DIRECT LIMITS, INVERSE LIMITS, AND PROFINITE GROUPS

MATH 519

The first three sections of these notes are compiled from [L, Sections I.10, I.11, III.10], while the fourth section follows [RV, Section 1.3].

1. Universal objects

A *category* $\mathcal{C}$ is a collection of *objects*, denoted $\mathrm{Ob}(\mathcal{C})$, together with a collection of *morphisms*, denoted $\mathrm{Ar}(\mathcal{C})$ (standing for "arrows"), such that for any $A, B \in \mathrm{Ob}(\mathcal{C})$, there is a set of morphisms $\mathrm{Mor}(A, B)$, called the *morphisms from A to B*, which satisfy the following:

(1) For any $f \in \mathrm{Ar}(\mathcal{C})$, there are unique objects A and B such that $f \in \mathrm{Mor}(A, B)$.
(2) For any three objects $A, B, C \in \mathrm{Ob}(\mathcal{C})$, there is a map, called the *composition map*,
$$\mathrm{Mor}(B, C) \times \mathrm{Mor}(A, B) \to \mathrm{Mor}(A, C),$$
denoted $(f, g) \mapsto f \circ g$, where $f \in \mathrm{Mor}(B, C)$, $g \in \mathrm{Mor}(A, B)$, such that
   (a) For every $A \in \mathrm{Ob}(\mathcal{C})$, there is a morphism $\mathrm{id}_A \in \mathrm{Mor}(A, A)$, such that for any $B \in \mathrm{Ob}(\mathcal{C})$, $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, A)$, we have $f \circ \mathrm{id}_A = f$ and $\mathrm{id}_A \circ g = g$.
   (b) For any $A, B, C, D \in \mathrm{Ob}(\mathcal{C})$, and any $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, C)$, $h \in \mathrm{Mor}(C, D)$, we have
$$(h \circ g) \circ f = h \circ (g \circ f).$$

Condition (a) above says that there are always morphisms which act as the identity under composition, and condition (b) says that the composition law is associative. Generally speaking, morphisms may be thought of as functions between objects which preserve certain defining structures of objects, and for this reason we use the notation $f : A \to B$ if $f \in \mathrm{Mor}(A, B)$.

A morphism $f \in \mathrm{Mor}(A, B)$ is called an *isomorphism* if there exists a morphism $g \in \mathrm{Mor}(B, A)$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. An isomorphism in $\mathrm{Mor}(A, A)$ is called an *endomorphism* of A.

The following are typical examples, which can be checked directly to satisfy the above conditions.

Example 1. If $\mathrm{Ob}(\mathcal{C})$ is the collection of all sets, and morphisms are functions between sets, then $\mathcal{C}$ is a category. Bijective correspondences between sets are isomorphisms in $\mathrm{Ar}(\mathcal{C})$.

Example 2. Let $\mathrm{Ob}(\mathcal{C})$ be the collection of topological spaces, with morphisms being continuous maps. This is the category of topological spaces. Homeomorphisms are isomorphisms in this category.

Example 3. Consider the collection of all groups, which are viewed as objects with group homomorphisms as morphisms. This is the category of groups, which we will denote **Grp**. We could also restrict the objects to consist of abelian groups, with group homomorphisms as morphisms, which is the category of abelian groups, denoted **Ab**. Similarly, we have the category of rings with ring homomorphisms, denote **Rng**, or given a ring R, the category of modules over R with homomorphisms of R-modules, denoted by R-**Mod**. Note that since abelian groups are exactly modules over $\mathbb{Z}$, then the category **Ab** may be identified with the category $\mathbb{Z}$-**Mod**. Another example which we have dealt with quite a bit is the category of topological groups, **TopGrp**, with morphisms being continuous homomorphisms.

Example 4. Fix some set S. Consider objects to be functions from S to some group, so any function $f : S \to G$, where G is any group. If f_1 is a function from S to a group G_1, and f_2 is a function from S to a group G_2, define a morphism from f_1 to f_2 to be any homomorphism $\phi : G_1 \to G_2$ such that $\phi \circ f_1 = f_2$. It is straightforward to check that this is indeed a category.

