Profinite Groups and Infinite Galois Theory Notes
(Independent Study with Dr. Margaret Bilu)

Luke Poeppel
luke.poeppel@gmail.com
Courant Institute of Mathematical Sciences, NYU
2020-06-01

1. Basic Category Theory

We begin with a short introduction to category theory to motivate projective limits.

Definition 1.1. A *Category* $\mathscr{C}$ consists of a class of objects $\text{Ob}(\mathscr{C})$ along with a class of morphisms $\text{Arr}(\mathscr{C})$ such that for any $A, B \in \text{Ob}(\mathscr{C})$, there exists a subclass $\text{Hom}_{\mathscr{C}}(A, B)$ of morphisms from A to B with a composition law,

$$\text{Hom}_{\mathscr{C}}(A, B) \times \text{Hom}_{\mathscr{C}}(B, C) \to \text{Hom}_{\mathscr{C}}(A, C)$$

that sends $(f, g) \mapsto g \circ f$. For all $A \in \text{Ob}(\mathscr{C})$, there exists an identity morphism, $id_A \in \text{Hom}_{\mathscr{C}}(A, A)$. Finally, composition of maps must be associative, i.e., $h \circ (g \circ f) = (h \circ g) \circ f$.

When $f \in \text{Hom}_{\mathscr{C}}(A, B)$, we write that $f : A \to B$ in $\mathscr{C}$ and if

$$A \xrightarrow{f} B \xrightarrow{g} C$$

then $g \circ f : A \to C$ for $A, B, C \in \text{Ob}(\mathscr{C})$. Formally, $\text{Hom}_{\mathscr{C}}(A, B)$ is a *monoid* since there exists an identity element and the operation is associative. There are instances in which either $\text{Ob}(\mathscr{C})$ or $\text{Hom}_{\mathscr{C}}(A, B)$ forms a set rather than a class. In this case, we call $\mathscr{C}$ a *small* category. An element $f \in \text{Hom}_{\mathscr{C}}(A, B)$ is an *isomorphism* if there exists a $g \in \text{Hom}_{\mathscr{C}}(B, A)$ such that $g \circ f = \text{id}_A$ and $f \circ g = \text{id}_B$. First we present several classical categories.

(a) Denote by **Set** the category of sets where $\text{Ob}(\textbf{Set})$ is the class of all sets and for any $X, Y \in \text{Ob}(\textbf{Set})$, $\text{Hom}_{\textbf{Set}}(X, Y)$ is the class of all functions between X and Y. Isomorphisms in the category of sets are bijections.

(b) Denote by **Grp** the category of groups where $\text{Ob}(\textbf{Grp})$ is the class of all groups and $\text{Hom}_{\textbf{Grp}}(G, H)$ is the class of all group homomorphisms from G to H. In other words, $\varphi \in \text{Hom}_{\textbf{Grp}}(G, H) \iff \varphi(x * y) = \varphi(x) \diamond \varphi(y)$ for all $x, y \in G$.

(c) Denote by **Met** the category of metric spaces. Then for any $(X, d_1), (Y, d_2) \in \text{Ob}(\textbf{Met})$, we have that $\text{Hom}_{\textbf{Met}}((X, d_1), (Y, d_2))$ is the class of all metric functions between the spaces (i.e. Lipschitz function of metric spaces with constant $K = 1$.)

(d) Denote by **Top** the category of topological spaces. $\text{Arr}(\textbf{Top})$ is therefore the class of all continuous maps between topological spaces in $\text{Ob}(\textbf{Top})$. In this case, homeomorphisms (i.e. bijective, continuous maps with a continuous inverse) are the isomorphisms of the category.

Definition 1.2. A *Subcategory* $\mathscr{D}$ of a category $\mathscr{C}$ consists of a subclass of $\text{Ob}(\mathscr{C})$ along with a subclass of $\text{Arr}(\mathscr{C})$ such that the morphisms in $\mathscr{D}$ agree with the morphisms in $\mathscr{C}$.

A few examples of subcategories include: (i) the category of *Abelian* groups, **Ab**, is a subcategory of **Grp**, (ii) the category of all Hausdorff topological spaces, **Haus**, is a subcategory of **Top**.

Definition 1.3. If $A \in \text{Ob}(\mathscr{C})$ for a category $\mathscr{C}$, we say that A is *universally repelling* if for every $B \in \text{Ob}(\mathscr{C})$, there is a unique morphism from A to B. Equivalently,

$$A \text{ is universally repelling} \iff |\mathrm{Hom}_{\mathscr{C}}(A, B)| = 1$$

We say that A is *universally attracting* if for every $B \in \mathrm{Ob}(\mathscr{C})$, there is a unique morphism from B to A. Equivalently,

$$A \text{ is universally attracting} \iff |\mathrm{Hom}_{\mathscr{C}}(B, A)| = 1$$

Proposition 1.1. In the category **Set**, the empty set $\emptyset$ is universally repelling.

