THE ABSOLUTE GALOIS GROUP AS A PROFINITE GROUP

RYAN BURKHART

Abstract. In this paper we will discuss the absolute Galois group, the Galois group of $\overline{\mathbb{Q}}$ where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. We will begin with a discussion of Galois groups and Galois theory and why they are important. Then we will form a better understanding of what a profinite group looks like by examining the p-adic integers $\hat{\mathbb{Z}}_p$. In particular we will prove several properties for profinite groups as a whole so that we can then apply those properties to the absolute Galois group. Finally we will apply the structure and topology we learned for profinite groups to form the absolute Galois group, while discussing the differences from the p-adic integers and the complications that arise. Included in this discussion will be a somewhat unorthodox proof of the uncountability of the absolute Galois group involving compactness and some basic Galois theory applied to the splitting fields of $x^2 - p$ for all primes p.

Contents

Date: May 2, 2016.

1. Introduction: Definitions and Relevance

Let us give a quick overview of what the Galois group is. We will not prove the following statements and will instead take the following as given. The proofs can be found in the annotated sources.

1.1. Basic Definitions.

Let K/F be a finite extension of fields. That is, let K and F be fields where $F \subseteq K$ and the degree of K over F is finite. Then we define $Aut(K/F)$ as the set of automorphisms of K which fix F. In this case, $Aut(K/F)$ is a group under composition.

Definition 1. K is said to be Galois over F if $|Aut(K/F)| = [K : F]$, that is if the number of automorphisms of K which fix F is the same as the degree of K over F.

While this condition may at first seem difficult to characterize, it turns out that this is equivalent to saying that K is a splitting field over F for some separable polynomial $f(x) \in F[x]$. That is, if K is Galois over F then if K contains one root of an irreducible polynomial $f(x)$ with coefficients in F, then $f(x)$ must split completely into linear factors, in other words all roots of $f(x)$ are in K. [1, p. 562] (Note that in a perfect field every irreducible polynomial is separable and every separable polynomial is a product of irreducible polynomials. So for a perfect field, like $\mathbb{Q}$, we can consider irreducible polynomials in the place of separable ones.) With this in mind, if K is a splitting field of F then we refer to $Aut(K/F)$ as the Galois group of K/F. In this paper we will be focusing on extensions of the form $K/\mathbb{Q}$, eventually culminating in $\overline{\mathbb{Q}}/\mathbb{Q}$, the extension of $\mathbb{Q}$ to include all algebraic roots. This theory is used to solve many problems in group theory. For example, determining whether a polynomial is solvable in radicals relies on Galois Theory. This theory also helps in determining the constructibility of angles. It is also interesting to note that since the absolute Galois group deals with automorphisms of the algebraic closure of $\mathbb{Q}$, by looking at restrictions of these elements we can find information pertaining to almost any topic in algebra and number theory.

2. The p-adic Integers

Now that we have a basic idea of our goal, we will discuss a simple example to prepare us for the more complex structure of $\overline{\mathbb{Q}}$.

2.1. Construction of $\hat{\mathbb{Z}}_p$.

Let p be a prime in $\mathbb{Z}$. In order to construct elements of $\hat{\mathbb{Z}}_p$ we first choose an element $x \in \mathbb{Z}/p^n\mathbb{Z}$ for some $n \in \mathbb{N}$. Then by letting x be mapped to its value modulo p^m for any $m < n$ we obtain a natural mapping and homomorphism from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^m\mathbb{Z}$. Using this, we will define our concept of an inverse limit as well as of $\hat{\mathbb{Z}}_p$. In particular our elements of $\hat{\mathbb{Z}}_p$ are written as $(x_1, x_2, x_3, ...)$ where all x_n are elements of $\mathbb{Z}/p^n\mathbb{Z}$ and for all $n > m$ x_n is congruent to x_m modulo p^m. More generally, we define an inverse limit as follows.

Definition 2. Let $\{G_n : n \in \mathbb{N}\}$ be a collection of groups, and suppose that for every $n > m$ there is a homomorphism $\phi_{n,m} : G_n \to G_m$. Then we define the inverse limit

$$\hat{G} = \varprojlim_n G_n = \{(x_1, x_2, x_3, ...)\ : x_n \in G_n \text{ and for all } n > m, x_m = \phi_{n,m}(x_n)\}$$

That is, the inverse limit is the set of infinite dimensional vectors such that given the n^{th} element we can determine x_1 through x_{n-1} by applying the appropriate homomorphisms to our n^{th} element. It is significant to note that this inverse limit depends on both the collection of groups and the homomorphisms $\phi_{n,m}$ used.

Claim 1. *$\hat{G} = \varprojlim_n G_n$ is a group under the operation $x + y = (x_1 +_1 y_1, x_2 +_2 y_2, ..., x_n +_n y_n)$ where $+_k$ is the operation in G_k for any groups G_n and any homomorphisms ϕ_{nm}.*

Proof. For our 0 element, we take $(0_1, 0_2, ..., 0_n)$, where 0_k is the additive identity in G_k. Then $x + 0 = (x_1 +_1 0_1, ..., x_n +_n 0_n) = x$ for any $x \in \hat{G}$. But is $0 \in \hat{G}$? Since ϕ_{nm} are homomorphisms, we know that $\phi_{nm}(0_n) = (0_m)$ for any $n > m$. So $\hat{G}$ has an additive identity.

