GALOIS CATEGORIES

MELISSA LYNN

Abstract. In abstract algebra, we considered finite Galois extensions of fields with their Galois groups. Here, we noticed a correspondence between the intermediate fields and the subgroups of the Galois group; specifically, there is an inclusion reversing bijection that takes a subgroup to its fixed field. We notice a similar relationship in topology between the fundamental group and covering spaces. These ideas can be generalized and related using category theory, through the definition of a Galois category. Here we build up the basic theory necessary to understand and recognize these categories.

Contents

1. Categories

We begin by defining a category. A category gives us a way to express the idea that most of what we deal with in mathematics consists of some objects (think of sets) and morphisms (think of functions) between these objects. Using the idea of a category, we can relate these frameworks and get a deeper understanding of their structure. Furthermore, most of the things we consider are conveniently representable as categories.

Definition 1.1. A category consists of objects and arrows (or morphisms) such that:

(1) For each arrow f, there exist objects A and B which are the domain and codomain of f; we write $f : A \to B$.

(2) For any arrows $f : A \to B$, $g : B \to C$, there exists an arrow $g \circ f : A \to C$ called the composition of f and g.

Date: July 20, 2009.

(3) For each object A there exists an arrow $1_A : A \to A$ such that for every arrow $f : A \to B$, $f \circ 1_A = f = 1_B \circ f$.
(4) For all arrows $f : A \to B$, $g : B \to C$, and $h : C \to D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$.
The collection of arrows from A to B is written as $Hom(A, B)$.

To understand why this definition is desirable, we now go through several examples of categories:

Example 1.2. The most obvious example of a category consists of sets for objects and functions on these sets for arrows. The category axioms are obviously satisfied by the properties of functions.

Example 1.3. A less obvious example of a category is based on a total order on a set S. In this case, we consider the elements of S to be objects and require that there be exactly one arrow between any two objects (this means that for distinct objects A, B there exists $f : A \to B$ or $g : B \to A$, but not both). By replacing " $\to$ " with " $\leq$ ", we can see that the category axioms become equivalent to the definition of a total order. (We can similarly make a partial order on a set into a category by taking at most one arrow between any two objects.)

Example 1.4. A monoid can be realized as a category with one object, where the elements of the monoid appear as arrows. Multiplication of elements of the monoid appears as composition of arrows. We can also make a group into a category the same way; in this case, the arrows would all be invertible.

Example 1.5. We can also take monoids (or groups) as objects and homomorphisms as arrows to form a category. Note that this forms a subcategory of the category of sets and functions.

We define subcategory explicitly:

Definition 1.6. A subcategory of a category $\mathcal{C}$ is a category $\mathcal{D}$ whose objects and arrows are objects and arrows in $\mathcal{C}$, with the same 1_A and compositions.

More intuitively, a subcategory is obtained from the category by removing some of the objects and morphisms.

Example 1.7. Topological spaces with continuous maps form a category.

We can translate the idea of an isomorphism, a morphism that is surjective and injective, to categories.

Definition 1.8. A morphism $\phi \in Hom(A, B)$ is called an isomorphism if there exists $\psi \in Hom(B, A)$ with $\psi \circ \phi = 1_A$, $\phi \circ \psi = 1_B$.

Given a category, we can define another category simply by reversing the arrows. While intuitively this doesn't make much sense for sets, this idea does prove to be useful later, when we consider Galois categories.

Definition 1.9. The opposite category $\mathcal{C}^{op}$ of a category $\mathcal{C}$ has the same objects as $\mathcal{C}$, but the arrows are reversed, so we have a natural bijection $Hom_{\mathcal{C}}(A, B) \leftrightarrow Hom_{\mathcal{C}^{op}}(B, A)$.

We define two very special kinds of objects that can exist in a category:

Definition 1.10. In a category, an object Z is final if for each object B there exists exactly one arrow $B \to Z$.

Definition 1.11. In a category, an object A is initial if for each object B there exists exactly one arrow $A \to B$

In the category of sets, the empty set is an initial object and the set containing one element in a final object. Note that, from the definitions, initial and final objects are unique up to isomorphism.

2. Functors

In order to relate one category to another category, we now introduce the idea of a functor, which preserves the basic structure of the category.

Definition 2.1. A covariant functor (usually just called a functor) $F : \mathcal{C} \to \mathcal{D}$ between categories $\mathcal{C}$ and $\mathcal{D}$ is a mapping of objects to objects and arrows to arrows such that for any objects A, B, C and arrows $f : A \to B$ and $g : B \to C$ in $\mathcal{C}$:

(1) $F(f : A \to B) = F(f) : F(A) \to F(B)$
(2) $F(g \circ f) = F(g) \circ F(f)$
(3) $F(1_A) = 1_{F(A)}$

A contravariant functor from $\mathcal{C}$ to $\mathcal{D}$ is a covariant functor from $\mathcal{C}$ to $\mathcal{D}^{op}$.

Example 2.2. The simplest example of a functor between two categories is called the "forgetful functor". This is because it "forgets" some of the structure of the objects and morphisms. For example, if we let $\mathcal{C}$ be the category of monoids with homomorphisms and $\mathcal{D}$ be the category of sets with functions, the forgetful functor U would take a monoid M to its underlying set $U(M)$ and a homomorphism f to its underlying function $U(f)$. Thus the forgetful functor forgets the monoid and homomorphism structures of the objects and arrows in order to map them into the category of sets and functions. (Similarly, the forgetful functor maps the category of groups and group homomorphisms to the category of monoids and monoid homomorphisms by forgetting that the elements of a group must have inverses.)

Forgetful functors are very useful for expressing ideas such as "all groups are monoids" in terms of categories.

Example 2.3. A more interesting example of a functor goes from the category of groups to the category of abelian groups. Let $\mathcal{G}$ be the category of groups with homomorphisms and $\mathcal{A}$ be the category of abelian groups. Let G be an object in $\mathcal{G}$. Recall that the commutator of a group is the subgroup generated by the set $\{xyx^{-1}y^{-1} : x, y \in G\}$, say $H_G =< \{xyx^{-1}y^{-1} : x, y \in G\} >$. Then G/H_G is an abelian group. We thus define a functor F from $\mathcal{G}$ to $\mathcal{A}$ by $F(G) = G/H_G$.

