such that $\theta \circ \pi = \theta' \circ \pi$. Then $\theta(b') = \theta'(b')$ because $\pi(b) = b'$. □

There is one final lemma to consider.

LEMMA 4.12. Let $\pi : B \to B'$ be a surjective homomorphism of R-algebras. Then we have

$$\mathrm{im}\ \tilde{\pi} = \{\theta : B \to C \mid \ker \pi \subset \ker \theta\}.$$

PROOF. Let θ be in the image of $\tilde{\pi}$. We need to show that $\ker \pi \subset \ker \theta$. Since $\theta \mathrm{im}\ \tilde{\pi}$, there exists an R-algebra homomorphism $\theta' : B' \to C$ such that $\theta = \theta' \circ \pi$. Suppose that $k \in \ker \pi$. Then $\theta(k) = \theta' \circ \pi(k) = \theta'(\pi(k)) = \theta'(0) = 0$ because θ' is

a homomorphism of R-algebras.

For the reverse inclusion, assume that $\ker \pi \subset \ker \theta$ for an arbitrary homomorphism of R-algebras $\theta : B \to C$. Consider an arbitrary $b' \in B'$. Then $b' = \pi(b)$ for some b in B because π is surjective by assumption. We need to find a homomorphism of R-algebras $\theta' : B' \to C$ such that $\theta = \theta' \circ \pi$. It would be nice if we could simply use the map $\theta' : B' \to C$ given by $b' \mapsto \theta(b)$ because it automatically satisfies the desired condition, but we need to make sure that it is well-defined. To that end, we first need to check that θ' is a homomorphism of R-algebras. This is easy enough by using the relevant commutative diagrams of π and θ along with the surjectivity of π. Now suppose b_1 and b_2 are two choices in B' for θ', so that $b_1 = b_2$. Then $b_1 - b_2 = 0$, so $b_1 - b_2$ is in the kernel of π. But $\ker \pi \subset \ker \theta$, so $b_1 - b_2$ must also be in the kernel of θ, i.e. $\theta(b_1 - b_2) = 0$. Since θ is a homomorphism of R-algebras, we have $\theta(b_1) = \theta(b_2)$, and we conclude that θ' does not depend on our choice of $b' \in B'$. □

We finally come to the theorem we set off to prove.

THEOREM 4.13. Let $p(x)$ be a polynomial with coefficients in R and let B be any R-algebra. Denote $Y = \mathrm{Hom}_{R\text{-alg}}(R[x]/(p), B)$ and $Z = \{b \in B \mid p(b) = 0\}$. Then there exists a bijection between Y and Z.

PROOF. Consider the map $\pi : R[x] \to R[x]/(p)$ defined by $q(x) \mapsto q(x) \bmod p$. The map π is surjective and its kernel is the ideal generated by p [**1**]. It is a homomorphism of R-algebras because given the homomorphisms of rings $\varphi_{R[x]} : R \to R[x]$ defined by $r \mapsto r.1 = r$ and $\psi : R \to R[x]/(p)$ defined by $r \mapsto r \bmod p$, we have $\psi = \pi \circ \varphi_{R[x]}$. We will use each of the previous three lemmas as follows. It is direct from lemma 4.12 that we know the equality

$$\begin{aligned} \mathrm{im}\ \tilde{\pi} &= \{\theta : R[x]/(p) \to B \mid \ker \pi \subset \ker \theta\} \\ &= \{\theta : R[x]/(p) \to B \mid (p) \subset \ker \theta\} \end{aligned}$$

holds for the R-algebra B. Furthermore, the above map $\tilde{\pi}$ (written now for convenience)

$$\tilde{\pi} : Y \to \mathrm{Hom}(R[x], B)$$

defined by $\theta' \mapsto \theta' \circ \pi$ is injective by lemma 4.11. Now by lemma 4.10, we can associate any homomorphism of R-algebras $\theta : R[x] \to B$ to an element $\alpha \in B$ and vice versa via the bijection given in said lemma, so that $\theta(x) = \alpha$. Considering this arbitrary R-algebra homomorphism θ and recalling that (p)'s underlying set is nothing more than the set of R-multiples of p, we deduce that $(p) \subset \ker \theta$ if and only if $p(x)$ is in the kernel of θ because any multiple of p is killed by θ if and only if θ kills p. So we have $\theta(p(x)) = 0$. But $\theta(p)$ evaluates p at α by the above use of lemma 4.10, so $0 = \theta(p(x)) = p(\alpha)$. Therefore θ is in the image of $\tilde{\pi}$ if and only if $p(\alpha) = 0$, i.e. if and only if α is a root of p. □

As a specific instance of this mapping, consider $R = \mathbb{R}$, $B = \mathbb{C}$, and $p(x) = x^2 + 1$. Let's work out the mapping F and show that it is a bijection. Because $x^2 = -1$ in the quotient ring, we can write every polynomial in it as $a + bx$ for some reals a and b. Now since the homomorphisms in the class $Y = \mathrm{Hom}_{R\text{-alg}}(R[x]/(p), B)$ fix R pointwise, they are determined by where they send x. This is because for some $\varphi \in Y$ we have $\varphi(a + bx) = \varphi(a) + \varphi(b)\varphi(x) = a + b\varphi(x)$. But since we

have a quotient ring of $R[x]$ over the ideal (x^2+1), we know that all multiples of x^2+1 are sent to zero. Thus we have two possible values that φ in G can send x to: i and $-i$, so we have two morphisms in Y given by $\varphi_i(a+bx) = a+bi$ and $\varphi_{-i}(a+bx) = a-bi$, where we have labeled each morphism with a subscript denoting where x is sent. There are two roots of f in $\mathbb{C}$, namely i and $-i$, which gives us the codomain $Z = \{z \in \mathbb{C} \mid p(z) = z^2+1 = 0\} = \{i, -i\}$. Thus if we are given a root $\alpha \in Z$, we have $F(\varphi_\alpha) = \alpha$, and we see that F is surjective. But also if we have $F(\varphi_\alpha) = F(\varphi_\beta)$ for some $\alpha, \beta \in \mathbb{R}$, then $\varphi_\alpha(x) = \varphi_\beta(x)$, so $\alpha = \beta$ because $\mathbb{R}[x]/(x^2+1)$ is generated by 1 and x. We conclude that the mapping F gives a bijection in this specific example.

For a ring R, the tensor product allows us to attain a bigger R-algebra given two R-algebras A and B. All we have to do is take the tensor product of A and B over R, $A \otimes_R B$, and equip it with the multiplication rule

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb').$$

The tensor product $A \otimes_R B$ is an R-module with the standard R-action on the first factor. It can also be shown that the multiplication rule above is R-bilinear, commutative, associative, and takes identity to identity [**5**].

Since tensoring is functorial, it will be useful to characterize R-algebras in terms of tensor products. We will construct such a category of algebras and show that it is equivalent to category R-alg.

Consider the category $\mathcal{C}$ consisting of objects (M, μ, i) where M is an R-module,

$$\mu : M \otimes_R M \to M$$

is an R-linear map, and

$$i : R \to M$$

is an R-linear map, which satisfy the following three commutative diagrams:

(1) The R-linear map μ is commutative, i.e. the following diagram commutes:

$$\begin{array}{ccc} M \otimes_R M & \xrightarrow{\quad c \quad} & M \otimes_R M \\ & {\scriptstyle\mu}\searrow \quad \swarrow{\scriptstyle\mu} & \\ & M & \end{array}$$

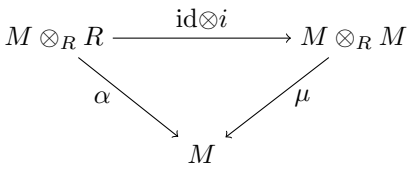
where $c : x \otimes y \mapsto y \otimes x$.

(2) The map μ is associative, i.e.,

$$\begin{array}{ccc} M \otimes_R M \otimes_R M & \xrightarrow{\mu\otimes \mathrm{id}} & M \otimes_R M \\ \downarrow{\scriptstyle \mathrm{id}\otimes\mu} & & \downarrow{\scriptstyle \mu} \\ M \otimes_R M & \xrightarrow[\mu]{} & M \end{array}$$

commutes.

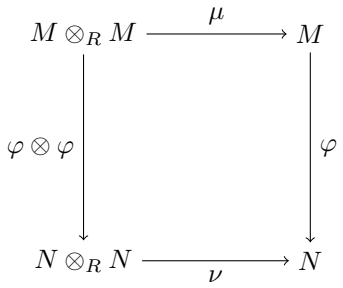
(3) The multiplications rules in R and M are compatible, i.e.,



where $\alpha : a \otimes \lambda \mapsto \lambda a$, commutes.

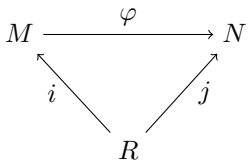
The morphism class of any two objects (M, μ, i) and (N, ν, j) consists of R-module homomorphisms $\varphi : M \to N$ such that the following two properties hold:

(1′) The map φ respects the multiplication rules, i.e.,



commutes.

(2′) The map φ respects the unit maps i and j, i.e.,



commutes.

It is straightforward to check that this collection of objects together with these morphism classes is a category. We will show that $\mathcal{C}$ is equivalent to R-alg as categories. Consider the map

$$\Gamma : R\text{-alg} \to \mathcal{C}$$

sending each object (M, μ) to $(M, \tilde{\mu}, i_M)$, where $\tilde{\mu}$ is the corresponding unique R-linear map that exists by the universal property of bilinear maps, and $i_M : R \to M$ is the unique unit map sending r to $r.1$ given by lemma 4.5. Further, Γ sends each morphism

$$\varphi \in \mathrm{Hom}_{R\text{-alg}}[(M, \mu), (N, \nu)]$$

to the same set theoretic map in $\mathrm{Hom}_{\mathcal{C}}[(M, \tilde{\mu}, i_M), (N, \tilde{\nu}, i_N)]$.

It is straightforward to check that Γ is a functor, so we will now show that it is an equivalence of categories. [2] ←2

LEMMA 4.14. The functor Γ is an equivalence of categories.

PROOF. (Full) Pick an arbitrary φ in $\mathrm{Hom}_{\mathcal{C}}((M,\tilde{\mu},i),(N,\tilde{\nu},j))$. The goal is to find a ring homomorphism from M to N that respects the R-action and the multiplication rule. The corresponding morphism in R-alg is the same set theoretic map φ, which is a homomorphism of rings by lemma 4.6. Since $\varphi \in \mathcal{C}$, we know that

$$\varphi \circ \mu(m_1 \otimes m_2) = \nu \circ (\varphi \otimes \varphi)(m_1 \otimes m_2)$$

for all $m_i \in M$. By the universal property of bilinear maps, there exist unique R-bilinear maps $\tilde{\mu} : M \times M \to M$ and $\tilde{\nu} : N \times N \to N$ such that

$$\begin{array}{ccc} M \times M & \xrightarrow{\text{inclusion}} & M \otimes_R M \\ & {\scriptstyle\mu}\searrow \quad \swarrow{\scriptstyle\tilde{\mu}} & \\ & M & \end{array}$$

and

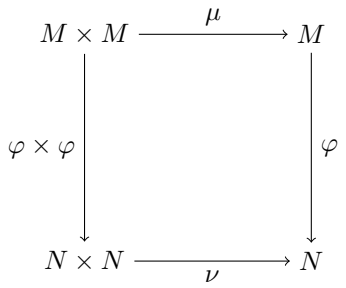
$$\begin{array}{ccc} N \times N & \xrightarrow{\text{inclusion}} & N \otimes_R N \\ & {\scriptstyle\nu}\searrow \quad \swarrow{\scriptstyle\tilde{\nu}} & \\ & N & \end{array}$$

commute. Notice that the diagram

$$\begin{array}{ccccc} M \times M & \xrightarrow{\text{inc.}} & M \otimes_R M & \xrightarrow{\tilde{\mu}} & M \\ \downarrow{\scriptstyle\varphi\times\varphi} & & \downarrow{\scriptstyle\varphi\otimes\varphi} & & \downarrow{\scriptstyle\varphi} \\ N \times N & \xrightarrow[\text{inc.}]{} & N \otimes_R N & \xrightarrow[\tilde{\nu}]{} & N \end{array}$$

commutes. Since the outer rectangle commutes if and only if the left and right rectangles commute, we conclude that

[2] What we're doing here is showing that R-algebras are the monoid objects in the category R-mod.



commutes, from which we know that φ respects the multiplication rules μ and ν.

Finally, notice that

$$\varphi(\mu(m, r.1)) = \nu(\varphi(m), \varphi(r.1)) = \nu(\varphi(m), r.1),$$

so φ respects the R-action.

(Faithful) Obvious.

(Essentially surjective) Pick an arbitrary $(M, \tilde{\mu}, i)$ in $\mathcal{C}$. We have automatically that M is an R-module. By composition with the inclusion $M \times M \to M \otimes_R M$, there exists a unique F-bilinear map $\mu : M \times M \to M$.

We need to check that μ is commutative. Consider the maps $c : M \otimes M \to M \otimes M$ defined by $m_1 \otimes m_2 \mapsto m_2 \otimes m_1$, $c' : M \times M \to M \times M$ defined by $(m_1, m_2) \mapsto (m_2, m_1)$, and the inclusion $u : M \times M \to M \otimes M$. Notice that $c \circ u = u \circ c'$ and $\tilde{\mu} \circ c = \tilde{\mu}$. From this we deduce that $\mu \circ c' = \mu$.

We also need to show that μ is associative. By using the commutative diagram (2) in the construction of the category $\mathcal{C}$ above the theorem statement, and composing $\tilde{\mu}$ with the inclusion $M \times M \to M \otimes M$, we obtain the corresponding commutative diagram to (2), with direct products instead of tensor products and in terms of the unique F-bilinear map μ.

Note that $i(1) = 1_M$. By using the commutative diagram (3), the isomorphism $M \cong M \otimes_R R$ defined by $m \mapsto m \otimes 1$, and the fact that $\tilde{\mu}$ is commutative, we obtain that

$$\tilde{\mu}(1 \otimes m) = \tilde{\mu}(m \otimes 1) = 1.m = m$$

for all m. This implies that

$$\mu(1, m) = \mu(m, 1) = m$$

for all $m \in M$.

Now, the map $\psi : M \to M$ sending m to itself is clearly an isomorphism in $\mathcal{C}$ that satisfies $(1')$ and $(2')$. Therefore, Γ is essentially surjective. □

4.1. Group Actions on Algebras

Let G be a group that acts on the commutative ring E. Similar to how we took sets and included G-actions with them to create G-sets, we can take E-algebras (where E is a commutative ring) together with G-actions to create what we will call G-E-algebras. Of course, we would like the action of G on E-algebras to be defined in such a way that the G-action and E-action (scaling by elements in E) interact nicely (look for the word compatible in the upcoming definition). Doing

so intertwines the E-action and G-action in a useful way, and will allow us to learn about the E-algebra structure.

Let's begin with defining a way we can have a group G of automorphisms of E act on any E-module.

DEFINITION 4.15. Let B be an E-module and pick some $\sigma \in G$. A *σ-E-linear map* $s : B \to B$ is an additive map such that $s(\lambda b) = \sigma(\lambda)s(b)$ for every $\lambda \in E$ and $b \in B$.

We require the map to be additive so that can attain a group action on a ring structure. Notice that the scaling of the E-module B is twisted by the group action when a σ-E-linear map is applied. From now on, we will adopt the notation where s is labeled with σ itself. This is similar to how we wrote a G-action on a set X as $g.x$ as opposed to a map $\varphi_g(x)$. Furthermore, we will write the G-action as a left superscript and the E-action with a dot. We will generally use this left superscript notation for the G-action whenever we find it with the E-action in the same place, and dots for either whenever they are alone. Putting these notations together, we see that a σ-E-linear map on an E-module B is given by ${}^{\sigma}(\lambda.b) = ({}^{\sigma}\lambda).({}^{\sigma}b)$, and we will think of such a map as a G-action on B. We would like to stress that $\sigma(b)$ is not strictly correct since σ is an automorphism of E, but is a harmless convenience of notation. This shouldn't be confusing because every σ-E-linear map is associated to its own $\sigma \in G$.

We can extend the G-action on E to a G-action on any E-module by giving ourselves the freedom to use any $\sigma \in G$ in such a way that defines a G-action on a ring (definition 2.26).

DEFINITION 4.16. Let E be a commutative ring. A *G-E-algebra*[3] is an E-algebra (B, β) together with a set of σ-E-linear maps $\{s_\sigma\}_{\sigma \in G}$, such that for each $\sigma \in G$, $s_{\mathrm{id}} = \mathrm{id}_B$ and $s_\sigma \circ s_\tau = s_{\sigma\tau}$[4]. The set together with these conditions will be called a *G-E-module structure*. It will be useful to give the underlying E-module together with the G-action with the above compatibility a name. Naturally, let's call it a *G-E-module*. ←3 ←4

We now give an example of a G-E-module.

EXAMPLE 4.17. Let V be an F-vector space and consider an automorphism of E $\sigma \in G$. The map

$$s_\sigma : E \otimes_F V \to E \otimes_F V$$

defined by $x \otimes v \mapsto {}^{\sigma}x \otimes v$ is σ-E-linear. We see that s_σ is E-linear by the universal property of base extension (lemma 1.17) (and is hence independent of our choice of simple tensors). Note that we are using the standard E-module structure on $E \otimes_F V$, where E acts on the first factor (example 1.16). Now let $\lambda \in E$ and

[3]The naming of this term is inspired by how we endowed any set with a G-action to make a G-set.

[4]The combination of these two conditions, together with the fact that σ-E-linear maps are additive, gives us a G-action on any E-module. The first condition requires id-E-linear maps to behave like the identity on any E-module B, and the second condition requires the σ-E-linear maps to be associative.

observe that

$$\begin{aligned}{}^{\sigma}(\lambda.(x\otimes v)) &= {}^{\sigma}((\lambda x)\otimes v), \quad \text{by standard } E\text{-action}\\ &= {}^{\sigma}(\lambda x)\otimes v\\ &= {}^{\sigma}\lambda.({}^{\sigma}x\otimes v)\\ &= {}^{\sigma}\lambda.{}^{\sigma}(x\otimes v).\end{aligned}$$

Hence s_σ is σ-E-linear.

Now, if we take the E-module $E\otimes_F V$ together with the set $\{s_\sigma\}_{\sigma\in G}$, we get a G-E-module. The two conditions to verify this are given as follows. The identity behaves as expected for all simple tensors because

$$\begin{aligned}{}^{\mathrm{id}}(x\otimes v) &= {}^{\mathrm{id}}x\otimes v\\ &= x\otimes v\\ &= \mathrm{id}(x\otimes v),\end{aligned}$$

and s_σ is associative because

$$\begin{aligned}{}^{\sigma\tau}(x\otimes v) &= ({}^{\sigma\tau}x)\otimes v\\ &= ({}^{\sigma}({}^{\tau}x))\otimes v\\ &= {}^{\sigma}({}^{\tau}(x\otimes v)).\end{aligned}$$

We will call this structure the *standard G-E-module structure* on $E\otimes_F V$.

