Math 454: Galois Theory

Contents

A Few First Words

The aim of this course is a fairly detailed account of the theory of fields and the particular subtopic of Galois theory. This topic requires a good deal of language from the broad area of algebra. Though our interest is in fields, we will need results from group theory, ring theory, and linear algebra. These notes will, as best as one can, be self-contained. One corollary of this is that these notes will be quite brisk in the treatment of various topics that typically are covered in several weeks; my treatment of group theory in chapter 1 is a good example.

The reader seeking a deeper understanding of this topic should work all of the exercises. Many are trivial, some are of moderate difficulty, and a few are difficult. Text that appears in blue indicates that there is a link to an external webpage. The reader seeking a deeper understanding of this topic should read most/all of these link pages in some level of detail. There are supplemental sections for the reader. If the supplemental section has $*$, then this supplemental section is "required reading". The reader seeking a deeper understanding of this topic should read the supplemental sections as part of the main text. Supplemental sections will not be covered in my lectures but are, generally, quite important.

To understand mathematics, you must be unafraid to make mistakes. Misunderstandings of topics are expected and lead to a better understanding. Examples are central to those starting out. You must find examples and know them well. They help one test/probe abstract concepts. These notes are quite sparse from the perspective of examples and this is intentional. You must find the examples on your own. You must make them part of you. New topics in mathematics are like new worlds and like any good explorer, you must venture out. You walk fifty steps east and discover a river. You walk 1.3 miles south and discover a cave. Good explores make notes of the important features of the lands around them. Over time, you will have some crude map of the world based on your explorations. If I were to hand you a map on the first day of your arrival, you would not appreciate what it said nor have any more knowledge of the land than a foreigner. You must explore and make your own maps for real understanding. That said, I am your guide and you should check often with me the accuracy of your views of the mathematical world we explore. Though I cannot tell you how the world is, I can tell you how it is not.

Chapter 1

Preliminaries

In this first chapter, we will review the requisite material on groups required in this course. Our treatment will center around group actions. A reader even with a moderate mastery of group theory will hopefully find some merits to this section though much of it should be review for a student who is well versed in this topic. We will also require some material on polynomial rings and the theory of ideals in rings but will postpone a discussion on these topics until the next chapter.

Notation

Throughout these notes, the natural numbers will be denoted by $\mathbf{N}$, the integers by $\mathbf{Z}$, the rational numbers by $\mathbf{Q}$, the real numbers by $\mathbf{R}$, and the complex numbers by $\mathbf{C}$. G will typically denote a group, R will typically denote a ring, F will typically denote a field, A will typically denote an F–algebra, and ψ will typically represent a homomorphism of groups or rings or fields or algebras.. Ideals with typically be denoted in german gothic $\mathfrak{a}$ with $\mathfrak{p}$ and $\mathfrak{m}$ typically denote prime and maximal ideals, respectively.

1.1 *Groups: Basics*

The theory of groups resides in the broader topic of algebraic structures on sets. **Groups** are one of the most basic algebraic structures that one can have on a set; **monoids**, **semi-groups**, and **magmas** provide even less structure (more structure is less general).

Definition 1.1 (Group Structure). *A group structure on a set G is a 2–tuple or pair (μ, e) where $e \in G$, $\mu : G \times G \to G$ is a function, and subject to the following:*

(a) For each $g \in G$, we have $\mu(g,e) = \mu(e,g) = g$.

(b) For each $g \in G$, there exists $h_g \in G$ such that $\mu(g,h_g) = \mu(h_g,g) = e$.

(c) For each $g,h,k \in G$, we have $\mu(g,\mu(h,k)) = \mu(\mu(g,h),k)$.

The function μ is special type of **binary operation** on G. For notational simplicity, we will define

$$g \cdot h \stackrel{\text{def}}{=} \mu(g,h).$$

The notation $\cdot$ should be thought of as a multiplication operation. The element $e \in G$ satisfying (a) in Definition 1.1 is referred to as the **identity element** and plays the role of 1 under multiplication or 0 under addition. In the next section, we will further simplify our notation for the group operation. We have postponed this simplification in order to emphasize the group operation in this section.

Exercise 1.1. *Let (μ, e) be a group structure on G. If $g_0 \in G$ satisfies $g_0 \cdot g = g \cdot g_0 = g$ for all $g \in G$, prove that $g_0 = e$. In particular, e is the unique element satisfying (a) in Definition 1.1.*

Given an element $g \in G$, the element $h_g \in G$ in (b) of Definition 1.1 is referred to as the **inverse** of g.

Exercise 1.2. *Let (μ, e) be a group structure on G and $g \in G$. Prove that if $h_1, h_2 \in G$ satisfy (b) in Definition 1.1, then $h_1 = h_2$.*

By Exercise 1.2, inverses are unique. For each $g \in G$, we denote the unique inverse by g^{-1} and note that in our simplified notation, (b) in Definition 1.1 can be written as $g \cdot g^{-1} = g^{-1} \cdot g = e$.

For the readers' clarity, we rewrite Definition 1.1 in our simplified notation. A group structure on G is a 2–tuple $(\cdot, e)$ where $\cdot$ is a binary operation on G, $e \in G$, and satisfying the following three properties:

(a) For all $g \in G$, we have $g \cdot e = e \cdot g = g$.

(b) For each $g \in G$, there exists a unique $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

(c) For each $g,h,k \in G$, we have $g \cdot (h \cdot k) = (g \cdot h) \cdot k$.

In this new notation, the reader can now clearly see that (c) in Definition 1.1 is merely an **associativity law** for our multiplication operation.

We will not develop the theory of groups beyond what we require for this class. Two important concepts in basic group theory are the concepts of morphisms between groups (functions between groups that are compatible with the group operations) and subgroups (subsets of the group for which the group operation restricts to endow the subset with a group structure).

Definition 1.2 (Group Homomorphism)**.** *Given a pair of groups G, H and a function $\psi\colon G \to H$, we say that ψ is a* ***group homomorphism*** *if $\psi(g_1 \cdot g_2) = \psi(g_1) \cdot \psi(g_2)$ for all $g_1, g_2 \in G$.*

Note that in Definition 1.2, we have two different group operations in our condition for ψ to be a homomorphism. Being more pedantic with which operations we are using, we denote the group operation on G by $\cdot_G$ and the group operation on H by $\cdot_H$. In this notation, $\psi\colon G \to H$ is a homomorphism if

$$\psi(g_1 \cdot_G g_2) = \psi(g_1) \cdot_H \psi(g_2).$$

As it is typically clear which group operation we are using, we will rarely distinguish in our notation which operation is which. We hope that this will not lead to any unnecessary confusion and note that this choice is merely to simplify our notation; strictly speaking, it is lazy to do such.

Exercise 1.3. *Prove that if $\psi\colon G \to H$ is a homomorphism of groups, then the following holds:*

(i) $\psi(e_G) = e_H$ *where $e_G \in G$ and $e_H \in H$ are the identity elements.*

(ii) $\psi(g^{-1}) = (\psi(g))^{-1}$.

Exercise 1.4. *Let G be a group and $g \in G$. Prove that $\mathrm{Ad}_g\colon G \to G$ defined by $\mathrm{Ad}_g(h) = g^{-1}hg$ is a homomorphism.*

We next introduce the concept of a subgroup.

Definition 1.3 (Subgroup)**.** *We say that $H \subseteq G$ of a group G is a* ***subgroup*** *if $e \in H$ and the restriction of μ to $H \times H$, namely, $\mu_H = \mu_{|H\times H}$, is such that (μ_H, e) is a group structure on H. When $H \subseteq G$ is a subgroup, we will write $H \leq G$.*

The following exercise, specifically (i), provides an alternative for Definition 1.3. From a practical viewpoint, (i) is preferred as the definition of subgroup. However, (i) is, on face value, merely a condition on a subset and does not fully revel that the subset is a subgroup.

Exercise 1.5. *Let G be a group.*

(i') *Prove that if $\{H_i\}_{i\in I}$ is a collection of subgroups of a group G, then bigcap$_{i\in I}H_i$ is a subgroup of G. Find an example of a group G with subgroups $H_1, H_2 \leq G$ such that $H_1 \cup H_2$ is not a subgroup*

(i) *Prove that $H \subseteq G$ is a subgroup if and only if $e \in H$ and for each $h_1, h_2 \in H$, we have $h_1 \cdot h_2^{-1} \in H$.*

(ii) *Prove that $\{e\}$ is a subgroup of G. This subgroups is called the* ***trivial subgroup****.*

(iii) *Prove that G is a subgroup of G. [Hint: Don't think too hard about this]*

(iv) *Given a subset $S \subseteq G$, let $G_S \subseteq G$ be the subset of all elements of G of the form*

$$s_1 \cdot s_2 \cdot \ldots \cdot s_\ell$$

where for each $i = 1, \ldots, \ell$, either $s_i \in S$ or $s_i^{-1} \in S$. Prove that G_S is a subgroup of G and $S \subseteq G_S$. For future reference, we will denote G_S simply by $\langle S \rangle$ and call this the ***subgroup generated by*** *S.*

(v) *Given $S \subseteq G$ and G_S as in (iv), prove that if $H \leq G$ is any subgroup of G with $S \subseteq H$, then $G_S \subseteq H$. In particular,*

$$G_S = \bigcap_{\substack{H \leq G, \\ S \subseteq H}} H.$$

From Exercise 1.5 (ii) and (iii), we see that every group comes with at least two subgroups, provided G is not equal to the trivial group $\{e\}$. Additionally, Exercise 1.5 (iv) indicates that one expects that there should be additional subgroups beyond the two trivial "bookend" examples $\{e\}$ and G. Provides G is not finite with $|G| = p$ where p is a prime, there will always be subgroups strictly between $\{e\}$ and G.

Before moving to some important concepts related to subgroups, we further discuss the meaning of (i) in Exercise 1.5. A subset $H \subseteq G$ of a group G is a subgroup if $e_G \in H$ and H is closed under multiplication and inverses. Specifically, for each $h_1, h_2 \in H$, we have $h_1 \cdot h_2 \in H$ and for each $h \in H$, we have $h^{-1} \in H$. The reference to "closed" in with regard to the fact that in a subgroup, multiplication and inversion of elements in the subset remain in the subset. Exercise 1.5 (i) is a condensed version of this discussion and packages both of these closure properties into one property. The condition that $e \in H$ ensures that H is not the empty set as the empty set vacuously satisfies the closure condition but is not a subgroup since any group is necessary non-empty.

We next introduce an special subclass of subgroups that will afford us with a general method for constructing new groups from a given group G via a quotient procedure.

Definition **1.4** (Normal Subgroup)**.** *We say that a subgroup $H \leq G$ is* ***normal*** *if $\mathrm{Ad}_g(H) \subseteq H$ for all $g \in G$. When $H \leq G$ is a normal subgroup, we write $H \lhd G$.*

We will see momentarily that normal subgroups of G are in bijection with surjective group homomorphisms $\psi \colon G \to H$. This fact, which is part of the content of the First Isomorphism Theorem (see Theorem 1.3 below) is an analog of the Rank-Nullity Theorem from linear algebra. In order to establish

this connection, we will need to first introduce the concept of cosets associated to a subgroup of a group. Keeping with our analogy with vector spaces, if normal subgroups of a group are the analog of a vector subspace of a vector space, the cosets associated to the group are the analogies of affine subspaces of a vector space. As the reader might not be familiar with affine subspaces, we briefly discuss them here. Given a vector space V and a vector subspace W, there is a family of affine subspaces of V that we can construct from W. Specifically, given a vector $v \in V$, we can form the subset

$$W + v = \{w + v \ : \ w \in W\}.$$

For example, if $V = \mathbf{R}^3$ and W is the vector subspace spanned by the first and second coordinates (i.e., the xy–plane), then the affine subspaces $W + v$ are planes that are parallel to W but do not contain the zero vector in $\mathbf{R}^3$ unless $v \in W$. Affine subspaces are important in several areas of mathematics. They are nearly as structured as vector spaces as one can still defining a scalar multiplication operation on them. However, they lack the "base point" or choice of zero vector. For example, given a (smooth) surface S in $\mathbf{R}^3$ and a point $p \in S$, from calculus, we define a tangent plane for S at p which is the 2–dimensional analog of a tangent line to a curve in $\mathbf{R}^2$. This plane, viewed as a subset of $\mathbf{R}^3$, is not a vector subspace but is an affine subspace. We can easily endow it with a vector space structure since the point $p \in S$ is a point on the tangent plane. Specifically, we can view p as the zero vector in this affine space. Indeed, the tangent plane T_pS is an affine subspace of the form $W + p$ and we have a bijective function $W \to T_pS$ given by $w \mapsto w + p$. In particular, the zero vector in W maps to p under this mapping. The inverse endows T_pS with a natural vector space structure where p plays the role of the zero vector.

We now define a coset associated to a general subgroup of a group.

Definition 1.5 (Cosets)**.** *Given a subgroup $H \leq G$ and $g \in G$, we define the **left coset of g with respect to H** to be the subset*

$$gH = \{g \cdot h \ : \ h \in H\}$$

*and the **right coset of g with respect to H** to be the subset*

$$Hg = \{h \cdot g \ : \ h \in H\}.$$

The following exercise shows that one can partition a group into H–cosets for any subgroup $H \leq G$; the exercise is stated in terms of an equivalence relation on G which is equivalent to a partitioning of G.

Exercise 1.6. *Let G be a group and H be a subgroup of G.*

*(i) Define the **partial relation** $\sim_H$ on G by $g_1 \sim_H g_2$ if and only if $g_2^{-1} g_1 \in H$. Prove that $\sim_H$ is an **equivalence relation** on G.*

(ii) Prove that $g_1 \sim_H g_2$ if and only if $g_1 H = g_2 H$.

(iii) Prove that if $g_1, g_2 \in G$, then either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$. [Hint: Use (i), (ii)].

(iv) Prove that H is normal in G if and only if $gH = Hg$ for all $g \in G$.

Given a subgroup $H \leq G$, by Exercise 1.6, we can **partition** G into equivalence classes via the equivalence relation $\sim_H$. Moreover, if $g \in G$, we see that

$$gH = \left\{ g' \in G \,:\, g \sim_H g' \right\}.$$

We define the quotient set G/H to be the set of distinct equivalence classes gH. The set G/H is often referred to as the set of cosets or the coset space.

Our next concept of index is a very coarse analog of codimension of a vector subspace; it is specifically related but the codimension and index are not literally the same concepts.

***Definition* 1.6** (Index)**.** *Let G be a group and $H \leq G$. We define the **index** of H in G to be the cardinality of the coset space G/H. In particular, if G/H is finite, we say that H is **finite index**. Finally, we denote the index of H in G by $[G : H]$.*

If H is a normal subgroup, the set G/H can be equipped with a group structure as follows. We define $\overline{e} = eH = H$ and given $g_1H, g_2H \in G/H$, we define $\overline{\mu} \colon G/H \times G/H \to G/H$ by

$$\overline{\mu}(g_1H, g_2H) = (g_1 \cdot g_2)H.$$

It is critical to point out that we must show that our multiplication operation $\overline{\mu}$ is independent of the choices of g_1, g_2. Specifically, if $k_1 \in g_1H$ and $k_2 \in g_2H$, we have $k_1H = g_1H$ and $k_2H = g_2H$. In order for our multiplication operation on G/H to be well defined, we must prove that $(k_1 \cdot k_2)H = (g_1 \cdot g_2)H$. We will do this in perhaps the most simple minded way by proving

$$(k_1 \cdot k_2)H \subseteq (g_1 \cdot g_2)H$$

and

$$(g_1 \cdot g_2)H \subseteq (k_1 \cdot k_2)H.$$

To that end, let $g \in (k_1 \cdot k_2)H$. By definition, there exists $h_1 \in H$ such that $g = k_1 \cdot k_2 \cdot h_1$. Since $k_1 \in g_1H$, there exists $h_2 \in H$ such that $k_1 = g_1 \cdot h_2$. Likewise, since $k_2 \in g_2H$, there exists $h_3 \in H$ such that $k_2 = g_2 \cdot h_3$. In particular, we have

$$g = g_1 \cdot h_2 \cdot g_2 \cdot h_3 \cdot h_1. \tag{1.1}$$

Now, $h_2 \cdot g_2 \in Hg_2$ and by Exercise 1.6 (iv), we know that $g_2H = Hg_2$; note that this requires that H be normal in G. Consequently, there exists $h_4 \in H$ such that $h_2 \cdot g_2 = g_2 \cdot h_4$. Replacing $h_2 \cdot g_2$ with $g_2 \cdot h_4$ in (1.1), we obtain

$$g = g_1 \cdot g_2 \cdot h_4 \cdot h_3 \cdot h_1.$$

Since H is a subgroup, we know that $h_4 \cdot h_3 \cdot h_1 \in H$. Setting $h_5 = h_4 \cdot h_3 \cdot h_1$, we obtain

$$g = g_1 \cdot g_2 \cdot h_5 \in (g_1 \cdot g_2)H.$$

Thus, we conclude that $(k_1 \cdot k_2)H \subseteq (g_1 \cdot g_2)H$.

