THE GALOIS ANTI-ISOMORPHISM

ANDREW VILLADSEN

Abstract. Galois theory studies the algebraic field extensions of a given base field. In this paper, we develop the basics of Galois theory, including the Fundamental Theorem of Galois Theory. We also construct an anti-isomorphism between the category of separable extensions under a separable closure of a field and the category of transitive left coset spaces of closed subgroups of the absolute Galois group. This anti-isomorphism strengthens the usual statement of the Fundamental Theorem of Galois theory.

Contents

1. Introduction

Galois theory arises out of the study of polynomials over fields and adjoining roots of polynomials to construct new fields; the classical example is the construction of the complex numbers by adjoining a root of $x^2 + 1$ to the real numbers. Specifically, one studies certain algebraic field extensions (defined below) by looking at the action of a group of automorphisms of a given extension. Informally, the Fundamental Theorem of Galois Theory states that the structures of an extension and its associated automorphism group totally determine each other. In this paper we will develop the basics of Galois theory up to the Fundamental Theorem, and construct an anti-isomorphism of categories suggested by the Fundamental Theorem, which refines the anti-equivalence constructed by Szamuely in [2]. Importantly, unlike Szamuely's result, the anti-isomorphism that we construct is an evidently stronger statement than the Fundamental Theorem.

In section 2, we introduce the basic definitions for field extensions, and examine the structure of algebraic field extensions. In section 3, we define and characterize normality and separability of algebraic extensions, and introduce the algebraic closure and separable closure of a field. In section 4, we provide the necessary definitions to state the Fundamental Theorem, and prove the results leading to the

Date: August 25, 2011.

Fundamental Theorem and the Fundamental Theorem in case of finite extensions. In section 5, we introduce the necessary pieces of profinite group theory, and prove the Fundamental Theorem for infinite extensions. In section 6, we construct an anti-isomorphism between the category of separable extensions under a separable closure of a field and the category of transitive left coset spaces of closed subgroups of the absolute Galois group, and compare this anti-isomorphism to Szamuely's anti-equivalence.

2. Field Extensions

Definitions 2.1. A field L is called a *field extension* of a *base field* k, denoted $L|k$, if L contains k as a subfield. An element α of L is *algebraic over* k if it is the root of a polynomial over k; otherwise it is called *transcendental*. The extension L is also called algebraic over k if all of its elements are algebraic over k.

The *minimal polynomial over* k of an algebraic element α of L is the (unique) monic polynomial over k of lowest degree that has α as a root. Equivalently, it is the monic greatest common divisor of the set of polynomials over k that have α as a root.

With the goal of treating the field extensions of a given base field categorically, it is important to also define the morphisms between extensions. Given extensions $L|k$ and $M|k$, a morphism $\phi : L \to M$ is a field homomorphism that preserves the extension structure, that is, which fixes k element-wise. We will call such functions *k-homomorphisms*. Note that since it is a non-trivial field homomorphism, a k-homomorphism must be an embedding. Furthermore, a k-homomorphism $\phi : L \to M$ takes every algebraic element of L to an algebraic element of M with the same minimal polynomial.

If L is an extension of k, it is easy to verify that L is a vector space (in fact an algebra) over k, and that k-homomorphisms are linear transformations (respectively k-algebra homomorphisms).

Definition 2.2. Let $L|k$ be a field extension. The dimension of L as a vector space is called the *degree* of the extension L, and is written $\deg(L|k)$. An extension is called *finite* if it has finite degree, and *infinite* otherwise.

Proposition 2.3. *Every finite extension of a field k is algebraic.*

Proof. Let $L|k$ be a finite extension. If $\alpha \in L$ is transcendental, then the set $1, \alpha, \alpha^2, \ldots$ must be linearly independent over k, as any relation between them would specify a polynomial over k of which α is a solution. □

In order to give richer structure to the extensions of a field, it will often be necessary to fix a particular extension of the base field, and restrict consideration to just the category of subextensions of that extension. The inclusion structure notably gives this category a inverse limit, the field compositum. Further, the inclusion structure is central to the Fundamental Theorem of Galois Theory. We will see later in the section that there are "fully general" choices for the containing extension.

For the following four propositions, fix an extension $K|k$.

Corollary 2.4. *For any non-zero algebraic element α of K, the multiplicative inverse of α in K can be expressed as a polynomial of α with coefficients in k.*

Proof. Let $m(x)$ be the minimal polynomial of α over k. Then $m(x)$ and x are relatively prime in the ring of polynomials over k, as otherwise $m(x)$ would not be minimal. Since $k[x]$ is a principal ideal domain, there exist polynomials $f(x)$ and $g(x)$ such that $m(x)f(x) + xg(x) = 1$. Evaluating at α, we find $\alpha g(\alpha) = 1$ as $m(\alpha) = 0$. Hence $g(\alpha)$ is the inverse of α. □

Proposition 2.5. *Let S be a set consisting of algebraic elements of K. Then $k(S) = k[S]$, that is, the field closure of S adjoined to k is the ring closure of S adjoined to k.*

Proof. In concrete terms this means that any rational expression of elements of S with coefficients in k can be rewritten as a polynomial expression of elements of S with coefficients in k. But by the previous proposition the inverse of the denominator of such a rational expression can be rewritten as a polynomial of the denominator, and thus of the elements of S. □

Proposition 2.6. *The degree of a finite extension is multiplicative. That is, if $M|L$ and $L|k$ are finite extensions, then $M|k$ is a finite extension and* $\deg(M|k) = \deg(M|L)\deg(L|k)$.