Given an $x \in \hat{G}$, note that $-x = (-x_1, ..., -x_n)$ satisfies $x + (-x) = 0$. But is $-x \in \hat{G}$? Since ϕ_{nm} are homomorphisms, we know that $\phi_{nm}(-x_n) = -\phi_{nm}(x_n) = -x_m$ for any $n > m$. So each element $x \in \hat{G}$ has an additive inverse, $-x \in \hat{G}$.

Finally, let $x, y \in \hat{G}$. Then $x + y = (x_1 +_1 y_1, ..., x_n +_n y_n)$. Is this new vector in $\hat{G}$? Since the ϕ_{nm} are homomorphisms, we know that $\phi_{nm}(x_n +_n y_n) = \phi_{nm}(x_n) +_m \phi_{nm}(y_n) = x_m +_m y_m$ for any $n > m$. So indeed, $x + y \in \hat{G}$ for any $x, y \in \hat{G}$.

So, thanks to our downward mappings being homomorphisms, $\hat{G}$ is always a group.

□

Going back to our example of $\hat{\mathbb{Z}}_p$, we see that we can define $\hat{\mathbb{Z}}_p$ as an inverse limit,

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

where for $n > m$ our $\phi_{n,m}$ is the natural projection from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^m\mathbb{Z}$.

This completes our construction of $\hat{\mathbb{Z}}_p$, our example profinite group, where profinite refers to the fact that each of the groups used in the inverse limit are finite. Now that we have defined this group, we will look more closely at some of its properties and structure.

2.2. **Uncountability.**

The first result we want to prove about $\hat{\mathbb{Z}}_p$ is that it has uncountably many elements.

Proof. Assume for the sake of contradiction that $\hat{\mathbb{Z}}_p$ is countable. Then we can list the elements in the form

$$\begin{gathered} x_1 = (x_{11}, x_{12}, x_{13}, ...) \\ x_2 = (x_{21}, x_{22}, x_{23}, ...) \\ x_3 = (x_{31}, x_{32}, x_{33}, ...) \\ ... \end{gathered}$$

Now let $y = (y_1, y_2, y_3, ...)$ where $y_1 \neq x_{11}$, and we then define the other elements inductively. In particular, if $y_{n-1} \not\equiv x_{nn} \bmod p^{n-1}$ then we let $y_n = y_{n-1}$, and if $y_{n-1} \equiv x_{nn} \bmod p^{n-1}$ then we let $y_n = x_{nn} + p^{n-1}$.

In this construction, $y_n \neq x_{nn}$ for any n as y_n is either defined as not equivalent to x_{nn} mod p^{n-1} and thus not equivalent mod p^n, or it is defined as $x_{nn} + p^{n-1}$, which also can not be equivalent to x_{nn} mod p^n. Thus $y \neq x_n$ for any n.

Yet, each y_n is defined such that either $y_n = y_{n-1}$ and thus clearly has the same modulus, or $y_n = x_{nn} + p^{n-1}$ and so $y_n \equiv x_{nn} \equiv y_{n-1} \bmod p^{n-1}$. Thus $y \in \hat{\mathbb{Z}}_p$ and yet is not equal to any of our listed elements. Thus we have our contradiction, and we have our result.

□

The next thing we need to discuss about $\hat{\mathbb{Z}}_p$ is its topology. Like most sets, there are multiple topologies that we could define for $\hat{\mathbb{Z}}_p$, so how do we choose which one to use? Well we want to be able to nicely define restrictions onto $\mathbb{Z}/p^n\mathbb{Z}$, that is we want the mappings $\phi_n : \hat{\mathbb{Z}}_p \to \mathbb{Z}/p^n\mathbb{Z}$ defined by $(x_1, x_2, x_3, ...) \to x_n$ to be as nice as possible. In particular, we want them to be continuous. As this is the only condition we are really concerned with, we will want our topology to be the simplest one which satisfies this property. In other words we will choose the smallest topology, the topology with the fewest open sets, which satisfies this property.

2.3. **Basic Definitions in Topology.**

Before we jump in to the topology of $\hat{\mathbb{Z}}_p$ let us state some basic definitions from elementary topology.

Definition 3. A metric space is a set X along with a mapping $d : X \times X \to \mathbb{R}$ such that d satisfies the following properties for all $x, y, z \in X$:

(1) $d(x, y) \geq 0$
(2) $d(x, y) = 0 \iff x = y$
(3) $d(x, y) = d(y, x)$
(4) $d(x, z) \leq d(x, y) + d(x, z)$

So given a metric space as defined above we can then define a topology on that metric space, that is we can define a set of subsets of our metric space that qualify as open sets. Any topology τ over a metric space X must satisfy the following:

Definition 4. A set τ of subsets of a metric space X is a topology of X if

(1) $\emptyset, X \in \tau$
(2) For any $A \subseteq \tau$, $\bigcup\limits_{U \in A} U \in \tau$
(3) For every $n \in \mathbb{N}$, if $U_1, ..., U_n \in \tau$, then $U_1 \cap ... \cap U_n \in \tau$

So then τ is our set of open subsets. We then define C as closed if C^c, that is the subset of X containing all elements not in C, is open.

One very important topology that is used on many metric spaces is the so called metric topology, a topology which is defined entirely by what metric is used on the space.

Definition 5. Let X be a metric space with metric d, then we refer to τ as the metric topology on X if $A \in \tau$ implies that for all $x \in A$ there must be a $\delta > 0$ such that $\{y \in X : d(x, y) < \delta\} \subseteq A$.

We refer to the set of points within δ of x used above as the open ball of radius δ around x, or $B(x, \delta)$.

Now that our definition of a topology is in place, since our topology in $\hat{\mathbb{Z}}_p$ is defined based on whether certain mappings are continuous, we probably should define what it means for a mapping from one metric space to another to be continuous.

