Rose-
Hulman
Undergraduate
Mathematics
Journal

# Category Theory and Galois Theory

Amanda Bower[a]

Volume 14, No. 1 , Spring 2013

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]University of Michigan–Dearborn

Rose-Hulman Undergraduate Mathematics Journal
Volume 14, No. 1 , Spring 2013

# Category Theory and Galois Theory

Amanda Bower

**Abstract.** Galois theory translates questions about fields into questions about groups. The fundamental theorem of Galois theory states that there is a bijection between the intermediate fields of a field extension and the subgroups of the corresponding Galois group. After a basic introduction to category and Galois theory, this project recasts the fundamental theorem of Galois theory using categorical language and illustrates this theorem and the structure it preserves through an example.

**Acknowledgements**: I would like to sincerely thank Professor Thomas Fiore for his continual support, encouragement, and invaluable guidance throughout this entire project.

# 1 Introduction

Category theory finds similar relationships between objects and properties in different fields, like analysis, algebra, and topology. In some cases, recasting certain problems in the language of category theory can even make these problems easier to deal with and solve. In fact, when using category theory to prove certain statements, many of the details that would normally be needed can be avoided. For instance, epsilons and deltas can be avoided in continuity proofs on product spaces in analysis when using categorical methods. However, it should be noted that category theory is not just a language. It also has its own deep, important theorems.

In this paper, we restate the fundamental theorem of Galois theory using the language of category theory. The fundamental theorem of Galois theory explains the correspondence between the subgroup lattice and the subfield lattice at the end of Section 3. Galois theory is a bridge between field theory and group theory. In other words, through Galois theory, certain problems in field theory can be translated to problems in group theory. A functor in category theory models this type of relationship, which is the motivation for why we can restate the fundamental theorem of Galois theory using categorical language. A functor is a structure preserving way to move from one mathematical area (e.g. fields) to another mathematical area (e.g. groups). Categorical aspects of Galois theory have been considered by Borceux and Janelidze [1].

# 2 Categories, Functors, and Natural Transformations

In the early 1940s, Eilenberg and MacLane formulated the notions of categories, functors, and natural transformations in the setting of group theory and algebraic topology, where category theory thrived and took off. For the first two papers in category theory, see [3] and [4]. In this section, we define category, functor, and natural transformation. We then briefly look at simple examples to build intuition.

**Definition 2.1.** A *category* $\mathscr{C}$ consists of a class $\mathrm{ob}(C)$ of *objects* and a class $\mathrm{mor}(C)$ of *morphisms* together with functions called domain, codomain, and composition, and identities as follows.

- Each morphism $f$ of $\mathscr{C}$ has a domain $c_1$ and codomain $c_2$, which are objects of $\mathscr{C}$. This relationship is denoted $f : c_1 \to c_2$.
- For any pair of morphisms $f$ and $g$ such that $f : c_1 \to c_2$ and $g : c_2 \to c_3$, there exists a chosen morphism $h$ in $\mathscr{C}$ called the *composite*, so that $g \circ f = h : c_1 \to c_3$. In other words, $\mathscr{C}$ is closed under composition of morphisms.
- For each object $c \in \mathscr{C}$, there exists an identity morphism $1_c : c \to c$ in $\mathscr{C}$ such that for any morphisms $g : c_1 \to c$ and $h : c \to c_2$, we have $1_c \circ g = g$ and $h \circ 1_c = h$.

- Composition of morphisms is associative. In other words, for any morphims

$$c_1 \xrightarrow{f} c_2 \xrightarrow{g} c_3 \xrightarrow{h} c_4$$

in $\mathscr{C}$, we have $(h \circ g) \circ f = h \circ (g \circ f)$.

**Definition 2.2.** A category is called *small* when the classes $\mathrm{ob}(C)$ and $\mathrm{mor}(C)$ are sets, as opposed to proper classes.

The basic idea of a category is ubiquitous throughout mathematics as the following example illustrates.

**Example 2.3.**
1. **Set** is the category where the objects of **Set** are sets and the morphisms of **Set** are functions.
2. **Grp** is the category where the objects are small[1] groups and the morphisms are group homomorphisms.
3. For a fixed field $k$, $\mathbf{Vect_k}$ is the category where the objects are small vector spaces over $k$ and the morphisms are linear maps. We will take a closer look at an extended example concerning vector spaces at the end of this section.
4. **Top** is the category of small topological spaces where continuous maps are the morphisms.