Proof. Given a basis $\{x_i\}$ of a finite extension $L|k$ and a basis $\{y_j\}$ of M over L, the set $\{x_i y_j\}$ is a basis of M over k. □

Observing that

$$k[\alpha_1, \alpha_2, \ldots, \alpha_n] = k[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n]$$

and

$$k(\alpha_1, \alpha_2, \ldots, \alpha_n) = k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n)$$

for any $\alpha_1, \alpha_2, \ldots, \alpha_n$ in K, the multiplicativity of degree allows the computation of finite degrees. We also need to treat the base case to be able to compute degrees.

Proposition 2.7. *If $\alpha \in K$ is algebraic with minimal polynomial m over k, then* $\deg(k(\alpha)|k) = \deg(m)$.

Proof. Let $n = \deg(m)$, and $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Then B is linearly independent over k, as a non-trivial linear relation between the elements of B would give a non-zero polynomial over k with α as a root and lower degree than m, a contradiction. For any $\beta \in k(\alpha) = k[\alpha]$, there is some polynomial f over k such that $\beta = f(\alpha)$. Applying the division algorithm in the ring of polynomials over k, we find $f(x) = q(x)m(x) + g(x)$ where q and g are polynomials over k with $\deg(g) < \deg(m) = n$. Substituting $x = \alpha$, we find $\beta = f(\alpha) = g(\alpha)$, which is in the span of B. So B spans $k(\alpha)$, and thus is a basis. □

Let $\alpha \in K$ be algebraic. As observed earlier, a k-homomorphism $\phi : k(\alpha) \to L$ sends α to a root of its minimal polynomial. Moreover from the k-algebra structure of ϕ, specifying the image of α uniquely determines the k-homomorphism. Conversely, there is a k-homomorphism that sends α to any root. Thus with Proposition 2.7 there are at most $\deg(k(\alpha)|k)$ k-homomorphisms $k(\alpha) \to L$.

In general, a k-homomorphism $k(S) \to L$ where S is a set of algebraic elements sends each element of S to a root of its minimal polynomial and is uniquely determined by where S is sent. However, S must be a minimal generating set of $k(S)$ as an algebra for there to be a k-homomorphism for an arbitrary choice of roots.

We have now described the basic structure of finite extensions. The basic structure of infinite extensions is a short jump up from finite extensions. Now fix an infinite extension $K|k$, and consider the category of subextensions of K. If $L|k$ is an infinite subextension of K, it is easily seen that L is the inverse limit of the system of all subextensions of L with the inclusions taken as the morphisms. Furthermore, noting that every element of L is in a finite subextension (simply adjoin the element to k), L is in fact the inverse limit of the system of *finite* subextensions of L. Hence L is in some sense *profinite*. This observation will be crucial to the extension of finite Galois theory to infinite Galois theory.

3. Normality, Separability, and Closures

Galois theory will require two "niceness" conditions on (algebraic) extensions: normality and separability. Both of these admit several useful and equivalent definitions; we will now give intrinsic definitions of these properties, and after discussing certain universal extensions we will give alternative definitions that will also be of use.

Definition 3.1. An extension $L|k$ is a *splitting field* of a set P of polynomials over k if it is a minimal extension of k such that every polynomial in P factors linearly over L. An (algebraic) extension $M|k$ is a *normal extension of* k if M is a splitting field of some set of polynomials over k.

A splitting field is intuitively the extension generated by "all" the roots of a set of polynomials. Note that by (carefully) sending roots to roots, any two splitting fields of a set of polynomials are k-isomorphic. Further, fixing an extension $K|k$, if K has a subextension L that is normal, a k-homomorphism $L \to K$, sending roots to roots, must have an image contained in L. In fact, restricting its codomain to L it is a k-automorphism of L as we will see. Thus, as long as a containing extension is specified, there is only one splitting field of a given set of polynomials.

Definition 3.2. An algebraic element α of an extension $L|k$ is *separable* if its minimal polynomial is separable, that is, has no repeated roots in a splitting field of the minimal polynomial. An (algebraic) extension $L|k$ is a *separable* extension if every element of L is separable.

As examples, all algebraic extensions of a finite field or a field with characteristic zero are separable. On the other hand, the splitting field of the polynomial $f(X) = X^p - T$ over the rational function field $k(T)$ is inseparable, where k is a field with characteristic $p > 0$. Both these facts can be demonstrated using a simple test with the formal derivative, which is discussed in section 13.5 of [1].

A useful fact about separability of elements is that it is preserved by addition and multiplication; that is, the sum and product of two separable elements of an extension are both separable. Thus if an extension is generated by a separable set of elements, that extension is separable.