Definition 6. Let X be a metric space with metric d_x and Y be a metric space with metric d_y. Then a mapping $\phi : X \to Y$ is continuous if for every $\epsilon > 0$ there exists a $\delta > 0$ such that $d_x(x, y) < \delta \Rightarrow d_y(\phi(x), \phi(y)) < \epsilon$.

With these definitions in place we are ready to look at our specific example of the topology of $\hat{\mathbb{Z}}_p$.

2.4. **The Topology of $\hat{\mathbb{Z}}_p$.**

We want to define our topology based on the topology of $\mathbb{Z}/p^n\mathbb{Z}$ so let us first discuss that. We want to give $\mathbb{Z}/p^n\mathbb{Z}$ a fairly basic topology so that we can focus on $\hat{\mathbb{Z}}_p$. We want our topology to be a metric topology for some metric as this gives us the most power in proofs, but what metric should we use? Two common metrics to try are the standard metric or the discrete metric. The standard metric is defined as $d(x, y) = |x - y|$. However, in $\mathbb{Z}/p^n\mathbb{Z}$ this function need not be well defined, so this metric won't work. So instead, we will use the discrete metric, defined as $d(x, y) = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{if } x \neq y \end{cases}$. Using this metric it is easy to see that by using $\delta = 1/2$ in Definition 5, each point by itself qualifies as an open set. But then since arbitrary unions of these individual points must also be open, we get that every subset of $\mathbb{Z}/p^n\mathbb{Z}$ is open. This topology where every subset is open is referred to as the discrete topology.

Now that we have our topology on $\mathbb{Z}/p^n\mathbb{Z}$ we would like to use this and the fact that we want our projection maps ϕ_n to be continuous to define our topology on $\hat{\mathbb{Z}}_p$. The problem is we do not have a metric defined on $\hat{\mathbb{Z}}_p$, so we need some way of characterizing continuous maps based on our topology on $\mathbb{Z}/p^n\mathbb{Z}$. To do this we need a definition that will match our previous definition in the case that our topology is the metric topology. Thus we have the next theorem.

Theorem 1. *Let X and Y be metric spaces. Then $\phi : X \to Y$ is a continuous mapping $\iff$ for all open $A \in Y$, $\phi^{-1}(A)$ is open in X.* [2, p. 232]

So according to this theorem, in order for our ϕ_n to be continuous every open set of $\mathbb{Z}/p^n\mathbb{Z}$ must be mapped to by an open set in $\hat{\mathbb{Z}}_p$, but as we have already shown every point of $\mathbb{Z}/p^n\mathbb{Z}$ is an open set by itself. Given an $x \in \mathbb{Z}/p^n\mathbb{Z}$, $\phi_n^{-1}(x) = \{(x_1, x_2, ...) \in \hat{\mathbb{Z}}_p : x_n = x\}$. Thus since $\{x\}$ is an open set, by Theorem 2 $\{(x_1, x_2, ...) \in \hat{\mathbb{Z}}_p : x_n = x\}$ must be open. Since we need this to be true for all $n \in \mathbb{N}$ we have some elements for our topology.

Let $A \subseteq \hat{\mathbb{Z}}_p$ such that $A = \{(x_1, x_2, ...) : x_n = x \text{ for some } x \in \mathbb{Z}/p^n\mathbb{Z}\}$. Then from the above A is open. Note that here A could be empty, so this requirement is met, but the entire set $\hat{\mathbb{Z}}_p$ is not yet included. By definition, we need arbitrary unions of such sets to also be open. So then we now have that a set A must be open if for any $(x_1, x_2, ...) \in A$ there is an $n \in \mathbb{N}$ such that $\{(y_1, y_2, ...) \in \hat{\mathbb{Z}}_p : y_n = x_n\} \subseteq A$. So this definition of an open set takes care of arbitrary unions, the empty set, and now $\hat{\mathbb{Z}}_p$ is trivially open as well since these open sets are defined by whether or not they contain subsets of $\hat{\mathbb{Z}}_p$. The last thing we need to check is finite intersections.

Let A and B be open sets as above. If $A \cap B$ is empty then the intersection is open and we are done. Otherwise let $(x_1, x_2, ...) \in A \cap B$. Then there must be $n, m \in \mathbb{N}$ such that $\{(y_1, y_2...) \in \hat{\mathbb{Z}}_p : y_n = x_n\} \in A$ and similarly for B and m. Assume without loss of generality that $n \geq m$. Then by definition of $\hat{\mathbb{Z}}_p$, $x_n \equiv x_m \bmod p^m$ and thus we have that $\{y \in \hat{\mathbb{Z}}_p : y_n = x_n\} \subseteq \{y \in \hat{\mathbb{Z}}_p : y_m = x_m\} \subseteq B$. Thus $\{y \in \hat{\mathbb{Z}}_p : y_n = x_n\} \subseteq A$ and B and thus is a subset of $A \cap B$.Thus by our current definition $A \cap B$ is open. We have now shown that for any open sets A and B, $A \cap B$ is open. It is a trivial matter to use induction to extend this to any finite intersection. And with that all of our criterion for open sets is met and since all the open sets defined were required, we have our simplest topology.

Definition 7. Let $A \subseteq \hat{\mathbb{Z}}_p$. Then A is open if and only if for all $x = (x_1, x_2, ...) \in A$ there is an $n \in \mathbb{N}$ such that $\{y \in \hat{\mathbb{Z}}_p : y_n = x_n\} \in A$.

