Galois Theory

Galois Theory has its origins in the study of polynomial equations and their solutions. What is has revealed is a deep connection between the theory of fields and that of groups. We first will develop the language of field extensions. From there, we will push towards the Fundamental Theorem of Galois Theory, gives a way of realizing roots of a polynomial via automorphisms of a certain group (called the Galois group).

1. Vector Spaces

This material is review from Linear Algebra but we include it for completeness.

**Definition 1.** Let $K$ be a field and $V$ an additive abelian group together with a function

$$K \times V \to V$$

$$(k, v) \mapsto kv.$$

Then $V$ is a $K$-vector space provided that for all $k, \ell \in K$ and $u, v \in V$,

- $k(u + v) = ku + kv$
- $(k + \ell)v = ku + \ell v$
- $k(\ell v) = (k\ell)v$
- $1_Kv = v$.

**Definition 2.** Let $V$ be a vector space over a field $K$. A subset $X \subseteq V$ is a basis of $V$ provided that

- (linear independence) For distinct $x_1, \ldots, x_n \in X$ and $k_i \in K$,

  $$r_1x_1 + \cdots + r_nx_n = 0 \Rightarrow r_i = 0 \text{ for every } i$$

- (spans) For every $v \in V$ there exists $x_i \in X$ and $k_i \in K$ such that

  $$v = r_1x_1 + \cdots + r_nx_n.$$

**Theorem 1.** If $V$ is a vector space over a field $K$, then any two bases of $V$ have the same cardinality.

We denote the dimension of a (any) vector space by $\dim_K(V)$. 

Definition 3. Let $K$ be a field and $\phi : V \to W$ a map of $K$-vector spaces. Then $\phi$ is a homomorphism (linear map) if $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$, $v_i \in V$, and $\phi(kv) = k\phi(v)$, $v \in V$, $k \in K$.

2. Field Extensions

Definition 4. A field $F$ is said to be an extension field of $K$ provided that $K$ is a subfield of $F$. (Note: a subfield is a subring which is also a field.)

If $E$ is an extension field of $K$ and $F$ an extension field of $E$, then $E$ is said to be an intermediate field of $K$ and $F$.

If $F$ is an extension field of $K$, then $1_F = 1_K$. Note that $F$ is a vector space over $K$. We denote $\dim_K(F)$ by $[F : K]$. This notation should look familiar (index of a subgroup) and the following theorem should remind you of a theorem from last semester.

Theorem 2. Let $F$ be an extension field of $E$ and $E$ an extension field of $K$. Then $[F : K] = [F : E][E : K]$. Furthermore, $[F : K]$ is finite if and only $[F : E]$ and $[E : K]$ are finite.

Proof. Let $U$ be a basis of $F$ over $E$ and $V$ a basis of $E$ over $K$. We claim $X = \{vu \mid v \in V, u \in U\}$ is a basis of $F$ over $K$.

Let $f \in F$, then $f = \sum_{i=1}^{n} e_i u_i$ ($e_i \in E, u_i \in U$) and for each $e_i$, $e_i = \sum_{j=1}^{m} k_{ij} v_j$ ($k_{ij} \in K, v_j \in V$). Thus

$$f = \sum_{i=1}^{n} e_i u_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} k_{ij} v_j \right) u_i = \sum_{i} \sum_{j} k_{ij} v_j u_i.$$ 

Thus, $X$ spans $F$ as a vector space over $K$.

Suppose $\sum_{i=1}^{n} \sum_{j=1}^{m} k_{ij} v_j u_i = 0$ ($k_{ij} \in K, v_j \in V, u_i \in U$). Let $e_i = \sum_{j=1}^{m} k_{ij} v_j \in E$. Then

$$0 = \sum_{i} \sum_{j} k_{ij} v_j u_i = \sum_{i} e_i u_i.$$ 

Because $U$ is linearly independent over $E$, then for each $i$, $0 = s_i = \sum_{j} r_{ij} v_j$. Now because $V$ is linearly independent over $K$, $r_{ij} = 0$ for all $i, j$. It follows that $X$ is linearly independent over $K$, and hence a basis.

Since $U$ is linearly independent over $E$, then the the $vu$ are distinct. It follows that

Definition 5. Let $F$ be a field and $X \subset F$. The subring generated by $X$ is the intersection of all subrings of $F$ that contain $X$.

If $F$ is an extension field of $K$ and $X \subset F$, then the subring generated by $K \cup X$ is called the subring generated by $X$ over $K$ and is denoted $K[X]$. When $X$ is finite, say $X = \{u_1, \ldots, u_n\}$, then we denote $F = K[X]$ by $K[u_1, \ldots, u_n]$.

Note that in the above definition we could replace subring with subfield. The only thing that changes is the notation $K(X)$. The relation between $K[X]$ and $K(X)$ is analogous to the relation between polynomials and rational functions. The next theorem gives us an idea of what the elements of $K[X]$ and $K(X)$ actually look like. We will focus almost entirely on finitely generated extensions (i.e., $|X| < \infty$), though much of the theory carries through in the infinite case.

Theorem 3. Let $F$ be an extension field of a field $K$ and $u_i \subset F$.

(i) The subring $K[u_1, \ldots, u_m]$ consists of elements of the form $g(u_1, \ldots, u_m)$ where $g \in K[x_1, \ldots, x_m]$.

(ii) The subfield $K(u_1, \ldots, u_m)$ consists of elements of the form

$$h(u_1, \ldots, u_m)/k(u_1, \ldots, u_m) = h(u_1, \ldots, u_m)k(u_1, \ldots, u_m)^{-1}$$

where $h, k \in K[x_1, \ldots, x_m]$ and $k(u_1, \ldots, u_m) \neq 0$.

Proof. We’ll prove (i) in the case that $m = 1$. The general case, along with (ii), are left as an exercise.

Let $u \in F$ and $E = \{f(u) \mid f \in K[x]\}$. We claim $K[u] = E$. It is clear that $f(u) \in K[u]$ for all $f \in K[x]$ since $f(u)$ is an element of every ring containing $K$ and $u$. Hence, $E \subset K[u]$.

For the opposite inclusion we will show that $E$ is a ring containing $K$ and $u$. It then follows by definition that $K[u] \subset E$. But this follows from old-school theory of functions. Let $f, g \in K[x]$. Then $f(u) + g(u) = (f + g)(u)$ and $f(u)g(u) = (fg)(u)$. It is routine to check that $E$ is a group under addition and a monoid under multiplication. Moreover, the left and right distributive properties hold.

Of course, (ii) is a little trickier because you are dealing with fractions, but this just requires being more careful with addition. □
Not all field extensions are created equal. They type of extensions $K[u]$ depend on whether $u$ is the root of some polynomial in $K[x]$. Intuitively we know what this means, but let’s make it a little more precise.

**Definition 6.** Let $R$ be a subring of a commutative ring $S$, $c_1, \ldots, c_n \in S$ and $f \in R[x_1, \ldots, x_n]$ such that $f(c_1, \ldots, c_n) = 0$, Then $(c_1, \ldots, c_n)$ is said to be a root of $f$.

**Theorem 4** (Remainder Theorem). Let $R$ be a ring with identity and $f(x) \in R[x]$. For any $c \in R$, there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$.

*Proof.* If $f = 0$ then let $q = 0$. Now suppose $f \neq 0$. Then the Division Algorithm implies that there exist unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x)(x - c) + r(x)$ and $\deg(r(x)) < \deg(x - c) = 1$. Thus, $r(x) = r$ is a constant polynomial. It is left to show that $f(c) = r$.