For the reverse implication, which is logically identical, we start with $g \in (g_1 \cdot g_2)H$. By definition, there exists $h_6 \in H$ such that $g = g_1 \cdot g_2 \cdot h_6$. Since $g_1 \in k_1 H$ and $g_2 \in k_2 H$, there exist $h_7, h_8 \in H$ such that $g_1 = k_1 \cdot h_7$ and $g_2 = k_2 \cdot h_8$. Hence

$$g = k_1 \cdot h_7 \cdot k_2 \cdot h_8 \cdot h_6 \tag{1.2}$$

Since H is normal, we know that $k_2 H = H k_2$ and so there exists $h_9 \in H$ such that $h_7 \cdot k_2 = k_2 \cdot h_9$. Replacing $h_7 \cdot k_2$ with $k_2 \cdot h_9$ in (1.2) yields

$$g = k_1 \cdot k_2 \cdot h_9 \cdot h_8 \cdot h_6.$$

Finally, setting $h_{10} = h_9 \cdot h_8 \cdot h_6 \in H$, we see that

$$g = k_1 \cdot k_2 \cdot h_{10} \in (k_1 \cdot k_2)H.$$

Hence, $(g_1 \cdot g_2)H \subseteq (k_1 \cdot k_2)H$.

It remains to prove that $(\overline{\mu}, \overline{e})$ is a group structure on G/H. By definition of $\overline{\mu}$, we see that

$$\overline{\mu}(eH, gH) = (e \cdot g)H = gH, \quad \overline{\mu}(gH, eH) = (g \cdot e)H = gH.$$

Hence, eH satisfies the property of the identity element. Given $gH \in G/H$, we assert that $g^{-1}H \in G/H$ is a multiplicative inverse. Again, by definition of $\overline{\mu}$, we have

$$\overline{\mu}(gH, g^{-1}H) = (g \cdot g^{-1})H = eH, \quad \overline{\mu}(g^{-1}H, gH) = (g^{-1} \cdot g)H = eH.$$

Hence, $g^{-1}H$ satisfies the property of a multiplicative inverse for gH. Finally, we must prove that

$$\overline{\mu}(g_1 H, \overline{\mu}(g_2 H, g_3 H)) = \overline{\mu}(\overline{\mu}(g_1 H, g_2 H), g_3 H).$$

To that end, we have

$$\begin{aligned} \overline{\mu}(g_1 H, \overline{\mu}(g_2 H, g_3 H)) &= \overline{\mu}(g_1 H, (g_2 \cdot g_3)H) = (g_1 \cdot (g_2 \cdot g_3))H \\ &= ((g_1 \cdot g_2) \cdot g_3)H = \overline{\mu}((g_1 \cdot g_2)H, g_3 H) \\ &= \overline{\mu}(\overline{\mu}(g_1 H, g_2 H), g_2 H). \end{aligned}$$

We now summarize the above construction in the following definition.

Definition 1.7 (Quotient Group)**.** *Given a group G and normal subgroup $H \lhd G$, we call the set G/H with the group structure $(\overline{\mu}, \overline{e})$ the **quotient group** of G by H.*

Given a normal subgroup $H \lhd G$, we have an associated quotient function $\psi_H \colon G \to G/H$ given by $\psi_H(g) = gH$. We assert that ψ_H is a group homomorphism. To see this assertion, we must prove that $\psi_H(g_1 \cdot g_2) = \psi_H(g_1) \cdot \psi_H(g_2)$. For that, simply note that

$$\psi_H(g_1 \cdot g_2) = (g_1 \cdot g_2)H = g_1 H \cdot g_2 H = \psi_H(g_1) \cdot \psi_H(g_2).$$

We again summarize the above observation in the following definition.

Definition 1.8 (Canonical Homomorphism)**.** *Given a group G and normal subgroup H, the homomorphism $\psi_H \colon G \to G/H$ is called the **canonical homomorphism**.*

Concepts of "equal" in algebra are more structured examples of the concept of "equal" sets. Two sets X, Y, in a practical sense, are "equal" if there exists a bijective function $f \colon X \to Y$. For groups to be "equal", we further require that the function be a group homomorphism. This leads us to the concept of isomorphic groups and isomorphisms (i.e. the function that identifies them).

Definition 1.9 (Isomorphism)**.** *We say that two groups G_1, G_2 are **isomorphic** if there exists a **bijective** group homomorphism $\psi \colon G_1 \to G_2$. We call ψ an **isomorphism** in this case.*

We now move to the concept of kernel and image of a homomorphism. These are fairly direct analogs of the kernel and image of a linear function between vector spaces. Given a group homomorphism $\psi \colon G \to H$, we have a pair of associated subsets, one in G and one in H. First, we have

$$\ker \psi = \{g \in G \ : \ \psi(g) = e_H\}$$

which is referred to as the **kernel** of ψ. Second, we have

$$\psi(G) = \{h \in H \ : \ h = \psi(g) \text{ for some } g \in G\}$$

which is referred to as the **image**.

Lemma 1.1. *If $\psi \colon G \to H$ is a group homomorphism, then $\ker \psi$ is a normal subgroup of G and $\psi(G)$ is a subgroup of H.*

Proof. By Exercise 1.3 (i), we know that $e_G \in \ker \psi$. Given $g_1, g_2 \in \ker \psi$, by Exercise 1.5 (i), it suffices to prove that $g_1 \cdot g_2^{-1} \in \ker \psi$. To that end, we have

$$\psi(g_1 \cdot g_2^{-1}) = \psi(g_1) \cdot \psi(g_2^{-1}) = \psi(g_1) \cdot (\psi(g_2))^{-1} = e_H \cdot e_H^{-1} = e_H.$$

Hence, $g_1 \cdot g_2^{-1} \in \ker \psi$. To see that $\ker \psi$ is normal, for each $g \in G$ and $g_1 \in \ker \psi$, we must prove that $g^{-1} \cdot g_1 \cdot g \in \ker \psi$. Again, we have

$$\psi(g^{-1} \cdot g_1 \cdot g) = (\psi(g))^{-1} \cdot \psi(g_1) \cdot \psi(g) = (\psi(g))^{-1} \cdot e_H \cdot \psi(g) = (\psi(g))^{-1} \cdot \psi(g) = e_H.$$

Next, we prove that $\psi(G)$ is a subgroup of H. By Exercise 1.3 (i), $\psi(e_G) = e_H$, and so $e_H \in \psi(G)$. Hence, by Exercise 1.5 (i), it suffices to prove that if $h_1, h_2 \in \psi(G)$, then $h_1 \cdot h_2^{-1} \in \psi(G)$. To that end, since $h_1, h_2 \in \psi(G)$, there exists $g_1, g_2 \in G$ such that $h_1 = \psi(g_1)$ and $h_2 = \psi(g_2)$. Finally, since ψ is a homomorphism, we have

$$h_1 \cdot h_2^{-1} = \psi(g_1) \cdot (\psi(g_2))^{-1} = \psi(g_1) \cdot \psi(g_2^{-1}) = \psi(g_1 \cdot g_2^{-1}) \in \psi(G).$$

♠

The following lemma is straightforward and left for the reader to prove.

***Lemma* 1.2.** *If $\psi\colon G \to G'$ is a homomorphism of groups and $H \leq G$, then the restriction $\psi_{|H}\colon H \to G'$ is a homomorphism of groups. In particular, $\psi(H) \leq G'$.*

***Exercise* 1.7.** *Prove Lemma 1.2*

The following result is often referred to as the **First Isomorphism Theorem**.

***Theorem* 1.3** (First Isomorphism Theorem)**.** *Let G, H be groups and $\psi\colon G \to H$. Then the function $\overline{\psi}\colon G/\ker\psi \to \psi(G)$ given by $\overline{\psi}(g \ker \psi) = \psi(g)$ is an isomorphism. In particular, $G/\ker\psi$ and $\psi(G)$ are isomorphic groups.*

Proof. We have the function $\overline{\psi}\colon G/\ker\psi \to \psi(G)$ given by $\overline{\psi}(g\ker\psi) = \psi(g)$. We must prove four things:

(1) $\overline{\psi}$ is well defined (i.e. does not depend on the choice of g).

(2) $\overline{\psi}$ is a group homomorphism.

(3) $\overline{\psi}$ is **one-to-one**/injective.

(4) $\overline{\psi}$ is **onto**/surjective.

For (1), given $g\ker\psi \in G/\ker\psi$ and any $g' \in g\ker\psi$, we must prove that $\psi(g) = \psi(g')$. This will prove that of definition of $\overline{\psi}$ does not depend on the choice of the element in $g\ker\psi$. Since $g' \in g\ker\psi$, there exists $g_1 \in \ker\psi$ such that $g' = g \cdot g_1$. In particular,

$$\psi(g') = \psi(g \cdot g_1) = \psi(g) \cdot \psi(g_1) = \psi(g) \cdot e_H = \psi(g).$$

For (2), given $g_1\ker\psi, g_2\ker\psi \in G/\ker\psi$, we must prove that

$$\overline{\psi}(g_1\ker\psi \cdot g_2\ker\psi) = \overline{\psi}(g_1\ker\psi) \cdot \overline{\psi}(g_2\ker\psi).$$

To that end, we have

$$\begin{aligned}\overline{\psi}(g_1\ker\psi \cdot g_2\ker\psi) = \overline{\psi}((g_1 \cdot g_2)\ker\psi) &= \psi(g_1 \cdot g_2) \\ &= \psi(g_1) \cdot \psi(g_2) = \overline{\psi}(g_1\ker\psi) \cdot \overline{\psi}(g_2\ker\psi).\end{aligned}$$

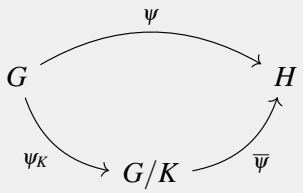
For (3), to show that $\overline{\psi}$ is injective, we must prove that for any $g_1\ker\psi, g_2\ker\psi \in G/\ker\psi$ with $g_1\ker\psi \neq g_2\ker\psi$, we have $\overline{\psi}(g_1\ker\psi) \neq \overline{\psi}(g_2\ker\psi)$. By Exercise 1.6 (i) and (ii), we know that $g_1 \cdot g_2^{-1} \notin \ker\psi$. By definition of $\ker\psi$, we must have $\psi(g_1 \cdot g_2^{-1}) \neq e_H$ and so $\psi(g_1) \neq \psi(g_2)$. In particular, by definition of $\overline{\psi}$, we see that

$$\overline{\psi}(g_1\ker\psi) = \psi(g_1) \neq \psi(g_2) = \overline{\psi}(g_2\ker\psi).$$

For (4), to show that $\overline{\psi}$ is surjective, we must prove that for any $h \in \psi(G)$, there exists $g\ker\psi \in G/\ker\psi$ such that $\overline{\psi}(g\ker\psi) = h$. Since $h \in \psi(G)$, there exists $g \in G$ such that $\psi(g) = h$. By definition of $\overline{\psi}$, we see that $\overline{\psi}(g\ker\psi) = \psi(g) = h$, as needed. ♠

The following corollary of the First Isomorphism Theorem is the analog of the fact that given any surjective linear function $L\colon V \to W$, there exists a basis $\mathscr{B}_V = \{v_1, \ldots v_m\}$ of V and a basis $\mathscr{B}_W = \{w_1, \ldots, w_m\}$ such that $L(v_i) = w_i$.

Corollary 1.4. *Let G, H be groups, $\psi\colon G \to H$ a surjective group homomorphism, and $K = \ker\psi$. Then H and G/K are isomorphic and the diagram*



commutes. Namely, $\psi = \overline{\psi} \circ \psi_K$.

The following result is often referred to as the **Second Isomorphism Theorem**.

***Theorem* 1.5** (Second Isomorphism Theorem)**.** *Let G be a group, $K \leq G$, and $H \lhd G$. Then*

(a) The set

$$HK = \{h \cdot k \ : \ h \in H, \ k \in K\}$$

is a subgroup of G.

(b) $H \cap K$ is a normal subgroup of K.

(c) The groups HK/H and $K/(H \cap K)$ are isomorphic.

Proof. For (a), since both H, K are subgroups of G, we know that $e \in H$ and $e \in K$. In particular, $e \in HK$. Given $h_1 \cdot k_1, h_2 \cdot k_2 \in HK$, we see that

$$h_1 \cdot k_1 \cdot (h_2 \cdot k_2)^{-1} = h_1 \cdot k_1 \cdot k_2^{-1} \cdot h_2^{-1}.$$

Since H is normal, we know that $(k_1 \cdot k_2^{-1})H = H(k_1 \cdot k_2^{-1})$. Hence, there exists $h_3 \in H$ such that $k_1 \cdot k_2^{-1} \cdot h_2 = h_3 \cdot k_1 \cdot k_2^{-1}$. Therefore,

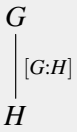
$$h_1 \cdot k_1 \cdot k_2^{-1} \cdot h_2^{-1} = h_1 \cdot h_3 \cdot k_1 \cdot k_2^{-1}.$$

Since H, K are subgroups, $h_1 \cdot h_3 \in H$ and $k_1 \cdot k_2^{-1} \in K$. In particular, $h_1 \cdot h_3 \cdot k_1 \cdot k_2^{-1} \in HK$ and so $h_1 \cdot k_1 \cdot (h_2 \cdot k_2)^{-1} \in HK$. It now follows that HK is a subgroup by Exercise 1.5.

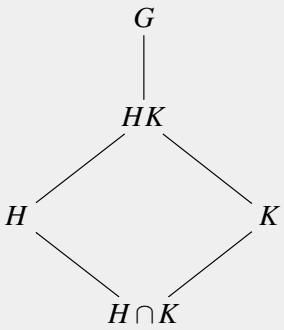
For (b), by Exercise 1.5 (-i), we know that $H \cap K$ is a subgroup of G and so we need only verify that it is normal. For that, given $h \in H \cap K$ and $k \in K$, we must prove that $k^{-1} \cdot h \cdot k \in H \cap K$. Since H is normal in G and $h \in H$, it follows that $k^{-1} \cdot h \cdot k \in H$. Since K is a subgroup of G and $h, k \in K$, it follows that $k^{-1} \cdot h \cdot k \in K$. Thus, $k^{-1} \cdot h \cdot k \in H \cap K$.

For (c), we will construct an isomorphism $\psi \colon K/(H \cap K) \to HK/H$. By definition of HK, $K \leq HK$. Taking $\psi_H \colon HK \to HK/H$ to be the canonical homomorphism, by Lemma 1.2, the restriction of ψ_H to K is a homomorphism. Since $\ker \psi_H = H$, the kernel of the restriction of ψ_H to K is $H \cap K$. By Theorem 1.3, it follows that $\psi_H(K)$ is isomorphic to $K/(H \cap K)$. It remains to show that the restriction of ψ_H to K is surjective. For that, given $kH \in HK/H$, we must find $k_1 \in K$ such that $\psi_H(k_1) = kH$. First, we can write $k = h_1 \cdot k_1$ for $h_1 \in H$ and $k_1 \in K$. Since H is normal, we know that $k_1 H = H k_1$ and so $h_1 \cdot k_1 = k_1 \cdot h_2$ for some $h_2 \in H$. In particular, we see that $k = k_1 \cdot h_2$ and so $k \cdot k_1^{-1} \in H$. Hence, $kH = k_1 H$ by Exercise 1.6. By definition of ψ_H, we have $\psi_H(k_1) = k_1 H = kH$. Therefore, $\psi_H(K) = HK/H$ and so $K/(H \cap K)$ and HK/H are isomorphic. ♠

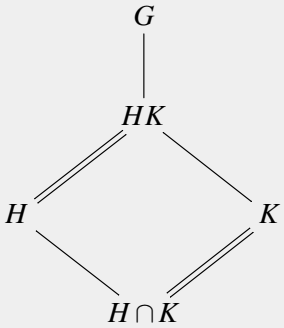
When $H \leq G$, it is common to associate to G, H a diagram



We have the following "diamond" associated to the Second Isomorphism Theorem:



By (c) in Theorem 1.5 the opposite sides of the diamond



are the "same". Theorem 1.5 is also sometimes called the diamond isomorphism theorem.