Note that every open set A can then be described as the union of some $\phi_n^{-1}(x_n)$ for some amount of $x_n \in \mathbb{Z}/p^n\mathbb{Z}$.

Given this definition, let $A = \phi_n^{-1}(x_n)$ for some $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ for some $n \in \mathbb{N}$. Then A is open by definition, but also if we look at A^c we see that it it can be written as the union of the $\phi_n^{-1}(y_n)$ for all $y_n \neq x_n$ in $\mathbb{Z}/p^n\mathbb{Z}$, and thus A^c is also open. So then, A is both closed and open. The question then is, does this apply to all open sets in $\hat{\mathbb{Z}}_p$? The answer as it turns out is yes, and we will prove this later on.

It is easy to see from this definition that ϕ_n^{-1} of any subset U of $\mathbb{Z}/p^n\mathbb{Z}$ is going to be open for any n, as it would be a set containing all elements where x_n was equal to some element of U. Thus by Theorem 1, all of the ϕ_n are continuous, our desired result.

2.5. Total Disconnectedness of $\hat{\mathbb{Z}}_p$.

Once again we will make a couple of basic definitions to be sure that we understand what we are looking for.

Definition 8. Let $A \subseteq X$ where X is a topological space. Then we say A is disconnected if there exist open sets U,$V \subseteq X$, $U \cap A \neq \emptyset$, $V \cap A \neq \emptyset$, where $U \cap V \cap A = \emptyset$ and $A = (A \cap U) \cup (A \cap V) = A \cap (U \cup V)$.

Also, as expected we define a set as being connected if it is not disconnected. At first glance it may not be obvious how to interpret this statement. Speaking informally, if a set is connected it means that in the sense defined by the topology of the set, it is possible to travel from one point to any other point without leaving the set. In a disconnected set then there must be some sense of seperation between parts of the set, that is there need to be points in the set that no matter what path you take are separated by something outside the set. So this brings us to an interesting case: what would happen if every point had this sense of separation with every other point in the set? With this idea we have our next definition.

Definition 9. Let X be a topological space. Then we say that X is totally disconnected if the only connected subsets of X are individual points.

Notice that in terms of connectedness, this is the worst possible scenario, as a subset with only one element must always be connected in any topology. This is fairly easy to see from the conditions $U \cap A \neq \emptyset$, $V \cap A \neq \emptyset$, and $U \cap V \cap A = \emptyset$. Clearly no U and V could satisfy these conditions if A only has one element.

Now that our definitions are in place, let us look at $\hat{\mathbb{Z}}_p$.

Claim 2. *$\hat{\mathbb{Z}}_p$ is totally disconnected*

Proof. Let $A \subseteq \hat{\mathbb{Z}}_p$ such that there are $x, y \in A$ such that $x \neq y$ and let $x = (x_1, x_2, ...)$ and $y = (y_1, y_2, ...)$. Then there must be an $n \in \mathbb{N}$ such that $x_n \neq y_n$. So let $U_k = \{(z_1, z_2, ...) \in \hat{\mathbb{Z}}_p : z_n = k\}$ for all $k \in \mathbb{Z}/p^n\mathbb{Z}$. Note that in our topology on $\hat{\mathbb{Z}}_p$, U_k is open for all k. So let $U = U_{x_n}$ and let $V = \bigcup_{k \in \mathbb{Z}/p^n\mathbb{Z}, k \neq x_n} U_k$. Then since unions of open sets are open both V and U are open. In U every element has x_n as its nth component whereas in V the nth component of every element is something other than x_n so $U \cap V = \emptyset$. This also gives us that $x \in U$ and $y \in V$ so $U \cap A \neq \emptyset$ and $V \cap A \neq \emptyset$. Finally, $U \cup V = \hat{\mathbb{Z}}_p$ since it would contain every element with nth component x_n and every element with nth component not equal to x_n. So $A \cap (U \cup V) = A \cap \hat{\mathbb{Z}}_p = A$. Thus for any set A containing two distinct elements we can find two open sets such that all of the properties in definition 9 are satisfied. So every subset of $\hat{\mathbb{Z}}_p$ containing two or more elements is disconnected. Thus the only connected subsets are individual points, and so $\hat{\mathbb{Z}}_p$ is totally disconnected.

□

2.6. **Compactness of $\hat{\mathbb{Z}}_p$.** To wrap up our discussion of $\hat{\mathbb{Z}}_p$ we will look at one more basic property of our example group. We want to define some sense of how dense a set is, so we introduce the following definition.

Definition 10. Given a set X with a topology τ, we say $K \subset X$ is compact if for any collection of open sets $\{U_\lambda\}_{\lambda \in I}$ such that $K \subset \bigcup_{\lambda \in I} U_\lambda$ there exists a finite subset such that $K \subset \bigcup_{j=1}^{k} U_{\lambda_j}$.

In other words, a set is compact if every arbitrary union of open sets can be expressed as a finite union of sets in the original union.

Claim 3. *$\hat{\mathbb{Z}}_p$ is Compact*

Proof. We know that $\hat{\mathbb{Z}}_p \subset \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$, that is that each element of $\hat{\mathbb{Z}}_p$ is of the form $(x_1, x_2, ...,)$ with $x_n \in \mathbb{Z}/p^n\mathbb{Z}$. We still want our restriction functions ϕ_n to be continuous in the larger group, so we get that $\phi_n^{-1}(x_n)$ is still open in the big group. More particularly, we still have that the complement of these sets are finite unions of similar sets, that is finite unions of open sets. So then, sets of this form are closed and open. Now, note that these inverses are now defined in the larger group. In particular, the restriction that further elements restrict to lower elements isn't there. So let this larger inverse be denoted Φ_n^{-1}. Then in order to get $\phi_n^{-1}(x_n)$ we need only the elements of $\Phi_n^{-1}(x_n)$ that are also in $\Phi_m^{-1}(x_m)$ for all $m < n$ and also for $m > n$ we need only those that are in $\Phi_m^{-1}(y_m)$ for any y_m that restricts to x_n.