If $q(x) = \sum_{j=0}^{n-1} b_j x^j$, then

$$f(x) = q(x)(x - c) + r = -b_0 c + \sum_{k=0}^{n-1} (-b_k c + b_k - 1)x^k + b_{n-1} x^n + r.$$

It follows that

$$f(c) = -b_0 c + \sum_{k=0}^{n-1} (-b_k c + b_k - 1)c^k + b_{n-1} c^n + r$$

$$= - \sum_{k=0}^{n-1} b_k c^{k+1} + \sum_{k=1}^{n} b_{k-1} c^k + r = 0 + r = r.$$  

\[\square\]

**Corollary 5.** Let $R$ be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of $f$ if and only if $x - c$ divides $f$.

**Definition 7.** Let $F$ be an extension field of $K$. An element $u \in F$ is said to be **algebraic** (resp. **transcendental**) provided that $u$ is (resp. is not) the root of some nonzero polynomial $f \in K[x]$. $F$ is called an **algebraic extension** of $K$ if every element of $F$ is algebraic over $K$. $F$ is called a **transcendental extension** if at least one element of $F$ is transcendental over $K$.

**Example 6.** Since $i \in \mathbb{C}$ is a root of $x^2 + 1 \in \mathbb{R}[x]$, then $i$ is is algebraic over $\mathbb{R}$. Moreover, $\mathbb{C} = \mathbb{R}(i)$.

On the other hand, $\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$.
**Theorem 7.** Let $F$ be an extension field of $K$ and $u \in F$. If $u$ is transcendental over $K$, then there is an isomorphism of fields $K(u) \cong K(x)$ which is the identity on $K$.

*Proof.* Suppose $u$ is transcendental over $K$, then for all $f, g \in K[x]$, $f(u), g(u) \neq 0$. Define a map

$$
\phi : K(x) \rightarrow F
$$

$$
f/g \mapsto f(u)/g(u) = f(u)g(u)^{-1}.
$$

Then $\phi$ is a well-defined monomorphism of fields and $\phi(k) = k$ for all $k \in K$. Since $\text{im} \phi = K(u)$ (by Theorem 3), then $K(x) \cong K(u)$. \hfill \square

**Theorem 8.** Let $F$ be an extension field of $K$ and $u \in F$. If $u$ is algebraic over $K$, then $K(u) = K[u]$ and $K(u) \cong K[x]/(f)$ where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(u) = 0$ and $g(u) = 0$ ($g \in K[x]$) if and only if $f$ divides $g$.

*Proof.* Let $\phi : K[x] \rightarrow K[u]$ be the substitution map. This is a nonzero ring epimorphism. Since $K[x]$ is a PID, then $\ker \phi = (f)$ for some $f \in K[x]$ with $f(u) = 0$. Since $u$ is algebraic, $\ker \phi \neq 0$ and since $\phi \neq 0$, $\ker \phi \neq K[x]$. Hence, $f \neq 0$ and $\deg f \geq 1$.

The leading coefficient, $c$, of $f$ is a unit in $K[x]$ and hence $c^{-1}f$ is monic and $(f) = (c^{-1}f)$. Thus, we may assume $f$ is monic.

Now by the First Isomorphism Theorem,

$$
K[x]/(f) = K[x]/\ker \phi \cong \text{im} \phi = K[u].
$$

Since $K[u]$ is an integral domain, the ideal $(f)$ is prime in $K[x]$. Therefore, $f$ is irreducible and hence the ideal $(f)$ is maximal, so $K[x]/(f)$ is a field. Since $K(u)$ is the smallest subfield of $F$ containing $K$ and $u$ and since $K[x]/(f) \cong K[u] \subset K(u)$, then $K(u) = K[u]$.

Uniqueness follows from

$$
g(u) = 0 \iff g \in \ker \phi = (f) \iff f \text{ divides } g.
$$

\hfill \square

**Theorem 9.** Let $F$ be an extension field of $K$ and $u \in F$. If $u$ is algebraic over $K$, then $U = \{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over $K$. Consequently, $[K(u) : K] = n$. 


Proof. By the previous theorem, \( K[u] = K(u) = K[x]/(f) \) for a monic irreducible polynomial \( f \in K[x] \) of degree \( n \) with \( f(u) = 0 \). Let \( k \in K[u] \), then \( k = g(u) \) for some \( g \in K[x] \). By the division algorithm, \( g = qf + h \) for some unique \( q, h \in K[x] \) and \( \deg h < \deg f \). Therefore,

\[
g(u) = q(u)f(u) + h(u) = 0 + h(u) = h(u) = b_0 + b_1u + \cdots + b_mu^m
\]

with \( m < n = \deg f \). Thus, \( U \) spans \( K(u) \) as a \( K \)-vector space.

Now suppose \( a_0 + a_1u + \cdots + a_{n-1}u^{n-1} = 0 \) with \( a_i \in K \). Then \( g = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in K[x] \) has \( u \) as a root and degree \( \leq n - 1 \). Since \( f | g \) and \( \deg f = n \), we must have \( g = 0 \) by the uniqueness of \( f \). Thus, \( a_i = 0 \) for all \( i \) so \( U \) is linearly independent. \( \square \)

**Definition 8.** Let \( F \) be an extension field of \( K \) and \( u \in F \) algebraic over \( K \). The monic irreducible polynomial \( f \) such that \( K(u) = K[x]/(f) \) is call the **minimal polynomial** of \( u \) (or the irreducible polynomial). The **degree of \( u \) over \( K \)** is \( \deg f = [K(u) : K] \).

Let’s recall some of our discussion on divisibility.

**Definition 9.** A polynomial \( f \in \mathbb{Z}[x] \) is called **primitive** if its coefficients have no common integer factor except for the units ±1.

**Proposition.** Let \( f \in \mathbb{Z}[x] \) and let \( p \) be a prime integer which does not divide the leading coefficient of \( f \). If the residue of \( f \) modulo \( p \) is irreducible, then \( f \) is irreducible in \( \mathbb{Q}[x] \).

**Example 10.** The polynomial \( f = x^3 - 3x - 1 \) is irreducible over \( \mathbb{Q}[x] \).

To see this, reduce mod 3. We have \( f \mod 3 = x^3 + 2 \). Sieving we find that this polynomial is irreducible in \( \mathbb{Z}_3[x] \) and hence irreducible in \( \mathbb{Q}[x] \).

Let \( u \) be a real root of \( f \). Such a root exists by the Intermediate Value Theorem. Then \( u \) has degree 3 over \( \mathbb{Q} \) and \( \{1, u, u^2\} \) is a basis of \( \mathbb{Q}(u) \) over \( \mathbb{Q} \).

Choose an element, say \( u^4 + 2u^3 + 3 \in \mathbb{Q}(u) = \mathbb{Q}[u] \). How do we write such an element as a linear combination of basis elements? First use the division algorithm to get

\[
x^4 + 2x^3 + 3 = (x + 2)(x^3 - 3x - 1) + (3x^2 + 7x + 5).
\]

This implies that in \( \mathbb{Q}(u) \),

\[
u^4 + 2u^3 + 3 = (u + 2)(u^3 - 3u - 1) + (3u^2 + 7u + 5)
= (u + 2)(0) + 3u^2 + 7u + 5
= 3u^2 + 7u + 5.
\]

6
Let’s summarize what we know and extend a little bit. Just a note/acknowledgement here that while this info is buried in Hungerford, the treatment presented here is shamelessly borrowed from Allen Bell’s graduate Algebra notes\(^1\).

**Proposition.** Let \( F \) be a field extension of \( K \) and \( u \in F \). The following statements are equivalent.

1. \( u \) is algebraic over \( K \)
2. \( [K[u] : K] < \infty \)
3. \( K[u] = K(u) \)

The proof of the above is left as an exercise. We’ve shown several directions. I’ll leave it to you to fill in the blanks.

**Corollary 11.** Let \( F \) be a field extension of \( K \) and \( u_1, \ldots, u_n \in F \). Then \( u_1, \ldots, u_n \) are algebraic over \( K \) if and only if they lie in a finite extension of \( K \).

