AN INTRODUCTION TO GALOIS THEORY

JULIAN MANASSE-BOETANI

Abstract. This paper explores Galois Theory over the complex numbers, building up from polynomials to corresponding field extensions and examining these field extensions. Ultimately, the paper proves the Fundamental Theorem of Galois Theory and provides a basic example of its application to a polynomial.

Contents

1. Introduction

In this paper, we will explicate Galois theory over the complex numbers. We assume a basic knowledge of algebra, both in the classic sense of division and remainders of polynomials, and in the sense of group theory. Although the build-up to the result which we want is quite long, the subject matter along with its historical place in mathematics provide strong motivation. Galois theory has applications in classic problems such as squaring the circle and determining solvability of polynomials (its original purpose), as well as in number theory, differential equations, and algebraic geometry. Moreover, in the history of mathematics, Galois theory was one of the things which sparked the modern understanding of groups, and as a result Galois is regarded as one of the founders of modern algebra. We will define more terms later, but to give an idea of where we are going, consider the polynomial $x^2 + 2 = 0$. It's roots are plus or minus $i\sqrt{2}$. The smallest subfield of $\mathbb{C}$ which contains these roots is $\mathbb{Q}(i, \sqrt{2}) = \{\sqrt{2}a + bi \mid a, b \in \mathbb{Q}\}$, which has 4 subfields: $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(i, \sqrt{2})$. Now, consider all of the automorphisms

Date: August 30, 2013.

of $\mathbb{Q}(i, \sqrt{2})$ which fix $\mathbb{Q}$. There is the identity, I, one which sends $\sqrt{2}$ to $-\sqrt{2}$ and fixes i, τ, one which sends i to $-i$ and fixes $\sqrt{2}$, σ, and one which sends i to $-i$ and $\sqrt{2}$ to $-\sqrt{2}$, π. Thus, the functions I, τ, σ,and π form a group under composition of maps, called the Galois group, which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Moreover, considering the subgroups of the Galois group, we can see that each fixes some subfield. For example, the subgroup formed by I and τ fixes $\mathbb{Q}(i)$. This is an elementary example of the correspondence between the subfields (called intermediate fields) of a field extension and the subgroups of the Galois group.

2. Irreducibility of Polynomials

We begin by defining the notion of irreducibility and proving some basic theorems about irreducibility for later use.

Definition 2.1 (Divisor)**.** Let f, g be polynomials over a field K. f divides g if there exists a polynomial h over K such that $g = fh$. This is notated by $f \mid g$.

Definition 2.2 (Degree)**.** Let f be a polynomial over $\mathbb{C}$ such that $f \neq 0$. The degree of f is the power of the highest term with non-zero coefficient. The degree of a polynomial f is written ∂f

Definition 2.3 (Reducible)**.** Let f be a polynomial over a subring R of $\mathbb{C}$. f is reducible if it is the product of two polynomials over R of smaller degree. Otherwise f is irreducible.

Theorem 2.4. *Any polynomial over a subring R of $\mathbb{C}$ is a product of irreducible polynomials over R.*

Proof. Proof by induction on the degree of polynomials. Polynomials of degree 0 and 1 are clearly irreducible, so we have our base case. Now assume that polynomials of degree up to $n-1$ are the product of irreducible polynomials over R. Let f be a polynomial over R with $\partial f = n$. If f is irreducible, the theorem is proven. If f is not irreducible, then it is reducible, so $f = hk$, where h, k are polynomials over R with $\partial h, \partial k < n$. By the inductive hypothesis, h and k are the product of irreducible polynomials over R, so f is also a product of irreducible polynomials over R. □

Lemma 2.5 (Gauss' Lemma)**.** *If a polynomial f over $\mathbb{Z}$ is irreducible over $\mathbb{Z}$, then f as a polynomial over $\mathbb{Q}$ is irreducible over $\mathbb{Q}$*

Proof. Proof by contradiction. Let f be a polynomial over $\mathbb{Z}$. Assume f is irreducible over $\mathbb{Z}$, but is reducible over $\mathbb{Q}$ as a polynomial over $\mathbb{Q}$. This implies $f = gh$ where g, h are polynomials over $\mathbb{Q}$ with $\partial g, \partial h < \partial f$. Multiplying $f = gh$ through by the denomenators of each term of g and h gives $nf = g'h'$ where $n \in \mathbb{Z}$ and g', h' are polynomials over $\mathbb{Z}$. Let p be a prime factor of n. If $g' = g_0 + g_1 t + \ldots + g_n t^n$ and $h' = h_0 + h_1 + \ldots + h_n t^n$, then p divides all the coefficients of g' or all the coefficients of h'. If not, then there exist smallest values i, j such that $p \nmid g_i$ and $p \nmid h_j$. But p divides the coefficient of t^{i+j} in $g'h'$, which is $h_0 g_{i+j} + h_1 g_{i+j-1} + \ldots + h_j g_i + \ldots + h_{i+j} g_0$. By our choice of i and j, p divides every term except perhaps $h_j g_i$. But p divides the whole sum, so $p \mid h_j g_i$, contradiction because $p \nmid h_j$ and $p \nmid g_i$. So without loss of generality, p divides every coefficient g_i, which implies $g' = pg''$ where g'' is a polynomial over $\mathbb{Z}$ with the same degree as g'. Let $n = pn_1$ which implies $pn_1 f = pg''h'$ which implies $n_1 f = g''h'$. Continuing

the process removes all primes from n, giving $f = g^*h^*$ where $\partial g^* = \partial g$, $\partial h^* = \partial h$, and $g^*, h^* \in \mathbb{Z}[t]$ which implies f is reducible over $\mathbb{Z}$. □

The next theorem provides a very practical way to determine irreducibility for many polynomials with integer coefficients. Note that any polynomial over $\mathbb{Q}$ can be converted into a polynomial over $\mathbb{Z}$ multiplied by a constant in $\mathbb{Q}$, which expands the applicability of the following theorem even further.

Theorem 2.6 (Eisenstein's Criterion)**.** *Let $f(t) = a_0 + a_1t + \ldots + a_nt^n$ be a polynomial over $\mathbb{Z}$. Suppose there exists some prime q such that:*

(1) $q \nmid a_n$
(2) $q \mid a_i (i = 0, \ldots, n-1)$
(3) $q^2 \nmid a_0$

Then f is irreducible over $\mathbb{Q}$.

Proof. Proof by contradiction. By Gauss's Lemma, it suffices to that f is irreducible over $\mathbb{Z}$. Assume by way of contradiction that $f = gh$, where

$$g = b_0 + b_1t + \ldots + b_rt^r$$

and

$$h = c_0 + c_1t + \ldots + c_st^s$$

are polynomials of smaller degree over $\mathbb{Z}$. Then $r \geq 1, s \geq 1$, and $r+s = n$. Because $b_0c_0 = a_0$ by condition 1 on f, we have $q \mid b_0$ or $q \mid c_0$. By condition 3 on f, q cannot divide both b_0 and c_0, so without loss of generality let $q \mid b_0$ and $q \nmid c_0$. If all b_j are divisible by q, then a_n is divisible by q, contrary to condition 1 on f. Let b_j be the first coefficient of g not divisible by q. Then

$$a_j = b_jc_0 + \ldots + b_0c_j$$

with $j < n$. This implies $q \mid c_0$ because $q \mid a_j, q \mid b_i (b = 0, \ldots, j-1)$, but $q \nmid b_j$. This is a contradiction, so f is irreducible. □

3. Field Extensions and Minimal Polynomials

Definition 3.1 (Field Extension)**.** Let L and K be subfields of $\mathbb{C}$. A field extension is a monomorphism $i : K \to L$, written $L : K$. We call L the large field and K the small field.