Looking back at definition 4.1, notice that we defined an E-algebra as an E-module V together with an E-linear multiplication map $V\otimes_E V\to V$ that is associative. So for G-E-algebras, what does it mean to tensor over G-E in the associative G-E-linear multiplication map $V\otimes_{G\text{-}E} V\to V$, where V is a G-E-module? We handle this in the same we handle G-sets[5]: if A and B are two G-E-modules, then $A\otimes_{G\text{-}E} B$ is the pair $(A\otimes_E B,\alpha)$, where the G-action α acts on both factors, i.e. $g.(a\otimes b)=(g.a)\otimes(g.b)$ for all $a\in A$ and $b\in B$. ←5

Lemma 4.18. Suppose that B is a G-E-algebra and let $f:E\to B$ be a map of E-algebras. Then f is G-equivariant, i.e. ${}^{g}f(y)=f({}^{g}y)$.

Proof. Since f is a map of E-algebras, $f(x)=x.1$. Thus $f({}^{g}x)=({}^{g}x).1=({}^{g}x).({}^{g}1)={}^{g}(x.1)={}^{g}f(x)$. □

Let E^X denote the set of all functions from X to E. We have a natural E-action on E^X which is simply scaling by E, i.e. the mapping $E\times E^X\to E^X$ defined by $(\lambda.f)(x)=\lambda f(x)$ for $\lambda\in E$, $f\in E^X$, and $x\in X$ is an E-action on E^X. It is straightforward to check that the map $E\to E^X$ defined by $\lambda\mapsto\underline{\lambda}$, where $\underline{\lambda}$ is the constant function sending every $x\in X$ to λ, gives E^X an E-algebra structure. But we can also define a G-action on the set of functions E^X as follows (we will define the G-action in the following lemma statement and prove that it is in fact a G-action).

[5]This can be more rigorously framed in terms of topoi (singular: topos), which can informally be thought of as frameworks in which we do mathematics. Omitting the detail, topois are types of categories. For example, the category of G-sets is an alternative topos to the category of sets, and the category of G-E-algebras is an alternative topos to the category of E-algebras.

LEMMA 4.19. Let E be a commutative ring and X be a finite G-set. Suppose that $g \in G$, $x \in X$, and $f \in E^X$. Then the mapping $G \times E^X \to E^X$ defined by ${}^g f(x) = g.f(g^{-1}.x)$ is a G-action on E^X.

PROOF. Let $1 \in G$ be the identity element in the group G. We have

$$\begin{aligned}(1.f)(x) &= 1.(f(1^{-1}.x)) \\ &= 1.f(1.x) \\ &= 1.f(x) \\ &= f(x),\end{aligned}$$

where we used the fact that X and E are G-sets. Thus the action of the identity element behaves as desired. Furthermore, given two group elements $g, h \in G$, we have

$$\begin{aligned}(g.(h.f))(x) &= g.((h.f)(g^{-1}.x)) \\ &= g.(h.f(h^{-1}.(g^{-1}.x))) \\ &= (gh).f((h^{-1}g^{-1}).x) \\ &= (gh).f((gh)^{-1}.x) \\ &= ((gh).f)(x),\end{aligned}$$

so that the mapping is associative. □

LEMMA 4.20. If a group G acts on a commutative ring E and a finite set X, then the set of all maps from X to E, denoted E^X, is a G-E-algebra.

Here we define the (left) E-action on E^X to be scaling, i.e. for $f \in E^X$ and $\lambda \in E$, define $(\lambda.f)(x) = \lambda f(x)$, and the (left) G-action by lemma 4.19. Here we say that the action of G on E^X *extends* the action of G on E.

PROOF. If we define addition and multiplication of elements $a, b \in E^X$ by $(a+b)(x) = a(x)+b(x)$ and $(ab)(x) = a(x)b(x)$, respectively, it is easy to check that E^X together with these operations is a commutative ring. The ring homomorphism that gives E^X an E-algebra structure is the constant function $u : E \to E^X$ defined by $\lambda \mapsto \underline{f}$ where $\underline{f}(x) = \lambda$ for all $x \in X$. Given all of the data up until now, (E^X, u) is an E-algebra. If we take this together with the left G-action on E^X given above, we get a G-E-algebra, because the E-action and G-action are compatible, i.e. for $\lambda \in E$, $g \in G$, $f \in E^X$, and $x \in X$, we have

$$\begin{aligned}{}^g(\lambda.f)(x) &= {}^g((\lambda.f)({}^{g^{-1}}x)) \\ &= {}^g(\lambda f({}^{g^{-1}}x)) \\ &= ({}^g\lambda)({}^g(f({}^{g^{-1}}x))) \\ &= {}^g\lambda({}^g f(x)) \\ &= ({}^g\lambda.{}^g f)(x).\end{aligned}$$

□

We will make use of the fact that E^X is a G-E-algebra in the proof of the fundamental theorem of Galois theory.

EXAMPLE 4.21. Note that an element of a group G acts on the ring of complex numbers either trivially or by complex conjugation, giving an $\mathbb{R}$-algebra homomorphism. Let's examine the action of G on finite dimensional extensions of $\mathbb{C}$, thereby extending the action of G on $\mathbb{C}$.

Let's first consider a two-dimensional extension of $\mathbb{C}$. Let $\mathbb{C} \hookrightarrow \mathbb{C} \times \mathbb{C}$ be an injective map that sends z to (z, z) be a two-dimensional extension of $\mathbb{C}$. Extend the map $\sigma : \mathbb{C} \to \mathbb{C}$ to a map $\tilde{\sigma} : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ defined by $\tilde{\sigma}(z, z) = (\sigma(z), \sigma(z))$. We can have two possible actions of G on $\mathbb{C} \times \mathbb{C}$:

(1) $\tilde{\sigma}(x, y) = (\sigma(x), \sigma(y))$ and
(2) $\tilde{\sigma}(x, y) = (\sigma(y), \sigma(x))$.

These are indeed actions on a ring. Consider the first action. We have $\tilde{\sigma}((a + b), (c + d)) = (\sigma(a + b), \sigma(c + d)) = (\sigma(a) + \sigma(b), \sigma(c) + \sigma(d)) = (\sigma(a), \sigma(c)) + (\sigma(b), \sigma(d)) = \tilde{\sigma}(a, c) + \tilde{\sigma}(b, d)$. We also have that $\tilde{\sigma}((a, b)(c, d)) = \tilde{\sigma}(ac, bd) = (\sigma(ac), \sigma(bd)) = (\sigma(a)\sigma(c), \sigma(b)\sigma(d)) = (\sigma(a), \sigma(b))(\sigma(c), \sigma(d)) = \tilde{\sigma}(a, b)\tilde{\sigma}(c, d)$ and $\tilde{\sigma}(1, 1) = (\sigma(1), \sigma(1)) = (1, 1)$. Showing that the second action is also an action on a ring is similar to what we just did for the first one.

Notice that the set of elements in $\mathbb{C} \times \mathbb{C}$ that are fixed by the first action is simply $\mathbb{R} \times \mathbb{R}$, and the set of elements fixed by the second action is $\mathbb{C}$.

4.2. Field Theory and Classical Galois Theory

Before we get into Galois theory, we should briefly talk about field theory and provide some key results in it. Recall that a *field* is a commutative ring where every nonzero element has a multiplicative inverse. In this chapter there will be a lot of focus on fields which contain smaller fields inside of them, which are called field extensions. Field extensions are the major object of study in field theory.

DEFINITION 4.22. Let F be a field. A field E which contains the field F, $F \subset E$ is called a *field extension* of F, and we denote it by E/F, read "E over F". Note that E/F is not a quotient field, but is just some formal notation.

For the remainder of this chapter, F is a field and E is an extension field over F.

It would be nice to have a general way to build field extensions of some field F with desired properties. We will want to do this in Galois theory, where we will need to build a field extension of some field which contains all the roots of some polynomial with coefficients in the underlying field.

If E/F is a field extension, then E is a vector space over the field F. The dimension of E as a vector space over F is denoted $[E : F]$. For example, the field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has dimension two as a vector space over $\mathbb{Q}$. By $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, we mean that the field $\mathbb{Q}$ is generated by $\sqrt{2}$ over $\mathbb{Q}$. In this case it turns out that $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$, but let's state a definition and a general theorem regarding this, as it is a useful way to construct field extensions. However, we will consider stricter statements involving algebras rather than fields, from which the analogous statements involving field extensions follow.

DEFINITION 4.23. Let F be a field and A be an F-algebra. An element $a \in A$ is said to be *algebraic* if there is some polynomial $p(x) \in F[x]$ such that a is a root

of $p(x)$, i.e. if $p(a) = 0$. We say that the F-algebra A is algebraic if every element $a \in A$ is algebraic.

There is a nice fact about F-algebras that are finite dimensional as vector spaces over F, which is that all of them are algebraic.

LEMMA 4.24. Let A be a finite dimensional F-algebra. Then A is algebraic.

PROOF. Choose an arbitrary $a \in A$ and suppose that A has dimension n. Then the set $\{1, a, \ldots, a^n\}$ must be linearly dependent over F, i.e. there exists a positive integer k, inclusively between 1 and n, and nonzero coefficients $c_i \in F$ such that

$$\sum_{i=1}^{k} c_i a^i = 0.$$

Therefore, the polynomial

$$p(x) = \sum_{i=1}^{k} c_i x^i \in F[x]$$

has root a, i.e. $p(a) = 0$. □

DEFINITION 4.25. Let $\alpha \in A$ be an algebraic element in the F-algebra A. Then the *minimal polynomial* of α over F, $m_{\alpha,F} \in F[x]$, is the monic polynomial of least degree having α as a root. It is irreducible over F.

THEOREM 4.26. Let A be a finite dimensional F-algebra. The minimal polynomial $m_{\alpha,F} \in F[x]$ exists and is unique if $\alpha \in A$ is algebraic over F, i.e. if α is a root of some nonzero polynomial $f(x) \in F[x]$.

PROOF. To prove existence, let's assume that the degree of a monic (which can done by scaling the polynomial by the necessary constant in F) polynomial $g(x)$ having α as a root is minimal among all others having α as a root and assume that it is reducible by way of contradiction. Say $g = ab$ for nonzero polynomials a and b, where the degree of a and the degree of b must both be less than the degree of g. Since $g(x) = a(x)b(x)$ for all $x \in E$, we know that $0 = g(\alpha) = a(\alpha)b(\alpha)$. But E is a field, so either $a(\alpha) = 0$ or $b(\alpha) = 0$. Both have lesser degree than g, which is a contradiction of the fact that g is the minimal polynomial having α as a root.

For uniqueness, assume that we have some polynomial $f \in F[x]$ having α as a root (which can be done since α is algebraic over F). The Euclidean algorithm tells us that in $F[x]$, there exists polynomials q and r such that $f = qg + r$. Choosing the quotient polynomial q such that qg has the same leading term as f, we see that the degree of the remainder polynomial r must be smaller than g, because otherwise the leading term of $qg + r$ would be different than the leading term of f. As $f = qg + r$ holds for all x, it must hold for α, i.e. $f(\alpha) = q(\alpha)g(\alpha) + r(\alpha)$. But $f(\alpha) = g(\alpha) = 0$, so $r(\alpha) = 0$, and because g is minimal, it must be that $r(x) = 0$. Thus g divides all polynomials having α as a root, as f is arbitrary in this regard. More specifically, g divides any monic irreducible polynomial in $F[x]$ having α as a root, which means that g has minimal degree among all such polynomials, i.e. $g = m_{\alpha,F}$. □

We now come to a well-known means by which we can construct field extensions.

LEMMA 4.27. Let A be an F-algebra and let $a \in A$ be a nonzero algebraic element with minimal polynomial $m(x)$ over F with degree n. Then

$$F(a) \cong F[x]/(m(x))$$

as F-algebras. In particular,

$$[F(a) : F] = \deg\, m(x) = \deg\, a.$$

PROOF. The map $\varphi : F[x] \to F(a)$ defined by $p(x) = p(a)$ is a homomorphism. This map is obviously surjective. Since a is algebraic, $m(a) = 0$, so that $m(x)$ is in the kernel of φ. Hence, the induced map

$$\psi : F[x]/(m(x)) \to F(a)$$

defined by $p(x) \bmod (m(x)) \mapsto p(a)$ is bijective. The map ψ is also a homomorphism of commutative rings[**1**] because $m(x)$ is irreducible. We endow the domain and codomain with F-algebra structure via the ring homomorphisms

$$F \to F[x]/(m)$$

and

$$F \to F(a)$$

by sending $\lambda \in F$ to itself in both cases' codomains. These maps are clearly respected by ψ, from which the result follows. □

We now show that the preceding statements work for field extensions as well.

COROLLARY 4.28. Let A be an F-algebra with no zero divisors. Then every algebraic element in A has an inverse in A.

PROOF. Let $a \in A$ be algebraic with minimal polynomial $m(x) \in F[x]$. The polynomial m is irreducible[**1**]. The result follows from lemma 4.27. □

So we have seen that a field extension E/F is an F-algebra (and so is the field F). We also need to whether this is true for intermediate F-algebras $F \subset I \subset E$. It turns out that intermediate F-algebras are also fields:

LEMMA 4.29. Let E/F be a finite dimensional extension field and let $F \subset I \subset E$ be an intermediate F-algebra. Then I is also a field.

PROOF. The F-algebra I contains no zero divisors because it is contained in the field E, which has none. So every algebraic element in I has an inverse by corollary 4.28. Furthermore, I is finite dimensional because E is, so every element in I is algebraic by lemma 4.24. □

There are a few different types of fields which we will now consider that abstracts the study of factoring polynomials and finding their roots by enlarging the field of coefficients. Definitions of these types of fields are given below.

DEFINITION 4.30. Let F be a field and let $p(x) \in F[x]$ be a polynomial with coefficients in F. A *splitting field* of the polynomial p is a field extension E/F such that p splits into linear factors in $E[x]$, i.e. in $E[x]$ we have

$$p(x) = \prod_{i}^{\deg\, p} (x - a_i),$$

such that the set of coefficients $\{a_i\}$ in E is an F-basis for E.

DEFINITION 4.31. The extension field E/F is said to be *normal* if it is the splitting field of a family of polynomials in $E[x]$. In other words, a normal extension E/F is one in which every polynomial p in $F[x]$ that has at least one root in E can be split into linear factors in $E[x]$.

DEFINITION 4.32. A *separable* extension field E/F is an algebraic extension field over F such that for all $\alpha \in E$, the minimal polynomial of α over F is a separable polynomial, i.e. it has distinct roots.

We are now able to define a special kind of field extension that has a special group and obeys the fundamental theorem of Galois theory. Keep in mind that there are several different but equivalent ways of characterizing Galois extensions. The definition we give below characterizes them as finite, normal, and separable extensions.

DEFINITION 4.33. An algebraic extension field E/F is said to be *Galois* if it is normal and separable.

We can also characterize Galois extensions of a field F as splitting fields of separable polynomials over F. Theorem 13 of section 14.2 in [**1**], it is proves that the extension E/F is Galois if and only if E is the splitting field of some separable polynomial over F (perhaps I should expand on this). We now frame this in a more general framework using tensor products.

DEFINITION 4.34. Let E/F be a field extension and let A be an F-algebra. We say that A is *E-split* if $A \otimes_F E \cong E^n$ as E-algebras for some positive integer n.

In the above definition of E-split, notice that if we tensor over E rather than F, then we get $A \otimes_E E = A \cong E^n$.

Indeed, another way of characterizing Galois extensions is through the concept of splitting fields:

LEMMA 4.35. The field extension E/F is Galois if and only if the field extension E splits the F-algebra E.

PROOF. This is a straightforward check using the relevant definitions. □

PROPOSITION 4.36. Let E/F be a separable extension that is finite dimensional as a vector space over F. Then E/F is E-split, i.e. $E \otimes_F E \cong E^m$ as E-algebras for some positive integer m.

PROOF. Since E is an algebraic extension field that is finite dimensional over F, there exists a finite set of elements $\{a_i\}$ in E such that $E = F(a_1, \ldots, a_n)$.

Furthermore, each a_i has minimal polynomial f_i over F. Thus

$$\begin{aligned}
E \otimes_F E &= E \otimes_F \{F[x_1, \dots, x_n]/(f_1 \cdots f_n)\} \\
&= \{E \otimes_F F[x_1]/(f_1)\}[x_2, \dots, x_n]/(f_2 \cdots f_n), \quad \text{adjoining one element at a time} \\
&\cong (E[x_1]/(f_1))[x_2, \dots, x_n]/(f_2 \cdots f_n), \quad \text{changing coefficients in the polynomial ring} \\
&= (E^j)[x_2, \dots, x_n]/(f_2 \cdots f_n), \quad f_1 \text{ is split in } E \text{ by CRT, and } j \in \mathbb{N} \\
&\cong (E^j \otimes_F F)[x_2, \dots, x_n]/(f_2 \cdots f_n) \\
&= \{E^j \otimes_F F[x_2]/(f_2)\}[x_3, \dots, x_n]/(f_3 \cdots f_n), \quad \text{adjoining the next element} \\
&\cong \{E \otimes_F F[x_2]/(f_2)\}^j[x_3, \dots, x_n]/(f_3 \cdots f_n), \quad \text{by } (x_i)_i \otimes y \mapsto (x_i y)_i \\
&\cong \{E[x_2]/(f_2)\}^j[x_3, \dots, x_n]/(f_3 \cdots f_n), \quad \text{changing coefficients again} \\
&\cong (E^k)^j[x_3, \dots, x_n]/(f_3 \cdots f_n), \quad f_2 \text{ is split in } E \\
&\vdots \\
&\cong E^m, \quad \text{continuing this process up to and including } a_n.
\end{aligned}$$

□

DEFINITION 4.37. If E is an extension field of F which is Galois, then the *Galois group* of E over F, $\mathrm{Gal}(E/F)$, is the automorphism group of E where all of the automorphisms fix F pointwise, i.e. $\mathrm{Gal}(E/F) = \mathrm{Aut}_{F\text{-alg}}(E) = \{\sigma : E \to E \mid \forall a \in F : \sigma(a) = a\}$.

EXAMPLE 4.38. The group of automorphisms of complex numbers that fix $\mathbb{R}$ pointwise, $\mathrm{Aut}_{\mathbb{R}\text{-alg}}(\mathbb{C})$ contains two automorphisms. One automorphism is the trivial automorphism, found in all automorphism groups, and the other is the one commonly known as complex conjugation. This automorphism group is called the *Galois group* of $\mathbb{C}$ over $\mathbb{R}$, and is written $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

We now come to the classical statement of the fundamental theorem of Galois theory.

THEOREM 4.39. (Classical fundamental theorem of Galois theory) Let E/F be a Galois extension. There exists a bijection between the intermediate fields $F \subset I \subset E$ and the subgroups H of the Galois group $G = \mathrm{Gal}(E/F)$. The bijection between the two sends I to the set of elements of G fixing I, and sends the subgroup H to the set of elements in I that are fixed by all $g \in G$.

Note: we will *not* assume this theorem in proving the categorical version of the fundamental theorem of Galois theory.

PROOF. A standard proof can be found in, e.g., [**1**]. □

CHAPTER 5

Categorical Galois Theory of Field Extensions

For this chapter, F is a field and we will suppose that field extensions E/F are finite dimensional as F-vector spaces unless otherwise noted.