**Proof.** (\( \Rightarrow \)) By hypothesis, \( K(u_i) \) is finite over \( K \), so \( u_i \) is algebraic over \( K \) by the previous proposition.

(\( \Leftarrow \)) Set \( K_i = K(u_1, \ldots, u_i) \), \( 1 \leq i \leq n \), with \( K_0 = K \). Then \( u_i \) is algebraic over \( K \) and hence over \( K_{i-1} \). By the proposition, \( F_i = F_{i-1}[u_i] \) is finite over \( F_{i-1} \). Thus, inductively by our first theorem,

\[
\dim_K F(u_1, \ldots, u_n) = \prod_{i=1}^{n} [F_i : F_{i-1}] < \infty.
\]

\( \square \)

**Proposition.** Let \( F \) be a field extension of \( K \) and \( u, v \in F \) algebraic over \( K \). Then \( u \pm v \), \( uv \), and \( u/v \) are algebraic over \( K \).

**Proof.** Any rational function of \( u \) and \( v \) lies in \( K(u,v) = K(u)(v) \). Now apply the previous corollary. \( \square \)

\( ^1 \)Allen Bell was my PhD advisor. The complete notes can be found at https://pantherfile.uwm.edu/adbell/www/Teaching/731/2008/book.pdf
3. Galois Groups

In this section we define the Galois group of a field extension as well as the notion of a Galois extension.

**Definition 10.** A nonzero map \( \sigma : E \to F \) of \( K \)-field extensions is a **\( K \)**-homomorphism if it is simultaneously a field homomorphism and a \( K \)-vector space.

**Exercise.** Let \( \sigma : E \to F \) be a map of \( K \)-field extensions. Prove that if \( \sigma \) is a field homomorphism then \( \sigma(1_E) = 1_F \). Prove that if \( \sigma(k) = k \) for all \( k \in K \) then \( \sigma \) is a \( K \)-homomorphism.

**Definition 11.** Let \( F \) be a field extension of a \( K \). If a field automorphism \( \sigma \in \text{Aut} F \) is a \( K \)-homomorphism, then \( \sigma \) is called a **\( K \)**-automorphism of \( F \). The group of all \( K \)-automorphisms of \( F \) is called the Galois group of \( F \) over \( K \) and is denoted \( \text{Aut}_K F \).

**Example 12.** Let \( F = K(x) \), with \( K \) any field.

For each \( a \in K \) with \( a \neq 0 \), the map

\[
F \to F \\
f(x)/g(x) \mapsto f(ax)/g(ax)
\]

is a \( K \)-automorphism of \( F \) (check!).

For each \( b \in K \), the map

\[
F \to F \\
f(x)/g(x) \mapsto f(x + b)/g(x + b)
\]

is a \( K \)-automorphism of \( F \) (check!).

If \( a \neq 1_K \) and \( b \neq 0 \), then \( \sigma_a \circ \tau_b \neq \tau_b \circ \sigma_a \) and \( \text{Aut}_K F \) is nonabelian.

**Example 13.** \( \mathbb{C} = \mathbb{R}(i) \). Complex conjugation,

\[
\mathbb{C} \to \mathbb{C} \\
a + bi \mapsto a - bi
\]

is a non-identity \( \mathbb{R} \)-automorphism of \( \mathbb{C} \).

It’s worth noting in the previous example that the map (complex conjugation) switches the two roots of the minimal polynomial \( x^2 + 1 \) of the field extension. This is not a coincidence.
Theorem 14. Let $F$ be an extension field of $K$ and $f \in K[x]$. If $u \in F$ is a root of $f$ and $\sigma \in \text{Aut}_K F$, then $\sigma(u) \in F$ is also a root of $f$.

Proof. Write $f = \sum_{i=1}^{n} k_i x^i$. Then

$$0 = \sigma(0) = \sigma(f(u)) = \sigma\left(\sum k_i u^i\right) = \sum \sigma(k_i)\sigma(u^i) = \sum k_i \sigma(u^i) = f(\sigma(u)).$$

\[\square\]

Corollary 15. Let $F$ be a field extension of $K$ and $u \in F$ algebraic over $K$ with minimal polynomial $f \in K[x]$ of degree $n$. If $m$ is the number of distinct roots of $f$ in $K(u)$, then $|\text{Aut}_K K(u)| \leq m$.

Example 16. • $|\text{Aut}_K K| = 1$.

• It follows from the corollary that $|\text{Aut}_K \mathbb{C}| \leq 2$. But complex conjugation is an order 2 automorphism, hence equality holds.

• If $u$ is a real cube root of 2, then $|\text{Aut}_\mathbb{Q} \mathbb{Q}(u)| = 1$ as the other roots of $x^3 - 2$ are complex.

• $|\text{Aut}_\mathbb{Q} \mathbb{R}| = 1$ (exercise)

Example 17. If $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$, then since $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$ then $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is a basis of $F$ over $\mathbb{Q}$. Let $\sigma \in \text{Aut}_\mathbb{Q} F$, then $\sigma$ is completely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Thus, by the previous theorem, $\sigma(\sqrt{2}) = \pm \sqrt{2}$ and $\sigma(\sqrt{3}) = \pm \sqrt{3}$. Thus, there are at most four distinct $\mathbb{Q}$-automorphisms of $F$ and each is indeed an automorphism. It follows that $\text{Aut}_\mathbb{Q} F \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Definition 12. Let $F$ be an extension field of $K$, $E$ an intermediate field and $H$ a subgroup of $\text{Aut}_K F$. The fixed field of $H$ in $F$ is defined as

$$F^H = \{ v \in F \mid \sigma(v) = v \text{ for all } \sigma \in H \}.$$ 

Furthermore, we define a subgroup of $\text{Aut}_K F$,

$$\text{Aut}_E F = \{ \sigma \in \text{Aut}_K F \mid \sigma(u) = u \text{ for all } u \in E \}.$$ 

Exercise. Prove that $F^H$ is an intermediate field of the extension $K \subset F$. Prove that $\text{Aut}_E F$ is a subgroup of $\text{Aut}_K F$.

Note that Hungerford denotes $F^H$ by $H'$ and $\text{Aut}_E F$ by $E'$.

Definition 13. Let $F$ be a field extension of $K$ such that the fixed field of the Galois group $\text{Aut}_K F$ is $K$ itself. Then $F$ is said to be a Galois extension (field) of $K$ or to be Galois over $K$. 

9
Another way to think of the above definition is that for every \( u \in F \setminus K \) there is a \( K \)-algebra homomorphism such that \( \phi(u) \neq u \).

**Example 18.** We claim that \( F = \mathbb{Q}(\sqrt{3}) \) is Galois over \( \mathbb{Q} \).

The minimal polynomial of \( u = \sqrt{3} \) over \( \mathbb{Q} \) is \( x^2 - 3 \). Hence, any \( K \)-automorphism of \( F \) either fixes \( u \) or sends it to \(-u\). It is clear that \( G = \text{Aut}_K F = \{ \text{id}, \sigma \} \) where \( \sigma(u) = -u \). Since a basis for \( F \) over \( K \) is \( \{ 1, u \} \), then it follows that \( F^G = K \) and \( F \) is Galois over \( \mathbb{Q} \).

**Definition 14.** If \( L, M \) are intermediate fields of an extension with \( L \subset M \), the dimension \([M : L]\) is called the **relative dimension** of \( L \) and \( M \). Similarly, if \( H, J \) are subgroups of the Galois group with \( H < J \), the index \([J : H]\) is called the **relative index** of \( H \) and \( J \).