Definitions 3.3. An extension $L|k$ that is both separable and normal is called a *Galois extension of* k. In this case, the group of k-automorphisms of L, generally denoted $Aut(L|k)$, is called the *Galois group of* L *over* k and is denoted $Gal(L|k)$.

Before proceeding with Galois theory, we will construct two "universal" extensions. Up to this point, it has been necessary to preface most statements about field

extensions with the choice of a containing field extension such that all extensions in questions are subextensions. This gives rise to the question of whether there exist "universal" algebraic extensions, which precisely contain "all possible elements" algebraic or separable over a base field. For example, the complex numbers are precisely the set of "all" algebraic or separable elements over the real numbers. In fact, it is possible to demonstrate the existence of such universal extensions for any field.

Definitions 3.4. An algebraic extension $F|k$ is an *algebraic closure of* k if every polynomial over k has a root in F. A field k is *algebraically closed* if it is an algebraic closure of itself.

Using Zorn's lemma, it can be shown that every field has an algebraic closure. This is worked out by Dummit and Foote in section 13.4 of [1]. By induction using the definition, if F is an algebraic closure of k, any polynomial over k factors linearly over F, that is, F contains "all" roots of all polynomials over k. Thus F has no proper k-algebraic extensions, and so is a candidate for a "universal" algebraic extension. The following result confirms this hypothesis.

Theorem 3.5. (Isomorphism Extension). *If $L|k$ is an algebraic extension, $\phi : k \to F$ a field isomorphism, and $\bar{F}$ an algebraic closure of F, then there exists an embedding $\bar{\phi} : L \to \bar{F}$ such that the following diagram commutes, the vertical arrows being the inclusions.*

$$\begin{array}{ccc} L & \xrightarrow{\bar{\phi}} & \bar{F} \\ \uparrow & & \uparrow \\ k & \xrightarrow[\cong]{\phi} & F \end{array}$$

With the following lemma, the isomorphism extension theorem establishes a (non-unique) field isomorphism between any two algebraic closures of a field.

Lemma 3.6. *If $L|k$ is an algebraic extension and $\bar{k}$ an algebraic closure of k, then $\bar{k}$ is an algebraic closure of L. In particular, an algebraic closure of a field is* algebraically closed*; that is, it is its own algebraic closure.*

Proof. The basis of this lemma is that if $K|L$ and $L|k$ are algebraic extensions, then so is $K|k$. See section 13.4 of [1] for a full proof. □

Corollary 3.7. *Given a field k and two algebraic closures $\bar{k}$ and $\bar{k}'$ of k, there is a field isomorphism $\bar{k}' \to \bar{k}$.*

Proof. Extend $id : k \to k$ to an embedding $\phi : \bar{k} \to \bar{k}'$. Then $\phi^{-1} : \phi(\bar{k}) \to \bar{k}$ is an isomorphism, hence surjective. By the lemma, $\bar{k}$ is its own algebraic closure, so as $\bar{k}'$ is an extension of $\phi(\bar{k})$, we can extend ϕ^{-1} to an embedding $\psi : \bar{k}' \to \bar{k}$. But as ϕ^{-1} is surjective, so must be the extended map ψ. Thus ψ is an isomorphism. □

Thus the study of the algebraic extensions of a given field can be restricted to the study of the subextensions of a fixed algebraic closure of that field, with essentially no loss of information or structure.

The application of the isomorphism extension theorem to extend ϕ^{-1} in the above proof admits a very useful generalization.

Proposition 3.8. *Let $M|L|k$ be a tower of extensions, and $\phi : L \to \bar{k}$ a k-homomorphism. Then there exists a k-homomorphism $\bar{\phi} : M \to \bar{k}$ that restricts to ϕ on L.*

Proof. By Lemma 3.6, $\bar{k}$ is an algebraic closure of $\phi(L)$. Taking M as an extension of L, the isomorphism $\phi : L \to \phi(L)$ extends to a field embedding $\bar{\phi} : M \to \bar{k}$. As ϕ fixes k, so does $\bar{\phi}$, so $\bar{\phi}$ is a k-homomorphism. □

The other type of "universal" extension that will be important is a separable closure.

Definition 3.9. A separable extension $L|k$ is a *separable closure of k* if there is no separable extension of k properly containing it.

Immediately from the definition, a separable closure is equivalently a splitting field of all separable (irreducible) polynomials. That is, a separable closure is normal, hence Galois.

Definition 3.10. The *absolute Galois group* $Gal(k)$ of a field k is $Gal(k_s|k)$, where k_s is a separable closure of k.

Choosing an algebraic closure, there is a unique separable closure contained in that algebraic closure: the inverse limit of all (finite) separable subextensions. More simply, the separable closure is the set of all separable elements of the algebraic closure.

Notation 3.11. From this point onwards, algebraic extensions of a field k will be assumed to be subextensions of a chosen algebraic closure $\bar{k}$. We will call this *the* algebraic closure of k, with associated separable closure $\bar{k}_s$, called *the* separable closure of k.