The following result is often referred to as the **Third Isomorphism Theorem**. It is essentially a conglomerate of observations about the subgroup group structure of G and the subgroup structure of the quotient group G/H for $H \lhd G$. The most note worth of these results is (e).

***Theorem* 1.6** (Third Isomorphism Theorem)**.** *Let G be a group and $H \lhd G$.*

(a) If $K \leq G$ and $H \subseteq K \subseteq G$, then K/H is a subgroup of G/H.

(b) Every subgroup of G/H is of the form K/H, for some $K \leq G$ such that $H \subseteq K \subseteq G$.

(c) If $K \lhd G$ and $H \subseteq K \subseteq G$, then K/H is a normal subgroup of G/H.

(d) Every normal subgroup of G/H is of the form K/H, for some $K \lhd G$ such that $H \subseteq K \subseteq G$.

(e) If $K \lhd G$ and $H \subseteq K \subseteq G$, then the groups $(G/H)/(K/H)$ and G/K are isomorphic.

Proof. For (a), we can restrict the canonical homomorphism $\psi_H \colon G \to G/H$ to K. The image $\psi_H(K) = K/H$ and by Lemma 1.2, $\psi_H(K) \leq G/H$.

For (b), given a subgroup $L \leq G/H$, we assert that the pullback $\psi_H^{-1}(L)$ of L is a subgroup of G. Recall,

$$\psi_H^{-1}(L) \stackrel{\text{def}}{=} \{g \in G \ : \ \psi_H(g) \in L\}.$$

Since L is s subgroup, $e_{G/H} \in L$. As $\psi_H(e_G) = e_{G/H}$, we see that $e_G \in \psi_H^{-1}(L)$. Given $g_1, g_2 \in \psi_H^{-1}(L)$, there exist $\ell_1, \ell_2 \in L$ such that $\psi_H(g_1) = \ell_1$ and $\psi_H(g_2) = \ell_2$. Since L is a subgroup of G/H, by Exercise 1.5, we have $\ell_1 \cdot \ell_2^{-1} \in L$. Additionally, we have

$$\psi_H(g_1 \cdot g_2^{-1}) = \psi_H(g_1) \cdot (\psi_H(g_2))^{-1} = \ell_1 \cdot \ell_2^{-1} \in L.$$

Hence $g_1 \cdot g_2^{-1} \in \psi_H^{-1}(L)$ and so by Exercise 1.5, $\psi_H^{-1}(L)$ is a subgroup of G. By definition, $\psi_H(\psi_H^{-1}(L)) = L = \psi_H^{-1}(L)/H$, as needed to verify (b).

For (c), given $kH \in K/H$ and $g \in G/H$, we must show that $(gH)^{-1} \cdot kH \cdot gH \in K/H$. Since K is normal, we know that $g^{-1} \cdot k \cdot g = k_1 \in K$. As $\psi_H(k) = kH$ and $\psi_H(g) = gH$, we see that

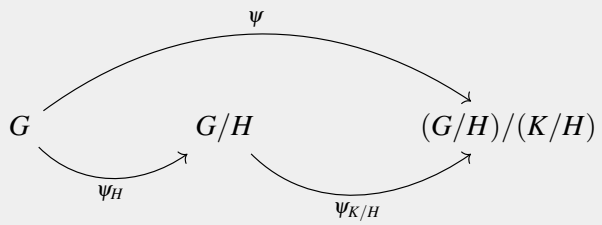
$$(gH)^{-1} \cdot kH \cdot gH = (\psi_H(g))^{-1} \cdot \psi_H(k) \cdot \psi_H(g) = \psi_H(g^{-1} \cdot k \cdot g) = \psi_H(k_1) \in K/H.$$

For (d), given $L \lhd G/H$, we assert that $\psi_H^{-1}(L) \lhd G$. Given $g_0 \in \psi_H^{-1}(L)$ and $g \in G$, we must prove that $g^{-1} \cdot g_0 \cdot g \in \psi_H^{-1}(L)$. First, since $g_0 \in \psi_H^{-1}(L)$, there exists $\ell_0 \in L$ such that $\psi_H(g_0) = \ell_0$. Now, we have

$$\psi_H(g^{-1} \cdot g_0 \cdot g) = (\psi_H(g))^{-1} \cdot \ell_0 (\psi_H(g)) \in L$$

since L is normal. Hence, $g^{-1} \cdot g_0 \cdot g \in \psi_H^{-1}(L)$. As in (b), we have $\psi_H(\psi_H^{-1}(L)) = L = \psi_H^{-1}(L)/H$.

For (e), we have



where $\psi = \psi_{K/H} \circ \psi_H$. By Theorem 1.3, we know that $\psi(G)$ and $G/\ker\psi$ are isomorphic. Since both ψ_H and $\psi_{K/H}$ are surjective, it follows that ψ is surjective. In particular, $\psi(G) = (G/H)/(K/H)$. Given $g \in \ker\psi$, since $\ker\psi_{K/H} = K/H$, we must have $\psi_H(g) = \ker\psi_{K/H} = K/H$. Therefore, $g \in \psi_H^{-1}(K/H) = K$. Hence, $\ker\psi = K$, as needed. ♠

It is customary to suppress even further our notation for the group operation $\cdot$ in a group G with group structure $(\cdot, e)$. Specifically, if G is a group and $g_1, g_2 \in G$, we will write $g_1 g_2 = g_1 \cdot g_2$.

It seems to be popular to point out one aesthetically appealing (notationally) view of (e) as an analog of fractional cancellation. Specifically, if we write $G/H = \frac{G}{H}$, then (e) of Theorem 1.6 asserts that

$$\frac{\frac{G}{H}}{\frac{K}{H}} \cong \frac{G}{K}.$$

1.1.1 *Supplemental Material: Special Subgroups.*⋆

Given a group G, we have a number of special subgroups of G. Before describing some of these subgroups, we require some terminology and notation. Given $g_1, g_2 \in G$, we define the **commutator** of g_1, g_2 to be

$$[g_1, g_2] \stackrel{\text{def}}{=} g_1^{-1} g_2^{-1} g_1 g_2.$$

We say that g_1, g_2 **commute** if $[g_1, g_2] = e$.

Exercise **1.8.** *Let $g_1, g_2 \in G$.*

(i) Prove that $[g_2, g_1] = [g_1, g_2]^{-1}$. In particular, $[g_1, g_2] = e$ if and only if $[g_2, g_1] = e$.

(ii) Prove that $g_1 g_2 = g_2 g_1$ if and only if $[g_1, g_2] = e$.

The **center** of G is defined to be the subgroup

$$Z(G) = \{g_0 \in G \,:\, [g, g_0] = e \text{ for all } g \in G\}.$$

Exercise **1.9.** *Let G be a group.*

(i) Prove that $Z(G)$ is a subgroup of G.

(ii) Prove that $Z(G)$ is normal in G.

Given an element $g \in G$, we define the **centralizer** of g in G to be the subgroup

$$C_G(g) = \{g_0 \in G \,:\, [g, g_0] = e\}.$$

Exercise **1.10.** *Prove that $C_G(g)$ is a subgroup of G and that $g \in C_G(g)$.*

Given a subgroup $H \leq G$, we define the **centralizer** of H in G to be the subgroup

$$C_G(H) = \{g_0 \in G \,:\, [h, g_0] = e \text{ for all } h \in H\}.$$

We define the **normalizer** of H in G to be the subgroup

$$N_G(H) = \left\{g_0 \in G \,:\, g_0^{-1} H g_0 \subseteq H\right\}.$$

Exercise **1.11.** *Let G be a group and $H \leq G$.*

(i) Prove that $N_G(H)$ and $C_G(H)$ are subgroups of G.

(ii) Prove that $H \leq N_G(H)$.

(iii) Prove that H is normal in $N_G(H)$.

(iv) Prove that if $H \lhd K \leq G$ for some subgroup K of G, then $K \leq N_G(H)$.

(v) Prove that $C_G(H) \leq N_G(H)$.

(vi) Prove that $C_G(H)$ is normal in $N_G(H)$.

Remark **1.7.** *Note that H need not be contained in $C_G(H)$ nor contain $C_G(H)$.*

Given any element $g \in G$, the subgroup generated by $\{g\}$ is called the **cyclic subgroup** generated by g and is denoted by $\langle g \rangle$.

Exercise **1.12.** *Prove that if $g_0 \in \langle g \rangle$, then there exists $n \in \mathbf{Z}$ such that $g_0 = g^n$.*

Given a subgroup $H \leq G$ and $g \in G$, the conjugate of H by g is the subgroup $g^{-1}Hg$. We say a pair of subgroups H, K are **conjugate** in G if there exists $g \in G$ such that $g^{-1}Hg = K$. We say a pair of elements $g_1, g_2 \in G$ are conjugate in G if there exists $g \in G$ such that $g_2 = g^{-1}g_1 g$. The **conjugacy class** of g_0 in G is defined to be

$$[g_0]_G \stackrel{\text{def}}{=} \left\{g^{-1} g_0 g \,:\, g \in G\right\}.$$

The subset $[g_0]_G$ is typically not a subgroup of G.

Exercise 1.13. *Let G be a group.*

(i) If $g_1, g_2 \in G$, prove that either $[g_1]_G = [g_2]_G$ or $[g_1]_G \cap [g_2]_G = \emptyset$.

(ii) Prove that $[g_1]_G = [g_2]_G$ if and only if g_1, g_2 are conjugate in G.

(iii) Prove that G is a disjoint union of all of the distinct conjugacy classes in G. [Hint: Use (i)]

We have two descending families of normal subgroups that will be required later in this text. Both are defined recursively and make use of commutators. Given a pair of subgroups $H, K \leq G$, the subgroup generated by the set

$$\{[h,k] \ : \ h \in H, \ k \in K\}$$

will be denoted by $[H,K]$. The subgroup $[G,G]$ is called the **commutator subgroup** of G.

Exercise 1.14. *Prove that $[G,G]$ is a normal subgroup of G.*

The **lower central series** of G is the collection of subgroups $\{G_i\}_{i=0}^{\infty}$ defined as follows. We define $G_0 = G$ and $G_i = [G, G_{i-1}]$.

Exercise 1.15. *Let G be a group.*

(i) Prove that G_i is normal in G for all $i \geq 0$.

(ii) Prove that $G_{i+1} \subseteq G_i$ for all $i \geq 0$.

The **derived series** of G is the collection of subgroups $\left\{G^i\right\}_{i=0}^{\infty}$ defined as follows. We define $G^0 = G$ and $G^i = [G^{i-1}, G^{i-1}]$.

Exercise 1.16. *Let G be a group.*

(i) Prove that G^i is normal in G for all $i \geq 0$.

(ii) Prove that $G^{i+1} \subseteq G^i$ for all $i \geq 0$.

(iii) Prove that $G^i \subseteq G_i$ for all $i \geq 0$.

(iv) Prove that $G^1 = G_1$; there are groups G where $G^i \neq G_i$ for $i \geq 2$.

We conclude this supplemental section with an exercise of indices.

Exercise 1.17. *Let G be a group; the reader can assume that G is finite. Prove the following:*

(i) *If $H \leq K \leq G$, then $[G:H] = [G:K][K:H]$.*

(ii) *If $H \leq G$, then*

$$\frac{|G|}{|H|} = [G:H].$$

*This is sometimes referred to as **Lagrange's Theorem**.*

(iii) *If $H, K \leq G$, then $H \cap K \leq G$.*

(iv) *If $H, K \leq G$, then $[G : H \cap K] \leq [G:H][G:K]$.*

(v) *If $H \lhd G$ and $K \leq G$, then $[HK:H] = [K : H \cap K]$.*

1.1.2 *Supplemental Material: Special Groups.*⋆

We say that a group G is **abelian** if $[G,G] = e$.

Exercise 1.18. *Prove that G is abelian if and only if every pair $g, g' \in G$ commute.*

One sometimes refers to abelian groups as commutative groups; the name abelian is in honor of the mathematician **Abel**.

Exercise 1.19. *Let G be an abelian group.*

(i) *Prove that if $H \leq G$, then $H \lhd G$. That is, every subgroup of an abelian group is normal.*

(ii) *Prove that if $\psi\colon G \to G'$ is a group homomorphism then $\psi(G)$ is an abelian subgroup of G'.*

(iii) *Prove that if $H \leq G$, then G/H is abelian and H is abelian. That is, subgroups and quotients of abelian groups are also abelian.*

We say that a non-trivial group G is **nilpotent** if $G_i = \{e\}$ for some $i \geq 1$. Since $G_{i+1} \subseteq G_i$, if $G_i = \{e\}$ for some i, then there exists a smallest $j_G \in \mathbf{N}$ for which $G_{j_G} = \{e\}$. The integer j_G is called the **step size** and one says G is a nilpotent group of step size j_G.

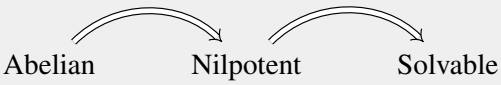
Exercise 1.20. *Prove that abelian groups are precisely the nilpotent groups of step size 1.*

We say that a non-trivial group G is **solvable** if $G^i = \{e\}$ for some $i \geq 1$. Since $G^{i+1} \subseteq G^i$, if $G^i = \{e\}$ for some i, then there exists a smallest $j^G \in \mathbf{N}$ for which $G^{j^G} = \{e\}$. The integer j^G is called the **step size** and one says G is a solvable group of step size j^G.

Exercise 1.21. *Prove that abelian groups are precisely the solvable groups of step size 1.*

Exercise 1.22. *Prove that if G is nilpotent of step size j_G, then G is solvable of step size j^G and $j^G \leq j_G$.*

In particular, we have



Any group G such that $G = \langle g \rangle$ for some $g \in G$ is called a **cyclic group**. If G is a finite cyclic group and $|G| = n$, we will denote such a group by C_n and call this group the cyclic group of order n.

Exercise 1.23. *Prove that cyclic groups are abelian. Prove that if G_1, G_2 are finite cyclic groups and $|G_1| = |G_2|$, then G_1, G_2 are isomorphic.*

Exercise 1.24. *Let G be a group.*

(i) Prove that G/G_j is nilpotent of step size at least j.

(ii) Prove that G/G^j is solvable of step size at least j.

(iii) Prove that if $\psi\colon G \to A$ is a homomorphism of groups and A is an abelian group, then $[G,G] \leq \ker \psi$.

(iv) Prove that if $\psi\colon G \to A$ is a surjective homomorphism of groups and A is an abelian group, then there exists a surjective homomorphism $\varphi_A\colon G/[G,G] \to A$ such that $\psi = \varphi \circ \psi_{[G,G]}$ where $\psi_{[G,G]}\colon G \to G/[G,G]$ is the canonical homomorphism.