**Lemma 19.** Let \( F \) be an extension field of \( K \) with intermediate fields \( L \) and \( M \). Let \( H \) and \( J \) be subgroups of \( G = \text{Aut}_K F \). Then

- \( \text{Aut}_F F = \langle \text{id} \rangle \) and \( \text{Aut}_K F = G \);
- \( F^{\langle \text{id} \rangle} = F \);
- \( L \subset M \Rightarrow \text{Aut}_M F < \text{Aut}_L F \);
- \( H < J \Rightarrow F^J \subset F^H \);
- \( L \subset F^{\text{Aut}_L F} \) and \( H \subset \text{Aut}_{F^H} F \);
- \( \text{Aut}_L F = \text{Aut}_{F^{\text{Aut}_L F}} F \) and \( F^H = F^{\text{Aut}_{F^H} F} \).

The proof of this lemma is left as an exercise. Most follow directly from the definitions above.

**Theorem 20** (Fundamental Theorem of Galois Theory). If \( F \) is a finite dimensional Galois extension of \( K \), then there is a 1-1 correspondence between the set of all intermediate field of the extension and the set of all subgroups of the Galois group \( \text{Aut}_K F \) (given by \( E \mapsto \text{Aut}_E F \)) such that

- the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups, in particular, \( \text{Aut}_K F \) has order \([F : K]\);
- \( F \) is Galois over every intermediate field \( E \), but \( E \) is Galois over \( K \) if and only if the corresponding subgroup \( \text{Aut}_E F \) is normal in \( \text{Aut}_K F \); in this case \( \text{Aut}_K F / \text{Aut}_E F \) is isomorphic to the Galois group \( \text{Aut}_K E \) of \( E \) over \( K \).

The theorem claims that the mapping \( E \mapsto \text{Aut}_E F = H \) is a 1-1 correspondence. So what’s the inverse? It’s obtained by taking the fixed field of \( F \) by \( H \). That is, \( F^H = E \).
Here’s the picture we want to keep in mind. Suppose $F$ is a (finite-dimensional) Galois extension of $K$ and $E$ an intermediate field such that $H = \text{Aut}_E F$ is normal in $G = \text{Aut}_K F$.

\[
\begin{align*}
\text{Aut}_F F &= \{e\} \quad \text{with} \quad F^{\{e\}} = F \\
\text{Aut}_E F &= H \quad \text{with} \quad F^H = E \\
\text{Aut}_K F &= G \quad \text{with} \quad F^G = K
\end{align*}
\]

**Example 21.** Let $F = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Then $F$ is Galois over $\mathbb{Q}$ (check!). We have already shown that $G = \text{Aut}_Q F \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Define the automorphisms $\sigma_i$ by

\[
\begin{align*}
\sigma_1 &= \text{id} \\
\sigma_2(\sqrt{2}) &= \sqrt{2}, \quad \sigma_2(\sqrt{3}) = -\sqrt{3} \\
\sigma_3(\sqrt{2}) &= -\sqrt{2}, \quad \sigma_3(\sqrt{3}) = \sqrt{3} \\
\sigma_4(\sqrt{2}) &= -\sqrt{2}, \quad \sigma_4(\sqrt{3}) = -\sqrt{3}
\end{align*}
\]

Each of the $\sigma_i, i \neq 1$ generates a proper (normal) subgroup of order 2.

The fixed fields are

\[
F^{(\sigma_2)} = \mathbb{Q}[\sqrt{2}], \quad F^{(\sigma_3)} = \mathbb{Q}[\sqrt{3}], \quad F^{(\sigma_4)} = \mathbb{Q}[\sqrt{6}].
\]

Hence, the correspondence can be visualized as

\[
\begin{array}{c}
\langle \sigma_1 \rangle \\
\langle \sigma_2 \rangle \\
\langle \sigma_3 \rangle \\
\langle \sigma_4 \rangle \\
G
\end{array}
\quad
\begin{array}{c}
\langle \sigma_1 \rangle \\
\langle \sigma_2 \rangle \\
\langle \sigma_3 \rangle \\
\langle \sigma_4 \rangle \\
\mathbb{Q}[\sqrt{2}] \\
\mathbb{Q}[\sqrt{3}] \\
\mathbb{Q}[\sqrt{6}]
\end{array}
\quad
\begin{array}{c}
F \\
\mathbb{Q}[\sqrt{2}] \\
\mathbb{Q}[\sqrt{3}] \\
\mathbb{Q}[\sqrt{6}]
\end{array}
\]

In each case $[F : \mathbb{Q}[\sqrt{k}]] = 2$ and $[G : \langle \sigma_i \rangle] = 2$.

We will now proceed with proving the fundamental theorem.

**Definition 15.** Let $F$ be a field extension of $K$. An intermediate field $E$ is called closed if $E = E^{\text{Aut}_E F}$. Similarly, a subgroup $H$ of the Galois group $\text{Aut}_K F$ is closed if $H = \text{Aut}_{F^H} F$. 
In Hungerford’s notation, this says $E = E''$ and $H = H''$. Recall that we always have one containment by Lemma 19. Note that $F$ is Galois over $K$ if and only if $K$ is closed.

**Theorem 22.** If $F$ is an extension field of $K$, then there is a 1-1 correspondence between the closed intermediate fields of the extension and the closed subgroups of the Galois group.

*Proof.* First note that if $E$ is a closed intermediate field, then by Lemma 19, $\text{Aut}_E F$ is closed. Similarly, if $H$ is a closed subgroup of the Galois group, then $F^H$ is closed.

Let $\mathcal{F}$ be the closed intermediate fields of the extension and $\mathcal{G}$ the closed subgroups of the Galois group $\text{Aut}_K F$. The Galois correspondence map gives maps

$$\phi: \mathcal{F} \to \mathcal{G}$$

$$E \mapsto \text{Aut}_E F$$

and

$$\psi: \mathcal{G} \to \mathcal{F}$$

$$H \mapsto F^H.$$

By closure, $\psi \circ \phi = \text{id}_\mathcal{F}$ and $\phi \circ \psi = \text{id}_\mathcal{G}$. □

If we knew that all intermediate field extensions of a finite dimensional Galois extension were closed and subgroups of the Galois group were closed then we would be done. Alas, we don’t know this...yet.

**Lemma 23.** Let $F$ be an extension field of $K$ and $L, M$ intermediate fields with $L \subset M$. If $[M : L]$ is finite, then $[\text{Aut}_L F : \text{Aut}_M F] \leq [M : L]$. In particular, if $[F : K]$ is finite, then $|\text{Aut}_K F| \leq [F : K]$.

*Proof.* Let $[M : L] = n < \infty$. If $n = 1$, then the result is trivial so suppose $n > 1$. By induction, suppose the result holds for all $i < n$ and choose $u \in M \setminus L$. Since $[M : L]$ is finite, $u$ is algebraic over $L$ with irreducible polynomial $f \in L[x]$ of degree $k > 1$. Then $[L(u) : L] = k$ and $[M : L(u)] = n/k$.

Case 1 ($k < n$) We have in this case $1 < n/k < n$. By the inductive hypothesis,

$$[\text{Aut}_L F : \text{Aut}_{L(u)} F] \leq k \text{ and } [\text{Aut}_{L(u)} F : \text{Aut}_M F] \leq n/k.$$  

Hence,

$$[\text{Aut}_L F : \text{Aut}_M F] = [\text{Aut}_L F : \text{Aut}_{L(u)} F][\text{Aut}_{L(u)} F : \text{Aut}_M F] \leq k \cdot n/k = n = [M : L].$$
Case 2 ($k = n$) We have in this case $[M : L(u)] = 1$ so $M = L(u)$. Let $S$ the set of all left cosets of $\text{Aut}_M F$ in $\text{Aut}_L F$, so $|S| = [\text{Aut}_L F : \text{Aut}_M F]$. Let $T$ be the set of all distinct roots of $f$ in $F$, so $|T| \leq n$. Let $H = \text{Aut}_M F$ and $J = \text{Aut}_L F$. Note that $H < J$. We claim there exists an injection $S \to T$ given by

$$\phi : S \to T$$

$$\tau H \mapsto \tau(u),$$

whence $|S| \leq |T|$.