Example 3.2. The inclusion maps $i_1 : \mathbb{Q} \to \mathbb{R}$, $i_2 : \mathbb{R} \to \mathbb{C}$, and $i_3 : \mathbb{Q} \to \mathbb{C}$ are all field extensions

Definition 3.3. Let X be a subset of $\mathbb{C}$. Then the subfield of $\mathbb{C}$ generated by X is the intersection of all subfields of $\mathbb{C}$ that contain X.

Because every subfield of $\mathbb{C}$ contains $\mathbb{Q}$, we can use the notation

$$\mathbb{Q}(X)$$

for the subfield of $\mathbb{C}$ generated by X. In general, if $L : K$ is a field extension and $Y \subset L$, then the subfield of $\mathbb{C}$ generated by $K \cup Y$ is written $K(Y)$. Also, when X is a set of discrete elements we omit the set brackets.

Example 3.4. $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$

Definition 3.5 (simple extension)**.** A simple extension is a field extension $L : K$ such that $L = K(\alpha)$ for some $\alpha \in L$.

Warning 3.6. An extension may be simple without appearing to be. Consider $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This does not at first appear to be a simple extension. However, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ because $(\sqrt{2}+\sqrt{3})^3 = (5+\sqrt{2}\sqrt{3})(\sqrt{2}+\sqrt{3}) = 8\sqrt{2}+7\sqrt{3}$. Subtracting $7(\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ gives $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and subtracting $\sqrt{2}$ from $\sqrt{2} + \sqrt{3}$ gives $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Therefore this is a simple extension.

Definition 3.7 (monic)**.** A polynomial $f(t) = a_0 + a_1 t + \ldots + a_n t^n$ over a subfield K of $\mathbb{C}$ is monic if $a_n = 1$.

Definition 3.8 (algebraic)**.** Let K be a subfield of $\mathbb{C}$ and let $\alpha \in \mathbb{C}$. Then α is algebraic over K if there exists a nonzero polynomial p over K such that $p(\alpha) = 0$. Otherwise, α is transcendental over K.

Definition 3.9 (minimal polynomial)**.** Let $L : K$ be a field extension and suppose that $\alpha \in L$ is algebraic over K. Then the minimal polynomial of α over K is the unique monic polynomial m of smallest degree such that $m(\alpha) = 0$.

Example 3.10. $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ because if $p(t) = t^2 + 1$, $p(i) = 0$. $i \notin \mathbb{R}$, so no polynomial of degree 0 or 1 can have i as a root. Thus, because $p(t)$ is monic and degree 2, $p(t)$ must be the minimal polynomial for i over $\mathbb{R}$.

Definition 3.11. Two polynomials $a, b \in K[t]$ are congruent modulo m if $a(t)-b(t)$ is divisible by $m(t)$ in $K[t]$. This is written $a \equiv b (\text{mod } m)$.

Lemma 3.12. *Suppose $a_1 \equiv a_2 (mod\ m)$ and $b_1 \equiv b_2 (mod\ m)$. Then $a_1 + a_2 \equiv b_1 + b_2 (mod\ m)$ and $a_1 a_2 \equiv b_1 b_2 (mod\ m)$.*

Proof omitted.

Lemma 3.13. *Every polynomial $a \in K[t]$ is congruent modulo m to a unique polynomial of degree $< \partial m$.*

Proof. Divide a by m with remainder, so that $a = qm + r$ with $q, r \in K[t]$ and $\partial r < \partial m$. Then $a - r = qm$, so $a \equiv r (\text{mod } m)$. Now we want to show uniqueness. Suppose $r \equiv s (\text{mod } m)$ where $\partial r, \partial s < \partial m$. Then $r - s$ is divisible by m but has smaller degree than m. Therefore, $r - s = 0$, so $r = s$, proving uniqueness. □

The relation $\equiv (\text{mod } m)$ is an equivalence relation on $K[t]$, so it partitions $K[t]$ into equivalence classes. We write $[a]$ for the equivalence class of $a \in K[t]$. This means

$$[a] = \{f \in K[t] : m \mid (a - f)\}$$

The sum and product of $[a]$ and $[b]$ can be defined as:

$$[a] + [b] = [a + b]$$

and

$$[a][b] = [ab]$$

Each equivalence class contains a unique polynomial of degree $< \partial m$, the reduced form of a. This means that to compute in $K[t]$, we can just add and multiply these reduced polynomials, with $m(t)$ identified with 0. We write

$$K[t]/(m)$$

for the set of equivalence classes of $K[t]$ modulo m.

Theorem 3.14. *Let $K(\alpha) : K$ be a simple algebraic extension, and let the minimal polynomial of α over K be m. Then $K(\alpha)$ is isomorphic to $K[t]/(m)$. The isomorphism $K[t]/(m) \to K(\alpha)$ can be chosen to map t to α and be the identity on K.*

Proof. The isomorphism is defined by $[p(t)] \mapsto p(\alpha)$, where $[p(t)]$ is the equivalence class of $p(t) (\text{mod } m)$. This map is well-defined becauce $p(\alpha) = 0$ if and only if $m \mid p$. It is clearly a field monomorphism. It maps t to α, and its restriction to K is the identity. □

Corollary 3.15. *Suppose $K(\alpha) : K$ and $K(\beta) : K$ are simple algebraic extensions such that α and β have the same minimal polynomial m over K. Then the two extensions are isomorphic and the isomorphism of the large fields can be taken to map α to β and be the identity on K.*

Proof. Both extensions are isomorphic to $K[t]/(m)$. The isomorphisms concerned map t to α and t to β, respectively. Call them i, j, respectively. Then ji^{-1} is an isomorphism from $K(\alpha)$ to $K(\beta)$ that is the identity on K and maps α to β. □

Lemma 3.16. *Let $K(\alpha) : K$ be a simple algebraic extension, where the minimal polynomial of α over K is m and $\partial m = n$. Then $[1, \alpha, \ldots, \alpha^{n-1}]$ is a basis for $K(\alpha)$ over K. In particular, $[K(\alpha) : K] = n$.*

Proof. Based on the previous theorem and corollary, this is a restatement of lemma 3.13. □

4. Degree of Field Extensions and the Tower Law

Theorem 4.1. *If $L : K$ is a field extension, then the operations*

$$(\lambda, u) \mapsto \lambda u$$

where $\lambda \in K, u \in L$ and

$$(u, v) \mapsto u + v$$

where $u, v \in L$ define on L the structure of a vector space over K.

The theorem follows immediately from the definition of a vector space because K, L are subfields of $\mathbb{C}$ and $K \subset L$

Definition 4.2. The degree $[L : K]$ of a field extension $L : K$ is the dimension of L considered as a vector space over K.