Given a set I and a collection of groups $\{G_\alpha\}_{\alpha \in I}$, the **direct product** $\prod_{\alpha \in I} G_\alpha$ is the group with underlying set $\prod_{\alpha \in I} G_\alpha$ with group structure $e = (e_\alpha)_{\alpha_\in I}$ and multiplication operation

$$(g_\alpha)_{\alpha \in I} \cdot (g'_\alpha)_{\alpha \in I} \stackrel{\text{def}}{=} (g_\alpha g'_\alpha)_{\alpha \in I}.$$

Exercise 1.25. *Let I be a set and $\{G_\alpha\}_{\alpha \in I}$ be a collection of groups. Prove the following statements:*

(i) *If each G_α is abelian, then $\prod_\alpha G_\alpha$ is abelian.*

(ii) *If each G_α is nilpotent of step size at most j, then $\prod_\alpha G_\alpha$ is nilpotent of step size at most j*

(iii) *If each G_α is solvable of step size at most j, then $\prod_\alpha G_\alpha$ is solvable of step size at most j.*

(iv) *If I is finite and each G_α is finite, then $\prod_\alpha G_\alpha$ is finite and*

$$\left|\prod_\alpha G_\alpha\right| = \prod_\alpha |G_\alpha|\,.$$

Exercise 1.26. *Let G be a group and $H \leq G$ a subgroup.*

(i) *Prove that if G is nilpotent of step size j, then H is nilpotent of step size at most j.*

(ii) *Use (i) to prove that if G is abelian, then H is abelian.*

(iii) *Prove that if G is solvable of step size j, then H is solvable of step size at most j.*

(iv) *Prove that if G is cyclic, then H is cyclic.*

Exercise 1.27. *Let G be a group and $(\mathbf{Z},+,0)$ a group under addition. For each $g \in G$, define $\psi_g \colon \mathbf{Z} \to G$ by $\psi(n) = g^n$ where*

$$g^n \stackrel{def}{=} \underbrace{g \cdot g \cdot \cdots \cdot g}_{n \text{ times}}.$$

(i) *Prove that ψ_g is a homomorphism.*

(ii) *Prove that $\ker \psi_g = m_g\mathbf{Z}$ where $m_g \in \mathbf{N}$ is the smallest positive integer such that $g^{m_g} = 1_G$ and*

$$m_g\mathbf{Z} = \{m_g n \ : \ n \in \mathbf{Z}\}\,.$$

*We define the **order of** g to be m_g.*

1.2 *Groups: Actions, I*

We start this section with the concept of a group action. In some sense, group actions on sets were discovered before groups. Group actions generalize the concept of symmetries of an object/space. This is fairly evident via Exercise 1.28. As a result, the abstract concept of a group action afford groups with connections to many areas of mathematics. One can use groups (i.e. symmetries) as a tool for studying

objects/spaces. Additionally, we can use objects/spaces as a tool for studying groups. For instance, we can construct actions of groups on "well known" spaces as a method for understanding the group. One concrete example of this is the study of a group through its so-called representation theory. A representation of a group G is a homomorphism to the symmetry group of a vector space, a topic we will discuss at greater length later. These methods are central in current programs for understanding Galois groups which are symmetry groups of fields and a main topic of interest in this class.

Definition 1.10 (Group Action)**.** *Given a group G and a set X, a* ***(left) group action*** *of G on X is a function $\varphi\colon G\times X\to X$ that satisfies the following two properties:*

(a) For each $x\in X$, we have $\varphi(e,x)=x$.

(b) For each $g,h\in G$ and $x\in X$, we have $\varphi(gh,x)=\varphi(g,\varphi(h,x))$.

The following exercise is important in revealing the nature of what a group action is.

Exercise 1.28. *Let $\varphi\colon G\times X\to X$ be a group action on X and let $\mathrm{Aut}_{\mathrm{set}}(X)$ denote the set of bijection function $\lambda\colon X\to X$.*

(i) Prove that $\mathrm{Aut}_{\mathrm{set}}(X)$ is a group where the identity element is given by the function $\mathrm{Id}_X\colon X\to X$ defined by $\mathrm{Id}_X(x)=x$ and the binary operation on $\mathrm{Aut}_{\mathrm{set}}(X)$ is composition of functions.

(ii) For each $g\in G$, define the function $\varphi_g\colon X\to X$ by $\varphi_g(x)=\varphi(g,x)$. Prove that $\varphi_g\in\mathrm{Aut}_{\mathrm{set}}(X)$.

(iii) Define the function $\Phi\colon G\to\mathrm{Aut}_{\mathrm{set}}(X)$ by $\Phi(g)=\varphi_g$. Prove that Φ is a homomorphism.

The group $\mathrm{Aut}_{\mathrm{set}}(X)$ is typically referred to as the **symmetric group on the set X** and is denoted by $\mathrm{Sym}(X)$.

Exercise 1.29. *Prove that if X is finite, then $|\mathrm{Aut}_{set}(X)|=|\mathrm{Sym}(X)|=|X|!$.*

Exercise 1.30. *Prove that if $\Phi\colon G\to\mathrm{Sym}(X)$ is a homomorphism, then the function $\varphi\colon G\times X\to X$ given by $\varphi(g,x)=\Phi(g)(x)$ is a group action of G on X.*

In summary, Exercise 1.28 and Exercise 1.30 show that a group action of G on X is equivalent to a homomorphism $\Phi\colon G\to\mathrm{Sym}(X)$. Consequently, when we have a group action $\varphi\colon G\times X\to X$, we will simplify our notation and write $g\cdot x=\varphi(g,x)$. This notation is somewhat abusive and more precisely should be written as $\Phi(g)(x)=\varphi(g,x)$. However, it is extremely common to suppress the dependence on Φ so long as one is not considering several different actions of G on a fixed set X at once.

For the readers' clarity, we rewrite the definition of a group action in this simplified notation. A group action of G on X is a function $G\times X\to X$ denoted by $(g,x)\mapsto g\cdot x$ that satisfies the following properties:

(a) $e_G \cdot x = x$ for all $x \in X$ (i.e., e_G acts by the function Id_X).

(b) For each $g, h \in G$ and $x \in X$, we have $(gh) \cdot x = g \cdot (h \cdot x)$ (i.e., the group multiplication is the same as composition of functions).

We now discuss some basic examples of group actions. We start with one that we have already seen.

***Example* 1.1** (Symmetry Groups of Sets)**.** *Given a set X, the group* $\mathrm{Sym}(X)$ *of bijective functions $\lambda \colon X \to X$ acts on X. We will prove that $(\lambda, x) \mapsto \lambda(x)$ is a group action. The identity element of* $\mathrm{Sym}(X)$ *is the identity function* Id_X*. We see that* $\mathrm{Id}_X(x) = x$ *and so property (a) for a group action holds. Likewise, given $\lambda_1, \lambda_2 \in \mathrm{Sym}(X)$ and $x \in X$, we see that*

$$(\lambda_1 \lambda_2) \cdot x \stackrel{def}{=} (\lambda_1 \circ \lambda_2)(x) = \lambda_1 \cdot (\lambda_2 \cdot x).$$

Group actions play a central role in this course, albeit somewhat implicitly, and also play an important role in the study of groups. All group actions are in essence a special case of Example 1.1; that is, they are restrictions of the action of $\mathrm{Sym}(X)$ to a subgroup of $\mathrm{Sym}(X)$. Indeed, we saw above that an action of G on a set X is equivalent to having a homomorphism $\Phi \colon G \to \mathrm{Sym}(X)$. Moreover, the action of $\mathrm{Sym}(X)$ on X can be restricted to the subgroup $\Phi(G)$. For future reference, we state the following result.

***Lemma* 1.8.** *Let G be a group and $H \leq G$. If G acts on X, then H acts on X via restriction. Specifically, if $\Phi \colon G \to \mathrm{Sym}(X)$ is the homomorphism that gives rise to the action of G on X, then H acts on X via the homomorphism $\Phi_{|H} \colon H \to \mathrm{Sym}(X)$. In particular, any subgroup $\Delta \leq \mathrm{Sym}(X)$ acts on X.*

Lemma 1.8 is an immediate consequence of the fact that if $\psi \colon G \to G'$ is a homomorphism of groups and $H \leq G$, then the restriction of ψ to H is also a homomorphism of groups.

Given a G–action on a set X, we next discuss the G–action on the space of complex valued function $f \colon X \to \mathbf{C}$. It is often the case that the set X is equipped with some additional structure, like a topology, and that the action of G on X is continuous/smooth/analytic with respect to this additional structure. In this case, the G–action on the space of functions will preserve the subspace of continuous/smooth/analytic functions. For simplicity, we will only consider the case when X is a set in the following example.

***Example* 1.2** (Function Spaces)**.** *Let G be a group with an action on a set X. We define* $\mathrm{Fun}(X)$ *to be the set of function $f \colon X \to \mathbf{C}$. We can endow* $\mathrm{Fun}(X)$ *with a G–action via*

$$(g \cdot f)(x) = f(g^{-1} \cdot x) \tag{1.3}$$

where $g \in G$, $f \in \mathrm{Fun}(X)$, and $x \in X$. Equivalently, for $g \in G$, we have the function $F_g \colon X \to X$ given by $F_g(x) = g \cdot x$, and define $g \cdot f \stackrel{def}{=} f \circ F_{g^{-1}}$. We will prove that this gives a G–action on $\mathrm{Fun}(X)$ *so that*

the reader can see why the action is defined this way (i.e. why we take inverses). To see that the identity element of G acts as the identity, we have

$$(e_G \cdot f)(x) \stackrel{def}{=} f(e_G^{-1} \cdot x) = f(e_G \cdot x) = f(x).$$

Next, we check the compatibility condition, and must show that

$$((gh) \cdot f)(x) = (g \cdot (h \cdot f))(x).$$

To that end, we have

$$\begin{aligned}((gh) \cdot f)(x) &= f((gh)^{-1} \cdot x) = f((h^{-1}g^{-1}) \cdot x) \\ &= f(h^{-1} \cdot (g^{-1} \cdot x) = (h \cdot f)(g^{-1} \cdot x) = (g \cdot (h \cdot f))(x).\end{aligned}$$

The action of G on $\mathrm{Fun}(X)$ is called the ***contragradient action***.

***Remark* 1.9.** *For additional clarity, we discuss further why we must define the contragradient action as we did. If we replace (1.3) with*

$$(g \cdot f)(x) = f(g \cdot x), \tag{1.4}$$

we see that

$$((gh) \cdot f)(x) = f((gh) \cdot x) = f(g \cdot (h \cdot x)) = (g \cdot f)(h \cdot x) = (h \cdot (g \cdot f))(x).$$

In general, $(h \cdot (g \cdot f))(x) \neq (g \cdot (h \cdot f))(x)$. Hence, (1.4) does not in general satisfy (b) in Definition 1.10.

We will relate the contragradient action of G on $\mathrm{Fun}(G)$ and the left action of G on itself in the next section. This relation will further illustrate why we define the contragradient action via (1.3).

***Remark* 1.10.** *The set $\mathrm{Fun}(X)$ is a vector space over $\mathbf{C}$. Scalar multiplication and vector addition are done point-wise via*

$$(\alpha f)(x) = \alpha f(x), \quad (f_1 + f_2)(x) = f_1(x) + f_2(x)$$

where $f_1, f_2 \in \mathrm{Fun}(X)$, $x \in X$, and $\alpha \in \mathbf{C}$. If $g \in G$, we see that

$$(g \cdot (\alpha f))(x) = (\alpha f)(g^{-1} \cdot x) = (\alpha (g \cdot f))(x)$$

and

$$(g \cdot (f_1 + f_2))(x) = (f_1 + f_2)(g^{-1} \cdot x) = f_1(g^{-1} \cdot x) + f_2(g^{-1} \cdot x) = ((g \cdot f_1) + (g \cdot f_2))(x).$$

In particular, the function $T_g \colon \mathrm{Fun}(X) \to \mathrm{Fun}(X)$ define by $T_g(f) = g \cdot f = f \circ F_{g^{-1}}$ is a linear function. Let $\mathrm{Aut}_{\mathrm{vec}}(\mathrm{Fun}(X))$ be the set of bijective linear functions $T \colon \mathrm{Fun}(X) \to \mathrm{Fun}(X)$. We can endow $\mathrm{Aut}_{\mathrm{vec}}(\mathrm{Fun}(X))$ with a group structure where the identity element is the identity function and the group operation is composition of functions. The contragradient action of G on $\mathrm{Fun}(X)$ induces a group homomorphism $\Phi_{\mathrm{contra}} \colon G \to \mathrm{Aut}_{\mathrm{vec}}(\mathrm{Fun}(X))$. Specifically, $\Phi_{\mathrm{contra}}(g) = T_g$.

Exercise 1.31. *Prove that Φ_{contra} is a group homomorphism.*

We will require a certain amount of language with regard to group actions. One that we will make some use of in Galois theory is the concept of a transitive action.

Definition 1.11 (Transitive Action)**.** *Let G be a group with an action on a set X. We say that G acts **transitively** on X if for each pair $x_1, x_2 \in X$, there exists $g \in G$ such that $g \cdot x_1 = x_2$.*

One often views X as a space/universe and in this view, a transitive G–action on X is a G–action in which one can go from any point in X to any other point in X via an application of an element of G. The group $\text{Sym}(X)$ acts transitively on the set X. In fact, this action is highly transitive in the following sense. Given any subsets $S_1, S_2 \subset X$ with $|S_1| = |S_2|$, there exists $\sigma \in \text{Sym}(X)$ such that $\sigma(S_1) = S_2$. One the other hand, if we take the subgroup of $\text{Sym}(X)$ of all elements that fix $x_0 \in X$ (i.e. $\sigma(x_0) = x_0$), this subgroup of $\text{Sym}(X)$ does not act transitively on X; it does act transitively on $X - \{x_0\}$.

Exercise 1.32. *Prove that if $S_1, S_2 \subset X$ and $|S_1| = |S_2|$, then there exists $\sigma \in \text{Sym}(X)$ such that $\sigma(S_1) = \sigma(S_2)$. [Hint: First define σ to be any bijective function between S_1, S_2 and then try to extend this function to all of X.]*

Our next example is a well known one with roots in linear algebra. We will use a construction in group theory called a semi-direct product. This construction will be discussed in more detail in the next section.

Example 1.3 (Affine Group)**.** *The group $\text{Aff}(\mathbf{R}^n) \stackrel{def}{=} \mathbf{R}^n \rtimes \text{GL}(n, \mathbf{R})$ is called the **n–dimensional affine group**. It consists of pairs (v, A) where $v \in \mathbf{R}^n$ and $A \in \text{GL}(n, \mathbf{R})$; the group $\text{GL}(n, \mathbf{R})$ is comprised of the n by n matrices of non-zero determinant. Being a semi-direct product (see Remark 1.13 below for more on semi-direct products), the group operation on $\mathbf{R}^n \rtimes \text{GL}(n, \mathbf{R})$ is defined by*

$$(v, A)(w, B) = (v + Bw, AB).$$

We have a natural action of $\text{Aff}(\mathbf{R}^n)$ on $\mathbf{R}^n$ given by

$$(v, A)(w) = Aw + v.$$

This action combines two separate actions on $\mathbf{R}^n$. First, we have the action on $\mathbf{R}^n$ by $\mathbf{R}^n$ given by

$$v \cdot w \stackrel{def}{=} w + v.$$

In particular, the vector $v \in \mathbf{R}^n$ acts on $\mathbf{R}^n$ by translation by v. Second, we have the action of $\text{GL}(n, \mathbf{R})$ on $\mathbf{R}^n$ given by

$$A \cdot w \stackrel{def}{=} Aw.$$

One can view $A \in \text{GL}(n, \mathbf{R})$ as a "change of basis" for $\mathbf{R}^n$. The action of $\mathbf{R}^n$ on $\mathbf{R}^n$ is transitive whereas the action of $\text{GL}(n, \mathbf{R})$ on $\mathbf{R}^n$ is not; for the latter assertion, simply note that every $A \in \text{GL}(n, \mathbf{R})$ fixes the zero vector. The action of $\text{Aff}(\mathbf{R}^n)$ on $\mathbf{R}^n$ is transitive.

Exercise 1.33. *Prove that if $w_1, w_2, u_1, u_2 \in \mathbf{R}^2$, then there exists $\gamma = (v, A) \in \mathrm{Aff}(\mathbf{R}^2)$ such that $\gamma \cdot w_i = u_i$.*

We next define the concept of a faithful action.

Definition 1.12 (Faithful Action)**.** *Let G be a group with an action on a set X. We say that G acts **faithfully** on X if for each non-trivial $g \in G$, there exists $x \in X$ such that $g \cdot x \neq x$.*

The following lemma shows that faithful actions arise precisely from injective homomorphisms $\Phi\colon G \to \mathrm{Sym}(X)$.

Lemma 1.11. *Let G be a group with an action on a set X. Then the following are equivalent:*

(a) G acts faithfully on X.

(b) The associated homomorphism $\Phi\colon G \to \mathrm{Sym}(X)$ is injective.

We leave the proof of Lemma 1.11 as an exercise.

Exercise 1.34. *Let G be a group.*

(i) Let $\psi\colon G \to G'$ be a group homomorphism. Prove that ψ is injective if and only if $\ker \psi = \{e_G\}$.

(ii) Prove Lemma 1.11.