This map makes sense because $\tau \in J$ and $u$ is a root of $f \in L[x]$. Hence $\tau(u)$ is also a root of $f$, so $\tau(u) \in H$. We need only check that the map $\phi$ is well-defined and injective.

If $\sigma \in H$, then since $u \in M$ we have $(\tau \circ \sigma)(u) = \tau(\sigma(u)) = \tau(u)$ Thus, every element of $H$ has the same effect on $u$ and maps $u \mapsto \tau(u)$ and so the map is well-defined.

For injectivity, choose $\tau, \rho \in J$ such that $\tau(u) = \rho(u)$. Then $\rho^{-1}(\rho(u)) = u$ so $\rho^{-1} \circ \tau$ fixes $u$ and therefore fixes $L(u) = M$ element-wise. Thus, $\rho^{-1} \circ \tau \in H$. Thus $\rho H = \tau H$ so $\phi$ is injective.


Proof. Let $[J : H] = n$ and suppose that $[F^H : F^J] > n$. Then there exists $u_1, \ldots, u_{n+1} \in F^H$ that are linearly independent over $F^J$. Let $\{\tau_1, \ldots, \tau_n\}$ be a complete set of left coset representatives of $H$ in $J$ and consider the system of $n$ homogeneous linear equations in $n = 1$ unknowns with coefficients $\tau_i(u_j) \in F$:

$$\tau_1(u_1)x_1 + \tau_1(u_2)x_2 + \cdots + \tau_1(u_{n+1})x_{n+1} = 0$$

$$\tau_2(u_1)x_1 + \tau_2(u_2)x_2 + \cdots + \tau_2(u_{n+1})x_{n+1} = 0$$

$$\vdots$$

$$\tau_n(u_1)x_1 + \tau_n(u_2)x_2 + \cdots + \tau_n(u_{n+1})x_{n+1} = 0.$$  \hspace{1cm} (1)

Let $S$ be the set of all nontrivial solutions to this system. $S \neq \emptyset$ (exercise). Choose a solution $(a_1, \ldots, a_{n+1}) \in S$ minimal with respect to the number of nonzero $a_i$. By reindexing, we may assume there exists $r \geq 1$ such that $a_1, \ldots, a_r \neq 0$ and $a_k = 0$ for $k > r$. Note that there is no loss in taking $a_1 = 1_F$. 

13
Here is an outline of our strategy. By hypothesis, the \( u_1, \ldots, u_{n+1} \in F^H \) are linearly independent over \( F^J \). We will show that this gives \( \sigma \in J \) such that \((\sigma(a_1), \ldots, \sigma(a_{n+1}))\) is a solution to the system. But then \((a_1 - \sigma(a_1), \ldots, a_{n+1} - \sigma(a_{n+1}))\) is also a solution and \( a_1 - \sigma(a_1) = 0 \). This solution has fewer nonzero entries than our original solution, contradicting minimality. Hence, the \( u_i \) cannot be linearly independent. That is, \( [F^H : F^J] \leq n = [J : H] \).

Choose the coset rep \( \tau_j \) such that \( \tau_j H = H \). WLOG, assume \( j = 1 \). Then \( \tau_1(u_i) = u_i \in F^H \) for all \( i \). Since the \( a_i \) form a solution to the system, then the first equation yields:

\[
u_1a_1 + \cdots + u_ra_r = 0.
\]

Because the \( u_i \) are linearly independent over \( F^J \) and the \( a_i \neq 0 \), then some \( a_i \), say \( a_2 \), is not in \( F^J \). Thus, there exists \( \sigma \in J \) such that \( \sigma(a_2) \neq a_2 \). Now consider the system

\[
\begin{align*}
\sigma \tau_1(u_1)x_1 + \sigma \tau_1(u_2)x_2 + \cdots + \sigma \tau_1(u_{n+1})x_{n+1} &= 0 \\
\sigma \tau_2(u_1)x_1 + \sigma \tau_2(u_2)x_2 + \cdots + \sigma \tau_2(u_{n+1})x_{n+1} &= 0 \\
& \vdots \\
\sigma \tau_n(u_1)x_1 + \sigma \tau_n(u_2)x_2 + \cdots + \sigma \tau_n(u_{n+1})x_{n+1} &= 0.
\end{align*}
\]

(2) Since \( \sigma \) is an automorphism and \((a_1, \ldots, a_r, 0, \ldots, 0)\) is a solution to (1), then it follows that \((\sigma(a_1), \ldots, \sigma(a_r), 0, \ldots, 0)\) is a solution to (2).

Our final claim is that (1) and (2) are in fact the same system (up to ordering of equations). (Exercise). \( \square \)

We are now ready to prove the main part of the fundamental theorem.

**Lemma 25.** Let \( F \) be an extension field of \( K \), \( L \) and \( M \) intermediate fields with \( L \subset M \), and \( H, J \) subgroups of \( \text{Aut}_K F \) with \( H < J \).

1. If \( L \) is closed and \([M : L] < \infty\), then \( M \) is closed and \([\text{Aut}_L F : \text{Aut}_M F] = [M : L] \);
2. if \( H \) is closed and \([J : H] < \infty\), then \( J \) is closed and \([F^H : F^J] = [J : H] \);
3. if \( F \) is a finite dimensional Galois extension of \( K \), then all intermediate fields and all subgroups of the Galois group are closed and \( \text{Aut}_K F \) has order \([F : K]\).

**Proof.** (1) Since \( M \subset F^{\text{Aut}_M F} \) and \( L = F^{\text{Aut}_L F} \) (by closure), then

\[
[M : L] \leq [F^{\text{Aut}_M F} : L] = [F^{\text{Aut}_M F} : F^{\text{Aut}_L F}] \leq [\text{Aut}_L F : \text{Aut}_M F] \leq [M : L].
\]

Thus, \( M = F^{\text{Aut}_M F} \) and \([M : L] = [\text{Aut}_L F : \text{Aut}_M F] \).

(2) Similar.
(3) If $E$ is an intermediate field then $[E : K]$ is finite. Since $F$ is Galois over $K$, $K$ is closed and (1) implies that $E$ is closed and $[\text{Aut}_K F : \text{Aut}_E F] = [E : K]$.

If $E = F$, then

$$|\text{Aut}_K F| = [\text{Aut}_K F : 1] = [\text{Aut}_K F : \text{Aut}_F F] = [F : K].$$

Therefore, $|\text{Aut}_K F| < \infty$ and so every subgroup of the Galois group is finite. Since 1 is closed, so is every subgroup by (2). □

All that is left of the fundamental theorem is to find the intermediate fields corresponding to normal subgroups of the Galois group.

**Definition 16.** If $E$ is an intermediate field of the extension $K \subset F$, then $E$ is said to be **stable** if every $K$-automorphism $\sigma \in \text{Aut}_K F$ maps $E$ to itself.

**Lemma 26.** Let $F$ be an extension field of $K$.

1. If $E$ is a stable intermediate field of the extension, then $\text{Aut}_E F$ is a normal subgroup of $\text{Aut}_K F$.
2. If $H$ is a normal subgroup of $\text{Aut}_K F$, then $F^H$ is a stable intermediate field of the extension.

**Proof.** (1) Let $\tau \in \text{Aut}_E F$ and $\sigma \in \text{Aut}_K F$. We claim $\sigma^{-1} \tau \sigma \in \text{Aut}_E F$, and normality follows directly from this. For any $u \in E$, $\sigma(u) \in E$ by stability. Hence $\tau(\sigma(u)) = \sigma(\tau(u))$. Therefore, $(\sigma^{-1} \tau \sigma)(u) = (\sigma^{-1} \sigma)(u) = u$, so $\sigma^{-1} \tau \sigma \in \text{Aut}_E F$.