Galois theory connects field theory and group theory, which provides many useful results that allow us to simplify field theoretic problems into group theoretic problems. We will develop the fundamental theorem of Galois theory in a categorical language and prove it. We will begin by proving some results involving bases of extension fields and their smaller fields. Note that this formulation of Galois theory is not original, and it is typically known as Grothendieck's formulation of Galois theory. We have only taken the equivalence of categories and presented our own proof of it by considering an intermediate category.

5.1. Grothendieck's Galois theory for finite field extensions

The fundamental theorem of Galois theory states that there is a one-to-one correspondence between group actions and field extensions for extensions that are nice enough (in the sense that they are Galois). Here we generalize these extensions with split algebras and Galois group G-actions with G-sets. We ultimately want to prove that the category of finite E-split F-algebras is equivalent to the category of finite G-sets (**we will stop writing the word finite for these categories**), but we split this into two equivalences by intermediately looking at split E-algebras (by ascending from F-algebras to E-algebras) together with a G-E-module structure of the Galois group G.

THEOREM 5.1. Let F be a field and let E/F be a field extension of F. Then there are equivalences of categories (everything is finite)

$$E\text{-split } F\text{-algebras} \xrightarrow{\sim} E\text{-split } G\text{-}E\text{-algebras} \xrightarrow{\sim} G\text{-sets},$$

the first between E-split F-algebras and E-split G-E-algebras, and the second an anti-equivalence between E-split G-E-algebras and (finite) G-sets.

Some definitions and notation involving the categories in theorem 5.1 will be helpful at this point. To reduce clutter, we denote the class of E-algebra maps from Z to E as

$$\mathcal{E}(Z) \equiv \mathrm{Hom}_{E\text{-alg}}(Z, E).$$

Recall that the mapping in lemma 4.20 defines a G-action on E-algebra morphisms for we will make much use of this fact. We will always be use this G-action on any map of sets.

5.1.1. The (Anti-)equivalence of E-split G-E-algebras and (finite) G-sets. Let G be a group. In this section we prove the anti-equivalence between E-split G-E-algebras and (finite) G-sets. Let $\mathcal{C}$ be the category of finite E-split G-E-algebras (with E-algebra maps) and let $\mathcal{D}$ be the category of finite G-sets (with G-equivariant maps). We will first construct a functor Φ from $\mathcal{C}$ to $\mathcal{D}$.

Note that each of the E-split E-algebras $A \cong E^k$ (for some positive integer k) given below are the ones whose E-algebra structure is given by the ring homomorphism $\delta : E \to A$ sending x to the $x.1_A$. We will often abuse notation and denote all of these ring homomorphisms with just δ. Note that we may also drop these homomorphisms from the notation altogether when the algebra structure is understood.

Consider the map Φ sending any finite E-split G-E-algebra (A, α) to the finite G-set $(\mathcal{E}(A), \zeta)$, where the G-action ζ on $\mathcal{E}(A)$ is given by lemma 4.19. The map Φ also sends E-split G-E-algebra homomorphisms to G-equivariant maps through

$$\mathrm{Hom}_{\mathcal{C}}((A,\alpha),(B,\beta)) \to \mathrm{Hom}_{\mathcal{D}}((\mathcal{E}(B),\xi),(\mathcal{E}(A),\zeta))$$

defined by

$$\phi \mapsto \psi,$$

where $\psi : \mathcal{E}(B) \to \mathcal{E}(A)$ satisfies $\psi(f) = f \circ \phi$ for all f. The G-actions ξ is also given by lemma 4.19. It is straightforward to verify that Φ is a functor, as follows.

To see that Φ preserves composition, consider the E-split G-E-algebras $(A, \alpha), (B, \beta)$ and (C, γ) in $\mathcal{C}$ and two E-algebra maps $f : A \to B$ and $g : C \to A$. Now Φ sends fg to the map ψ_{fg} given by $\phi \mapsto \phi \circ (fg)$. Additionally, the map Φ sends f to ψ_f and g to ψ_g (adopting the notation in the previous sentence), so $\Phi(g)\Phi(f)$ is $\psi_g \circ \psi_f$, which sends $\phi \in \mathcal{E}(B)$ to $(\phi \circ f) \circ g = \phi \circ (fg) \in \mathcal{E}(C)$ (by the associativity of composition). Furthermore, the map Φ preserves identity morphisms because, given some E-split G-E-algebra (A, α), whose identity morphism sends each element in A to itself, we have $\Phi(\mathrm{id}_{(A,\alpha)}) = \psi$, where $\psi : \mathcal{E}(A) \to \mathcal{E}(A)$ is given by $\phi \mapsto \phi \circ \mathrm{id}_A$. But $\phi \circ \mathrm{id}_A = \phi$, so ψ is the identity morphism of the G-set $\Phi(A, \alpha) = (\mathcal{E}(A), \xi)$, and we see that Φ preserves identity morphisms.

THEOREM 5.2. The functor Φ is an anti-equivalence of categories.

A few lemmas will come in handy for proving this theorem.

LEMMA 5.3. Let E/F be a field extension and let A be a split E-algebra that has dimension n as a vector space over F. Then the class of E-algebra maps from (A, δ) to (E, id),

$$\mathcal{E}(A) = \mathrm{Hom}_{E\text{-alg}}((A,\delta),(E,\mathrm{id})) \cong \mathrm{Hom}_{E\text{-alg}}((E^n,\delta),(E,\mathrm{id})),$$

consists of the n projections $p_i(x) = x_i$ for $i \in \{1, \ldots, n\} = N$, where $x \in A$.

PROOF. The n indecomposable idempotents of E^n are $e_1 = (1, 0, \ldots, 0), \ldots, e_n$ and they generate E^n. So we can write any $x \in E^n$ as $x = \sum_{i=1}^{n} \delta(x_i)e_i$ if we define the multiplication componentwise as usual. Let $\varphi \in \mathcal{E}(E^n)$. Recall that the E-algebra E^n is defined by the map $\delta : E \to E^n$ given by $a \mapsto (a, \ldots, a)$. Then $\varphi(a, \ldots, a) = a$ for all $a \in E$ because $\varphi \circ \delta = \mathrm{id}$. Thus to prove the lemma, we can show that $\varphi(e_i) = 1$ for exactly one $i \in N$ and $\varphi(e_j) = 0$ for all $j \neq i$. Suppose we have an indecomposable idempotent e such that $\varphi(e) \neq 0$. Now pick an idempotent $e' \neq e$ distinct from e. Then $0 = \varphi((0, 0)) = \varphi(ee') = \varphi(e)\varphi(e')$, so $\varphi(e') = 0$. We

can continue to look at each pair of indecomposable idempotents in this manner to conclude that for exactly one $i \in N$, $\varphi(e_i) = x$ for some nonzero $x \in E$ and that $\varphi(e_j) = 0$ for all $j \neq i$. But

$$1 = \varphi(1, \ldots, 1) = \varphi(e_1 + \cdots + e_n) = \varphi(e_1) + \cdots + \varphi(e_n),$$

so $\varphi(e_i) = 1$ for exactly one $i \in N$. Now

$$\begin{aligned}\varphi(x) &= \varphi\left(\sum_{j=1}^{n} \delta(x_j)e_j\right) \\ &= \sum_{j=1}^{n} \varphi(\delta(x_j))\varphi(e_j) \\ &= \sum_{j=1}^{n} x_j\varphi(e_j) \\ &= x_i\end{aligned}$$

for some $i \in N$. □

The above lemma shows that the action of G on E-split G-E-algebras naturally permutes indecomposable idempotents in the E-algebras. Since the indecomposable idempotents $\{e_i\}_{i\in\{1,\ldots,n\}}$ of an E-algebra E^n form an E-basis of E^n (because $(x_1, \ldots, x_1)e_1 + \cdots + (x_n, \ldots, x_n)e_n = (x_1, \ldots, x_n)$ and they are E-linearly independent), knowing the G-action on each of them uniquely determines the action E^n. In fact, the G-action on projections correspond to the actions on indecomposable idempotents because the G-action permutes indecomposable idempotents, and the indecomposable idempotents generate E^n. This should provide us some intuition about how G acts on E-split G-E-algebras. We will prove this with the aid of the following lemma.

LEMMA 5.4. Let (E^n, δ, α) be a G-E-algebra. The action of α permutes the n indecomposable idempotents $\{e_i\}$ of E^n. In particular, since any n-dimensional split E-algebra A is isomorphic to E^n, the G-action permutes the indecomposable idempotents of any split E-algebra of any dimension.

PROOF. Pick out some arbitrary indecomposable idempotent $e \in E^n$. The action of α on e gives another idempotent in E^n because $(g.e)^2 = (g.e)(g.e) = g.(ee) = g.e$, but is $g.e$ indecomposable as well? It turns out that it is, for suppose that $g.e = e' + e''$ where e' and e'' are nonzero idempotents in E^n. Then $e = g^{-1}.(g.e) = g^{-1}.(e' + e'') = g^{-1}.e' + g^{-1}.e''$. But both $g^{-1}.e'$ and $g^{-1}.e''$ are nonzero because if for any nonzero $h \in G$ and any $x \in E^n$, $h.x = 0$, then $x = 0$. But this contradicts the fact that e is indecomposable. □

We now come to the statement that the G-action on a basis of any E-algebra A is the same as the G-action on the projections in $\mathrm{Hom}(A, E)$.

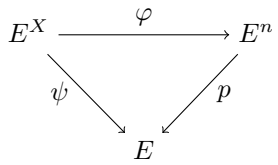
PROPOSITION 5.5. Let $p_i : E^n \to E$ be the E-algebra projection defined by $x \mapsto x_i$ and suppose that we know the action of α on the indecomposable idempotent e_i, say $g.e_i = e_j$ for fixed $i, j \in \{1, \ldots, n\}$. Then the left action of G on the projection p_i is simply p_j, i.e. ${}^g p_i = p_j$.

PROOF. By direct computation of the left action of G on p_i, we see that for any $x \in E^n$,

$$\begin{aligned}
{}^g p_i(x) &= g.p_i(g^{-1}.x) \\
&= g.p_i\left(g^{-1}.\sum_k \delta(x_k)e_k\right) \\
&= \sum_k g.p_i(\delta(g^{-1}.x_k))p_i(g^{-1}.e_k) \\
&= \sum_k g.p_i(g^{-1}x_k, \ldots, g^{-1}.x_k)p_i(g^{-1}.e_k) \\
&= \sum_k g.(g^{-1}.x_k)p_i(g^{-1}.e_k) \\
&= \sum_k x_k p_i(g^{-1}.e_k) \\
&= \sum_k x_k \begin{cases} 0 & \text{if } g^{-1}.e_k \neq e_i \\ 1 & \text{if } g^{-1}.e_k = e_i \end{cases} \\
&= x_l \quad \text{where } g^{-1}.e_l = e_i \text{ for a fixed } l \in \{1, \ldots, n\} \\
&= p_j(x) \quad \text{because } g^{-1}.e_l = e_i \Rightarrow l = j.
\end{aligned}$$

Behold, ${}^g p_i = p_j$. □

For any two sets E and X, we have the set of functions E^X mapping X to E. If X is finite with cardinality n, we have a map $E^X \to E$ for each $x \in X$ (this is why the exponential notation is natural here). This can be seen by requiring the diagram



to commute. If we label the n elements in the set X with $\{x_i\}_{i\in\{1,\ldots,n\}}$, then the map φ is given by $f \mapsto (f(x_1), \ldots f(x_n))$ and is an isomorphism. We saw in lemma 5.3 that the only possible E-algebra maps from E^n to E are the n projections p_i. Thus we have a map ψ_x mapping E^X to E defined by $f \mapsto f(x)$ for each $x \in X$, i.e.

$$\mathcal{E}(E^X) = \mathrm{Hom}_{E\text{-alg}}(E^X, E) = \{\psi_x\}$$

where $\psi_x(f) = f(x)$ is indexed by X. This brings us to the following useful lemma.

LEMMA 5.6. If X is a finite set, then the map

$$\epsilon : X \to \mathcal{E}(E^X)$$

given by $x \mapsto \psi_x$, where ψ_x is the map described in the paragraph above, is bijective.

PROOF. We can say without loss of generality that the cardinality of X is n and label the elements in X as $X = \{a_1, \ldots, a_n\}$. Since $E^X \cong E^n$, $\mathcal{E}(E^X)$ has cardinality n by lemma 5.3, the same as the cardinality of X. We now just need to

show that ϵ is injective. To this end, note that for each $x \in X$, we have the map $\psi_x \in E^X$ given by

$$\psi_x(x') = \begin{cases} 1 & \text{if } x' = x, \\ 0 & \text{if } x' \neq x. \end{cases}$$

The set $\{\psi_x \mid x \in X\}$ forms an E-basis of E^X. But $\epsilon(x)(\psi_x) = \epsilon(x')(\psi_x)$ if and only if $x = x'$, so ϵ is injective. □

LEMMA 5.7. Let A be an m-dimensional split E-algebra. Suppose $x, y \in A \cong E^m$ and $f(x) = f(y)$ for all $f \in \mathcal{E}(A)$. Then $x = y$.

PROOF. Choosing an E-basis for A, $\{e_i\}_{i\in\{1,\dots,m\}}$, we can write x and y as $x = \sum_i \delta(x_i)e_i$ and $y = \sum_i \delta(y_i)e_i$ for x_i and y_i in E. We have for each $f \in \mathcal{E}(A)$,

$$f\left(\sum_i \delta(x_i)e_i\right) = f\left(\sum_i \delta(y_i), e_i\right).$$

Because f is a ring homomorphism, this reduces to

$$\sum_i x_i f(e_i) = \sum_i y_i f(e_i)$$

for all $f \in \mathcal{E}(A)$. But $\mathcal{E}(A)$ consists of the m projections p_i described in lemma 5.3, so $x_i = y_i$ for all $i \in \{1, \dots, m\}$. Therefore $x = y$. □

We are now set up to prove the anti-equivalence between E-split G-E-algebras and (finite) G-sets (theorem 5.2).

PROOF. (of theorem 5.2)
Let $A \cong E^n$ and $B \cong E^m$ be two split G-E-algebras.

(Faithful) We need to show that the map

$$\Phi : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\mathcal{E}(B), \mathcal{E}(A))$$

defined by $f \mapsto \psi_f$, where $\psi_f(\pi) = \pi \circ f$, is injective.

To that end, suppose we have two morphisms $\varphi, \psi \in \mathrm{Hom}_{\mathcal{C}}((A, \alpha), (B, \beta))$ such that $\Phi(\varphi) = \Phi(\psi)$. Then for all $f \in \mathcal{E}(B)$, we have $\Phi(\varphi)(f) = \Phi(\psi)(f)$, which implies that $f \circ \varphi = f \circ \psi$ for all f. Then for any $x \in A$, $f(\varphi(x)) = f(\psi(x))$ for all f. Hence, by lemma 5.7, $\varphi(x) = \psi(x)$ for all $x \in A$, i.e. $\varphi = \psi$, and we conclude that the functor in question is faithful.

(Full) We need to show that the map

$$\Phi : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\mathcal{E}(B), \mathcal{E}(A))$$

defined by $f \mapsto \psi_f$, where $\psi_f(\pi) = \pi \circ f$, is bijective.

Pick an arbitrary G-equivariant map $\tau : \mathcal{E}(B) \to \mathcal{E}(A)$. The G-set $\mathcal{E}(B)$ is endowed with the G-action ξ given by (in view of lemma 4.19)

$$\xi_g(p)(x) = \sigma_g(p(\alpha_{g^{-1}}(x)))$$

for each $p \in \mathcal{E}(B)$, and the G-set $\mathcal{E}(A)$ is endowed with the G-action ζ given by

$$\zeta_g(\rho)(y) = \sigma_g(\rho(\beta_{g^{-1}}(y)))$$

for each $\rho \in \mathcal{E}(A)$, where the G-action σ on E is known. We need to show that there exists an f in $\mathrm{Hom}_{\mathcal{C}}((A, \alpha), (B, \beta))$ such that $\tau(p) = p \circ f$ for all p. To this

end, choose a basis $\{e_i\}$ for B and label the projections in $\mathcal{E}(B)$ with this index. Consider the map $f : A \to B$, defined by

$$f(x) = \sum_i \tau(p_i)(x)e_i$$

for each $x \in A$, where $\{p_i\}$ are the usual E-algebra projections in $\mathcal{E}(B)$.

Let's see that we get the desired result by calculating $\Phi(f)$ as follows. The map f given above is sent to the G-equivariant map $\mathcal{E}(B) \to \mathcal{E}(A)$ defined by $p_i \mapsto p_i \circ f$. But for any $x \in A$, we have

$$\begin{aligned}(p_i \circ f)(x) &= p_i(f(x)) \\ &= p_i\left(\sum_i \tau(p_i)(x)e_i\right) \\ &= \tau(p_i)(x),\end{aligned}$$

so that $p_i \circ f = \tau(p_i)$ for all i.

We need to check that f is a map of E-algebras, i.e. that f is a ring homomorphism and that $\delta_B = f \circ \delta_A$. The fact that f is a ring homomorphism follows from the fact that $\tau(p)$ is a ring homomorphism for all projections $p \in \mathcal{E}(B)$. The second condition is verified by computing, for an arbitrary $x \in E$,

$$\begin{aligned}f(\delta_A(x)) &= f(x.1_A) \\ &= \sum_{i=1}^{m} \tau(p_i)(x.1_A)e_i \\ &= \sum_{i=1}^{m} xe_i \\ &= \delta_B(x).\end{aligned}$$

We also need to check that $p_i \circ f$ is an E-algebra homomorphism, i.e. that

$$\begin{array}{ccc} A & \xrightarrow{\quad p_i \circ f \quad} & E \\ & {\scriptstyle\delta}\nwarrow \quad \nearrow{\scriptstyle \mathrm{id}} & \\ & E & \end{array}$$

commutes and that $p_i \circ f$ is a homomorphism of rings. Well

$$\begin{aligned}((p_i \circ f) \circ \delta)(x) &= p_i(f(\delta_A(x))) \\ &= p_i\delta_B(x) \\ &= p_i(x.1_B) \\ &= x \\ &= \mathrm{id}(x),\end{aligned}$$

so the diagram commutes. Obviously $p_i \circ f$ is a ring homomorphism because it is the composition of two ring homomorphisms.

We finally need to show that f is G-equivariant. Recall that the actions of α and β on A and B are specified by how they permute the basis elements of A

and B, respectively, and that in turn, by proposition 5.5, there is a one-to-one correspondence between these permutations and the E-algebra projections. Since τ is G-equivariant, we know that for all $\varphi \in \mathcal{E}(B)$, $x \in A$, and $g \in G$,

$$\xi_g(\tau(\varphi))(x) = \tau(\zeta_g(\varphi))(x).$$

But the left hand side gives

$$g.(\tau(\varphi))(g^{-1}.x) = g.(\varphi \circ f)(g^{-1}.x),$$

and the right hand side gives

$$(\zeta_g(\varphi) \circ f)(x) = \zeta_g(\varphi)(f(x)) = g.\varphi(g^{-1}.f(x))$$

for all $\varphi \in \mathcal{E}(B)$, $x \in A$, and $g \in G$. Therefore

$$\varphi(f(g^{-1}.x)) = \varphi(g^{-1}.f(x))$$

for all φ and g, so that $f(g^{-1}.x) = g^{-1}.f(x)$ for all $g \in G$ and $x \in A$ (by lemma 5.7), completing the proof that the functor Φ is full.