If $\mathcal{C}$ is a category, then an object A of $\mathcal{C}$ is called *universally attracting* if for every object B of $\mathcal{C}$, there is a unique morphism from B to A (that is, $\mathrm{Mor}(B, A)$ is a singleton set). An object A of $\mathcal{C}$ is called *universally repelling* if for every object B of $\mathcal{C}$, there is a unique morphism from A to B (that is, $\mathrm{Mor}(A, B)$ is a singleton set). An object which is universally attracting or universally repelling is more generally called a *universal object*, and will be referred as such if the context makes it clear as to whether it is attracting or repelling. The following tells us that universal objects are unique up to isomorphism within a category.

Proposition 1.1. *Let $\mathcal{C}$ be a category, and let $A, B \in \mathrm{Ob}(\mathcal{C})$ be two universal objects of $\mathcal{C}$, either both attracting or both repelling. Then there exist unique isomorphisms $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, A)$.*

Proof. Since A and B are both universal objects, we know that there are unique morphisms $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, A)$. It also follows that id_A and id_B are the unique morphisms in $\mathrm{Mor}(A, A)$ and $\mathrm{Mor}(B, B)$, respectively. Since $f \circ g \in \mathrm{Mor}(B, B)$ and $g \circ f \in \mathrm{Mor}(A, A)$, we must have $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$, hence f and g are isomorphisms. $\square$

Exercise 1. Suppose that A is a universal object (either attracting or repelling) in the category $\mathcal{C}$. Let $B \in \mathrm{Ob}(\mathcal{C})$ such that there is an isomorphism $f \in \mathrm{Mor}(A, B)$. Prove that B must also be a universal object (the same type as A).

Example 5. Let S be a set, and consider the category $\mathcal{C}$ described in Example 4, where objects are pairs (f, G), where G is a group and $f : S \to G$ is a function. Let $F(S)$ denote the free group on the set S, which is constructed in every graduate algebra text. Let $f : S \to F(S)$ be the function which maps $s \in S$ to the equivalence class of words $[s] \in F(S)$. Then $(f, F(S))$ is a universally repelling object in $\mathcal{C}$, in that given any $(h, G) \in \mathrm{Ob}(\mathcal{C})$, there is a unique homomorphism $\phi : F(S) \to G$ such that $\phi \circ f = h$.

As in the case of free groups, it is typical that a universal object is defined by its universal property in a category, but then must be specifically constructed in order to show that it exists.

2. Direct limits

Let $(I, \preceq)$ be a partially ordered set. Then $(I, \preceq)$ is a *directed set* if for any elements $\alpha, \beta \in I$, there exists an element $\gamma \in I$ such that $\alpha \preceq \gamma$ and $\beta \preceq \gamma$.

Now let $\mathcal{A}$ be a category, let $(I, \preceq)$ be a directed set, and let $\{A_i\}_{i\in I}$ be a set of objects of $\mathcal{A}$ indexed by I. A *directed family of morphisms* for $\{A_i\}_{i\in I}$ is a collection of morphisms $\{f_j^i\}_{i,j\in I, i\preceq j}$ such that $f_j^i \in \mathrm{Mor}(A_i, A_j)$, $f_i^i = \mathrm{id}_{A_i}$, and if $i \preceq j \preceq k$, then $f_k^j \circ f_j^i = f_k^i$.

Given $\{A_i\}_{i\in I}$ a directed family of morphisms in $\mathcal{A}$, now consider the following category $\mathcal{C}$. Let the objects of $\mathcal{C}$ consist of pairs $(A, (f^i)_{i\in I})$, where A is an object of $\mathcal{A}$, and $(f^i)_{i\in I}$ is a collection of morphisms $f^i : A_i \to A$ of $\mathcal{A}$ such that for every $j \in I$, $i \preceq j$, we have $f^i = f^j \circ f_j^i$. If $(A, (f^i)_{i\in I})$ and $(B, (h^i)_{i\in I})$ are objects of $\mathcal{C}$, then a morphism in $\mathcal{C}$ from the first to the second is a morphism $\phi : A \to B$ of $\mathcal{A}$ such that $h^i = \phi \circ f^i$ for every $i \in I$. The *direct limit* of $\{A_i\}_{i\in I}$ with respect to the morphisms $\{f_j^i\}_{i,j\in I, i\preceq j}$ is defined to be a universally repelling object in the category $\mathcal{C}$. If $(A, (f^i)_{i\in I})$ is the direct limit of $\{A_i\}_{i\in I}$, we write

$$A = \varinjlim_i A_i.$$

Note that this is a very slight abuse of notation, since the universal object A could be replaced by another object B if there is an isomorphism in $\mathrm{Mor}(A, B)$, by Exercise 1. But we usually think of objects in a category as the same in the case that there is an isomorphism between them, as is usual in all of the examples we have seen so far.