Example 2.4. Now let $\mathcal{M}$ be the category of abelian monoids and $\mathcal{G}$ the category of abelian groups. Given an object M in $\mathcal{M}$, define an eguivalence relation by $(m, n) \sim (m', n')$ if there exists q such that $m + n' + q = m' + n + q$. We define addition on the equivalence classes by $[m, n] + [p, q] = [m + p, n + q]$. Note that $M/\sim$ forms an abelian group with this operation. Thus we define a functor F from $\mathcal{M}$ to $\mathcal{G}$ by $F(M) = M/\sim$. (Note that this construction does not work for taking monoids to groups in general.)

Now we define functors from one category to another. This gives us a way to compare categories and determine when they are "equal", in some sense. In order to do this, we need to define a morphism of functors.

Definition 2.5. Let F and G be functors from $\mathcal{C}_1$ to $\mathcal{C}_2$. A morphism of functors (or natural transformation) Ψ is a collection of morphisms $\psi_A : F(A) \to G(A)$ in $\mathcal{C}_2$ for each $A \in \mathcal{C}_1$ such that for every morphism $\phi : A \to B \in \mathcal{C}_1$, the following diagram commutes:

$$\begin{array}{ccc} F(A) & \xrightarrow{\psi_A} & G(A) \\ \Big\downarrow{\scriptstyle F(\phi)} & & \Big\downarrow{\scriptstyle G(\phi)} \\ F(B) & \xrightarrow{\psi_B} & G(B) \end{array} \tag{2.6}$$

Then Ψ is an isomorphism if and only if all ψ_A are isomorphisms.

Definition 2.7. Two categories $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if there exist functors $F : \mathcal{C}_1 \to \mathcal{C}_2$ and $G : \mathcal{C}_2 \to \mathcal{C}_1$, and isomorphisms of functors $\Phi : F \circ G \tilde{\to} id_{\mathcal{C}_2}$ and $\Psi : G \circ F \tilde{\to} id_{\mathcal{C}_1}$. We say that G is a quasi-inverse for F.

Definition 2.8. If we can find F and G as above so that in fact $F \circ G = id_{\mathcal{C}_2}$ and $G \circ F = id_{\mathcal{C}_1}$, we say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are isomorphic.
We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are anti-equivalent if $\mathcal{C}_1$ is equivalent to $\mathcal{C}_2^{op}$.
We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are anti-isomorphic if $\mathcal{C}_1$ is isomorphic to $\mathcal{C}_2^{op}$.

Now, we can actually define a category of functors from one category to another:

Definition 2.9. We define a functor category to consist of objects which are functors from $\mathcal{C}_1$ to $\mathcal{C}_2$ and arrows which are morphisms of functors.

3. Epimorphisms and Monomorphisms

We have already defined an isomorphism of objects in order to get some sense of a bijection in a category; now, we introduce epimorphisms and monomorphisms to take the part of surjections and injections (respectively) in a category.

Definition 3.1. In a category $\mathcal{C}$, an arrow $f : A \to B$ is called a monomorphism if for all $g, h : C \to A$, $fg = fh$ implies that $g = h$.

As we had wanted, in the category $Sets$, the monomorphisms are the injective functions.

Definition 3.2. In a category $\mathcal{C}$, an arrow $f : A \to B$ is called an epimorphism if for all arrows $i, j : B \to D$, $if = jf$ implies that $i = j$.

In the category $Sets$, the epimorphisms are the surjective functions.

The following discussion of subobjects is not necessary to understanding Galois categories, but gives a very interesting way to see how we can identify a very intuitive idea (of subsets, subgroups, etc.) in a category and generalize this idea.

3.1. **Subobjects.** Given a subset A of B, we always have a natural embedding of A into B, simply by sending each element to itself. Also, if we have an injection from a set C into B, we know that C is isomorphic to a subset of B. Using this idea and recalling that injections become monomorphisms when we are considering a category, we arrive at the following definition of a subobject.

Definition 3.3. A subobject of an object X in a category $\mathcal{C}$ is a monomorphism $m : M \to X$.

We can make sense of this definition in the category $Sets$. Here, a subobject would be an embedding of a set M into a set X. We have that $\{m(y)|y \in M\} \subset X$, and $m : M \to m(M) \subset X$, and m is actually an isomorphism. We can see here that this idea of a subobject is closely related to the idea of a subset.

We now define a morphism between subobjects.

Definition 3.4. For m, m' subobjects of X, a morphism $f : m \to m'$ is an arrow in $\mathcal{C}/X$, i.e. an arrow $f : M \to M'$ so that $m = m' \circ f$.

With this definition, we have a category of subobjects of X in $\mathcal{C}$, which we write $Sub_{\mathcal{C}}(X)$. In this category, we say that $m \subset m'$ if and only if there exists an arrow $f : m \to m'$. Then m, m' are equivalent if they are isomorphic as subobjects, so if $m \subset m'$ and $m' \subset m$.

4. Limits and Colimits

In this section, we introduce the ideas of limits and colimits in a category. Limits and colimits are useful in category theory for defining structures such as the p-adic integers, and we will use the definition of a fiber product for Galois Categories and the definition of a profinite group when we consider field extensions (in the context of algebras).

Definition 4.1. Let $\mathcal{C}$ be a category and $f : A \to C$ and $g : B \to C$ be arrows. A pullback of f and g consists of arrows p_1, p_2 so that the following diagram commutes:

$$\begin{array}{ccc} P & \xrightarrow{p_2} & B \\ \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array} \tag{4.2}$$

and it has the universal property: for all arrows $x_1 : Z \to A$, $x_2 : Z \to B$ such that $fx_1 = gx_2$, there exists unique $u : Z \to P$ such that $x_1 = p_1 u$ and $x_2 = p_2 u$. We call P the fiber product of A and B over C, and write $P = A \times_C B$. A pullback is unique up to isomorphism (this is ensured by the universal property).