In Example 2.3, the morphisms in each case were functions. However, morphisms do not necessarily have to be functions.

**Example 2.4.** Consider the natural numbers $\mathbb{N}$. For any $x, y \in \mathbb{N}$ define a unique morphism $f : x \to y$ if and only if $x \leq y$. If there is a morphism from $x$ to $y$, we will denote this morphism by $x \leq y$. The set $\mathbb{N}$ along with " $\leq$ " forms a category. This example generalizes to any partially ordered set (poset).

In linear algebra, what is important to study are the linear maps between vector spaces, not necessarily the vector spaces themselves. Studying the linear maps can reveal much structure about the vector spaces. For instance, under certain conditions, given a linear operator $T : V \to V$ on a vector space, we can decompose $V$ into its eigenspaces corresponding to $T$, which reveals much structure of $V$. Moreover, this same idea is true in subjects such as algebra and topology. In fact, in representation theory, studying a class of group homomorphisms from a fixed group to the general linear group of certain vector spaces can lead to important information about the group itself. Similarly, in category theory, studying the maps between categories is fruitful and provides insight into the structure of the categories themselves.

[1]By a *small* group, we mean each group is composed of a set with a binary operation as opposed to a proper class with a binary operation. In general, a mathematical object consisting of a *set* and some other structure is called *small*. For instance, a small vector space (or a small topological space) has an underlying set, as opposed to an underlying proper class.

**Definition 2.5.** Let $\mathscr{C}$ and $\mathscr{B}$ be categories. A *(covariant) functor* $F : \mathscr{C} \to \mathscr{B}$ is composed of two functions: an object function and a morphism function both denoted by $F$. The object function of $F$ assigns to objects of $\mathscr{C}$ objects of $\mathscr{B}$. The morphism function of $F$ assigns to morphisms $f : c_1 \to c_2$ of $\mathscr{C}$ morphisms $Ff : Fc_1 \to Fc_2$ of $\mathscr{B}$ subject to the following:

- If $f : c_1 \to c_2$ and $g : c_2 \to c_3$ are morphisms of $\mathscr{C}$, then $F(g \circ f) = Fg \circ Ff$.
- For any identity morphism $1_c : c \to c$ of $\mathscr{C}$, $1_{Fc} = F1_c : Fc \to Fc$.

A *contravariant functor* $T$ between two categories $\mathscr{C}$ and $\mathscr{B}$, as opposed to a covariant functor, also assigns to objects of $\mathscr{C}$ objects of $\mathscr{B}$. However, $T$ assigns to morphisms $f : c_1 \to c_2$ of $\mathscr{C}$ morphisms $Tf : Tc_2 \to Tc_1$ of $\mathscr{B}$ such that identity morphisms are sent to identity morphisms and for any $f : c_1 \to c_2$ and $g : c_2 \to c_3$ of $\mathscr{C}$, $T(g \circ f) = T(f) \circ T(g)$. In other words, contravariant functors reverse the direction of the morphisms.

In algebraic topology, an important example of a covariant functor is the functor from pointed topological spaces to **Grp** given by the fundamental group. We will encounter a contravariant functor in the next section. Moreover, functors are used to describe another basic idea in category theory: natural transformations.

**Definition 2.6.** Let $\mathscr{C}$ and $\mathscr{D}$ be categories and $F, G : \mathscr{C} \to \mathscr{D}$ be functors. A *natural transformation* $\eta : F \to G$ is a function that assigns to every object $c$ of $\mathscr{C}$ a morphism $\eta_c : Fc \to Gc$ of $\mathscr{D}$ such that for every morphism $f : c_1 \to c_2$ of $\mathscr{C}$, the diagram below commutes.

$$\begin{array}{ccc} Fc_1 & \xrightarrow{\eta_{c_1}} & Gc_1 \\ {\scriptstyle Ff}\downarrow & & \downarrow{\scriptstyle Gf} \\ Fc_2 & \xrightarrow[\eta_{c_2}]{} & Gc_2 \end{array}$$

To illustrate the importance of natural transformations, we show how a familiar result from linear algebra can be described by a natural transformation. Recall from linear algebra that given a vector $v$ in a vector space $V$ with a chosen ordered basis $\beta$, we write the *coordinate vector of $v$ with respect to $\beta$* as $[v]_\beta$. Similarly, given a linear transformation $T : (V, \beta) \to (W, \gamma)$, we denote the *matrix representation of $T$ with respect to $\beta$ and $\gamma$* as $[T]^\gamma_\beta$.