(Essentially Surjective) Let (X, α) be a finite G-set. Consider the G-E-algebra (E^X, u, ξ), where $u : E \to E^X$ maps each $\lambda \in E$ to the constant function $\underline{\lambda} \in E^X$, and ξ is the map conjugation action described in lemma 4.19. By lemma 5.6, the map $X \to \mathcal{E}(E^X)$ sending $x \in X$ to $\psi_x \in \mathcal{E}(E^X)$, where $\psi_x : E^X \to E$ is defined by $f \mapsto f(x)$, is a bijection.

To complete this part of the proof, we would like to show that the map $\mathcal{E}(E^X) \to X$ given by $\psi_x \mapsto x$ with $\psi_x(f) = f(x)$ is G-equivariant. To do this, we will instead show that this map's inverse $L : X \to \mathcal{E}(E^X)$ sending x to ψ_x is G-equivariant. So we would like to show that $(\xi_g \circ L)(x) = (L \circ \alpha_g)(x)$ for all $x \in X$ and $g \in G$, i.e. that $g.\psi_x = \psi_{g.x}$ for all x and g. To this end, consider a map $f \in E^X$. By definition we have $\psi_{g.x}(f) = f(g.x)$. Now

$$\begin{aligned}(g.\psi_x)(f) &= g.\psi_x(g^{-1}.f) \\ &= g.((g^{-1}.f)(x)) \\ &= g.(g^{-1}.f(g.x)) \\ &= (gg^{-1}).f(g.x) \\ &= f(g.x),\end{aligned}$$

so that $(g.\psi_x)(f) = \psi_{g.x}(f)$ for all $x \in X$, $g \in G$, and $f \in E^X$. By lemma 2.16, the functor Φ is essentially surjective.

Therefore the category of E-split G-E-algebras is anti-equivalent to the category of finite G-sets, completing the proof of theorem 5.2. □

5.1.2. The Equivalence of F-vector spaces and G-E-vector spaces. Turning to the claimed equivalence between the category of E-split F-algebras and E-split G-E-algebras, we will begin by proving the following more general statement. In contrast to our consideration of the anti-equivalence between E-split G-E-algebras and finite G-sets, we now require that the extension field E/F is Galois and that $G = \mathrm{Gal}(E/F)$ is the Galois group of E over F (and is finite). We now give the general statement.

THEOREM 5.8. Let F be a field and let E/F be Galois. Let G be the Galois group of E over F. Consider the map

$$\eta : F\text{-vec} \to G\text{-}E\text{-vec}$$

defined by

$$A \mapsto (E \otimes_F A, \alpha \otimes A) \text{ and } \varphi \mapsto E \otimes \varphi,$$

where the action of $\alpha \otimes A$ on $E \otimes_F A$ is the standard G-E-module structure, so that for all $e \in E$ and $a \in A$, we have $g.(e \otimes a) = (g.e) \otimes a$. The map η is an equivalence of categories.

—

Let's begin working our way up to the equivalence between E-split F-algebras and E-split G-E-algebras. We would like to first consider the category of F-algebras and the category of G-E-algebras, from which the E-split cases will follow. Since F-algebras are F-vector spaces with some additional structure (F-linear maps and associativity) and, similarly, G-E-algebras are G-E-vector spaces with some additional structure (G-E-linear maps and associativity), we can prove that F-vector spaces and G-E-vector spaces are equivalent and then show that the equivalence respects the additional structure that make them each algebras.

We will now state a useful result about vector spaces which share a common basis. Recall that we can enlarge an F-vector space V into an E-vector space $E \otimes_F V$ (given the standard E-module structure) by using the tensor product. If we choose an F-basis $\{e_i\}$ of V and then tensor up to E, we happen to get an E-basis $\{1 \otimes e_i\}$ of $E \otimes_F V$. In Galois theory, we will want to be able to move from V to $E \otimes_F V$ so that an F-basis of the former is taken to an E-basis of the latter, but we will also want to be able to move from an E-vector space W to F-vector spaces that have this same property. The following lemma will help us sort this problem out.

LEMMA 5.9. Let W be an E-vector space and let $V \subset W$ be a K-vector space that is a subspace of W. Then the following are equivalent:

(1) The map $E \otimes_F V \to W$ sending $x \otimes v$ to xv is an isomorphism of E-vector spaces,
(2) any F-basis of V is also an E-basis of W, and
(3) there exists an F-basis of V that is also an E-basis of W.

PROOF. ($1 \Rightarrow 2$) Choose an arbitrary F-basis $\{e_i\}$ of V. Then $\{1 \otimes e_i\}$ is an E-basis of $E \otimes_F V$, using the standard E-module structure on it. Assume that $E \otimes_F V \to W$ defined by $x \otimes v \mapsto xv$ is an E-vector space isomorphism. Now, each basis element $1 \otimes e_i$ in $E \otimes_F V$ is sent to $1e_i = e_i$ in W by this map. Since the map is an isomorphism, it takes bases to bases, so each e_i is an E-basis element for W.

($2 \Rightarrow 3$) The F-vector space V has at least one F-basis.

($3 \Rightarrow 1$) Let $\{e_i\}$ be an F-basis of V that is also an E-basis of W. The map $E \otimes_F V \to W$ sending $x \otimes v$ to xv sends each $1 \otimes e_i$ to e_i, so every basis element of $E \otimes_F V$ is sent to a basis element of W. Thus the given map is an E-vector space isomorphism. □

With the aid of the following lemma, we are able to transport G-E-module structures between certain E-vector spaces.

LEMMA 5.10. Let $f : W \to W'$ be an E-vector space isomorphism and suppose that W has a G-E-module structure $\{s_\sigma\}_\sigma$. Then there exists a unique G-E-module structure $\{t_\sigma\}_\sigma$ on W' such that

$$\begin{array}{ccc} W & \xrightarrow{f} & W' \\ {\scriptstyle s_\sigma}\downarrow & & \downarrow{\scriptstyle t_\sigma} \\ W & \xrightarrow[f]{} & W' \end{array}$$

commutes for all $\sigma \in G$.

PROOF. It is straightforward to verify that the expression

$$t_\sigma(w') = f(s_\sigma(f^{-1}(w')))$$

defines a σ-E-linear map for all $\sigma \in G$: For the compatibility of the G- and E-actions, observe that for $x \in E$, $w' \in W'$, and $\sigma \in G$,

$$\begin{aligned} {}^\sigma x.{}^\sigma w' &= f{}^\sigma f^{-1}(x.w') \\ &= f[{}^\sigma(x.f^{-1}(w'))] \\ &= f[{}^\sigma x.{}^\sigma f^{-1}(w')] \\ &= {}^\sigma x.f({}^\sigma f^{-1}(w')) \\ &= {}^\sigma x.{}^\sigma w' \\ &= {}^\sigma(x.w'). \end{aligned}$$

For any a and b in W', the map t_σ is additive because

$$\begin{aligned} {}^\sigma(a+b) &= f({}^\sigma f^{-1}(a+b)) \\ &= f({}^\sigma(f^{-1}(a) + f^{-1}(b))) \\ &= f({}^\sigma f^{-1}(a) + {}^\sigma f^{-1}(b)) \\ &= f({}^\sigma f^{-1}(a)) + f({}^\sigma f^{-1}(b)) \\ &= {}^\sigma a + {}^\sigma b. \end{aligned}$$

With these two conditions verified, we know that t_σ given above is σ-E-linear for all σ. The fact that they are associative and that $t_{\mathrm{id}} = \mathrm{id}_{W'}$ is easily checked in a similar manner. The uniqueness of this G-E-module structure falls out of the requirement that the diagram in the lemma statement commutes. □

As an example of lemma 5.10 that has much utility, consider any E-vector space W and any F-vector subspace $V \subset W$ such that any one of the conditions in lemma 5.9 holds. Now, $E \otimes_F V$ has a standard G-E-module structure (that acts on the first factor). By lemma 5.10, this G-E-module structure on $E \otimes_F V$ gets transported to a unique G-E-module structure on W in a natural way. In other words, we can use these lemmas to calculate G-E-module structures on E-vector spaces, by base extending an F-vector subspace $V \subset W$ up to E, if V and W share a common basis.

Now, extension of scalars has several nice properties which we will exploit in proving the equivalence in question.

LEMMA 5.11. The E-vector spaces $E \otimes_F \ker \varphi$ and $\ker(E \otimes \varphi)$ are isomorphic.

PROOF. Note that $\ker \varphi$ is an F-subspace of V because it contains zero and is closed under both addition and scaling by F. Base extending the kernel, we get that the map $f : \ker \varphi \to E \otimes_F \ker \varphi$ defined by $k \mapsto 1 \otimes k$ is F-linear, where the codomain has the standard E-module structure. We can also take the kernel of the base extended map $E \otimes \varphi$ and obtain an E-subspace (with the standard structure), $K = \ker(E \otimes \varphi)$. Let's check that this is an E-subspace. Zero is clearly contained in K by definition of the kernel. If $x \otimes k, y \otimes j \in K$, then $E \otimes \varphi(x \otimes k) = E \otimes \varphi(y \otimes j) = 0$, so their sum is also mapped to zero by $E \otimes \varphi$ since $E \otimes \varphi$ is additive. Turning now to the final verification: if $x \otimes k \in K$ and $c \in E$, then $E \otimes \varphi(c(x \otimes k)) = E \otimes \varphi((cx) \otimes k) = (cx) \otimes 0 = 0$ because for nonzero x, $x \otimes k \in K \Rightarrow \varphi(k) = 0$.

Define a new map, $\psi : \ker \varphi \to K$, by $k \mapsto 1 \otimes k$. It is straightforward to check that the map ψ is F-linear. By the universal property of base extension, there exists a unique E-linear map $\kappa : E \otimes \ker \varphi \to K$ defined by $x \otimes k \mapsto x \otimes k$. We need to check that κ is bijective. We obtain immediately that κ is surjective.

We now need to show that κ is injective. Note that the map $\alpha : \ker \varphi \to V$ defined by $k \mapsto k$ is injective by definition of the kernel of φ. Since E is flat (by lemma 1.31), the map $\alpha' = E \otimes \alpha$ is also injective. Furthermore, the map $\beta : K \to E \otimes_F V$ defined by $x \otimes k \mapsto x \otimes k$ is also injective by definition of the kernel of $E \otimes \varphi$. But $\alpha' = \beta \circ \kappa$, so κ must be injective. Thus $E \otimes \ker \varphi \cong \ker(E \otimes \varphi)$ as E-modules. □

We now come to a very important result relating fixed points of the Galois group G and tensoring with a Galois extension E/F. Recall that if G is a group and X is a G-F-module, then we denote $X^G = \{x \in X \mid g.x = x\}$ as the fixed points in X by G.

LEMMA 5.12. If V is a G-F-module, then $E \otimes (V^G) \cong (E \otimes_F V)^G$ as E-modules.

Each of these modules, the G-action is on the second factor and yields a G-E-module structure for them.

PROOF. Let $\#G = n$. Define the map $\varphi : V \to V^n$ by $x \mapsto ({}^g x - x)_g$. Given scaling on V^n by each component, component-wise addition, and that fact that G fixes F point-wise, it is easy to check that the map φ is F-linear.

Now let's compute some kernels. The kernel of φ is computed to be

$$\begin{aligned} \ker \varphi &= \{x \in V \mid ({}^g x - x)_g = 0\} \\ &= \{x \in V \mid \forall g \in G :^g x - x = 0\} \\ &= V^G, \end{aligned}$$

by definition of the G-invariants. Similarly, the kernel of $E \otimes \varphi$ is computed to be $(E \otimes_F V)^G$. By lemma 5.11, $E \otimes \ker \varphi \cong \ker(E \otimes \varphi)$ as E-modules, so $E \otimes V^G \cong (E \otimes_F V)^G$ with the above kernel calculations in place. □

If we have a Galois extension E/F and its corresponding Galois group G, we can make E more manageable by enlarging it via the tensor product. When we do this, E unwinds into $\#G$ copies of E.

LEMMA 5.13. Let E/F be a Galois extension. Then $E \otimes_F E \cong E^{\#G}$ as E-algebras.

The fact that E can be an E-algebra over itself in more than one way if $\#G > 1$ (theorem 4.8) shows up clearly in this isomorphism.

PROOF. Note that $E \otimes_F E$ is E-split by proposition 4.36 and $E^{\#G}$ is obviously E-split, that $E \otimes_F E$ is an E-module with its standard E-module structure, and that $E^{\#G}$ is an E-module by $\lambda.(x_\sigma)_\sigma = (\lambda x_\sigma)_\sigma$, for any $\lambda \in E$.

We will show that the map

$$\nu : E \otimes_F E \to E^{\#G}$$

defined by $x \otimes y \mapsto (x^\sigma y)_\sigma$ is an isomorphism of E-algebras by showing that the map of sets

$$\bar{\psi} : \mathrm{Hom}_{E\text{-split } E\text{-alg}}(E^{\#G}, A) \to \mathrm{Hom}_{E\text{-split } E\text{-alg}}(E \otimes_F E, A)$$

defined by $\pi \mapsto \pi \circ \nu$ is an isomorphism for all E-split E-algebras A. We only need to consider E-split E-algebras because $E \otimes_F E$ and $E^{\#G}$ are E-split E-algebras themselves. The lemma statement will then be implied by the corollary to Yoneda's lemma (corollary 3.27).

Let B be an arbitrary E-split E-algebra. Then there exists a positive integer m such that $B \cong E^m$ as E-algebras. Now $\mathrm{Hom}(—, B) \cong \mathrm{Hom}(—, E^m) \cong \mathrm{Hom}(—, E)^m$, so we only have to show that

$$\psi : \mathrm{Hom}_{E\text{-alg}}(E^{\#G}, E) \to \mathrm{Hom}_{E\text{-alg}}(E \otimes_F E, E)$$

defined by $\pi_\sigma \mapsto \pi_\sigma \circ \nu$ is an isomorphism, where the elements in the domain are the familiar projections indexed by G (lemma 5.3). The reasoning for this is that ψ is an isomorphism if and only if the map between each component of $\mathrm{Hom}(E^{\#G}, E)^m \to \mathrm{Hom}(E \otimes_F E, E)^m$ is an isomorphism if and only if $\bar{\psi}$ is an isomorphism. The map ψ is independent of our choice of projections indexed by G because if $\pi_g = \pi_h$, then

$$\pi_g \circ \nu(x \otimes y) = \pi_g((x^\sigma y)_\sigma) = x^g y = x^h y = \pi_h \circ \nu(x \otimes y).$$

The step $x^g y = x^h y$ follows from the fact that $\pi_g = \pi_h$ if and only if $g = h$ if and only if ${}^g a = {}^h a$ for all $a \in E$.

We will now show that ψ is surjective. Note that the field E is both an F-vector space and an E-vector space. Pick an arbitrary but fixed $\sigma \in G$. Since σ is an F-algebra automorphism of E, it is a homomorphism of F-vector spaces by forgetting only the structure that makes it an algebra automorphism. By the universal property of base extending E to $E \otimes_F E$ by $x \mapsto 1 \otimes x$, there exists a unique homomorphism of E-vector spaces

$$f : E \otimes_F E \to E$$

defined by $x \otimes y \mapsto x^\sigma y$. We now observe that the map f is also an E-algebra homomorphism. The E-module E is given an E-module structure by $E \to E : x \mapsto {}^\sigma x$ and the E-module $E \otimes_F E$ is given an E-algebra structure by $E \to E \otimes_F E : y \mapsto 1 \otimes y$. Thus the universal property of base extension yields

$$\begin{aligned} \mathrm{Hom}_{E\text{-alg}}(E \otimes_F E, E) &= \mathrm{Hom}_{F\text{-alg}}(E, E) \\ &= \mathrm{Aut}(E/F) \\ &= G. \end{aligned}$$

In other words, an arbitrary E-algebra homomorphism $\varphi : E \otimes_F E \to E$ sends $x \otimes y$ to $x^\tau y$, for a fixed $\tau \in G$. The corresponding E-algebra homomorphism mapping $E^{\#G}$ to E is then the projection π_τ on index τ.

Since $\mathrm{Hom}_{E\text{-alg}}(E^{\#G}, E)$ consists only of the $\#G$ projections, its cardinality is the size of G. We have just shown that $\mathrm{Hom}_{E\text{-alg}}(E \otimes_F E, E)$ is equivalent to G, so its cardinality is also the size of G. Therefore ψ is an isomorphism. □

We now come to a proof of the essential surjectvity of η. The key idea in this proof is that for a Galois extension E/F, the fixed field E^G is F.

PROPOSITION 5.14. The functor η given in theorem 5.8 is essentially surjective.

PROOF. We need to show that for each G-E-vector space W, there exists an F-vector space V such that $E \otimes_F V \cong W$ as G-E-vector spaces.

Let B be an arbitrary G-E-vector space endowed with the G-E-module structure $\{i_g : B \to B \mid i_g(x.b) = {}^g(x.b) = ({}^g x).({}^g b)\}_g$. The g-E-linear maps i_g are written with an i to remind us that these make up the G-E-module structure we are using to find the G-invariants in B. For the remainder of this proof, we will call this G-action the G_i-action, and is what will be used to calculate G-invariants.

Consider the F-subspace consisting of the G-invariants in B, B^G (it is easy to check that this is an F-subspace). When we apply the functor η to B^G, we obtain the E-vector space $E \otimes_F B^G$. It is an E-vector space with the standard E-vector space structure (the E-action is on the first factor). The functor η provides it with the standard G-E-module structure

$$\{s_g : E \otimes_F B^G \to E \otimes_F B^G \mid s_g(x \otimes b) = ({}^g x) \otimes b\},$$

with a G-action (as opposed to the G_i-action) on the first factor. We will call this particular G-action the G-E-action. So we have two ways in which elements in G act on $E \otimes_F B$. One, the G_i-action, is used to construct the G-invariants $E \otimes_F B^G$ in $E \otimes_F B$ (it is now on the second factor), while the other, is the G-E-action which gives the G-E-module structure for $E \otimes_F B$.

Let's extend the F-vector space B^G to the E-vector space $E \otimes_F B^G$ by $b \mapsto 1 \otimes b$. The map $B^G \to B$ defined by $b \mapsto b$ is F-linear, so by the universal property of base extension (lemma 1.17), there exists a unique E-linear map

$$\varphi : E \otimes_F B^G \to B$$

defined by $x \otimes b \mapsto xb$. We need to show that this is an isomorphism of G-E-vector spaces. To do this, we will first prove the following string of G-E-vector space isomorphisms:

$$E \otimes_F B^G \cong (E \otimes_F B)^G \tag{5.1}$$

$$\cong (E \otimes_F E \otimes_E B)^G \tag{5.2}$$

$$\cong (E^{\#G} \otimes_E B)^G \tag{5.3}$$

$$\cong (B^{\#G})^G \tag{5.4}$$

$$\cong B, \tag{5.5}$$

for certain E-vector space structures, G-E-vector space structures, and G_i-actions on each of these (given the ones on B and $E \otimes_F B$). We will then show that this composition of isomorphisms is identically equal to φ, so that φ must also be a G-E-vector space isomorphism.