Example 4.3. A basis for $\mathbb{C}$ over $\mathbb{R}$ is $\{1, i\}$, so $[\mathbb{C} : \mathbb{R}] = 2$

Theorem 4.4 (Short Tower Law)**.** *If K, L, M are subfields of $\mathbb{C}$ and $K \subset L \subset M$, then:*

$$[M : K] = [M : L][L : K]$$

Proof. Let $(x_i)_{i \in I}$ be a basis for L as a a vector space over K and let $(y_j)_{j \in J}$ be a basis for M over L, so for all $i \in I$ and $j \in J$ we have $x_i \in L, y_i \in M$. We want to show $(x_i y_j)_{i \in I, j \in J}$ is a basis for M over K, with $x_i y_i$ the product in M because the dimensions are cardinalities of the bases. First we will show linear independence. Suppose:

$$\sum_{i,j} k_{ij} x_i y_j = 0$$

where $k_{ij} \in K$. We can rearrange this as

$$\sum_j (\sum_i k_{ij} x_i) y_j = 0$$

Since the coefficients $\sum k_{ij} x_i$ are in L and the y_j are linearly independent over L, we have

$$\sum_i k_{ij} x_i = 0$$

By similar argument with $\sum k_{ij} x_i$, we find $k_{ij} = 0$ for all $i \in I, j \in J$. So the elements x_i, y_j are linearly independent over K. Now we want to show that the $x_i y_j$ span M over K. We can write any $m \in M$ as

$$m = \sum_j \lambda_j y_j$$

for some $\lambda_j \in L$ because the y_j span M over L. Similarly, for any $j \in J$

$$\lambda_j = \sum_i \lambda_{ij} x_i$$

for $\lambda_{ij} \in K$. This gives

$$m = \sum_{i,j} \lambda_{ij} x_i y_j$$

so the $x_i y_j$ span M over K □

Corollary 4.5 (Tower Law)**.** *If $K_0 \subset K_1 \subset \ldots \subset K_n$ are subfields of $\mathbb{C}$, then*

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \ldots [K_1 : K_0]$$

Proof. This follows easily by induction from the Short Tower Law. □

Theorem 4.6. *Let $K(\alpha) : K$ be a simple extension. If it is transcendental, then $[K(\alpha) : K] = \infty$. If it is algebraic, then $[K(\alpha) : K] = \partial m$, where m is the minimal polynomial of α over K.*

Proof. For the transcendental case, it suffices to note that the elements $1, \alpha, \alpha^2, \ldots$ are linearly independent over K. For the algebraic case, see lemma 3.16 □

Using the tower law along with this theorem, we can actually compute the degree of an extension quite easily if we know what simple extensions it is composed of.

Example 4.7. $[\mathbb{Q}(\sqrt{2}, i)] : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$

Definition 4.8. A finite extension is one whose degree is finite.

Definition 4.9. An extension $L : K$ is algebraic if every element of L is algebraic over K.

Lemma 4.10. *$L : K$ is a finite extension if and only if L is algebraic over K and there exist finitely many elements $\alpha_1, \ldots, \alpha_s \in L$ such that $L = K(\alpha_1, \ldots, \alpha_s)$*

Proof. Induction using the Short Tower Law and theorem 4.6 shows that any algebraic extension $K(\alpha_1, \ldots, \alpha_s) : K$ is finite. Conversely, let $L : K$ be a finite extension. Then there is a basis $\{\alpha_1, \ldots, \alpha_n\}$ for L over K, whence $L = K(\alpha_1, \ldots, \alpha_s)$. It remains to show that $L : K$ is algebraic. Let x be any element of L and let

$n = [L : K]$. The set $\{1, x, \ldots, x^s\}$ contains $n + 1$ elements, which must therefore be linearly dependent over K. Hence

$$k_0 + k_1 x + \ldots + k_n x^n = 0$$

for $k_0, \ldots, k_n \in K$ and x is algebraic over K. □

5. Galois Groups and Fixed Fields

Now we will finally define the objects which we want to study along with a few basic properties. First we define a special kind of automorphism.

Definition 5.1 (K-automorphism of L)**.** Let $L : K$ be a field extension, so that K is a subfield of the subfield L of $\mathbb{C}$. A K-automorphism of L is an automorphism α of L such that

$$\alpha(k) = k \text{ for all } k \in K$$

We say that α fixes $k \in K$ if this equation holds.

Theorem 5.2. *If $L : K$ is a field extension, then the set of all K-automorphisms of L forms a group under composition of maps*

Proof. Suppose that α and β are K-automorphisms of L. Then $\alpha\beta$ is clearly an automorphism; further, if $k \in K$, then $\alpha\beta(k) = \alpha(k) = k$, so $\alpha\beta$ is a K-automorphism. The identity map on L is obviously a K-automorphism. Finally, α^{-1} is an automorphism of L, and for any $k \in K$ we have

$$k = \alpha^{-1}\alpha(k) = \alpha^{-1}(k)$$

so α^{-1} is a K-automorphism. Composition of maps is associative, so the set of all K-automorphisms of L is a group. □

Definition 5.3 (Galois group!)**.** The Galois group $\Gamma(L : K)$ of a field extension $L : K$ is the group of all K-automorphism of L under the operation of composition of maps

Example 5.4. Consider the extension $\mathbb{C} : \mathbb{R}$. Suppose that α is an $\mathbb{R}$-automorphism of $\mathbb{C}$. Let $j = \alpha(i)$, where $i = \sqrt{-1}$. We have

$$j^2 = (\alpha(i))^2 = \alpha(i^2) = \alpha(-1) = -1$$

since $-1 \in \mathbb{R}$ and α fixes $\mathbb{R}$. Hence, either $j = i$ or $j = -i$. Now for any $x, y \in \mathbb{R}$, we have

$$\alpha(x + iy) = \alpha(x) + \alpha(i)\alpha(y) = x + jy$$

Thus we have two candidates for $\mathbb{R}$-automorphisms:

$$\alpha_1 : x + iy \mapsto x + iy$$

and

$$\alpha_2 : x + iy \mapsto x - iy$$

α_1 is the identity, and hence an $\mathbb{R}$-automorphism of $\mathbb{C}$, while α_2 is complex conjugation, also an $\mathbb{R}$-automorphism of $\mathbb{C}$. $\alpha_2^2 = \alpha_1$, so the Galois group $\Gamma(\mathbb{C} : \mathbb{R})$ is a cyclic group of order 2.

Definition 5.5 (intermediate field)**.** Let $L : K$ be a field extension. If M is a field such that $K \subset M \subset L$, then M is an intermediate field.

If $G = \Gamma(L : K)$, then to each intermediate field we associate the group $G_M = \Gamma(L : M)$. Thus G_K is the whole Galois group and $G_L = 1$. This mapping reverses inclusions because if $M \subset N$, then $G_M \supset G_N$ because any automorphism of L that fixes the elements of N fixes the elements of M. Conversely, to each subgroup H of $\Gamma(L : K)$ we associate the set L^H of all elements $x \in L$ such that $\alpha(x) = x$ for all $\alpha \in H$. In fact, this set is an intermediate field.