(2) Choose $u \in F^H$ and $\sigma \in \text{Aut}_K F$. We claim $\sigma(u) \in F^H$. For any $\tau \in H$, $\sigma^{-1} \tau \sigma \in H$ by normality. Therefore, $(\sigma^{-1} \tau \sigma)(u) = u$. Then $\tau(\sigma(u)) = \sigma(\sigma^{-1} \tau \sigma)(u)$, so the claim follows and $F^H$ is stable. □

**Lemma 27.** Let $F$ be an extension field of $K$ and $E$ an intermediate field.

- If $F$ is Galois over $K$ and $E$ is stable, the $E$ is Galois.
- If $E$ is algebraic and Galois over $K$, then $E$ is stable (relative to $F$ and $K$).

**Proof.** (1) If $u \in E \setminus K$, then there exists $\sigma \in \text{Aut}_K F$ such that $\sigma(u) \neq u$ since $F$ is Galois over $K$. Since $\sigma$ maps $E$ to itself, then so does $\sigma^{-1}$. Hence, $\sigma \mid_E \in \text{Aut}_K E$ by stability. Therefore $E$ is Galois over $K$.

(2) Let $u \in E$ with minimal polynomial $f \in K[x]$ and let $u_1, \ldots, u_r$ be the distinct roots of $f$ that lie in $E$. Then $r \leq n = \deg f$. If $\tau \in \text{Aut}_K E$, then $\tau$ permutes the $u_i$. Hence, the
coefficients of \( g = (x - u_1) \cdots (x - u_r) \in E[x] \) are fixed by every \( \tau \in \text{Aut}_KE \). Since \( E \) is Galois over \( K \), we must have \( g \in K[x] \). Now \( u = u_1 \) is a root of \( g \) and hence \( f \mid g \). Since \( g \) is monic and \( \deg g \leq \deg f \), we must have \( f = g \). Thus, all roots of \( f \) are distinct and lie in \( E \).

Now if \( \sigma \in \text{Aut}_KF \), then \( \sigma(u) \) is a root of \( f \), whence \( \sigma(u) \in E \). Therefore, \( E \) is stable relative to \( F \) and \( K \). \( \square \)

**Definition 17.** Let \( E \) be an intermediate field of the extension \( K \subset F \). A \( K \)-automorphism \( \tau \in \text{Aut}_KE \) is said to be extendible to \( F \) if there exists \( \sigma \in \text{Aut}_KF \) such that \( \sigma \mid_F = \tau \).

**Lemma 28.** Let \( F \) be an extension field of \( K \) and \( E \) a stable intermediate field of the extension. Then the quotient group \( \text{Aut}_KF/\text{Aut}_EF \) is isomorphic to the group of all \( K \)-automorphisms of \( E \) that are extendible to \( F \).

**Proof.** Since \( E \) is stable, the assignment \( \sigma \to \sigma \mid_E \) defines a group homomorphism \( \text{Aut}_KF \to \text{Aut}_KE \) whose image is the subgroup of all \( K \)-automorphisms of \( E \) that are extendible to \( F \). Then the kernel of the map is \( \text{Aut}_EF \) and so the result follows by the First Isomorphism Theorem. \( \square \)

**Lemma 29.** Let \( F \) be a finite dimensional Galois extension over \( K \). Then \( F \) is Galois over every intermediate field \( E \), but \( E \) is Galois over \( K \) if and only if the corresponding subgroup \( \text{Aut}_EF \) is normal in \( \text{Aut}_KF \); in this case \( \text{Aut}_KF/\text{Aut}_EF \) is isomorphic to the Galois group \( \text{Aut}_EE \) of \( E \) over \( K \).

**Proof.** \( F \) is Galois over \( E \) since \( E \) is closed. \( E \) is finite dimensional over \( K \) (since \( F \) is) and hence algebraic over \( K \). Thus, if \( E \) is Galois over \( K \), then \( E \) is stable. It follows that \( \text{Aut}_EF \) is normal in \( \text{Aut}_KF \). Conversely if \( \text{Aut}_EF \) is normal in \( \text{Aut}_KF \), then \( F^{\text{Aut}_EF} \) is a stable intermediate field. But \( E = F^{\text{Aut}_EF} \) by closure and hence \( E \) is Galois over \( K \).

Suppose \( E \) is an intermediate field that is Galois over \( K \) (so that \( \text{Aut}_EF \) is normal in \( G = \text{Aut}_KF \). Since \( E \) and \( \text{Aut}_EF \) are closed and \( F^G = K \), then
\[
|G/\text{Aut}_EF| = [G : \text{Aut}_EF] = [F^{\text{Aut}_EF} : F^G] = [E : K].
\]

Now \( G/\text{Aut}_EF = \text{Aut}_KF/\text{Aut}_EF \) is isomorphic to a subgroup of \( \text{Aut}_KE \). But \( |\text{Aut}_KE| = [E : K] \). Hence, \( G/\text{Aut}_EF = \text{Aut}_KE \). \( \square \)
4. Splitting Fields

Definition 18. Let $F$ be an extension of a field $K$. A polynomial $f \in K[x]$ of positive degree is said to split over $F$ if $f$ can be written as a product of linear factors in $F[x]$. If $f$ splits over $F$ and $F = K(u_1, \ldots, u_n)$ where the $u_i$ are the roots of $f$ in $F$, then $F$ is said to be the splitting field over $K$ of $f$.

Any splitting field is algebraic over the base field. If $S \subset K[x]$ is finite, then the splitting field of (all polynomials in) $S$ coincides with the splitting field of the product of the polynomials in $S$.

Example 30. The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$. The splitting field of $x^2 + 1$ over $\mathbb{R}$ is $\mathbb{C}$.

Theorem 31. If $K$ is a field and $f \in K[x]$ has degree $n \geq 1$, then there exists a splitting field $F$ of $f$ with $[F : K] \leq n!$.

Proof. If $n = 1$, then $F = K$ is a splitting field of $f$. Suppose $n > 1$ and $f$ does not split over $K$, then choose an irreducible factor $g \in K[x]$ of degree greater than one. Since $g$ is irreducible, the ideal $(g)$ is maximal so $L = K[x]/(g)$ is a field. Let $\pi : K[x] \to K[x]/(g)$ be the canonical projection. Note that $\pi(K) \cong K$ so that $L$ may be considered as an extension field of $K$. Let $u = \pi(x) \in L$. Then $L = K(u)$, $g(u) = 0$, and $[L : K] = \deg g > 1$.

Now $u$ is a root of $g$ so $f = (x - u)h$ with $h \in K(u)[x]$. By induction, there exists a splitting field $F$ of $h$ over $K(u)$ of dimension at most $(n - 1)!$. It follows that

$$[F : K] = [F : K(u)](K(u) : K] \leq (n - 1)!(\deg g) \leq n!.$$

Definition 19. A field is algebraically closed if every nonconstant polynomial splits. An algebraically closed field extension $F$ of a field $K$ is said to be the algebraic closure of $K$.

Example 32. $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ (though this fact is nontrivial).

Theorem 33. Let $F$ be a field. TFAE:

1. Every nonconstant polynomial $f \in F[x]$ has a root in $F$;
2. Every nonconstant polynomial $f \in F[x]$ splits over $F$;
3. Every irreducible polynomial $f \in F[x]$ has degree one;
4. There is no algebraic extension field of $F$ (except $F$ itself);
5. there exists a subfield $K$ of $F$ such that $F$ is algebraic over $K$ and every polynomial in $K[x]$ splits in $F[x]$. 

17
The following theorem is proved in Hungerford (pages 259-260) but we will not prove it here. Nevertheless it is a good theorem to have around.

**Theorem 34.** Every field has an algebraic closure. Any two algebraic closures of \( K \) are \( K \)-isomorphic.

**Corollary 35.** If \( K \) is a field and \( S \) a set of polynomials (of positive degree) in \( K[x] \), then there exists a splitting field of \( S \) over \( K \).

We will focus almost entirely on splitting fields over finite sets of polynomials.

