# MATH 6122
# Algebra II

Joe Tran

Winter 2025

# Preface

These are the first edition of these lecture notes for MATH 6122 (Algebra II). Consequently, there may be several typographical errors, missing exposition on necessary background, and more advanced topics for which there will not be time in class to cover. Future iterations of these notes will hopefully be fairly self-contained provided one has the necessary background. If you come across any typos, errors, omissions, or unclear expositions, please feel free to contact me so that I may continually improve these notes.

# Contents

# Chapter 1

# Module Theory

This chapter will complete some of the remaining material on Module Theory from MATH 6121, including projective and injective modules, modules over PIDs (in particular, the structure theorem for finitely generated modules over PIDs), and algebras.

## 1.1 Projective and Injective Modules

In this section, we define projective modules in terms of modules, homomorphisms, and exact pairs of module homomorphisms. Since this definition depends on modules (the "objects" of interest) and homomorphisms (the "morphisms" on the objects), the idea of projective modules will be useful in the category setting. Just as we had dual statements in the category setting that resulted by reversing the "arrows" in a statement, the dual of projectivity is injectivity and the idea of an injective module.

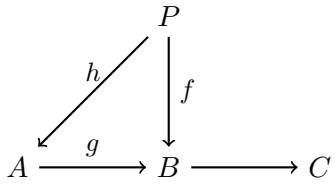
**Definition 1.1.1**

For modules $A$, $B$ and $C$ over $R$, and $f : A \to B$, $g : B \to C$ are $R$-module homomorphisms, that is $A \xrightarrow{f} B \xrightarrow{g} C$, the pair of homomorphisms is *exact* if $\Im(f) = \ker(g)$.

**Definition 1.1.2**

A module $P$ over a ring $R$ is said a *projective module* if given any diagram of $R$-module homomorphisms with bottom row $A \xrightarrow{g} B \to 0$ exact (that is, $g$ is an onto homomorphism), there exists an $R$-module homomorphism $h : P \to A$ such that $gh = f$.

The following diagram describes Definition 1.1.2 in terms of commuting maps.



**Remark 1.1.3**

Suppose $R$ is a ring with identity and $A$ and $B$ are $R$-modules. Then there are submodules $A_1, A_2$ and $B_1, B_2$ of $A$ and $B$, respectively, such that

(i) $A_1$ and $B_1$ are unitary.

(ii) $A = A_1 \oplus A_2$ and $B = B_1 \oplus B_2$ with $RA_2 = RB_2 = 0$.

Suppose for unitary $R$-module $P$ we have $R$-module homomorphism $f : P \to B$. Then we have that $f(R) \subset B_1$. Let $g$ be an $R$-module homomorphism with $g : A \to B$. If $g$ is an onto homomorphism, then both $g|_{A_1} : A_1 \to B_1$ and $g|_{A_2} : A_2 \to B_2$ are onto homomorphisms. Consider the three diagrams as shown:

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ A_1 \oplus A_2 & \xrightarrow{g} & B_1 \oplus B_2 & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ A_1 & \xrightarrow{g_1} & B_1 & \longrightarrow & 0 \end{array}$$

Let $h : P \to A$ be the $R$-module homomorphism such that $gh = f$. Then we also have that $h(P) \subset A_1$. So the claim $gh = f$ or $g(h(P)) = f(P) \subset B_1$ is the claim that for all $p \in P$, we have $g(h(p)) = f(p)$ or $h(p) \in A_1$, $f(p) \in B_1$ and $g : A_1 \to B_1$, we have $g|_A(h(p)) = f(p)$. So the elements of $A_2$ and $B_2$ (the "non-unitary" parts of $A$ and $B$) play no role in the claim that $gh = f$. So now we can show that $h_1 : P \to A_1$ exists such that for onto homomorphism $g_1 : A_1 \to B_1$ (in the above diagram on the right) we have $g_1 g_1 = f$, then we can take $h = h_1$ to give the desired function $f$ to establish that $P$ is projective (and conversely, we can take $g_1 = g|_A$ if we are given the diagram on the left and/or center above); notice that there si no claim of surjectivity except for $g$. That is, without loss of generality, we can show that unitary $R$-module $P$ is projective by assuming $R$-modules $A$ and $B$ are unitary.

Our first result gives us a family of examples of projective modules by showing that every free module over a ring with identity is projective.

**Theorem 1.1.4**

*Every free module $F$ over a ring with identity is projective.*

*Proof.*

By Remark 1.1.3, we see that it is sufficient to consider the diagram on the right, where $A$ and $B$ are unitary modules, $g$ is an onto homomorphism, and $F$ is a free $R$-module with, say, basis $X \subset F$. Let $\iota : X \to F$ be the inclusion map. For each $x \in X$, we have $f(\iota(x)) \in B$. Since $g$ is onto, there exists $a_x \in A$ such that $g(a_x) = f(\iota(x))$. Since $F$ is a free $R$-module, then the map $X \to A$ given by $x \mapsto a_x$ induces a unique $R$-module homomorphism $h : F \to A$ such that $h(c(x)) = a_x$ for all $x \in X$.

Consequently, $gh\iota(x) = g(a_x) = f(\iota(x))$ for all $x \in X$ so that $gh\iota = f\iota : X \to B$. Since $h$ is

unique, then with $g$ given and the inclusion mapping uniquely defined, then $gh\iota$ can be uniquely extended to all of $F$ to give $gh : F \to B$ as the only $R$-module homomorphism mapping $F \to B$ that takes on the given values on $X \subset F$. Since $f$ also has this property, $gh = f$. That is, by Definition 1.1.2, $F$ is a projective $R$-module, as desired. ∎

**Remark 1.1.5**

Theorem 1.1.4 holds if we drop the condition of $R$ having an identity and require $F$ to be a free module in the category of *all* left $R$-modules. The proof is the same as given for Theorem 1.1.4, but with Theorem 4.2.1 [1], and dropping "unitary". This is the sense in which the following corollary is stated. We can insert the condition that $R$ has an identity in the corollary and use the definition of "free $R$-module" based on Theorem 4.2.1 [1].

**Corollary 1.1.6**

*Every module $A$ over a ring $R$ is the homomorphic image of a projective module.*

*Proof.*

By Corollary 4.2.2 [1], $A$ is the homomorphic image of a free $R$-module $F$. By Theorem 1.1.4, modified as described in Remark 1.1.5, we have that free $R$-module $F$ is projective, so that $A$ is the homomorphic image of projection module $F$, as desired. ∎

**Remark 1.1.7**

The next result classified projective $R$-modules in terms of short exact and split exact sequences, and in terms of direct sums. Recall that a *short exact seqeunce* is of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

where $f$ is an into homomorphism and $g$ is an onto homomorphism, and $\Im(f) = \ker(g)$. A short exact sequence is *split exact* if there exists an $R$-module homomorphism $h : C \to b$ such that $gh = 1_C$ (or one of the equivalent conditions given in Theorem 4.1.18 [1]). Part (iii) of the following result refers to a free module $F$. This may be a free module either in sense of Theorem 4.2.1 [1] (though this case requires $R$ to have an identity and module $P$ of the next result to be unitary).

**Theorem 1.1.8**

*Let $R$ be a ring and let $P$ be a $R$-module. The following are equivalent.*

*(a) $P$ is projective.*

*(b) Every short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is split exact (hence, $B \simeq A \oplus P$)*

*(c) There exists a free module $F$ and an $R$-module $K$ such that $F \simeq K \oplus P$.*

*Proof.*

(a) $\Rightarrow$ (b) Consider the diagram given as follows

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle 1_P} & & \\ B & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

Since $P$ is projective, then $g$ is an onto homomorphism and there exists an $R$-module homomorphism $h : P \to B$ such that $gh = 1_P$. So the short exact sequence we need for (ii), $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ satisfies the condition $g^{-1} = h$.

Hence, $0 \to A \xrightarrow{f} B \underset{h}{\overset{g}{\leftrightarrows}} P \to 0$ where $gh = 1_P$. So by Theorem 4.1.18 (i) [1] (Theorem 4.1.18 [1] gives equivalent conditions for a short exact sequence to be split exact), the sequence is split exact, as claimed. By Theorem 4.1.18 (iii) [1], $B \simeq A \oplus P$ as claimed.

(b) $\Rightarrow$ (c) By Corollary 4.2.2 [1], there exists a free $R$-module $F$ and an onto homomorphism $g : F \to P$. Let $K = \ker(g)$. Then $0 \to K \xrightarrow{\iota} F \xrightarrow{g} P \to 0$ is an exact sequence (by Definition 4.1.16 [1]) and so by Theorem 4.1.18 (iii) [1] (where a split exact sequence is defined), we have $F \simeq K \oplus P$ as desired.

(c) $\Rightarrow$ (a) By assumption, since $F \simeq K \oplus P$, then there exists an isomorphism $\phi : F \to K \oplus P$. Define $\pi : F \to P$ as $\pi = \pi_P \phi$ with $\pi_P$ as the canonical projection onto $P$. Similarly, let $\iota : P \to F$ be the composition of the canonical injection map $P \to K \oplus P$ with $\phi^{-1}$.

With the following diagram of $R$-module homomorphisms (left), where the bottom row is exact, consider the augmented diagram (center)

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccc} & & F & & \\ & & \pi \uparrow \downarrow \iota & & \\ & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccc} & & F & & \\ & \swarrow^{h} & \pi \uparrow \downarrow \iota & & \\ & & P & & \\ & \swarrow^{h_1\iota} & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

Since $F$ is a free module by assumption, then by Theorem 1.1.4, $F$ is projective. We can modify the center diagram by composing $f$ and $\pi$ so that $f\pi : F \to B$ as in the diagram on the right. So the projectivity of $F$ then implies that there exists an $R$-module homomorphism $h_1 : F \to A$ such that $gh_1 = f\pi$. Let $h = h_1\iota : P \to A$ (since $\iota : P \to F$ and so $h_1 : F \to A$). Then

$$gh = g(h_1\iota) = (gh_1)\iota = (f\pi)\iota = f(\pi\iota) = f1_P = f$$

Therefore, by Definition 1.1.2, $P$ is projective. ∎

**Example 1.1.9**

$\mathbb{Z}_6$ is a free $\mathbb{Z}_6$-module with basis, say $\{1\}$. Then $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are $\mathbb{Z}_6$-modules. Since $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3$ by Theorem 1.1.8 (c) $\Rightarrow$ (a), we have that $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are projective as $\mathbb{Z}_6$-modules. But then if we consider $\mathbb{Z}_3 \simeq \{0, 2, 4\}$, then it is not a free $\mathbb{Z}_6$-module since there are no linearly independent subset of $\{0, 2, 4\}$; similarly, $\mathbb{Z}_2 \simeq \{0, 3\}$ is not a free $\mathbb{Z}_6$-module.

So we see that by Example 1.1.9, that the $R$-module $K$ and $P$ for which $F = K \oplus P$ need not be free $R$-modules.

**Proposition 1.1.10**

*Let $R$ be a ring. A direct sum of $R$-modules $\bigoplus_{i\in I} P_i$ is projective if and only if for all $i \in I$, $P_i$ is projective.*

*Proof.*

Suppose that $\bigoplus_{i\in I} P_i$ is projective. Consider the diagram given as follows:

$$\begin{array}{ccccc} & & \bigoplus_{i\in I} P_i & & \\ & & \Big\uparrow{\scriptstyle \pi_j} \Big\downarrow{\scriptstyle \iota_j} & & \\ & & P_j & & \\ & & \Big\downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

where $\bigoplus_{i\in I} P_i \simeq P_j \oplus \bigoplus_{\substack{i\in I \\ i\neq j}} P_i$. Then this is the same situation we had in the proof of Theorem 1.1.8 (c) $\Rightarrow$ (a) with $F = \bigoplus_{i\in I} P_i$, $P = P_j$, and $K = \bigoplus_{\substack{i\in I \\ i\neq j}} P_i$. The proof in Theorem 1.1.8 is only based on the fact that $F$ is projective. Since we have $F = \bigoplus_{i\in I} P_i$ is projective, then the same proof holds here to prove that $P_j$ is projective. SInce $j$ is an arbitrary element of $I$, we have $P_i$ is projective for all $i \in I$, as claimed.

Conversely, suppose $P_i$ is projective for all $i \in I$. Consider the diagram

$$\begin{array}{ccccc} & & P_j & & \\ & & \Big\uparrow{\scriptstyle \iota_j} \Big\downarrow{\scriptstyle \pi_j} & & \\ & & \bigoplus_{i\in I} P_i & & \\ & & \Big\downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

Since $P_j$ is projective, then there exists $h_j : P_j \to A$ such that $gh_j = f\iota_j$. Then by Theorem

4.1.13 [1], there exists a unique homomorphism $h : \bigoplus_{i\in I} P_i \to A$ with $h\iota_j = h_j$ for all $j \in I$. Now for $p$ in the direct sum $\bigoplus_{i\in I} P_i$, we have $p(i) = p_i \in P_i$ for finitely many $i \in I$, say $1 \leq i \leq n$, without loss of generality, and that $p(i) = 0 \in P_i$ for the remaining $i \in I$. Write $p = \sum_{k=1}^{n} y_k$, where $y_k(i) = p_i$ if $i = k$, and $y_k(i) = 0$ if $i \neq k$ so that $\iota(p_k) = y_k$ for all $1 \leq k \leq n$. Then we have that

$$\begin{aligned} gh(p) = gh\left(\sum_{k=1}^{n} y_k\right) &= \sum_{k=1}^{n} gh(y_k) = \sum_{k=1}^{n} gh(\iota_k p_k) = \sum_{k=1}^{n} gh_k(p_k) = \sum_{k=1}^{n} f\iota_k(p_k) \\ &= f\left(\sum_{k=1}^{n} \iota_k(p_k)\right) = f\left(\sum_{k=1}^{n} y_k\right) = f(p) \end{aligned}$$

Since $p$ is was arbitrary, we have $gh = f$, as desired, and thus, $\bigoplus_{i\in I} P_i$ is projective. ∎

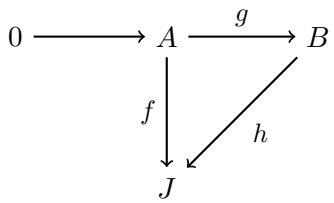
**Remark 1.1.11**

Recall that the dual of a statement in category theory results by "reversing arrows" in diagrams. In this spirit, we might say the dual of an onto homomorphism mapping $A \to B$ is an into homomorphism mapping $B \to A$. This is imprecise and incorrect if we think in terms of inverse functions, but that is not the intent, but is motivated by the fact that $B \to A$ is an onto homomorphism if and only if $B \to A \to 0$ is exact, and $A \to B$ is an into homomorphism if and only if $0 \to A \to B$ is exact. We mimic the definition of projective module, but with an attempt at duality.