So then, we have $\phi_n^{-1}(x_n) = \bigcap_{m=1}^{n-1} \Phi_m^{-1}(x_m) \cap \bigcap_{m>n} \bigcup\{\Phi_m^{-1}(y_m) : x_n = y_m \bmod n \text{ and } y_k = y_m \bmod k \text{ for all } k < m\}$. Note that the unions at the end are always finite, and thus since they are unions of closed sets those sets are closed (by the fact that a finite intersection of open sets is open). Therefore we have that $\phi_n^{-1}(x_n)$ is an arbitrary intersection of closed sets, and thus is closed (by the fact that an arbitrary union of open sets is open).

So, since $\hat{\mathbb{Z}}_p$ can be written as a finite union of these ϕ_n^{-1} we get that $\hat{\mathbb{Z}}_p$ is closed in our larger group. But our larger group is a product of finite groups, and finite groups must be compact (since the full group can be written as the union of finitely many disjoint sets, namely the sets containing single elements of the group). We now site Tychonoff's theorem [3, p. 4], which states that any arbitrary direct product of compact sets is itself compact. So then we have that $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ is compact. But since $\hat{\mathbb{Z}}_p$ is a closed subset of this set, the basic rules of compactness in topology tell us that $\hat{\mathbb{Z}}_p$ is also compact. (In particular if a closed set were not compact then there would be an arbitrary union of open sets U such that $\hat{\mathbb{Z}}_p \subset U$ but there would be no finite subset. So then $U \cup \hat{\mathbb{Z}}_p^c$ would be an arbitrary union of open sets covering the full group, but without a finite subcover. Thus the larger group would not be compact, a contradiction). So $\hat{\mathbb{Z}}_p$ is compact.

□

Now that we have that $\hat{\mathbb{Z}}_p$ is compact we can prove the claim we made earlier that every open set in $\hat{\mathbb{Z}}_p$ is also closed. In particular, any open set can be written as some arbitrary union of sets of the form $\phi_n^{-1}(x_n)$, that is of closed and open sets. But then since $\hat{\mathbb{Z}}_p$ is compact any open set can then be written as some finite union of these closed and open sets. So then, if we take the complement, the logical complement of the union of finitely many closed sets is a finite intersection of open sets. This is then open, and so the complement of our original set is open. Thus sets in $\hat{\mathbb{Z}}_p$ are either both closed and open or neither.

This concludes our discussion of $\hat{\mathbb{Z}}_p$. As our example profinite group, this gives us a feeling for how inverse limits work as well as some intuition about the shape of profinite groups. In particular we have an uncountable group that is compact yet totally disconnected. Intuitively, this means the group is dense, and yet with some space always between its elements, an interesting structure. We will now move on to our main discussion, remembering and adjusting the ideas from this section.

3. **The Absolute Galois Group over $\mathbb{Q}$**

We begin with the definition of what we mean by an absolute Galois group.

Definition 11. Let F be a perfect field and let $\overline{F}$ denote the algebraic closure of F, that is the minimal extension of F in which every polynomial splits completely into linear factors. Then let $Aut(\overline{F}/F)$ be the set of automorphisms of $\overline{F}$ which fix F. Then we refer to $Aut(\overline{F}/F)$ as the absolute Galois group over F.

(Note: The standard definition of the absolute Galois group uses F^{sep}, the algebraic closure of separable polynomials, instead of $\overline{F}$, but if F is perfect these are equivalent.[1, p. 551])

To begin examining the absolute Galois group, we are going to need to have a good understanding of what makes an extension Galois. In section 1 we noted that an extension K is Galois over a perfect field F if and only if K is a splitting field over F. Without going into the full proof of the biconditional statement, the next theorem is important in understanding why this is the case.

Theorem 2. *Let K be Galois over a field F, and let $\phi \in Aut(K/F)$, that is let ϕ be an automorphism of K which fixes F. Then if α is the root of some polynomial $f(x) \in F[x]$, $\phi(\alpha)$ is also a root of f.*

This theorem is easily proven by seeing that $\phi(0) = \phi(f(\alpha)) = f(\phi(\alpha)) = 0$. All of these equalities are direct consequences of ϕ being a field isomorphism.

This gives us a good idea of why an extension is only Galois if it is a splitting field. If there were an irreducible polynomial $f(x)$ such that $\alpha \in K$ was a root but $\beta \notin K$ was also a root then the degree of K over F, which is directly related to the degree of f would be greater than the number of automorphisms in $Aut(K/F)$. That is, this theorem directly relates the number of roots in K to the number of automorphisms in $Aut(K/F)$.

Now that we have established this theorem, we can start looking at homomorphisms between Galois groups. To start, lets make sure we are right in referring to $Aut(K/F)$ as a group. We know $Aut(K)$ is always a group for any field K, but is the property of fixing F preserved? Let ϕ_1 and ϕ_2 be in $Aut(K/F)$. Then it is fairly easy to see that since ϕ_1 and ϕ_2 fix F then the composition $\phi_1(\phi_2(x)) = x$ for all $x \in F$. So indeed $Aut(K/F)$ is a group.

