DRP Presentation: The Fundamental Theorem of Galois Theory

by Omar Aceval

"Presented" May 6th, 2020

1 Introduction and Important Definitions

Galois Theory is named in honor of Évariste Galois, who lived a fascinating but short life. It began as a study in search of general equations for finding the roots of polynomials of degree fifth and above. A "general equation" here means an equation or set of equations that define the roots of a polynomial using only the coefficients in the polynomial, the four basic operations, exponentiation and taking nth roots. For example, it has been known since before the 9th century that the quadratic equation now commonly taught before university level is such a solution to any polynomial of degree 2. Similar equations were later discovered for the third and fourth degree, which inspired the question of which degree polynomials have such an equation. It was known from previous results that there in fact does not exist a general solution to fifth order polynomials, namely polynomial counterexamples could be obtained that are not solvable via a general equation. But Galois' work instead found exact conditions for when polynomials could be solved via the four basic operations and radicals, which fruit a much deeper understanding as to why there is no general equation for fifth order and certain above orders.

The *Fundamental Theorem of Galois Theory* (FTGT) is simple enough to understand, at least without proof, and yet incredibly insightful about Galois' ideas. In order to understand the language of Galois Theory, I will first give a few definitions and explanations on the more basic level.

Unless otherwise stated, let **F** denote a field, and let **E** denote an *extension* of **F**, that is that **E,F** are fields such that $\mathbf{E} \supseteq \mathbf{F}$. Also G will denote a group.

Definition (Degree of a field extension)**.** *The degree of a field extension* ***E*** *is the degree of* ***E*** *as an* ***F****-vector space, and will be denoted by* [**E**/**B**].

Definition (Algebraic Extensions)**.** *A extension* ***E*** *is called an algebraic extension of* ***F*** *if every element in* ***E*** *is the root of some polynomial* f *in* ***F****[x].*

These extensions in particular are useful for *adjoining* roots of a polynomial f to the field **F**.

Definition (Normal Extension)**.** ***E*** *is a normal extension of* ***F*** *if every irreducible in* ***F[x]*** *with a root in* ***E*** *can be expressed as linear factors in* ***E****[x].*

When this is true we say that f *splits* in **E**[x].

Definition (Galois Group)**.** *The Galois Group of* ***E****, an algebraic extension of* ***F****, is the group of automorphisms of* ***F*** *that fix* ***F****. This group is denoted by* Gal(**E**/**F**)

To fix a field **F** means that elements in **F** map to themselves under every automorphism in G. A group of automorphisms uses composition as the group operation.

Definition (Fixed Field)**.** *The fixed field of a group of automorphisms of a field* ***F*** *is the set of all elements that are mapped to themselves for any automorphism in G.*

Note the distinction between the previous two definitions: the Galois *group* refers to a set of automorphisms while a fixed *field* refers to a set of elements, which can be shown to be a field.

Definition (Galois Extension)**.** ***E*** *is a Galois extension of* ***F*** *if the fixed field of the Galois group of* ***E*** *is exactly* ***F****.*

2 The Theorem Statement (without proof)

We are ready to discuss the statement in more detail.

The Fundamental Theorem of Galois Theory. *Let* $\boldsymbol{E}$ *be a finite Galois Extension of* $\boldsymbol{F}$ *and let* G *be the Galois group* $\mathrm{Gal}(\mathbf{E}/\mathbf{F})$.

1. *Then there is a one-to-one correspondence between the intermediate fields* $\boldsymbol{E} \supseteq \boldsymbol{B} \supseteq \boldsymbol{F}$ *and the subgroups* $\{1\} \subseteq \{G_{\mathbf{B}}\} \subseteq \{G\}$
   In particular, the correspondence is given by $\mathbf{B} = Fix(G_{\mathbf{B}})$*, where* $G_{\mathbf{B}}$ *denotes a subgroup of* G*, and* B *is the fixed field of that subgroup* $G_{\boldsymbol{B}}$.

2. *Furthermore, the intermediate fields* $\boldsymbol{B}$ *are normal extensions if and only if* $G_{\mathbf{B}}$ *is a normal subgroup of* G*. In fact, this is only the case whenever* $\boldsymbol{B}$ *is a Galois extension of* $\boldsymbol{F}$*, and we have the important isomorphism given by:*
$$\mathrm{Gal}(\mathbf{B}/\mathbf{F}) \cong G/G_{\mathbf{B}}$$

3. *For each subfield* $\boldsymbol{B}$*, the degree* $[\mathbf{E}/\mathbf{B}] = |G_{\mathbf{B}}|$*, and likewise the index of* $G_{\mathbf{B}}$ *in* G *is* $[\mathbf{B}/\mathbf{F}]$.

Some important consequences are highlighted below.

One-to-one mapping: More generally, a subgroup H of G can be mapped to its corresponding field extension $\mathbf{B}$ by declaring $\mathbf{B}$ as the fixed field of H. A field extension $\mathbf{B}$ is mapped to its corresponding subgroup H by finding the set of elements in G that are the identity on $\mathbf{B}$.

We have that distinct subgroups H_1, H_2 of G map to distinct extensions of $\mathbf{F}$, $\mathbf{B}_1$ and $\mathbf{B}_2$: Let $\mathbf{B}_1$= Fix(H_1), $\mathbf{B}_2$= Fix(H_2). If $\mathbf{B}_1$=$\mathbf{B}_1$, then every automorphism in H_2 fixes $\mathbf{B}_1$ and so $H_2 \subseteq H_1$, and vice versa, and so therefore $H_1 = H_2$. Then by the contrapositive there is exactly one subgroup of G that corresponds to each field extension of $\mathbf{F}$.