We consider the category of sets to make some sense of this definition. In terms of products, we can see that $A \times_C B = \{(x_1, x_2) \in A \times B | fx_1 = gx_2\}$.

We now go quickly through the rest of the definition of a limit, and then use abelian groups to understand what is happening.

Definition 4.3. Let $\mathcal{J}$ and $\mathcal{C}$ be categories. A diagram of type $\mathcal{J}$ in $\mathcal{C}$ is a functor $D : \mathcal{J} \to \mathcal{C}$.

Here, $\mathcal{J}$ is an index category, with objects $i, j, ...$ We write the values of the functor $D_i, D_j, ...$

Definition 4.4. A cone to a diagram D consists of an object C in $\mathcal{C}$ and a collection of arrows $c_j : C \to D_j$ (one for each j in $\mathcal{J}$) in $\mathcal{C}$ such that for all $\alpha : i \to j$ in $\mathcal{J}$, $D_\alpha \circ c_i = c_j$.

Definition 4.5. A morphism of cones $\nu : (C, c_j) \to (C', c'_j)$ is an arrow in $\mathcal{C}$ such that $c_j = c'_j \circ \nu$ for all j in $\mathcal{J}$.

With these morphisms, we have a category of cones to D, which we write $Cone(D)$.

Definition 4.6. A limit for a diagram $D : \mathcal{J} \to \mathcal{C}$ is a terminal object in $Cone(D)$. A finite limit is a limit for a diagram on a finite index category. We denote this limit $\varprojlim D_j$.

Proposition 4.7. *The limit has the universal mapping property: for every cone (C, c_j) to D, there exists unique $u : C \to \varprojlim D_j$ such that for all j, $p_j \circ u = c_j$.*

We can see how the limit works more concretely when we consider the category of abelian groups:

Definition 4.8. Let I be a partially ordered index set for a collection of abelian groups, A_i. Now suppose for all $i \leq j$ there is a map $\mu_{ji} : A_j \to A_i$ such that $\mu_{ji} \circ \mu_{kj} = \mu_{ki}$ for all $i \leq j \leq k$ and $\mu_{ii} = 1$ for all $i \in I$. Let P be the set of elements $(a_i)_{i \in I}$ in the direct product $\prod_{i \in I} A_i$ such that for $i \leq j$, $\mu_j i(a_j) = a_i$. P is called the inverse limit of the system $\{A_i\}$, written $\varprojlim A_i$.

Proposition 4.9. *If all μ_{ji} are group homomorphisms, P is a subgroup, and the inverse limit has the following universal property: if D is any group such that for each $i \in I$ there is a homomorphism $\pi_i : D \to A_i$ with $\pi_i = \mu_{ji} \circ \pi_j$ whenever $i \leq j$, then there is a unique homomorphism $\pi : D \to P$ such that $\mu_i \circ \pi = \pi_i$ for all i.*

Proof. Define $\pi : D \to P$ by $\pi(d) = (\pi_i(d))_{i \in I}$. This satisfies the requirements. □

Example 4.10. Let p be a prime let $I = \mathbb{Z}^+$, let $A_i = \mathbb{Z}/p^i\mathbb{Z}$ and let μ_{ji} be the natural projection maps $\mu_{ji} : a \pmod{p^j} \mapsto a \pmod{p^i}$. The inverse limit of this system is the ring of p-adic integers, denoted $\mathbb{Z}_p$.

The following example will be important later in this paper.

Example 4.11. Let I be a directed index set, $(\pi_i)_{i \in I}$ a collection of finite groups, $(f_{ij})_{i,j \in I, i \geq j}$ a collection of group homomorphisms as above. Then $\pi = \varprojlim \pi_i$ is a group. We say that π is a profinite group, and by giving each π_i the discrete topology, we get that π is a topological group.

We now define a colimit, which is dual to the limit. Defining it explicitly follows a similar process, and once again we use the example of abelian groups to understand it.

Definition 4.12. In a category $\mathcal{C}$, a pushout of arrows $f : A \to B$, $g : A \to C$ consists of an object D with arrows $p_1 : B \to D$ and $p_2 : C \to D$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle p_1} \\ C & \xrightarrow{p_2} & D \end{array} \tag{4.13}$$

and such that for all arrows $u : B \to T$ and $v : C \to T$, there exists an arrow $h : D \to T$ such that $hp_1 = u$ and $hp_2 = v$.

Definition 4.14. A cocone for a diagram $D : \mathcal{J} \to \mathcal{C}$ consists of an object C and arrows $c_j : D_j \to C$ for each j in $\mathcal{J}$, such that for all $\alpha : i \to j$ in $\mathcal{J}$, $c_j \circ D(\alpha) = c_i$.

Definition 4.15. A morphism of cocones $f : (C, (c_j)) \to (C', (c'_j))$ is an arrow $f : C \to C'$ in $\mathcal{C}$ such that $f \circ c_j = c'_j$ for all j in $\mathcal{J}$.

From this we have a category of cocones, from which we define the colimit.

Definition 4.16. The colimit is the initial object in the category of cocones, which we write $\varinjlim D_j$.

Once again, we can consider the colimit for the category of abelian groups.

Definition 4.17. Let I be a nonempty index set with partial order $\leq$. For all $i \in I$, let A_i be an abelian group. Let I be a directed set (for all $i, j \in I$, there exists $k \in I$ such that $i \leq k$ and $j \leq k$. Now suppose for every pair of indices i, j with $i \leq j$ there is a group homomorphism $\rho_{ij} : A_i \to A_j$ such that the following hold:

(1) $\rho_{jk} \circ \rho_{ij} = \rho_{ik}$ whenever $i \leq j \leq k$ and
(2) $\rho_{ii} = 1$ for all $i \in I$.