**Definition 1.1.12**

A module $J$ over a ring $R$ is said to be an *injective module* if for any diagram of $R$-module homomorphisms with top row exact, i.e. $g$ is an into homomorphism, there exists an $R$-module homomorphism $h : B \to J$ such that $hg = f$.

The following diagram describes Definition 1.1.12 in terms of commuting maps.




**Remark 1.1.13**

The observations of Remark 1.1.3 concerning projective $R$-modules hold for injective modules as well. Indeed, without loss of generality, we can show that unitary $R$-modules $J$ is injective, by assuming $R$-modules $A$ and $B$ are unitary.

Recall that in categories, the dual concept of a direct sum (also called a coproduct, denoted by $\coprod$) is a direct product. Some, but not all, of the results on projective modules have dual results

on injective modules. The dual of Proposition 1.1.10 is the following.

**Proposition 1.1.14**

*A direct product of $R$-modules $\coprod_{i\in I} J_i$ is injective if and only if $J_i$ is injective for all $i \in I$.*

**Remark 1.1.15**

It is shown in Exercise 4.3.13 [1] that there is no dualized version of the concept of a free module (such a module, if it exists, would be called cofree). Since Theorem 1.1.4 and Theorem 1.1.8 (c) refer to free modules in the projective module setting, they do not have duals in the injective module setting. However, Theorem 1.1.4 does have a dual version in which it is claimed that every module can be embedded in an injective module. This proved in proposition **??**, after presenting the proofs of four preliminary lemmas. The dual versions of (a) and (b) of Theorem 1.1.8 is also given below in Proposition **??**. This proof is not needed, so we just state the lemmas and give some commentary.

**Lemma 1.1.16**

*Let $R$ be a ring with identity and let $J$ be an $R$-module. The following are equivalent.*

*(a) $J$ is injective.*

*(b) For every left ideal $L$ of $R$, any $R$-module homomorphism $L \to J$ may be extended to an $R$-module homomorphism $R \to J$.*

**Definition 1.1.17**

An abelian group $D$ is *divisible* if for any $d \in D$ and $k \in \mathbb{Z} \setminus \{0\}$, there exists a $x \in D$ such that $kx = d$.

It is shown in Exercise 4.3.4 [1] that $\mathbb{Q}$ is divisible, but $\mathbb{Z}$ is not. In Exercise 4.3.7 [1], it shown that the homomorphic image of a divisible group is divisible (part (a) and the direct sum of abelian groups is divisible if and only if each summand is divisible (parts (b) and (c))).

**Lemma 1.1.18**

*Let $D$ be a group. The following are equivalent.*

*(a) $D$ is divisible.*

*(b) $D$ is an injective unitary $\mathbb{Z}$-module.*

Divisible abelian groups (and hence, injective unitary $\mathbb{Z}$-modules, by Lemma 1.1.18) are classified in Example 4.3.11 [1]: *Every divisible abelian group is a direct sum of copies of $\mathbb{Q}$ and copies*

*of $Z(p^\infty)$ for various primes $p$.* Here, $Z(p^\infty)$ is defined as

$$Z(p^\infty) = \{a/b \in \mathbb{Q}/\mathbb{Z} : a, b \in \mathbb{Z}, b = p^i \text{ for some } i \geq 0\}$$

**Lemma 1.1.19**

*Every abelian group $A$ may be embedded in a divisible abelian group.*

**Lemma 1.1.20**

*If $J$ is a divisible abelian group and $R$ is a ring with identity, then $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an injective left $R$-module.*

**Proposition 1.1.21**

*Every unitary module $A$ over a ring with identity $R$ may be embedded in an injective $R$-module.*

**Proposition 1.1.22**

*Let $R$ be a ring with identity and $J$ be a unitary $R$-module. The following are equivalent.*

*(a) $J$ is injective.*

*(b) Every short exact sequence $0 \to J \xrightarrow{f} B \xrightarrow{g} C \to 0$ is split exact (hence, $B \simeq J \oplus C$).*

*(c) $J$ is a direct sum of any module $B$ of which it is a submodule.*

## 1.2 Modules Over a Principal Ideal Domain

This section is largely only necessary for Chapter 4 when discussing about Rank and Equivalence and Decompositions of a Single Linear Transformation and Similarity in Chapter 4 on Linear Algebra. We will focus on the structure of finitely generated modules over a principal ideal domain. In the process, we carry most results on finitely generated abelian groups to our setting. By convention, in this section, all modules are assumed to be unitary modules.

A free (unitary) module over a principal ideal domain $R$ with identity has the invariant property (since $R$ is a PID, then it is an integral domain so commutative). So the rank of a free rank $R$-module is well-defined. Two free $R$-modules are isomorphic if and only if they have the same rank. The next result is a generalization from the setting of finite rank free abelian groups.

**Theorem 1.2.1**

*Let $F$ be a free module over a principal ideal domain $R$ and $G$ be a submodule of $F$. Then $G$ is a free $R$-module and* $\mathrm{rank}(G) \leq \mathrm{rank}(F)$.

*Proof.*

Let $\{x_i\}_{i\in I}$ be a basis for $F$. Then $F = \sum_{i\in I} Rx_i$ with each $Rx_i$ isomorphic to $R$ as a left $R$-module. Choose a well-ordering $\leq$ of the set $I$. For each $i \in I$, denote the immediate successor of $i$ by $i+1$. Jet $J = I \cup \{\alpha\}$ where $\alpha \notin I$, and by definition $i < \alpha$ for all $i \in I$. Then $J$ is a well-ordered and every element of $I$ has an immediate successor in $J$. For each $j \in J$, define $F_i$ to be the submodule of $F$ generated by the set $\{x_i\}_{i<j}$. Then it can be checked that the submodules $F_i$ has the following properties:

(i) If $j < k$, then $F_j \subset F_k$.

(ii) $\bigcup_{j\in J} F_j = F$.

(iii) For each $i \in I$, $F_{i+1}/F_i \simeq Rx_i \simeq R$.

For each $j \in J$, let $G_i = G \cap F_j$,

(iv) If $j < k$ i, then $G_j \subset G_k$

(v) $\bigcup_{j\in J} G_j = G$.

(vi) For each $i \in I$, $G_i = G_{i+1} \cap F_i$.

(iv) implies that $G_{i+1}/G_i = G_{i+1}/(G_{i+1} \cap F_i) \simeq (G_{i+1} + F_i)/F_i$. But $(G_{i+1} + F_i)/F_i$ is a submodule of $F_{i+1}/F_i$. Therefore, $G_{i+1}/G_i$ is isomorphic to a submodule of $R$ by (iii). But every submodule of $R$ is necessarily an ideal of $R$ and hence of the form $\langle c\rangle = Rc$ for some $c \in R$. If $c \neq R$, then the $R$-module onto homomorphism $R \to \langle c\rangle$ is an isomorphism. Thus every submodule of $R$ is free of rank 0 or 1. The sequence then, $0 \to G_i \xrightarrow{\subset} G_{i+1} \to G_{i+1}/G_i \to 0$ is split exact for every $i \in I$. Then $G_{i+1}$ is an internal direct sum $G_{i+1} = G_i \oplus Rb_i$ where $b_i \in G_{i+1} - G_i$ and $Rb_i \simeq R$ if $G_{i+1} \neq G_i$, and $b_i = 0$ if $G_{i+1} = G_i$ (that us, $G_{i+1}/G_i = \{0\}$). Thus, $b_i \in G$ is defined for each $i \in I$. Let $B = \{b_i : b_i \neq 0\}$. Then $|B| \leq |I| = \text{rank}(F)$. To complete the proof, we need to show that $B$ is a basis of $G$.

Assume that $u = \sum_{j\in I} r_j b_j = 0$, where $j \in I$, $r_j \in R$ and we consider finite sum. Let $k$ be the largest index (if one exists) such that $r_k \neq 0$. Then $u = \sum_{j=1}^{k-1} r_j b_j + r_k b_k \in G_k \oplus Rb_k = G_{k+1}$. But $u = 0$ implies that $r_k = 0$, which is a contradiction. Hence, $r_j = 0$ for all $j$. Therefore, $B$ is linearly independent.

Finally, we need to show that $B$ spans $G$. It suffices by (v) to show that for each $k \in J$, the subset $B_k = \{b_j \in B : j < k\}$ of $B$ spans $G_k$. We shall use transfinite induction. Suppose therefore that $B_j$ spans $G_j$ for all $j < k$ and let $u = v + rb_j$ with $v \in G_j$. By inductive hypothesis, $v$ is a finite sum $v = \sum r_i b_i$ with $r_i \in R$ and $b_i \in B_j \subset B_k$. Therefore, $u = \sum r_i b_i + rb_k$ and so $B_k$ spans $G_k$. Now suppose that $k \neq j+1$ for all $j \in I$. Since $u \in G_k = G \cap F_k$, $u$ is a finite sum, $u = \sum r_i x_i$ with $j < k$. If $t$ is the largest index such that $r_t \neq 0$, then $u \in F_{i+1}$ with $t + 1 < k$ by assumption. Therefore, $u \in G \cap F_{t+1} = G_{t+1}$ with $t + 1 < k$. By assumption then, $u$ is a linear combination of elements of $B_{t+1}$, which is a subset of $B_k$. Moreover, $B_k$ spans $G_k$. ∎

**Corollary 1.2.2**

*Let $R$ be a principal ideal domain. If $A$ is a finitely generated $R$-module generated by $n$ elements, then every submodule of $A$ may be generated by $m$ elements with $m \leq n$.*

*Rest coming soon...*

## 1.3 Algebras

# Chapter 2

# Fields and Galois Theory

This chapter contains the most important results for this chapter: The Fundamental Theorem of Algebra and the Unsolvability of the Quintic. Hungerford's treatment of Galois theory is based on the approach of Irving Kaplansky who extended the ideas of Emil Artin. In Galois theory, we consider field $F$ an extension of field $K$; that is, $K$ is a subfield of $F$. The Galois group of extension $F$ of $K$ is the group of all automorphisms of $F$ that fix $K$ elementwise. The Fundamental Theorem of Galois Theory states that there exists a bijection between the intermediate fields of a finite-dimensional Galois field extension and the subgroups of the Galois group of the extension. The fundamental theorem allows us to translate problems involving fields, polynomials, and field extensions into group theoretic terms (thus making group theory the central part of abstract algebra as well as classical algebra–particularly, the algebraic solvability of a polynomial equation).

## 2.1 Field Extension

The basic facts needed for the study of field extensions are presented first, followed by a discussion of simple extensions. Finally, a number of essential properties of algebraic extensions are proved.

**Definition 2.1.1**

A field $F$ is said to be an *extension field* of $K$ (or simply an extension of $K$) provided that $K$ is a subfield of $F$.

If $F$ is an extension of $K$, then it is easy to note that $1_K = 1_F$. Furthermore, $F$ is a vector space over $K$. Throughout this chapter, the dimension of the vector space $F$ over $K$ will be denoted by $[F : K]$ rather than $\dim_K(F)$.

**Definition 2.1.2**

If $F$ is a field and $K$ is a subfield of $F$, then $F$ is said to be a *finite-dimensional extension* if $[F : K]$ is finite. If $[F : K]$ is not finite, then we say that $F$ is an *infinite-dimensional extension* if $[F : K]$ is infinite.

**Theorem 2.1.3**

*Let $F$ be a field extension of $E$, and $E$ be an extension field of $K$. Then*

$$[F : K] = [F : E][E : K]$$

*i.e. $F$ is a field extension of $K$. Furthermore, $[F : K]$ is finite if and only if $[F : E]$ and $[E : K]$ are finite.*

*Proof.*

The proof is very easy; to see that $F$ is a field extension of $K$, then note since we have $F$ is a field extension of $E$, then we have $[F : E]$, and similarly, since $E$ is a field extension of $K$, then we have $[E : K]$, and therefore,

$$[F : K] = [F : E][E : K]$$

Therefore, $F$ is a field extension of $K$.

To prove the second assertion, first note that if $[F : E]$ and $[E : K]$ are finite, then $[F : K]$ is also finite. Conversely, if $[F : E]$ and $[E : K]$ are infinite, then so is $[F : K]$.

**Definition 2.1.4**

If $F$ is a field extension of $E$ and $E$ is a field extension of $K$, i.e. $K \leq E \leq F$, then we call $E$ an *intermediate field*.

**Definition 2.1.5**

If $F$ is a field and $X \subset F$, then the *subfield* (resp. *subring*) *generated by* $X$ is the intersection of all subfields (resp. subrings) of $F$ that contain $X$. If $F$ is a field extension of $K$ and $X \subset F$, then the subfield (resp. subring) generated by $K \cup X$ is called the *subfield* (resp. *subring*) *generated by* $X$ *over* $K$ and is denoted by $K(X)$ (resp. $K[X]$). Note that $K[X]$ is necessarily an integral domain.

**Definition 2.1.6**

If $X = \{x_1, ..., x_n\}$, then the subfield $K(X)$ (resp. subring $K[X]$) of $F$ is denoted by $K(x_1, ..., x_n)$ (resp. $K[x_1, ..., x_n]$). The field $K(x_1, ..., x_n)$ is said to be *finitely generated extension* of $K$ (but it need not be finite-dimensional over $K$). If $X = \{x\}$, then $K(x)$ is said to be a *simple extension of* $K$.