Lemma 5.6. *If H is a subgroup of $\Gamma(L : K)$, then $H^\diamond$ is a subfield of L containing K.*

Proof. Let $x, y \in L^H$ and $\alpha \in H$. Then

$$\alpha(x + y) = \alpha(x) + \alpha(y) = x + y$$

so $x + y \in H^\diamond$. Similarly, $H^\diamond$ is closed under subtraction, multiplication, and division (by nonzero elements), so L^H is a subfield of L. Since $\alpha \in \Gamma(L : K)$, we have $\alpha(k) = k$ for all $k \in K$, so $K \subset L^H$ □

Definition 5.7. With the above notation, L^H is the fixed field of H.

6. Normality and Separability

Definition 6.1 (splits)**.** If K is a subfield of $\mathbb{C}$ and f is a polynomial over K, then f splits over K if it can be expressed as a product of linear factors

$$f(t) = k(t - \alpha_1) \dots (t - \alpha_n)$$

where $k, \alpha_1, \dots, \alpha_n \in K$.

This means that the zeroes of f in K are $\alpha_1, \dots, \alpha_n$. By The Fundamental Theorem of Algebra, f splits over K if and only if all of its zeroes in $\mathbb{C}$ lie in K. This means that K must contain the subfield generated by all the zeroes of f.

Definition 6.2 (splitting field)**.** A subfield Σ of $\mathbb{C}$ is a splitting field for the polynomial f over the subfield K of $\mathbb{C}$ if $K \subset \Sigma$ and

(1) f splits over Σ.
(2) If $K \subset \Sigma' \subset \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

The second condition is equivalent to the condition that $\Sigma = K(\sigma_1, \dots, \sigma_n)$ where $\sigma_1, \dots, \sigma_n$ are the zeroes of f in Σ. Clearly, every polynomial over a subfield K of $\mathbb{C}$ has a splitting field.

Example 6.3. The polynomial $f(t) = t^3 - 1 \in \mathbb{Q}[t]$ splits over $\mathbb{C}$ because it can be written as

$$f(t) = (t - 1)(t - \omega)(t - \omega^2)$$

where $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. This implies that f also splits over $\mathbb{Q}(i, \sqrt{3})$ and $\mathbb{Q}(\omega)$ because 1, ω, and ω^2 are elements of all three of these fields. In particular, $\mathbb{Q}(\omega)$ is the splitting field for f.

Theorem 6.4. *If K is any subfield of $\mathbb{C}$ and f is any polynomial over K, then there exists a unique splitting field Σ for f over K. Moreover, $[\Sigma : K]$ is finite.*

Proof. We can take $\Sigma = K(\sigma_1, \dots, \sigma_n)$ where the σ_j are the zeroes of f in $\mathbb{C}$. In fact, this is the only possibility, so Σ is unique. The degree $[\Sigma : K]$ is finite because $K(\sigma_1, \dots, \sigma_n)$ is finitely generated and algebraic, so lemma 4.10 applies. □

Definition 6.5. A field extension $L : K$ is normal if every irreducible polynomial f over K that has at least one zero in L splits in L

Example 6.6. $\mathbb{C} : \mathbb{R}$ is normal since every polynomial (irreducible or not) splits in $\mathbb{C}$. However, the extension $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ is not normal because the irreducible polynomial $t^3 - 2$ has a zero in $\mathbb{Q}(\sqrt[3]{2})$, but it does not split in $\mathbb{Q}(\sqrt[3]{2})$

Lemma 6.7. *Suppose that $i : K \to K'$ is an isomorphism of subfields of $\mathbb{C}$. Let f be a polynomial over K and let $\Sigma \supset K$ be the splitting field for f. Let L be any extension field of K' such that $i(f)$ splits over L. Then there exists a monomorphism $j : \Sigma \to L$ such that $f \restriction_K = i$*

Proof. We will construct $j : \Sigma \to L$ using induction on ∂f. As a polynomial over Σ,

$$f(t) = k(t - \sigma_1) \dots (t - \sigma_n)$$

The minimal polynomial m of σ_1 over K is an irreducible factor of f. Now $i(m)$ divides $i(f)$ which splits over L, so that over L,

$$i(m) = (t - \alpha_1) \dots (t - \alpha_r)$$

where $\alpha_1, \dots, \alpha_r \in L$. Since $i(m)$ is irreducible over K', it must be the minimal polynomial of α_1 over K'. So there is an isomorphism

$$j_1 : K(\alpha_1) \to K'(\alpha_1)$$

such that $j_1 \restriction_K = i$ and $j_1(\sigma_1) = \alpha_1$. Now Σ is a splitting field over $K(\sigma_1)$ of the polynomial $g = f/(t - \sigma_1)$. By induction there exists a monomorphism $j : \Sigma \to L$ such that $j \restriction_{K(\sigma_1)} = j_1$. But then $j \restriction_K = i$ and we are finished. □

This enables us to prove the uniqueness theorem.

Theorem 6.8. *Let $i : K \to K'$ be an isomorphism. Let Σ be the splitting field for f over K, and let Σ' be the splitting field for $i(f)$ over K'. Then there is an isomorphism $j : \Sigma \to \Sigma'$ such that $j \restriction_K = i$.*

Proof. We want to find $j : \Sigma \to \Sigma'$. By the previous lemma, there is a monomorphism $j : \Sigma \to \Sigma'$ such that $j \restriction_K = i$. But $j(\Sigma)$ is clearly the splitting field for $i(f)$ over K', and is contained in Σ'. Since Σ' is also the splitting field for $i(f)$ over K', we have $j(\Sigma) = \Sigma'$, so that j is onto. Hence j is an isomorphism. □

Normality will be essential for creating good Galois groups, but luckily we have an easy way of checking that an extension is normal.

Theorem 6.9. *A field extension $L : K$ is normal and finite if and only if L is a splitting field for some polynomial over K.*

Proof. Suppose $L : K$ is normal and finite. By lemma 4.10, $L = K(\alpha_1, \dots, \alpha_s)$ for certain α_j algebraic over K. Let m_j be the minimal polynomial of α_j over K and let $f = m_1 \dots m_s$. Each m_j is irreducible over K and has a zero $\alpha_j \in L$. Since L is generated by K and the zeroes of f, it is the splitting field for f over K. To prove the converse, suppose that L is the splitting field for some polynomial g over K. The extension $L : K$ is then obviously finite; we must show that it is normal. To do this we will take an irreducible polynomial f over K with a zero in L and show that it splits in L. Let $M \supset L$ be a splitting field for fg over K. Suppose that θ_1

and θ_2 are zeroes of f in M. By irreducibility, f is the minimal polynomial of θ_1 and θ_2 over K. We claim that

$$[L(\theta_1) : L] = [L(\theta_2) : L]$$

To prove this, consider the subfields $K, L, K(\theta_1), L(\theta_1), K(\theta_2), L(\theta_2)$ of M and the towers

$$K \subset K(\theta_1) \subset L(\theta_1) \subset M$$

$$K \subset K(\theta_2) \subset L(\theta_2) \subset M$$

We also know that $K \subset K(\theta_i)$ and $L \subset L(\theta_j)$ for $j = 1, 2$, and $K \subset L \subset M$. The claim will follow from computation of degrees. For $j = 1, 2$, we have

$$[L(\theta_j) : L][L : K] = [L(\theta_j) : K] = [L(\theta_j) : K(\theta_j)][K(\theta_j) : K] \tag{6.10}$$

By theorem 4.6, $[K(\theta_1) : K] = [K(\theta_2) : K]$. Clearly, $L(\theta_j)$ is the splitting field for g over $K(\theta_j)$, and so by corollary 3.15 $K(\theta_1)$ is isomorphic to $K(\theta_2)$. Therefore by theorem 6.8 the extensions $L(\theta_j) : K(\theta_j)$ are isomorphic for $j = 1, 2$, and hence have the same degree. Substituting into equation 6.10 and cancelling we get

$$[L(\theta_1) : L] = [L(\theta_2) : L]$$

as claimed. The rest is easy. If $\theta_1 \in L$, then $[L(\theta_1) : L] = 1$, so $[L(\theta_2) : L] = 1$ and $\theta_2 \in L$. Hence $L : K$ is normal. □

Definition 6.11 (normal closure)**.** Let L be a finite extension of K. A normal closure of $L : K$ is an extension N of L such that

(1) $N : K$ is normal.
(2) If $L \subset M \subset N$ and $M : K$ is normal, then $M = N$.