Let B be the disjoint union of all the A_i. Define a relation $\sim$ on B by $a \sim b$ if and only if there exists k with $i, j \leq k$ and $\rho_{ik}(a) = \rho_{jk}(b)$ for $a \in A_i$ and $b \in A_j$. The set of equivalence classes is called the direct limit of the directed system $\{A_i\}$ and is denoted $\varinjlim A_i$.

Note that $\sim$ is an equivalence relation on B, making this definition valid. (The proof that $\sim$ is an equivalence class is straightforward, we will not do it here.)

Proposition 4.18. *Let $\overline{x}$ denote the class of x in A and define $\rho_i : A_i \to A$ by $\rho_i(a) = \overline{a}$. If each ρ_{ij} is injective, then so is ρ_i for all i. (Thus we can identify each A_i as a subset of A.)*

Proof. If $\rho_i(a) = \rho_i(b)$ with $a, b \in A_i$, then $a \sim b$, so there exists k with $i \leq k$ such that $\rho_{ik}(a) = \rho_{ik}(b)$. Then $a = b$ because ρ_{ik} is injective. Therefore ρ_i is injective for all i. □

Proposition 4.19. *For $a \in A_i$, $b \in A_j$, the operation $\overline{a} + \overline{b} = \overline{\rho_{ik}(a) + \rho_{jk}(b)}$ where k is any index with $i, j \leq k$ is well-defined and makes A into an abelian group. Then the maps ρ_i as above are group homomorphisms from A_i to A.*

Proof. We show that this operation is well-defined and leave the rest to the reader. Let $a' \sim a$ and $b' \sim b$ where $a \in A_i$, $a' \in A_{i'}$, $b \in A_j$, and $b' \in A_{j'}$. Then there exists k_a with $i, i' \leq k_a$ such that $\rho_{ik_a}(a) = \rho_{i'k_a}(a')$, and there exists k_b with $j, j' \leq k_b$ such that $\rho_{jk_b}(b) = \rho_{j'k_b}(b')$.
We want to show that $\rho_{i'k'}(a') + \rho_{j'k'}(b') \sim \rho_{ik}(a) + \rho_{jk}(b)$ for k, k' any indices with $i, j \leq k$ and $i', j' \leq k'$.
Take $m \geq k, k'$. Then

$$\begin{aligned}
\rho_{km}(\rho_{ik}(a) + \rho_{jk}(b)) &= \rho_{im}(a) + \rho_{jm}(b) \\
&= \rho_{k_a m} \circ \rho_{ik_a}(a) + \rho_{k_b m} \circ \rho_{jk_b}(b) \\
&= \rho_{k_a m} \circ \rho_{i'k_a}(a') + \rho_{k_b m} \circ \rho_{j'k_b}(b') \\
&= \rho_{i'm}(a') + \rho_{j'm}(b') \\
&= \rho_{k'm}(\rho_{i'k'}(a') + \rho_{j'k'}(b'))
\end{aligned}$$

Therefore the addition is well-defined. We leave the proof that A forms an abelian group under this operation. □

Proposition 4.20. *The direct limit has the following universal property: if C is any abelian group such that for each $i \in I$ there is a homomorphism $\phi_i : A_i \to C$ with $\phi_i = \phi_j \circ \rho_{ij}$ whenever $i \leq j$, then there is a unique homomorphism $\phi : A \to C$ such that $\phi \circ \rho_i = \phi_i$ for all i.*

Proof. Define $\phi(a) = \phi_i(a_i)$ if $\overline{a_i} = a$. We show that this definition is well-defined: if $\overline{a_i} = \overline{a_j}$ for $a_i \in A_i$ and $a_j \in A_j$, there exists $k \geq i, j$ with $\rho_{ik}(a_i) = \rho_{jk}(a_j)$. Then $\phi_i(a_i) = \phi_k(\rho_{ik}(a_i)) = \phi_k(\rho_{jk}(a_j)) = \phi_j(a_j)$, so ϕ is well-defined. The rest is straight forward. □

Example 4.21. Let I be the collection of open intervals $U = (a, b)$ in $\mathbb{R}$ containing fixed p. These intervals are ordered by reverse inclusion, so $U \leq V$ if $V \subset U$. For each U, A_U is the ring of continuous functions $U \to \mathbb{R}$. For $V \subset U$, define $\rho_{UV} : A_U \to A_V$ by $f \mapsto f|_V$, restricting f to V. Let $A = \varinjlim A_U$ be the direct limit, which we call the ring of germs of continuous functions at p. In this case, all ρ_U are surjective.

Note that a pushout of abelian groups is not necessarily the same as a pushout of underlying sets given abelian group structure. For example, consider the abelian groups $\mathbb{Z}$ and $\mathbb{Q}$ with the usual inclusion maps, as below.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ \downarrow & & \\ \mathbb{Q} & & \end{array} \tag{4.22}$$

Then the pushout of this diagram, as one of abelian groups, is $\mathbb{Q}/\mathbb{Z}$ with the corresponding maps (the zero map $\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, and the usual quotient map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array} \tag{4.23}$$

However, the pushout of the diagram, as one of sets, is simply $\mathbb{Q}$ with the usual inclusion maps:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q} \end{array} \tag{4.24}$$

Now, we note that the coproduct of commutative rings R and S over Z is the tensor product of R and S over Z. For this, we use the universal property of the tensor product. We begin with the diagram of commutative rings and ring homomorphisms below.

$$\begin{array}{ccc} Z & \xrightarrow{f} & R \\ \downarrow{\scriptstyle g} & & \\ S & & \end{array} \tag{4.25}$$

We can view R and S as Z-modules (in fact, Z-algebras). We do this for S by

defining the action by $z \cdot s = f(z)s$, and similarly for R. Thus we can construct the tensor product $S \otimes_Z R$, and define maps $u : R \to S \otimes_Z R$ and $v : S \to S \otimes_Z R$ by $u : r \mapsto 1 \otimes r$ and $v : s \mapsto s \otimes 1$. Then we have a commutative diagram:

$$\begin{array}{ccc} Z & \xrightarrow{f} & R \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle u} \\ S & \xrightarrow{v} & S \otimes_Z R \end{array} \tag{4.26}$$

Now suppose we have a commutative ring T and some ring homomorphisms $t_1 : R \to T$ and $t_2 : S \to T$. Then we can define a map $t : S \times R \to T$ by $t : (s, 0) \mapsto t_2(s)$ and $t : (0, r) \mapsto t_1(r)$, which is Z-balanced. Then, by the universal property of tensor products, there is a unique homomorphism $\Phi : S \otimes_Z R \to T$ such that $t = \Phi \circ \iota$, where $\iota : S \times R \to S \otimes_Z R$ is defined by $\iota : (s, r) \mapsto s \otimes r$. Then we have, from the definitions of u and v, $t_1 = \Phi \circ v$ and $t_2 = \Phi \circ u$. Thus, we have satisfied the definition of a pushout.