**Theorem 2.1.7**

*If $F$ is an extension field of a field $K$, $x$, $x_1, ..., x_n \in F$, and $X \subset F$, then*

*(i) The subring $K[x]$ consists of all elements of the form $f(x)$, where $f$ is a polynomial*

*with coefficients in $K$.*

*(ii) The subring $K[x_1, ..., x_n]$ consists of all elements of the form $f(x_1, ..., x_n)$ where $f$ is a polynomial in $n$ indeterminates with coefficients in $K$.*

*(iii) The subring $K[X]$ consists of all elements of the form $f(x_1, ..., x_n)$, where each $x_i \in X$, $n \in \mathbb{N}$, and $f$ is a polynomial in $n$ indeterminates with coefficients in $K$.*

*(iv) The subfield $K(x)$ consists of all elements of the form $f(x)g^{-1}(x)$ where $f, g \in K[x]$ and $g(x) \neq 0$.*

*(v) The subfield $K(x_1, ..., x_n)$ consists of all elements of the form $f(x_1, ..., x_n)g^{-1}(x_1, ..., x_n)$ where $f, g \in K[x_1, ..., x_n]$ and $g(x_1, ..., x_n) \neq 0$.*

*(vi) The subfield $K(X)$ consists of all elements of the form $f(x_1, ..., x_n)g^{-1}(x_1, ..., x_n)$ where $n \in \mathbb{N}$, $f, g \in K[x_1, ..., x_n]$, $x_1, ..., x_n \in X$ and $g(x_1, ..., x_n) \neq 0$.*

*(vii) For each $v \in K(X)$ (resp. $K[X]$), there exists a finite subset $Y$ subset of $X$ such that $v \in K(Y)$ (resp. $K[Y]$).*

*Proof.*

We will only prove (vi) and (vii).

To see that (vi) holds, note that every field that contains $K$ and $X$ must contain the set

$$E = \left\{ \frac{f(x_1, ..., x_n)}{g(x_1, ..., x_n)} : n \in \mathbb{N}, f, g \in K[x_1, ..., x_n], x_1, ..., x_n \in X, g(x_1, ..., x_n) \neq 0 \right\}$$

and so $E \subset K(X)$. For the other inclusion, if $f, g \in K[x_1, ..., x_m]$ and $f_1, g_1 \in K[x_1, ..., x_n]$, then define $h, k \in K[x_1, ..., x_{m+n}]$ by

$$h(x_1, ..., x_{m+n}) = f(x_1, ..., x_m)g_1(x_{m+1}, ..., x_{m+n}) - g(x_1, ..., x_m)f_1(x_{m+1}, ..., x_{m+n})$$

and $k(x_1, ..., x_{m+n}) = g(x_1, ..., x_m)g_1(x_{m+1}, ..., x_{m+n})$. Then for any $x_1, ..., x_m$, $y_1, ..., y_n \in X$ such that $g(x_1, ..., x_m) \neq 0$ and $g(y_1, ..., y_n) \neq 0$,

$$\frac{f(x_1, ..., x_m)}{g(x_1, ..., x_m)} - \frac{f_1(y_1, ..., y_n)}{g_1(y_1, ..., y_n)} = \frac{h(x_1, ..., x_m, y_1, ..., y_n)}{k(x_1, ..., x_m, y_1, ..., y_n)} \in E$$

Therefore, $E$ is an additive subgroup of $F$. Similarly,

$$\frac{\frac{f(x_1,...,x_m)}{g(x_1,...,x_m)}}{\frac{f_1(y_1,...,y_n)}{g_1(y_1,...,y_n)}} = \frac{f_2(x_1, ..., x_m, y_1, ..., y_n)}{g_2(x_1, ..., x_m, y_1, ..., y_n)} \in E$$

and so $E \setminus \{0\}$ is a multiplicative subgroup. So $E$ is a field. Since $K(X)$ is the intersection of all fields containing $K \cup X$, then $K(X) \subset E$. Therefore, $K(X) = E$.

To see that (vii) holds, if $x \in K(X)$, then by (vi),

$$x = \frac{f(x_1, ..., x_n)}{g(x_1, ..., x_n)}$$

for some $n \in \mathbb{N}$ and $f, g \in K[x_1, ..., x_n]$. So with $X' = \{x_1, ..., x_n\}$, we have $x \in K(X')$. ■

**Definition 2.1.8**

If $K$ and $L$ are subfields of a field $F$, the *composite* of $K$ and $L$ in $F$, denoted by $KL$, is the subfield generated by the set $X = K \cup L$.

We now distinguish between two types of elements of an extension field. This is fundamental to all that follows.

**Definition 2.1.9**

Let $F$ be an extension field of $K$.

(i) An element $\alpha \in F$ is *algebraic* over $K$ if $\alpha$ is a root of some polynomial $p \in K[x]$.

(ii) If $\alpha$ is not a root of any nonzero $p \in K[x]$, then $\alpha$ is *transcendental* over $K$.

(iii) $F$ is an *algebraic extension* of $K$ if every element of $F$ is algebraic over $K$.

(iv) $F$ is a *transcendental extension* if at least one element of $F$ is transcendental over $K$.

**Example 2.1.10**

The most common example of an algebraic extension field is

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

Another useful algebraic extension is

$$\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} \simeq \mathbb{C}$$

The list of known transcendental real numbers is brief, but includes $\pi$ and $e$. A readable account of transcendental numbers is *Making Transcendence Transparent: An Intuitive Approach to Classical Transcendental Number Theory* by E. Burger and R. Tubbs, Springer (2004).

**Example 2.1.11**

If $K$ is a field, then the polynomial ring $K[x_1, ..., x_n]$ is an integral domain. The field of quotients of $K[x_1, ..., x_n]$ is denoted $K(x_1, ..., x_n)$. The elements of field $K(x_1, ..., x_n)$ consist of all fractions $fg^{-1}$ where $f, g \in K[x_1, ..., x_n]$ and $g \neq 0$. The field $K(x_1, ..., x_n)$ is the *field of rational functions* in indeterminates $x_1, ..., x_n$ over $K$.

In the following two theorems, we classify simple extensions (first, extending by a transcendental and second extending by an algebraic).

**Theorem 2.1.12**

*If $F$ is an extension field of $K$ and $\alpha \in F$ is transcendental over $K$, then there exists an isomorphism of fields $K(\alpha) \simeq K(x)$ which is the identity when restricted to $K$.*

*Proof.*

Assume that $\alpha$ is transcendental. Then $f(\alpha), g(\alpha) \neq 0$ for all nonzero $f, g \in K[x]$. Let $\phi : K(x) \to F$ by the map $fg^{-1} \mapsto f(\alpha)g(\alpha)^{-1}$. "Clearly", $\phi$ is a homomorphism. Now for $f_1 g_1^{-1} \neq f_2 g_2^{-1}$ then $f_1 g_2 \neq f_2 g_1$ and $f_1 g_2 - f_2 g_1 \neq 0$ (not the zero polynomial). Now,

$$f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha) \neq 0$$

and so

$$\phi(f_1 g_1^{-1}) = f_1(\alpha)g_1(\alpha)^{-1} \neq f_2(\alpha)g_2(\alpha)^{-1} = \phi(f_2 g_2^{-1})$$

Therefore, $\phi$ is an injection. Also, $\phi$ is the identity on $K$ (treating $K$ as a subfield of $K(x)$; think of $K$ as the constant rational functions in $F(x)$). Therefore, by Theorem 2.1.7 (iv), the image of $\phi$ is $K(\alpha)$, so $\phi$ is an isomorphism from $K(x)$ to $K(\alpha)$ which is the identity on $K$. ∎

**Theorem 2.1.13**

*If $F$ is an extension field of $K$ and $\alpha \in F$ is algebraic over $K$, then*

*(i)* $K(\alpha) = K[\alpha]$.

*(ii)* $K(\alpha) \simeq K[x]/\langle f \rangle$, *where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(\alpha) = 0$ and $g(\alpha) = 0$, where $g \in K[x]$, if and only if $f \mid g$.*

*(iii)* $[K(\alpha) : K] = n$

*(iv)* $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ *is a basis of the vector space $K(\alpha)$ over $K$.*

*(v) Every element of $K(\alpha)$ can be written uniquely of the form*

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$$

*where each $a_i \in K$.*

Theorem 2.1.13 tells us what elements of the algebraic extension $K(\alpha)$ of $K$ "look like". That is, there exists a fixed $n \in \mathbb{N}$ such that every element of $K(\alpha)$ is of the form

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

for some $a_i \in K$. Notice that Theorem 2.1.12 and Theorem 2.1.7 (iv) tell us what elements of the

transcendental extension $K(\alpha)$ of $K$ "look like":

$$\frac{a_0 + a_1\alpha + \cdots + a_n\alpha^n}{b_0 + b_1\alpha + \cdots + b_m\alpha^m}$$

where $a_1, ..., a_n, b_1, ..., b_m \in K$ and $b_0 + b_1\alpha + \cdots + b_m\alpha^m \neq 0$.
*Proof.*

We first prove (i) and (ii). Define $\phi : K[x] \to K[\alpha]$ by $g \to g(\alpha)$. It is easy to see that $\phi$ is a ring homomorphism. By Theorem 2.1.7 (i), $\phi$ is onto. Since $K$ is a field, then $K[x]$ is a principal ideal domain. Now, $\ker(\phi)$ is an ideal, so $\ker(\phi) = \langle f \rangle$ for some $f \in K[x]$. Notice that $\phi(f) = f(\alpha) = 0$. Since $\alpha$ is algebraic, $\ker(\phi) \neq \{0\}$. Also, $\ker(\phi) \neq K[x]$ (for example, nonzero constant polynomials are not mapped to zero). So $f \neq 0$ and $\deg(f) \geq 1$. Furthermore, if $c$ is the leading coefficient of $f$, then $c$ is a unit in $K[x]$, and so $c^{-1}f$ is monic. Consequently, without loss of generality, assume that $f$ is monic. Then by the First Isomorphism Theorem of Rings, $K[x]/\langle f \rangle = K[x]/\ker(\phi) \simeq \text{Range}(\phi) = K[\alpha]$. Since $K[\alpha]$ is an integral domain, since $K$ is a field, the ideal of $\langle f \rangle$ is prime. Since $\langle f \rangle$ is a prime ideal, then $f$ itself is a prime element of $K[x]$ and so, $f$ is irreducible in $K[x]$ (notice that $K[x]$ is a principal ideal domain as explained above), and thus, $\langle f \rangle$ is a maximal ideal in $K[x]$. Consequently, $K[x]/\langle f \rangle$ is a field. Now, since $K(\alpha)$ is the smallest subfield of $F$ containing $K \cup \{\alpha\}$ (since $K(\alpha)$ is the intersection of all subfields of $F$ containing $K \cup \{\alpha\}$), and $K[\alpha]$ is a ring containing $K \cup \{\alpha\}$, but $K[\alpha]$ is a subfield since $K[\alpha] \simeq K[x]/\langle f \rangle$, then $K(\alpha) \subset K[\alpha]$. However, in general, the ring $K[\alpha]$ is a subset of the field $K(\alpha)$, so $K(\alpha) \supset K[\alpha]$, so we must have $K(\alpha) = K[\alpha]$, and (i) follows. We have established (ii), except for the uniqueness claim. Suppose $g(\alpha) = 0$ for $g \in K[x]$. Then $\phi(g) = g(\alpha) = 0$, and so $g \in \ker(\phi) = \langle f \rangle$. Since the principal ideal $\langle f \rangle$ consists of all multiples of $f$, then $g$ is a multiple of $f$, that is, $f$ divides $g$, so (i) follows.

We next prove (iv). By Theorem 2.1.7 (i), every element of $K[\alpha] = K(\alpha)$ is of the form $g(\alpha)$ for some $g \in K[x]$. By the Division Algorithm, we know that $g(x) = q(x)f(x) + r(x)$ with $q, r \in K[x]$, and $\deg(r) < \deg(f)$. Therefore,

$$g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = 0 + r(\alpha) = b_0 + \cdots + b_m\alpha^m$$

with $m < n = \deg(f)$. Thus, every element of $K(\alpha)$ can be written as a linear combination of $1_K, \alpha, \alpha^2, ..., \alpha^{n-1}$. That is, $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ spans $K(\alpha)$. Now, to see that $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is linearly independent over $K$, assume

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

for some $a_0, ..., a_{n-1} \in K$. Then

$$g = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in K[x]$$

has $\alpha$ as a root and has a degree of at most $n-1$. Then by (ii), $f \mid g$ and $\deg(f) = n$, so it must be that $g = 0$; i.e. $a_i = 0$ for all $i$, and so $\{1_K, ..., \alpha^{n-1}\}$ is linearly independent and hence is a basis of $K(\alpha)$.

Next, we prove (iii). Note that $[K(\alpha) : K]$ denotes the dimension of $K(\alpha)$ as a vector space.

So by (iv), we have

$$K[(\alpha) : K] = n$$

Now we prove (v). By (iv), every element of $K(\alpha)$ can be written in the form

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

for some $a_0, ..., a_{n-1} \in K$, since $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis. For uniqueness, suppose

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

Then

$$(a_0 - b_0) + (a_1 - b_1)\alpha + \cdots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0$$

and since $\{1_K, \alpha, ..., \alpha^{n-1}\}$ is linearly independent, so

$$a_0 - b_0 = \cdots = a_{n-1} - b_{n-1} = 0$$

and thus, $a_i = b_i$ for all $0 \leq i \leq n-1$, and the representation is unique. ∎

**Definition 2.1.14**

Let $F$ be an extension field of $K$ and $\alpha \in F$ algebraic over $K$. The monic irreducible polynomial $f$ of Theorem 2.1.13 (ii) is the *irreducible polynomial of* $\alpha$. The *degree of* $\alpha$ *over* $K$ is $\deg(f) = [K(\alpha) : K]$.

**Example 2.1.15**

The polynomial $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$, since the only possible rational roots are $\pm 1$, neither of which is a root (we have also used the Factor Theorem here). By the Intermediate Value Theorem, there exists a real root $\alpha$. Now, $x^3 - 3x - 1$ is irreducible polynomial of $\alpha$, so $\alpha$ has degree 3 over $\mathbb{Q}$, and $\{1, \alpha, \alpha^2\}$ is a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ by Theorem 2.1.13 (iv). Now, $\alpha^4 + 2\alpha^3 + 3 \in \mathbb{Q}(\alpha)$ and so must be some linear combination of $1, \alpha, \alpha^2$. The division algorithm in $\mathbb{Q}[x]$ gives

$$x^4 + 2x^3 + 3 = (x + 2)(x^3 - 3x - 1) + (3x^2 + 7x + 5)$$

and so

$$\begin{aligned} \alpha^4 + 2\alpha^3 + 3 &= (\alpha + 2)(\alpha^3 - 3\alpha - 1) + (3\alpha^2 + 7\alpha + 5) \\ &= (\alpha + 2)(0) + (3\alpha^2 + 7\alpha + 5) \\ &= 3\alpha^2 + 7\alpha + 5 \end{aligned}$$

In notation of linear algebra, we would say that $\alpha^4 + 2\alpha^3 + 3$ has coordinate representation $[5, 7, 3]_B$ with respect to the ordered basis $B = \{1, \alpha, \alpha^2\}$.

