TOPOLOGY IN INFINITE GALOIS THEORY

DAVID NIELSEN

1. Introduction

The idea of taking topology from analysis and using it in a algebraic group structure seemed interesting to me, so I chose to look at topological groups. One place where topology brings clarity to an algebraic topic is in Galois theory. Galois theory provides very nice relations between groups of automorphisms and their underlying fields so long as the fields are finite extensions of some other field. However, if the field extensions in question are infinite then the relations break down. By applying a topology to the groups of automorphisms the relations become clear once again.

I will attempt to walk you through the process by which I approached learning about this infinite Galois theory. I used "Field Extensions and Galois Theory" by Julio R. Bastida as my primary source for information and any references to page numbers come from it.

2. Finite Galois Theory

My first step was to gain a basic understanding of how Galois theory worked in the finite case. This entailed learning the definitions of concepts central to Galois theory.

Definition 2.1 (Field Extension). *Given a field K, the field F is an extension of K iff $K \subset F$.*

So an extension field is simply a larger field that the initial field is embedded into. The examples that helped made this clear to me were the real numbers as an extension of the rational numbers and the complex numbers as an extension of the reals. Being able to think of extensions in terms of fields I already knew was helpful.

Definition 2.2. *Given a field F, with subfield K and subset D then the field generated by $K \cup D$ is denoted $K(D)$*

This is a simple way to create field extensions of K that is used in a number of Bastida's examples and proofs, so it is handy to note now.

In Galois theory, we are most concerned with extensions that are both **normal** and **separable**. If an extension has both these properties we call it **Galois**. I will omit these definitions because they rely on a series of definitions that are more clearly laid out in Bastida's book, and the specifics did not impact my study of infinite Galois theory. It was simply assumed that we were dealing with Galois extensions and the properties of the fields were secondary. More often, we were concerned with the group of automorphisms of a field, $Aut(F)$.

Definition 2.3 (Invariant)**.** *For a field F, let $s \in Aut(F)$. Every $\alpha \in F$ such that $s(\alpha) = \alpha$, α is said to be s-invarient which we notate $\alpha \in Inv(s)$, with Inv(s) being the subset of F invariant under s*

This definition clearly generalizes to groups of functions, where the invariant subset of the field with respect to the group is the intersection of the invariant subsets with respect to all the group elements.

Definition 2.4 (Galois Group)**.** *For a field K with extension F, we define the* **Galois Group** *to be the group of automorphisms of F for which K is invariant. We notate this Gal(F/K)*

So the Galois group is the group of automorphisms that leave K untouched, while doing anything to the remainder of F.

With these definitions we can state the fundamental theorem of finite Galois theory as found on page 124 of Bastida.

Theorem 2.5 (Galois)**.** *Let K be a field, and let F be a finite Galois extension of K.*

- **(i):** *If E is an intermediate field between K and F, then Gal(F/E) is a subgroup of Gal(F/K).*
- **(ii):** *If Γ is a subgroup of Gal(F/K), then Inv(Γ) is an intermediate field between K and F.*
- **(iii):** *The mapping $E \longmapsto$ Gal(F/E) from the set of all intermediate fields between K and F to the set of all subgroups of Gal(F/K) and the mapping $\Gamma \longmapsto Inv(\Gamma)$ from the set of all subgroups of Gal(F/K) to the set of all intermediate fields between K and F are mutually inverse inclusion-reversing bijections.*

This bijective relation between the Galois group and the intermediate fields is one of the most important results of Galois theory. These are the main topics from finite Galois theory that I was examining in an infinite context.

3. The Problem with Infinity

When looking at a field K with *infinite* extension F, the intermediate groups between F and K still relate to subgroups of $Gal(F/K)$ by the relation $E \longmapsto Gal(F/E)$ but not every subgroup of the Galois group relates to an intermediate field.

Bastida shows this in an example on page 197. This example took me a couple of readings to understand, but that was mostly due to having to scour the book to completely understand the notation and the specific fields/functions being used. This is one of the problems I had with learning from this book. The examples which were supposed to illustrate the theorems often referenced things which were unfamiliar to me, so they didn't actually help me figure out what was happening, and I was no sure how to construct simpler example that would help me see what was going on. I will attempt to reconstruct the example and parenthetically fill in the gaps that made gave me trouble when I was first reading it:

Example 1. Let P be a field with prime characteristic p (P is finite and isomorphic to $\mathbf{Z}/p\mathbf{Z}$). Let F be the algebraic closure of P (this means F is infinite and a Galois extension of P). Let Γ be a subgroup of the $Aut(F)$ defined by the Frobenius mapping[1] ($\alpha \longmapsto \alpha^p$)

If n is a positve integer, F contains a *unique* subfield of cardinality p^n, and $X^{p^n} - X$ from $P[X]$ splits over $F[X]$ (since F is an algebraic extension of P). Let $D = \{$all zeros of $X^{p^n} - X$ in $F\}$. This means that $P(D)$ is the only splitting field of $X^{p^n} - X$ in F which further means $P(D)$ is the only field of cardinality p^n in F (these properties of fields are explained further in Bastida, but there is not space here to do so).