So, if $(A, (f^i)_{i\in I})$ is the direct limit of $\{A_i\}_{i\in I}$ with respect to a directed family of morphisms, and if $(B, (h^i)_{i\in I})$ is any other object in the category $\mathcal{C}$ described above, then there is a unique morphism $\phi : A \to B$ such that, for every $i \in I$, $h^i = \phi \circ f^i$.

Theorem 2.1. *For any ring R, direct limits exist in the category R-**Mod** of R-modules. In particular, direct limits exist in the category **Ab** of abelian groups.*

Proof. Let $(I, \preceq)$ be a directed set, and let $\{M_i\}_{i\in I}$ be a directed system of R-modules, with $\{f_j^i\}_{i\in I, i\preceq j}$ a corresponding directed family of R-homomorphisms. Define M to be the direct sum of the M_i,

$$M = \bigoplus_{i\in I} M_i.$$

Now let N be a submodule of M which is generated by elements x_{ij}, $i \preceq j$, which has component $x \in M_i$ in position i, and component $-f_j^i(x) \in M_j$ in position j, and 0 in all other positions, where we range over all $x \in M_i$, $i, j \in I$, $i \preceq j$. That is, if $\iota_i : M_i \to M$ is the natural injection map, then N is generated by all elements of the form $x_{ij} = \iota_i(x) - \iota_j(f_j^i(x))$, for $x \in M_i$, $i, j \in I$, $i \preceq j$.

Now let M/N be the quotient module, where $p : M \to M/N$ is the projection map, and for each $i \in I$, let $f^i : M_i \to M/N$ be defined by $f^i = p \circ \iota_i$. The claim is that $(M/N, (f^i)_{i\in I})$ is a direct limit. Given any object $(B, (h^i)_{i\in I})$, we must show that there is a unique R-module homomorphism $\phi : M/N \to B$ such that $\phi \circ f^i = h^i$ for every $i \in I$. Given $x \in M_i$, the only choice is that we must have $\phi(\iota_i(x) + N) = h^i(x)$. This is well defined, since $h^i(x) = h^j \circ f_j^i(x)$ by definition, and this extends by linearity to a homomorphism on all of M/N. Thus M/N is the desired direct limit. $\square$

Example 6. Let X be a topological space. By a *presheaf of abelian groups on X*, written $\mathcal{F}$, we mean the following. For every open set $U \subset X$, there is assigned to U an abelian group, written $\mathcal{F}(U)$. If V is another open subset of X such that $V \subset U$, there is a group homomorphism called the *restriction homomorphism*, $\rho^U_V : \mathcal{F}(U) \to \mathcal{F}(V)$, such that ρ^U_U is the identity, and if $W \subset V \subset U$ are open sets, then $\rho^V_W \circ \rho^U_V = \rho^U_W$. In addition, we assume that $\mathcal{F}(\varnothing)$ is the trivial group. One natural example of a presheaf is on $\mathbb{C}$, where if $U \subset \mathbb{C}$ is open, let $\mathcal{F}(U)$ be the set on analytic functions on U, which is an abelian group under addition. In this case, if $V \subset U$, then ρ^U_V is just restriction of domains.