Thus N is the smallest extension of L that is normal over K.

Within $\mathbb{C}$ we can always find unique normal closures, as per the next theorem.

Theorem 6.12. *If $L : K$ is a finite extension in $\mathbb{C}$, then there exists a unique normal closure $N \subset \mathbb{C}$ of $L : K$, which is a finite extension of K.*

Proof. Let $x_1, \ldots, x_r$ be a basis for L over K, and let m_j be the minimal polynomial of x_j over K. Let N be the splitting field for $f = m_1 m_2 \ldots m_r$ over L. Then N is also the splitting field for f over K, so $N : K$ is normal and finite by theorem 6.9. Suppose that $L \subset P \subset N$ where $P : K$ is normal. Each polynomial m_j has a zero $x_j \in P$ so by normality f splits in P. Since N is the splitting field for f, we have $P = N$. Therefore N is a normal closure. Now suppose that M and N are both normal closures. f splits in M and N, so both M and N contain the splitting field for f over K. This splitting field contains L and is normal over K, so it must be equal to both M and N. □

Definition 6.13 (separable)**.** An irreducible polynomial f over a subfield K of $\mathbb{C}$ is separable over K if it has simple zeroes in $\mathbb{C}$, or equivalently, simple zeroes in its splitting field, so

$$f(t) = k(t - \sigma_1) \ldots (t - \sigma_n)$$

where the σ_j are different.

Although separability is also critical for having a nice Galois group, we will largely ignore it because separability is automatic over $\mathbb{C}$

7. Counting Lemmas

First we present some lemmas without proof which rely on basic linear algebra.

Lemma 7.1 (Dedekind)**.** *If K and L are subfields of $\mathbb{C}$, then every set of distinct monomorphisms $K \to L$ is linearly independent over L.*

Lemma 7.2. *If $n > m$, then a system of m homogenous linear equations*

$$a_{m1}x_1 + \ldots + a_{mn}x_n = 0$$

in n unknowns $x_1, \ldots, x_n$, with complex xoefficients a_{ij}, has a solution in which the x_i are not all zero.

Now a quick group-theoretic lemma.

Lemma 7.3. *If G is a group whose distinct elements are $g_1, \ldots, g_n$, and if $g \in G$, then as j varies from 1 to n the elements gg_j run through the whole of G, each element of G occurring precisely once.*

Proof. If $h \in G$, then $g^{-1}h = g_j$ for some j and $h = gg_j$. If $gg_i = gg_j$, then $g_i = g^{-1}gg_i = g^{-1}gg_j = g_j$. Thus the map $g_i \mapsto gg_i$ is a bijection $G \to G$, and the theorem follows. □

With all of this, we can prove the following key theorem.

Theorem 7.4. *Let G be a finite subgroup of the group of automorphisms of a field K, and let K_0 be the fixed field of G. Then $[K_0 : K] = |G|$.*

Proof. Let $|G| = n$, and suppose that the elements of G are $g_1, \ldots, G_n$, where $g_1 = 1$. We will show $[K_0 : K] \geq n$, then $[K_0 : K] \leq n$ 1. Suppose for contradiction that $[K_0 : K] = m$, with $m < n$. Let $[x_1, \ldots, x_m]$ be a basis for K over K_0. By lemma 7.2 there exist $y_1, \ldots, y_n \in K$, not all zero, such that

$$y_1 g_1(x_j) + \ldots + y_n g_n(x_j) = 0 \tag{7.5}$$

for $j = 1, \ldots, m$. Let x be any element of K. Then

$$x = \alpha_1 x_1 + \ldots + \alpha_m x_m$$

where $\alpha_1, \ldots, \alpha_m \in K_0$. Hence

$$\begin{aligned} y_1 g_1(x) + \ldots + y_n g_n(x) &= y_1 g_1\big(\sum_l \alpha_l x_l\big) + \ldots + y_n g_n\big(\sum_l \alpha_l x_l\big) \\ &= \sum_l \alpha_l [y_1 g_1(x_l) + \ldots + y_n g_n(x_l)] \\ &= 0 \end{aligned}$$

using equation 7.5. Hence the distinct monomorphisms $g_1, \ldots, g_n$ are linearly independent, contrary to lemma 7.1. Therefore $m \geq n$. 2. Suppose for contradiction that $[K_0 : K] > n$. There there exists a set of $n+1$ elements of K that are linearly independent over K_0; let such a set be $\{x_1, \ldots, x_{n+1}\}$. By lemma 7.1 there exist $y_1, \ldots, y_{n+1} \in K$, not all zero, such that for $j = 1, \ldots, n$

$$y_1 g_j(x_1) + \ldots + y_{n_1} g_j(x_{n+1}) = 0 \tag{7.6}$$

Now choose $y_1, \ldots, y_{n+1}$ so that as few as possible are nonzero, and renumber so that

$$y_1, \ldots, y_r \neq 0$$

and

$$y_{r+1}, \ldots, y_{n+1} = 0$$

Thus equation 7.6 becomes

$$y_1 g_j(x_1) + \ldots + y_r g_j(x_r) = 0 \tag{7.7}$$

Let $g \in G$ and operate on equation 7.7 with g. This gives a system of equations

$$g(y_1)gg_j(x_1) + \ldots + g(y_r)gg_j(x_r) = 0$$

By lemma 7.3, as j varies, this system of equations is equivalent to the system

$$g(y_1)g_j(x_1) + \ldots + g(y_r)g_j(x_r) = 0 \tag{7.8}$$

Multiply equation 7.7 by $g(y_1)$ and equation 7.8 by y_1 and subtract, to get

$$[y_2 g(y_1) - g(y_2)y_1]g_j(x_2) + \ldots + [y_r g(y_1 - g(y_r)y_1]g_j(x_r) = 0$$

This is a system of equations like equation 7.7 but with fewer terms, which is a contradiction unless all the coefficients

$$y_i g(y_1) - y_1 g(y_i)$$

are zero. However, if this happens, then

$$y_i y_1^{-1} = g(y_i y_1^{-1})$$

for all $g \in G$, so that $y_i y_1^{-1} \in K_0$. Thus there exist $z_1, \ldots, z_r \in K_0$ and an element $k \in K$ such that $y_i = kz_i$, for all i. Then equation 7.7 with $j = 1$ becomes

$$x_1 kz_1 + \ldots + z_r kz_r = 0$$

and since $k \neq 0$ we may divide by k, so the x_i are linearly dependent over K_0, contradiction. Therefore $[K_0 : K] = n = |G|$ □

Corollary 7.9. *If G is the Galois group of the finite extension $L : K$, and H is a finite subgroup of G, then*

$$[L^H : K] = [L : K]/|H|$$

Proof. By the tower law, $[L : K] = [L : L^H][L^H : K]$, so $[L^H : K] = [L : K]/[L : L^H]$. But this equals $[L : K]/|H|$ by theorem 7.4. □

8. Field Automorphism Lemmas

Definition 8.1 (K-Monomorphisms)**.** Suppose that K is a subfield of each of the subfields M and L of $\mathbb{C}$. Then a K-monomorphism of M into L is a field monomorphism $\phi : M \to L$ such that $\phi(k) = k$ for every $k \in K$.