5. Galois Categories

Before defining a Galois category, we first give some additional preliminary definitions:

Definition 5.1. Let $(X_i)_{i \in I}$ be a collection of objects in $\mathcal{C}$. The coproduct of the X_i is an object $\bigsqcup_{i \in I} X_i$, with morphisms $q_j : X_j \to \bigsqcup_{i \in I} X_i$ for each $j \in I$, such that for any object Y of $\mathcal{C}$ and any collection of morphisms $f_j : X_j \to Y_j$, $j \in I$, there is a unique morphism $f : \bigsqcup_{i \in I} X_i \to Y$ such that $f_j = f q_j$ for all $j \in I$.

In the category $Sets$, we can define coproducts to be simply the disjoint union of the collection of objects (this justifies the notation used above). It is easy to see that this satisfies the definition.

Definition 5.2. Let X be an object in $\mathcal{C}$ and G be a subgroup of the group of automorphisms of X (isomorphisms of X with itself) in $\mathcal{C}$. The quotient of X by G is an object X/G in $\mathcal{C}$ with a morphism $p : X \to X/G$ such that $p = p\sigma$ for all $\sigma \in G$, and so that for any morphism $f : X \to Y$ in $\mathcal{C}$ such that $f = f\sigma$ for all $\sigma \in G$, there exists a unique $g : X/G \to Y$ such that $f = gp$.

In the category $Sets$, we can take X/G to be the collection of orbits, and p the natural map that takes x to its orbit. Once again, it is easy to see that this satisfies the requirements.

Definition 5.3. A morphism $u : X \to Y$ is called an isomorphism of X with a direct summand of Y if there exists a morphism $q_2 : Z \to Y$ such that Y, together with $q_1 = u$ and q_2, is the coproduct of X and Z.

In $Sets$, we can simply let $Z = Y - u(X)$.

Now we can give the definition of a Galois category.

Definition 5.4. Let $\mathcal{C}$ be a category, $F : \mathcal{C} \to sets$ a covariant functor from $\mathcal{C}$ to the category of finite sets. $\mathcal{C}$ is a Galois category with fundamental functor F if the following conditions are satisfied:

(1) $\mathcal{C}$ has a final object, and the fiber product of any two objects over a third

exists in $\mathcal{C}$.

(2) $\mathcal{C}$ has an initial object, finite coproducts exist in $\mathcal{C}$, and the quotient of an object by a finite group of automorphisms exists in $\mathcal{C}$.

(3) Any morphism u in $\mathcal{C}$ can be written $u = u'u''$, where u'' is an epimorphism, and u' is a monomorphism. Any monomorphism from X to Y is an isomorphism of X with a direct summand of Y.

(4) F maps final objects to final objects, and commutes with fiber products.

(5) F commutes with finite coproducts and quotients (as above) and maps epimorphisms to epimorphisms.

(6) If u is a morphism in $\mathcal{C}$, and $F(u)$ is an isomorphism, then u is an isomorphism.

In the final few sections, we give some examples of Galois categories and show how they satisfy these axioms.

6. Finite Sets

We now consider the simplest example of a Galois category, the category of finite sets, *sets*, with the identity functor to itself. We verify the axioms for this example:

(1) *sets* has a final object, namely the set $\mathbf{1}$ consisting of only one element (note that final objects are unique up to isomorphism). If f is a map from a set X to $\mathbf{1}$, every element is sent to the single element, so the map is unique.

Let $f : Y \to Z$ and $g : X \to Z$. We define the fiber product of X and Y over Z to be $X \times_Z Y = \{(x, y) \in X \times Y | f(y) = g(x)\}$.

(2) The initial object is the empty set, $\emptyset$, since the map f from $\emptyset$ to X is unique (any two such maps are vacuously the same).

We define the finite coproduct of a finite collection of sets X_i, $i \in I$, to be $\bigsqcup_{i \in I} X_i$, the usual disjoint union of sets.

We define the quotient of on object by a finite subgroup G of automorphisms of that object to be the set of orbits, so $X/G = \{Gx | x \in X\}$ (recall $Gx = \{gx | g \in G\}$), and define $p : X \to X/G$ by $p(x) = Gx$.

(3) In the category *sets*, surjections are epimorphisms and injections are monomorphisms, and every function can be written as the composition of an injection and a surjection.

To show that any monomorphism $u : X \to Y$ is an isomorphism of X with a direct summand of Y, we simply let $Z = Y - u(X)$ and q_2 be the natural containment $q_2 : Z \to Y$.

(4),(5),(6) These axioms are trivial because F is the identity functor.

7. Finite Covering Spaces

Now we consider the category $\mathcal{C}$ of finite coverings of a connected topological space X with the following functor: fix $x \in X$. Define $F_x : \mathcal{C} \to sets$ by $(f : Y \to X) \mapsto f^{-1}(x)$ for any finite covering $f : Y \to X$ of X. Before we verify the Galois theory axioms, we recall some definitions.

Definition 7.1. If X is a topological space, a space over X is a topological space Y with a continuous map $p : Y \to X$.