We are wanting to look at the absolute Galois group over $\mathbb{Q}$ as a profinite group. Before we start constructing this, we need an understanding of what the end result will look like. We want an inverse limit whose result fully describes automorphisms on $\overline{\mathbb{Q}}$ which fix $\mathbb{Q}$. That is, the inverse limit needs to describe where the algebraic roots in $\overline{\mathbb{Q}}$ which are not in $\mathbb{Q}$ are sent. But by theorem 2 we know that any root of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ must be sent to another root of that polynomial. In other words, if K is the splitting field for $f(x)$ over $\mathbb{Q}$ then where the roots of $f(x)$ are sent is entirely described by an automorphism in $Aut(K/\mathbb{Q})$. So then, if we can decide on an element of $Aut(K/\mathbb{Q})$ to use for every algebraic extension K, then we have described an element of the absolute Galois group.
Also note that any irreducible polynomial must have some degree, $n \in \mathbb{N}$ and that the most roots this polynomial could have is n. So then, since each root must be sent to another root of the same polynomial, there are at most n choices for where an automorphism sends a root. But since these automorphisms are isomorphisms each root can only be mapped to by one root, thus we see that $Aut(K/\mathbb{Q})$ has at most $n!$ elements and thus is always finite. So then, we have our candidates for the finite groups to be used in our inverse limit.

We now run into a slight problem with our previous definition of an inverse limit. Previously, for simplicity, we defined inverse limits on an ordered and countable collection of groups. We will need to adjust our definition to account for partially ordered sets. The natural ordering for sets is the subset, that is $J < K$ if $J \subsetneq K$. However this is only a partial ordering, as there could be sets J and K such that none of the statements $J \subset K$, $J = K$, or $K \subset J$ are true. So we account for this in our new definition. Note that we also make our definition include sets of arbitrary size, although this isn't necessary for our needs.

Definition 12. Let $\{G_i : i \in I\}$ be a collection of groups, where I is a partially ordered set and suppose for every $n > m$, $n, m \in I$, there is a homomorphism $\phi_{n,m} : G_n \to G_m$. Then we define the inverse limit

$$\hat{G} = \varprojlim_i G_i = \{(x_i)_{i \in I} : x_i \in G_i \text{ and if } n > m \text{ then } x_m = \phi_{n,m}(x_n)\}$$

Note that this matches our old definition if $I = (\mathbb{N}, >)$.

3.1. **Construction of** $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$**.**

With our current theorems and definitions, we are now ready to tackle the main issue in constructing the absolute Galois group over $\mathbb{Q}$. We have our finite groups, and we expect that we will be using an inverse limit, but what about the homomorphisms? We want our set to be partially ordered based on subsets. In other words, in our definition of the inverse limit we let I be $\mathcal{K}$, the set of all Galois extensions of $\mathbb{Q}$ and we say that for $J, K \in \mathcal{K}$, $J < K$ if $J \subsetneq K$. So then for any Galois extensions J and K such that $J \subsetneq K$ we need to be able to define some standard homomorphism $\phi_{K,J} : Aut(K/\mathbb{Q}) \to Aut(J/\mathbb{Q})$. With this in mind, let $\sigma_K \in Aut(K/\mathbb{Q})$. Let $\phi_{K,J}(\sigma_K) = \sigma_K|_J$, the restriction of the automorphism σ_K onto J. Then let $p(x)$ be some irreducible polynomial in $\mathbb{Q}[x]$ such that there is an $\alpha \in J$ where $p(\alpha) = 0$. Then $\alpha \in K$ so since K is Galois, all roots of $p(x)$ are in K and by theorem 2 $\sigma_K(\alpha) = \beta$ where β is some other root of $p(x)$. We can then do this for all roots of all polynomials which split over J. Then $\sigma_K|_J$ still fixes $\mathbb{Q}$ and sends roots to other roots, so this defines an automorphism in $Aut(J/\mathbb{Q})$. So we will be using these restriction functions for our inverse limit, but we still have to prove that they are homomorphisms.

Claim 4. *Let J and K be Galois extensions of $\mathbb{Q}$ such that $J \subsetneq K$. Then the function $\phi_{K,J} : Aut(K/\mathbb{Q}) \to Aut(J/\mathbb{Q})$ which sends an automorphism σ_K to its restriction in J is a homomorphism.*

Proof. We have three properties to check to prove something is a homomorphism.

First note that if σ is the identity automorphism then the restriction of σ onto J does not change the fact that it maps every element to itself. So $\phi_{K,J}$ satisfies the property that it sends the identity in the first group to the identity in the second.

Now let σ_1 and σ_2 be elements of $Aut(K/\mathbb{Q})$. Then for all roots α in J that aren't in $\mathbb{Q}$, $\sigma_1(\alpha) = \beta$ for some compatible root β. Then if we look at $\sigma_2(\sigma_1(\alpha))$ this must be some root γ of the same polynomial as α and β. If we then look at $\phi_{K,J}(\sigma_1)$ we get the automorphism in $Aut(J/\mathbb{Q})$ which sends α to β. So then the composition in $Aut(J/\mathbb{Q})$, $\phi_{K,J}(\sigma_2)(\phi_{K,J}(\sigma_1))$ would first map a root α to β and then map β to another root γ. So this composition would be the automorphism mapping α to γ in J. But this is the same thing as $\sigma_2(\sigma_1)|_J$. Thus we have that $\phi_{K,J}$ satisfies the condition that composition in the first group corresponds to composition in the second group.