If $\mathcal{F}$ is a presheaf on the topological space X, and $x \in X$, consider the collection $\mathcal{U}_x$ of open neighborhoods of x. Partially order $\mathcal{U}_x$ by reverse inclusion, so that $U \preceq V$ means $V \subset U$. This makes $\mathcal{U}_x$ a directed set, since if $U, V \in \mathcal{U}_x$, then $U \cap V \in \mathcal{U}_x$. By the definition of a presheaf, the collection $\{\rho^U_V \mid V \subset U\}$ of restriction homomorphisms form a directed family of morphisms for the family $\{\mathcal{F}(U)\}_{U \in \mathcal{U}_x}$ of abelian groups. We may then look at the direct limit

$$\varinjlim_{U} \mathcal{F}(U),$$

which is called the *stalk* at the point $x \in X$, and is denoted $\mathcal{F}_x$. We will encounter presheaves and sheaves later in the context of representation theory.

3. Inverse limits

Inverse limits (also called *projective* limits) are defined similarly to direct limits, except that arrows are reversed. Again let $(I, \preceq)$ be a directed set, $\mathcal{A}$ a category, and $\{A_i\}_{i \in I}$ a set of objects in $\mathcal{A}$ indexed by I. An *inverse family of morphisms* for $\{A_i\}_{i \in I}$ is a collection $\{f^j_i\}_{i,j \in I, i \preceq j}$ such that $f^j_i \in \mathrm{Mor}(A_j, A_i)$, $f^i_i = \mathrm{id}_{A_i}$, and if $k \preceq i \preceq j$, then $f^k_i \circ f^j_i = f^j_k$.

Now let $\{A_i\}_{i \in I}$ be a set of objects in $\mathcal{A}$, with $\{f^j_i\}$ an inverse family of morphisms. Define $\mathcal{C}$ to be the category with objects $(A, (f_i)_{i \in I})$, where $A \in \mathrm{Ob}(\mathcal{A})$, and for each i, $f_i : A \to A_i$ is a morphism such that $f_i = f^j_i \circ f_j$ for every $j \in I$ such that $i \preceq j$. The morphisms of $\mathcal{C}$ from $(B, (h_i)_{i \in I})$ to $(A, (f_i)_{i \in I})$ consist of morphisms $\phi : B \to A$ from $\mathcal{A}$ such that $h_i = f_i \circ \phi$ for every $i \in I$. A universally attracting object in the category $\mathcal{C}$ is called the *inverse limit* of $\{A_i\}_{i \in I}$ with respect to the inverse family of morphisms $\{f^j_i\}$. If $(A, (f_i)_{i \in I})$ is the direct limit, then we write

$$A = \varprojlim_{i} A_i.$$

So, if $(B, (h_i)_{i \in I})$ is any object in $\mathcal{C}$ and $(A, (f_i)_{i \in I})$ is the direct limit, then there is a unique morphism $\phi : B \to A$ such that $h_i = f_i \circ \phi$.

As is done for direct limits, the existence of inverse limits in categories is proven by construct the inverse limit.

Theorem 3.1. *Inverse limits exist in the categories* **TopGrp** *of topological groups (and so in* **Grp***),* **Rng** *of rings, and R-***Mod** *of modules over a given ring R.*

Proof. The construction of the inverse limit in each of these categories is the same, and so we just look at the category of topological groups. Let $\{G_i\}_{i \in I}$ be a collection of topological groups indexed by the directed set $i \in I$, and let $\{f^j_i\}_{i,j \in I, i \preceq j}$ be an inverse system of continuous homomorphisms. Now let G be the direct product of all of the G_i, so

$$G = \prod_{i \in I} G_i,$$

and let Γ consist of all elements of G of the form $(g_i)_{i\in I}$ such that whenever $i \preceq j$, we have $f_i^j(g_j) = g_i$. Let $f_i : \Gamma \to G_i$ be the natural projection map. The claim is that $(\Gamma, (f_i)_{i\in I})$ is the inverse limit.