As a consequence of Lemma 1.11, we see that $\mathrm{Sym}(X)$ acts faithfully on X since Φ in this special setting is the identity homomorphism which is visibly injective. Whenever we have a G–action on a set X, we can always reduce to a faithful action by replacing G with the quotient group $G/\ker\Phi$.

Exercise 1.35. *Let G be a group with an action on a set X and associated homomorphism $\Phi\colon G \to \mathrm{Sym}(X)$.*

(i) Prove that $G/\ker\Phi$ acts on X by $(g\ker\Phi)(x) = g \cdot x$. That is, prove that this is a well defined group action.

(ii) Prove that the action from (i) is faithful.

If G is a group with an action on a set X, we define two basic subsets of G and X, respectively. For any subset $S \subseteq X$, we define

$$\mathrm{Stab}_G(S) = \{g \in G \ : \ g \cdot s \in S \text{ for all } s \in S\}$$

and

$$\mathcal{O}_{G,S} = \{g \cdot s \ : \ g \in G, \ s \in S\}.$$

We call $\mathrm{Stab}_G(S)$ the **stabilizer** of S and $\mathcal{O}_{G,S}$ the **orbit** of S (see also **here**).

Exercise **1.36.** *Prove that if G is a group with an action on X and $S \subseteq X$, then $\mathrm{Stab}_G(S) \leq G$.*

The concept of a free action is a strengthening of a faithful action.

Definition **1.13** (Free Action)**.** *Let G be a group with an action on a set X. We say that the action of G on X is **free** if for each $x \in X$, $\mathrm{Stab}_G(x) = \{e\}$.*

Exercise **1.37.** *Let G be a group with an action on a set X and associated homomorphism $\Phi\colon G \to \mathrm{Sym}(X)$.*

(i) Prove that $g \in \ker\Phi$ if and only if $g \in \mathrm{Stab}_G(x)$ for all $x \in X$.

(ii) Deduce that if G acts freely on X, then G acts faithfully on X.

(iii) Prove that $\mathrm{Sym}(X)$ acts freely on X if and only if $|X| \leq 2$. In particular, a faithful action need to be free.

Exercise **1.38.** *Let G be a group with an action on X with associated homomorphism $\Phi\colon G \to \mathrm{Sym}(X)$. Prove that*

$$\bigcap_{x \in X} \mathrm{Stab}_G(x) = \ker\Phi.$$

We now state a basic result for group actions that is often referred to as the **Orbit-Stabilizer Theorem**.

Theorem **1.12** (Orbit-Stabilizer Theorem)**.** *Let G be a group, X a set with a G–action, and $x \in X$.*

(a) For each $x_1, x_2 \in \mathcal{O}_x$, there exists $g_{2,1} \in G$ such that $\mathrm{Stab}_G(x_2) = g_{2,1}^{-1}\,\mathrm{Stab}_G(x_1)\,g_{2,1}$.

(b) There exists a bijective function $\lambda\colon G/\mathrm{Stab}_G(x) \to \mathcal{O}_x$.

(c) If G acts transitively on X, then there exists a bijective function $\lambda\colon G/\mathrm{Stab}_G(x) \to X$.

Proof. For (a), since $x_1, x_2 \in \mathcal{O}_x$, there exists $g_1, g_2 \in G$ such that $g_1 \cdot x = x_1$ and $g_2 \cdot x = x_2$. In particular, $g_1 g_2^{-1} \cdot x_2 = x_1$. Set $g_{2,1} = g_1 g_2^{-1}$. Given $g \in g_{2,1}^{-1}\,\mathrm{Stab}_G(x_1)\,g_{2,1}$. Then $g = g_{2,1}^{-1} g_0 g_{2,1}$ for some $g_0 \in \mathrm{Stab}_G(x_1)$. We have

$$\begin{aligned}(g_{2,1}^{-1} g_0 g_{2,1}) \cdot x_2 &= (g_{2,1}^{-1} g_0) \cdot (g_{2,1} x_2) = (g_{2,1}^{-1} g_0) \cdot x_1 \\ &= g_{2,1}^{-1} \cdot (g_0 x_1) = g_{2,1}^{-1} \cdot x_1 = x_2.\end{aligned}$$

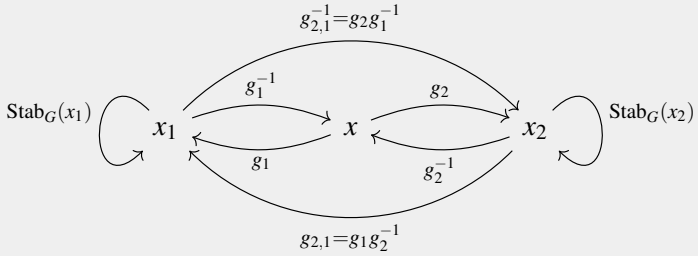
Hence, $g \in \mathrm{Stab}_G(x_2)$. Given $g \in \mathrm{Stab}_G(x_2)$, it follows that

$$g = g_{2,1}^{-1}(g_{2,1} g g_{2,1}^{-1}) g_{2,1}.$$

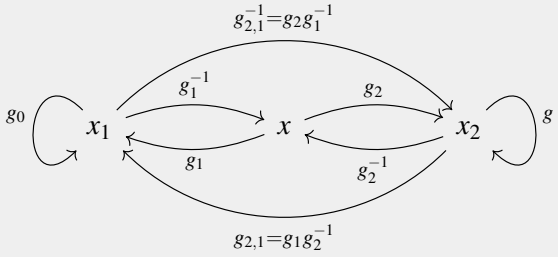
We assert that $g_{2,1} g g_{2,1}^{-1} \in \mathrm{Stab}_G(x_1)$. To see this, we have

$$\begin{aligned}(g_{2,1} g g_{2,1}^{-1}) \cdot x_1 &= (g_{2,1} g) \cdot (g_{2,1}^{-1} x_1) = (g_{2,1} g) \cdot x_2 \\ &= g_{2,1} \cdot (g \cdot x_2) = g_{2,1} \cdot x_2 = x_1.\end{aligned}$$

Setting $g_0 = g_{2,1} g g_{2,1}^{-1}$, we see that $g = g_{2,1}^{-1} g_0 g_{2,1} \in g_{2,1}^{-1} \mathrm{Stab}_G(x_1) g_{2,1}$. We summarize pictorially the process of conjugating $\mathrm{Stab}_G(x_1)$ and $\mathrm{Stab}_G(x_2)$:



In the notation of the proof of (a), we also have the diagram with specific elements in place of the stabilizers:



For (b), we define $\lambda(g\,\mathrm{Stab}_G(x)) = g \cdot x$. To show that λ is well defined, we must show that if $g' \in g\,\mathrm{Stab}_G(x)$, then $g' \cdot x = g \cdot x$. By definition, $g' = g g_0$ where $g_0 \in \mathrm{Stab}_G(x)$. In particular, $g' \cdot x = (g g_0) \cdot x = g \cdot (g_0 \cdot x) = g \cdot x$, as needed. To prove that λ is bijective, we will prove that it is both injective and surjective. If $\lambda(g\,\mathrm{Stab}_G(x)) = \lambda(g'\,\mathrm{Stab}_G(x))$, we must show that $g\,\mathrm{Stab}_G(x) = g'\,\mathrm{Stab}_G(x)$. By definition, we have

$$g \cdot x = \lambda(g\,\mathrm{Stab}_G(x)) = \lambda(g'\,\mathrm{Stab}_G(x)) = g' \cdot x.$$

In particular, $g' g^{-1} \cdot x = x$ and so $g' g^{-1} \in \mathrm{Stab}_G(x)$. Hence $g\,\mathrm{Stab}_G(x) = g'\,\mathrm{Stab}_G(x)$ by Exercise 1.6. For surjectivity, given $x' \in \mathscr{O}_x$, we must find $g\,\mathrm{Stab}_G(x) \in G/\mathrm{Stab}_G(x)$ such that $\lambda(g\,\mathrm{Stab}_G(x)) = x'$. Since $x' \in \mathscr{O}_x$, there exists $g \in G$ such that $g \cdot x = x'$. By definition of λ, we see that $\lambda(g\,\mathrm{Stab}_G(x)) = x'$.

Part (c) follows immediately from (b) as $X = \mathscr{O}_x$ for any $x \in X$ when G acts transitively. ♠

Exercise 1.39. *Let G be a group which acts on X and $x \in X$ be fixed.*

(i) Prove that the function $\lambda_x \colon G \to X$ given by $\lambda_x(g) = g \cdot x$ is a bijective function if and only if G acts freely and transitively on X.

(ii) Assume that X is finite and $H \leq \mathrm{Sym}(X)$ acts freely and transitively on the set X. Prove that H is a cyclic group and $|H| = |X|$. Deduce that $\mathrm{Sym}(X)$ is not cyclic provided $|X| \geq 3$.

Exercise 1.40. *Let G be a group and X a set with a G–action. We define an equivalence relation on X as follows. Given $x, y \in X$, we say $x \sim_G y$ if and only if there exists $g \in G$ such that $g \cdot x = y$.*

(i) Prove that $\sim_G$ is an equivalence relation on X.

(ii) Prove that the set

$$[x]_G \stackrel{def}{=} \{y \in X \ : \ x \sim_G y\}$$

is equal to $\mathscr{O}_x$.

(iii) Using the axiom of choice, prove that there exists a subset $S \subset X$ such that for each $y \in X$, there exists a unique $x \in S$ such that $x \sim_G y$.

(iv) Prove that

$$X = \bigcup_{x \in S} \mathscr{O}_x.$$

(v) Deduce that there is a bijection between X and the set

$$\bigsqcup_{x \in S} G/\mathrm{Stab}_G(x)$$

*where $\sqcup$ denotes the **disjoint union**.*

Given sets X, Y, each with a G–action, we say that a function $f \colon X \to Y$ is **G–equivariant** if for each $x \in X$ and $g \in G$, we have $f(g \cdot x) = g \cdot f(x)$. After discussing some actions of G on itself, we will see that the function in the orbit stabilizer theorem $G/\mathrm{Stab}_G(x) \to \mathscr{O}_x$ is a G–equivariant map.

1.3 *Groups: Actions, II*

In this section, we focus our attention on specific group actions of G on itself and sets associated to G. We start with an example which is not quite of this type explicitly but fits the main theme of the previous

section. In the previous section, the first "concrete" example of a group action we considered on a set X was the action of $\mathrm{Aut}_{\mathrm{set}}(X)$. That is, we considered the symmetries of X as a set. Our first example in this section will be to consider the symmetries of a group. We should, in keeping with our notation in these notes, write $\mathrm{Aut}_{\mathrm{group}}(G)$ for the group of bijective group homomorphisms $\lambda : G \to G$. However, we will instead write simply $\mathrm{Aut}(G)$; as this is the only structure on a set where we use this notation, it should not lead to any confusion. That we use this notation only for group surely incriminates the author of these notes of having a bias for groups beyond all other algebraic structures on sets. Given that most of this first chapter is not explicitly required in the sequel, this bias has already be demonstrated.

***Example* 1.4** (Automorphism Groups of Groups)**.** *Given a group G, we define $\mathrm{Aut}(G)$ to be the set of bijective group homomorphisms $\lambda : G \to G$. For future reference, we refer to a bijective group homomorphism $\psi : G \to G$ as an **automorphism**. By definition, $\mathrm{Aut}(G) \subseteq \mathrm{Sym}(X)$ and we assert that $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Sym}(X)$. To see this assertion, we must prove two basic facts. First, that Id_G is a group homomorphism. Second, if $\psi_1, \psi_2 : G \to G$ are automorphisms, then $\psi_1 \circ \psi_2^{-1}$ is an automorphism. For the first part, note that*

$$\mathrm{Id}_G(g_1 g_2) = g_1 g_2 = \mathrm{Id}_G(g_1)\mathrm{Id}_G(g_2).$$

For the second part, we will split this into two separate steps. First, if $\psi : G \to G$ is an automorphism, then $\psi^{-1} : G \to G$ is also an automorphism. Second, if $\psi_1, \psi_2 : G \to G$ are automorphisms, then $\psi_1 \circ \psi_2$ is an automorphism. For the first part, we must prove that

$$\psi^{-1}(g_1 g_2) = \psi^{-1}(g_1)\psi^{-1}(g_2).$$

By definition of the inverse function, $\psi^{-1}(g_1) = g_3$ where $g_3 \in G$ is the unique element such that $\psi(g_3) = g_1$. Likewise, $\psi^{-1}(g_2) = g_4$ where $g_4 \in G$ is the unique element such that $\psi(g_4) = g_2$. Since

$$\psi(g_3 g_4) = \psi(g_3)\psi(g_4) = g_1 g_2,$$

by definition of inverses, we see that $\psi^{-1}(g_1 g_2) = g_3 g_4$. In total, we have

$$\psi^{-1}(g_1 g_2) = g_3 g_4 = \psi^{-1}(g_3)\psi^{-1}(g_4).$$

Hence, ψ^{-1} is a group homomorphism. Since ψ^{-1} is visibly a bijective function, it follows that ψ^{-1} is an automorphism of G. For the second part, since the composition of bijective functions is a bijective function, we simply need to verify that the composition of group homomorphism is a group homomorphism. For that, we have

$$\begin{aligned}(\psi_1 \circ \psi_2)(g_1 g_2) &= \psi_1(\psi_2(g_1 g_2)) = \psi_1(\psi_2(g_1)\psi_2(g_2)) \\ &= \psi_1(\psi_2(g_1))\psi_1(\psi_2(g_2)) = (\psi_1 \circ \psi_2)(g_1)(\psi_1 \circ \psi_2)(g_2).\end{aligned}$$

*Hence, $\psi_1 \circ \psi_2$ is an automorphism. This concludes the proof that $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Sym}(G)$. We will call $\mathrm{Aut}(G)$ the **automorphism group** of G. Finally, by Lemma 1.8, $\mathrm{Aut}(G)$ acts on G.*

Remark 1.13. *Given a group G, we can form a new group that contains both G and $\mathrm{Aut}(G)$ via **semi-direct products** that utilizes the action of $\mathrm{Aut}(G)$ on G. The construction is as follows. We define $G \rtimes \mathrm{Aut}(G)$ to be the set $G \times \mathrm{Aut}(G)$ with the group structure $e = (e_G, \mathrm{Id}_G)$ and multiplication given by*

$$(g_1, \lambda_1) \cdot (g_2, \lambda_2) \stackrel{def}{=} (g_1 \lambda_1(g_2), \lambda_1 \circ \lambda_2).$$

In fact, given any homomorphism $\Phi\colon H \to \mathrm{Aut}(G)$, we can form a semi-direct product $G \rtimes_\Phi H$. The underline set is $G \times H$ and the identity element in $G \rtimes_\Phi H$ is (e_G, e_H). The multiplication operation is defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \Phi(h_1)(g_2), h_1 h_2).$$

Exercise 1.41. *Prove that $G \rtimes_\Phi H$ is a group.*

Exercise 1.42. *Let G be a group.*

(i) Prove that $\{(g, \mathrm{Id}_G) \ : \ g \in G\}$ is a subgroup of $G \rtimes \mathrm{Aut}(G)$.

(ii) Prove that G is isomorphic to the subgroup from (i).

(iii) Prove that the subgroup from (i) is normal in $G \rtimes \mathrm{Aut}(G)$.

We now turn to four fundamental actions of a group G on itself. We start with the left (right) action.