Proof. We have that $\emptyset$ is universally repelling if for every $B \in \mathrm{Ob}(\mathbf{Set})$, there is a unique morphism from $\emptyset \to B$. But $f : \emptyset \to B$ is the empty function. The fact that the empty function is unique is vacuously true. Thus, $\emptyset$ is universally repelling in **Set**. □

Proposition 1.2. The trivial group $\{e\}$ is both universally attracting and universally repelling in the category of groups.

Proof. We must show that $|\mathrm{Hom}_{\mathbf{Grp}}(\{e\}, H)| = |\mathrm{Hom}_{\mathbf{Grp}}(G, \{e\})| = 1$. Note that the only function $\varphi : G \to \{e\}$ is the 0-map (or, more generally, the e-map) which sends each element g to the identity of the group. Also, $\phi : \{e\} \to H$ is simply the canonical inclusion map (which is always unique). Thus, $\{e\}$ is both universally attracting and universally repelling in the category of groups. □

Most functions encountered in algebra send objects to others within the same category. Consider, for example, the determinant function $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}$. The domain is the group of $n \times n$ invertible matrices over a field $\mathbb{F}$ and the codomain is a field. But, trivially, since all fields can be seen as groups (with far more structure), the morphism still exists in the category of groups. However, we are often interested in functions that take us from one category to a distinct category. To accomplish this, we use *Functors*.

Definition 1.4. A functor is a map between categories that preserves structure. Formally, if $\mathscr{C}$ and $\mathscr{D}$ are categories and $F : \mathscr{C} \to \mathscr{D}$, then F assign to each object $A \in \mathscr{C}$ an object $F(A) \in \mathscr{D}$ and each arrow $f : A \to B$ in $\mathscr{C}$ to another arrow, $Ff : F(A) \to F(B)$ such that

(a) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$

(b) $F(g \circ f) = F(g) \circ F(f)$

In this case, F is called a *covariant functor*. If condition (a) is met but we instead have $F(g \circ f) = F(f) \circ F(g)$, then F is called *contravariant*.

A subcategory $\mathscr{D}$ of $\mathscr{C}$ is endowed with a canonical inclusion functor that takes all elements to their identity in the larger category. Within a category, we have similar definitions for injectivity, surjectivity, and bijectivity.

Definition 1.5. A functor $F : \mathscr{C} \to \mathscr{D}$ is called *faithful* if it is injective on morphisms.

Definition 1.6. A functor $F : \mathscr{C} \to \mathscr{D}$ is called *full* if it is surjective on morphisms.

Definition 1.7. A functor $F : \mathscr{C} \to \mathscr{D}$ is called *fully faithful* if it is bijective on morphisms.

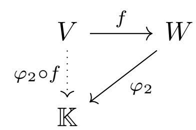
Definition 1.8. An *endofunctor* is a functor from a category $\mathscr{C}$ to itself.

We now consider several important examples of functors.

(a) Consider the covariant functor $F : \mathbf{Grp} \to \mathbf{Set}$ that faithfully takes every group G to its underlying set $U(G)$. Functors of this type are called *forgetful*; broadly, they are maps that lose some structure/axioms.

(b) Let $F : \mathbf{Set} \to \mathbf{Grp}$ be the functor that sends each set to the free group generated by that set.

(c) Denote by $\mathbf{Vect}_{\mathbb{K}}$ the category of vector spaces over the field $\mathbb{K}$. A *linear functional* on a vector space V is a linear map $V \to \mathbb{F}$. We denote by $\mathscr{L}(V, \mathbb{F}) = V^*$ the set of all linear functionals, i.e., the *dual* of V. Consider the endofunctor $F : \mathbf{Vect}_{\mathbb{K}} \to \mathbf{Vect}_{\mathbb{K}}$ that sends a vector space $V \in \mathrm{Ob}(\mathbf{Vect}_{\mathbb{K}})$ to its dual space V^*. What does this functor do to the morphisms? Given a linear transformation $f : V \to W$, can we get a map $Ff : V^* \to W^*$? So, Ff sends a linear functional $\varphi_1 : V \to \mathbb{K}$ to another linear functional $\varphi_2 : W \to \mathbb{K}$. But this map can only be made with a *pullback* (composition). Indeed, we have the following commutative diagram:



Thus, we define $F(f) := f^*$ where $f^*(\varphi) = \varphi \circ f$. Then,

$$\varphi_2 : (W \to \mathbb{K}) \mapsto \varphi_2 \circ f : (V \to \mathbb{K})$$

which shows that the arrows are reversed; therefore, F is contravariant.