Suppose we have the fields $K \leq E$ and $L \leq F$ and $\sigma : K \to L$ is an isomorphism between $E$

and $F$. The following result addresses this for simple extensions.

**Theorem 2.1.16**

*Let $\sigma : K \to L$ be an isomorphism of fields, $\alpha$ be an element of some extension field of $K$ and $\beta$ be an element of some extension field of $L$. Assume either*

*(i) $\alpha$ is transcendental over $K$ and $\beta$ is transcendental over $L$.*

*(ii) $\alpha$ is a root of an irreducible polynomial $f \in K[x]$ and $\beta$ is a root of $\sigma f \in L[x]$.*

*Then $\sigma$ extends to an isomorphism of fields $K(\alpha) \simeq L(\beta)$ which maps $\alpha$ onto $\beta$.*

*Proof.*

Assume that (ii) does not hold. We will show that (i) holds. Since $\sigma : K \to L$ is an isomorphism, then the mapping $K[x] \to L[x]$ given by

$$\sum_{i=0}^{n} r_i x^i \mapsto \sum_{i=0}^{m} \sigma(r_i) x^i$$

is an isomorphism. By Theorem 2.1.7 (iv), every element of $K(x)$ is of the form $hg^{-1}$ for some $h, g \in K[x]$ and every element of $L(x)$ is of the form $k\ell^{-1}$, for some $k, \ell \in L(x)$. Since the mapping above, (which we also denote as $\sigma$), is a bijection, then $\sigma$ extends to a bijection mapping of $K(x)$ to $L(x)$ as $g\ell^{-1} \mapsto \sigma(g)\sigma(\ell)^{-1}$. It is easy to verify that this extended $\sigma$ is an isomorphism. Then since $\alpha$ is transcendental, then by Theorem 2.1.12, we have

$$K(\alpha) \simeq K(x) \simeq L(x) \simeq L(\beta)$$

The isomorphism from $K(\alpha)$ to $K(\beta)$ is an extension of $\sigma$, so the extension still maps $K$ to $L$. Since the isomorphism of $K(\alpha)$ to $K(x)$ maps $\alpha$ to $x$, the isomorphism of $K(x)$ to $L(x)$ maps $x$ to $x$, and the isomorphism of $L(x)$ to $L(\beta)$ maps $x$ to $\beta$, then the extension of $\sigma$ maps $\alpha$ to $\beta$. This proves (i).

Now assume that (i) does not hold, and we will show that (ii) holds. Without loss of generality, assume that $f$ is monic (since the extended isomorphism $\sigma : K[x] \to L[x]$ maps polynomial $kf$ to $\sigma(kf) = k\sigma(f)$ for all $k \in K$) and the roots of $f$ and $kf$ coincide. Since $\sigma : K[x] \to L[x]$ is an isomorphism, then $\sigma f \in L[x]$ is monic and irreducible. In the proof of Theorem 2.1.13 (ii), the mappings $\phi : K[x]/\langle f \to K[\alpha] = K(\alpha)$ and $\psi : L[x]/\langle \sigma f \rangle \to L[\beta] = L(\beta)$ given respectively by

$$\phi(g + \langle f \rangle) = g(\alpha)$$

and

$$\psi(h + \langle \sigma f \rangle) = h(\beta)$$

are isomorphisms. Then, the mapping $\theta : K[x]/\langle f \to L[x]/\langle \sigma f \rangle$ given by $\theta(g + \langle f \rangle) = \sigma g + \langle \sigma f \rangle$

is an isomorphism. Therefore, the composition

$$K(\alpha) \xrightarrow{\phi^{-1}} K[x]/\langle f\rangle \xrightarrow{\theta} L[x]/\langle \sigma f\rangle \xrightarrow{\psi} L(\beta)$$

is an isomorphism of fields $K(\alpha)$ and $L(\beta)$ such that $g(\alpha) \mapsto g(x) + \langle f\rangle \mapsto \sigma g(x) + \langle \sigma f\rangle + \sigma g(\beta)$. Also, $\psi\theta\phi^{-1}$ agrees with $\sigma$ on $K$ (the "constant" rational functions of $\alpha$ in $K(\alpha)$) and maps $\alpha \mapsto x + \langle f\rangle \mapsto x + \langle \sigma f\rangle \mapsto \beta$. This proves (ii). ∎

**Corollary 2.1.17**

*Let $E$ and $F$ be extension fields of $K$ and let $\alpha \in E$ and $\beta \in F$ be algebraic over $K$. The following assertions are equivalent:*

*(a) $\alpha$ and $\beta$ are roots of the same irreducible polynomial $f \in K[x]$.*

*(b) there exists an isomorphism of fields $K(\alpha) \simeq K(\beta)$ which sends $\alpha$ onto $\beta$ and it is the identity on $K$.*

*Proof.*

(a) ⇒ (b) First assume that $\alpha$ and $\beta$ are roots of the same irreducible polynomial $f \in K[x]$. Then by Theorem 2.1.16 (ii) with $\sigma = 1_K$, we have $\sigma f = f$, and so $\alpha$ (a root of $f$) and $\beta$ (a root of $f = \sigma f$) and $K(\alpha) \simeq K(\beta)$, where the isomorphism between $K(\alpha)$ and $K(\beta)$ sends $\alpha$ onto $\beta$.

(b) ⇒ (a) Now assume that $\sigma : K(\alpha) \to K(\beta)$ is an isomorphism with $\sigma(\alpha) = \beta$ and $\sigma(k) = k$ for all $k \in K$. Let $f \in K[x]$ be the irreducible monic polynomial for which algebraic $\alpha$ is a root. If $f = \sum_{i=0}^{n} k_i x^i$, then

$$0 = f(\alpha) = \sum_{i=0}^{n} k_i \alpha^i$$

Since $\sigma(0) = 0$, then

$$0 = \sigma(0) = \sigma\left(\sum_{i=0}^{n} k_i\alpha^i\right) = \sum_{i=0}^{n} \sigma(k_i\alpha^i) = \sum_{i=0}^{n} \sigma(k_i)\sigma(\alpha^i) = \sum_{i=0}^{n} k_i\sigma(\alpha)^i = \sum_{i=0}^{n} k_i\beta^i = f(\beta)$$

So $\beta$ is a root of $f$ as well. ∎

So far, we have dealt with a field $K$ and some element $\alpha$ which is algebraic over $K$ and is an element of some (mysterious) given extension field of $F$. The following result shows that for any polynomial $f \in K[x]$, there exists some field extension $F$ such that $F$ contains a root of $f$. This is a step towards the Fundamental Theorem of Algebra in that we now know of the existence of an extension field containing a root of a given polynomial. Of course, the Fundamental Theorem of Algebra states that $\mathbb{C}$ is algebraically closed. The next result is commonly called Kronecker's Theorem.

**Theorem 2.1.18: Kronecker's Theorem**

*If $K$ is a field and $f \in K[x]$ is a polynomial of degree $n$, then there exists a unique simple extension $F = K(\alpha)$ of $K$ such that*

*(i)* $\alpha \in F$ *is a root of* $f$.

*(ii)* $[K(\alpha) : K] \leq n$ *with equality holding if and only if* $f$ *is irreducible in* $K[x]$.

*(iii) If* $f$ *is irreducible in* $K[x]$, *then* $K(\alpha)$ *is unique up to an isomorphism which is the identity on* $K$.

*Proof.*

Without loss of generality, we may assume that $f$ is irreducible (if not, we replace $f$ by one of its irreducible factors). Then the ideal $\langle f \rangle$ is maximal in $K[x]$, and so $F = K[x]/\langle f \rangle$ is a field. Furthermore, the canonical projection $\pi : K[x] \to K[x]/\langle f \rangle$ given by the mapping $g \mapsto g + \langle f \rangle$ when restricted to $K$ (the constant polynomials in $K[x]$) is a one-to-one homomorphism (the canonical projection is a homomorphism, the only "constant" in $\langle f \rangle$ is the zero function since $\langle f \rangle$ contains all multiples of $f$ by elements in $K[x]$, and so the kernel of the canonical projection is one-to-one). Then since $\pi$ is one-to-one, $\pi(K) \simeq K$ can be considered as a subfield of a field $F$; that is, $F$ is an extension field of $K$ (provided that $K$ is identified with $\pi(K)$). For $x \in K[x]$, let $\alpha = \pi(x) = x + \langle f \rangle = K[x]/\langle f \rangle$. Then by Theorem 2.1.13 (ii) and since coset addition and multiplication is performed on representatives, then

$$f(\alpha) = f(x + \langle f \rangle) = f(x) + \langle f \rangle = 0 + \langle f \rangle$$

since $0 + \langle f \rangle$ is the additive identity in $K[x]/\langle f \rangle = F$, so (i) follows.

To see that (ii) holds, note that Theorem 2.1.13 shows that $[K(\alpha) : K] = n$ for irreducible $f$ of degree $n$. As commented above, if $f$ is not irreducible, then we consider an irreducible factor of $f$ (of degree less than $n$) and (ii) follows.

Finally, to see that (iii) holds, Corollary 2.1.17 implies (iii) and that the extension field does not depend on which root of $f$ is used. ∎

We now establish some "basic facts" about algebraic extension fields.

**Theorem 2.1.19**

*If $F$ is a finite dimensional extension field of $K$, then $F$ is finitely generated and algebraic over $K$.*

*Proof.*

If $F$ is a finite-dimensional extension of $K$, say $[F : K] = n$. Let $\alpha \in F$ be arbitrary. Then the set of $n + 1$ elements $\{1_K, \alpha, ..., \alpha^n\}$ must be linearly dependent over $F$. So there exists $a_0, ..., a_n \in K$ not all zero such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

which implies that $\alpha$ is algebraic over $K$. Since $\alpha$ was arbitrary, $F$ is an algebraic extension of $K$. If $\{x_1, ..., x_n\}$ is a basis of $F$ over $K$, then by Theorem 2.1.7 (v) that $F = K(x_1, ..., x_n)$. This completes the proof. ∎

**Theorem 2.1.20**

*If $F$ is a field extension of $K$, and $X \subset F$ such that $F = K(X)$, and every element of $X$ is algebraic over $K$, then $F$ is an algebraic extension of $K$. If $X$ is a finite set, then $F$ is finite-dimensional over $K$.*

*Proof.*

If $\alpha \in F$, then by Theorem 2.1.7 (iv),

$$\alpha = \frac{f(u_1, ..., u_n)}{g(u_1, ..., u_n)}$$

for some $n \in \mathcal{N}$ and $f, g \in F[x_1, ..., x_n]$ and some $u_1, ..., u_n \in X$. So $x \in K(u_1, ..., u_n)$. So there exists a tower of subfields

$$K \subset K(u_1) \subset K(u_1, u_2) \subset \cdots \subset K(u_1, ..., u_n)$$

For fixed $i \geq 2$, $u_i$ is algebraic over $K$ and so $u_i$ is algebraic over $K(u_1, ..., u_{i-1})$, say $u_i$ is of degree $r_i$ over $K(u_1, ..., u_{i-1})$. Since

$$K(u_1, ..., u_{i-1})(u_i) = K(u_1, ..., u_i)$$

we have

$$[K(u_1, ..., u_i) : K(u_1, ..., u_{i-1})] = r_i$$

by Theorem 2.1.13 (iii). Now let $r_1$ be the degree of $u_1$ over $K$ (we had $i \geq 2$ above), then by an inductive application of Theorem 2.1.3, shows that

$$[K(u_1, ..., u_n) : K] = r_1 \cdots r_n$$

By Theorem 2.1.19, $K(u_1, ..., u_n)$ (since the dimension $r_1 \cdots r_n$ is finite) is algebraic over $K$, and so $\alpha \in K(u_1, ..., u_n)$ is algebraic over $K$. Since $\alpha$ was arbitrary, then $F$ is algebraic over $K$.

If $X$ was a finite set, say $X = \{u_1, ..., u_n\}$, then as argued above,

$$[F(u_1, ..., u_n) : K] = r_1 \cdots r_n$$

is finite. This completes the proof. ∎

**Theorem 2.1.21**

*If $F$ is an algebraic extension field of $E$, and $E$ is an algebraic extension field of $K$, then $F$ is an algebraic extension of $K$.*

*Proof.*

Let $\alpha \in F$ be arbitrary. Since $F$ is an algebraic extension of $E$, then $\alpha$ is algebraic over $E$, and so

$$b_n\alpha^n + \cdots + b_0 = 0$$

for some $b_0, ..., b_n \in E$ with $b_n \neq 0$. Therefore, $\alpha$ is algebraic over the subfield $K(b_0, ..., b_n)$ of $E$. Consequently, there is a tower of fields

$$K \subset K(b_0, ..., b_n) \subset K(b_0, ..., b_n)(\alpha)$$

where $[K(b_0, ..., b_n)(u) : K(b_0, ..., b_n)]$ is finite by Theorem 2.1.13 (iii) since $\alpha$ is algebraic over $K(b_0, ..., b_n)$, and $[K(b_0, ..., b_n) : K]$ is finite by Theorem 2.1.13 (iii) since $\alpha$ is algebraic over $K(b_0, ..., b_n)$, and $[K(b_0, ..., b_n) : K]$ is finite by Theorem 2.1.20 since there is a finite number of $b_i$ and each is algebraic over $K$. Therefore, $[K(b_0, ..., b_n)(\alpha) : K]$ is finite by Theorem 2.1.3. Hence, by Theorem 2.1.19, $\alpha$ is algebraic over $K$. Since $\alpha \in F$ is arbitrary, $F$ is algebraic over $K$. ∎

**Theorem 2.1.22**

*Let $F$ be an extension field of $K$ and $E$ the set of all elements of $F$ which are algebraic over $K$. Then $E$ is a subfield of $F$.*

*Proof.*

For any $\alpha, \beta \in E$, $K(\alpha, \beta)$ is an algebraic extension of $K$ by Theorem 2.1.20. Since $K(\alpha, \beta)$ is a field, then $\alpha - \beta \in K(\alpha, \beta)$ and $\alpha\beta^{-1} \in K(\alpha, \beta)$ for $\beta \neq 0$. Hence, $\alpha - \beta \in E$ and $\alpha\beta^{-1} \in E$ and so $E$ is an additive group and $E \setminus \{0\}$ is a multiplicative group. Therefore, $E$ is a field. ∎

Theorem 2.1.22 justifies the claim that the algebraic real numbers $\mathcal{A}$ are a field:

$$\mathcal{A} = \{r \in \mathbb{R} : p(r) = 0 \text{ for some } p \in \mathbb{Q}[x]\}$$

## 2.2 The Fundamental Theorem of Galois Theory

In this section, we define the Galois group of an arbitrary field extension. We prove the Fundamental Theorem of Galois Theory. The Fundamental Theorem allows us to translate problems involving fields, polynomials, and extensions into group theoretical terms.