**Theorem 36.** Let \( \sigma : K \to L \) be an isomorphism of fields, \( S = \{ f_i \} \) a set of polynomials (of positive degree) in \( K[x] \), and \( S' = \{ \sigma(f_i) \} \) the corresponding set of polynomials in \( L[x] \). If \( F \) is a splitting field of \( S \) over \( K \) and \( M \) is a splitting field of \( S' \) over \( L \), then \( \sigma \) is extendible to an isomorphism \( F \cong M \).

We may sum up the previous theorem with the (commutative) diagram,

\[
\begin{array}{ccc}
K & \xrightarrow{\sigma} & L \\
\downarrow & & \downarrow \\
F & \xrightarrow{=} & M
\end{array}
\]

**Proof.** Assume \( S = \{ f \} \), which is equivalent to \( S \) consisting of finitely many polynomials. Let \( n = [F : K] \).

If \( n = 1 \), then \( F = K \) and \( f \) splits over \( K \). But then \( \sigma f \) splits over \( L \) so \( L = M \). Thus, \( \sigma \) is the desired isomorphism.

Proceed by induction. If \( n > 1 \), then \( f \) has an irreducible factor \( g \in K[x] \) with \( \deg g > 1 \). Let \( u \) be a root of \( g \) in \( F \). We claim \( \sigma(g) \) is irreducible in \( L[x] \). Suppose otherwise. Then \( \sigma(g) = pq \) with \( p, q \in L[x] \) of positive degree. But then

\[
g = \sigma^{-1}(\sigma(g)) = \sigma^{-1}(pq) = \sigma^{-1}(p)\sigma^{-1}(q),
\]

contradicting \( g \) irreducible. Let \( v \) be a root of \( \sigma(g) \). Then \( \sigma \) extends to an isomorphism \( \tau : K(u) \cong L(u) \) with \( \tau(u) = v \) (check!). Since \([K(u) : K] = \deg g > 1 \), then \([F : K(u)] < n \). Now \([F : K] = [F : K(u)][K(u) : K] \) (and similarly for \( M \) and \( L \)). Hence, since \( F \) is a splitting field of \( f \) over \( K(u) \) and \( M \) is a splitting field of \( \sigma(f) \) over \( L(u) \), the the induction hypothesis implies \( F \cong M \). \( \Box \)

**Definition 20.** Let \( K \) be a field and \( f \in K[x] \). The Galois group of \( f \) over \( K \) is defined to be \( \operatorname{Gal}_K(f) = \operatorname{Aut}_K F \) where \( F \) is any splitting field of \( f \).
Example 37. Let \( f = x^4 + 1 \in \mathbb{Q}[x] \). Then \( f \) is irreducible (exercise) and has roots \( e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4} \). Thus, the splitting field is \( F = \mathbb{Q}[e^{\pi i/4}] \). Any \( \sigma \in \text{Gal}(f) = \text{Aut}_\mathbb{Q} F \) is determined by its action on \( \sigma \), so \(|\text{Gal}(f)| = 4\). It is left as an exercise that any automorphism has order 2. Thus, \( \text{Gal}(f) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \).

Splitting fields satisfy a (sort of) universal property as follows. Let \( f \in K[x] \) and \( F \) a splitting field for \( f \). If \( E \) is an extension field of \( K \) in which \( f \) splits completely then there is a \( K \)-algebra homomorphism \( \phi : F \rightarrow E \) such that the following diagram commutes:

\[
\begin{array}{ccc}
K & \rightarrow & F \\
\downarrow \phi & & \downarrow \\
E & & \\
\end{array}
\]

The reason I added the (sort of) is because this \( \phi \) may not be unique (as required for this to truly be a universal property).

Definition 21. Let \( K \) be a field, \( f \in K[x] \) nonzero, and \( c \) a root of \( f \). Then \( f = (x-c)^m g(x) \) where \( g(c) \neq 0 \) and \( m \) is uniquely determined. If \( m = 1 \), then \( c \) is said to be a simple root. If \( m > 1 \), then \( c \) is said to be a multiple root.

Definition 22. Let \( K \) be a field. An irreducible polynomial \( f \in K[x] \) is said to be separable if in some splitting field of \( f \) over \( K \) every root of \( f \) is a simple root.

Example 38. \( x^2 + 1 \in \mathbb{Q}[x] \) is separable since \( x^2 + 1 = (x + i)(x - i) \in \mathbb{C}[x] \) (each root \( \pm i \) is simple). On the other hand, \( x^2 + 1 \in \mathbb{Z}_2[x] \) has no simple roots \( (x^2 + 1 = (x + 1)^2) \).

Theorem 39. If \( F \) is an extension field of \( K \), then the following are equivalent:

1. \( F \) is algebraic and Galois over \( K \);
2. \( F \) is separable over \( K \) and \( F \) is a splitting field over \( K \) of a set \( S \) of polynomials in \( K[x] \);
3. \( F \) is a splitting field over \( K \) of a set \( T \) of separable polynomials.

Definition 23. An algebraic extension field of \( F \) of \( K \) is normal over \( K \) if every irreducible polynomial in \( K[x] \) that has a root in \( F \) actually splits in \( F \).

Theorem 40. Let \( F \) be a finite field extension of \( K \). TFAE:

1. \( F \) is normal over \( K \);
2. \( F \) is a splitting field for some \( f \in K[x] \);
3. If \( E \) is any field extension of \( F \) and \( \phi : F \rightarrow E \) is a \( K \)-homomorphism, then \( \phi(F) = F \).
Proof. (1) $\Rightarrow$ (2) Let $F = K(u_1, \ldots, u_n)$ and let $f$ be the product of the minimal polynomials of the $u_i$. By normality, all roots of $f$ like in $E$, so $E$ is a splitting field for $f$.

(2) $\Rightarrow$ (3) Let $F$ be a splitting field for $f \in K[x]$, let $E$ be a field extension of $F$ and $\phi : F \to E$ a $K$-homomorphism. We know $F = K(u_1, \ldots, u_n)$ for the roots $u_i$ of $f$. Each $\phi(u_i)$ is another root, and so must lie in $F$. Hence, $\phi(F) \subset F$ and we have equality by comparing dimensions.

(3) $\rightarrow$ (1) Let $F = K(u_1, \ldots, u_n)$, and let $g \in K[x]$ be irreducible with $u \in F$. Let $f$ be the product of $g$ and the minimal polynomials of the $u_i$. Let $E$ be a splitting field for $f$ over $F$. Then $E$ is also a splitting field for $f$ over $K$. Choose $v$ a root of $g$ in $E$. Then there is an isomorphism $\phi : K(u) \to K(v)$ (check!). Now $\phi$ extends to an isomorphism $\phi : E \to E$. By hypothesis, $\phi(F) \subset \phi(F)$, so $v = \phi(u) \in F$. Hence, all roots of $g$ lie in $F$ so $F$ is normal over $K$. \qed
5. Solvability by radicals

Galois Theory has its roots in solving polynomial equations\(^2\). Here we will focus on low-degree polynomials and ask the question whether they can be solved by radical extensions. Let \( K \) be a field, \( f(x) = \sum_{i=0}^{n} a_i x^i \in K[x] \) irreducible and \( a_n = 1 \) (that is, \( f \) is monic). What are the roots of \( f \)? When \( n = 1 \) this is easy. When \( n = 2 \) we have the quadratic formula (so long as \( \text{char} K \neq 2 \)). That is, the roots of \( x^2 + bx + c \) are \( x = \frac{1}{2}(-b \pm \sqrt{b^2 - 4c}) \).

When \( n = 3 \), there is a formula but it is much more involved and bit trickier to derive (it’s still all high school algebra, though). Look up Cardano’s formula sometime if you want to see it.