Now it is possible to revisit the definitions of normal and separable given above and provide equivalent conditions in terms of homomorphisms into the algebraic closure.

Theorem 3.12. *An algebraic extension $L|k$ is normal if and only if for every k-homomorphism $\phi : L \to \bar{k}$, we have $\phi(L) \subseteq L$, or equivalently $\phi(L) = L$.*

Proof. The proof of this statement revolves around the fact that k-homomorphisms send a root of a polynomial over k to some root of the same polynomial. We will apply this to minimal polynomials.

Suppose $L|k$ is normal. Then L is the splitting field of some set P of polynomials over k, and in fact $L = k(S)$, where S is the set of roots in $\bar{k}$ of polynomials in P. Any k-homomorphism $\phi : L \to \bar{k}$ sends S into S, so $\phi(L) \subseteq L$.

Suppose instead that $\phi(L) \subseteq L$ for every $\phi : L \to \bar{k}$. It is sufficient to show that for any element α of L, L contains every root of the minimal polynomial of α, as then L must be the splitting field of the set of the minimal polynomials of the elements of L. Let α be an element of L, and β a root of the minimal polynomial of α. Then as discussed previously, there is a k-homomorphism $\psi : k(\alpha) \to \bar{k}$ sending α to β. By Proposition 3.8, we can extend ψ to $\bar{\psi} : L \to \bar{k}$. As ψ is a k-homomorphism, so is $\bar{\psi}$. Hence we have $\beta \in \psi(k(\alpha)) \subseteq \bar{\psi}(L) \subseteq L$. Therefore as noted L is a normal extension of k.

Finally it remains to show that in fact $\phi(L) = L$ when L is normal. Observe first that $\phi(L)$ is also normal, being a splitting field of the same polynomials as is

L since ϕ fixes k. As ϕ is an embedding, we can define an inverse k-homomorphism $\phi^{-1} : \phi(L) \to L \subset \bar{k}$. By the normality of $\phi(L)$, we find $L = \phi^{-1}(\phi(L)) \subseteq \phi(L)$. Thus $\phi(L) = L$. □

Definition 3.13. Given two extensions $L|k, M|k$, we denote the set of k-homomorphisms $L \to M$ by $Emb_k(L, M)$. For an algebraic extension L, the *separable degree of L over k* is the cardinality of $Emb_k(L, \bar{k})$, and is denoted $\text{sepdeg}(L|k)$.

Note that the separable degree of a finite extension is finite: there is a finite generating set of the extension, and each element of the generating set can only be sent to one of the roots of its minimal polynomial, which is a finite set.

Proposition 3.14. *Separable degree is multiplicative. That is, for finite extensions $M|L|k$, we have* $\text{sepdeg}(M|k) = \text{sepdeg}(M|L)\,\text{sepdeg}(L|k)$.

Proof. For an algebraic extension $L|k$, there is a canonical bijection

$$Emb_k(L, \bar{k}) \to Aut(\bar{k}|k)/Aut(\bar{k}|L)$$
$$\phi \mapsto \bar{\phi}Aut(\bar{k}|L).$$

The proof of this is entirely analogous to the proof that η is well-defined and an isomorphism in Theorem 6.7 below. Since they are (finite) coset spaces, we find that $Aut(\bar{k}|L)/Aut(\bar{k}|M) \times Aut(\bar{k}|k)/Aut(\bar{k}|L)$ and $Aut(\bar{k}|k)/Aut(\bar{k}|M)$ have the same cardinality. So $Emb_L(M, \bar{k}) \times Emb_k(L, \bar{k})$ and $Emb_k(M, \bar{k})$ have the same cardinality. □

Theorem 3.15. *The separable degree of a finite extension is less than or equal to its degree, with equality holding if and only if the extension is separable.*

Proof. We first consider the case of $k(\alpha)$ for some α in $\bar{k}$. As previous discussed, for a k-homomorphism $k(\alpha) \to \bar{k}$, the image of α uniquely determines the k-homomorphism, and must be a root of the minimal polynomial of α. Hence $\text{sepdeg}(k(\alpha)|k) \leq \deg(k(\alpha)|k)$, with equality holding if and only if the minimal polynomial of α is separable if and only if $k(\alpha)$ is separable.

Let L be a finite extension. Take $\alpha_1, \ldots \alpha_n$ in $\bar{k}$ such that $L = k(\alpha_1, \ldots \alpha_n)$. Note that L is separable if and only if all of $\alpha_1, \ldots, \alpha_n$ are separable. Separability is preserved over towers of extensions, as shown in Corollary 4.4 below. Thus we can induct on n using the multiplicativity of degree and separable degree, and the first result. □

4. Finite Galois Theory

Definition 4.1. Let L, K be extensions of k, and H a subset of $Emb_k(L, K)$. Then the *subfield fixed by H* is $L^H = \{x \in L \mid \sigma(x) = x \ \forall \sigma \in H\}$.

This definition implicitly asserts that L^H is a field; this is easy to verify.