Finally we look quickly at σ_1^{-1}, the automorphism of K which would send a root β to α. Clearly the restriction onto J would do the same, and thus correspond to the inverse of σ_1 restricted to J.

Thus $\phi_{K,J}$ satisfies all of the properties of a homomorphism. □

With this we have finished our construction of the absolute Galois group. In summary

$Aut(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{K \in \mathcal{K}} Aut(K/\mathbb{Q})$ where the homomorphisms down onto subgroups are given by restrictions.

3.2. **Topology of** $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$.

As with $\hat{\mathbb{Z}}_p$ we want to define a topology on the absolute Galois group. Just as with the p-adic integers, we are going to base our topology on certain functions being continuous. In particular, given an element σ of $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ we want the functions which send σ to its restriction in $Aut(K/\mathbb{Q})$ for any Galois extension K to be continuous. Once again, to do this we first need a topology on $Aut(K/\mathbb{Q})$. We give these groups the same natural topology as our $\mathbb{Z}/p^n\mathbb{Z}$, namely the discrete topology, as is typical for finite groups. From here, the discussion looks exactly like section 2.4 and 2.5. The arguments in those sections can be fully generalized for any uncountable group which can be described as the inverse limit of groups with the discrete topology.

As a quick recap, recall that the requirement that our functions be continuous gives us that a set is open in our profinite group if each element has a component where every other possible element in the group with the same choice in that component is in that set. So in our absolute Galois group, that means a set is open if every element x of the set has an extension K such that every other element of the group which when restricted to K is equivalent to x restricted to K is in the set.

Moving on to connectedness, recall that any time we had a set with at least two distinct elements, x and y, we could then take a component where x and y differ then take the union of the set of all elements of our group with that component the same as x's and the set containing every other element of our group. Since those two sets are disjoint, open, and their union is the whole set, clearly any set that contains more than just a point is disconnected. So then, we can easily apply this to the absolute Galois group over $\mathbb{Q}$. Just like that, thanks to our work with $\hat{\mathbb{Z}}_p$ we have shown that $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ is totally disconnected. In fact, this shows us that as long as we give the finite groups the discrete topology, any profinite group is totally disconnected!

Finally we have compactness. Once again, the proof for $\hat{\mathbb{Z}}_p$ has given us everything we need to know. Our group $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ is a subset of $\prod\limits_{K \in \mathcal{K}} Aut(K/\mathbb{Q})$. So then, since the latter is a direct product of finite groups, Tychonoff's theorem once again tells us that are larger group is compact. We can then again show that $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ is an arbitrary intersection of closed sets in the larger group, thus showing that the smaller group is a closed subset, thus making the absolute Galois group over $\mathbb{Q}$ compact. In fact, it is not hard to generalize our proof from $\hat{\mathbb{Z}}_p$ to work for any profinite group. It mostly just involves rewriting the arbitrary intersection of inverses to match the corresponding homomorphisms.

So, topologically speaking, we see that $\hat{\mathbb{Z}}_p$ and $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ are identical. In fact, we now see that most of the topological properties of $\hat{\mathbb{Z}}_p$ were simply properties of all profinite groups. This is why writing the absolute Galois group as a profinite group is so helpful. There are many things we can prove for profinite groups in general, thus foregoing having to explicitly deal with such a complicated group. There are still some structural differences between our two groups though. For example, $\hat{\mathbb{Z}}_p$ is abelian. This is easy to see since the operation in this group is just component-wise addition in each $\mathbb{Z}/p^n\mathbb{Z}$. The absolute Galois group on the other hand is not. The operation in this group is composition of functions, so if σ_1 sends α to β and σ_2 sends β to γ then $\sigma_2(\sigma_1(\alpha)) = \gamma$ whereas $\sigma_1(\sigma_2(\alpha))$ need not be. It's possible that $\sigma_2(\alpha) = \alpha$ in which case our second composition would give us β. This lack of commutativity is one factor which complicates computations in the absolute Galois group.

Another thing that makes things difficult deals with the partial ordering of our extensions in $\mathcal{K}$. In $\hat{\mathbb{Z}}_p$ if we made a choice at some level p^n, this would decide all elements below it and then we could make all the elements above it equal, or add something each time that wouldn't change the element mod p^n. This allows us to describe many different elements of this group. Because $\mathcal{K}$ is only partially ordered, if we make a choice of where to send some root α, this still leaves infinitely many other roots that aren't determined by where α was sent, as well as many that are partially determined by it. In other words, no matter how many choices we make there are still more choices to be made, and we have to be careful and precise with those choices. Because of this, determining elements of the absolute Galois group is extremely complex. In fact, only two elements can be explicitly given: the identity element which sends every root to itself, and the automorphism which sends each root to its complex conjugate. This is incredible, considering, as we are about to prove, this group is uncountable.

3.3. Uncountability of $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$.

The last thing we need to prove about $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ is that it is uncountable. This is another thing that can be generalized from a proof for any nontrivial profinite groups, but since we used an argument for $\hat{\mathbb{Z}}_p$ that relied on it being fully ordered, we will have to give a full proof here.

Claim 5. *$Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ is uncountable.*

Proof. We will begin with a basic result from Galois theory.

Theorem 3. *Let K and H be Galois extensions of a field F such that $K \cap H = F$. Then KH, the smallest field containing both K and H is Galois over F and its automorphism group over F is isomorphic to $Aut(K/F) \times Aut(H/F)$.* [1, p. 593]

So in other words, if we have two fields who only have the base field in common then an automorphism in the combined field can truly be thought of as a choice in each of the smaller fields.