The E-actions, G_i-actions, and G-E-actions on each of the objects above, and the maps will now be given. It will then be shown that these maps are G-E-vector space isomorphisms. The following tables describe the E-actions and G-E-actions on each of these objects (without taking G-invariants), for an arbitrary $g \in G$. The superscript G's tell us what we are taking the G-invariants of (via the G_i-action).

Object	G-E-action
$E \otimes_F B^G$	${}^g(x \otimes b) = ({}^g x) \otimes b$
$(E \otimes_F B)^G$	${}^g(x \otimes b) = ({}^g x) \otimes b$
$(E \otimes_F E \otimes_E B)^G$	${}^g(x \otimes y \otimes b) = ({}^g x) \otimes y \otimes b$
$(E^{\#G} \otimes_E B)^G$	${}^g[(x_\sigma)_\sigma \otimes b] = ({}^g x_{g^{-1}\sigma})_\sigma \otimes b$
$(B^{\#G})^G$	${}^g(b_\sigma)_\sigma = (b_{g^{-1}\sigma})_\sigma$
B	${}^g b$

Object	E-action
$E \otimes_F B^G$	$\lambda.(x \otimes b) = (\lambda x) \otimes b$
$(E \otimes_F B)^G$	$\lambda.(x \otimes b) = (\lambda x) \otimes b$
$(E \otimes_F E \otimes_E B)^G$	$\lambda.(x \otimes y \otimes b) = (\lambda x) \otimes y \otimes b$
$(E^{\#G} \otimes_E B)^G$	$\lambda.[(x_\sigma)_\sigma \otimes b] = [(\lambda x_\sigma)_\sigma \otimes b]$
$(B^{\#G})^G$	$\lambda.(b_\sigma)_\sigma = ({}^{\sigma^{-1}}\lambda b_\sigma)_\sigma$
B	$\lambda.b$

The definitions for the G-E-actions together with the definitions of the E-actions on each object in the top two tables makes each object a G-E-vector space. To show this, we can check that each of the expressions for the G-E-actions gives a g-E-linear map (definition 4.16) that is associative for all $g \in G$ and that gives the identity on the corresponding objects for $g = \mathrm{id}$. We must also check that the E-actions on each object gives each object an E-module structure. It is straightforward to show all of these conditions.

Now we will give the G-E-vector space isomorphisms, using the above two tables of actions. After we show the following maps are G-E-vector space isomorphisms with respect to the G-E-module structure and the E-module structure, we will show that they also respect the G_i-action.

Note that we will be numbering these maps with subscripts according to how they are written above (equations 5.1 to 5.5), and we will denote the ones where we don't yet take the G-invariants with a bar. On some of these objects, we won't yet take the G-invariants, but the isomorphisms we are aiming for will still hold once we show that the G_i-action is respected by them.

First of all, the map

$$\varphi_1 : E \otimes_F B^G \to (E \otimes_F B)^G$$

defined by $x \otimes b \mapsto x \otimes b$ is an isomorphism of E-vector spaces by lemma 5.12. It is also obviously equivariant with respect to the G-E-action, so it is an isomorphism of G-E-vector spaces.

Now consider the map

$$\bar{\varphi}_2 : E \otimes_F B \to (E \otimes_F E) \otimes_E B$$

defined by $x \otimes b \mapsto x \otimes 1 \otimes b$. This map is the base extension of the E-linear isomorphism $B \to E \otimes_E B$ defined by $b \mapsto 1 \otimes b$. Since $E \otimes_F —$ is a functor

from the category of F-vector spaces to itself and functors preserve isomorphisms (example 3.16 and lemma 3.17), $\bar{\varphi}_2$ is an F-linear isomorphism. It is also E-linear under the given actions. The map $\bar{\varphi}_2$ is equivariant with respect to the G-E-action because for any $g \in G$,

$$^g(x \otimes b) = (^g x) \otimes b$$

is mapped to

$$^g x \otimes 1 \otimes b = {}^g(x \otimes 1 \otimes b).$$

Thus $\bar{\varphi}_2$ is a G-E-vector space isomorphism.

Let's move on to the map

$$\bar{\varphi}_3 : E \otimes_F E \otimes_E B \to E^{\#G} \otimes_E B$$

defined by $x \otimes y \otimes b \mapsto (x^\sigma y)_\sigma \otimes b$. By lemma 5.13, the map $E \otimes_F E \to E^{\#G}$ defined by $x \otimes y \mapsto (x^\sigma y)_\sigma$ is an isomorphism of E-vector spaces. Therefore $\bar{\varphi}_3$ is an isomorphism of E-vector spaces because for every E-module X, $— \otimes_E X$ is a functor from the category of E-modules to itself. It is also easy to check that $\bar{\varphi}_3$ is equivariant with respect to the G-E-action.

The fourth map we will consider is

$$\bar{\varphi}_4 : E^{\#G} \otimes_E B \to B^{\#G}$$

defined by $(x_\sigma)_\sigma \otimes b \mapsto ({}^{\sigma^{-1}} x_\sigma b)_\sigma$. The proof that this is an E-linear isomorphism is the same as the proof of lemma 1.26. It is also straightforward to check that this fourth map respects the G-E-action.

One can check that each of the above G-E-vector space isomorphisms (φ_1, $\bar{\varphi}_2$, $\bar{\varphi}_3$, and $\bar{\varphi}_4$) are equivariant with respect to the G_i-actions on the objects, where each of the G_i-actions on each of the objects are given in the following table:

Object	G_i-action
$E \otimes_F B^G$	$^g(x \otimes b) = x \otimes (^g b)$
$(E \otimes_F B)^G$	$^g(x \otimes b) = x \otimes (^g b)$
$(E \otimes_F E \otimes_E B)^G$	$^g(x \otimes y \otimes b) = x \otimes (^g y) \otimes (^g b)$
$(E^{\#G} \otimes_E B)^G$	$^g[(x_\sigma)_\sigma \otimes b] = (x_{\sigma g})_\sigma \otimes b$
$(B^{\#G})^G$	$^g(b_\sigma)_\sigma = (^g b_{\sigma g})_\sigma$
B	$^g b$

Thus

$$\begin{aligned} E \otimes_F B^G &\cong (E \otimes_F B)^G \\ &\cong (E \otimes_F E \otimes_E B)^G \\ &\cong (E^{\#G} \otimes_E B)^G \\ &\cong (B^{\#G})^G \end{aligned}$$

as G-E-vector spaces, because each of the four G-E-vector space isomorphisms above respect the G_i-actions.

Suppose that the first element in G is the identity. The G-invariants in $B^{\#G}$ can now be calculated. They are

$$\begin{aligned}(B^{\#G})^G &= \{(b_\sigma)_\sigma \mid \forall g \in G : ({}^g b_{\sigma g})_\sigma = (b_\sigma)_\sigma\} \\ &= \{(b_\sigma)_\sigma \mid \forall \sigma, g \in G : {}^g b_{\sigma g} = b_\sigma\} \\ &= \{(b_\sigma)_\sigma \mid \forall \sigma, g : b_{\sigma g} = {}^{g^{-1}} b_\sigma\} \\ &= \{(b_\sigma)_\sigma \mid \forall \sigma \in G : b_\sigma = {}^{\sigma^{-1}} b\}, \quad \text{choosing } b = b_{\mathrm{id}} \\ &= \{({}^{\sigma^{-1}} b)_\sigma \mid b \in B\}.\end{aligned}$$

In light of this, we finally turn our attention to the fifth map of interest:

$$\varphi_5 : (B^{\#G})^G \to B$$

defined by $({}^{\sigma^{-1}} b)_\sigma \mapsto b$. This map is well-defined because if ${}^{\sigma^{-1}} b = {}^{\sigma^{-1}} b'$ for all σ, then $b = b'$. Clearly φ_5 is bijective. It is E-linear because, for any $\lambda \in E$,

$$\lambda.({}^{\sigma^{-1}} b)_\sigma = ({}^{\sigma^{-1}} \lambda^{\sigma^{-1}} b)_\sigma = ({}^{\sigma^{-1}} (\lambda b))_\sigma$$

is mapped to λb. It is G-equivariant with respect to the G-E-action because

$${}^g({}^{\sigma^{-1}} b)_\sigma = ({}^{(g^{-1}\sigma)^{-1}} b)_\sigma = ({}^{\sigma^{-1} g} b)_\sigma = ({}^{\sigma^{-1}} ({}^g b))_\sigma$$

is sent to ${}^g b$. Similarly, φ_5 is G-equivariant with respect to the G_i-action, so G-invariants are preserved.

We must now check that

$$\varphi_5 \circ \bar{\varphi}_4 \circ \bar{\varphi}_3 \circ \bar{\varphi}_2 \circ \varphi_1 = \varphi.$$

To that end, pick an arbitrary simple tensor $x \otimes b$ in $E \otimes_F B^G$. Then

$$\begin{aligned}\varphi_5 \circ \bar{\varphi}_4 \circ \bar{\varphi}_3 \circ \bar{\varphi}_2 \circ \varphi_1(x \otimes b) &= \varphi_5 \circ \bar{\varphi}_4 \circ \bar{\varphi}_3 \circ \bar{\varphi}_2(x \otimes b) \\ &= \varphi_5 \circ \bar{\varphi}_4 \circ \bar{\varphi}_3(x \otimes 1 \otimes b) \\ &= \varphi_5 \circ \bar{\varphi}_4((x^\sigma 1)_\sigma \otimes b) \\ &= \varphi_5 \circ \bar{\varphi}_4((x)_\sigma \otimes b) \\ &= \varphi_5(({}^{\sigma^{-1}} xb)_\sigma) \\ &= \varphi_5(({}^{\sigma^{-1}} (xb))_\sigma), \quad \because b \in B^G \\ &= xb \\ &= \varphi(x \otimes b),\end{aligned}$$

completing the proof. □

The proof of the above proposition in a sense proves in more generality the standard result of classical Galois theory which says that the fixed field of a Galois extension E/F is F.

COROLLARY 5.15. If E/F is a Galois extension, then $E^G = F$.

PROOF. By the above lemma (taking $B = E$), we have that $E \otimes_F E^G = E = E \otimes_F F$, which implies that $E^G = F$. □

LEMMA 5.16. The functor η given in theorem 5.8 is faithful.

PROOF. Consider two F-vector space homomorphisms φ and ψ, and suppose that $\eta(\varphi) = \eta(\psi)$. Using the same notation as in corollary 1.28, the E-vector space maps $E \otimes_F \varphi$ and $E \otimes_F \psi$ are equivalent. Then by corollary 1.28, $\varphi = \psi$, proving the faithfulness of η. □

LEMMA 5.17. Let E/F be a Galois extension and let V be an F-module. Suppose $E \otimes_F V$ is given its standard E-module structure. Then $(E \otimes_F V)^G = F \otimes_F V$.

PROOF. The F-vector space $F \otimes_F V$ is a subspace of the E-vector space $E \otimes_F V$. Consider the map

$$\varphi : E \otimes_F (F \otimes_F V) \to E \otimes_F V$$

defined by $x \otimes (1 \otimes v) \mapsto x.(1 \otimes v) = x \otimes v$. We will show that φ is an isomorphism of E-vector spaces. The map $F \otimes_F V \to E \otimes_F V$ sending $1 \otimes v$ to itself is F-linear (easy to check), so the map φ given above is a unique E-linear map, by the universal property of base extension. Similarly, the map $V \to E \otimes_F (F \otimes_F V)$ defined by $v \mapsto 1 \otimes 1 \otimes v$ is F-linear, so there exists a unique E-linear map $\psi : E \otimes_F V \to E \otimes_F (F \otimes_F V)$ sending $x \otimes v$ to $x \otimes 1 \otimes v$. It is clear that the E-linear map ψ is an inverse to the E-linear map φ, so φ is an isomorphism of E-vector spaces. It then follows from lemma 5.9 that any F-basis of $F \otimes_F V$ is also an E-basis of $E \otimes_F V$.

Let $\{s_\sigma\}$ be the standard G-E-module structure on $E \otimes_F (F \otimes_F V)$. Then by the preceding two lemmas, there is a unique G-E-module structure on $E \otimes_F V$, which is trivially the standard G-E-module structure $\{t_\sigma\}_\sigma$. Note that

$$(E \otimes_F V)^G = \{x \otimes v \mid \forall \sigma \in G : \sigma(x) \otimes v = x \otimes v\}.$$

Clearly $F \otimes_F V \subset (E \otimes_F V)^G$.

Now let's prove the other inclusion. Choose an F-basis $\{1 \otimes e_i\}$ of $F \otimes_F V$. Then $\{1 \otimes e_i\}$ is an E-basis of $E \otimes_F V$. Thus any element in $E \otimes_F V$ is of the form $\sum_i x_i \otimes e_i$, where $x_i \in E$. Suppose that $\sum_i x_i \otimes e_i \in (E \otimes_F V)^G$. Then for every $\sigma \in G$, $t_\sigma(\sum_i x_i \otimes e_i) = \sum_i {}^\sigma x_i \otimes e_i$, which implies that $\sum_i ({}^\sigma x_i - x_i) \otimes e_i = 0$ for all $\sigma \in G$. But $\{1 \otimes e_i\}$ is a basis, so they are linearly independent. Hence ${}^\sigma x_i = x_i$ for all $x_i \in E$ and all $\sigma \in G$, which means that all x_i are in the fixed field F (we know this is the fixed field by corollary 5.15). Consequently, $\sum_i x_i \otimes e_i \in F \otimes_F V$ and we conclude that $(E \otimes_F V)^G = F \otimes_F V$. □

PROPOSITION 5.18. The functor η given in theorem 5.8 is full.

PROOF. Let V and W be two F-vector spaces. We need to show that for every G-E-vector space homomorphism

$$\varphi : E \otimes_F V \to E \otimes_F W,$$

where $E \otimes V$ and $E \otimes W$ both have the standard G-E-module structure, there exists a homomorphism of F-vector spaces $\psi : V \to W$ such that $\eta(\psi) = E \otimes \psi = \varphi$.

Let φ be such a G-E-vector space homomorphism sending $1 \otimes v$ to $\varphi(1 \otimes v)$. This map specifies where every simple tensor in $E \otimes_F V$ goes because it is assumed to be E-equivariant. We also know where every tensor goes because φ is assumed to be additive. We need to show that φ is the base extension of some F-vector space homomorphism from V to W. Consider the F-vector space homomorphism $\bar{\psi} : (E \otimes_F V)^G \to (E \otimes_F W)^G$ defined by $x \otimes v \mapsto \varphi(x \otimes v)$, where $x \in F$ because the G-invariants in the domain are calculated with respect to the standard G-E-module structure. We know that $\varphi(x \otimes v)$ is in $(E \otimes_F W)^G$ because

$${}^\sigma \varphi(x \otimes v) = \varphi({}^\sigma(x) \otimes v) = \varphi(x \otimes v)$$

for all $\sigma \in G$. This map is clearly F-linear because φ is E-linear by definition and $F \subset E$, so the map is uniquely defined by $1 \otimes v \mapsto \varphi(1 \otimes v)$. By lemma 5.17, $(E \otimes_F V)^G = F \otimes_F V$ and $(E \otimes_F W)^G = F \otimes_F W$, so we have an F-vector space homomorphism $\bar{\psi} : F \otimes_F V \to F \otimes_F W$ sending $1 \otimes v$ to $\varphi(1 \otimes v)$. Base extending this map, the expression $E \otimes \bar{\psi}(x \otimes 1 \otimes v) = \varphi(x \otimes v)$ holds. But $\mathrm{Hom}_F(F \otimes_F V, F \otimes_F W) \cong \mathrm{Hom}_F(V, W)$, so there is a unique F-vector space homomorphism $\psi : V \to W$ corresponding to $\bar{\psi}$, such that the diagram

$$\begin{array}{ccccccc}
V & \xrightarrow{\sim} & F \otimes_F V & \xrightarrow{=} & (E \otimes_F V)^G & \xrightarrow{\subset} & E \otimes_F V \\
\downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \bar{\psi}} & & \downarrow{\scriptstyle \bar{\psi}} & & \downarrow{\scriptstyle \varphi} \\
W & \xrightarrow{\sim} & F \otimes_F W & \xrightarrow{=} & (E \otimes_F W)^G & \xrightarrow{\subset} & E \otimes_F W
\end{array}$$

commutes Thus, $E \otimes \psi = \varphi$. □

This marks the end of the proof of theorem 5.8.

5.1.3. The E-split Algebra Case. The fundamental theorem of Galois theory (theorem 5.1) can now be attained in the categorical framework set up in the preceding two sections. We have proved that E-split G-E-algebras are equivalent to G-sets and that F-vector spaces are equivalent to G-E-vector spaces. What we need to do now is construct the equivalence

$$\Psi : E\text{-split } F\text{-algebras} \to E\text{-split } G\text{-}E\text{-algebras}$$

from the equivalence of categories η defined in theorem 5.8. To do this, we will characterize the categories $\mathcal{C} = E$-algebras and $\mathcal{D} = G$-E-algebras using the tensor product. Since functors respect tensor products, we will then automatically get the equivalence

$$\eta' : F\text{-algebras} \to G\text{-}E\text{-algebras}.$$

The sought equivalence Ψ will then just be a specific instance of η' because

$$E\text{-split } F\text{-algebras} \subset F\text{-algebras}$$

and

$$E\text{-split } G\text{-}E\text{-algebras} \subset G\text{-}E\text{-algebras}.$$

Lemma 5.19. Let M and N be two F-vector spaces. Then

$$\eta(M \otimes_F N) \cong \eta(M) \otimes_E \eta(N)$$

as G-E-vector spaces.

Proof. We begin by looking at $\eta(M \otimes_F N)$ and $\eta(M) \otimes_E \eta(N)$ more closely. For the former, we have

$$\eta(M \otimes_F N) = E \otimes_F (M \otimes_F N)$$

together with the standard G-E-module structure on it

$${}^g(x \otimes m \otimes n) = ({}^g x) \otimes m \otimes n.$$

The latter is

$$\eta(M) \otimes_E \eta(N) = (E \otimes_F M) \otimes_E (E \otimes_F N)$$

together with a combination of the two G-E-module structures on $(E \otimes_F M)$ and $(E \otimes_F N)$ given by η, so that

$${}^g(x \otimes m \otimes y \otimes n) = ({}^g x) \otimes m \otimes ({}^g y) \otimes n.$$

This expression, when defined for all $\sigma \in G$, does give $(E \otimes_F M) \otimes_E (E \otimes N)$ a G-E-module structure. Note that we give it an E-module structure via the rule

$$\lambda.(x \otimes m \otimes y \otimes n) = x \otimes m \otimes (\lambda y) \otimes n.$$

It is clear that the G-action is compatible with this E-module structure and that the G-action is additive. Furthermore, for $\sigma = \mathrm{id}$, we recover the identity on $(E \otimes_F M) \otimes_E (E \otimes N)$. Finally, the expression for the G-action is also associative.

We know that $(E \otimes_F M) \otimes_E E \cong E \otimes_F M$ as E-modules by $x \otimes m \otimes y \mapsto (xy) \otimes m$. Since $- \otimes_F N$ is a functor from the category of F-modules to itself (example 3.16), and functors preserve isomorphisms, we attain the E-linear isomorphism

$$\phi : (E \otimes_F M) \otimes_E (E \otimes_F N) \to (E \otimes_F M) \otimes_F N$$

defined by $x \otimes m \otimes y \otimes n \mapsto (xy) \otimes m \otimes n$.