Theorem 4.2. *An algebraic extension $K|k$ is Galois if and only if $K^{Aut(K|k)} = k$.*

Proof. Suppose $K|k$ is Galois. Any k-homomorphism fixes k, so we have $k \subseteq K^{Aut(K|k)}$.

We now show the reverse inclusion. Take α in $K - k$. Then the minimal polynomial of α has degree greater than one and is separable, hence has a root β in $\bar{k}$ other than α. Let $\phi : k(\alpha) \to \bar{k}$ be the k-homomorphism sending α to β. Using Proposition

3.8, extend ϕ to $\bar{\phi} : K \to \bar{k}$. As $K|k$ is normal, $\bar{\phi}(K) = K$, so $\bar{\phi}$ is a k-automorphism of K, and $\bar{\phi}$ does not fix α. Thus $K^{Aut(K|k)} = k$.

Now we prove the other direction. Suppose $K|k$ satisfies $K^{Aut(K|k)} = k$. Take α in K. Let $B = \{\sigma(\alpha)|\sigma \in Gal(K|k)\}$. Each element of B is a root of the minimal polynomial of α, so B is finite. Let $f_\alpha(x) = \prod_{\beta \in B}(x - \beta)$. Then f_α is fixed under $Aut(K|k)$ (extending the action of $Aut(K|k)$ to polynomials); so f_α must have coefficients in k. But f_α is separable by construction, hence α is separable. Finally, K must be the splitting field of $\{f_\alpha\}_{\alpha \in K}$. Thus $K|k$ is Galois. □

Proposition 4.3. *Let $K|L|k$ be a tower of algebraic extensions. Then for any α in K, the minimal polynomial of α over L divides the minimal polynomial of α over k.*

Proof. The minimal polynomial of α over k has α as a root and is also a polynomial over L. Thus it is divisible by the minimal polynomial of α over L. □

Corollary 4.4. *Let $K|L|k$ be a tower of extensions, where $K|k$ is separable. Then $K|L$ is separable.*

Proof. Any divisor of a separable polynomial is separable. So with the above, if α in K is separable over k, then it is separable over L. □

Proposition 4.5. *Let $K|L|k$ be a tower of extensions, where $K|k$ is normal. Then $K|L$ is normal.*

Proof. If $\phi : K \to \bar{k}$ is an L-homomorphism, then as $k \subset L$, ϕ is also a k-homomorphism. Hence by Theorem 3.12 $\phi(K) = K$, and thus $K|L$ is normal. □

Theorem 4.6. *Let $K|L|k$ be a tower of extensions, where $K|k$ is Galois. Then $K|L$ is Galois, and $Gal(K|L)$ is a subgroup of $Gal(K|k)$. Further, $L|k$ is Galois if and only if $Gal(K|L)$ is a normal subgroup of $Gal(K|k)$, in which case $Gal(L|k) \cong Gal(K|k)/Gal(K|L)$.*

Proof. The first part is immediate from the previous two results, and that any map fixing L must then fix k, as $k \subset L$.

Suppose that $L|k$ is Galois. Then there is a homomorphism $\rho : Gal(K|k) \to Gal(L|k)$ given by restriction to L. But the kernel of this homomorphism is evidently $Gal(K|L)$: a map σ in $Gal(K|k)$ is in the kernel of ρ if and only if σ restricts to the identity on L if and only if σ is a L-homomorphism. Thus $Gal(K|L)$ is a normal subgroup of $Gal(K|k)$, and $Gal(L|k) \cong Gal(K|k)/Gal(K|L)$.

Suppose conversely that $Gal(K|L)$ is normal in $Gal(K|k)$. Every subextension of K is separable over k (separability over a fixed field being an element-wise property), so it suffices to show that $L|k$ is normal. Take a k-homomorphism $\phi : L \to \bar{k}$. Extend ϕ to $\bar{\phi} : K \to \bar{k}$. As K is normal, the image of $\bar{\phi}$ is K, and $\bar{\phi} \in Gal(K|k)$. We find

$$\phi(L) = \bar{\phi}(L) = K^{\bar{\phi}Gal(K|L)\bar{\phi}^{-1}} = K^{Gal(K|L)} = L$$

using Theorem 4.2. Thus L is normal over k by Theorem 3.12. □

It is now possible to state and prove the Fundamental Theorem of Galois Theory for finite extensions.

Theorem 4.7. (Finite Fundamental Theorem of Galois Theory) *Let $K|k$ be a finite Galois extension. Then the maps*

$$L \mapsto Gal(K|L),$$
$$H \mapsto K^H$$

establish a one-to-one correspondence between subextensions L of K and subgroups H of $Gal(K|k)$. Further, this correspondence reverses inclusions.

Proof. That $L = K^{Gal(K|L)}$ for any subextension L follows immediately from Theorem 4.2.

That $H \subseteq Gal(K|K^H)$ is also immediate: if σ in $Gal(K|k)$ is in H, then σ restricts to the identity on K^H, hence σ is in $Gal(K|K^H)$. The reverse inclusion needs substantially more work to prove, and requires the finiteness of K. Dummit and Foote use the notion of characters of a group to provide a proof in section 14.2 of [1].