Definition 1.9. A pair of functors $F : A \to B$ and $G : B \to A$ is called *adjoint* if for every pair of objects (a, b) with $a \in A$ and $b \in B$, there is a functorial bijection,

$$\tau : \mathrm{Hom}_B(F(a), b) \to \mathrm{Hom}_A(a, G(b))$$

Equivalently, there is a bijection such that for all $f : a \to a'$ in A and $g : b \to b'$ in B, the following diagram commutes:

$$\begin{array}{ccccc} \mathrm{Hom}_B(F(a'), b) & \longrightarrow & \mathrm{Hom}_B(F(a), b) & \longrightarrow & \mathrm{Hom}_B(F(a), b') \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Hom}_A(a', G(b)) & \longrightarrow & \mathrm{Hom}_A(a, G(b)) & \longrightarrow & \mathrm{Hom}_A(a, G(b')) \end{array}$$

Proposition 1.3. Let $F : \mathbf{Set} \to \mathbf{Grp}$ be the functor that sends each set to the free group generated by the set and let $G : \mathbf{Grp} \to \mathbf{Set}$ be the forgetful functor that sends G to its underlying set $U(G)$ (see the above examples). Then F is left adjoint to G and G is right adjoint to F.

Proof. This is beyond the scope of this paper. □

2. Direct and Inverse Systems

In constructing direct and inverse limits for the creation of profinite groups, we must first consider direct and inverse systems within a category. Then we may examine the universally repelling/attracting objects of these systems that provides the desired limit. First, we require two simple definitions.

Definition 2.1. A *partially ordered set* (or *poset*) is a set along with a relation $\preceq \subseteq A \times A$ such that for every $x, y, z \in A$, the following are satisfied:

(a) *Reflexivity*: $x \preceq x$

(b) *Antisymmetry*: $(x \preceq y \land y \preceq x) \implies x = y$

(c) *Transitivity*: $(x \preceq y \land y \preceq z) \implies x \preceq z$

It is important to note that the trichotemy $x \preceq y$, $y \preceq x$, or $x = y$ does not necessarily hold for all $x, y \in A$ in a partial order. Consider, for example, the poset $(\mathbb{N}, |)$ where $|$ is the divisibility relation. It is easy to see that the axioms are satisfied, but note that $2 \nmid 3$, $3 \nmid 2$, and $2 \neq 3$. If, on the other hand, one of the relations *does* hold for all $x, y \in A$, then the set is *totally ordered*; one standard example of this is $(\mathbb{Z}, \leq)$.

Definition 2.2. A *directed set* is a partially ordered set $(A, \preceq)$ such that for all $x, y \in A$, there exists a $z \in A$ such that $x \preceq z$ and $y \preceq z$. Equivalently, a set is directed if there exist pairwise upper bounds for all elements of the set.

Proposition 2.1. Every totally ordered set is directed.

Proof. TODO (result from lattice theory) □

We briefly discuss an important example of a directed set that will be discussed in detail later.

Proposition 2.2. Let (X, τ) be a topological space. Suppose $x_0 \in T$ and let U_{x_0} and V_{x_0} be neighborhoods around x_0 (not necessarily open). We can turn all of the neighbourhoods of x_0 into a directed set by defining $U \preceq V \iff V \subseteq U$. Intuitively, for any two neighborhoods of x_0 (one contained in the other), the pairwise upper bound will be a smaller neighborhood.

Proof. We must first show that $((X, \tau), \preceq)$ is a partial order. Suppose U, V, and W, are neighbourhoods around $x_0 \in X$. By definition of $\subseteq$, it always holds that $U \subseteq U$, so $\preceq$ is reflexive. If $U \subseteq V$ and $V \subseteq U$, then $U = V$, so antisymmetry holds. Finally, if $U \subseteq V$ and $V \subseteq W$, then $U \subseteq W$, so transitivity of $\preceq$ holds. Now we must show that for any U, V such that $V \subseteq U$, there exists a W such that $U \subseteq W$ and $V \subseteq W$. But this is trivial since we may always choose $\{x_0\}$. Thus, (X, τ) under the $\preceq$ relation is a directed set. □

We are now able to define direct systems.

Definition 2.3. Suppose I is a directed set under $\preceq$ and $\mathscr{C}$ is a category. Let $\{A_i\}_{i \in I}$ be a collection of objects in $\mathrm{Ob}(\mathscr{C})$ indexed by I and let $\varphi_{i \preceq j} : A_i \to A_j$ be a homomorphism for all $i \preceq j$ such that,

(a) $\varphi_{i \preceq i} = id_{A_i} : A_i \to A_i$.

(b) $\varphi_{j \preceq k} \circ \varphi_{i \preceq j} = \varphi_{i \preceq k}$ when $i \preceq j \preceq k$.

Then, $\langle A_i, \varphi_{i \preceq j} \rangle$ is called a *direct system* in $\mathscr{C}$. Note that "homomorphism" is meant in the context of the category in which the system exists; in the category of rings, for example, $\varphi_{i \preceq j}$ is understood to be a ring homomorphism.