It follows immediately that we have $f_i = f_j \circ f_i^j$ whenever $i \preceq j$. Given any other object $(B, (h_i)_{i\in I})$, we need to show that there is a unique continuous homomorphism $\phi : B \to \Gamma$ such that $f_i \circ \phi = h_i$ for every $i \in I$. If $x \in B$ and $\phi(x) = (g_j)_{j\in I}$, then we must have $g_j = h_j(x)$ for this to be possible. So, we need only check that this ϕ is a well-defined continuous homomorphism from B to Γ. If $i \preceq j$, then we have

$$f_i^j(g_j) = (f_i^j \circ h_j)(x) = h_i(x) = g_i,$$

so that $\phi(x) \in \Gamma$, and $\phi : B \to \Gamma$ is a well-defined map. It follows immediately that ϕ is a continuous homomorphism since each h_j is. $\square$

Example 7. Let p be any prime, and consider the rings $\mathbb{Z}/p^n\mathbb{Z}$ for each $n \geq 1$. When $n \leq m$, we have the natural projection map

$$f_n^m : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z},$$

which gives an inverse family of homomorphisms. We may then take the inverse limit, denoted $\mathbb{Z}_p$,

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z},$$

which is called the ring of *p-adic integers*. In particular, $\mathbb{Z}_p$ is an additive group which is the inverse limit of finite groups, and is thus an example of a *profinite group* which we discuss in the next section.

We could also partially order the positive integers by letting $n \preceq m$ when $n|m$. This gives rise to the inverse family of homomorphisms for the rings $\mathbb{Z}/n\mathbb{Z}$, where if $n|m$,

$$f_n^m : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

is the natural projection. In this case, the inverse limit is denoted $\hat{\mathbb{Z}}$,

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z},$$

and is called the *profinite completion of* $\mathbb{Z}$. In fact, we have an isomorphism of rings:

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

4. Profinite groups

A *profinite group* is the inverse limit of finite groups. Both $\hat{\mathbb{Z}}$ and $\mathbb{Z}_p$ are examples, as we saw above. The main purpose of this section is to give a characterization of profinite groups as a topological group.

Let $(I, \preceq)$ be a directed set, let $\{G_i\}_{i\in I}$ be a collection of finite groups indexed by I, and let $\{f_i^j\}_{i,j\in I, i\preceq j}$ be an inverse family of homomorphisms. Now let G be the inverse limit,

$$G = \varprojlim_i G_i.$$

Each G_i may be viewed as a topological group with the discrete topology, and the product $\prod_i G_i$ may be given the product topology. Now, as in Theorem 3.1, G may be constructed as a subgroup of the product $\prod_i G_i$, and so we may give G the subspace topology. This is called the *profinite topology.*

Lemma 4.1. *Let G be a profinite group with the profinite topology, as defined above. Then G is a compact Hausdorff topological group which is a closed subset of $\prod_i G_i$.*

Proof. Each G_i is Hausdorff, and so their product is Hausdorff. Since G is the subspace of a Hausdorff space, it is also Hausdorff. Since each G_i is also compact, then their product is also compact by Tychonoff's theorem. To conclude that G is compact, then, it is enough to show it is closed in $\prod_{k\in I} G_k$, where $(I, \preceq)$ is the indexing directed set.

Let $\{f_i^j\}_{i,j\in I, i\preceq j}$ be the inverse system of homomorphisms. Fix $i, j \in I$, $i \preceq j$, and fix $g_j \in G_j$. Consider the set

$$\{(x_k)_{k\in I} \in \prod_{k\in I} G_k \mid x_j = g_j, x_i \neq f_i^j(g_j)\}.$$

Since every subset of each G_k is open, then this set is open in $\prod_{k\in I} G_k$. Now we have

$$\bigcup_{g_j\in G_j} \{(x_k)_{k\in I} \in \prod_{k\in I} G_k \mid x_j = g_j, x_i \neq f_i^j(g_j)\} = \{(x_k)_{k\in I} \in \prod_{k\in I} G_k \mid x_i \neq f_i^j(x_j)\}$$

is open. Finally, we have that G as a subset of $\prod_{k\in I} G_k$ is exactly the complement of the open set

$$\bigcup_{i\in I} \bigcup_{j\in I, i\preceq j} \{(x_k)_{k\in I} \in \prod_{k\in I} G_k \mid x_i \neq f_i^j(x_j)\}.$$

Thus, G is closed in $\prod_{k\in I} G_k$. □

Let G be a compact group, and let $\mathcal{N}$ be the collection open normal subgroups of G, all of which have finite index. For each $N \in \mathcal{N}$, we know that G/N is a finite group, and we may $\mathcal{N}$ as a directed set by reverse inclusion, so that $M \preceq N$ is defined to mean $N \subset M$, where we have $M \preceq M \cap N$ and $N \preceq M \cap N$.