For the reversal of inclusions, if $K|M|L|k$, then the inclusion $L \subset M$ induces an inclusion $Gal(K|M) \subset Gal(K|L)$ since any automorphism fixing M automatically fixes L. Conversely, if $H \subset G \subset Gal(K|k)$ are subgroups, then an element of K fixed by all of G must be fixed by H. So $K^G \subset K^H$. □

5. Infinite Galois Theory

Extending the Fundamental Theorem to infinite extensions will require some profinite group theory. As the theory in itself is somewhat tangential to the topic of this paper, some of the necessary results will be stated here without proof. A more thorough treatment including these proofs is found in [2].

Definition 5.1. A *profinite group* is a topological group G that is the inverse limit of an inverse system of finite groups. The topology on G is the inverse limit topology of its finite quotients, endowing the quotients with the discrete topology. Namely, it is the coarsest topology such that all the quotient maps are continuous.

Remark 5.2. Any profinite group G is the inverse limit of its finite quotients as a group, hence the choice to canonically topologize it as such. In fact, any inverse system of finite groups having G as its inverse limit induces the same topology.

Proposition 5.3. *The open subgroups of a profinite group are exactly the closed subgroups of finite index.*

Proposition 5.4. *Let G be a profinite group. Under the quotient maps, the preimages of the identities of the finite quotients of G form a local basis for the identity of the profinite group.*

Proof. Each preimage of an identity is open, as the finite quotients of G are discrete. Let V be an open subset of G containing the identity. Suppose V does not contain the preimage of the identity of some finite quotient of G. Then G has a finer topology than is strictly necessary to make all the finite quotient maps of G continuous, a contradiction. □

Theorem 5.5. *Let $K|k$ be Galois. Then $Gal(K|k)$ is isomorphic to the inverse limit of the system of $Gal(L|k)$ for finite Galois subextensions $L|k$; the morphisms of this system are the quotients induced by the restriction homomorphism, as in*

Theorem 4.6. Finally, the local basis of the identity in the previous proposition is the set of $Gal(K|L)$ for finite subextensions L.

So the "profinite" structure of field extensions that we observed earlier induces a profinite structure of the Galois groups. This allows the Fundamental Theorem to be generalized to infinite extensions.

Theorem 5.6. (Fundamental Theorem of Galois Theory) *Let $K|k$ be a Galois extension. Then the maps*

$$L \mapsto Gal(K|L),$$
$$H \mapsto K^H$$

establish a one-to-one correspondence between subextensions L of K and closed *subgroups H of $Gal(K|k)$. Further, this correspondence reverses inclusions.*

Proof. The following proof is adapted from that of Szamuely in [2].

The only portion of the proof for the finite case that was dependent on the finiteness of the extension was to show that $Gal(K|K^H) \subseteq H$. Thus all that must be proved is this inclusion, and that $Gal(K|L)$ is closed for all subextensions L.

For the latter, let A be the set of finite subextensions of L. Recall that L is the inverse limit of its finite subextensions, that is, the field compositum, which is the smallest subfield of $\bar{k}$ containing $\bigcup_{M\in A} M$. However, for all α in L, we have $\alpha \in k(\alpha) \in A$, hence $L = \bigcup_{M\in A} M$. For all M in A, $Gal(K|M)$ is a finite subgroup, hence closed. So then

$$Gal(K|L) = \bigcap_{M\in A} Gal(K|M)$$

is closed.

For the former, let H be a subgroup of $Gal(K|k)$. Take the local basis

$$\{Gal(L|K^H) \mid L \text{ is a finite extension of } K^H\}$$

of the identity of $Gal(K|L)$. Take σ in $Gal(K|K^H)$ and a finite extension L of K^H. Let

$$\rho : H \to Gal(L|K^H) \cong Gal(K|K^H)/Gal(K|L)$$

be the projection induced by the restriction homomorphism (see Theorem 4.6). Suppose ρ is not surjective. Then $L^{\rho(H)} \supsetneq K^H$, applying the Fundamental Theorem in the finite case. But this implies that there is at least one element of L that is not in K^H, and is not moved by the action of H, a contradiction. So ρ is surjective. Importantly, there is some element of H sent to the restriction of σ to K^H, implying

$$\sigma Gal(K|L) \cap H \neq \emptyset.$$

So with Theorem 5.5, σ is in the closure $\bar{H}$ of H. So $Gal(K|K^H) \subseteq \bar{H}$ in general, whence $Gal(K|K^H) \subseteq H$ when H is closed. □

6. The Galois Anti-Isomorphism

Now that we have proven the Fundamental Theorem for an arbitrary Galois Extension, we can construct an anti-isomorphism connecting separable extensions to transitive $Gal(k)$-sets. First we will name and define the relevant categories, and introduce some simplifying notation.

Definitions 6.1. For a field k, denote by $Sep(k)$ the category of subextensions of k_s. For a profinite group G, denote by $Trans(G)$ the category of transitive left G-sets with G-equivariant maps as morphisms. Denote by $Coset(G)$ the full subcategory whose objects are the left coset spaces of *closed* subgroups of G.