Definition 7.2. A morphism between spaces $p_i : Y_i \to X$ (for $i = 1, 2$) over X is a continuous map $f : Y_1 \to Y_2$ such that $p_1 = p_2 \circ f$.

Definition 7.3. A space $p : Y \to X$ over X is a cover of X if for each point in X there is a neighborhood V so that $p^{-1}(V)$ is a disjoint union of open sets U_i in Y, and $p|_{U_i}$ is a homeomorphism of U_i with V.

Now, we verify the axioms:

(1) The final object is X with the identity map $Id : X \to X$.

The fiber product of Y_1 and Y_2 over Z with $f : Y_1 \to Z$ and $g : Y_2 \to Z$ is $Y_1 \times_Z Y_2 = \{(y_1, y_2) | f(y_1) = g(y_2)\}$ with the subspace topology inherited from $Y_1 \times Y_2$.

(2) The initial object is the empty covering $f : \emptyset \to X$.

The finite coproduct of X_i, $i \in I$, is $\bigsqcup_{i \in I} X_i$, the disjoint union with the usual topology.

The quotient of Y by a finite subgroup G of the automorphism group of Y is the set of orbits, given the quotient topology.

(3) Let f be a morphism from $p_1 : Y_1 \to X$ to $p_2 : Y_2 \to X$. Let $f'' : Y_1 \to \{f^{-1}(y_2) | y_2 \in Y_2\}$, with $y_1 \mapsto f^{-1}(y_2)$ if $y_1 \in f^{-1}(y_2)$, and $f' : \{f^{-1}(y_2) | y_2 \in Y_2\} \to Y_2$, with $f^{-1}(y_2) \mapsto y_2$. Then $f = f'f''$, f' is injective and f'' is surjective.

If $f : Y_1 \to Y_2$ is a monomorphism, let $X = Y_2 - f(Y_1)$ with the subspace topology.

(4) $F : (Id : X \to X) = f^{-1}(x) = x = \mathbf{1}$, so F takes final objects to final objects.

Let $f_{Y_1} : Y_1 \to X$, $f_{Y_2} : Y_2 \to X$, and $f_Z : Z \to X$ be covers and $f : Y_1 \to Z$ and $g : Y_2 \to Z$ morphisms. Let $\overline{f}$ and $\overline{g}$ be the images of f and g under F. Then

$$\begin{aligned} F(h : Y_1 \times_Z Y_2 \to X) &= f^{-1}(x) \\ &= \{(y_1, y_2) | f_s : f(y_1) = g(y_2) \mapsto x \\ &= \{(y_1, y_2) | f(y_1) = g(y_2)\} \text{ (a subset of } f_{Y_1}^{-1}(x) \times f_{Y_2}^{-1}(x)) \\ &= \{(y_1, y_2) | \overline{f}(y_1) = \overline{g}(y_2)\} \text{ (a subset of } f_{Y_1}^{-1}(x) \times f_{Y_2}^{-1}(x)) \\ &= f_{y_1}^{-1}(x) \times_Z f_{y_2}^{-1}(x) \\ &= F(Y_1 \to X) \times_Z F(Y_2 \to X) \end{aligned}$$

Thus we have F commutes with fiber products.

(5) We show that F commutes with finite coproducts:

$$\begin{aligned} F(f : X_1 \sqcup \cdots \sqcup X_n \to X) &= f^{-1}(x) \\ &= \{x_1 \in X_1 | f(x_1) = x\} \sqcup \cdots \sqcup \{(x_n \in X_n | f(x_n) = x\} \\ &= f_1^{-1}(x) \sqcup \cdots \sqcup f_n^{-1}(x) \\ &= F(f_1 : X_1 \to X) \sqcup \cdots \sqcup F(f_n : X_n \to X) \end{aligned}$$

Let $p_1 : Y_1 \to X$ and $p_2 : Y_2 \to X$ be covers, and $f : Y_1 \to Y_2$ an epimorphism (meaning onto). Then $F(f : p_1 \to p_2) = \overline{f} : p_1^{-1}(x) \to p_2^{-1}(x)$. We can clearly see that f is onto implies that $\overline{f}$ is onto, so F takes epimorphisms to epimorphisms.

We show that F commutes with quotients (note that each element of $F(G)$ is in some sense a restriction of an element in G):

$$\begin{aligned} F(p_G : Y/G \to X &= p_G^{-1}(x) \\ &= \{Gy | p_G(Gy) = x\} \\ &= \{Gy | p(y) = x\} \\ &= \{y | p(y) = x\}/G \\ &= p^{-1}(x)/G \\ &= F(p : Y \to X)/G \\ &= F(Y)/G \end{aligned}$$

(6) Finally, $\overline{f} : p_1^{-1}(x) \to p_2^{-1}(x)$ is an isomorphism implies that $f : (p_1 : Y_1 \to$

$X) \to (p_2 : Y_2 \to X)$ is an isomorphism.

This completes the proof that the category of finite coverings of a fixed topological space is, in fact, a Galois category.

8. Field Extensions, Separable Algebras

We now go through a quick review of the ideas leading to the Main Theorem of Galois Theory, which we then generalize using category theory by showing that the category of free separable k-algebras and the category of π-sets with a continuous action are antiequivalent, where k is a field, and π is its absolute Galois group. We go through these theorems quickly and largely without proof; proofs can in found in Chapter 2 of [4].

We begin by reviewing some definitions:

If k is a field, a k-algebra is a ring A with 1 with a ring homomorphism $f : k \to A$, such that $1_k \mapsto 1_A$ and $f(k)$ is in the center of A. We can think of a k-algebra as a ring containing k.

A k-algebra homomorphism from A to B (both k-algebras) is a ring homomorphism $\phi : A \to B$ such that $1_A \mapsto 1_B$ and $\phi(ra) = r\phi(a)$ for all $r \in k$ and all $a \in A$.