**Definition 2.2.1**

Let $F$ be a field. Let $\text{Aut}(F)$ denote the set of all field automorphisms mapping $F$ to $F$. $\text{Aut}(F)$ is a group under function composition called the *automorphisms group of $F$*.

Let us recall the following definition from Module Theory.

**Definition 2.2.2**

Let $A$ and $B$ be modules over a ring $R$. A function $\phi : A \to B$ is called an *$R$-module homomorphism* if

(i) For all $a, b \in A$, $f(a+b) = f(a) + f(b)$.

(ii) For all $r \in R$ and $a \in A$, $f(ra) = rf(a)$.

Recall that a vector space is an $R$-module where $R$ is a division ring with identity $1_R$ such that $1_R a = a$ for all $a \in A$.

Let $E$ and $F$ be extension fields of $K$. If $\sigma : E \to F$ is a nonzero field homomorphism, then $\sigma(1_E) = 1_F$. If $\sigma$ is also a $K$-module homomorphism, then for all $k \in K$, we have

$$\sigma(k) = \sigma(k1_E) = k\sigma(1_E) = k1_E = k$$

that is, $\sigma$ fixes the elements of $K$. Conversely, if a field homomorphism $\sigma : E \to F$ fixes $K$ elementwise, then $\sigma$ is nonzero and for any $e \in E$,

$$\sigma(ke) = \sigma(k)\sigma(e) = k\sigma(e)$$

and so $\sigma$ is a $K$-module homomorphism.

**Definition 2.2.3**

Let $E$ and $F$ be extension fields of a field $K$. A nonzero map $\sigma : E \to F$ which is both a field and $K$-module homomorphism is a *$K$-homomorphism*. Similarly, if $\sigma \in \mathrm{Aut}(F)$ is a $K$-homomorphism, then $\sigma$ is a *$K$-automorphism* of $F$. The group of all $K$-automorphisms of $F$ is the *Galois group of $F$ over $K$* denoted by $\mathrm{Gal}(F/K) = \mathrm{Aut}_K(F)$. Note that $\mathrm{Gal}(F/K)$ is the set that can be written as

$$\mathrm{Gal}(F/K) = \{\sigma \in \mathrm{Aut}(F) : \sigma(\alpha) = \alpha \text{ for all } \alpha \in F\}$$

Note that we can omit this "$K$-module" talk by simply defining $\mathrm{Gal}(F/K)$ to be the set of all automorphisms of $F$ which fix subfield $K$.

**Example 2.2.4**

Let $K$ be any field and let $F = K(x)$. Then $F$ is an extension field of $K$ (where we interpret $K$ as the collection of constant rational functions in $K(x)$). For each $k \in K$, define $\sigma_k : F \to F$ given by

$$\sigma_k\left(\frac{f(x)}{g(x)}\right) = \frac{f(kx)}{g(kx)}$$

Then $\sigma_k$ certainly fixes $K$. $\sigma_k$ is a ring homomorphism (easy to check), and it is also onto

since for any $\frac{f(x)}{g(x)} \in K(x)$, we have $\frac{f(x/k)}{g(x/k) \in K(x)}$ and

$$\sigma_k \left( \frac{f(x/k)}{g(x/k)} \right) = \frac{f(x)}{g(x)}$$

Now, $\sigma_k^{-1} = \sigma_{k^{-1}}$ and so $\sigma$ is one-to-one. Thus, $\sigma_k$ is an automorphism in $K(x)$, which fixes $K$; that is, $\sigma_k \in \text{Gal}(F/K) = \text{Gal}(K(x)/K)$ for all $k \in K \setminus \{0\}$. Hence, if $K$ is infinite, then $\text{Gal}(K(x)/K)$ is also infinite.

Similarly, for each $k \in K$, define the map $\tau_k : F \to F$ be given by

$$\tau_k \left( \frac{f(x)}{g(x)} \right) = \frac{f(x+k)}{g(x+k)}$$

which is also in $\text{Gal}(K(x)/K)$. If $k_1 \neq 1_K$ and $k_2 \neq 0$, then $\sigma_{k_1}\tau_{k_2} \neq \tau_{k_2}\sigma_{k_1}$ since

$$(\sigma_{k_1}\tau_{k_2})(x) = \sigma_{k_1}(x + k_2) = (k_1 x) + k_2 = k_1 x + k_2$$

and

$$(\tau_{k_2}\sigma_{k_1})(x) = \tau_{k_2}(k_1 x) = k_1(x + k_2) = k_1 x + k_1 k_2$$

Therefore, $\text{Gal}(K(x)/K)$ is nonabelian.

**Theorem 2.2.5**

*Let $F$ be an extension field of $K$ and $K[x]$. If $\alpha \in F$ is a root of $f$ and $\sigma \in \text{Gal}(F/K)$, then $\sigma(\alpha) \in F$ is also a root of $f$.*

*Proof.*

Let $f = \sum_{i=0}^{n} k_i x^i$. Since $\sigma$ fixes $K$, $\sigma(0) = 0$ and so $f(\alpha) = 0$ implies that

$$0 = \sigma(0) = \sigma(f(\alpha)) = \sigma\left( \sum_{i=0}^{n} k_i x^i \right) = \sum_{i=0}^{n} \sigma(k_i)\sigma(\alpha^i) = \sum_{i=0}^{n} k_i(\sigma(\alpha))^i = f(\sigma(\alpha))$$

This completes the proof. ∎

If $\alpha$ is algebraic over $K$ and $f(\alpha) = 0$ is irreducible for $f \in K[x]$ of degree $\alpha$, then by Theorem 2.1.13 (iv), $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis for $K(\alpha)$. So any $\sigma \in \text{Gal}(K(\alpha)/K)$ is completely determined by its action on $\alpha$. We will use this property to restrict the number of elements of $\text{Gal}(F/K)$ and to get some idea of the structure of $\text{Gal}(F/K)$.

**Example 2.2.6**

If $F = K$, then $\text{Gal}(F/K)$ only contains the identity isomorphism. The converse is false. Consider for example, $\alpha$ the real root of $x^3 - 2$. Then $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{R}$ as fields. Then $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ consists only of the identity, since by Theorem 2.2.5, the image of $\alpha$ must also

be a root of $x^3 - 2$, but the other two roots of $x^3 - 2$ are complex, so $\alpha$ must be mapped to itself. Similarly, $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ contains only the identity.

**Example 2.2.7**

We now consider $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. We have $\mathbb{C} = \mathbb{R}(i)$ where $i$ is a root of $x^2 + 1$. By Theorem 2.2.5, the only possible image of $i$ by an element of $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ is either $i$ itself (in which case the automorphism is the identity) or $-i$. It is easy to verify that the mapping $a+bi \mapsto a-bi$ is an automorphism of $\mathbb{C}$, so $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$. Similarly, $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$.

**Example 2.2.8**

Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. A basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$ by Theorem 2.1.13 (iv). Now, $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, so a basis for $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{3}\}$. But, as given by Theorem 2.1.3, we know that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

In the proof of Theorem 2.1.3 it is shown that for fields $E \subset K \subset F$ with a basis $A$ of $K$ over $E$ and basis $B$ of $F$ over $K$, we have a basis of $F$ over $E$ of

$$AB = \{ab : a \in A, b \in B\}$$

So the four elements of a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Now, by Theorem 2.2.5, for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, we must have $\sigma(1) = 1$, $\sigma(\sqrt{2}) \in \{-\sqrt{2}, \sqrt{2}\}$, and $\sigma(\sqrt{3}) \in \{-\sqrt{3}, \sqrt{3}\}$; notice that the behaviour of $\sigma$ on $\sqrt{2}$ and $\sqrt{3}$ determines its behaviour on $\sqrt{6}$. Therefore, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ consists of four $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. It is readily verified that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

The plan for Galois theory is to create a chain of extension fields (algebraic extensions, in practice) and to create a corresponding chain of automorphism groups. The first step in this direction is the following.

**Theorem 2.2.9**

*Let $F$ be an extension field of $K$, $E$ an intermediate field, and $H$ a subgroup of $\mathrm{Gal}(F/K)$. Then*

*(i) $H' = \{\alpha \in F : \sigma(\alpha) = \alpha$ for all $\sigma \in H\}$ is an intermediate field of the extension.*

*(ii) $E' = \{\sigma \in \mathrm{Gal}(F/K) : \sigma(\alpha) = \alpha$ for all $\alpha \in E\} = \mathrm{Gal}(F/E)$ is a subgroup of $\mathrm{Gal}(F/K)$.*

**Definition 2.2.10**

Let $F$ be an extension field of $K$ and $H$ be a subgroup of $\mathrm{Gal}(F/K)$. The field

$$H' = \{\alpha \in F : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

is called the *fixed field* of $H$ in $F$.

We use the prime notation to indicate fixed fields and to indicate a Galois group $\mathrm{Gal}(F/K) = K'$. Note that $F' = \mathrm{Gal}(F/F) = \{e\}$ is the trivial group consisting of the identity permutation, which is called the *identity group*.

**Definition 2.2.11**

Let $F$ be an extension field of $K$ such that the fixed field of the Galois group $\mathrm{Gal}(F/K)$ is $K$ itself. Then $F$ is a *Galois extension of* $K$, and $F$ is said to be *Galois* over $K$.

It follows from the definition that $F$ is Galois over $K$ if and only if for any $\alpha \in F \setminus K$, there exists some $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(\alpha) \neq \alpha$.

Note that in the sense of Definition 2.2.10 and Theorem 2.2.9, when we say that the fixed field of $\mathrm{Gal}(F/K)$ is $K$ itself, we mean that $\mathrm{Gal}(F/K)' = K$, where in this case,

$$\mathrm{Gal}(F/K)' = \{\alpha \in F : \sigma(\alpha) = \alpha \text{ for all } \sigma \in \mathrm{Gal}(F/K)\}$$

**Example 2.2.12**

($\alpha$) If $d \in \mathbb{Q}$ and $d \geq 0$, then $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$.

($\beta$) $\mathbb{C}$ is Galois over $\mathbb{R}$.

($\gamma$) $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ is the identity group, so $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ has fixed field $\mathbb{R}$ and hence, $\mathbb{R}$ is not Galois over $\mathbb{Q}$.

**Example 2.2.13**

Let us show that $\mathbb{Q}(\sqrt{2})$ is Galois over $\mathbb{Q}$. That is, we need to show that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})' = \mathbb{Q}$, where in this case,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})' = \{\alpha \in \mathbb{Q}(\sqrt{2}) : \sigma(\alpha) = \alpha \text{ for all } \sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\}$$

First observe that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, so the only field automorphisms of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ are the maps $\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$ (the identity map) and $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ (the conjugation map).

Let $\alpha \in \mathbb{Q}$ be arbitrary. Then we have $\alpha \in \mathbb{Q}(\sqrt{2})$ since $\alpha = a + 0\sqrt{2}$ for some $a \in \mathbb{Q}$. If

$\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ is the map defined by $\sigma(a+b\sqrt{2}) = a+b\sqrt{2}$, then observe that

$$\sigma(\alpha) = \sigma(a+0\sqrt{2}) = a = \alpha$$

which shows that $\alpha \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})'$.

On the other hand, if $\alpha \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, note that $\alpha \in \mathbb{Q}$ if and only if $a+b\sqrt{2} = a-b\sqrt{2}$ for some $a, b \in \mathbb{Q}$ if and only if $b = 0$, so we have $\alpha \in \mathbb{Q}$.

Therefore, we have shown that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})' = \mathbb{Q}$, and thus, $\mathbb{Q}(\sqrt{2})$ is Galois over $\mathbb{Q}$.

**Definition 2.2.14**

If $F$ is an extension field of $K$ and $L, M$ are intermediate fields with $K \subset L \subset M \subset F$, then the dimension $[M : L]$ is the *relative dimension* of $L$ and $M$. If $H, J$ are subgroups of $\mathrm{Gal}(F/K)$ with $H \leq J$, then the index $[J : H]$ is the *relative index* of $H$ and $J$.

We now have the equipment to state the Fundamental Theorem of Galois Theory. However, we need several preliminary results before we have the equipment to prove it.

**Theorem 2.2.15: Fundamental Theorem of Galois Theory**

*If $F$ is a finite-dimensional Galois extension of $K$, then there exists a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group* $\mathrm{Gal}(F/K)$ *given by* $E \mapsto \mathrm{Gal}(F/E)$ *such that*

*(i) The relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups; in particular,* $\mathrm{Gal}(F/K)$ *has order* $[F : K]$.

*(ii) $F$ is Galois over every intermediate field $E$, but $E$ is Galois over $K$ if and only if the corresponding subgroup* $\mathrm{Gal}(F/E)$ *is normal in* $\mathrm{Gal}(F/K)$*; in this case,* $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/K)$.

The one-to-one correspondence, which we call the *Galois correspondence*, assigns to each intermediate field $E$, the Galois group $\mathrm{Gal}(F/E)$ and assign to each subgroup $H \leq \mathrm{Gal}(F/K)$ the fixed field $H'$. These assignments of fields to groups and groups to fields are inverses of each other.

The goal is to establish these mappings as inverses of each other, as well as the relative dimension and normality claims of the Fundamental Theorem.

**Lemma 2.2.16**

*Let $F$ be an extension field of $K$ with intermediate fields $L$ and $M$ (say $K \subset L \subset M \subset F$). Let $H$ and $J$ be subgroups of* $\mathrm{Gal}(F/K)$. *Then*

*(i) $F' = \{e\}$ and $K' = \mathrm{Gal}(F/K)$. Moreover, $\{e\}' = F$.*

*(ii) $L \subset M$ implies $M' \leq L'$. Moreover, $H \leq J$ implies $J' \subset H'$.*

*(iii)* $L \subset L''$ *and* $H \leq H''$, *where* $L'' = (L')'$ *and* $H'' = (H')'$.