We must check that ϕ is G-equivariant. To this end, let $g \in G$ be an arbitrary automorphism of E fixing F, and $x \otimes m \otimes y \otimes n$ be an arbitrary simple tensor in the domain of ϕ. Then

$${}^g(x \otimes m \otimes y \otimes n) = ({}^g x) \otimes m \otimes ({}^g y) \otimes n$$

is sent to

$$({}^g x {}^g y) \otimes m \otimes n = {}^g(xy) \otimes m \otimes n = {}^g(xy \otimes m \otimes n)$$

by ϕ (the second equality is true because g is a ring automorphism), completing the proof.

□

The preceding lemma tells us that η respects linear maps, so that η takes any F-module M with an F-linear map $\mu : M \otimes_F M \to M$ to an E-linear map

$$(E \otimes \mu) \circ \phi : (E \otimes_F M) \otimes_E (E \otimes_F M) \to E \otimes_F M$$

defined by $x_1 \otimes m_1 \otimes x_2 \otimes m_2 \mapsto x_1 x_2 \otimes \mu(m_1 \otimes m_2)$.

We will now check that the functor η also respects unit maps. Let (M, μ, i) be an F-algebra. The unit map $i : F \to M$ is transported to a unit map on E in the category of E-algebras given by

$$(E \otimes i) \circ \gamma : E \to E \otimes_F M$$

where $\gamma : E \to E \otimes_F F$ sending x to $x \otimes 1$ is an isomorphism and $E \otimes i$ is the base extension of i.

So η' sends any F-algebra (M, μ, i) to a G-E-algebra

$$(E \otimes_F M, (E \otimes \mu) \circ \phi, (E \otimes i) \circ \gamma),$$

where ϕ and γ are the isomorphisms defined in the above discussions.

It is straightforward to check that η' is a functor. The next step is to prove:

THEOREM 5.20. The functor η' is an equivalence of categories from F-algebras to G-E-algebras.

The functor η' respects the additional data we add to the category of F-modules to attain the category of F-algebras (see the discussion preceding and relating to lemma 4.14). That is, given an F-algebra (M, μ, i), and applying the functor η' to it, we attain a G-E-algebra. To this end, let (M, μ, i) be a fixed F-algebra, and consider $\eta'((M, \mu, i))$ calculated above. Then (using the same number as in the discussion preceding lemma 4.14):
(1) The multiplication rule $(E \otimes \mu) \circ \phi$ is commutative, because the diagram

$$\begin{array}{ccc} & x_1 \otimes m_1 \otimes x_2 \otimes m_2 \mapsto x_2 \otimes m_2 \otimes x_1 \otimes m_1 & \\ (E \otimes_F M) \otimes_E (E \otimes_F M) & \longrightarrow & (E \otimes_F M) \otimes_E (E \otimes_F M) \\ & (E \otimes \mu) \circ \phi \searrow \quad \swarrow (E \otimes \mu) \circ \phi & \\ & E \otimes_F M & \end{array}$$

commutes.

(2) The multiplication rule $\mu' = (E \otimes \mu) \circ \phi$ is associative, because the diagram

$$\begin{array}{ccc} (E \otimes_F M)^{\otimes 3} & \xrightarrow{\mu' \otimes \mathrm{id}} & (E \otimes_F M)^{\otimes 2} \\ \downarrow{\scriptstyle \mathrm{id} \otimes \mu'} & & \downarrow{\scriptstyle \mu'} \\ (E \otimes_F M)^{\otimes 2} & \xrightarrow[\mu']{} & E \otimes_F M \end{array}$$

commutes.

(3) The multiplication rules in E and $E \otimes_F M$ are compatible, because the diagram

$$\begin{array}{ccc} & x \otimes m \otimes \lambda \mapsto (x \otimes m) \otimes (\lambda \otimes 1) & \\ (E \otimes_F M) \otimes_E E & \longrightarrow & (E \otimes_F M)^{\otimes 2} \\ x \otimes m \otimes \lambda \mapsto (\lambda x) \otimes m \searrow & & \swarrow x \otimes m \otimes \lambda \otimes m' \mapsto (\lambda x) \otimes (mm') \\ & E \otimes_F M & \end{array}$$

commutes.

Now let's consider another F-algebra (N, ν, j). This F-algebra is sent to

$$(N, (E \otimes \nu) \circ \psi, (E \otimes j) \circ \zeta),$$

where

$$\psi : (E \otimes_F N) \otimes_E (E \otimes_F N) \to (E \otimes_F N) \otimes_F N,$$

sending $x_1 \otimes n_1 \otimes x_2 \otimes n_2$ to $x_1 x_2 \otimes n_1 \otimes n_2$, is the isomorphism of lemma 5.19, and

$$\zeta : E \to E \otimes_F F$$

sending x to $x \otimes 1$ is an isomorphism. After applying η' to an arbitrary F-algebra morphism $\varphi : M \to N$, we need to check that the resulting morphism $E \otimes \varphi : E \otimes_F M \to E \otimes_F N$ respects the multiplication rules and unit maps on $E \otimes M$ and $E \otimes N$, which were transported from the ones on M and N by η', and that it is G-equivariant. Doing so involves more diagram chasing. Note that the G-E-module structures on both $E \otimes M$ and $E \otimes N$ are the standard ones, which we will denote with $\{r_\sigma\}_{\sigma \in G}$ and $\{s_\sigma\}_{\sigma \in G}$, respectively.

(1') The map $E \otimes \varphi$ respects the multiplication rules because the diagram

$$\begin{array}{ccc} & \xrightarrow{(E \otimes \mu) \circ \phi} & \\ (E \otimes_F M)^{\otimes 2} & \longrightarrow & E \otimes_F M \\ \Big\downarrow{\scriptstyle (E \otimes \varphi) \otimes (E \otimes \varphi)} & & \Big\downarrow{\scriptstyle E \otimes \varphi} \\ (E \otimes_F N)^{\otimes 2} & \longrightarrow & E \otimes_F N \\ & \xrightarrow[(E \otimes \mu) \circ \psi]{} & \end{array}$$

commutes.

(2') The map $E \otimes \varphi$ respects the unit maps i and j because the diagram

$$\begin{array}{ccc} E \otimes_F M & \xrightarrow{E \otimes \varphi} & E \otimes_F N \\ & {\scriptstyle (E \otimes i) \circ \gamma} \nwarrow \quad \nearrow {\scriptstyle (E \otimes j) \circ \zeta} & \\ & E & \end{array}$$

commutes.

(3') The map $E \otimes \varphi$ is G-equivariant because for all $\sigma \in G$, the diagram

$$\begin{array}{ccc} & \xrightarrow{x \otimes m \mapsto x \otimes \varphi(m)} & \\ E \otimes_F M & \longrightarrow & E \otimes_F N \\ \Big\downarrow{\scriptstyle x \otimes m \mapsto ({}^\sigma x) \otimes m} & & \Big\downarrow{\scriptstyle x \otimes n \mapsto ({}^\sigma x) \otimes n} \\ E \otimes_F M & \longrightarrow & E \otimes_F N \\ & \xrightarrow[x \otimes m \mapsto x \otimes \varphi(m)]{} & \end{array}$$

commutes.

PROOF. (of theorem 5.20) This follows immediately from theorem 5.8 and the preceding discussion. □

How is the classical fundamental theorem of Galois theory derived from the equivalences we just proved? The equivalences of categories,

$$E\text{-split } F\text{-algebras} \xrightarrow[A \mapsto E \otimes_F A]{} E\text{-split } E\text{-algebras} \xrightarrow[B \mapsto \mathrm{Hom}_{E\text{-alg}}(B,E)]{} G\text{-sets},$$

gives the equivalence of categories (by transitivity),

$$\Omega : E\text{-split } F\text{-algebras} \to G\text{-sets},$$

defined by $A \mapsto \mathrm{Hom}_{E\text{-alg}}(E \otimes_F A, E) = \mathrm{Hom}_{F\text{-alg}}(A, E)$. The G-action on

$$\mathrm{Hom}_{F\text{-alg}}(A, E)$$

is given by $(g.f)(a) = g(f(a))$. Further, since equivalences preserve monomorphisms (lemma 3.23) and Ω is an anti-equivalence, the functor Ω sends monomorphisms to epimorphisms (because the morphisms are reversed). As a result, there is a bijection between intermediate algebras

$$F \hookrightarrow I \hookrightarrow E$$

and G-sets

$$\mathrm{Hom}_F(E,E) \twoheadrightarrow \mathrm{Hom}_F(I,E) \twoheadrightarrow \mathrm{Hom}_F(F,E).$$

Note that $\mathrm{Hom}_F(E,E) \cong G$ and $\mathrm{Hom}_F(F,E) = \{\mathrm{id}\}$. Now if I is an E-split F-algebra, then I is also a field by lemma 4.29. On top of that, the category of G-sets and the category of subgroups of G are equivalent, by lemma 3.25. Therefore, there is a bijection between intermediate field extensions I/F and subgroups H of the Galois group G. This is precisely the classical fundamental theorem of Galois theory (theorem 4.39).

EXAMPLE 5.21. Consider the Galois extension $\mathbb{C}/\mathbb{R}$, which has Galois group $G = \{1, \sigma\}$, where σ is complex conjugation. The $\mathbb{C}$-split $\mathbb{R}$-algebra $\mathbb{C}$ is sent to the G-set G, equipped with the G-action given by the above equivalence of categories.

However, we could equip the set G with a different G-set structure and ask what $\mathbb{C}$-split $\mathbb{R}$-algebra it corresponds to. Suppose the G-action on G is defined by sending everything in G to itself. In this case, following the equivalence of categories backwards yields the algebra $\mathbb{R} \times \mathbb{R}$ (c.f. example 4.21).

5.2. A Few Words on Infinite Field Extensions

We have dealt with the case of finite Galois extensions. But for an infinite Galois extension, not all subgroups of the Galois group are subgroups which fix some intermediate extension. A treatment of this case is found in the first chapter of [**8**], which we will very briefly summarize here. Let E be a (possibly infinite) Galois extension of a field F. Then any intermediate finite field extension can be embedded in a finite intermediate Galois extension. We can take the inverse limit of these intermediate finite Galois extensions $F \subset L \subset M \subset E$ together with the surjective homomorphisms $\mathrm{Gal}(M) \to \mathrm{Gal}(L)$ given by the fundamental theorem of Galois theory for finite field extensions we already proved. In particular, $G = \mathrm{Gal}(E)$ is a profinite group (it is the inverse limit of the system of groups above). Now one can

put a suitable topology on G so that the intermediate extensions corresponded to closed subgroups of G.

Fix separable and algebraic closures of F, $F_s \subset \bar{F}$. Note that these are Galois. If L is a finite separable extension of F, then one can define a continuous and transitive left action of the *absolute Galois group* $\mathrm{Gal}(F_s)$ on $\mathrm{Hom}_F(L, F_s)$ by precomposing with the absolute Galois group.

DEFINITION 5.22. A finite dimensional F-algebra is *etale* over F if it is isomorphic to a finite product of separable extensions of F.

LEMMA 5.23. A finite dimensional F-algebra A is etale if and only if $A \otimes_F \bar{F} \cong (\bar{F})^n$.

The more general statement for the fundamental theorem of Galois theory is the following.

THEOREM 5.24. Let F be a field. The functor from the category of finite etale F-algebras to the category of finite left continuous $\mathrm{Gal}(F_s)$-sets defined by $A \mapsto \mathrm{Hom}_F(A, F_s)$ is an equivalence of categories.

If E is a finite Galois extension of F, then theorem 5.1 is a restriction of the above theorem to finite etale F-algebras that are products of copies of E.

CHAPTER 6

Galois theory of Covering Spaces

We assume the reader is familiar with topological spaces (and basic properties of them such as connectedness), homotopy, and the fundamental group. We write the unit interval $[0,1] = I$.

There is a theory in topology that is deeply similar to the one we have considered so far in algebra. This topological theory is that of classifying covering spaces. In our treatment of the Galois theory of field extensions, we saw three major themes: (1) extensions splitting into simpler structures, (2) automorphism groups, and (3) classifying intermediate field extensions by subgroups of the Galois group. We will see all three of these themes in the classification of covering spaces.

The classification of covering spaces can be succinctly given as an equivalence of categories from the category of covering spaces of a given sufficiently nice topological space B to the category of $\pi_1(B)$-sets. Further, if we give the topological spaces under consideration additional structure, we can get more information about the covering spaces. In particular, Riemann surfaces are topological manifolds of complex dimension one with a complex structure and if we study their covering spaces, we obtain a connection between the Galois theory of fields and that of covering spaces. If X is a connected compact Riemann surface, then the category of compact Riemann surfaces Y with holomorphic maps $Y \to X$ is equivalent to the category of finite split algebras over the field of meromorphic functions of X. In this equivalence, finite Galois branched covers of X are in bijective correspondence with finite Galois extensions of the field of meromorphic functions of the same degree, providing the mentioned connection.

6.1. Classification of Covering Spaces

DEFINITION 6.1. Let E and B be topological spaces, and let $p : E \to B$ be a continuous surjective map. The space E is said to be a *covering space* of B, or *B-cover*, and p a *covering map*, if for every point $b \in B$ in the base space, there exists an open neighborhood U of b such that $p^{-1}(U)$ is a disjoint union of open subsets of E, each of which are mapped homeomorphically onto U by p. We will refer to a B-cover with a chosen basepoint b_0 as a *pointed B-cover*.

We will see that covering spaces E of B are analogous to field extensions E of F.

Given a covering space $p : E \to B$, we get an induced map p_* on fundamental groups for any $b \in B$ and $e \in p^{-1}(b)$, given by $p_* : \pi_1(E,e) \to \pi_1(B,b)$, $[\gamma] \mapsto [p \circ \gamma]$.

DEFINITION 6.2. If $p : E \to B$ is a covering space and $\varphi : B' \to B$ is any continuous map, then a *lift of φ* is a continuous map $\tilde{\varphi} : B' \to E$ such that $p \circ \tilde{\varphi} = \varphi$.

We will often use these two well-known lifting lemmas.

LEMMA 6.3. (Unique lifting property) If two lifts of a path agree at some point, then they are identically equal.

COROLLARY 6.4. (Path lifting property) Let $p : E \to B$ be a covering space. If $\alpha : I \to E$ is a path and $e \in E$ is given, with $p(e) = \alpha(0)$, then there exists a unique path $\tilde{\alpha}_e : I \to E$ such that $p \circ \tilde{\alpha} = \alpha$ and $\tilde{\alpha}_e(0) = e$ (the subscript e denotes where the path starts).

LEMMA 6.5. (Homotopy lifting property for paths) If $H : I \times I \to B$ is a homotopy and $e \in E$ is given, with $p(e) = H(0,0)$, then there exists a unique homotopy $\tilde{H}_e : I \times I \to E$ such that $\tilde{H}_e \circ p = H$ and $\tilde{H}_e(0) = e$.

Proofs of these lemmas are found in, e.g., [**6**].

The following is a useful result that tells us about homotopy of paths based on their initial and terminal points.

THEOREM 6.6. (Monodromy theorem) Let $(E, p : E \to B)$ be a covering space. Suppose f and g are two paths in B with the same initial point and the same terminal point, and let $\tilde{f}_e$ and $\tilde{g}_e$ be their lifts with the same starting point $e \in E$. Then $\tilde{f}_e \sim \tilde{g}_e$ if and only if $f \sim g$. In particular, if $f \sim g$, then $\tilde{f}_e(1) = \tilde{g}_e(1)$.

PROOF. ($\Rightarrow$) Composition with p preserves homotopy.
($\Leftarrow$) If $f \sim g$, then there is a homotopy H from f to g, which lifts to a homotopy $\tilde{H}$ from $\tilde{f}_e$ and some lift of g with initial point e by the homotopy lifting property. But the lift of g starting at e must be identically equal to $\tilde{g}_e$ by the unique lifting property.

In particular, since $\tilde{f}_e \sim \tilde{g}_e$, they must end at the same point. □

Given a covering space $(E, p : E \to B)$ and a basepoint $b_0 \in B$, there is a right group action of $\pi_1(B, b_0)$ on the fiber $p^{-1}(b_0)$.

THEOREM 6.7. (Monodromy action) Let $G = \pi_1(B, b_0)$. Continuing the discussion above, the map

$$G \times p^{-1}(b_0) \to \pi_1(B, b_0)$$

defined by

$$([\alpha], e) = e.[\alpha] \mapsto \tilde{\alpha}_e(1),$$

where $\tilde{\alpha}_e$ is the unique lift of α starting at e given by the path lifting property, is a right G-action. We call this G-action the *monodromy action*. If E is path-connected, then this action is transitive.

PROOF. We need to check that the map is well-defined. If e is any point in the fiber $p^{-1}(b_0)$, then by the path lifting property, and loop α based at b_0 has a unique lift to the path $\tilde{\alpha}_e$. Since α is a loop, $e.[\alpha] = \tilde{\alpha}_e(1) \in p^{-1}(b_0)$. The monodromy theorem tells us that our choice of α doesn't matter, because $\tilde{\alpha}_e(1)$ depends only on the path class of α.

Now let's check that this gives a right group action, i.e. that $e.[c_{b_0}] = e$ and that $(e.[\alpha]).[\beta] = e.(\alpha\beta)$, where c_{b_0} is the constant loop at b_0. The former follows immediately from the fact that c_e is the unique lift of c_{b_0}. For the latter, let $m = e.[\alpha]$. Then

$$e.([\alpha][\beta]) = e.[\alpha\beta] = (\tilde{\alpha}_e \tilde{\beta}_m)(1) = \tilde{\beta}_m(1) = (e.[\alpha]).[\beta].$$

Suppose that E is path-connected. Let e and e' be any two points in the fiber $p^{-1}(b_0)$. Since E is path-connected, there is a path α from e to e'. Project this path down to a path α' in B via $\alpha' = p \circ \alpha$. Clearly α is the unique lift of α' and $e.[\alpha'] = \alpha(1) = e'$. □

Note that this construction also works for paths in B, not just loops. If α is a path from b to b' in B, then we get a similar map

$$p^{-1}(b) \to p^{-1}(b')$$

by $e \mapsto \tilde{\alpha}_e(1)$. We will call this *transport* of e along the path α.

Until otherwise stated, the base space B and the basepoint b_0 are fixed. We define the category B-cov of B-covering spaces by declaring the objects to be covering spaces (E, p) and morphisms from (E, p) to (E', p') to be *maps of covering spaces* $\varphi : E \to E'$ such that $p' \circ \varphi = p$.

Since covers are the topological analogues of field extensions, we should have a notion of Galois covers.

Definition 6.8. A cover $p : E \to B$ is *Galois* if E is connected and E-split, i.e. $E \times_B E \cong E \times S$ for some discrete set S.

The above definition is equivalent to the standard definition of a Galois cover found in, e.g, [**6**].

Lemma 6.9. Let $p : E \to B$ be a connected cover. Then the following are equivalent:

(1) p is Galois
(2) $\mathrm{Aut}(E)$ acts transitively in $p^{-1}(b)$ for any $b \in B$,
(3) For all $b \in B$ and $e \in p^{-1}(b)$, $p_*\pi_1(E, e)$ is a normal subgroup of $\pi_1(B, b)$.