Theorem 8.2. *Suppose that $L : K$ is a finite normal extension and $K \subset M \subset L$. Let τ be any K-monomorphism $M \to L$. Then there exists a K-automorphism σ of L such that $\sigma \restriction_M = \tau$.*

Proof. By theorem 6.9, L is the splitting field over K of some polynomial f over K. Hence it is both the splitting field over M for f and over $\tau(M)$ for f. But $\tau \restriction_K$ is the identity, so $\tau(f) = f$. By theorem 6.8, there is an isomorphism $\sigma : L \to L$ such that $\sigma \restriction_M = \tau$. Therefore, σ is an automorphism of L, and since $\sigma \restriction_K = \tau \restriction_K$ is the identity, σ is a K-automorphism of L. □

Using this we can construct K-automorphisms.

Theorem 8.3. *Suppose that $L : K$ is a finite normal extension, and α, β are zeroes in L of the irreducible polnomial p over K. Then there exists a K-automorphism σ of L such that $\sigma(\alpha) = \beta$.*

Proof. By corollary 3.13 there is an isomorphism $\tau : K(\alpha) \to K(\beta)$ such that $\tau \restriction_K$ is the identity and $\tau(\alpha) = \beta$. By theorem 11.3, τ extends to a K-automorphism σ of L. □

Now we can explore the theme of K-monomorphisms as they relate to normal closures.

Lemma 8.4. *Suppose that $K \subset L \subset N \subset M$ where $L : K$ is finite and N is the normal closure of $L : K$. Let τ be any K-monomorphism $L \to M$. Then $\tau(L) \subset N$.*

Proof. Let $\alpha \in L$. Let m be the minimal polynomial of α over K. Then $m(\alpha) = 0$ so $\tau(m(\alpha)) = 0$. But $\tau(m(\alpha)) = m(\tau(\alpha))$ since τ is a K-monomorphism, so $m(\tau(\alpha)) = 0$ and $\tau(\alpha)$ is the zero of m. Therefore $\tau(\alpha)$ lies in N since $N : K$ is normal. Therefore, $\tau(L) \subset N$. □

Theorem 8.5. *For a finite extension $L : K$ the following are equivalent:*

1. *$L : K$ is normal.*
2. *There exists a finite normal extension N of K containing L such that every K-monomorphism $\tau : L \to N$ is a K-automorphism of L.*
3. *For every finite extension M of K containing L, every K-monomorphism $\tau : L \to M$ is a K-automorphism of L.*

Proof. We wll show (1) $\implies$ (3) $\implies$ (2) $\implies$ (1). First (1) $\implies$ (3). If $L : K$ is normal, then L is the normal closure of $L : K$, so by lemma 8.4, $\tau(L) \subset L$. But τ is a K-linear map define on the finite dimensional vector space L over K, and is a monomorphism. Therefore $\tau(L)$ has the same dimension as L, so $\tau(L) = L$ and τ is a K-automorphism of L.
Now (3) $\implies$ (2). Let N be the normal closure for $L : K$. Then N exists by theorem 6.12, and has the necessary properties by (3)
Now (2) $\implies$ (1). Suppose that f is any irreducible polynomial over K with a zero $\alpha \in L$. Then f splits over N by normality, and if β is any zero of f in N, then by theorem 8.3 there exists an automorphism σ of N such that $\sigma(\alpha) = \beta$. By hypothesis, σ is a K=automorphism of L, so $\beta = \sigma(\alpha) \in \sigma(L) = L$. Therefore f splits over L and $L : K$ is normal. □

Theorem 8.6. *Suppose that $L : K$ is a finite extension of degree n. Then there are precisely n distinct K-monomorphisms of L into the normal closure N of $L : K$, and hence into any given normal extension M of K containing L.*

Proof. Proof by induction on $[L : K]$. If $[L : K] = 1$, then the result is clear. Suppose that $[L : K] = k > 1$. Let $\alpha \in L \setminus K$ with minimal polynomial m over K. Then

$$\partial m = [K(\alpha) : K] = r > 1$$

m is an irreducible polynomial over a subfield of $\mathbb{C}$ with one zero in the normal extension N, so m splits in N and its zeros $\alpha_1 \dots \alpha_r$ are distinct. By induction there are precisely s distinct $K(\alpha)$-monomorphisms $p_1, \dots, p_s : L \to N$, where

$s = [L : K(\alpha)] = k/r$. By theorem 8.3, there are r distinct K-autmorphisms $\tau_1, \ldots, \tau_r$ of N such that $\tau_i(\alpha) = \alpha_i$. The maps

$$\phi_{ij} = \tau_i p_j$$

give $rs = k$ distinct K-monomorphisms $L \to N$. We will show that these exhaust the K-monomorphisms $L \to N$. Let $\tau : L \to N$ be a K-monomorphism. Then $\tau(\alpha)$ is a zero of m in N, so $\tau(\alpha) = \alpha_i$ for some i. The map $\phi = \tau_j^{-1}\tau$ is a $K(\alpha)$-monomorphism $L \to N$, so by induction $\phi = p_j$ for some j. Hence $\tau = \tau p_j = \phi_{ij}$ and the theorem is proved. □

Now we can calculate the order of the Galois group of a finite normal extension.

Corollary 8.7. *If $L : K$ is a finite normal extension inside $\mathbb{C}$, then there are precisely $[L : K]$ distinct K-automorphisms of L.*

Proof. Apply theorems 8.5 and 8.6, and the result follows. □

From this we can reach another important result.