*(iv)* $L' = L'''$ *and* $H' = H'''$.

*Proof.*

We first prove (i). Note $\mathrm{Gal}(F/F) = F'$ is the group of automorphisms of $F$ which fixes $F$ and hence, must consist only of the identity permutation and so $F'$ is the identity group. Next, $K' = \mathrm{Gal}(F/K)$ is easy to note. To see the moreover part, note that $\{e\}'$ is the fixed field of the identity group. $F$ is the universal field and the identity group fixes all of $F$, so $\{e\}' = F$.

To prove the second assertion, suppose that $L$ and $M$ are intermediate fields such that $L \subset M$. An element of $M' = \mathrm{Gal}(F/M)$ fixes $M$ and with $L \subset M$, such an element must also fix $L$ and so the element is in $L' = \mathrm{Gal}(F/L)$, so $M' \leq L'$. To see the moreover part, suppose $H$ and $J$ are subgroups of $\mathrm{Gal}(F/K)$ satisfying $H \leq J$. Note that an element of $J'$ is fixed by every element of $J$, and since $H \leq J$, also fixed by every element of $H$. So an element of $J'$ is also an element of $H'$. That is, $J' \subset H'$.

To prove the third assertion, let $L$ be an intermediate field. Then $\mathrm{Gal}(F/L)$ is a group, and $L''$ is the fixed field of $L'$. Now any element of $L$ is fixed by $\mathrm{Gal}(F/L) = L'$. Also, $L''$ includes everything in $F$ fixed by the elements of $L' = \mathrm{Gal}(F/L)$, so $L''$ includes all of $L$, so $L \subset L''$. For the second part, let $H$ be a subgroup of $\mathrm{Gal}(F/K)$. Then $H'$ is the fixed field of $H$. Now $(H')' = H''$ is the group of permutations of $F$ which fix $H'$, so every element of $H$ fixes all of $H'$ and such an element is therefore also in $H''$, so $H \leq H''$.

Finally, to prove the last assertion, let $L$ be an intermediate field. By (iii), $L \subset L''$, so by (ii), $L''' \leq L'$. Now $L'$ is a subgroup of $\mathrm{Gal}(F/K)$, so by (iii), with $H$ replaced with $l'$, we have $L' \leq L'''$, and so $L' = L'''$. For the second part, let $H$ be a subgroup of $\mathrm{Gal}(F/K)$. By (iii), $H \leq H''$, so by (ii), $H''' \subset H'$. Now $H'$ is an intermediate field so by (iii) with $L$ replaced with $H'$, we have $H' \subset H'''$, so $H' = H'''$. ∎

It is possible in Lemma 2.2.16 (iii) for $L$ to be a proper subset of $L''$. For example, we have $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ is the identity group. With $L = \mathbb{Q}$, we have $L' = \mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \{1\}$ (the identity group on $\mathbb{R}$), and so the fixed field of $L'$ is $L'' = \mathbb{R}$. Also, $H$ may be a proper subgroup of $H''$ in Lemma 2.2.16 (iii).

By the definition of Galois extension, in terms of prime notation, we have that $F$ is Galois over $K$ if and only if $G' = \mathrm{Gal}(F/K)'$. We always have $K' = \mathrm{Gal}(F/K)$ so $F$ is Galois over $K$ if and only if $K = \mathrm{Gal}(F/K)' = K''$.

**Definition 2.2.17**

Let $F$ be an extension field of $K$. Let $X$ be either (i) an intermediate field, $K \subset X \subset F$, or (ii) a subgroup of the Galois group $X \leq \mathrm{Gal}(F/K)$. Then $X$ is *closed* if $X = X''$.

**Remark 2.2.18**

Subfield $K$ of $F$ is Galois over $K$ if and only if $K$ is closed.

**Theorem 2.2.19**

*If $F$ is an extension field of $K$, then there exists a one-to-one correspondence between the closed intermediate fields of the extension and the closed subgroups of the Galois group, given by $E \mapsto \mathrm{Gal}(F/E)$.*

Theorem 2.2.19 only deals with closed fields and groups. This will be useful once we prove Lemma 2.2.22.

**Lemma 2.2.20**

*Let $F$ be an extension field of $K$ and $L$ and $M$ be intermediate fields with $L \subset M$. If $[M : L]$ is finite, then $[L' : M'] \leq [M : L]$. In particular, if $[F : K]$ is finite, then $|\mathrm{Gal}(F/K)| \leq [F : K]$.*

*Proof.*

Notice that $[M : L]$ and $[F : K]$ are dimensions of vector spaces; $[L' : M']$, the index of $L'$ over $M'$ is the number of cosets of $L$ in $M$. Since $[M : L]$ is finite, we give a proof based on induction.

Let $n = [M : L]$. For $n = 1$, then $M + L$ and so $M' = L'$ and $[L' : M'] = 1$, so the result holds. Now let $n > 1$, and suppose the theorem holds for all $1 \leq i \leq n$. Since $n > 1$, there exists some $\alpha \in M \setminus L$. Since $[M : L]$ is finite, then $\alpha$ is algebraic over $L$ by Theorem 2.1.19. let $f \in L[x]$ be the irreducible monic polynomial of $\alpha$, say of degree $k > 1$. Then by Theorem 2.1.13 (iii), $[L(\alpha) : L] = k$. By Theorem 2.1.3,

$$[M : L] = [M : L(\alpha)][L(\alpha) : L]$$

and so $[M : L(\alpha)] = n/k$.

We now consider the following cases:

- Case 1: (If $k < n$, then $1 < n/k < n$) By the inductive hypothesis, since $i = n/k < n$, we have that $L \subset L(\alpha)$ implies $[L' : (L(\alpha))'] \leq [L(\alpha) : L] = k$ and that $L(\alpha) \subset M$ implies $[L(\alpha)' : M'] \leq [M : L(\alpha)] = n/k$. Hence,

  $$[L' : M'] = [L' : L(\alpha)'][L(\alpha)' : M] \leq k(n/k) = n = [M : L]$$

  and the theorem holds in this case.

- Case 2: If $k = n$, then by Theorem 2.1.3,

  $$[M : L] = [M : L(\alpha)][L(\alpha) : L]$$

  and so $[M : L(\alpha)] = 1$ as above. So $M = L(\alpha)$. In the final part of the proof, we will construct an injective map from the set $S$ of all left cosets of $M'$ in $L'$ (of which there are $[L' : M']$ such cosets) to the set $T$ of all distinct roots in $F$ of the polynomial $f \in L[x]$ (of which there are at most $k \leq n$ such roots). So we have $|S| = [L' : M']$ and $|T| \leq n$, the existence of the injective map from $S$ to $T$ gives us that $|S| \leq |T|$ and it will then follow that $[L' : M'] \leq [M : L]$, establishing the theorem in this second case. Now for

the construction of the injective map from $S$ to $T$, let $\tau \in L'$ and $\tau M'$ a left coset of $M'$ in $L'$. If $\sigma \in M' = \mathrm{Gal}(F/M)$, then since $\alpha \in M$, we have that $\sigma(\alpha) = \alpha$, and so $\tau\sigma(\alpha) = \tau(\alpha)$; so every element of the coset $\tau M'$ (this is a group element which acts on elements of $F$, $\alpha$ in particular) has the same effect on $\alpha$ and maps $\alpha \mapsto \tau(\alpha)$ (that is, there is independence of element $\sigma \in M'$). Since $\tau \in L' = \mathrm{Gal}(F/L)$ (since $\tau M'$ is a coset in $L'$) and $\alpha$ is a root of $f \in L[x]$, then $\tau(\alpha)$ is also a root of $f$ by Theorem 2.2.5. This implies that the map $S \to T$ given by $\tau M' \mapsto \tau(\alpha)$ is well-defined. If $\tau(\alpha) = \tau_0(\alpha)$ for $\tau, \tau_0 \in L'$, then $\tau_0^{-1}\tau(\alpha) = \alpha$ ($L'$ is a group of permutations, so inverses exist) and hence $\tau_0\tau$ fixes $\alpha$. Since $\tau, \tau_0 \in L' = \mathrm{Gal}(F/L)$ then certainly $\tau, \tau_0$ and $\tau_0^{-1}$ fixes $L$, so $\tau_0^{-1}\tau$ fixes $L(\alpha) = M$ elementwise and $\tau_0\tau \in M'$. Consequently, $\tau_0 M' = \tau M'$ and so the map $S \to T$ is injective and this completes the second case of the induction. Hence, $[L' : M'] \leq [M : L]$.

For the "in particular" part of the proof, notice that

$$\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(F/K)/\{e\}$$

so $|\mathrm{Gal}(F/K)| = [\mathrm{Gal}(F/K) : \{e\}]$. Also, in the prime notation, $K' = \mathrm{Gal}(F/K)$ and $F' = \mathrm{Gal}(F/F) = \{e\}$, so $|\mathrm{Gal}(F/K)| = [\mathrm{Gal}(F/K) : \{e\}] = [K' : F'] \leq [F : K]$ with $L = K$ and $M = F$ from the above result. ∎

**Lemma 2.2.21**

*Let $F$ be an extension field of $K$ and let $H$ and $J$ be subgroups of the Galois group $\mathrm{Gal}(F/K)$ with $H \leq J$. If $[J : H]$ is finite, then $[H' : J'] \leq [J : H]$.*

*Proof.*

Let the number of cosets of $H$ in $H$ be denoted by $[J : H] = n$, and assume for a contradiction that $[H' : J'] > n$. Then a basis of $H'$ over $J'$ has more than $n$ elements and so there exists $\alpha_1, ..., \alpha_{n+1} \in H'$ that are linearly independent over $J'$. Let $\{\tau_1, ..., \tau_n\}$ be a complete set of representatives of the $n$ left cosets of $H$ in $J$. That is,

$$J = \bigcup_{i=1}^{n} \tau_i H$$

since cosets of a group partition the group, and $\tau_i^{-1}\tau_j \in h$ if and only if $i = j$. Consider the system of $n$ homogeneous linear equations of $n + 1$ unknowns with coefficients $\tau_i(u_j)$ in field $F$:

$$\begin{cases} \tau_1(\alpha_1)x_1 + \tau_1(\alpha_2)x_2 + \cdots + \tau_1(\alpha_{n+1})x_{n+1} = 0 \\ \tau_2(\alpha_1)x_1 + \tau_2(\alpha_2)x_2 + \cdots + \tau_2(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ \tau_n(\alpha_1)x_1 + \tau_n(\alpha_2)x_2 + \cdots + \tau_n(\alpha_{n+1})x_{n+1} = 0 \end{cases} \tag{1}$$

Such a system has a nontrivial solution. Among all such nontrivial solutions, choose one, say $x_1 = \lambda_1$,..., $x_{n+1} = \lambda_{n+1}$ with a minimal number of nonzero $\lambda_i$. By reindexing if necessary,

we may assume that $x_1 = \lambda_1$,..., $x_r = \lambda_r$ and $x_{r+1} = \cdots = x_{n+1} = 0$ where $\lambda_r \neq 0$. Since each multiple of a solution is alsoa solution, then we may also assume that $\lambda_1 = 1_F$. In the conclusion of the proof below, we will show that the hypothesis that $\alpha_1, ..., \alpha_{n+1} \in H'$ are linearly independent over $J'$ implies that there exists $\sigma \in J$ such that $x_1 = \sigma(\lambda_1), ..., x_r = \sigma(\lambda_r)$ and $x_{r+1} = \cdots = x_{n+1} = 0$ is also a nontrivial solution to the system of equations (1) and $\sigma(\lambda_2) = \lambda_2$. Since the difference of two solutions is also a solution, as the system (1) is linear and homogeneous, then $x_1 = \lambda_1 - \sigma(\lambda_1), ..., x_r = \lambda_r - \sigma(\lambda_r)$, and $x_{r+1} = \cdots = x_{n+1} = 0$ is also a solution of the system of equations (1). But since

$$\lambda_1 - \sigma(\lambda_1) = 1_F - 1_F = 0$$

and $\lambda_2 \neq \sigma(\lambda_2)$, then $x_1 = 0$, $x_2 = \lambda_2 - \sigma(\lambda_2) \neq 0$, $x_3 = \lambda_3 - \sigma(\lambda_3), ..., x_r = \lambda_r - \sigma(\lambda_r)$, and $x_{r+1} = \cdots = x_{n+1} = 0$ is a nontrivial solution of the system of equations (1) as $x_2 \neq 0$, with at most $r - 1$ nonzero entries, which is absurd by the minimality of $r$ of nonzero terms is a nontrivial solution to the system of equations (1).

To complete the proof, we must find $\sigma \in J$ with the desired properties. Now $\{\tau_1, ..., \tau_n\}$ is a set of representatives of the cosets of $H$, then exactly one of the $\tau_j$, say $\tau_1$ is in $H$ itself. Since $H' = \mathrm{Gal}(F/H)$, then $\tau_1$ fixes the elements of $H'$ and so $\tau(\alpha_i) = \alpha_i \in H'$ for all $1 \leq i \leq n + 1$. So the first equation in (1) becomes

$$\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r = 0$$

Now each $\lambda_i$ is nonzero for $1 \leq i \leq r$, and the $\alpha_i$ are linearly independent over $J'$, so it must be that some $\lambda_i$ is not in $J'$, say $\lambda_2 \notin J'$. Since $J'$ is the fixed field of $J$, then there exists some $\sigma \in J$ such that $\sigma(\lambda_2) \neq \lambda_2$.