**Example 2.7.** In this extended example, we revisit the familiar equation $[T]^\gamma_\beta[v]_\beta = [Tv]_\gamma$ from the point of view of naturality, and see how "compute the coordinate vector" is a natural transformation.[2] This equation means it does not matter if we first evaluate $T(v)$ and then write the coordinate vector of $T(v)$ with respect to $\gamma$ or if we first multiply the

[2]I thank Professor Thomas Fiore for explaining to us in our linear algebra class the basic categorical notions implicit in the approach of Friedberg, Insel, and Spence in [5] to this standard topic.

matrix representation of $T$ with respect to $\beta$ and $\gamma$ with the coordinate vector of $v$ with respect to $\beta$. We always arrive at the same column vector in both cases. This elementary equation can be found in any linear algebra textbook, see for instance [5, pg. 91]. We also revisit the change of basis matrix from the point of view of naturality and functoriality.

For concreteness, we work with real vector spaces, though everything is the same over any other field. Let **RVectBasis** be the category whose objects are real vector spaces with chosen ordered bases and whose morphisms are linear maps, not required to map a chosen basis to a chosen basis. For instance, $(\mathbb{R}^3, \{e_1, e_2, e_3\})$ is an object of **RVectBasis**. Let $\mathrm{Id} : \mathbf{RVectBasis} \to \mathbf{RVectBasis}$ be the identity functor. Let $\Phi : \mathbf{RVectBasis} \to \mathbf{RVectBasis}$ have object function $\Phi(V, \beta) = (\mathbb{R}^{\dim V}, \{e_1, \ldots, e_{\dim V}\})$ and morphism function $\Phi T = [T]^\gamma_\beta$ for all linear maps $T : (V, \beta) \to (W, \gamma)$ in **RVectBasis**. Here we are identifying the matrix $[T]^\gamma_\beta$ with the linear map it induces. It is easy to check that $\Phi$ is a (covariant) functor.

Consider the natural transformation $\eta : \mathrm{Id} \to \Phi$ given by "compute the coordinate vector." In other words, $\eta_{(V,\beta)} = [-]_\beta$. This is natural since the equation $[T]^\gamma_\beta [v]_\beta = [Tv]_\gamma$ holds for any linear map $T : (V, \beta) \to (W, \gamma)$ in **RVectBasis** and any $v \in V$. It says exactly that the following diagram commutes for any such $T$.

$$\begin{array}{ccc} (V,\beta) & \xrightarrow{[-]_\beta} & (\mathbb{R}^{\dim V}, \{e_1, \ldots, e_{\dim V}\}) \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle [T]^\gamma_\beta} \\ (W,\gamma) & \xrightarrow[[-]_\gamma]{} & (\mathbb{R}^{\dim W}, \{e_1, \ldots, e_{\dim W}\}) \end{array}$$

To concretely illustrate this important result, we consider a specific linear map $T$. Let $\beta = \{e_1, e_2, e_3\}$ and $\gamma = \{\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)\}$. Define $T : (\mathbb{R}^3, \beta) \to (\mathbb{R}^2, \gamma)$ to be the linear transformation given by $T(e_1) = \left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right), T(e_2) = 2\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$, and $T(e_3) = \left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right) + 3\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$. Let $v = ae_1 + be_2 + ce_3 \in \mathbb{R}^3$. Then $T(v) = a\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right) + 2b\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) + c\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right) + 3c\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = (a+c)\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right) + (2b+3c)\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$. Hence, $[T(v)]_\gamma = \left(\begin{smallmatrix}a+c\\2b+3c\end{smallmatrix}\right)$. On the other hand, $[v]_\beta = \left(\begin{smallmatrix}a\\b\\c\end{smallmatrix}\right)$ and $[T]^\gamma_\beta = \left(\begin{smallmatrix}1&0&1\\0&2&3\end{smallmatrix}\right)$. Hence, $[T]^\gamma_\beta([v]_\beta) = \left(\begin{smallmatrix}a+c\\2b+3c\end{smallmatrix}\right)$. We then see that $[T]^\gamma_\beta([v]_\beta) = [T(v)]_\gamma$ as guaranteed by the natural transformation $\eta$.