Now let p_n be a list of prime integers for all n, with $p_n = p_m$ only if $n = m$. Then note that $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$ does not contain $\sqrt{p_m}$ for any $m > n$ as this would imply that p_m was a multiple of the other p_n. So then, $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}) \cap \mathbb{Q}(\sqrt{p_m}) = \mathbb{Q}$. Thus, since $\mathbb{Q}(\sqrt{p_n})$ is always Galois for any prime p_n, we get that $Aut(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}))$ is isomorphic to $\prod_{m=1}^{n} Aut(\mathbb{Q}(\sqrt{p_m}))$. Each of these smaller automorphism groups are easily shown to have two elements: the identity automorphism and the automorphism which sends $\sqrt{p_n}$ to $-\sqrt{p_n}$.

Let $K = Aut(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$ and let $K_n = Aut(\mathbb{Q}(\sqrt{p_n}))$. Then let's take $k \in K$. We know that $\phi_K^{-1}(k)$ is nonempty for any automorphism group K and any $k \in K$, that is we can always find some element of the absolute Galois group which restricts down to an element of the automorphism group of any finite extension. Note that since $K = K_1 \times ... \times K_n$ then we can express the element k as $(k_1, k_2, ..., k_n)$ where k_m represents the restriction of k to K_m.

So then, the set of elements that restrict to k are the elements which restrict to k_m when restricted to K_m for all $m \leq n$. So then, we have that $\phi_K^{-1}(k) = \bigcap_{m=1}^{n} \phi_{K_m}^{-1}(k_m)$. This is true for any finite list of prime numbers. What if we instead had an infinite list of prime numbers? We would still have that that the inverse in the large group was equal to an intersection of individual inverses, but we don't yet know that $\phi_K^{-1}(k)$ is always nonempty since K is no longer a finite extension. But we do still have that $\phi_K^{-1}(k) = \bigcap\limits_{n\in\mathbb{N}} \phi_{K_m}^{-1}(k_m)$.

Is this arbitrary intersection empty? For this we need the following theorem.

Theorem 4. *Let X be a compact set and let $\{X_i\}$ be an arbitrary set of closed subsets of X. If all finite intersections of these X_i are nonempty then any arbitrary intersection of these X_i must also be nonempty.* [3, p. 4]

We have shown that the absolute Galois group is compact, that $\phi_{K_m}^{-1}(k_m)$ is closed for every m, and that any finite intersection of such sets is nonempty. Thus, by the above theorem, any arbitrary intersection of such sets is nonempty. In other words, there must be some element of the absolute Galois group such that it restricts down to k, where k is any element of $Aut(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ...))$.

Now we can finally get to the meat of our uncountability proof. Assume for the sake of contradiction that the absolute Galois group is countable. Then if we order our extensions $\mathcal{K}$ as $K_1, K_2, ...$ then we can list our elements as

$$x_1 = (x_{11}, x_{12}, x_{13}, ...)$$
$$x_2 = (x_{21}, x_{22}, x_{23}, ...)$$
$$...$$

But then let $\{p_n\}$ be a sequence of distinct prime numbers. Let $K_{k_1}, K_{k_2}, ...$ be a subsequence of our original sequence such that $K_{k_m} = \mathbb{Q}(\sqrt{p_m})$. Then if x_{mk_m} is the identity automorphism, we let $y_m \in K_{k_m}$ be the automorphism sending $\sqrt{p_m}$ to $-\sqrt{p_m}$. If x_{mk_m} is not the identity automorphism then we let $y_m \in K_{k_m}$ be the identity. We then know from the above discussion that $\bigcap\limits_{n\in\mathbb{N}} \phi_{K_{k_n}}^{-1}(y_n)$ is nonempty, that is there is in fact an element of the absolute Galois group satisfying the above properties. Thus, we have constructed an element of the absolute Galois group that was not in our above list. So we have our contradiction, and our conclusion.

□

4. **Closing Remarks**

This concludes our discussion of the absolute Galois group over $\mathbb{Q}$ as a profinite group, an incredibly helpful tool for any algebraist. We have seen how a simpler profinite group, like $\hat{\mathbb{Z}}_p$, can help us work with the complex structure of this group, to see that it is totally disconnected despite its uncountably many elements and compact construction. Here are just a couple more interesting facts about absolute Galois groups in general that did not pertain directly to our discussion.

(1) The absolute Galois group of $\mathbb{R}$ is finite. This is due to the fact that the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$, so the only root introduced is i. Thus

the only possible automorphisms on $\mathbb{C}$ which fix $\mathbb{R}$ are the identity automorphism and the automorphism which sends i to $-i$. Interestingly enough, when restricted to $\overline{\mathbb{Q}}$ these are exactly the two elements of $Aut(\overline{\mathbb{Q}}/\mathbb{Q})$ that we could define.

(2) $\hat{\mathbb{Z}}_p$ can actually be used to construct the absolute Galois group over finite fields. In particular, the absolute Galois group of a finite field is isomorphic to a direct product of $\hat{\mathbb{Z}}_p$ for all primes p.

References

[1] D. S. Dummit and R. M. Foote. *Abstract Algebra.* John Wiley and Sons, Inc., Hoboken, NJ, third edition, 2004.

[2] J. Lebl. *Basic Analysis.* December 16th 2014 edition, 2014.

[3] L. Ribes and P. Zalesskii. *Profinite Groups.* Springer, Verlag Berlin Heidelberg, second edition, 2010.

Oklahoma State University, Stillwater, OK 74077
E-mail address: ryan.m.burkhart@okstate.edu