Now, whenever $M \preceq N$, we have the natural projection $p_M^N : G/N \to G/M$, where $p_M^N(gN) = gM$. It immediately follows that if $L \preceq M \preceq N$, then $p_L^M \circ p_M^N = p_L^N$, giving us an inverse system of homomorphisms.

Lemma 4.2. *Let G be a compact group, and $\mathcal{N}$ the collection of open normal subgroups of G. Let $\tilde{G}$ be the profinite group*

$$\tilde{G} = \varprojlim_{N\in\mathcal{N}} G/N,$$

defined by the maps $p_M^N : G/N \to G/M$ when $N \subset M$. Then there exists a surjective continuous homomorphism $\alpha : G \to \tilde{G}$.

Proof. First, notice that since each $N \in \mathcal{N}$ is open, each G/N is discrete in the quotient topology, and is a finite group. By Theorem 3.1, the inverse limit exists, and we have a specific construction of it. For each $N \in \mathcal{N}$, let $p_N : \tilde{G} \to G/N$ be the projection map, as in the construction of the inverse limit in Theorem 3.1, so that $p_M^N \circ p_N = p_M$ for every $N, M \in \mathcal{N}$ with $N \subset M$. Now let $\alpha_N : G \to G/N$ be the natural projection map for each $N \in \mathcal{N}$, which is continuous. Also, whenever $N \subset M$, we have $p_M^N \circ \alpha_N = p_M$. By the definition of inverse limit, there is a unique continuous homomorphism $\alpha : G \to \tilde{G}$ such that $\alpha_N = p_N \circ \alpha$ for all $N \in \mathcal{N}$. We must show that α is surjective.

Since G is compact, $\alpha(G)$ is compact, and $\tilde{G}$ is Hausdorff by Lemma 4.1. Therefore $\alpha(G)$ is closed in $\tilde{G}$. So, it is enough to show that $\alpha(G)$ is dense in $\tilde{G}$ to conclude that α is surjective.

Let $U \subset \tilde{G}$ be an arbitrary open set, and we will show $U \cap \alpha(G)$ is nonempty. Every subset of each G/N, $N \in \mathcal{N}$, is open in G/N, and so by the construction of $\tilde{G}$ in Theorem 3.1, and the definition of product topology, the open sets of $\tilde{G}$ are generated by sets of the form $p_N^{-1}(S_N)$, for arbitrary subsets $S_N \subset G/N$. In other words, there are a finite number $N_1, \ldots, N_r \in \mathcal{N}$, and subsets $S_{N_j} \subset G/N_j$, $j = 1, \ldots, r$, such that

$$U = \{(x_N)_{N \in \mathcal{N}} \mid x_N \in G/N, x_N \in S_N \text{ if } N = N_j \text{ for some } j = 1, \ldots r\}.$$

Let $M = \cap_{j=1}^r N_j$. If $(x_N)_{N \in \mathcal{N}} \in U$, then since $M \subset N_j$ for each $j = 1, \ldots, r$, then $x_{N_j} = p_{N_j}^M(x_M)$. In other words, each coordinate x_{N_j} is determined by x_M, by the definition of an inverse system. Since $\alpha_M : G \to G/M$ is surjective, there is a $t \in G$ such that

$$\alpha_M(t) = (p_M \circ \alpha)(t) = \alpha(t)_M = x_M.$$

Now, for each $j = 1, \ldots, r$, we have

$$\alpha_{N_j}(t) = \alpha(t)_{N_j} = (p_{N_j} \circ \alpha)(t) = (p_{N_j}^M \circ p_M \circ \alpha)(t) = p_{N_j}^M(x_M) = x_{N_j}.$$

But now we have $\alpha(t)_{N_j} \in S_{N_j}$ for each $j = 1, \ldots, r$, so that $\alpha(t) \in U$. Now $\alpha(G) \cap U \neq \varnothing$, as claimed. $\square$

We will apply the following in the proof of the main result of this section.

Exercise 2. Let X be a compact space and Y a Hausdorff space, and suppose that $f : X \to Y$ is a continuous bijection. Prove that f is a homeomorphism by showing that f is an open map (consider the image of the complement of an open set).