For every positive integer n let E_n denote the subfield of F of cardinality p^{2^n}. Note that $2^n | 2^{n+1}$ for $n \geq 1$ so we have a strictly increase sequence of subfields of F. Let $E = \cup_{n=1}^{\infty} E_n$. This E is an infinite proper subfield of F since it has no subfield of cardinality p^3 which F does have.

Since F is Galois over P, it is Galois over E (Proposition 3.3.1 page 116). This means $E = Inv(Gal(F/E))$ and since E is a proper subfield, this is a nontrivial group. If $s \in Gal(F/E)$, $s \neq I_F$ there cannot be a positive integer n such that for all $\alpha \in F$, $s(\alpha) = \alpha^{p^n}$ because that would make each point of E a zero of $X^{p^n} - X$ which is a finite set, while E is infinite. This restriction on s means that $Gal(F/E) \nsubseteq \Gamma$ which further tells us $\Gamma \neq Aut(F)$.

We know that P is the set fixed points under the Frobenius mapping, which is also fixed under $Aut(F)$ which is its Galois group (page 99) so we have the following:

$$Inv(\Gamma) = P = Inv(Gal(F/P)) = Inv(Aut(F))$$

Now we have two distinct groups that both have P invariant. This means that Γ is a subgroup of the Galois group that does not correspond to an intermediate field. So this example has show that the fundamental theorem of finite Galois theory breaks down when we attempt to transition to infinite fields.

Topology comes into infinite Galois theory to solve this problem. By applying an appropriate topology to a Galois group, a bijective relation can once again be found. Krull pioneered this, but I will first look at the finite topology described by Bastida

4. Finite Topology

To create the finite topology, we first must describe the basic sets from which all the open sets are made.

Definition 4.1 (Basic Set in Finite Topology)**.** [2] *Let F be a field and let s be an automorphism of F. For every finite subset A of F, we denote the set of all automorphism that agree with s on A, $\Omega_s(A)$*

These basic sets along with the empty set make up the finite topology, which we will now assume is applied to any group of automorphisms. The first proposition that I was able to understand and reconstruct about this topology is the following:

Proposition 4.2. [3] *Let F be a field, Γ a group of automorphisms of F with closure $\bar{\Gamma}$. Then $Inv(\Gamma) = Inv(\bar{\Gamma})$*

[1]Bastida 8

[2]Bastida 197-198

[3]Proposition 3.12.3Bastida 198

Proof. Since $\Gamma \subset \bar{\Gamma}$ it is clear that everything that is invariant under $\bar{\Gamma}$ is also invariant under Γ so $Inv(\bar{\Gamma}) \subseteq Inv(\Gamma)$. To show that $Inv(\Gamma) \subseteq Inv(\bar{\Gamma})$ we look at any $\alpha \in Inv(\Gamma)$. If $s \in \bar{\Gamma}$ then from properties of closure we know that there is a $t \in \Gamma \cap \Omega_s(\alpha)$. This gives us the following relations for t, $s(\alpha) = t(\alpha) = \alpha$ so $\alpha \in Inv(\bar{\Gamma})$ □

The only tricky part of the proposition is that s being in the closure of Γ gives us such a t. Once you have that fact, it is very simple to see how things follow. This same idea can then be used to show that the Galois group is closed under the finite topology.

Proposition 4.3. [4] *Let K be a field, and let F be an extension field of K. then Gal(F/K) is closed in Aut(F)*

Proof. We must show that Gal(F/K) contains all the points in its closure, that is for any $s \in \overline{Gal(F/K)}$, $s(\alpha) = \alpha$ for all $\alpha \in K$. The same closure property used in 4.2 gives us a $t \in Gal(F/K) \cap \Omega_s(\alpha)$ from which follows the same relation: $s(\alpha) = t(\alpha) = \alpha$ □

These two propositions helped me see how the finite topology worked. It became clearer what being in a specific 'open set' meant, because that property was used to show agreement between the s and t in both propositions.

5. Finite Topology and Krull Topology

Krull's initial topology was not stated in the same language as the finite topology, but the Krull topology agrees with the finite topology on Galois groups of algebraic extensions. We will show this by stating the description Krull gave of the basis for the open sets in his topology, and showing how it reduces to the open sets defined by the finite topology.