Notation 6.2. For a field k, let G_k denote the absolute Galois group of k. Note in particular that if $L|k$ is a separable extension, then $G_L = Gal(L) = Gal(k_s|L)$.

First we will define a contravariant functor $\mathcal{F} : Sep(k) \to Coset(G_k)$. Let $L|k$ be a separable extension. By the Fundamental Theorem $G_L = Gal(k_s|L)$ is a closed subgroup of G_k. So let

$$\mathcal{F}L = G_k/G_L.$$

For a k-homomorphism $\phi : L \to M$ between separable extensions, let

$$\mathcal{F}\phi : \mathcal{F}M \to \mathcal{F}L : \psi G_M \mapsto \psi\bar{\phi}G_L,$$

where ψ is a coset representative, and $\bar{\phi} : k_s \to k_s$ is an extension of ϕ.

Proposition 6.3. *As defined, $\mathcal{F}$ is a well-defined faithful contravariant functor.*

Proof. First we will show that $\mathcal{F}$ is well-defined. Let $\phi : L \to M$, and choose extensions $\bar{\phi}$ and $\bar{\phi}'$ of ϕ. Take $\psi G_M \in \mathcal{F}M$. We have $\bar{\phi}|_L = \bar{\phi}'|_L$, so $\bar{\phi}^{-1}\bar{\phi}'|_L = id_L$, and $\bar{\phi}^{-1}\bar{\phi}' \in G_L$. Thus

$$\psi\bar{\phi}G_L = \psi\bar{\phi}\bar{\phi}^{-1}\bar{\phi}'G_L = \psi\bar{\phi}'G_L,$$

and $\mathcal{F}$ does not depend on the choice of extension of ϕ. Suppose $\psi G_M = \psi' G_M$. Then $\psi^{-1}\psi' \in G_M$, that is, $\psi^{-1}\psi' G_M = G_M$. Applying $\mathcal{F}\phi$, we find $\psi^{-1}\psi'\phi G_L = \phi G_L$, and $\psi'\phi G_L = \psi\phi G_L$. So $\mathcal{F}$ does not depend on the coset representative, and is well-defined.

Further, for a coset representative ψ and $\alpha \in G_k$,

$$\mathcal{F}\phi(\alpha\psi G_M) = \alpha\psi\bar{\phi}G_L = \alpha\mathcal{F}(\psi G_m)$$

so $\mathcal{F}\psi$ is G_k-equivariant. We find similarly from the associativity of composition and the definition of $\mathcal{F}$ that $\mathcal{F}$ preserves composition, and thus is a contravariant functor.

Suppose k-homomorphisms $\phi, \psi : L \to M$ are such that $\mathcal{F}\phi = \mathcal{F}\psi$. Then in particular $\mathcal{F}\phi(G_M) = \mathcal{F}\psi(G_M)$, that is, $\bar{\phi}G_L = \bar{\psi}G_L$. So $\bar{\psi}^{-1}\bar{\phi} \in G_L$, and $\bar{\psi}^{-1}\bar{\phi}|L = id_L$. Thus $\phi = \bar{\phi}|L = \bar{\psi}|L = \psi$, and $\mathcal{F}$ is faithful. □

Now we wish to construct a contravariant functor $\mathcal{G} : Coset(G_k) \to Sep(k)$ that inverts $\mathcal{F}$. How to invert on objects is evident: by the Fundamental Theorem, any object H in $Coset(G_k)$ is of the form G_k/G_L for some unique separable extension L in $Sep(k)$; let $\mathcal{G}H = L$. Recovering morphisms will require some more work.

Theorem 6.4. *Every morphism $H \to J$ in $Coset(G_k)$ is induced under $\mathcal{F}$ by a unique k-homomorphism $\mathcal{G}J \to \mathcal{G}H$. Equivalently, $\mathcal{F}$ is a full functor.*

Proof. Let $M = \mathcal{G}H$ and $L = \mathcal{G}J$. Take $\eta : H \to J$, and take a representative $\phi \in G_k$ such that $\eta(G_M) = \phi G_L$. As η is G_k-equivariant, the stabilizer in H of G_M, which is G_M itself, is a subset of the stabilizer in J of $\eta(G_M)$, which is $\phi G_L \phi^{-1}$. Applying the Fundamental Theorem, we reverse the inclusion to

$$\phi(L) = k_s^{\phi G_L \phi^{-1}} \subseteq k_s^{G_M} = M.$$

Thus $\phi|_L$ is a k-homomorphism $L \to M$. Moreover, $\mathcal{F}\phi|_L = \eta$, as $\mathcal{F}\phi|_L(G_M) = \eta(G_M)$, and a G_k-equivariant map of transitive G_k-sets is specified uniquely by the image of a single element. As $\mathcal{F}$ is faithful, $\phi|L$ is unique. □

So $\mathcal{F}$ is fully faithful, and we can define the action of $\mathcal{G}$ on morphisms as the inverse of $\mathcal{F}$.