Theorem 4.1. *Let G be a topological group. Then G is profinite if and only if G is compact and totally disconnected.*

Proof. ($\Rightarrow$): Assume that G is profinite, so let $(I, \preceq)$ be a directed set, $\{G_i\}_{i \in I}$ an inverse family of finite groups with some inverse family of homomorphisms, and let

$$G = \varprojlim_{i \in I} G_i,$$

with projection maps $f_i : G_i \to G$. From Lemma 4.1, we know that G is compact, and so we must show that G is totally disconnected, or $G^\circ = \{1\}$.

Since G is a compact Hausdorff space, then we know that G° is the intersection of all compact open neighborhoods of 1 in G (from the *Topological Groups* notes). If $\mathcal{U}$ is the collection of compact open neighborhoods of 1 in G, then we have

$$G^\circ = \bigcap_{U \in \mathcal{U}} U.$$

Now let $y = (y_i)_{i \in I} \in G$, with $y \neq 1$. That is, there is some index $j \in I$ such that y_j is not the identity in G_j, which we denote 1_j. Now let $V = f_j^{-1}(1_j)$. Since G_j is discrete and the projection maps are continuous homomorphisms, then V is a compact open neighborhood of 1 (since it is both closed and open) in G. (V is actually a compact open subgroup.) However, since $f_j(y) \neq 1_j$, then $y \in V$. Since y was arbitrary, we now have $G^\circ = \cap_{U \in \mathcal{U}} U = \{1\}$, and G is totally disconnected.

($\Leftarrow$): As in Lemma 4.2, let $\mathcal{N}$ be the collection of all open normal subgroups of G, and let G' be the inverse limit of the G/N, $N \in \mathcal{N}$, with respect to the natural projection maps $p^N_M : G/N \to G/M$, $N \subset M$. Then by Lemma 4.2, there is a surjective continuous homomorphism $\alpha : G \to \tilde{G}$. We will show that α is a homeomorphism of topological groups, showing that G is profinite. Since G is compact and $\tilde{G}$ is Hausdorff, then by Exercise 2 it is enough to show that α is injective.

Suppose that $g \in G$ and $g \in \ker(\alpha)$. Then $\alpha(g)_N$ is the identity in G/N for each $N \in \mathcal{N}$, which means we must have $g \in \cap_{N\in\mathcal{N}} N$. Since G is compact and totally disconnected, then every open neighborhood of 1 contains an open normal subgroup (from the *Topological Groups* notes). Since G is Hausdorff, then for each point $x \in G$, $x \neq 1$, there is an open neighborhood of 1 not containing x. This means that $\cap_{N\in\mathcal{N}} N = \{1\}$, and thus $\ker(\alpha)$ is trivial and α is injective. □

Example 8: Infinite Galois Theory. Let K/F be a separable and normal algebraic extension, or *Galois* extension. of fields, but not necessarily a finite extension. That is, the minimal polynomial over F of any element $a \in K$ has no repeated roots (separable), and every embedding of K into an algebraic closure $\overline{F}$ which fixes F pointwise is an automorphism of K (normal). Let $\mathrm{Gal}(K/F)$ be the group of automorphisms of K which fix F pointwise. It follows immediately that if K/F is Galois, and $F \subset L \subset K$, then K/L is Galois, and $\mathrm{Gal}(K/L)$ is a subgroup of $\mathrm{Gal}(K/F)$.

If S is a set of automorphisms of the field K, let K^S denote the set of points in K fixed by every automorphism in S, which is a subfield of K. Now let $\mathcal{N}$ be the collection of all normal subgroups of finite index in $G = \mathrm{Gal}(K/F)$. Then $\mathcal{N}$ is a directed set ordered by reverse inclusion, and if $N, M \in \mathcal{N}$ with $M \subset N$, then there is a natural projection map $p^M_N : G/M \to G/N$ giving an inverse system of homomorphisms. We also have the projections $p_N : G \to G/N$, which corresponds to restricting the action of elements in $\mathrm{Gal}(K/F)$ to acting on K^N, giving an element of $\mathrm{Gal}(K^N/F)$. Note that we have, when $M \subset N$, $p_N = p^M_N \circ p_M$, and we also have a projection from G to the inverse limit of all G/N,

$$p : G \to \varprojlim_{N\in\mathcal{N}} G/N.$$

In fact, we see now that p is an isomorphism, so that the infinite Galois group is actually a profinite group.