Next consider a second system of equations (which we will show to be equivalent to (1)):

$$\begin{cases} \sigma\tau_1(\alpha_1)x_1 + \sigma\tau_1(\alpha_2)x_2 + \cdots + \sigma\tau_1(\alpha_{n+1})x_{n+1} = 0 \\ \sigma\tau_2(\alpha_1)x_1 + \sigma\tau_2(\alpha_2)x_2 + \cdots + \sigma\tau_2(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma\tau_n(\alpha_1)x_1 + \sigma\tau_n(\alpha_2)x_2 + \cdots + \sigma\tau_n(\alpha_{n+1})x_{n+1} = 0 \end{cases} \tag{2}$$

Since $\sigma \in J \leq \mathrm{Gal}(F/K)$, then $\sigma(0) = 0$ and if we apply $\sigma$ to each of the equations in (1), then we get (2). Since $x_1 = \lambda_1$, $x_2 = \lambda_2, ..., x_r = \lambda_r$, and $x_{r+1} = \cdots = x_{n+1} = 0$ is a solution of (1), then $x_1 = \sigma(\lambda_1), ..., x_r = \sigma(\lambda_r)$ and $x_{r+1} = \cdots = x_{n+1} = 0$ is also a solution of (2). We claim that the system (2), except for the order of the equations, is identical to (1), so that $x_1 = \sigma(\lambda_1), ..., x_r = \sigma(\lambda_r)$ and $x_{r+1} = \cdots = x_{n+1} = 0$ is a solution of (1). We require the following claims:

(i) For any $\sigma \in J$, $\{\sigma\tau_1, ..., \sigma\tau_n\} \subset J$ is a complete set of coset representatives of the cosets of $H$ in $J$.

(ii) If $\phi$ and $\psi$ are both elements in the same coset of $H$ in $J$, then (since $\alpha_i \in H'$), $\phi(\alpha_i) = \psi(\alpha_i)$ for $1 \leq i \leq n + 1$.

Given the claim, it follows from (i) that there is some reordering $i_1, ..., i_{n+1}$ of $1, 2, ..., n+1$ such that for each $1 \leq k \leq n+1$, $\sigma\tau_k$ and $\tau_{i_k}$ are in the same coset of $H$ in $J$. Then by (ii), the $k$th equation of (2) is identical with the $i_k$th equation of (1). So we have in particular that the solution $x_1 = \lambda_1, ..., x_r = \lambda_r$ and $x_{r+1} = \cdots = x_{n+1} = 0$ of (2) is also a solution of (1). This then completes the proof by contradiction.

Now, to prove (i), note that since each $\tau_i \in J$ and $\sigma \in J$, then $\sigma\tau_i \in J$. Now, $\sigma\tau_i H = \sigma\tau_j H$ if and only if $(\sigma\tau_i)^{-1}(\sigma\tau_j) \in H$; that is,

$$\tau_i^{-1}\sigma^{-1}\sigma\tau_j = \tau_i^{-1}\tau_j \in H$$

and so $\tau_i^{-1}\tau_j \in H$ if and only if $\tau_i H = \tau_j H$, so $\sigma\tau_i H = \sigma\tau_j H$ if and only if $\tau_i H = \tau_j H$. Since $\{\tau_1, ..., \tau_n\}$ is a complete set of representatives of the left cosets of $H$ in $J$, then so is $\{\sigma\tau_1, ..., \sigma\tau_n\}$.

Now to prove (ii), let $\phi, \psi \in \lambda H$ . Then $\phi = \lambda h_1$ and $\psi = \lambda h_2$ for some $h_1, h_2 \in H$. Since $H'$ is a fixed field of $H$ and each $\alpha_i \in H'$, then

$$\phi(\alpha_i) = (\lambda h_1)(\alpha_i) = \lambda h_1(\alpha_i) = \lambda\alpha_i$$

and

$$\psi(\alpha_i) = (\lambda h_2)(\alpha_i) = \lambda h_2(\alpha_i) = \lambda\alpha_i$$

So $\phi(\alpha_i) = \psi(\alpha_i)$ for $1 \leq i \leq n+1$.

**Lemma 2.2.22**

*Let $F$ be an extension field of $K$ and $L$, and $M$ intermediate field with $L \subset M$, and $H$ and $J$ subgroups of the Galois group* $\mathrm{Gal}(F/K)$ *with $H \leq J$.*

*(i) If $L$ is closed and $[M : L]$ is finite, then $M$ is closed and $[L' : M'] = [M : L]$.*

*(ii) If $H$ is closed and $[J : H]$ is finite, then $J$ is closed and $[H' : J'] = [J : H]$.*

*(iii) If $F$ is a finite-dimensional Galois extension of $K$, then all intermediate fields and all subgroups of the Galois group are closed and* $\mathrm{Gal}(F/K)$ *has order $[F : K]$.*

*Proof.*

To see that (i) holds, by Lemma 2.2.16 (iii), we have $M \subset M''$. Since $L \subset M \subset M''$ by Theorem 2.1.3, we have

$$[M'' : L] = [M'' : M][M : L]$$

and so $[M : L] \leq [M'' : L]$. Now, $[L' : M'] \leq [M : L]$ by Lemma 2.2.20 and $[M'' : L''] \leq [L' : M']$ by Lemma 2.2.21. By combining these inequalities gives

$$[M : L] \leq [M'' : L] = [M'' : L''] \leq [L' : M'] \leq [M : L]$$

Therefore, the inequalities reduce to equalities and $[L' : M'] = [M : L]$. Also, $[M'' : L] = [M : L]$ so the dimension of $M''$ over $L$ is the same as the dimension of $M$ over $L$. Also, by Lemma

2.2.16 (iii), $M \subset M''$ and so $M = M''$, and thus, $M$ is closed.

To see that (ii) holds, by Lemma 2.2.16 (iii), $J \leq J''$. Since $H \leq J \leq J''$, then the number of cosets of $H$ in $J$, $[J : H]$ is less than or equal to the number of cosets $H$ in $J''$. That is, $[J : H] \leq [J'' : H]$. So

$$[J : H] \leq [J'' : H] = [J'' : H''] \leq [H' : J'] \leq [J : H]$$

So we have $[H' : J'] = [J : H]$ as required. Also, $[J'' : H] = [J : H]$ and so the number of cosets of $H$ in $J$ equals the number of cosets of $H$ in $J''$. Therefore, $|J| = |J''|$. Also $J \subset J''$, so we must have $J = J''$.

To see that (iii) holds, let $E$ be an intermediate field such that $K \subset E \subset F$. Then

$$[F : K] = [F : E][E : K]$$

by Theorem 2.1.3 and since $[F : K]$ is finite, then $[E : K]$ is also finite. Since $F$ is Galois over $K$, then $K$ is closed. So every intermediate field is closed and $[K' : E'] = [E : K]$. In particular, if $E = F$, then $|\operatorname{Gal}(F/K)| = [\operatorname{Gal}(E/K) : \{e\}] = [K' : F'] = [F : K]$ is finite. Therefore, every subgroup $J$ of $\operatorname{Gal}(F/K)$ is finite. Now, $\{e\}' = F$ and $\{e\}'' = F' = \operatorname{Gal}(F/F) = \{e\}$, so $\{e\}$ is closed. Now, by (ii), $J$ is closed and so every subgroup of $\operatorname{Gal}(F/K)$ is closed. ∎

Now we turn our attention to the intermediate fields. To prove the Fundamental Theorem, we focus our interest on when an intermediate fields has a corresponding group which is normal in $\operatorname{Gal}(F/K)$.

**Definition 2.2.23**

Let $K \subset E \subset F$ be fields. If $E$ is an intermediate field, then $E$ is said to be *stable relative to $K$ and $F$* if every $\sigma \in \operatorname{Gal}(F/K)$ maps $E$ into itself. That is, $\sigma|_E \in \operatorname{Gal}(E/K)$.

We may have $\sigma \in \operatorname{Gal}(F/K)$ mapping $E$ into itself, even onto $E$, but $E$ may not be fixed pointwise by $\sigma$, so we are not saying that $\operatorname{Gal}(F/K)' = E$.

**Lemma 2.2.24**

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

*(i) If $E$ is a stable intermediate field of the extension, then $E' = \operatorname{Gal}(F/E)$ is a normal subgroup of $\operatorname{Gal}(F/K)$.*

*(ii) If $H$ is a normal subgroup of $\operatorname{Gal}(F/K)$, then the fixed field $H'$ of $H$ is a stable intermediate field of the extension.*

*Proof.*

To see that (i) is true, if $\alpha \in E$ and $\sigma \in \operatorname{Gal}(F/K)$, then $\sigma(\alpha) \in E$ by the stability of $E$. Hence, for all $\tau \in E' = \operatorname{Gal}(F/E)$, we have $\tau\sigma(\alpha) = \sigma(\alpha)$. Therefore, for any $\sigma \in \operatorname{Gal}(F/K)$,

$\tau \in E' = \text{Gal}(F/E)$ and $\alpha \in E$, we have

$$\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}\sigma(\alpha) = \alpha$$

Consequently, $\sigma^{-1}\tau\sigma \in E' = \text{Gal}(F/E)$ and hence, $E'$ is a normal subgroup of $\text{Gal}(F/K)$.

To see that (ii) is true, if $\sigma \in \text{Gal}(F/K)$ and $\tau \in H$, then $\sigma^{-1}\tau\sigma \in H$ since $H$ is a normal subgroup of $\text{Gal}(F/K)$. Therefore, for any $\alpha \in H'$, $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ since $H'$ denotes the fixed field of $H$, which implies that $\tau\sigma(\alpha) = \sigma(\alpha)$ for all $\tau \in H$. Thus, $\sigma(\alpha) \in H'$ for any $\alpha \in H'$ and for any $\sigma \in \text{Gal}(F/K)$. This means that $H'$ is stable relative to $K$ and $F$. ∎

**Lemma 2.2.25**

*If $F$ is a Galois extension field of $K$ and $E$ is a stable intermediate field of the extension, then $E$ is Galois over $K$.*

*Proof.*

If $\alpha \in E \setminus K$, then there exists $\sigma \in \text{Gal}(F/K)$ such that $\sigma(\alpha) \neq \alpha$ since $F$ is Galois over $K$. Since $E$ is stable, then $\sigma$ maps $E$ into itself, that is, $\sigma|_E \in \text{Gal}(E/K)$. So for every $\alpha \in E \setminus K$, there exists an element of $\text{Gal}(F/K)$ which does not fix $\alpha$. So the fixed field of $\text{Gal}(F/K)$ is just $K$, i.e. $K = \text{Gal}(F/K)' = K'$. Therefore, $E$ is a Galois extension of $K$. ∎

**Lemma 2.2.26**

*If $F$ is an extension field of $K$ and $E$ is an intermediate field of the extension such that $E$ is algebraic and Galois over $K$, then $E$ is stable (relative to $F$ and $K$).*

*Proof.*

If $\alpha \in E$, let $f \in K[x]$ be the irreducible monic polynomial of $\alpha$ and let $\alpha_1, ..., \alpha_r$ be the distinct roots of $f$ that lie in $E$, where $\alpha = \alpha_1$. Then $r \leq n = \deg(f)$. If $\tau \in \text{Gal}(E/K)$, then by Theorem 2.2.5, $\tau$ permutes roots of $f$; that is, $\tau$ permutes the $\alpha_i$. Therefore, the coefficients of the monic polynomial

$$g(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_r) \in E[x]$$

are fixed by every $\tau \in \text{Gal}(E/K)$ since the coefficients are "symmetric" functions of the $\alpha_i$. Since $E$ is Galois over $K$, then $K = \text{Gal}(E/K)' = K'$ and so the coefficients are all in $K$ and $g \in K[x]$. Now, $\alpha = \alpha_1$ is a root of $g$ and hence, irreducible $f$ divides $g$ by Theorem 2.1.13 (ii). Since $g$ is monic and $\deg(g) \leq \deg(f)$, we must have $f = g$, otherwise, $g$ is a divisor of $f$ since $f$ is irreducible. Consequently, all the roots of $f$ are distinct and lie in $E$. Now if $\sigma \in \text{Gal}(F/K)$, then $\sigma(\alpha)$ is a root of $f$ by Theorem 2.2.5 and thus, $\sigma(\alpha) \in E$. Since $\alpha$ was arbitrary, $\sigma \in \text{Gal}(F/K)$ maps $E$ into itself; that is, $E$ is stable relative to $K$ and $F$. ∎

**Definition 2.2.27**

If $K \subset E \subset F$ are fields, an automorphism $\tau \in \mathrm{Gal}(E/K)$ is *extendable* to $F$ if there exists a $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma|_E = \tau$.

The automorphism in $\mathrm{Gal}(E/K)$ which are extendable to $F$ form a subgroup of $\mathrm{Gal}(E/K)$. Recall that if $E$ is stable, then $E' = \mathrm{Gal}(F/E)$ is a normal subgroup of $\mathrm{Gal}(F/K)$ by Lemma 2.2.24 (i). Consequently, the quotient group $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/E)$ is defined.

**Lemma 2.2.28**

*Let $F$ be an extension field of $K$ and let $E$ be a stable intermediate field of the extension. Then the quotient group $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/K)$ that are extendable to $F$.*

*Proof.*

Since $E$ is an intermediate field that is stable, so every automorphism $\sigma \in \mathrm{Gal}(F/K)$ maps $E$ into itself, and hence, the mapping $\sigma \mapsto \sigma|_E$ defines a group homomorphism from $\mathrm{Gal}(F/K)$ to $\mathrm{Gal}(F/E)$. The image of this homomorphism is a subgroup of $\mathrm{Gal}(E/K)$ of all automorphisms that are extendable to $F$. Now, the kernel of the homomorphism is all elements of $\mathrm{Gal}(F/K)$ which are the identity on $E$; so the kernel is $\mathrm{Gal}(F/E)$. By the First Isomorphism Theorem, the homomorphism induces an isomorphism between $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/E)$ and the image of the homomorphism. So $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/K)$ that are extendable to $F$. ∎

We now have the necessary tools to prove the Fundamental Theorem of Galois Theory (Theorem 2.2.15).

*Proof.*

(of Theorem 2.2.15) Theorem 2.2.19 shows that there is a one-to-one correspondence between the closed intermediate fields and closed subgroups of the Galois group. By Lemma 2.2.22 (iii), all intermediate fields are closed and all subgroups of $\mathrm{Gal}(F/K)$ are closed. So the one-to-one correspondence between closed intermediate fields and closed subgroups is in fact a one-to-one correspondence between all intermediate fields and all subgroups. This correspondence is given by the mapping each group $H$ to its fixed field $H'$ and by mapping each field $M$ to its Galois group $M' = \mathrm{Gal}(F/M)$.

To see that (i) is true, for intermediate fields $L \subset M$, by Lemma 2.2.22 (i), we have $[M : L] = [L' : M']$. The in particular part follows from Lemma 2.2.22 (iii) and so $|\mathrm{Gal}(F/K)| = [F : K]$.