Suppose B is a k-algebra that is finitely generated as a k-module. Also, for all $b \in B$ there is a map $m_b : B \to B$ such that $m_b(x) = bx$. This map is k-linear, and we define $Tr(b) := Tr(m_b)$. This trace map is also k-linear, and $Tr(a) = rank_k(B) \cdot a$ for all $a \in A$. $Hom_k(B, k)$ as a k-module is free over k and has the same rank as B. We define $\phi : B \to Hom_k(B, k)$ by $(\phi(x))(y) = Tr(xy)$ for all $x, y \in B$. Then, if ϕ is an isomorphism, we say that B is separable over A.

If L is a field extension of the field k, we say L is Galois if $k \subset L$ is algebraic and there exists a subgroup $G \subset Aut(L)$ such that $k = L^G$ (the field in L fixed by G). We define the Galois group $Gal(L/k) = Aut_k(L)$.

Let $\bar{k}$ be the algebraic closure of a field k. Let $F \subset k[X] - \{0\}$ be a collection of nonzero polynomials. The splitting field of F over k is the subfield of $\bar{k}$ generated by k and the roots in $\bar{k}$ of the polynomials in F.

A polynomial $f \in k[X] - \{0\}$ is separable if it has no repeated roots in $\bar{k}$. An element $\alpha \in \bar{k}$ is separable if its minimal polynomial f_k^α over k is separable.

If L is a subfield of $\bar{k}$, $k \subset L \subset \bar{k}$, L is separable over k if every $\alpha \in L$ is separable over k. L is normal over k if for all $\alpha \in L$, f_k^α splits completely in $L[X]$.

The following theorem enables us to see how profinite groups begin to appear.

Theorem 8.1. *Let k be a field, and L a field extension, so that $k \subset L \subset \bar{k}$. Let $I = \{$subfields E of L such that E is a finite Galois extension of $k\}$. This set is partially ordered by inclusion, and is a directed partially ordered set. The following*

are equivalent:

(1) L is a Galois extension of k.

(2) L is normal and separable over k.

(3) There exists a set $F \subset k[X] - \{0\}$ of separable polynomials such that L is the splitting field of F over k.

(4) $\bigcup_{E \subset I} E = L$.

If these conditions are satisfied:

$Gal(L/k) \simeq \lim_{\leftarrow E \in I} Gal(E/k)$.

Proof. Here, we only define the isomorphism from the final claim: $Gal(L/k) \to \lim_{\leftarrow E \in I} Gal(E/k)$, $\sigma \mapsto (\sigma|_E)_{E \in I}$. The rest of the proof can be found in [4]. □

The following theorem is familiar from Galois theory, once again the proof can be found in [4].

Theorem 8.2. *(Main Theorem of Galois Theory) Let $k \subset L$ be a Galois extension of fields with Galois group G. There is a bijective correspondence between the set of intermediate fields and the set of closed subgroups of G. We define*

$\phi : \{E | E$ is a subfield of L containing $k\} \to \{H | H$ is a closed subgroup of $G\}$

$\phi : E \mapsto Aut_E(L)$, and

$\psi : \{H | H$ is a closed subgroup of $G\} \to \{E | E$ is a subfield of L containing $k\}$

$\psi : H \mapsto L^H$.

Then ϕ and ψ are bijective and inverse to each other. This bijection reverses inclusions. If E corresponds to H:

(1) $k \subset E$ is finite if and only if H is open.

(2) If $E \subset L$ is Galois, $Gal(L/E) \simeq H$.

(3) $\sigma[E]$ corresponds to $\sigma H \sigma^{-1}$ for all $\sigma \in G$.

(4) $k \subset E$ is Galois if and only if H is a normal subgroup of G, and $Gal(E/k) \simeq G/H$ if $k \subset E$ is Galois.

Before we continue, we give some definitions:

The separable closure k_s of a field k is defined to be $k_s = \{x \in \bar{k} | x$ is separable over $k\}$. k_s is a field, and $k_s = \bar{k}$ if and only if k is perfect.

$Gal(k_s/k)$ is called the absolute Galois group of k.

Once again, proof of the following theorem can be found in [4].

Theorem 8.3. *Let $\bar{k}$ be the algebraic closure of a field k, B a finite dimensional k-algebra. Define $\bar{B} := B \otimes_k \bar{k}$, a $\bar{k}$-algebra. The following are equivalent:*

(1) B is separable over k.

(2) $\bar{B}$ is separable over $\bar{k}$.

(3) $\bar{B} \simeq \bar{k}^n$ as $\bar{k}$-algebras, for some $n \geq 0$.

(4) $B \simeq \Pi_{i=1}^t B_i$ as k-algebras, where each B_i is a finite separable extension of k.

Now we arrive at the main point of this section:

Theorem 8.4. *Let k be a field and π its absolute Galois group. Then the categories ${}_kSALg$ of separable k-algebras and π-sets of finite sets with a continuous action of π are antiequivalent.*

Proof. We give the contravariant functors $F :_k SAlg \to \pi$-sets and $G : \pi$-sets$\to_k SAlg$ such that FG and GF are equivalent to the identity functors. This proof is due to Lenstra, and can be found in a more complete form in [4].

We begin by defining F. Let k_s be the separable closure of k, so $\pi = Gal(k_s/k)$. If B is a free separable k-algebra, let $F(B) = Alg_k(B, k_s)$, the set of all k-algebra homomorphisms from B to k_s. If $g : B \to k_s$ is a homomorphism, $\sigma \in \pi$, then $\sigma \circ g : B \to k_s$ is a homomorphism, so we get an action of π on $Alg_k(B, k_s)$. This action is continuous. If $f : B \to C$ is a k-algebra homomorphism (a morphism in ${}_kSAlg$). Define $F(f) : F(C) \to F(B)$ by $F(f)(g) = g \circ f$, where $g : C \to k_s$.