The change of basis matrix also arises from the naturality viewpoint. To see this, let $Id_V : (V, \beta_1) \to (V, \beta_2)$ be the identity linear map on $V$. The naturality diagram for $\eta$ says in this case that the following diagram commutes.

$$\begin{array}{ccc} (V,\beta_1) & \xrightarrow{[-]_{\beta_1}} & (\mathbb{R}^{\dim V}, \{e_1, \ldots, e_{\dim V}\}) \\ {\scriptstyle Id_V}\downarrow & & \downarrow{\scriptstyle [Id_V]^{\beta_2}_{\beta_1}} \\ (V,\beta_2) & \xrightarrow[[-]_{\beta_2}]{} & (\mathbb{R}^{\dim V}, \{e_1, \ldots, e_{\dim V}\}) \end{array}$$

This means for any $v \in V$, we have $[Id_V(v)]_{\beta_2} = [v]_{\beta_2} = [Id_V]^{\beta_2}_{\beta_1}([v]_{\beta_1})$. Therefore, $Q = [Id_V]^{\beta_2}_{\beta_1}$ is the change of basis matrix which changes $\beta_1$-coordinates into $\beta_2$-coordinates. Moreover, given a linear operator $T : V \to V$ and two ordered bases $\beta_1$ and $\beta_2$ of $V$, we arrive

at the familiar result that $[T]_{\beta_1}^{\beta_1} = Q^{-1}[T]_{\beta_2}^{\beta_2}Q$ since $\Phi$ is a functor. In other words, by functoriality of $\Phi$, $[Id_V]_{\beta_1}^{\beta_2}[T]_{\beta_1}^{\beta_1} = [Id_V \circ T]_{\beta_1}^{\beta_2} = [T \circ Id_V]_{\beta_1}^{\beta_2} = [T]_{\beta_2}^{\beta_2}[Id_V]_{\beta_1}^{\beta_2}$, which implies $[T]_{\beta_1}^{\beta_1} = Q^{-1}[T]_{\beta_2}^{\beta_2}Q$. See page 112 of [5].

In this section, we have briefly introduced some basic yet important and ubiquitous ideas of category theory: categories, functors, and natural transformations. For more about category theory, see [6].

# 3 Galois Theory

Galois theory reduces certain problems in field theory to problems in group theory. Historically, Galois theory was motivated by the relationship between the roots of a polynomial and its coefficients. For instance, the familiar quadratic formula expresses the roots of a quadratic in terms of its coefficients using addition, multiplication, division, and square roots. In fact, there are formulas that relate the coefficients of cubics and quartics to their roots. However, for an arbitrary polynomial $g$ of degree five or higher, there is no simple relationship between the coefficients of $g$ and its roots, which can be explained by Galois theory [2, page 625].

**Definition 3.1.** Let $F$ be a field. Let $K$ be a field such that $F \subseteq K$. In this case, $K$ is called an *extension field* of $F$, which will be denoted $K/F$.

It is a standard result to show that given an extension field $K$ of $F$, $K$ can be regarded as a vector space over $F$. The dimension of $K$ over $F$ is denoted $[K : F]$. For instance, given the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, the vector space $\mathbb{Q}(\sqrt{2})$ has dimension two over $\mathbb{Q}$ where a basis is $\{1, \sqrt{2}\}$.

**Definition 3.2.** Given an extension field $K$ of $F$, $Aut(K/F)$ is the set of all field automorphisms $\sigma$ of $K$ such that $\sigma|_F = Id_F$.

It is easy to see that $Aut(K/F)$ with composition is a group. Moreover, $|Aut(K/F)| \leq [K : F]$. See [2, page 572].

**Definition 3.3.** Let $K$ be a field extension of $F$. If $|Aut(K/F)| = [K : F]$, then $K$ is said to be *Galois* over $F$. In this case, we will write $Aut(K/F)$ as $Gal(K/F)$, which is the *Galois group* of the extension $K/F$.