Proving that there is exactly one extension field that corresponds to each subgroup would require at least a page or two. The idea is that because $\mathbf{E}$ is a Galois extension of $\mathbf{F}$, then it must also be what is called the *splitting field* of some *separable polynomial*. A separable polynomial is an irreducible in $\mathbf{F}$[x] that splits into distinct linear factors in $\mathbf{E}$. Because each intermediate field $\mathbf{B}$ contains $\mathbf{F}$, we have that this separable polynomial is also an element in $\mathbf{B}$[x], and so $\mathbf{E}$ must also be a Galois extension of $\mathbf{B}$. So therefore $\mathbf{B}$= Fix(Gal($\mathbf{E}/\mathbf{B}$)), where now the corresponding subgroup of G for the extension field $\mathbf{B}$ is Gal($\mathbf{E}/\mathbf{B}$).

The correspondence between intermediate fields and subgroups is inclusion reversing. For example, $\mathbf{E}$, the largest field extension of $\mathbf{F}$, always corresponds to the smallest group of automorphisms, namely the identity automorphism $\{1\}$, because only the identity automorphism fixes all of $\mathbf{E}$. In the same sense, because $\mathbf{E}$ is a Galois extension, we have that the fixed field of G must be $\mathbf{F}$, and so the smallest field extension of $\mathbf{F}$, itself, corresponds to the largest subgroup of G, also itself. A more rigorous explanation is given below.

If we let $\mathbf{B}_1$, $\mathbf{B}_2$ be intermediate fields such that $\mathbf{E} \supseteq \mathbf{B_1} \supseteq \mathbf{B_2} \supseteq \mathbf{F}$, then we see that the subgroup $G_{\mathbf{B}_1}$ which corresponds to automorphisms that fix $\mathbf{B}_1$, also fixes all of $\mathbf{B}_2$. Therefore the subgroup $G_{\mathbf{B}_1}$ must be contained in $G_{\mathbf{B}_2}$, the set of automorphisms that fix $\mathbf{B}_2$. Therefore though $\mathbf{B}_1$ contains $\mathbf{B}_2$, the corresponding subgroup G_1 is contained in G_2.

Relation between order of subgroups and extension fields: Let $\mathbf{E}$ be a Galois extension of $\mathbf{F}$, with an intermediate field $\mathbf{B}$ given by $\mathbf{E} \supseteq \mathbf{B} \supseteq \mathbf{F}$, and let G be the Galois group of $\mathbf{E}/\mathbf{F}$.

If the degree of $\mathbf{E}$ as an $\mathbf{F}$ vector space, $[\mathbf{E}/\mathbf{F}]$= n, we can write every term in $\mathbf{E}$ using only n elements from $\mathbf{E}$. It can be shown that $[\mathbf{B}/\mathbf{F}]$ divides $[\mathbf{E}/\mathbf{F}]$, namely by $[\mathbf{E}/\mathbf{F}] = ([\mathbf{E}/\mathbf{B}])([\mathbf{B}/\mathbf{F}])$: If $[\mathbf{E}/\mathbf{B}]$= a, $[\mathbf{B}/\mathbf{F}]$= b, then we need a elements from $\mathbf{E}$ to span $\mathbf{E}$ using coefficients in $\mathbf{B}$, and for each of those we need b elements in $\mathbf{B}$ using coefficients in $\mathbf{F}$, so therefore $n = ab$.

We have shown that $[\mathbf{E}/\mathbf{F}] = [\mathbf{E}/\mathbf{B}][\mathbf{B}/\mathbf{F}]$. By the FTGT, we can conclude that the order of the Galois extension field $\mathbf{E}$ as a $\mathbf{B}$ vector space is equal to the order of the corresponding subgroup $G_{\mathbf{B}}$. Therefore by definition the index of that subgroup is given by the degree of $\mathbf{B}$ as an $\mathbf{F}$ vector space.

2.1 Implications for 5th Order Polynomial

The following is based on the "Abel-Rufini Theorem" article from Wikipedia.

The first proof that the general fifth order polynomials have no solutions was known as the Abel-Ruffini theorem, and was made before Galois theory became the predominant train of thought on the matter. A modern proof of the same problem using Galois theory relies on factoring the general polynomial into its five roots, by declaring 5 roots α_i for $i = 1, 2, 3, 4, 5$, and then splitting the general polynomial into a linear product $(x-\alpha_1)\cdots(a-\alpha_5)$. Notice that any isomorphisms that interchange the roots i.e. permute the roots leave this polynomial unchanged. The key essence of the proof is that we can find an isomorphism between a group known as the symmetric group on 5 letters S_5 and the Galois group of general polynomials of degree 5. But because this particular group only has a normal subgroup known as A_5, which itself has only simple subgroups i.e. subgroups that are not normal, the respective extension fields will not be normal and thus not solvable. For orders of degree $n \geq 5$, we can instead find isomorphisms to the symmetric groups S_n, and similar arguments may hold to prove similar results for higher orders.

3 Conclusion

The fundamental theorem of Galois theory tells us that the structure of extensions of a field $\mathbf{F}$ is exactly the same as the structure of subgroups of the group of automorphisms of the field $\mathbf{F}$.

For example: statement (2) given in the statement above tells us that an extension is normal only whenever its corresponding subgroup is a normal subgroup of G. By examining the structure of this group G, we can immediately determine the desired extension fields of $\mathbf{F}$.

Reference Text

This paper was based on the text *Galois Theory* by Steven H. Weintraub. Namely, the introductory chapter 2 of the text regarding the fundamental theorem of Galois theory, and in particular pages 18-32.