Theorem 8.8. *Let $L : K$ be a finite extension with Galois group G if $L : K$ is normal, then K is the fixed field of G.*

Proof. Let K_0 be the fixed field of G, and let $[L : K] = n$. Corollary 8.7 implies that $|G| = n$. By theorem 7.4, $[L : K_0] = n$. Since $K \subset K_0$, we must have $K = K_0$. □

Theorem 8.9. *Suppose that $K \subset L \subset M$ and $M : K$ is finite, Then the number of distinct K-automorphisms $L \to M$ is at most $[L : K]$.*

Proof. Let N be a normal closure of $M : K$. Then $N : K$ is finite by theorem 6.12 and every K-monomorphism $L \to M$ is also a K-monomorphism $L \to N$. Hence we may assume that M is a normal extension of K by replacing M by N. We now argue by induction on $[L : K]$ as in the proof of theorem 8.6 except that we can now deduce only that there are s' $K(\alpha)$- monomorphisms $L \to N$. , where $s' \leq s$ (by induction) and there are r' distinct K-automorphisms of N, where $r' \leq r$ (since the zeros of m in N need not be distinct). The rest of the argument goes through as before. □

Theorem 8.10. *If $L : K$ is a finite extension with Galois group G, such that K is the fixed field of G, then $L : K$ is normal.*

Proof. By theorem 7.4, $[L : K] = |G| = n$, say. There are exactly n distinct K-monomorphisms $L \to L$, the elements of the Galois group. We prove normality using theorem 8.5. Let N be an extension of K containing L, and let τ be a K-monomorphism $L \to N$. Since every element of the Galois group of $L : K$ defines a K-monomorphism $L \to N$, the Galois group proves n K-monomorphisms $L \to N$, and these are automorphism of L. But by theorem 8.9 there are at most n distinct K-monomorphisms τ so τ must be one of these monomorphisms. Hence τ is an automorphism of L. Finally, by theorem 8.5, $L : K$ is normal. □

9. The Fundamental Theorem of Galois Theory

After all this work, we are finally ready to establish the fundamental properties of the Galois correspondence between a field extension and its Galois group. First, a few definitions and reminders to clarify notation. Let $L : K$ be a field extension in $\mathbb{C}$ with Galois group G, which consists of all K-automorphisms of L. Let $\mathcal{F}$ be

the set of all intermediate fields, that is, subfields M such that $K \subset M \subset L$, and let $\mathcal{G}$ be the set of all subgroups H of G. If $M \in \mathcal{F}$, then G_M is the subgroup of G of elements that fix M, in other words, the group of all M-automorphisms of L. If $H \in \mathcal{G}$, then L^H is the fixed field of H. Furthermore, define $G_{(-)} : \mathcal{F} \to \mathcal{G}$ by $M \mapsto G_M$ and define $L^{(-)} : \mathcal{G} \to \mathcal{F}$ by $H \mapsto L^H$. We have seen that these maps reverse inclusions, that is $M \subset L^{G_M}$ and $H \subset G_{L^H}$.

Theorem 9.1 (Fundamental Theorem of Galois Theory)**.** *If $L : K$ is a finite normal field extension inside $\mathbb{C}$, with Galois group G, and if $\mathcal{F}$ and $\mathcal{G}$ are defined as above, then:*

1. *The Galois group G has order $[L : K]$.*
2. *The maps $G_{(-)}$ and $L^{(-)}$ are mutual inverses, and set up an order-reversing one-to-one correspondence between $\mathcal{F}$ and $\mathcal{G}$.*
3. *If M is an intermediate field, then*
$$[L : M] = |G_M|$$
and
$$[M : K] = |G|/|G_M|$$
4. *An intermediate field M is a normal extension of K if and only if G_M is a normal subgroup of G.*
5. *If an intermediate field M is a normal extension of K, then the Galois group of $M : K$ is isomorphic to the quotient group G/G_M.*

Proof. The first part is a restatement of corollary 8.7. For the second part, theorem 6.9 implies that $L : M$ is normal. Theorem 8.8 implies that M is the fixed field of G_M, so
$$L^{G_M} = M$$
Now consider $H \in \mathcal{G}$. We know that $H \subset G_{L^H}$. Therefore, $L^{G_{L^H}} = L^H$ by the above equation. By theorem 7.4, $|H| = [L : L^H]$. Therefore, $|H| = [L : L^{G_{L^H}}]$, and by theorem 7.4 again, $[L : L^{G_{L^H}}] = |G_{L^H}|$ so that $|H| = |G_{L^H}|$. The second part of the Fundamental Theorem follows at once. For the third part, note that $L : M$ is normal. Corollary 8.7 states that $[L : M] = |G_M|$, and the other equality follows immediately. We need a quick lemma for parts 4 and 5.

Lemma 9.2. *Suppose that $L : K$ is a field extension, M is an intermediate field, and τ is a K-automorphism of L. Then $G_{\tau(M)} = \tau G_M \tau^{-1}$.*

Proof. Let $M' = \tau(M)$, and take $\gamma \in G_M$, $x_1 \in M'$. Then $x_1 = \tau(x)$ for some $x \in M$. Compute:
$$(\tau\gamma\tau^{-1})(x_1) = \tau\gamma(x) = \tau(x) = x_1$$
so $\tau M^* \tau^{-1} \subset G_{M'}$. Similarly $\tau^{-1} G_{M'} \tau \subset G_M$, so $\tau G_M \tau^{-1} \supset G_{M'}$, and the lemma is proved. □

Now we can prove the fourth part of the Fundamental Theorem. If $M : K$ is normal, let $\tau \in G$. Then $\tau \restriction_M$ is a K-monomorphism $M \to L$, so it is a K-automorphism of M by theorem 8.5. Hence $\tau(M) = M$. By Lemma 12.2, $\tau G_M \tau^{-1} = G_M$, so G_M is a normal subgroup of G. Conversely, suppose that G_M is a normal subgroup of G. Let σ be any K-monomorphism $M \to L$. By theorem 8.2, there is a K-automorphism τ of L such that $\tau \restriction_M = \sigma$. Now $\tau G_M \tau^{-1} = G_M$ since G_M is a normal subgroup of G, so by lemma 9.2, $G_{\tau(M)} = G_M$. By part

2 of the Fundamental Theorem, $\tau(M) = M$. Hence $\sigma(M) = M$ and σ is a K-automorphism of M. By theorem 8.5, $M : K$ is normal. Now we prove the final part of the theorem. Let G' be the Galois group of $M : K$. We can define a map $\phi : G \to G'$ by

$$\phi(\tau) = \tau \restriction_M$$

where $\tau \in G$. This is clearly a group homomorphism $G \to G'$, because by theorem 8.5 $\tau \restriction_M$ is a K-automorphism of M. By theorem 8.2, ϕ is onto. The kernel of ϕ is clearly G_M, so by basic group theory we have

$$G' = \mathrm{im}(\phi) \cong G/\ker(\phi) = G/G_M$$

where im is the image and ker the kernel. □

10. An Example

To illustrate all of this theory on a relatively tractable but still interesting polynomial, we will consider $f(t) = t^4 - 2$. The example is quite long, so we will break it into a number of parts.

(1) f factors as

$$f(t) = (t - \omega)(t + \omega)(t - i\omega)(t + i\omega)$$

where $\omega = \sqrt[4]{2}$. Therefore, if K is the splitting field for f with $K \subset \mathbb{C}$, $K = \mathbb{Q}(\omega, i)$. K is a splitting field, so $K : \mathbb{Q}$ is normal and finite. Because we are working in $\mathbb{C}$, separability is automatic. This means that we can apply the Fundamental Theorem of Galois Theory to this extension.