To see that (ii) is true, if $F$ is Galois over $E$ and since $E$ is closed, so $F$ is Galois over every intermediate field. $E$ is finite-dimensional over $K$ since $F$ is finite-dimensional, and hence, by Theorem 2.1.19, $F$ is algebraic over $K$. Consequently, if $E$ is Galois over $K$, then $E$ satisfies the hypotheses of Lemma 2.2.26 and so $E$ is stable relative to $F$ and $K$. By Lemma 2.2.24 (i), $E' = \mathrm{Gal}(F/E)$ is normal in $\mathrm{Gal}(F/K)$. Conversely, if $E' = \mathrm{Gal}(F/E)$ is normal in $\mathrm{Gal}(F/K)$, then by Lemma 2.2.24 (ii), $E''$ is a stable intermediate field. We have established that all intermediate fields are closed, so $E = E''$ and $E$ is stable. Therefore, by Lemma 2.2.25, $E$ is Galois over $K$.

For the "in this case" part, let $E' = \mathrm{Gal}(F/E)$ be normal in $\mathrm{Gal}(F/K)$, or let $E$ be Galois

over $K$. We have shown that every intermediate fields and subgroups are closed, so $E$ and $E'$ are closed. Since $F$ is Galois over $K$, then $\mathrm{Gal}(F/K)' = K$. Now since the elements of $\mathrm{Gal}(F/K)/E'$ are cosets of $E'$ so $|\mathrm{Gal}(F/K)/E'| = [\mathrm{Gal}(F/K) : E']$. Hence,

$$|\mathrm{Gal}(F/K)/E'| = [\mathrm{Gal}(F/K) : E'] = [E'' : \mathrm{Gal}(F/K)'] = [E : K]$$

We saw above that $E''$ is stable and $E = E''$, so $E$ is stable. By Lemma 2.2.28, $\mathrm{Gal}(F/K)/\mathrm{Gal}(E/K)$ is isomorphic to a subgroup of $\mathrm{Gal}(E/K)$. Since we have shown that $|\mathrm{Gal}(F/K)/E'| = [E : K]$, then this subgroup of $\mathrm{Gal}(E/K)$ is of order $[E : K]$. Since $E$ is Galois over $K$, then by (i), $|\mathrm{Gal}(E/K)| = [E : K]$. Since $\mathrm{Gal}(F/K)/E'$ is isomorphic to a subgroup of $\mathrm{Gal}(E/K)$ of order $[E : K]$ and $\mathrm{Gal}(E/K)$ itself is of order $[E : K]$, we have

$$\mathrm{Gal}(F/K)/E' = \mathrm{Gal}(F/K)/\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/K)$$

This completes the proof. ∎

**Theorem 2.2.29: Artin**

*Let $F$ be a group, $G$ a group of automorphisms of $F$, and $K$ the fixed field of $G$ in $F$. Then $F$ is Galois over $K$. If $G$ is finite, then $F$ is a finite-dimensional Galois extension of $K$ with Galois group $G$.*

*Proof.*

Since $K$ is the fixed field of $G$ in $F$, then for every $\alpha \in F \setminus K$, there exists $\sigma \in G$ such that $\sigma(\alpha) \neq \alpha$. By definition of $G$ as a group of automorphisms of $F$ which fixes $K$ elementwise, we have $G \leq \mathrm{Gal}(F/K)$. So each $\sigma \in G$ is also in $\mathrm{Gal}(F/K)$ and therefore, the fixed field of $\mathrm{Gal}(F/K)$ is $K$ itself. By definition, $F$ is Galois over $K$, establishing the first claim.

If $G$ is finite, then by Lemma 2.2.21 with $H = \{e\}$ and $J = G$, which gives $|G| = [G : \{e\}]$ is finite, we have

$$[F : K] = [\{e\}' : G'] \leq [G : 1] = |G|$$

Consequently, $F$ is finite-dimensional over $K$, so $F$ is a finite-dimensional Galois extension of $K$, so by Lemma 2.2.24 (iii), all intermediate groups are closed and so $G = G''$. Since the fixed field of $G$ is $G' = K$, we have that the Galois group of $F$ over $K$ is

$$\mathrm{Gal}(F/K) = K' = G'' = G$$

This completes the proof. ∎

## 2.3 Splitting Fields, Algebraic Closure, and Normality

The topic of this section is the identification and construction of Galois extensions. Our attention is turned to factoring polynomials and finding their roots. We restrict our attention to finite collections of polynomials and omit the part of this section concerning infinite collections of polynomials. After this section, we have the equipment to give a mostly-algebraic proof of the Fundamental Theorem of Algebra.

**Definition 2.3.1**

Let $F$ be a field and $f \in F[x]$ be a polynomial of degree $n$. Then $f$ is said to *split* over $F$ if $f$ can be written as a product of linear factors in $F[x]$; that is,

$$f(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n)$$

with $\alpha_i \in F$.

In other words, $f$ splits over $F$ if $F$ contains all roots of $f$.

**Definition 2.3.2**

Let $K$ be a field and $f \in K[x]$ be a polynomial of degree $n$.

(i) An extension field $F$ of $K$ is a *splitting field over $K$ of polynomial $f$* if $f$ splits in $F[x]$, where $F = K(\alpha_1, ..., \alpha_n)$ with $\alpha_1, ..., \alpha_n$ are the roots of $f$ in $F$.

(ii) Let $S$ be a set of polynomials of positive degree in $K[x]$. An extension field $F$ of $K$ is a *splitting field over $K$ of the set $S$* of polynomials if every polynomial in $S$ splits in $F[x]$ and $F$ is generated over $K$ by the roots of all the polynomials in $S$.

**Example 2.3.3**

The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ has two roots, but the simple extension $\mathbb{Q}(\sqrt{2})$ is the splitting field since it contains both roots. Polynomial $x^3 - 2 \in \mathbb{Q}[x]$ has three roots in $\mathbb{C}$, but the simple extension $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field for $x^3 - 2$ since it contains neither complex root.

**Remark 2.3.4**

If $F$ is a splitting field of set $S$ of polynomials over $K$, then $F = K(X)$, where $X$ is the set of all roots of the polynomials in $S$. By Theorem 2.1.19, $F$ is algebraic over $K$. If $S$ is finite, say $S = \{f_1, ..., f_n\}$ then the set of roots for the polynomials in $S$, is the same as the set of roots for the single polynomial $f = f_1 \cdots f_n$. So when we consider splitting fields of a set $S$ of polynomials, we are really only interested in the cases where $S$ contains one polynomial or $S$ contains infinitely many polynomials. In these notes, we only consider the situation concerning the case where $S$ contains a finite number of polynomials. We have not yet established the existence of splitting fields and the following result starts this process.

**Theorem 2.3.5**

*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 dimension $[F : K] \leq n!$.*

*Proof.*

We prove this by induction on $n = \deg(f)$. For $n = 1$, then we have $F = K$ is a splitting field and $[F : K] = [F : F] = 1 \leq n!$. If $n > 1$ and $f$ does not split over $K$, let $g \in K[x]$ be an irreducible factor of $f$ of degree greater than one. By Theorem 2.1.18 there exists a simple extension field $K(\alpha)$ of $K$ such that $\alpha$ is a root of $g$ and $[K(\alpha) : K] = \deg(g) > 1$. Then by the Factor Theorem, we have $f(x) = (x - \alpha)h(x)$ for some $h \in K(\alpha)[x]$ of degree $n - 1$. Repeating this process and factoring $f$, we can product inductively a splitting field $F$ of $h \in K(u)[x]$ of degree at most $(n - 1)!$. Then $F$ is a splitting field of $f$ over $K$. By Theorem 2.1.3, $[F : K] = [F : K(\alpha)][K(\alpha) : K] \leq (n-1)!\deg(g) \leq (n-1)!n = n!$. The result now follows by induction. ∎

**Definition 2.3.6**

A field $F$ in which every nonconstant polynomial $f \in F[x]$ has a root in $F$ is *algebraically closed*. If $F$ is an extension field of field $K$ such that $F$ is algebraic over $K$ and $F$ is algebraically closed, then $F$ is an *algebraic closure* of field $K$.

If we start with $\mathbb{Q}$, then we have $\mathbb{Q} \subset \mathbb{A}$, where $\mathbb{A}$ is the field of algebraic complex numbers, and $\mathbb{Q} \subset \mathbb{C}$. Both $\mathbb{A}$ and $\mathbb{C}$ are algebraically closed. An algebraic closure of $\mathbb{Q}$ is $\mathbb{A}$. The complex numbers $\mathbb{C}$ are an algebraically closed extension field of $\mathbb{Q}$ but $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$ since $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$.

By the Factor Theorem, for any $f \in F[x]$ that has a root in $F$, then each such $f$ can be factored into a product of linear terms. That is, every nonconstant $f$ splits over $F$. This also means that there is no proper algebraic extension field of $F$.

**Theorem 2.3.7**

*Every field $K$ has an algebraic closure. Any two algebraic closures of $K$ are $K$-isomorphic.*

The proof of Theorem 2.3.7 requires Zorn's Lemma.

*Proof.*

Choose a set $S$ such that $\aleph_0|K| < |S|$ which can be done since $|\mathcal{P}(A)| > |A|$ for any $A$. Since $|K| \leq \aleph_0|K|$, there exists an injection $\theta : K \to S$. Since $S$ was chosen only for its cardinality, we could redefine the image of $K$ to be $K$ itself, so $\theta$ maps $k \in K$ to itself, and replace Range$(\theta)$ with $K$ to get $K \subset S$.

**Step 1:** Let $\mathcal{S}$ be the class of all finite fields $E$ such that $E$ is a subset of $S$ and $E$ is an algebraic extension of $K$. So we are using the set $S$ as a set of symbols on which extension fields of $K$ are defined. now we argue that $\mathcal{S}$ is a set. Now a field $E$ in $\mathcal{S}$ is completely determined by the subset $E$ of $S$ and the binary operations of addition and multiplication in $E$. Now, addition and multiplication are defined by the functions $\phi$ and $\psi$ mapping $E \times E \to E$.

So we identify $\phi$ and $\psi$ with their "graphs", which are subsets of $E \times E \times E \subset S \times S \times S$. Consequently, there is an injection $\tau : \mathcal{S} \to P$, where

$$P = \mathcal{P}(S \times (S \times S \times S) \times (S \times S \times S))$$

given by the mapping $E \mapsto (E, \phi, \psi)$. The injection property of $\tau$ follows from the fact that $\phi$

and $\psi$ are binary operations and for two different fields $E_1$ and $E_2$ in $\mathcal{S}$, either the corresponding $\phi$'s or $\psi$'s must differ, and so the graphs of the corresponding $\phi$'s or $\psi$'s must differ. Therefore, $\tau(E_1) \neq \tau(E_2)$. Now, Range$(\tau)$ is a set by the "Axiom of Class Formation", namely,

$$\text{Range}(\tau) = \{X \in P : X = \tau(E) \text{ for some } E \in \mathcal{S}\}$$

Since $\tau : \mathcal{S} \to P$ is injective, $\tau^{-1}$ is a function and $\tau^{-1}(\text{Range}(\tau)) = \mathcal{S}$. That is, $\mathcal{S}$ is the image of a set under a function.

**Step 2:** Note that $\mathcal{S} \neq \emptyset$ since $K \in \mathcal{S}$. Partially order the set $\mathcal{S}$ by defining $E_1 \leq E_2$ if and only if $E_2$ is an extension field of $E_1$. Then every chain under "$\leq$" has an upper bound, namely, the union of all fields in the chain. Therefore, by Zorn's Lemma, there exists a maximal element $F$ of $\mathcal{S}$.

**Step 3:** We now show that $F$ is algebraically closed. Assume for a contradiction that $F$ is not algebraically closed. Then there exists $f \in F[x]$ that does not split over $F$. By Theorem 2.1.18, there exists a proper algebraic extension $F_0 = F(\alpha)$ of $F$ where $\alpha$ is a root of $f$ which does not lie in $F$. Since $F$ is algebra ic over $K$ and $F(\alpha)$ is algebraic over $F$, then $F_0 = F(\alpha)$ is an algebraic extension of $K$ by Theorem 2.1.21. Notice that we cannot get a contradiction based on $F_0$ since we do not have $F_0 \in \mathcal{S}$. Therefore, $|F_0 \setminus F| \leq |F_0|$ since $F_0 \setminus F \subset F_0$ and $|F_0| \leq \aleph_0|K|$. So the argument in the first paragraph, $|F_0 \setminus F| \leq |F_0| \leq \aleph_0|K| < |S|$. Since $|F| \leq |F_0| < |S|$ and $|S| = |F \cup (S \setminus F)| = |S \setminus F| + |F|$, and so we have $|S| = |S \setminus F|$. Thus, $|F_0 \setminus F| < |S| = |S \setminus F|$ and there exists an injection $\xi : F_0 \setminus F \to X \setminus F$. Extend $\xi$ to all of $F_0$ by defining $\xi$ as the identity on $F$ and letting $\xi$ map $F_0$ into $S$; the extended $\xi$ is still injective.

Denote Range$(\xi) = F_1$. Define in $F_1$ the sum $\xi(a) + \xi(b)$ as $\xi(a + b)$ and define the product $\xi(a)\xi(b)$ as $\xi(ab)$. Then $F_1$ is a field isomorphic to $F_0$ and $\xi : F_0 \to F_1$ is an $F$-isomorphism. Since $F \subset F_1$, then $F_1$ is an extension field of $F$. Consequently, since $F_0$ is a proper algebraic extension of $F$, and hence, of $K$, then so is $F_1$. Also, by construction, $F_1 \in \mathcal{S}$, so under the partial ordering on $\mathcal{S}$, we have $F \leq F_1$, but this contradicts to the maximality of $F$ in $\mathcal{S}$. So the assumption that $F$ is not algebraically closed is false, and so $F$ is algebraically closed. Since $F_0$ is algebraic over $K$ and $F_1$ is $F$-isomorphic to $F_0$, then $F_1$ is algebraic over $K$. Therefore, $F$ is an algebraic closure of $K$. ∎

We now turn our attention to the uniqueness of splitting fields.

**Theorem 2.3.8: For $S$ Finite**

*Let $\sigma : K \to L$ be an isomorphism of fields, $S = \{f_1, ..., f_n\}$ be a set of polynomials of positive degree in $K[x]$ and $S' = \{\sigma f_1, ..., \sigma f_n\}$ 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 extendable to an isomorphism $F \simeq M$.*

# Index

# Bibliography

[1] Thomas W. Hungerford. *Algebra*. New York Springer, 2008.