Theorem 6.5. *The categories $Sep(k)$ and $Coset(G_k)$ are anti-isomorphic.*

Proof. Immediately from the definitions of $\mathcal{F}$ and $\mathcal{G}$, we have $\mathcal{F}\mathcal{G} = id_{Coset(G_k)}$ and $\mathcal{G}\mathcal{F} = id_{Sep(k)}$. □

Remark 6.6. This anti-isomorphism is a stronger statement than the Fundamental Theorem. The action of objects under $\mathcal{F}$ and $\mathcal{G}$ precisely induces the one-to-one correspondence in the Fundamental Theorem. The action on morphisms, in addition to inducing the reversal of inclusions, establishes a correspondence that is not in the Fundamental Theorem. Note that in fact the definition of $\mathcal{F}$ and $\mathcal{G}$ on objects was trivial given the Fundamental Theorem, while their definitions and properties on morphisms required additional work.

An observation central to Szamuely's anti-equivalence is that for an extension $L|k$, the set $Hom(L, k_s) = Emb_k(L, k_s)$ is a transitive left G_k-set under composition, and in fact the functor $Hom(-, k_s)$ can be taken to have codomain $Trans(G_k)$. Intuitively, there is a natural correspondence between elements of $Hom(L, k_s)$ and elements of G_k/G_L, a fact that we can make precise.

Theorem 6.7. *There is a natural isomorphism between $Hom(-, k_s)$ and $\mathcal{F}$ in $Trans(G_k)$.*

Proof. Take a separable extension $L|k$. Let $\eta : Hom(L, k_s) \to \mathcal{F}L : \phi \mapsto \bar{\phi}G_L$ where $\bar{\phi}$ is an extension of ϕ. Then η is G_k-equivariant.

Suppose $\bar{\phi}$ and $\bar{\phi}'$ are extensions of $\phi \in Hom(L, k_s)$. Then $\bar{\phi}|_L = \bar{\phi}'|_L$, so $\bar{\phi}^{-1}\bar{\phi}' \in G_L$. Thus $\bar{\phi}G_L = \bar{\phi}'G_L$, and η is well-defined.

For any element ψG_L of $\mathcal{F}L$, we see from the definition that $\eta(\psi|_L) = \psi G_L$. So η is surjective.

Suppose $\phi, \psi \in Hom(L, k_s)$ are such that $\eta(\phi) = \eta(\psi)$. That is, $\bar{\phi}G_L = \bar{\psi}G_L$. So $\bar{\phi}^{-1}\bar{\psi} \in G_L$, and $\bar{\phi}^{-1}\bar{\psi}|_L = id_L$. Hence $\phi = \bar{\phi}|_L = \bar{\psi}|_L = \psi$, and η is injective. Thus η is an isomorphism.

Take a k-homomorphism $\phi : L \to M$ and $\psi \in Hom(M, k_s)$. Let Φ be the image of ϕ under $Hom(-, k_s)$. Then

$$\eta(\Phi(\psi)) = \eta(\psi\phi) = \overline{\psi\phi}G_L,$$

and

$$\mathcal{F}\phi(\eta(\psi)) = \mathcal{F}\phi(\bar{\psi}G_M) = \bar{\psi}\bar{\phi}G_L.$$

Evidently $\bar{\psi}\bar{\phi}$ is an extension of $\psi\phi$, so $\eta(\Phi(\psi)) = \mathcal{F}\phi(\eta(\psi))$, and η is natural. □

Instead of this anti-isomorphism, Szamuely demonstrates an anti-equivalence important to Grothendieck's treatment of Galois theory in terms of étale algebras. This anti-equivalence follows immediately from the above.

Corollary 6.8. (Szamuely's Anti-Equivalence). *Fix a field k with separable closure k_s. The category of finite separable extensions of k under k_s is anti-equivalent to the category of finite transitive left G_k-sets with continuous G_k-action via the functor $Hom(-, k_s)$.*

Proof. Requiring that the G_k-action be continuous amounts to requiring that the stabilizer of the action is an open subgroup: the topology on a finite transitive G_k-set X is discrete (being given the quotient topology), but then the preimage under the action of a single element must be open, and is the stabilizer. By Proposition 5.3, the stabilizer is closed. Since X is isomorphic to the left coset space of its stabilizer, it is isomorphic in $Trans(G_k)$ to an object in $Coset(G_k)$, which is the image of $\mathcal{F}$. So using the natural isomorphism between $Hom(-, k_s)$ and $\mathcal{F}$, we find that $Hom(-, k_s)$ is fully faithful, and essentially surjective when restricted to the desired domain and codomain. □

Acknowledgments. I would like to thank my mentor, Asilata Bapat, for her help with this paper. Her guidance on both the content and style of this paper have been invaluable.

References

[1] David Dummit and Richard Foote. Abstract Algebra. 3rd edition. John Wiley and Sons, Inc. 2004.

[2] Tamás Szamuely. Galois Groups and Fundamental Groups. `http://www.renyi.hu/~szamuely/fg.pdf`