Example 1.5 (Left Action)**.** *Given a group G, we define the **left action** of G on G by $g \cdot g' = gg'$. This action is free and transitive. If $\mathbf{C}[G]$ denote the vector space with basis G, we can extend this action to $\mathbf{C}[G]$. Formally, an element $v \in \mathbf{C}[G]$ is represented as $v = \sum_{g \in G} \alpha_g g$ where $\alpha_g = 0$ for all but finitely many $g \in G$. Given $v, w \in \mathbf{C}[G]$ where $w = \sum_{g \in G} \beta_g g$, we define*

$$v + w = \sum_{g \in G} (\alpha_g + \beta_g) g$$

and

$$\lambda v = \sum_{g \in G} \lambda \alpha_g g.$$

One can check that $\mathbf{C}[G]$ is a vector space over $\mathbf{C}$. The left regular action of G on $\mathbf{C}[G]$ is given by

$$g_0 \cdot v = \sum_{g \in G} \alpha_g g_0 g.$$

This action is directly related to the contragradient action of G on $\mathrm{Fun}(G)$. Indeed, we can view $v \in \mathbf{C}[G]$ as a function $f_v\colon G \to \mathbf{C}$ where $f_v(g) = \alpha_g$. Moreover, this view gives us an injective $\mathbf{C}$–linear function $\mathbf{C}[G] \to \mathrm{Fun}(G)$ defined by $v \mapsto f_v$. Given $v \in \mathbf{C}[G]$, we know that

$$g_0 \cdot v = \sum_{g \in G} \alpha_g g_0 g.$$

Setting $w = g_0 \cdot v$ and writing $w = \sum_{g\in G} \beta_g g$, we see that $\beta_g = \alpha_{g_0^{-1}g}$. Hence,

$$f_{g_0\cdot v}(g) = f_v(g_0^{-1}g).$$

*In particular, if we view $\mathbf{C}[G]$ as a vector subspace of $\mathrm{Fun}(G)$, we see that the left action of G on $\mathbf{C}[G]$ is nothing more than the contragradient action of G on $\mathrm{Fun}(G)$ restricted to $\mathbf{C}[G]$. Additionally, we can view $\mathbf{C}[G]$ as the vector subspace of $\mathrm{Fun}(G)$ of functions with finite **support**. Recall that for $f \in \mathrm{Fun}(G)$, the support of f is defined to be the subset*

$$\mathrm{supp}(f) \stackrel{def}{=} \{g \in G \ : \ f(g) \neq 0\}.$$

*We say that f has **finite support** if $\mathrm{supp}(f)$ is finite subset of G. It is a simple matter to see that the set of functions in $\mathrm{Fun}(G)$ with finite support is isomorphic with $\mathbf{C}[G]$ and the isomorphism is G–equivariant.*

Exercise 1.43. *Prove that the linear function $\mathbf{C}[G] \to \mathrm{Fun}(G)$ given by $v \mapsto f_v$ is G–equivariant.*

Next, we have the conjugate action.

Example 1.6 (Conjugate Action)**.** *Another fundamental action of G on itself is the conjugate action. This action is defined by*

$$g_0 \cdot g \stackrel{def}{=} g_0^{-1} g g_0.$$

Unlike the left regular action, the conjugate action need not be free nor transitive. Given $g \in G$, we see that the orbit $\mathscr{O}_g$ of g under the conjugate action is $[g]_G$, the conjugacy class of G. The stabilizer of g under the conjugate action is $C_G(g)$, the centralizer of g in G. In particular, by the Orbit-Stabilizer Theorem, we see that

$$\mathscr{O}_g = \frac{|G|}{|C_G(g)|}.$$

*Assuming that G is finite, since G is a disjoint union of its conjugacy classes, we obtain the **class equation** for G:*

$$|G| = \sum_{i=1}^{r_G} \frac{|G|}{|C_G(g_i)|} \tag{1.5}$$

where $g_1, \ldots, g_{r_G}$ satisfy

$$G = \bigcup_{i=1}^{r_G} [g_i]_G, \quad [g_i]_G \cap [g_j]_G = \emptyset \text{ for } i \neq j.$$

As we can cancel $|G|$ from each side of (1.5), we obtain the following alternative form for the class equation:

$$\sum_{i=1}^{r_G} \frac{1}{|C_G(g_i)|} = 1. \tag{1.6}$$

By Exercise 1.17 (ii), we can also rewrite (1.5) as follows:

$$|G| = \sum_{i=1}^{r_G} [G : C_G(g_i)]. \tag{1.7}$$

Finally, since for each $g \in Z(G)$, we have $[g]_G = \{g\}$, we can split the elements $g_1, \ldots, g_{r_G}$ into two collections. First, after relabeling the g_i if necessary, we have $e = g_1, \ldots, g_{|Z(G)|}$, where

$$Z(G) = \left\{g_1, \ldots, g_{|Z(G)|}\right\}.$$

Then we have the remaining elements $g_{|Z(G)|+1}, \ldots, g_{r_G}$. This yields

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{r_G} [G : C_G(g_i)]. \tag{1.8}$$

Each of the equations (1.5), (1.6), (1.7), or (1.8) is sometimes referred to as the class equation for the group G. The conjugate action also provides us with a homomorphism $\mathrm{Ad}_G \colon G \to \mathrm{Aut}(G)$ where

$$\mathrm{Ad}_G(g_0)(g) = g_0^{-1} g g_0^{-1}.$$

We will refer to this as the adjoint homomorphism; this terminology is due to a specific instance of this homomorphism involving matrix groups.

Exercise 1.44. *Prove that the conjugate action of G on G is free if and only if G is the trivial group.*

Exercise 1.45. *Let G be a group.*

(i) Prove that $\ker \mathrm{Ad}_G = Z(G)$.

*(ii) Prove that $\mathrm{Ad}_G(G) \lhd \mathrm{Aut}(G)$. The normal subgroup $\mathrm{Ad}_G(G)$ is called the group of **inner automorphisms** of G. The quotient group $\mathrm{Aut}(G)/\mathrm{Ad}_G(G) \overset{def}{=} \mathrm{Out}(G)$ is called the group of outer automorphisms.*

Finally, we have the permutation action associated to a subgroup $H \leq G$.

Example 1.7 (Permutation Action: Coset Spaces)**.** *Given a group G and $H \leq G$, we have an action of G on the coset space G/H given by*

$$g_0 \cdot gH \overset{def}{=} (g_0 g)H.$$

This action is transitive but not free; it can be faithful. The stabilizer of the trivial coset $eH = H$ under this action is H. Since the action is transitive, by the Orbit-Stabilizer Theorem (i) (Theorem 1.12), we know that $\mathrm{Stab}_G(gH) = g\,\mathrm{Stab}_G(eH)g^{-1} = gHg^{-1}$. In particular, all of the stabilizers are conjugate to H. If

$\Phi_H : G \to \mathrm{Sym}(G/H)$ is the associated homomorphism, we will call Φ_H the permutation representation associated to H. We see that

$$\ker \Phi_H = \bigcap_{g \in G} gHg^{-1} \stackrel{def}{=} \mathrm{Core}_G(H).$$

*We will call $\mathrm{Core}_G(H)$ the **normal core** of H in G.*

Remark 1.14. *The bijective function given in Theorem 1.12 (ii) is G–equivariant where G acts on $G/\mathrm{Stab}_G(x)$ as in Example 1.7.*

Exercise 1.46. *Let G be a group and $H \leq G$.*

(i) Prove that $\mathrm{Core}_G(H)$ is a normal subgroup of G.

(ii) Prove that if $H_0 \lhd G$ and $H_0 \subseteq H$, then $H_0 \subseteq \mathrm{Core}_G(H)$. In particular, $\mathrm{Core}_G(H)$ is the largest normal subgroup of G that is contained in H.

(iii) Prove that

$$\overline{H} = \bigcap_{\substack{N \lhd G, \\ H \subseteq G}} N$$

*is a normal subgroup of G that contains H. This normal subgroup is called the **normal closure** (or the conjugate closure) of H in G.*

(iv) Prove that if $N \lhd G$ and $H \subseteq N$, then $\overline{H} \subseteq N$. In particular, $\overline{H}$ is the smallest normal subgroup of G that contains H.

Example 1.8 (Conjugate Action: Normal Subgroup)**.** *Given a group G and normal subgroup $H \lhd G$. Since H is normal, for each $g \in G$, we see that $\mathrm{Ad}_G(g)(H) = H$ and so we obtain $\mathrm{Ad}_{G,H} : G \to \mathrm{Aut}(H)$ given by*

$$\mathrm{Ad}_{G,H}(g)(h) \stackrel{def}{=} g^{-1}hg.$$

As in the case of the adjoint homomorphism Ad_G, one can show that $\mathrm{Ad}_{G,H}$ is a homomorphism and $\ker \mathrm{Ad}_{G,H} = C_G(H)$. If H is not necessarily normal, we can still produce an action but only with $N_G(H)$. Specifically, we have $\mathrm{Ad}_{G,H} : N_G(H) \to \mathrm{Aut}(H)$.

Exercise 1.47. *Let G be a group and $H \leq G$.*

(i) Prove that $\mathrm{Ad}_{G,H} : N_G(H) \to \mathrm{Aut}(H)$ is a homomorphism and $\ker \mathrm{Ad}_{G,H} = C_G(H)$.

(ii) Prove that $N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$.

Chapter 2

Fields: Basics

In this chapter, we introduce some more refined (i.e. less general structures) than groups. Our focus is on the concept of a field. However, we will require some basic language from ring theory first. In fact, ring theory will play a fairly prominent role in our investigation of fields. From the context of ring theory, there are two basic methods for producing fields. First and less general, when the ring is sufficiently nice (e.g. is an integral domain), there is a canonical construction of an associated field called the field of fractions. This field of fractions plays the role that the rational numbers play for the integers. A more general method for producing fields is via quotient rings via maximal ideals. Starting from the integers, we produce finite fields (i.e. field structures on finite sets). To produce the field **Q** from a quotient ring, we need to take rings that are larger than **Z**. Additionally, **Z** is not "large enough" to produce all finite fields. It turns out that rings of polynomials in a single variable with coefficients in a field are large enough to produce many associated fields to the base field of coefficients. It will take some time to develop this connection but it will be central to this chapter and the next.

2.1 *Rings: Definition and Examples*

We start our first section with the concept of a ring structure on a set.

***Definition* 2.1** (Ring)**.** *Given a set R, a **ring** structure (with identity) on R is a pair of binary operations $+, \cdot$ and elements $0_R, 1_R \in R$ such that the following properties hold:*

(a) $(R, +, 0_R)$ *is a commutative group.*

(b) *For all $r_1, r_2, r_3 \in R$, we have $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$.*

(c) *For all $r \in R$, we have $1_R \cdot r = r \cdot 1_R = r$.*

(d) *For all $r, r_1, r_2 \in R$, we have*

$$r \cdot (r_1 + r_2) = r \cdot r_1 + r \cdot r_2, \quad (r_1 + r_2) \cdot r = r_1 \cdot r + r_2 \cdot r.$$

We make two brief remarks before introducing several more basic concepts in ring theory.

Remark 2.1. *The reference to the identity in the phrase "ring structure with identity" is with regard to the element 1_R. One does not necessarily require that a ring have such an element. In such a setting, we obviously do not require (c) in Definition 2.1.*

Remark 2.2. *As with our notation for the multiplicative operation in a group structure, we will write $r_1 r_2$ instead of $r_1 \cdot r_2$ unless this more careful notation is required for clarity.*

The following exercise will be useful.

Exercise 2.1. *Let R be a ring. Prove that $0_R r = 0_R$. [Hint: consider $r(0_R + 0_R)$.]*

We now continue to introduce some basic concepts and definitions in ring theory. We resume with the concept of commutative ring. These rings will be especially important in this text.

Definition 2.2 (Commutative Ring)**.** *Given a ring R, we will say that a ring R is **commutative** if for each $r_1, r_2 \in R$, we have $r_1 r_2 = r_2 r_1$.*

Our next class of rings, integral domains, are rings which satisfy a natural cancellation property. We will see later that fields are a subclass of integral domains.

Definition 2.3 (Integral Domain)**.** *Given a commutative ring R with identity, we will say that R is an **integral domain** if $1_R \neq 0_R$ and for all $r_1, r_2, r \in R$ such that $r \neq 0_R$ and $rr_1 = rr_2$, we have $r_1 = r_2$; this is sometimes referred to as the cancellation property.*

The set of non-zero elements in a ring R with identity is, in general, not a group under multiplication since a general element in a ring need not have a multiplicative inverse. Elements which possess a multiplicative inverse form a subgroup of the R and are called units. We make this formal in our next definition.

Definition 2.4 (Unit)**.** *Given a ring R with identity, we will say that $r \in R$ is a **unit** if there exists $s \in R$ such that $rs = sr = 1_R$.*

When r is a unit in R, we also say that r is invertible. We will refer to s as a multiplicative inverse of r. The following exercise shows that the multiplicative inverse, when it exists, is unique.

Exercise 2.2. *Let R be a ring with identity and $r \in R$ a unit. Prove that if $s_1, s_2 \in R$ satisfy $rs_1 = s_1 r = 1_R$ and $rs_2 = s_2 r = 1_R$, then $s_1 = s_2$.*

Exercise 2.3. *Let R be a ring with identity. Define U_R to be the subset of R of units in R. Prove that U_R is a group under the multiplication operation on R and identity 1_R. The group U_R is sometimes referred to as the group of units. What is the group of units of $\mathbf{Z}$?*

As a consequence of Exercise 2.2, we will write r^{-1} for the multiplicative inverse of a unit $r \in R$. If R is a ring, $a, b \neq 0_R$, and $ab = 0_R$, the elements $a, b \in R$ are called **zero divisors**. Provided $0_R \neq 1_R$, if $r \in R$ is a unit, then r cannot be a zero divisor. Indeed, if $ra = 0_R$ for some $a \in R$, we see that $r^{-1}ra = a = 0_R$ be Exercise 2.1.

Example 2.1 (The Integers)**.** *The integers $\mathbf{Z}$ with the usual addition and multiplication operations and with the usual $0, 1 \in \mathbf{Z}$ are a commutative ring with identity. Moreover, $\mathbf{Z}$ is an integral domain.*

The concept of a subring is analogous to a subgroup in a group or a vector subspace in a vector space.

Definition 2.5 (Subring)**.** *Given a set R with a ring structure $(+, \cdot, 0_R, 1_R)$ and a subset $S \subseteq R$, we say that S is a **subring** the restriction of the ring structure on R to S endows S with a ring structure (not necessarily with identity). If S is a subring of R, we will write $S \leq R$.*

Definition 2.5 is rather dense and obfuscates the basic properties of a subring. As with a subgroup (see the paragraph following Exercise 1.5), a subring S of R is a subset $S \subseteq R$ which contains 0_R and is closed under multiplication and addition; if $1_R \in S$, then S is a subring with identity.

Definition 2.6 (Ring Homomorphism)**.** *Given a pair of rings R, R' and a function $\psi \colon R \to R'$, we say that ψ is a **ring homomorphism** if $\psi(1_R) = 1_{R'}$ and $\psi(r_1 r_2 + r_3 r_4) = \psi(r_1)\psi(r_2) + \psi(r_3)\psi(r_4)$ for all $r_1, r_2, r_3, r_4 \in R$.*

Ideals play the analogous role in rings that normal subgroups play in groups.

Definition 2.7 (Ideal)**.** *Let R be a commutative ring with identity. A subring $\mathfrak{a}$ of R is an **ideal** if given any $r \in R$ and $a \in \mathfrak{a}$, we have $ra \in \mathfrak{a}$. If $\mathfrak{a}$ is an ideal in R, we will write $\mathfrak{a} \lhd R$.*

In terms of the ring structure, we have binary operations

$$+ \colon R \times R \to R, \quad \cdot \colon R \times R \to R.$$

For a subset $S \subseteq R$, we denote the restriction of $+, \cdot$ to $S \times S$ by $+_S, \cdot_S$. For a general subset S, the image of $S \times S$ under $+, \cdot$ is not necessarily contained in S (i.e., S is not closed under addition or multiplication). When S is a subring, both $+(S \times S), \cdot(S \times S)$ are contained in S (i.e., S is closed under addition and multiplication). In the case of multiplication, we will refer to this as being closed under "internal" multiplication. Ideals satisfy a stronger closure condition under multiplication that we will refer to as being closed under "external" multiplication. Specifically, $\cdot(R \times \mathfrak{a}) \subseteq \mathfrak{a}$.

The following basic lemma will be useful later.