Proposition 4.1. *Let K/F be a Galois extension of fields, $G = \mathrm{Gal}(K/F)$, and $\mathcal{N}$ the collection of normal subgroups of finite index in G, with projection maps as above. Then the projection map*

$$p : G \to \varprojlim_{N\in\mathcal{N}} G/N$$

is an isomorphism of groups.

Proof. We first show that p is injective. If $\sigma \in G$, we have $p(\sigma)$ is the identity in the inverse limit if and only if $p(\sigma)_N$ is the identity in G/N for each $N \in \mathcal{N}$. That is, we have

$$\ker(p) = \bigcap_{N\in\mathcal{N}} N.$$

Let $\sigma \in \ker(p)$. For an arbitrary $\alpha \in K$, we may adjoin to F the roots of the minimal polynomial of α over F to obtain a finite Galois extension $\tilde{F}$ of F, where $F \subset \tilde{F} \subset K$.

Now consider the map

$$\mathrm{res}_{\tilde{F}} : G \to \mathrm{Gal}(\tilde{F}/F),$$

which restricts the action of an element in $G = \mathrm{Gal}(K/F)$ to acting on $\tilde{F}$. Then $\mathrm{res}_{\tilde{F}}$ is a group homomorphism with kernel equal to $\mathrm{Gal}(K/\tilde{F})$. So now $\mathrm{Gal}(K/\tilde{F})$ is a normal subgroup of G which is necessarily of finite index, since $\tilde{F}/F$ is a finite extension. But since $\sigma \in \ker(p)$, then $\sigma \in \mathrm{Gal}(K/\tilde{F})$, and in particular, $\sigma(\alpha) = \alpha$. Since α was arbitrary, then we must have that σ is the trivial automorphism, and so p is injective.

To prove that p is surjective, let $(\sigma_N)_{N\in\mathcal{N}}$ be an arbitrary element of the inverse limit of the G/N. If $\alpha \in K$, then as above we find a finite Galois extension $\tilde{F}$ of F containing α, and $\tilde{N} = \mathrm{Gal}(K/\tilde{F})$ is a normal subgroup of finite index in G, and every element of $G/\tilde{N}$ may be viewed as an element of $\mathrm{Gal}(\tilde{F}/F)$. Now define σ on α by $\sigma(\alpha) = \sigma_{\tilde{N}}(\alpha)$. The claim is that this defines an element of G. If E is any other finite Galois extension of F containing α, then $L = E\tilde{F}$ is another, which contains E and $\tilde{F}$. Letting $\mathrm{Gal}(K/E) = M$, $\mathrm{Gal}(K/L) = H$, we have $H \subset M, \tilde{N}$. By the construction of the inverse limit, we have $p^H_{\tilde{N}}(\sigma_H) = \sigma_{\tilde{N}}$ and $p^H_M(\sigma_H) = \sigma_M$, while these projection maps do not change the action on α, as they amount to being restriction maps on Galois elements. Thus, σ is a well-defined automorphism on all of K. Since the projection map p_N is also a restriction map of Galois elements, then we have $\sigma_N = p_N(\sigma)$ for each $N \in \mathcal{N}$, and thus $p(\sigma) = (\sigma_N)_{N\in\mathcal{N}}$. □

So, Galois groups of infinite Galois extensions may be given the profinite topology, and viewed as compact totally disconnected groups. One may formulate the Fundamental Theorem of Galois Theory for infinite extensions, where intermediate fields correspond to closed subgroups, and intermediate fields which are Galois over the ground field correspond to closed normal subgroups. A concise discussion of this is given in [RV, Theorem 1-20].

References

[L] S. Lang, Algebra. Revised third edition. Graduate Texts in Mathematics, 211. *Springer-Verlag, New York*, 2002.

[RV] D. Ramakrishnan and R.J. Valenza, Fourier Analysis on Number Fields. Graduate Texts in Mathematics, 186. *Springer-Verlag, New York*, 1999.