By the above lemma, if a cover $p : E \to B$ is Galois, then we can define the *relative fundamental group* $\pi_1(B, E) = \pi_1(B, b)/p_*\pi_1(E, e)$. The following lemma will be useful.

Lemma 6.10. Let $p : E \to B$ be a Galois cover. Then T is a $\pi_1(B, E)$-set if and only if it is a $\pi_1(B)$-set such that $\pi_1(E)$ acts on T trivially if and only if it is a $\pi_1(B, E)$-split $\pi_1(B)$-set.

Let's define a functor

$$F : B\text{-cov} \to G\text{-sets}$$

by sending each B-cover $(E, p : E \to B)$ to the G-set $p^{-1}(b_0)$ with the monodromy action, and each map of covering spaces $\varphi : (E, p) \to (E', p')$ to the induced map of fibers $p^{-1}(b_0) \to p'^{-1}(b_0)$ via the restriction of φ to the fiber $p^{-1}(b_0)$. This restriction maps onto the fiber $p'^{-1}(b_0)$ because $p' \circ \varphi = p$. It is also G-equivariant, as we will now show. Let $e \in E$ and suppose we have a loop $\alpha : I \to B$ in B based at $p(e)$. Then α lifts to a path $\tilde{\alpha}_e$ in E that starts at e and ends at $e.[\alpha]$. But it also lifts to a path $(\varphi \circ \tilde{\alpha})_{\varphi(e)}$ in E' that starts at $\varphi(e)$ and ends at $\varphi(e.[\alpha])$. Hence, $\varphi(e.[\alpha]) = \varphi(e).[\alpha]$, by the uniqueness of the lifts. It is easy to see that F is a functor.

The functor F is an equivalence of categories if we assume that the base space B is locally nice enough. In particular, we will assume that B satisfies the following three properties:

DEFINITION 6.11. (1) Let X be any topological space. The topological space X is *path-connected* if there exists a path between any two points in X.

(2) The space X is *locally path-connected* if it has a basis of path-connected open subsets.

(3) The space X is said to be *semi-locally simply connected* if for every point x in X, there exists a neighborhood U of x such that every loop in U is nullhomotopic, i.e., homotopic to a constant loop, in the whole space X.

Note that the space X is said to be *simply connected* if it is path-connected and $\pi_1(X, x)$ is trivial for every $x \in X$.

If the base space B satisfies these three properties, then it always has a simply connected covering space $(\tilde{B}, \tilde{p} : \tilde{B} \to B)$ that is universal in the sense that for any other covering space (E, p) of B, there is a unique map of covering spaces $Q : \tilde{B} \to B$ such that $\tilde{p} = p \circ Q$ [**6**]. The existence of such a covering space is proved in many references, including [**6**]. We will briefly outline the proof.

THEOREM 6.12. (Existence of universal covering space) If the space B is path-connected, locally path-connected, and semi-locally simply connected, then B has a simply connected (universal) covering space.

PROOF. Choose basepoint $b_0 \in B$. Let the points of the universal covering space $\tilde{B}$ be

$$\tilde{B} = \{[f] \mid f \text{ is a path from } b_0 \text{ to } b\}.$$

etc. □

We now come to the classification of covering spaces by conjugacy classes of subgroups of the fundamental group of the base space. This is the first step in finding the so-called fundamental theorem of Galois theory for covering spaces.

THEOREM 6.13. (Classification of covering spaces) If B is path-connected, locally path-connected and semi-locally path-connected, then F is an equivalence of categories.

We will prove that F is full, faithful, and essentially surjective in the following lemmas, which will imply theorem 6.13.

LEMMA 6.14. If B is path-connected, then the functor F is faithful.

PROOF. We closely follow Thomas Goodwillie's notes, [**7**]. We will show that

$$F : \mathrm{Hom}_{B\text{-cov}}((E, p), (E', p')) \to \mathrm{Hom}_{G\text{-set}}(p^{-1}(b_0), p'^{-1}(b_0))$$

is injective.

To that end, let $\varphi : E \to E'$ and $\psi : E \to E'$ be maps of B-covering spaces such that $F(\varphi) = F(\psi)$, i.e. $\varphi \restriction_{p^{-1}(b_0)} = \psi \restriction_{p^{-1}(b_0)}$. So if $e \in p^{-1}(b_0)$, then $\varphi(e) = \psi(e)$, and we need to show that this holds for all $e \in E$. Suppose α is a path from $p(e)$ to b_0 in B, which exists because B is path-connected. Let $\tilde{\alpha}$ be the unique lift of α to E that starts at e. Then both $\varphi \circ \tilde{\alpha}$ and $\psi \circ \tilde{\alpha}$ are unique lifts of α to E', and their reverses are unique lifts of the reverse of α. By assumption, they both start at $\varphi(\tilde{\alpha}(1)) = \psi(\tilde{\alpha}(1))$, since $\tilde{\alpha}(1) \in p^{-1}(b_0)$. The reverses are unique, so they are equal, and thus end at the same point, $\varphi(e) = \psi(e)$. □

LEMMA 6.15. If B is path-connected and locally path-connected, then the functor F is full.

PROOF. We closely follow Thomas Goodwillie's notes, [**7**]. We will show that

$$F : \mathrm{Hom}_{B\text{-cov}}((E,p),(E',p')) \to \mathrm{Hom}_{G\text{-set}}(p^{-1}(b_0), p'^{-1}(b_0))$$

is surjective.

Let (E,p) and (E',p') be covering spaces of B. We need to show that every G-equivariant map $f : p^{-1}(b_0) \to p'^{-1}(b_0)$ is $F(\varphi)$ for some map of covering spaces $\varphi : E \to E'$. We claim that the map $\varphi : E \to E'$ defined by

$$e \mapsto f(e.[\alpha]).[\bar{\alpha}],$$

where α is a path from $p(e)$ to b_0 and $\bar{\alpha}(t) = \alpha(1-t)$, is the corresponding map of covering spaces. The map φ does not depend on the choice of path α for the path class $[\alpha]$, for suppose that β is a different path from $p(e)$ to b_0. Then because $[\bar{\beta}][\alpha] \in G$ and f is G-equivariant,

$$\begin{aligned} f(e.[\alpha]) &= f\{e.([\beta][\bar{\beta}][\alpha])\}.[\bar{\alpha}] \\ &= f(e.[\beta]).([\bar{\beta}][\alpha][\bar{\alpha}]) \\ &= f(e.[\beta]).[\bar{\beta}]. \end{aligned}$$

We also need to check that φ is compatible with the projections p and p', i.e. that $p' \circ \varphi = p$ like so:

$$\begin{aligned} p' \circ \varphi(e) &= p'\{f(e.[\alpha]).[\bar{\alpha}]\} \\ &= p'\{f(e)\} \\ &= p(e). \end{aligned}$$

We will now show that φ is continuous. Let $e \in E$ be arbitrary. To show that φ is continuous at e, we will show that it is continuous near e, i.e. we will show local continuity. To this end, let $U \in B$ be a neighborhood of $p(e)$ such that $p^{-1}(U)$ and $p'^{-1}(U)$ are disjoint unions of open subsets of both E and E'. Such a neighborhood exists since p and p' are covering maps and we can take the intersection of each neighborhood that is evenly covered by E and E'. As such, there is a homeomorphism between $p^{-1}(U)$ and $U \times S$ for some discrete space S and a homeomorphism between $p'^{-1}(U)$ and $U \times S'$ for some discrete space S'. Let $t : U \times S \to E$ be the topological embedding of $E \times S$ into E, and similarly let $t' : U \times S' \to E'$ be the topological embedding of $E \times S'$ into E'. For our given point $e \in E$, there exists a unique $s \in S$ such that $t(e,s) = e$ (our point e lies on one of the sheets in E). We need to show that the restriction of φ to $U \times S$ is continuous at (e,s).

Writing the map $U \times S \to U \times S'$ as $(e,s) \mapsto (\xi(e,s), \zeta(e,s))$, our goal is to show that both ξ and ζ must be continuous at e. Let $\pi : U \times S \to U$ be the projection of $U \times S$ onto U and let $\pi' : U \times S' \to U$ be the projection of $U \times S'$ onto U. Since $\pi' \circ \varphi \restriction_{U \times S} = \pi$, we have that $\xi(e,s) = e$ for all $(e,s) \in U \times S$, which is continuous. We will now show that ζ is continuous. Let γ be a path in $U \times S$ from (e,s) to (e',s), which exists by local path-connectedness of B for a small enough subset of U (s is constant because any path in $U \times S$ must remain on the same sheet, so s is invariant). Next, notice that φ respects transport along paths in B (and so also in

N). For, suppose that β is a path from b to b' in B, let α_1 be any path from from b_1 to the basepoint b_0, and define $\alpha_2 = \bar{\beta}\alpha_1$. Then for any $x \in p^{-1}(b_1)$, we have

$$\begin{aligned}\varphi(e.[\beta]) &= f\{e.([\beta][\alpha_2])\}.[\bar{\alpha_2}] \\ &= f(e.[\alpha_1]).[\bar{\alpha_2}] \\ &= \varphi(e).([\alpha_1][\bar{\alpha_2}]) \\ &= \varphi(e).[\beta].\end{aligned}$$

Therefore, ζ must be constant on path components of U because our path was chosen to lie in $U \times \{s\}$. This implies that ζ is continuous at e. □

LEMMA 6.16. If B is path-connected, locally path-connected, and semi-locally simply connected, then the functor F is essentially surjective.

PROOF. The goal in this proof is to find the B-cover corresponding to the G-set G, and then to construct the cover of any G-set from this cover.

We claim that the covering space that corresponds to the G-set G is the universal cover $(\tilde{B}, \tilde{p} : \tilde{B} \to B)$, which exists by theorem 6.12. Let $e \in \tilde{B}$ be arbitrary. Consider the map

$$\psi : G \to F(\tilde{B}) = \tilde{p}^{-1}(b_0)$$

defined by $[\alpha] \mapsto \tilde{\alpha}_e(1)$.

The map ψ is well-defined by the monodromy theorem (theorem 6.6) and is clearly G-equivariant. To show that ψ is surjective, it is necessary and sufficient to show that the G-action on $F(\tilde{B})$ is simply transitive, i.e., that for every $x, y \in \tilde{B}$, there exists exactly one $g \in G$ with $x.g = y$. By theorem 6.7, the G-action is transitive on $F(\tilde{B})$. To see that it is simply transitive, suppose that α and β are loops in B based at b_0 with $e.[\alpha] = e.[\beta]$. Let $f = \tilde{\alpha}_e$ and $g = \tilde{\beta}_e$. Then fg^{-1} is a loop in $\tilde{B}$ based at e. Since $\tilde{B}$ is simply connected, $fg^{-1} \sim c_e$, i.e. $f \sim g$, and $\alpha \sim \beta$ by theorem 6.6.

Now suppose we have a transitive G-set S. Then $S = H \setminus G$, where H is the stabilizer group of some element s in S. To attain the corresponding covering space, we take the quotient of $\tilde{B}$ by the action of the H. This quotient is a cover of B because H acts properly discontinuously[1] on $\tilde{B}$. If S is any G-set, we can ←1 decompose it into its G-orbits (which are transitive G-sets) and take the disjoint union of the covers corresponding to each of these orbits. □

COROLLARY 6.17. Let $p : E \to B$ be a Galois cover. Then the restriction of the equivalence of categories above to the functor

$$E\text{-split } B\text{-cov } \to \pi_1(B, E)\text{-sets}$$

is an equivalence of categories.

PROOF. Since the above functor is an equivalence of categories, it respects fiber products. Since we are restricting the equivalence to subcategories that satisfy additional structure given in terms of fiber products (by lemma 6.10 and definition of splitness of covers), the functor in the corollary statement is an equivalence of categories. □

[1]If G is a group acting continuously from the left on a space E, then the action is *properly discontinuous* if each point $e \in E$ has an open neighborhood U such that $U \cap g.U = \emptyset$ for all $g \in G$, $g \neq 1$.

This corollary is really a more general statement than the above theorem. One can simply take the case of E being the universal cover of B to recover the theorem.

6.2. Riemann surfaces and their connection to field theory

Unless otherwise noted, holomorphic map will be taken to mean non-constant holomorphic map.

One way to find a relationship between the algebraic and topological Galois theories is to consider the covers of topological spaces with complex structure. In particular, we will consider covers of 1-dimensional complex manifolds, which are called Riemann surfaces. The main result will be that finite étale algebras over the field of meromorphic functions of a connected compact Riemann surface X correspond bijectively to Riemann surfaces with proper holomorphic surjections to X. These proper holomorphic surjections will be seen to be topological coverings away from closed discrete set of "bad" points. The treatment of this result follows chapter 3 of the excellent book [**8**]. For a detailed exposition of Riemann surfaces, see [**9**]. This reference also gives detailed account of the Riemann surfaces of algebraic functions, relevant to the following final topic we will consider. In particular, the power of above result will be shown by using it to translate the standard algebraic proof of the insolvability of quintic polynomials to a topological one. The treatment of this follows [**11**], which is a rigorous summary of the book [**12**].

6.2.1. Riemann surfaces and holomorphic maps.

Definition 6.18. A *Riemann surface* X is a Hausdorff space with an equivalence class of *complex atlases*, which are open coverings $\mathcal{U} = \{U_i\}_{i\in I}$ of X together with maps $\{f_i : U_i \to \mathbb{C}\}$, each of which mapping homeomorphically onto an open subset of $\mathbb{C}$ and such that $f_j \circ f_i^{-1} : f_i(U_i \cap U_j) \to \mathbb{C}$ is holomorphic (complex differentiable in a neighborhood of every point in its domain).

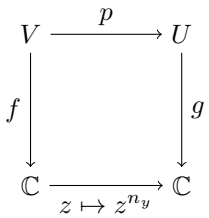
If we replace all of the $\mathbb{C}$'s in the above definition with $\mathbb{C}^n$, we obtain the definition of an n-dimensional complex manifold. The crucial aspect of Riemann surfaces is that we can define holomorphic maps between them. Intuitively, we expect morphisms of Riemann surfaces to be continuous maps that are locally holomorphic.

Definition 6.19. Let Y and X be Riemann surfaces. A *holomorphic* map $p : Y \to X$ is a continuous map such that for every pair $U \subset X$, $V \subset Y$ of open subsets satisfying $p(V) \subset U$ and complex charts $f : U \to \mathbb{C}$, $g : V \to \mathbb{C}$, the map $f \circ p \circ g^{-1} : g(V) \to \mathbb{C}$ is holomorphic.

Riemann surfaces with holomorphic maps form a category.

From now on, we will assume that all holomorphic maps are non-constant on connected components. The following lemma tells us that holomorphic maps of Riemann surfaces locally look like $\mathbb{C} \to \mathbb{C}$, $z \mapsto z^n$, where n is a positive integer.

Lemma 6.20. Let $p : Y \to X$ be a holomorphic map of Riemann surfaces, and pick a point $y \in Y$ with image $x = p(y) \in X$. Then there exist open neighborhoods V of y and U of x satisfying $p(Y) \subset X$, together with complex charts $g : V \to \mathbb{C}$, $f : U \to \mathbb{C}$ satisfying $f(x) = g(y) = 0$, and an integer $n_y > 0$ (independent of the charts) such that



commutes.

COROLLARY 6.21. Any holomorphic map $p : Y \to X$ of Riemann surfaces is open. Further, its fibers and set of branch points are closed discrete subsets of Y.

The map $z \mapsto z^n$ gives a cover of $\mathbb{C} \setminus \{0\}$, but not of $\mathbb{C}$. Nonetheless, the previous lemma shows that holomorphic maps locally look like this, and are thus locally are a point away from looking like topological covers.

DEFINITION 6.22. The positive integer n_y in the above lemma is called the *ramification index* of $p : Y \to X$ at the point $y \in Y$, and the points $y \in Y$ having ramification index $n_y > 1$ are called *branch points* of p.

Recall that a proper map of spaces means that its preimage of any compact subspace is compact. Proper holomorphic maps have desirable topological properties, as we will now observe.

DEFINITION 6.23. A *finite branched cover* $p : Y \to X$ is a proper surjective map of locally compact Hausdorff spaces such that there exists a closed discrete subset $S \subset Y$ so that p restricts to a finite topological cover $Y \setminus p^{-1}(p(S)) \to X \setminus p(S)$.

We can always obtain a finite branched cover from any proper holomorphic map of Riemann surfaces, as seen in the following lemma.

LEMMA 6.24. Let X be a connected Riemann surface, suppose $p : Y \to X$ is a proper holomorphic map, and denote by S the set of branch points of p. Then p is surjective, has finite fibers, and

$$Y \setminus p^{-1}(p(S)) \to X \setminus p(S)$$

is a finite (topological) covering space.

We now describe the connection between holomorphic maps and topological covers. Let X be a connected Riemann surface. Given a discrete closed subset $S \subset X$, denote by $\mathrm{Hol}(X, S)$ the category of Riemann surfaces Y together with holomorphic maps $Y \to X$, all of whose branch points are mapped to points in S. The morphisms in this category are holomorphic maps compatible with the projections onto X. Further, denote by $\mathrm{Cov}(X \setminus S)_f$ the category of finite (topological) covers of $X \setminus S$. It is proved in theorem 3.2.7 of [**8**] that these categories are equivalent. We state the key results used to prove this in the following two lemmas:

LEMMA 6.25. If $p : Y \to X$ is a connected covering space, then Y can be made into a Riemann surface so that p is a holomorphic map.

However, not every Riemann surface Y with a holomorphic map to X is a covering space in the topological sense.

EXAMPLE 6.26. Consider the holomorphic map $\mathbb{C} \to \mathbb{C}$ given by $z \mapsto z^2$. Then for the point $0 \in \mathbb{C}$, there is no neighborhood of it that is mapped homeomorphically onto an open subset of $\mathbb{P}^1$. Indeed, if $\epsilon \in U_0$, then $\epsilon^2 = (-\epsilon)^2$. However, if we remove 0 from both the target and source, then we get a covering map $\mathbb{C}^* \to \mathbb{C}^*$.

LEMMA 6.27. Let X be a connected Riemann surface. Suppose we have a discrete closed subset $S \subset X$ and a finite connected cover $p' : Y' \to X' = X \setminus S$. Then there exists a Riemann surface Y containing Y' as an open subset and a proper holomorphic map $p : Y \to X$ such that $p|_{Y'} = p'$ and $Y' = Y \setminus p^{-1}(S)$.

With the above two lemma, one can readily prove the following.

THEOREM 6.28. Let X be a connected Riemann surface and $S \subset X$ be a closed discrete subset of X. Then the functor $\mathrm{Hol}(X, S) \to \mathrm{Cov}(X \setminus S)_f$ defined by the restriction

$$(p : Y \to X) \mapsto (Y \setminus p^{-1}(S) \to X \setminus S)$$

is an equivalence of categories.

By the fully faithfulness of the above functor, we know that if $(p : Y \to X) \in \mathrm{Hol}(X, S)$, then

$$\mathrm{Aut}(Y) \cong \mathrm{Aut}_{\mathrm{Cov}(X \setminus S)}(Y \setminus p^{-1}(S)).$$

This justifies the following definition.