We’ll approach this problem from the viewpoint of Galois Theory. Let \( \alpha_1, \alpha_2, \alpha_3 \) be the roots of \( f \). Then

\[
f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3.
\]

The coefficients lie in \( K \). Let \( F \) be a splitting field for \( f \) over \( K \). Then \( F = K(\alpha_i, \alpha_j) \) for any two roots of \( f \). (Since \( \alpha_1 + \alpha_2 + \alpha_3 \in K \), then we only need to adjoin two roots to get a basis.) There are two cases: either \( F = K(\alpha_i) \) for any \( i \), or \( K \subset K(\alpha_i) \subset F \).

Recall that the Galois group of a polynomial \( f \in K[x] \) is the group \( \text{Gal}(f) = \text{Aut}_K F \) where \( F \) is a splitting field of \( f \) over \( K \).

**Definition 24.** A subgroup \( G \) of the symmetric group \( S_n \) is said to be transitive if given any \( i \neq j \) (\( 1 \leq i, j \leq n \)), there exists \( \sigma \in G \) such that \( \sigma(i) = j \).

**Theorem 41.** Let \( K \) be a field and \( f \in K[x] \) a polynomial with Galois group \( G \).

1. \( G \) is isomorphic to a subgroup of some symmetric group \( S_n \).
2. If \( f \) is irreducible separable of degree \( n \), then \( n \) divides \( |G| \) and \( G \) is isomorphic to a transitive subgroup of \( S_n \).

**Proof.** (1) Let \( u_1, \ldots, u_n \) be the distinct roots of \( f \) in some splitting field \( F \) (\( 1 \leq n \leq \deg f \)). Then \( \sigma \in \text{Aut}_K F \) induces a permutation of the \( u_i \). Identify \( S_n \) with the set of all permutations of the \( u_i \). Thus, there exists a monomorphism \( \text{Aut}_K F \to S_n \).

(2) \( F \) is Galois over \( K \) and \( [K(u_1) : K] = n = \deg f \). Therefore, \( G \) has a subgroup of index \( n \) by the Fundamental Theorem, whence \( n \mid |G| \). For any \( i \neq j \) there is a \( K \)-isomorphism

\(^2\)This is by far the best joke in these notes.
σ : K(u_i) → K(u_j) such that σ(u_i) = u_j. Then σ extends to a K-automorphism of F, whence G is isomorphic to a transitive subgroup of S_n. □

**Corollary 42.** Let K be a field and f ∈ K[x] an irreducible polynomial of degree 2 with Galois group G. If f is separable, then G ≅ Z_2. Otherwise G = 1.

Note that the hypothesis that f is separable in the previous corollary always holds when charK ≠ 2.

What about our degree 3 polynomial f? The above theorem implies that the Gal(f) is (isomorphic to) a transitive subgroup of S_3. The transitive subgroups of S_3 are A_3 and S_3. The case of A_3 is not that interesting (since A_3 ≅ Z_3). So suppose Gal(f) ≅ S_3. Then [F : K] = 6 (where again F is the splitting field of f). The Galois correspondence then looks like Hence, the correspondence can be visualized as

Here L is the 2-dimensional subfield fixed by A_3. It has the form K[Δ] where Δ = √D for some D ∈ K (because the minimal polynomial for Δ is degree 2). Since δ is fixed by the 3-cycles in A_3, then Δ = ∏_{1≤i<j≤3}(α_i − α_j) and D = Δ^2. It is left as an exercise to verify that this element is fixed by A_3. Now D is fixed by all elements of S_3 (exercise!) so D ∈ K = F^{Gal(f)}. This element D is called the discriminant of f.

**Definition 25.** Let K be a field with charK ≠ 2 and f ∈ K[x] a polynomial of degree n with n distinct roots u_1, ..., u_n in some splitting field F of f over K. Let

\[ \Delta = \prod_{i<j}(u_i - u_j) ∈ F. \]
The discriminant of \( f \) is the element \( D = \Delta^2 \).

**Exercise.** With notation as in the definition, show that \( \Delta^2 \in K \) in general.

Suppose \( \text{char} K \neq 2, 3 \). Write \( f(x) = x^3 + bx^2 + cx + d \in K[x] \) and suppose \( f \) has three distinct roots in some splitting field. Let \( g(x) = f(x - b/3) \in K[x] \) (change-of-variable) then \( g \) has the form \( x^3 + px + q \) (check this) and the discriminant of \( f \) is \(-4p^3 - 27q^2\).

**Proposition.** Let \( K \) be a field and \( f \in K[x] \) an irreducible separable polynomial of degree 3. The galois group of \( f \) is either \( S_3 \) or \( A_3 \). If \( \text{char} K \neq 2, 3 \), it is \( A_3 \) if and only if the discriminant of \( f \) is the square of an element of \( K \).

**Example 43.** The polynomial \( x^3 - 3x + 1 \in \mathbb{Q}[x] \) is irreducible and separable since \( \text{char} \mathbb{Q} = 0 \). The discriminant is 81, which is a square in \( \mathbb{Q} \). Hence, the Galois group is \( A_3 \).

The polynomial \( f(x) = x^3 + 3x^2 - x - 1 \in \mathbb{Q}[x] \) may be rewritten
\[
g(x) = f(x - 3/3) = f(x - 1) = x^3 - 4x + 2,
\]
which is irreducible by Eisenstein’s Criterion. Hence, the discriminant is 148, which is not a square in \( \mathbb{Q} \). Thus the Galois group is \( S_3 \).

Now we turn to the question of whether an equation may be solved by radicals, or via radical extensions as we define now. We won’t finish this topic, but at least we will see an overview.

**Definition 26.** Let \( F \) be a field extension of \( K \).

We call \( F \) a **simple radical extension** if \( F = K(\alpha) \) where \( \alpha \) is a root of a polynomial \( x^n - a \in K[x] \).

We call \( F \) a **polyradical** (or just radical) extension if there is a finite tower of extensions \( K = F_0 \subset F_1 \subset \cdots \subset F_{m-1} \subset F_m = F \) such that each \( F_i/F_{i-1} \) is a simple radical extension.

A polynomial \( f \in K[x] \) is said to be **solvable by radicals** if there is a polyradical extension of \( F \) in which \( f \) splits completely.

Polyradical extensions correspond to polycyclic groups. Recall that a group \( G \) is polycyclic if there exists a tower \( \langle e \rangle = G_0 < G_1 < \cdots < G_{m-1} < G_m = G \) such that each \( G_i/G_{i-1} \) is cyclic.
Proposition. Suppose $F$ is a Galois extension of $K$ with $[F : K] = n$.

1. If $F$ has a primitive $n$th root of unity and $\text{Aut}_K F$ is polycyclic, then $F$ is a polyradical extension of $K$.

2. Suppose $F$ is a polyradical extension of $K$ with tower $K = F_0 \subset F_1 \subset \cdots \subset F_{m-1} \subset F_m = F$ such that each $F_i = F_{i-1}(\alpha_i)$ where $\alpha_i$ is a root of $x^{n_i} - a_i \in F_{i-1}[x]$, and suppose that $F$ contains a primitive $n_i$th root of unity for each $i$. Then $\text{Aut}_K F$ is polycyclic.

Theorem 44. Suppose $\text{char } K = 0$ and let $E$ be a finite Galois extension of $K$. Then $\text{Aut}_K E$ is polycyclic if and only if there exists an extension field $F$ of $E$ such that $F$ is a polyradical Galois extension of $K$.

Corollary 45. Suppose $\text{char } K = 0$ and $f \in F[x]$ is nonconstant. Then $f$ is solvable by radicals if and only if $\text{Gal}(f)$ is polycyclic.

Theorem 46. Let $n$ be prime and let $f \in \mathbb{Q}[x]$ be irreducible of degree $n$. Suppose that $f$ has exactly $n - 2$ real roots (in $\mathbb{C}$). Then $\text{Gal}(f) \cong S_n$. Thus, if $n \geq 5$, $f$ is not solvable by radicals.