**Proposition 3.4.** *Let $K$ be an extension field of $F$ and $\alpha \in K$ algebraic over $F$. Then for any $\sigma \in Aut(K/F)$, $\sigma(\alpha)$ is a root of the minimal polynomial for $\alpha$ over $F$. In other words, $Aut(K/F)$ permutes the roots of irreducible polynomials.*

*Proof.* [2, page 559] Let $\alpha \in K$ be algebraic over $F$ and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be the minimal polynomial of $\alpha$ over $F$, i.e the monic polynomial of smallest degree in $F$ such

that $\alpha$ is a root, which exists since $\alpha$ is algebraic over $F$. Also let $\sigma \in Aut(K/F)$. Applying $\sigma$ to $f(\alpha)$, we have

$$\begin{aligned} 0 &= \sigma(f(\alpha)) \\ &= \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) \\ &= \sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \cdots + \sigma(a_0) \\ &= \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_0. \end{aligned}$$

The first line is true since $f$ is the minimal polynomial of $\alpha$, which implies $f(\alpha) = 0$. Therefore, $\sigma(\alpha)$ is also a root of the minimal polynomial for $\alpha$. □

Along with the fact that $|Aut(K/F)| \leq [K : F]$, Proposition 3.4 is useful in finding $Aut(K/F)$ as illustrated in the next example since each element of $Aut(K/F)$ is completely determined by where it sends the roots of certain irreducible polynomials.

**Example 3.5.** We will show that $Gal(\mathbb{R}(i)/\mathbb{R}) = Gal(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$. Notice that $i$ is algebraic over $\mathbb{R}$ and the minimal polynomial of $i$ in $\mathbb{R}$ is $f(x) = x^2 + 1$. The only two roots of $f$ are $i$ and $-i$. If $\tau \in Aut(\mathbb{C}/\mathbb{R})$ then by Proposition 3.4, $\tau(i) = i$ or $\tau(i) = -i$. In the former case, $\tau$ is the identity automorphism on $\mathbb{C}$. In the latter case, we have $\tau(a+bi) = a-bi$ since $\tau$ must fix $\mathbb{R}$. Note, $[\mathbb{C} : \mathbb{R}] = 2$ since $\{1, i\}$ is a basis. Therefore, since $|Aut(\mathbb{C}/\mathbb{R})| = 2 \leq [\mathbb{C} : \mathbb{R}] = 2$, $Aut(\mathbb{C}/\mathbb{R}) = \{1, \tau\} \cong \mathbb{Z}_2$, and $\mathbb{C}$ is Galois over $\mathbb{R}$.

It is also helpful to look at an example of a field extension which is not Galois.

**Example 3.6.** Consider the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Notice that any element of this extension can be written as $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ such that $a, b, c \in \mathbb{Q}$. For any $\sigma \in Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, $\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a + b\sigma(\sqrt[3]{2}) + c\sigma(\sqrt[3]{4})$. Also, $\sqrt[3]{2}$ is algebraic with minimal polynomial $f = x^3 - 2$. Therefore, $\sigma$ is completely determined by where it sends $\sqrt[3]{2}$ by Proposition 3.4. The other roots of $f$ are imaginary, which means they are not elements of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Therefore, $\sigma = Id$ by Proposition 3.4. Since $|Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$.

**Theorem 3.7** (Fundamental Theorem of Galois Theory)**.** *Let $K/F$ be a Galois extension. There is a bijection between the subfields $E$ of $K$ containing $F$ and the subgroups $H$ of $Gal(K/F)$. The correspondence sends $E$ to all the elements of $Gal(K/F)$ fixing $E$ and sends $H$ to the fixed field of $H$. Moreover, $K/E$ is Galois.*

A proof can be found in [2, pages 573-576].

We can restate the fundamental theorem of Galois theory using categorical language.

**Theorem 3.8** (Fundamental Theorem of Galois Theory in Categorical Language)**.** *Let $K$ be Galois over $F$. Let $\mathscr{L}$ be the category whose objects are the intermediate fields between $K$ and $F$ and morphisms are the inclusion homomorphisms. Let $\mathscr{G}$ be the category whose objects are subgroups of $Gal(K/F)$ and morphisms are inclusion homomorphisms. Note that $\mathscr{L}$ and $\mathscr{G}$ are posets. Then $S : \mathscr{L} \to \mathscr{G}$ is a contravariant isomorphism of categories where for any $L \in \mathscr{L}$, $S(L) = Gal(K/L)$ and for any morphism $i : L_1 \hookrightarrow L_2$ in $\mathscr{L}$, $Si : Gal(K/L_2) \hookrightarrow Gal(K/L_1)$ is the inclusion homomorphism.*

*Proof.* Clearly $\mathscr{L}$ and $\mathscr{G}$ are categories. By Theorem 3.7, the object function of $S$ is well defined. Let $L_1$ and $L_2$ be in $\mathscr{L}$ such that $L_1 \subseteq L_2$. We will show $Gal(K/L_2) \leq Gal(K/L_1)$. To see the containment, let $\sigma \in Gal(K/L_2)$. Then for any $l_1 \in L_1$, $\sigma(l_1) = l_1$ since $l_1 \in L_2$ and $\sigma$ is the identity on $L_2$. Hence, since $Gal(K/L_2)$ is a subset of $Gal(K/L_1)$ and $Gal(K/L_2)$ is a group, $Gal(K/L_2) \leq Gal(K/L_1)$, which proves that the morphism function of $S$ is well-defined. It is easy to see that $S$ is a functor because inclusions are mapped to inclusions.