Proposition 5.1 (Krull)**.** [5] *Let K be field, and let F be an algebraic extension of K. Then the Galois groups of F over its subfields that are finite extensions of K make up a fundamental system of neighborhoods of the elements in Gal(F/K)*

Proof. If D is a finite subset of F, $K(D)$ is a finite extension of K as Krull described. We then look at $Gal(F/K(D))$ We note that K is invariant under this mapping, as is D and any combination of elements of K and D This leads to the relation

$$Gal(F/K(D)) = Gal(F/K) \cap \Omega_{I_F}(D)$$

We also note that for any $s \in Gal(F/K)$, $\Omega_s(\emptyset) = Gal(F/K)$. This means that the Galois group of F over the the finite extensions of K can be described as the intersection of open sets from the finite topology □

Now that we have these two ways of describing the same sets on a Galois group, we consider why there was no topoloy necessary if the extension field was finite. If F is an finite Galois extension of K then the Krull topology tell us that $Gal(F/F)$ is a basis element for the set of open sets. However $Gal(F/F) = I_F$ which clearly leads to a discrete topology since the identity returns each automorphism in the Galois group as an open set. Once we have an discrete topology there isn't anything interesting to be learned by examining the properites of open or closed sets since

[4]Proposition 3.12.4, Bastida 199

[5]Proposition 3.12.6, Bastida 199

all sets are open and closed. We now follow Bastida as he turns to examine sets that are compact under the finite topology.

6. Product Topology Aside

Bastida began his discussion of compactness by introducing a product topology. This was initially quite confusing to me since I had forgotten about product topologies and was not sure how to construct examples for myself so that I could begin to figure things out. This is the proposition that introduced product topology:

Proposition 6.1. [6] *Let F be a field. For every $\alpha \in F$, let D_α denote the discrete topological space having F as its set of points. Then Aut(F)$\subseteq \times_{\alpha\in F} D_\alpha$, and the finite topology on Aut(f) coincides with the topology on Aut(F) induced that that on the product space $\times_{\alpha\in F} D_\alpha$*

The proof as written in the book did little to help me understand why this was true. However, I talked to Jerry about my confusion and he was able to clarify things. By drawing rough sketches of what the proposition was claiming I was able to begin to understand what was going on. I will attach my recreations of these drawings along with a brief explanation. Being able to simply draw a picture of the situation was very enlightening to me, and I will hopefully be able to do this in the future when I get stuck while reading through theorems. It helped make concrete examples of abstract ideas that I knew I had heard about but who's details I couldn't remember. This also highlighted the importance of getting someone else's viewpoint while studying math. Someone else was able to propose looking at the problem in a different manner that I would not have thought of or known how to create and things were greatly clarified. I have found this outside input to be very helpful in the past and hopefully will be able to continue to use it in my study of mathematics.

This product topology doesn't really bear on the rest of infinite Galois theory, it is simply a tool Bastida used in a few proofs to show things simiply. I include it hear because I wanted to understand it so I could parse the proofs that Bastida was providing. He goes on to prove a number of properties about compactness of Galois groups which allow him to state the fundemental theorem of infinite Galois Theory

7. Fundemental theorem of Infinite Galois Theory

Bastida provides two slightly different flavors of the fundamental theorem, but I will include the one that most closely relates to the finite theorem I already included:

Theorem 7.1. [7] *Let K be a field and let F be a Galois extension of K.*

- **(i):** *If E is an intermediate field between K and F, then Gal(F/E) is a closed subgroup of Gal(F/K).*
- **(ii):** *If Γ is a closed subgroup of Gal(F/K) then Inv(Γ) is a intermediate field between K and F.*

[6] Proposition 3.12.9, Bastida 200
[7] Theorem 3.12.19, Bastida 204

(iii): *The mapping $E \longmapsto Gal(F/E)$ from the set of all intermediate fields between K and F to the set of all closed subgroups of $Gal(F/K)$ and the mapping $\Gamma \longmapsto Inv(\Gamma)$ from the set of all closed subgroups of $Gal(F/K)$ to the set of all intermediate fields between K and F are mutually inverse inclusion-reversing bijections.*

The proof for this theorem comes very directly from the properties of compact sets and closed sets that Bastida relates following his introduction of the product topology. In my project I read over them and gained a basic understanding of what they said so that they made sense when referenced in this final proof. I am not going to simple copy the proof since I do not have anything meaningful to add to it.

This theorem once again gives us a bijective relation. Instead of the simple bijective relation in the finite case, we now must have a topological description of our Galois group before we can create this bijective relation. We also note that this also sadly does not tell us anything about how the open subsets of the Galois group relate to the underlying field. So in the infinite case we are left with a much rougher description of the Galois group, but at least we have found a way to make some sense of the relation between a field and its Galois groups.

8. Conclusion

This study of infinite Galois theory illustrates a useful combination of the techniques of analysis with algebra. The group structures from algebra give strong relations when Galois theory is applied to finite groups. In the finite case the fundament theorem provides a bijective relationship, which is extremely powerful. However, once the field extensions move into the realm of the infinite, the algebraic structure no longer gives clear relationships. Analysis often concerns itself with the infinite so applying the ideas of analysis appropriately brings clarity to the subject. The ability to classify subsets as open or closed provides a way to pick out the parts of the Galois group that behave even in the infinite case. This allows for the creation of a new fundamental theorem with a bijective relation between fields and their Galois groups.