Lemma 2.3. *Let R be a commutative ring with identity and $\mathfrak{a} \lhd R$. If $r \in \mathfrak{a}$ and r is a unit, then $\mathfrak{a} = R$. In particular, if $1_R \in \mathfrak{a}$, then $\mathfrak{a} = R$.*

Proof. If $r \in \mathfrak{a}$ and r is a unit, then by definition of units, there exists $r^{-1} \in R$ such that $rr^{-1} = 1_R$. Since $\mathfrak{a}$ is closed under external multiplication, we see that $1_R \in \mathfrak{a}$. Given any $r_0 \in R$, since $r_0 1_R = r_0 \in \mathfrak{a}$, we see that $\mathfrak{a} = R$. ♠

Given a subring $S \subseteq R$, we can define a quotient space R/S as in the case of groups. We define an equivalence relation $\sim_S$ on R by $r_1 \sim_S r_2$ if and only if $r_1 - r_2 \in S$. The quotient space R/S is the set of equivalence classes $[r]_S$ under this equivalence relation $\sim_S$. Note that since R is a commutative group under addition and S is a subgroup of R (as a group under addition), the quotient space R/S is a group since $S \lhd R$ by Exercise 1.19 (i). Moreover, R/S is an abelian group by Exercise 1.19 (iii). For clarity, we describe the additive operation on the quotient space. Given $r \in R$, we denote the equivalence class $[r]_S$ by $r+S$. Note that this notation is not randomly chosen. Specifically, given $r' \in [r]_S$, by definition of $\sim_S$, we know that $r' - r \in S$ and so there exists $s_0 \in S$ such that $r' = r + s_0$. In particular, every element in $[r]_S$ is of the form $r + s_0$ for some $s_0 \in S$. Consequently,

$$[r]_S = \{r + s_0 \ : \ s_0 \in S\} = r + S.$$

Given two equivalence classes $r_1 + S, r_2 + S \in R/S$, we have the binary operation

$$+ : R/S \times R/S \to R/S$$

given by

$$+(r_1 + S, r_2 + S) = (r_1 + r_2) + S.$$

One must check that this binary operation is well defined (i.e. independent of the choice of representatives r_1, r_2). Given $r_3 \in r_1 + S$ and $r_4 \in r_2 + S$, we must show that $(r_3 + r_4) \sim_S (r_1 + r_2)$. By definition of $\sim_S$, there exists $s_1, s_2 \in S$ such that $r_3 = r_1 + s_1$ and $r_4 = r_2 + s_2$. In particular,

$$(r_3 + r_4) - (r_1 + r_2) = r_1 + s_1 + r_2 + s_2 - r_1 - r_2 = s_1 + s_2 \in S.$$

For a general subring, we cannot endow the quotient space with a commutative ring structure. Specifically, we would like to define a multiplicative operation on R/S via

$$(r_1+S)\cdot(r_2+S) \stackrel{\text{def}}{=} (r_1r_2)+S.$$

In order for this operation to be well defined, we need to prove that it is independent of our choices of r_1, r_2. Given $r_3 \in r_1+S$ and $r_4 \in r_2+S$, we need $r_3r_4 \sim_S r_1r_2$. By definition of $\sim_S$, there exist $s_1, s_2 \in S$ such that $r_3 = r_1+s_1$ and $r_4 = r_2+s_2$. In particular, we have

$$r_3r_4 = (r_1+s_1)(r_2+s_2) = r_1r_2 + s_1r_2 + s_2r_1 + s_1s_2.$$

If $r_3r_4 \sim_S r_1r_2$, we see that

$$s_1r_2 + s_2r_1 + s_1s_2 \in S.$$

This need not be the case for a general subring. However, if S is an ideal, we know that $s_1r_2, s_2r_1, s_1s_2 \in S$ and so $r_1r_2 \sim_S r_3r_4$.

Definition* 2.8** (Quotient Ring)**.** *Let R be a commutative ring with identity and $\mathfrak{a} \lhd R$. Then $R/\mathfrak{a}$ is a commutative ring and is called the* ***quotient ring *associated to $\mathfrak{a}$.*

As before, we define the index of a subring $S \subseteq R$ to be $||S|| \stackrel{\text{def}}{=} |R/S|$. Note that we have chosen different notation for the index in the setting of rings than we used in the setting of groups. We have done this for future notational reasons. Specifically, when we begin our study of fields, we will use the notation $[L:K]$ to denote the degree of the field extension. Our use of $||\cdot||$ is somewhat common, especially when one is working with ideals in rings of integers of number fields.

Given a ring R and $\mathfrak{a} \lhd R$, we have the associated quotient ring $R/\mathfrak{a}$. There is a **canonical ring homomorphism** $\psi_{\mathfrak{a}} \colon R \to R/\mathfrak{a}$ given by $\psi_{\mathfrak{a}}(r) = r+\mathfrak{a}$. Note that this homomorphism is surjective.

***Exercise* 2.4.** *For each integer $m \in \mathbf{N}$, we define $m\mathbf{Z} = \{mn \ : \ n \in \mathbf{Z}\}$.*

(i) Prove that $m\mathbf{Z}$ is an ideal in $\mathbf{Z}$.

(ii) Prove that $||m\mathbf{Z}|| = m$.

***Exercise* 2.5.** *Let R be a commutative ring with identity and $\mathfrak{a}_1, \mathfrak{a}_2 \lhd R$ be ideals.*

(i) Prove that $\mathfrak{a}_1 \cap \mathfrak{a}_2$ is an ideal.

(ii) Prove that

$$\mathfrak{a}_1 + \mathfrak{a}_2 \stackrel{def}{=} \{a_1+a_2 \ : \ a_1 \in \mathfrak{a}_1, \ a_2 \in \mathfrak{a}_2\}$$

is an ideal.

(iii) Prove that

$$\mathfrak{a}_1\mathfrak{a}_2 \stackrel{def}{=} \left\{ \sum_{i=1}^{n} a_{i,1}a_{i,2} \ : \ a_{i,1} \in \mathfrak{a}_1,\ a_{i,2} \in \mathfrak{a}_2 \text{ for all } i = 1,\ldots,n \right\}$$

is an ideal.

Lemma 2.4. *Let R, R' be commutative rings with identity and $\psi\colon R \to R'$ be a ring homomorphism. Then $\psi(R)$ is a subring (with identity) of R and $\ker\psi$ is an ideal of R where*

$$\ker\psi \stackrel{def}{=} \{r \in R \ : \ \psi(r) = 0_{R'}\}.$$

*The ideal $\ker\psi$ is called the **kernel** of ψ.*

Proof. By Lemma 1.1, we know that $\psi(R)$ is an additive subgroup of R' and so we only need to show that $\psi(R)$ is closed under internal multiplication. Note that since ψ is a ring homomorphism, $\psi(1_R) = 1_{R'}$ and so $1_{R'} \in \psi(R)$. Given $s_1, s_2 \in \psi(R)$, we must show that $s_1 s_2 \in \psi(R)$. By definition of $\psi(R)$, there exists $r_1, r_2 \in R$ such that $\psi(r_1) = s_1$ and $\psi(r_2) = s_2$. Since ψ is a ring homomorphism, we see that

$$\psi(r_1 r_2) = \psi(r_1)\psi(r_2) = s_1 s_2 \in \psi(R).$$

To prove that $\ker\psi$ is an ideal, by Lemma 1.1, we know that $\ker\psi$ is an additive subgroup of R, and so it remains to prove that $\ker\psi$ is closed under external multiplication. Given $r_0 \in \ker\psi$ and $r \in R$, by Exercise 2.1 and the fact that ψ is a ring homomorphism, we have

$$\psi(rr_0) = \psi(r)\psi(r_0) = \psi(r)0_{R'} = 0_{R'}.$$

Hence $rr_0 \in \ker\psi$ and so $\ker\psi$ is closed under external multiplication. ♠

The Isomorphism Theorems have extensions to the setting of rings. Before stating these theorems, we introduce the concept of isomorphic rings.

Definition 2.9 (Isomorphism)**.** *A ring homomorphism $\psi\colon R \to R'$ is a **ring isomorphism** if ψ is bijective. Two rings R, R' are **isomorphic** if there exists a ring isomorphism $\psi\colon R \to R'$. When R, R' are isomorphic, we will denote this by $R \cong R'$.*

Theorem 2.5 (First Ring Isomorphism Theorem)**.** *Let R, R' be commutative rings with identity and $\psi\colon R \to R'$ be a ring homomorphism. Then $\psi(R)$ is isomorphic to $R/\ker\psi$. In particular, if ψ is surjective, R' is isomorphic to $R/\ker\psi$.*

Theorem 2.6 (Second Isomorphism Theorem)**.** *Let R be a commutative ring with identity, $S \leq R$ a subring (with identity), and $\mathfrak{a} \lhd R$. Then*

(a) *The subset*

$$S+\mathfrak{a} \stackrel{def}{=} \{s+a \ : \ s \in S,\ a \in \mathfrak{a}\}$$

is a subring of R.

(b) $S \cap \mathfrak{a}$ *is an ideal in* S.

(c) *The rings* $(S+\mathfrak{a})/\mathfrak{a}$ *and* $S/(S \cap \mathfrak{a})$ *are isomorphic.*

Theorem 2.7 (Third Isomorphism Theorem)**.** *Let* R *be a commutative ring with identity and* $\mathfrak{a} \lhd R$*. Then*

(a) *If* $S \leq R$ *and* $\mathfrak{a} \subseteq S \subseteq R$*, then* $S/\mathfrak{a}$ *is a subring of* $R/\mathfrak{a}$.

(b) *Every subring of* $R/\mathfrak{a}$ *is of the form* $S/\mathfrak{a}$*, for some* $S \leq R$ *such that* $\mathfrak{a} \subseteq S \subseteq R$.

(c) *If* $\mathfrak{b} \lhd R$ *and* $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$*, then* $\mathfrak{b}/\mathfrak{a}$ *is an ideal of* $R/\mathfrak{a}$.

(d) *Every ideal of* $R/\mathfrak{a}$ *is of the form* $\mathfrak{b}/\mathfrak{a}$*, for some* $\mathfrak{b} \lhd R$ *such that* $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$.

(e) *If* $\mathfrak{b} \lhd R$ *and* $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$*, then the rings* $(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ *and* $R/\mathfrak{b}$ *are isomorphic.*

As the proofs of Theorem 2.5, Theorem 2.6, and Theorem 2.7 are quite similar to the proofs of Theorem 1.3, Theorem 1.5, and Theorem 1.6, we have omitted them from the notes.

We now return to ideals and introduce a few fundamental types of ideals. First, we say that an ideal $\mathfrak{a}$ is **proper** if $\mathfrak{a} \neq R$ and **non-trivial** if $\mathfrak{a} \neq \{0_R\}$.

Definition 2.10 (Maximal Ideal)**.** *Let* R *be a commutative ring with identity. We say an ideal* $\mathfrak{m}$ *is* ***maximal*** *if* $\mathfrak{m}$ *is proper and when* $\mathfrak{m} \lhd \mathfrak{m}_0 \lhd R$*, then* $\mathfrak{m} = \mathfrak{m}_0$ *or* $\mathfrak{m}_0 = R$.

Definition 2.11 (Prime Ideal)**.** *Let* R *be a commutative ring with identity. We say an ideal* $\mathfrak{p}$ *is* ***prime*** *if* $\mathfrak{p}$ *is proper and when* $ab \in \mathfrak{p}$*, then* $a \in \mathfrak{p}$ *or* $b \in \mathfrak{p}$.

Given a subset S of a ring R, the ideal generated by S is defined to be

$$\mathfrak{a}_S \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{n} r_i s_i \ : \ s_1, \ldots, s_n \in S,\ r_1, \ldots, r_n \right\}.$$

That is, $\mathfrak{a}_S$ is the subset of all R–linear combinations of the elements of S. If $s_1, \ldots, s_r \in R$ and $S = \{s_1, \ldots, s_r\}$, we will write $\langle s_1, \ldots, s_r \rangle = \mathfrak{a}_S$

Definition 2.12 (Finitely Generated Ideal)**.** *Let* R *be a commutative ring with identity. We say that an ideal* $\mathfrak{a}$ *is* ***finitely generated*** *if there exists a finite subset* $S \subset \mathfrak{a}$ *such that* $\mathfrak{a}_S = \mathfrak{a}$.

Definition 2.13 (Principal Ideal)**.** *Let R be a commutative ring with identity. We say an ideal $\mathfrak{a}$ is **principal** if there exists $s_0 \in \mathfrak{a}$ such that $\langle s_0 \rangle = \mathfrak{a}$. In this case, we say that s_0 is a generator for $\mathfrak{a}$.*

The following fundamental result can be proven using Zorn's Lemma. We have omitted the proof and direct the reader to **this reference** for a proof. This result is sometimes referred to as **Krull's theorem**. In the statement of the result below, a ring R is non-zero if $R \neq \{0\}$. The ring $R = \{0\}$ is often referred to as the **zero ring**.

Lemma 2.8 (Krull's Theorem: Existence of Maximal Ideals)**.** *Let R be a non-zero, commutative ring with identity. Then R has a maximal ideal. In fact, every proper ideal $\mathfrak{a}$ is contained in a maximal ideal.*

Lemma 2.9. *Let R be a commutative ring with identity. An ideal $\mathfrak{a} \lhd R$ is a prime ideal if and only if $R/\mathfrak{a}$ is an integral domain.*

We will make use of the following alternative characterization of integral domains.

Exercise 2.6. *Let R be a commutative ring with identity. Prove that R is an integral domain if and only if whenever $ab = 0$ for some $a, b \in R$, either $a = 0$ or $b = 0$.*

Proof. We first assume that $\mathfrak{a}$ is a prime ideal and prove that $R/\mathfrak{a}$ is an integral domain. If $r_1 + \mathfrak{a}, r_2 + \mathfrak{a} \in R/\mathfrak{a}$ are such that $(r_1 + \mathfrak{a})(r_2 + \mathfrak{a}) = \mathfrak{a}$, it follows that $r_1 r_2 \in \mathfrak{a}$. Since $\mathfrak{a}$ is a prime ideal, either $r_1 \in \mathfrak{a}$ or $r_2 \in \mathfrak{a}$. Hence either $r_1 + \mathfrak{a} = \mathfrak{a}$ or $r_2 + \mathfrak{a} = \mathfrak{a}$. Hence, by Exercise 2.6, $R/\mathfrak{a}$ is an integral domain.

For the converse, we will assume that $R/\mathfrak{a}$ is an integral domain and must prove that $\mathfrak{a}$ is a prime ideal. If $r_1, r_2 \in R$ and $r_1 r_2 \in \mathfrak{a}$, it follows that $(r_1 + \mathfrak{a})(r_2 + \mathfrak{a}) = \mathfrak{a}$. Since $R/\mathfrak{a}$ is an integral domain, by Exercise 2.6, either $r_1 + \mathfrak{a} = \mathfrak{a}$ or $r_2 + \mathfrak{a} = \mathfrak{a}$. In particular, either $r_1 \in \mathfrak{a}$ or $r_2 \in \mathfrak{a}$. Therefore, $\mathfrak{a}$ is a prime ideal. ♠

Exercise 2.7. *For $m \in \mathbf{N}$, let $m\mathbf{Z} \lhd \mathbf{Z}$ be the ideal generated by m.*

*(i) Prove that $m_1\mathbf{Z} + m_2\mathbf{Z} = \gcd(m_1, m_2)\mathbf{Z}$ where $\gcd(m_1, m_2)$ is the **greatest common divisor** of m_1, m_2.*

*(ii) Prove that $m_1\mathbf{Z} \cap m_2\mathbf{Z} = \operatorname{lcm}(m_1, m_2)$ where $\operatorname{lcm}(m_1, m_2)$ is the **least common multiple** of m_1, m_2.*

*(iii) Prove that $m\mathbf{Z}$ is a prime ideal if and only if m is a **prime**. [Hint: Division algorithm]*

(iv) Prove that $m\mathbf{Z}$ is a prime ideal if and only if $m\mathbf{Z}$ is a maximal ideal. [Hint: Greatest common divisors]

(v) Prove that every non-zero ideal $\mathfrak{a}$ of $\mathbf{Z}$ is principal. [Hint: Greatest common divisors]

Given a commutative ring with identity R, $r \in R$, and $n \in \mathbf{N}$, we denote by nr the element (see Exercise 1.27)

$$nr \stackrel{\text{def}}{=} \underbrace{r + r + \cdots + r}_{n \text{ times}}.$$

Definition 2.14 (Characteristic: Ring)**.** *The* ***characteristic*** *of a ring R is defined to be*

$$\operatorname{char}(R) \stackrel{def}{=} \min\{n \in \mathbf{N} \ : \ n1_R = 0_R\}$$

provided $n_0 1_R = 0_R$ for some $n_0 \in \mathbf{N}$, and $\operatorname{char}(R) = \infty$ otherwise.

Exercise 2.8. *Let R be a commutative ring with identity.*

(i) If $\operatorname{char}(R) = \infty$, prove that $\mathbf{Z}$ is a subring of R generated by 1_R.