To show $S$ is a contravariant isomorphism, we must show that the object function of $S$ and the morphism function of $S$ are bijective. By the fundamental theorem of Galois theory, the object function of $S$ is bijective. The morphism function of $S$ is injective since inclusions are unique. Let $i : Gal(K/F_2) \hookrightarrow Gal(K/F_1)$ be the inclusion homomorphism. Note that $K/F$ is Galois if and only if $F$ is the fixed field of $Aut(K/F)$ [2, page 572]. Therefore, the fixed field of $Gal(K/F_2)$ is $F_2$ and the fixed field of $Gal(K/F_1)$ is $F_1$. For any $\sigma \in Gal(K/F_2)$, $\sigma|_{F_1} = Id_{F_1}$, but since $F_2$ is the largest field that $Gal(K/F_2)$ fixes, $F_1 \subseteq F_2$. Let $i' : F_1 \hookrightarrow F_2$ be the inclusion homomorphism. Then $Si' = i$. Hence, the morphism function of $S$ is surjective. Thus, $\mathscr{L}$ and $\mathscr{G}$ are isomorphic[3] categories. □

**Example 3.9.** Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and $F = \mathbb{Q}(\sqrt{2})$. Notice $K$ is a field extension of $F$ since $(\sqrt[8]{2})^4 = \sqrt{2}$. We will show $Gal(K/F) \cong D_8$. First notice that $\{1, \sqrt[8]{2}, \sqrt[8]{4}, \sqrt[8]{8}, i, i\sqrt[8]{2}, i\sqrt[8]{4}, i\sqrt[8]{8}\}$ is a basis for $K$ over $F$, so $|Aut(K/F)| \leq 8 = [K : F]$.

Notice that $i\sqrt[8]{2}$ is algebraic over $K$ with minimal polynomial $f(x) = x^4 - \sqrt{2}$ in $F$. The other roots of $f$ are $\sqrt[8]{2}$, $-\sqrt[8]{2}$, and $-i\sqrt[8]{2}$.

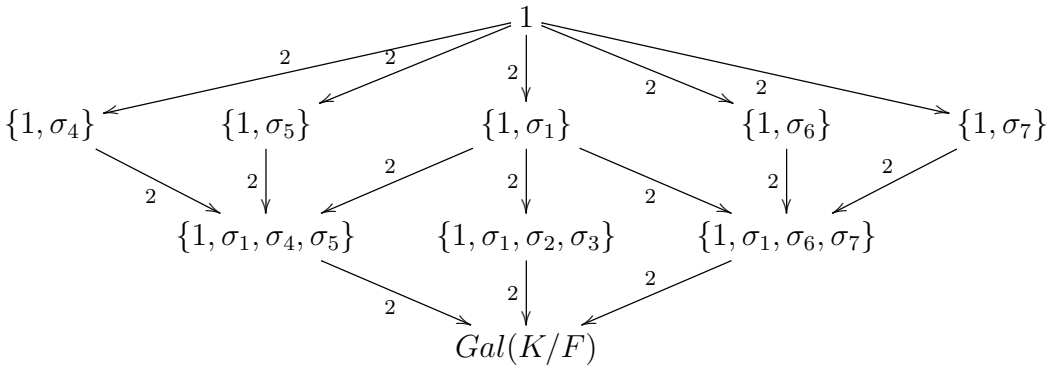
From Proposition 3.4, any $\sigma \in Aut(K/F)$ must permute the roots of $f$, so we want to find valid ways to permute the roots. Since $\sigma$ is a field automorphism, $\sigma(i\sqrt[8]{2}) = \sigma(i)\sigma(\sqrt[8]{2})$. Since $\sigma(i)$ must be an element of order 4, $\sigma(i) = \pm i$. Similarly, $\sigma(\sqrt[8]{2})^8 = 2$, so there are four choices: $\sigma(\sqrt[8]{2}) = \pm\sqrt[8]{2}$ or $\sigma(\sqrt[8]{2}) = \pm i\sqrt[8]{2}$. Therefore, there are 8 choices for $\sigma$:

1. the identity, 1,
2. $\sigma_1(i) = i$ and $\sigma_1(\sqrt[8]{2}) = -\sqrt[8]{2}$,
3. $\sigma_2(i) = i$ and $\sigma_2(\sqrt[8]{2}) = i\sqrt[8]{2}$,
4. $\sigma_3(i) = i$ and $\sigma_3(\sqrt[8]{2}) = -i\sqrt[8]{2}$,
5. $\sigma_4(i) = -i$ and $\sigma_4(\sqrt[8]{2}) = \sqrt[8]{2}$,
6. $\sigma_5(i) = -i$ and $\sigma_5(\sqrt[8]{2}) = -\sqrt[8]{2}$,
7. $\sigma_6(i) = -i$ and $\sigma_6(\sqrt[8]{2}) = i\sqrt[8]{2}$, and finally
8. $\sigma_7(i) = -i$ and $\sigma_7(\sqrt[8]{2}) = -i\sqrt[8]{2}$.

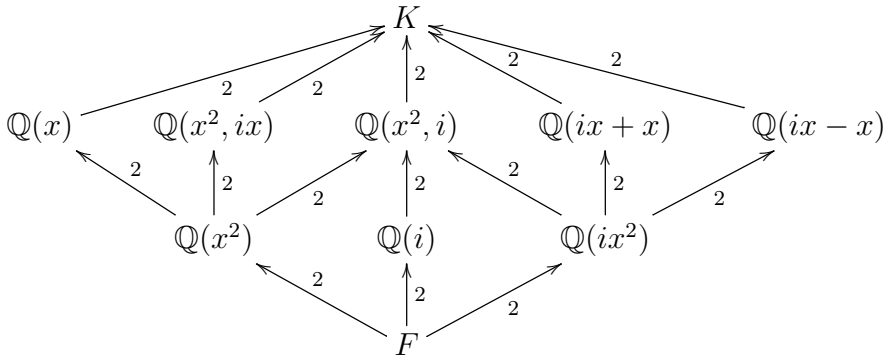
[3]In practice, very few categories are isomorphic. More common is the notion of *equivalence* of categories.

Since $|Aut(K/F)| = 8 \leq [K : F] = 8$, $K$ is Galois over $F$. To show that the Galois group is isomorphic to the dihedral group of order 8, we will show that there is an element $\beta$ of order two and an element $\alpha$ of order four such that $(\alpha\beta)^2 = Id$. It is easy to verify that $\sigma_4$ is an element of order two, $\sigma_3$ is an element of order four, and $(\sigma_4 \circ \sigma_3)^2 = Id$. Therefore, $Gal(K/F) \cong D_8$.

The subgroup lattice of $Gal(K/F)$ is pictured below where the index of a subgroup is indicated on its corresponding arrow.




The intermediate subfield lattice is pictured below where $x = \sqrt[8]{2}$ and the dimension of the field extension is indicated on its corresponding arrow.




Notice how the subfield and subgroup lattices are intimately related. The arrows in the subfield lattice are the arrows in the subfield lattice reversed, which is exactly what the contravariant functor does. Notice also that the index of a subgroup is the same as the dimension of the corresponding field extension. These diagrams illustrate the fundamental theorem of Galois theory.

The categorical view of the fundamental theorem of Galois theory is generalized to the notion of Galois connection in category theory. See [1].

# References

[1] Francis Borceux and George Janelidze. *Galois Theoeries*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, first edition, 2008.

[2] David Dummit and Richard Foote. *Abstract Algebra*. John Wiley and Sons, Inc., third edition, 2004.

[3] Samuel Eilenberg and Saunders MacLane. Group extensions and homology. *Ann. of Math. (2)*, 43:757–831, 1942.

[4] Samuel Eilenberg and Saunders MacLane. Natural isomorphisms in group theory. *Proc. Nat. Acad. Sci. U. S. A.*, 28:537–543, 1942.

[5] Stephen H. Friedberg, Arnold J. Insel, and Lawrence E. Spence. *Linear algebra*. Prentice Hall Inc., Upper Saddle River, NJ, fourth edition, 1997.

[6] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.