Now we define G. Let E be a finite π-set. We define $G(E) = Mor_\pi(E, k_s)$, the set of morphisms of π-sets from E to k_s. The k-algebra structure of k_s gives us a k-algebra structure on $G(E)$. $G(E)$ is also finite and dimensional and separable. If $f : E \to D$ is a morphism of π-sets, we define $G(f) : G(D) \to G(E)$ by $G(f)(g) = g \circ f$, a morphism of k-algebras. □

We end this paper by showing that the opposite of the category of separable k-algebras is, in fact, a Galois category. We define $F(A) = Alg_k(A, \bar{k}) \simeq Alg_k(A, k_s)$, and go through the Galois category axioms one by one, as before. In demonstrating the truth of these axioms it is important to remember that we are dealing with the *opposite* category, so arrows are reversed.

(1) The final object is k. (k is an initial object in ${}_kSAlg$, so is final in ${}_kSAlg^{op}$.)

We define the fiber product of A and B over C by defining the pushout in ${}_kSAlg$. From the universal property of tensor products (as in the previous example with rings), we have the tensor product of A and B over C is the pushout:

$$\begin{array}{ccc} C & \longrightarrow & A \\ \downarrow & & \downarrow \\ B & \longrightarrow & A \otimes_C B \end{array} \tag{8.5}$$

(2) The initial object is k^0, the k-algebra with only a zero-element (this is the final object in ${}_kSAlg$).

We define finite coproducts by defining a product in ${}_kSAlg$, so $A \sqcup B$ is the k-algebra generated by a kind of disjoint union of A and B, so if $A \simeq k^n$ and $B \simeq k^m$, $A \sqcup B \simeq k^{nm}$.

We define the quotient of X by G as the orbits of X under the action of $G^{op} = G$ ($G^{op} = G$ because G is a collection of automorphisms).

(3) This is the same as saying such a factorization exists in the category itself (as opposed to the opposite category), so given $u : X \to Y$, we define $u'' : X \to \{f^{-1}(y)\}$, $x \mapsto f^{-1}(x)$ and $u' : \{f^{-1}(y)\} \to Y$, $f^{-1}(y) \mapsto y$.

Given a monomorphism $f^{op} : X \to Y$, $f : Y \to X$ is an epimorphism in ${}_kSAlg$. We want an epimorphism $g : Y \to Z$ so that $Y \simeq X \sqcup Z$. Because we are dealing with free k-algebras, we can take a basis for the image of X, extend it to a basis

for Y, and let Z be generated by the basis elements not in X.

(4) We show that F takes final objects to final objects: $F(k) = Alg_k(k, \bar{k}) = \mathbf{1}$.

We show that the functor commutes with fiber products:

$$\begin{aligned} F(A \otimes_C B) &= Alg_k(A \otimes_C B, \bar{k}) \\ &= \{C\text{-bilinear maps } \Phi : A \times B \to \bar{k}\} \\ &= \{\Phi : A \times B \to \bar{k} | \Phi(c \cdot a, b) = c \cdot \Phi(a, b) = \Phi(a, c \cdot b)\} \\ &= \{(\phi \times \psi) \in Alg_k(A, \bar{k}) \times Alg_k(B, \bar{k}) | F(f)(\phi) = F(g)(\psi)\} \\ &= Alg_k(A, \bar{k}) \times_{Alg_k(C, \bar{k})} Alg_k(B, \bar{k}) \\ &= F(A) \otimes_{F(C)} F(B) \end{aligned}$$

(5) We show that F commutes with finite coproducts.

$$\begin{aligned} F(\bigsqcup X_i &= Alg_k(\bigsqcup X_i, \bar{k}) \\ &= \bigsqcup Alg_k(X_i, \bar{k}) \\ &= \bigsqcup F(X_i) \end{aligned}$$

This is because an algebra homomorphism is determined by how it works on the generators. We show that F maps epimorphisms to epimorphisms: if $f : A \to B$ is an epimorphism, $f^{op} : B \to A$, a k-algebra homomorphism, is a monomorphism. Then $F(f : A \to B) : Alg_k(A, \bar{k}) \to Alg_k(B, \bar{k})$, $\phi \mapsto \phi \circ f^{op}$. f^{op} is a monomorphism, so B is isomorphic to a subalgebra of A, so $F(f)$ is surjective, and so an epimorphism.

We show that F commutes with quotients:

$$\begin{aligned} F(X/G) &= Alg_k(X/G, \bar{k}) \\ &= \{\text{homomorphisms } \phi : X/G \to \bar{k}\} \\ &= \{\text{homomorphisms } \phi : \{Gx\} \to \bar{k}\} \\ &= \{\text{homomorphisms } \phi : \{\{\sigma x | \sigma \in G\}\} \to \bar{k}\} \\ &= \{\phi(\{\sigma | \sigma \in G\}) | \phi : X \to \bar{k}\} \\ &= \{\{\phi\sigma | \sigma \in G\} | \phi \in F(X)\} \\ &= \{\{\sigma^{op}\phi | \sigma^{op} \in F(G)\} | \phi \in Alg_k(X, \bar{k})\} \\ &= \{F(G)\phi | \phi \in Alg_k(X, \bar{k})\} \\ &= Alg_k(X, \bar{k})/F(G) \\ &= F(X)/F(G) \end{aligned}$$

(6) Finally , if $F(u)$ is an isomorphism, $F(u) : Alg(A, \bar{k}) \to Alg(B, \bar{k})$, we must have that u is an isomorphism.

This completes the proof that the opposite of the category of free separable k-algebras is a Galois category.

Acknowledgments. It is a pleasure to thank my mentor, Alan Anders, for constant inspiration and infinite energy and enthusiasm. I would also like to thank Matthew Thibault for introducing me to Alan. Finally, I would like to thank Peter May and Paul Sally Jr. for providing me with this opportunity, and Peter May in particular for introducing me to category theory and inspiring me to study this subject.

References

[1] Steven Awodey. Category Theory. Pittsburgh. 2005.
[2] Saunders Mac Lane. Categories for the Working Mathematician. Springer-Verlag New York. 1971.
[3] Tamàs Szamuely. Galois Groups and Fundamental Groups. Budapest. 2008.
[4] H. W. Lenstra. Galois Theory for Schemes. 2008.
[5] David S. Dummit and Richard M. Foote. Abstract Algebra. John Wiley and Sons. 2004.