(2) Now we find the degree of $K : \mathbb{Q}$. By the tower law,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\omega, i) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$$

The minimal polynomial of i over $\mathbb{Q}(\omega)$ is $t^2 + 1$ because $i^2 + 1 = 0$ but $i \notin \mathbb{R} \supset \mathbb{Q}(\omega)$. Therefore $[\mathbb{Q}(\omega, i) : \mathbb{Q}(\omega)] = 2$. ω is a zero of f over $\mathbb{Q}$ and f is irreducible by Eisenstein's Criterion, theorem 2.6. Thus f is the minimal polynomial of ω over $\mathbb{Q}$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. So we have

$$[K : \mathbb{Q}] = 2 \cdot 4 = 8$$

(3) Now we want to find the elements of the Galois group of $K : \mathbb{Q}$. There is a $\mathbb{Q}$-automorphism σ of K such that

$$\sigma(i) = i$$

and

$$\sigma(\omega) = i\sigma$$

and another, τ, such that

$$\tau(i) = -i$$

and

$$\tau(\omega) = \omega$$

σ and τ generate eight distinct $\mathbb{Q}$-automorphisms of K, as follows:

Automorphism	**Effect on ω**	**Effect on i**
1	ω	i
σ	$i\omega$	i
σ^2	$-\omega$	i
σ^3	$-i\omega$	i
τ	ω	$-i$
$\sigma\tau$	$i\omega$	$-i$
$\sigma^2\tau$	$-\omega$	$-i$
$\sigma^3\tau$	$-i\omega$	$-i$

No other products give distinct automorphisms because $\sigma^4 = \tau^2 = 1$, $\tau\sigma = \sigma^3\tau$, $\tau\sigma^2 = \sigma^2\tau$, and $\tau\sigma^3 = \sigma\tau$. Because we have found eight $\mathbb{Q}$-automorphisms of K and $[K : \mathbb{Q}] = 8$ by part 2, we know by the Fundamental Theorem of Galois theory that these are the only elelements of the Galois group.

(4) From this, we can find the abstract structure of the Galois group G. The generator-relation presentation

$$G = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$$

show that G is the dihedral group of order 8, written as $\mathbb{D}_8$.

(5) We can find the subgroups of G explicitly. The subgroups are as follows:

Name	**Elements**	**Order**	**Group-theoretic representation**
G	all	8	$\mathbb{D}_8$
S	$1, \sigma, \sigma^2, \sigma^3$	4	$\mathbb{Z}_4$
T	$1, \sigma^2, \tau, \sigma^2\tau$	4	$\mathbb{Z}_2 \times \mathbb{Z}_2$
U	$1, \sigma^2, \sigma\tau, \tau\sigma$	4	$\mathbb{Z}_2 \times \mathbb{Z}_2$
A	$1, \sigma^2$	2	$\mathbb{Z}_2$
B	$1, \tau$	2	$\mathbb{Z}_2$
C	$1, \sigma\tau$	2	$\mathbb{Z}_2$
D	$1, \sigma^2\tau$	2	$\mathbb{Z}_2$
E	$1, \sigma^3\tau$	2	$\mathbb{Z}_2$
I	1	1	1

(6) Using the Galois correspondence we can obtain the intermediate fields. Since the correspondence reverses inclusions, the following two lattice diagrams, where $X \subset Y$ if and only if there is a sequence of upward sloping lines from X to Y, represent the subgroups of G and the intermediate fields. (see figures 1 and 2 below)

(7) The normal subgroups of G are G, S, T, U, A, and I. By the Fundamental Theorem of Galois theory, K^G, K^S, K^T, K^U, K^A, K^I should be the only normal extensions of $\mathbb{Q}$ contained in K. Since these are all splitting fields over $\mathbb{Q}$ for the polynomials $t, t^2+1, t^2-2, t^2+2, t^4-t^2-2, t^4-2$, respectively, they are normal extensions of $\mathbb{Q}$. On the other hand, extensions of other intermediate fields are not normal. For example $K^B : \mathbb{Q}$ is normal because $t^4 - 2$ has a zero, ω, in K^B but does not split in K^B.

(8) According to the Fundamental Theorem of Galois theory, the Galois group of $K^A : \mathbb{Q}$ is isomorphic to G/A. Now G/A is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. We will directly calculate the Galois group of $K^A : \mathbb{Q}$. Since $K^A = \mathbb{Q}(i, \sqrt{2})$, there are four $\mathbb{Q}$-automorphisms:

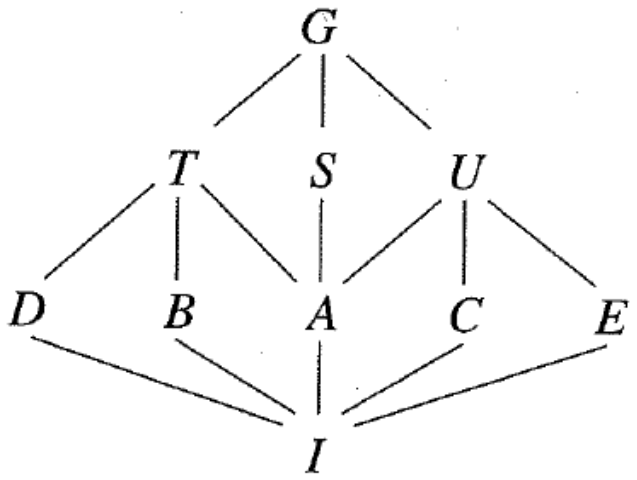

FIGURE 1. Lattice of Subgroups

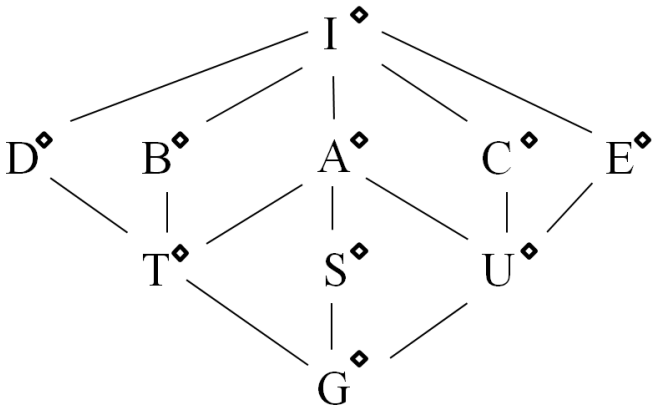

FIGURE 2. Lattice of Subfields

Automorphism	**Effect on i**	**Effect on $\sqrt{2}$**
1	i	$\sqrt{2}$
α	i	$-\sqrt{2}$
β	$-i$	$\sqrt{2}$
$\alpha\beta$	$-i$	$-\sqrt{2}$

Since $\alpha^2 = \beta^2 = 1$ and $\alpha\beta = \beta\alpha$, this group is $\mathbb{Z}_2 \times \mathbb{Z}_2$ as expected. Thus, everything which the Fundamental Theorem tells us to expect indeed occurs in this example.

11. Acknowledgements

Thank you to everyone who helped me through the process of writing this paper. In particular, I would like to thank my mentor Chang Mou Lim for guiding

me through the process of selecting and writing on a topic, as well as providing commentary to improve my drafts. I would also like to thank Peter May and the other coordinators of the REU for both funding my research and providing such a constructive environment to learn mathematics.

References

[1] Ian Stewart. Galois Theory. Chapman and Hall. 2003.
[2] Andrew Baker. An Introduction to Galois Theory. www.maths.gla.ac.uk/ ajb/dvi-ps/Galois.pdf.
[3] C.D.H. Cooper. Galois Theory. Ch. 10. web.science.mq.edu.au/ chris/galois/CHAP10
[4] David S. Dummit and Richard M. Foote. Abstract Algebra. John Wiley and Sons. 2004.