DEFINITION 6.29. Consider the above situation. If $Y \setminus p^{-1}(S) \to X \setminus S$ is a (topological) Galois cover, then we call $p : Y \to X$ a *finite Galois branched cover*.

This equivalence of categories provides a connection to the topological Galois theory (theorem 6.13).

LEMMA 6.30. If X is a connected Riemann surface and $S \subset X$ is a closed discrete subset of X, then $X \setminus S$ has a universal cover.

6.2.2. Connection to field theory. We now want to describe finite branched covers of a connected compact Riemann surface in terms of field theory.

DEFINITION 6.31. If X is a Riemann surface, define a *meromorphic function* $f : X \to \mathbb{C}$ to be a holomorphic function $X \setminus S \to \mathbb{C}$, where S is a closed discrete subset of X, such that for all complex charts $g : U \to \mathbb{C}$, the complex function $f \circ g^{-1} : g(U) \to \mathbb{C}$ is meromorphic (holomorphic on all of the domain except on a closed discrete subset).

Denote by $\mathcal{M}(X)$ the ring of meromorphic functions on X (it's a ring under the standard addition and multiplication of functions).

LEMMA 6.32. If X is a connected Riemann surface, then $\mathcal{M}(X)$ is a field.

Let $\hat{\mathbb{C}}$ be the Riemann sphere. Here are some facts about the field of meromorphic functions:

LEMMA 6.33. (1) Riemann existence theorem.
(2) $\mathcal{M}(X) \cong \{\text{holomorphic functions } X \to \hat{\mathbb{C}}\}$.
(3) $\mathcal{M}(X) \cong \mathbb{C}(x)$, the field of rational functions in $\mathbb{C}$.

If $p : Y \to X$ is a holomorphic map of Riemann surfaces, then we get a ring homomorphism $p^* : \mathcal{M}(X) \to \mathcal{M}(Y)$ defined by $f \mapsto f \circ p$. We will shortly see that if Y is a compact Riemann surface and X is a compact connected Riemann surface, $\mathcal{M}(Y)$ is a finite étale algebra over $\mathcal{M}(X)$.

LEMMA 6.34. If Y is a compact Riemann surface, X is a compact connected Riemann surface, and $p : Y \to X$ is a holomorphic map, then p is proper and surjective with finite fibers.

LEMMA 6.35. If Y is a compact Riemann surface, then $\mathcal{M}(Y) \cong \prod_i \mathcal{M}(Y_i)$, where each Y_i is a compact connected Riemann surface.

PROOF. If Y is compact, then $Y \cong \coprod_i Y_i$, where each Y_i is a compact connected Riemann surface. Thus, $\mathcal{M}(Y) = \mathcal{M}(\coprod_i Y_i) \cong \prod_i \mathcal{M}(Y_i)$. □

PROPOSITION 6.36. Let X and Y both be connected compact Riemann surfaces and let $p : Y \to X$ be a holomorphic map which has degree d as a branched cover. Then the field extension $\mathcal{M}(Y) \supset p^*\mathcal{M}(X)$ is a finite separable extension of degree d.

We are now ready to state the main result of this section, which relates the algebraic categorical Galois theory of field extensions to the topological categorical Galois theory of covers.

THEOREM 6.37. Let $\mathcal{C}$ be the category of compact Riemann surfaces Y mapping holomorphically onto a fixed compact connected Riemann surface X. Let $\mathcal{D}$ be the category of finite étale algebras over $\mathcal{M}(X)$. The functor $F : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ defined by $(p : Y \to X) \mapsto \mathcal{M}(Y)$ is an equivalence of categories. Under this equivalence, Galois branched covers of X correspond bijectively to Galois extensions of $\mathcal{M}(X)$.

We suspect that the above theorem provides a connection between the categorical Galois theory of field extensions (theorem 5.1) and the categorical Galois theory of covering spaces (corollary 6.17). But we need to find the correct definition for Y-split finite branched covers of X. We conjecture the following:

CONJECTURE 6.38. Let $p : Y \to X$ be a finite branched Galois cover with ramification points S and denote $(X', Y') = (X \setminus p^{-1}(S), Y \setminus S)$. Then

$$\begin{aligned}\text{finite } \pi_1(X', Y')\text{-sets} &\cong \text{finite } Y'\text{-split } \mathrm{Cov}(X') \\ &\cong \text{finite } Y\text{-split finite branched covers of } X \\ &\cong \text{finite } \mathcal{M}(Y)\text{-split } \mathcal{M}(X)\text{-algebras} \\ &\cong \text{finite } \mathrm{Gal}(\mathcal{M}(Y))\text{-sets.}\end{aligned}$$

6.3. The Abel-Ruffini theorem

We will now give a topological proof of the Abel-Ruffini theorem. This section follows [**11**] and [**12**].

THEOREM 6.39. (Abel-Ruffini) A general algebraic equation of degree 5 or more cannot be solved in radicals, i.e. there is no formula that expresses the roots of such an equation as functions of the coefficients by means of algebraic operations and extracting radicals.

For example, if $a, b, c \in \mathbb{Q}$, then we can express the roots of $ax^2 + bx + c$ with the quadratic formula. There are similar formulas for degrees 3 and 4. To prove the Abel-Ruffini theorem, we allow the coefficients to vary continuously in $\mathbb{C}$ minus the singular points.

DEFINITION 6.40. An *algebraic function* $y = f(x)$ is defined by the algebraic equation

$$F(x, y) = y^n + g_{n-1}(x)y^{n-1} + \cdots + g_0(x) = 0,$$

where each g_i is a polynomial. We will assume $g_n = 1$ because we don't lose any generality in doing so.

We can construct a Riemann surface for any algebraic function by analytically continuing the solutions to an algebraic function. We will briefly summarize how this is done. A detailed treatment can be found in [**9**].

Let $\{s_i\}$ be the singular points of an algebraic function $y = f(x)$ and write $\mathbb{C}' = \mathbb{C} \setminus \{s_i\}$. Pick an $a \in \mathbb{C}'$ satisfying $F(a, y) = 0$ with n distinct roots $y = z_i$. Then $\frac{dF(a,y)}{dy} \neq 0$ and the implicit function theorem says that there exists a neighborhood U_a of a such that for all $x \in U_a$, $F(x, y) = 0$ also has n distinct solutions. We label these solutions $y = f_{a,i}(x)$, and call them *branches* of the algebraic function $y = f(x)$. By shrinking U_a so that each branch $f_{a,i}$ has a convergent Taylor series at a. We call the pairs $(f_{a,i}, U_a)$ *analytic elements* of f.

We can continue an analytic element (f_a, U_a) along any path $\gamma : I \to \mathbb{C}'$ beginning at a and ending at any $a' \in \mathbb{C}'$. To do this, we can take a sufficiently fine partition $0 = x_0 < x_1 < \cdots < x_k = 1$ of I that partitions the path γ, and cover the path with analytic elements $(f_a^{(j)}, U_a^{(j)})$, one at each point $\gamma(x_j)$, such that $f_a^{(j)} = f_a^{(i-1)}$ on $U_a^{(j)} \cap U_a^{(j-1)}$ for each $j = 1, \ldots, k$. The final analytic element $(f_{a'}, U_{a'})$ obtained is called the *prolongation* of (f_a, U_a) along γ. This prolongation is unique by the monodromy theorem (theorem 6.6).

The union of all prolongations along all possible paths obtained from each branch $f_{a,i}$ is the Riemann surface M of the algebraic function f. The Riemann surface M comes with a projection $p : M \to \mathbb{C}'$ defined by $f_z(x) \mapsto x$, where f_z is a branch of $z \in \mathbb{C}'$. We can compactify M and smooth out its cusps[2] ←2

The following figure shows the Riemann surface of the algebraic function $f(x) = \sqrt{x}$, defined by $F(x, y) = y^2 - x = 0$, obtained via analytic continuation.

Consider a general degree n algebraic function f and pick a basepoint a. Let $(M, p : M \to \mathbb{C}')$ be the Riemann surface of f. Further, let α be a loop in $\mathbb{C}'$. Choosing a point $z_j \in p^{-1}(a)$ and lifting α, we obtain a path in M that terminates at some point $z_k \in p^{-1}(a)$. This is the monodromy action we have seen before. We thus obtain a homomorphism $\varphi : \pi_1(\mathbb{C}', a) \to S(p^{-1}(a))$, where $S(p^{-1}(a))$ is the group of permutations of the fiber $(p^{-1}(a)$.

DEFINITION 6.41. The *monodromy group* $\mathrm{Mon}(f)$ of f is defined to be the image of φ.

EXAMPLE 6.42. $\mathrm{Mon}(\sqrt{x}) \cong \mathbb{Z}/2\mathbb{Z}$.

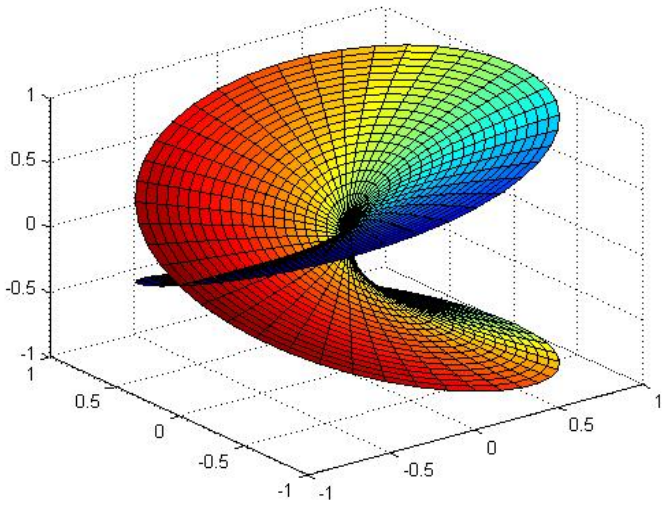
DEFINITION 6.43. A *typical algebraic function* is an algebraic function defined by $F(x, y) = 0$ such that

$$\Gamma = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

is smooth, the restriction of the map $\mathbb{C}^2 \to \mathbb{C}$ sending (x, y) to x to Γ has only non-degenerate critical points with different critical values as singularities[3], and F ←3

[2]One does this by filling in the singular points $\{s_i\}$ of the algebraic function, adding a point at infinity, and then compactify it by defining a hole chart $z \mapsto 1/z$ to fill in zero in the same way [**10**]. This will yield $\hat{\mathbb{C}}$. The Riemann surface $M \to \hat{\mathbb{C}}$ can then be shown to be compact as well.

[3]This means that only two branches of the algebraic function are glued at a time.



is an irreducible polynomial.

LEMMA 6.44. Let f be a typical algebraic function. Then Mon is generated by transpositions, which correspond to exchanging branches $f_k(x)$ and $f_j(x)$, and Mon acts transitively on each fiber.

LEMMA 6.45. If a subgroup $G \subset S_n$ is transitive and is generated by transpositions, then $G = S_n$.

COROLLARY 6.46. If f is a typical algebraic function of degree n, then $\mathrm{Mon}(f) \cong S_n$.

PROOF. Observe that $S(p^{-1}(a)) \cong S_n$. □

EXAMPLE 6.47. Let $F(x, y) = 3y^5 - 25y^3 + 60y - x = 0$. This is a typical algebraic function of degree 5. Thus Mon $\cong S_5$. One can fine a typical algebraic function of any degree greater than 5 as well. It is well known that S_n is not solvable for $n \geq 5$ [**1**].

By corollary 6.38 and the fact that the field of meromorphic functions of the Riemann sphere is the same as the field of rational functions in $\mathbb{C}$, we can deduce that the monodromy group of an algebraic function is isomorphic to the Galois group of the extension of the field of rational function by branches of the algebraic function.

DEFINITION 6.48. An algebraic function $y = f(x)$ is *represented in radicals* if it can be obtained with constant functions $x \mapsto c$ and the identity function $x \mapsto x$ by means of addition, subtraction, multiplication, division, and extracting positive integer radicals.

EXAMPLE 6.49. The algebraic function

$$f(x) = \frac{3i \pm \sqrt[7]{x^2 - \sqrt{x}}}{2x}$$

is one represented in radicals.

In light of the previous example, to prove the Abel-Ruffini theorem, it suffices to show that the monodromy group of an algebraic function represented in radicals is solvable. We will first describe how to construct the Riemann surface of an algebraic function represented in radicals by cutting and gluing sheets of $\mathbb{C}$.

Let f and g be algebraic functions with branches $f_1, \ldots, f_p$ and $g_1, \ldots, g_q$, respectively. To construct the Riemann surface of $h = f + g$, take pq sheets of $\mathbb{C}$ and on each of them cut from every singular point of f and g out to infinity in such a way that none of the cuts intersect (these are called *branch cuts*). Label each of these sheets by $h_{i,j}$ Suppose that after running around a singular point, we move from f_{i1} to f_{i2} and from g_{j1} to g_{j2}. Then we glue the edges of the cuts so that we move from the sheet $h_{i1,j1}$ to the sheet $h_{i2,j2}$ when going around the same singular point. After doing this for all possible combinations of branches of f and g, identify the sheets $h_{i,j}$ that have equal values on the sums of the branches $f_i + g_j$. This completes the construction of the Riemann surface of the algebraic function $f + g$. The constructions for $f - g$, fg, and f/g are similar.

The construction for $h = \sqrt[k]{f}$ goes a bit differently than above. The algebraic function h has kp branches $h_{j,l}(x) = e^{2\pi ij/k} h_{0,l}(x)$, where $j = 0, \ldots, k-1$, $l = 1, \ldots p$, and $h_{0,l}(x)$ is a chosen branch of $\sqrt[k]{f_l(x)}$. To construct the Riemann surface of h, replace every sheet of the Riemann surface of f by a file of k cut sheets. Now, when we run around a branch point of h (in this case we have the singular points of f, and the zeroes and poles of $f_l(x)$ for each l), we move from all the sheets of one file to all the sheets of another file. Moving from one file to another corresponds to moving from one sheet of the Riemann surface of f to another. Thus, if looping around a branch point b takes us from f_{l1} to f_{l2}, then we glue the cuts of the sheets of the $l1$th file to the cuts of the sheets of the $l2$th file like how we did in the previous paragraph. When moving from one file to another, the indexing of the sheets in the files is permuted cyclically (and is not permuted when $f_{l1} \neq 0, \infty$).

Here are some properties of solvable groups that we will use.

LEMMA 6.50.
(1) A subgroup of a solvable group is solvable.
(2) The product $G \times H$ of solvable groups is solvable.
(3) If H is solvable and there exists a surjective homomorphism $G \to H$ with abelian kernel, then G is solvable.
(4) If G is solvable and $G \to H$ is surjective, then H is solvable.

PROPOSITION 6.51. The monodromy group of an algebraic function expressed in radicals is solvable.

We can use corollary 6.38 to consider the Riemann surfaces of functions expressed in radicals as field extensions of $\mathbb{C}(x)$ and then use standard Galois theory. But this will be mostly a topological proof.

PROOF. Since the monodromy groups of constant functions and identity functions are solvable, it suffices to show that if f and g have solvable monodromy groups $\mathrm{Mon}(f)$ and $\mathrm{Mon}(g)$, then $\mathrm{Mon}(f \pm g)$, $\mathrm{Mon}(fg^{\pm 1})$, and $\mathrm{Mon}(\sqrt[k]{f})$ are solvable. In constructing the Riemann surface of $f + g$, the monodromy group of the surface Y obtained after gluing all the sheets is isomorphic to a subgroup K of $\mathrm{Mon}(f) \times \mathrm{Mon}(g)$. Thus, by (1) and (2) of the preceding lemma, K is solvable. When we identify entire sheets in the second step, the elements of K that permuted the sheets that were identified in this part of the construction are mapped to 1 in

$\mathrm{Mon}(f+g)$. But we have a surjective homomorphism $K \to \mathrm{Mon}(f+g)$ because any element in the codomain comes from a permutation of a fiber of Y. Part (4) of the above lemma then implies that $\mathrm{Mon}(f+g)$ is solvable. The proofs of the subtraction, multiplication, and division cases are similar.

All that's left to show is that $\mathrm{Mon}(\sqrt[k]{f})$ is solvable. Since moving from one sheet of the Riemann surface of f to another corresponds to moving from one file to another, we have a surjective homomorphism $\varphi : \mathrm{Mon}(\sqrt[k]{f}) \to \mathrm{Mon}(f)$. Since in the construction of h's Riemann surface, sheets in the files are permuted cyclically, the kernel of φ must be isomorphic a cyclic group whose order divides k. Thus, the kernel of φ is an abelian group, and invoking part (3) of the above lemma completes the proof. □

This concludes the proof of the Abel-Ruffini theorem.[4] ←4

In proving that $\mathrm{Mon}(\sqrt[k]{f})$ is solvable, we have seen a topological analogue of the following proposition.

PROPOSITION 6.52. Let F be a field of characteristic not dividing k and suppose it contains the kth roots of unity. Then the extension field $F(\sqrt[n]{a})$ for $a \in F$ is Galois, having cyclic Galois group of order dividing k.

Conclusion

The classical study of roots began the study of a new class of mathematical objects. Galois would probably be amazed to see how far his study of the roots of polynomials has come. We have seen how the classical fundamental theorem of Galois theory can be generalized in categorical language that allows us to see connections with an analogous theory in topology: that of classifying covering spaces. By considering covers of Riemann surfaces, we saw how these two similar theories in two different fields of mathematics relate. Although this is interesting in itself, we have also seen how it is a powerful tool by looking at a topological proof of the Abel-Ruffini theorem.

[4]This method of proving the Abel-Ruffini theorem seems stronger than the standard algebraic one. Say we add $exp(x)$ to the list of allowed operations. Standard Galois theory can't say anything about this.

Bibliography

[1] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 3rd ed., 2004.

[2] F. William Lawvere and Stephen H. Schanuel. *Conceptual Mathematics: A first introduction to categories*. Cambridge University Press, 1997.

[3] S. Mac Lane. *Categories for the Working Mathematician*. Springer Graduate Texts in Mathematics 5, 2nd edition, 1997.

[4] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Inc., 3rd edition, 1993.

[5] Christian Kassel. *Quantum groups*. Springer Graduate texts in Mathematics 155, 1995.

[6] John M. Lee . Introduction to Topological Manifolds. Springer Graduate Texts in Mathematics 202, 2nd ed., 2000.

[7] Thomas Goodwillie. *The Classification of Covering Spaces*. Personal Collection of Thomas Goodwillie, Brown University, Providence, RI. http://www.math.brown.edu/ tomg/covering%20spaces.pdf, accessed 2013.

[8] T. Szamuely. Galois Groups and Fundamental Groups. Cambridge Studies in Advanced Mathematics, Vol. 117, 2009.

[9] Otto Forster. *Lectures on Riemann Surfaces*. Springer Graduate Texts in Mathematics 81, 1981.

[10] Rick Miranda. *Algebraic Curves and Riemann Surfaces*. AMS Graduate studies in mathematics, Vol. 5, 1995.

[11] H. Zoladek. *The topological proof of the Abel-Ruffini theorem*. Topol. Methods Nonlinear Anal. 16, 2000, 253265.

[12] V. B. Alekseev. *Abel's Theorem in Problems and Solutions*. Springer, 2004.

[13] A. Grothendieck, et. al. *SGA1 Revêtements étales et groupe fondamental*, 1960-1961'. Lecture Notes in Mathematics 224. Springer Verlag, 1971.