(ii) If $\operatorname{char}(R) = m$, prove that $\mathbf{Z}/m\mathbf{Z}$ is a subring of R generated by 1_R.

Remark 2.10. *Given a subset $S \subseteq R$, the subring generated by S is the subset of all finite sums and products of elements of S. We leave it to the reader to verify that this is a subring. Note that we must allow for $-s$ to be used in any finite sum for any $s \in S$ even if $-s \notin S$. Alternatively, the ring generated by S can be defined to*

$$\bigcap_{\substack{R' \leq R, \\ S \subseteq R'}} R'.$$

That is, the intersection of all of the subrings R' of R that contains S.

Given a set I and a collection of rings $\{R_\alpha\}_{\alpha \in I}$, we define the **product ring** to be the set

$$\prod_{\alpha \in I} R_\alpha$$

with addition and multiplicative operations given coordinate-wise

$$(r_\alpha) + (s_\alpha) = (r_\alpha + s_\alpha), \quad (r_\alpha)(s_\alpha) = (r_\alpha s_\alpha)$$

and

$$0 = (0_{R_\alpha}), \quad 1 = (1_{R_\alpha}).$$

2.2 Fields: Basics and Examples

In this section, we introduce the central objects of this class called fields.

Definition 2.15 (Field)**.** *Given a set F, a **field** structure on F is a pair of binary operations $+,\cdot$ on F and a pair of (distinct) elements $0_F, 1_F \in F$ such that*

(a) $(F,+,0_F)$ *is a commutative group.*

(b) $(F-\{0_F\},\cdot,1_F)$ *is a commutative group.*

(c) For all $\alpha_1,\alpha_2,\alpha \in F$, we have

$$\alpha(\alpha_1+\alpha_2)=\alpha\alpha_1+\alpha\alpha_2.$$

Typically one denotes $F-\{0_F\}=F^\times$ and $F^\times$ is called the **group of units** of F; this is also sometimes called the **multiplicative group** of a field. A less formal description of a field is as a commutative ring with identity such that every non-zero element α is a unit.

Example 2.2. *The rational numbers $(\mathbf{Q},+,\cdot,0,1)$ with the usual addition and multiplication operations are a field. The real numbers $(\mathbf{R},+,\cdot,0,1)$ are a field. The complex numbers $(\mathbf{C},+,\cdot,0,1)$ are also a field.*

Exercise 2.9. *Let F be a commutative ring with identity. Prove that the following are equivalent:*

(i) The only two ideals in F are F and the trivial ideal $\{0_F\}$.

(ii) F is a field.

Definition 2.16 (Subfield)**.** *Given a field F, a subset $F_0 \subseteq F$ is a **subfield** of F if the binary operations $+,\cdot$ restrict to F_0 to endow F_0 with a field structure.*

The following exercise gives a concrete method for determining when a subset of a field is a subfield.

Exercise 2.10. *Let F be a field and $F_0 \subseteq F$. Then F_0 is a subfield of F if and only if F_0 $0_F, 1_F \in F_0$ and*

(i) For all $\alpha,\beta \in F$, we have $\alpha-\beta \in F_0$.

(ii) For all $\alpha,\beta \in F_0$ with $\beta \neq 0_F$, we have $\alpha\beta^{-1} \in F_0$.

It is worth unwrapping Exercise 2.10 into four separate parts. We leave the reader to check that the following four conditions are equivalent to the conditions in Exercise 2.10; we will still assume that $0_F, 1_F \in F_0$:

(1) For each $\alpha, \beta \in F_0$, we have $\alpha + \beta \in F_0$.

(2) For each $\alpha \in F_0$, we have $-\alpha \in F_0$.

(3) For each $\alpha, \beta \in F_0$, we have $\alpha\beta \in F_0$.

(4) For each $\alpha \in F_0$ with $\alpha \neq 0_F$, we have $\alpha^{-1} \in F_0$.

We note that it is necessary to assume that F_0 is closed under taking multiplicative inverses. For instance, $\mathbf{Z} \subset \mathbf{Q}$ satisfies (1), (2), and (3) but is not a subfield because the only non-zero units in $\mathbf{Z}$ are ± 1.

***Definition* 2.17** (Extension Field)**.** *Given a field E and a subfield F, we say that E is an **extension** of F and write E/F.*

Given a field F and an extension E/F, we can view E as an F–vector space. We recall the definition of an F–vector space for the reader as one is not necessarily exposed to vector spaces over general fields in a standard linear algebra class.

***Definition* 2.18** (F–vector space)**.** *Given a field F and a set V, an **F–vector space** structure on V is a binary operation $+$, a function $\cdot : F \times V \to V$, and an element 0_V such that*

(a) $(V, +, 0_V)$ is a commutative group.

(b) For each $v_1, v_2 \in V$ and $\alpha \in F$, we have

$$\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2.$$

(c) For each $\alpha_1, \alpha_2 \in F$ and $v \in V$, we have

$$\alpha_1 \cdot (\alpha_2 \cdot v) = (\alpha_1 \alpha_2) \cdot v, \quad (\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v.$$

(d) For each $v \in V$, we have $1_F \cdot v = v$.

***Exercise* 2.11.** *Let E/F be an extension of fields. Prove that E is an F–vector space.*

***Definition* 2.19** (Degree of an Extension)**.** *Given an extension of fields E/F, we define the **degree** of E/F to be*

$$\deg(E/F) = [E : F] = \dim_F E$$

*where $\dim_F E$ is the dimension of E as an F–vector space. We say that an extension is **finite** if $[E : F] < \infty$.*

We will make extensive use of basic concepts from linear algebra like linear dependence, linear independence, bases, and dimension. The reader unfamiliar with or in need of review of these concepts is referred to [2].

One of the main interests of this class is the study of extensions E/F of a field field F. We will start with some fairly elementary investigations using only linear algebra. We will see that there is a connection between certain elements in E and zeroes of polynomials with coefficients in F. Before starting this discussion, we consider a few explicit examples.

Example 2.3. *Consider $F = \mathbf{Q}$ and $E = \mathbf{Q}(\sqrt{2})$. Explicitly,*

$$\mathbf{Q}(\sqrt{2}) \stackrel{def}{=} \left\{ a + b\sqrt{2} \ : \ a,b \in \mathbf{Q} \right\}.$$

To see that $\mathbf{Q}(\sqrt{2})$ is a subfield of $\mathbf{R}$, we quickly note that if $\beta_1, \beta_2 \in \mathbf{Q}(\sqrt{2})$, one sees that $\beta_1 + \beta_2, \beta_1\beta_2 \in \mathbf{Q}(\sqrt{2})$. Likewise, if $\beta \in \mathbf{Q}(\sqrt{2})$, we see that $-\beta \in \mathbf{Q}(\sqrt{2})$. Finally, if $\beta = a + b\sqrt{2}$ and $\beta \neq 0$ we see that

$$\beta^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \left(\frac{b}{a^2-2b^2} \right) \sqrt{2} \in \mathbf{Q}(\sqrt{2}).$$

Given some $\beta = a + b\sqrt{2}$, we will assume that $b \neq 0$. We claim that β is a zero of the polynomial

$$P_\beta(t) = t^2 - 2at + (a^2 - 2b^2).$$

Note that P_β is a quadratic polynomial with rational coefficients. To see that $P_\beta(\beta) = 0$, we see that

$$\beta^2 = a^2 + 2ab\sqrt{2} + 2b^2, \quad 2a\beta = 2a^2 + 2ab\sqrt{2}.$$

Hence

$$P_\beta(\beta) = a^2 + 2ab\sqrt{2} + 2b^2 - 2a^2 - 2ab\sqrt{2} + a^2 - 2b^2 = 0.$$

Note that since $b \neq 0$, β cannot be a zero of a degree one polynomial with rational coefficients. Indeed, if $Q(t) = ct + d$ with $c,d \in \mathbf{Q}$ and $Q(\beta) = 0$, then we would have

$$Q(\beta) = ac + bc\sqrt{2} + d = 0.$$

As $c \neq 0$, we can solve for $\sqrt{2}$ and obtain

$$\sqrt{2} = -\frac{d+ac}{bc} \in \mathbf{Q}.$$

Since $\sqrt{2} \notin \mathbf{Q}$, we see that such a Q cannot exist. In summary, every $\beta \in \mathbf{Q}(\sqrt{2}) - \mathbf{Q}$ is a zero of a degree two polynomial with rational coefficients.

Example 2.4. *Let $F = \mathbf{R}$ and $E = \mathbf{C}$. Recall that*

$$\mathbf{C} = \{a + bi \ : \ a, b \in \mathbf{R}\}$$

and i satisfies $i^2 = -1$. Given $\beta = a + bi$ with $b \neq 0$, we claim that β is a zero of the quadratic polynomial

$$P_\beta(t) = t^2 - 2at + (a^2 + b^2).$$

To see this, we proceed as in the previous example. First,

$$\beta^2 = a^2 + 2abi - b^2, \quad 2a\beta = 2a^2 + 2abi.$$

Finally, we see that

$$P_\beta(\beta) = a^2 + 2abi - b^2 - 2a^2 - 2abi + a^2 + b^2 = 0.$$

It is worth mentioning that in both Example 2.3 and Example 2.4, the degree of E/F is two. That the elements in $E - F$ in these examples are zeroes of degree two polynomials with coefficient in F is directly related to $[E : F] = 2$. We now investigate the connection between elements $\beta \in E - F$ and zeroes of polynomials with coefficients in F.

Given en extension E/F and $\beta \in E - F$, consider the sets $B_n = \left\{\beta^i\right\}_{i=0}^n$. Note that the set $B_0 = \{1_F\}$ is a basis for F viewed as an F–vector space. Indeed, this is trivial since every $\alpha \in F$ can be expressed as $\alpha 1_F = \alpha$. Since $\beta \notin F$, we assert that B_1 is an F–linearly independent set. To see this, note that if B_1 were linearly dependent, there there would exists $\alpha_1, \alpha_2 \in F$ with α_1 or α_2 nonzero such that $\alpha_1 + \alpha_2\beta = 0_F$. If $\alpha_1 = 0$, since $\beta \neq 0_F$ and E is an integral domain, $\alpha_2 = 0$. Hence, we can assume $\alpha_1 \neq 0$. Likewise, if $\alpha_2 = 0$, we have $\alpha_1 = 0$, and so we can assume $\alpha_2 \neq 0$. In this case, we can solve for β and see that $\beta = -\alpha_1\alpha_2^{-1}$. Since F is a subfield of E, this would force $\beta \in F$ and so B_1 must be linearly independent. Let $n_\beta \in \mathbf{N}$ be the smallest integer such that B_n is linearly independent. It follows that $n_\beta \geq 2$.

Definition 2.20 (F–independence)**.** *Given an extension E/F of fields and $\beta \in E$, we say that β is F–**algebraically independent** if B_n is linearly independent for all $n \in \mathbf{N}$. Otherwise, we say that β is **algebraic** over F.*

Given an extension E/F of fields and $\beta \in E - F$ that is algebraic, we know that $B_1 = \{1_F, \beta\}$ is an F–linearly independent set and that for some $n_0 \in \mathbf{N}$, the set $B_{n_0} = \left\{\beta^i\right\}_{i=0}^{n_0}$ is an F–linearly dependent set. Let

$$n_\beta = \min\{n \in \mathbf{N} \ : \ B_n \text{ is } F\text{–linearly dependent}\}.$$

By definition of F–linear dependence, there exists $\alpha_0, \ldots, \alpha_{n_\beta} \in F$ such that

$$\sum_{i=0}^{n_\beta} \alpha_i \beta^i = 0. \tag{2.1}$$

Furthermore, by selection of n_β, we know that $\alpha_{n_\beta} \neq 0$. Indeed, if this were false, we would have

$$\sum_{i=0}^{n_\beta - 1} \alpha_i \beta^i = 0$$

and so $B_{n_\beta - 1}$ would be an F–linearly dependent set. Since $\alpha_{n_\beta} \neq 0$, we multiply (2.1) by $\alpha_{n_\beta}^{-1}$. Consequently, we can assume that $\alpha_{n_\beta} = 1_F$ in (2.1). Setting

$$P_\beta(t) = \sum_{i=0}^{n_\beta} \alpha_i t^i,$$

we see that $P_\beta(\beta) = 0_F$. In particular, β is a zero of a degree n_β polynomial with coefficients in F.

We will denote the **ring of F–polynomials** in an indeterminate t by $F[t]$. Recall that an F–polynomial is a function of the form

$$P(t) = \sum_{i=0}^{n} \alpha_i t^i$$

where $\alpha_0, \ldots, \alpha_n \in F$ and t is a variable. The addition and multiplication operations are the usual ones for polynomials. Specifically, if

$$Q(t) = \sum_{i=0}^{n'} \lambda_i t^i$$

then

$$P(t) + Q(t) = \sum_{i=0}^{\max\{n,n'\}} (\alpha_i + \lambda_i) t^i$$

where $\alpha_i = 0$ for all $i > n$ and $\lambda_i = 0$ for all $i > n'$. The multiplication operation is done via "**FOIL**"

$$P(t)Q(t) = \sum_{i=0}^{n} \sum_{j=0}^{n'} \alpha_i \lambda_j t^{i+j}.$$

We can rewrite this product as

$$P(t)Q(t) = \sum_{k=0}^{n+n'} \left(\sum_{\substack{i+j=k, \\ 0 \leq i \leq n, \\ 0 \leq j \leq n'}} \alpha_i \lambda_j \right) t^k.$$

Exercise **2.12.** *Let F be a field.*

(i) *Prove that $F[t]$ is a commutative ring with identity.*

(ii) *Prove that the subset of constant polynomials of $F[t]$ is a subring. Moreover, prove this set is a field and this field is isomorphic to F.*

(iii) *Prove that the group of units of $F[t]$ is $F^\times$, viewed as the group of units of the field of constant polynomials.*

We say that P has **degree** n provided $\alpha_n \neq 0$ and we say that P is **monic** if $\alpha_n = 1_F$. We will denote the degree of P by $\deg(P)$.

Exercise 2.13. *Let F be a field and $F[t]$ the ring of polynomials with coefficients in t.*

(i) *If $P,Q,R \in F[t]$, $P = QR$, and both $Q,R \neq 0_F$, prove that $\deg(P) = \deg(Q) + \deg(R)$.*

(ii) *If $P,Q,R \in F[t]$ and $P = Q + R$, prove that $\deg(P) \leq \max\{\deg(Q), \deg(R)\}$.*

From our discussion above, we can deduce the following lemma.

Lemma 2.11. *Let E/F be an extension of fields and $\beta \in E$ be algebraic over F. Then there exists a monic polynomial $P_\beta \in F[t]$ of degree n_β such that $P_\beta(\beta) = 0_F$.*

By selection of n_β, the polynomial P_β has minimal degree among the non-zero polynomials $P(t)$ with coefficients in F such that $P(\beta) = 0$. We call P_β the **minimal polynomial** for β over F.

Exercise 2.14. *Prove that if $P \in F[t]$ is a monic polynomial of degree n_β such that $P(\beta) = 0$, then $P = P_\beta$. That is, the minimal polynomial for β is the unique monic polynomial of degree n_β and with a zero at β.*

If E/F is a finite extension, then every $\beta \in E - F$ is algebraic and $n_\beta \leq [E : F]$. Consequently, we have the following immediate corollary of Lemma 2.11

Corollary 2.12. *Let E/F be a finite extension and $\beta \in E$. Then there exists a monic polynomial $P_\beta \in F[t]$ of degree $n_\beta \leq [E : F]$ such that $P_\beta(\beta) = 0_F$.*

We end this section with a basic result on finite extensions of finite extensions.

Lemma 2.13. *Let E_1/F and E_2/E_1 be extensions of fields. Then E_2/F is finite if and only if E_1/F and E_2/E_1 are finite. Moreover,*

$$[E_2 : F] = [E_2 : E_1][E_1 : F].$$

Proof. We will prove that if $\{\alpha_i\}_{i\in I}$ is a basis for E_1/F and $\{\beta_j\}_{j\in J}$ is a basis for E_2/E_1, then $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ is a basis for E_2/F where I,J are indexing sets. Given $\lambda\in E_2$, by definition of a basis, there exists a unique E_1–linear combination of the β_j that yields λ. Explicitly, we have

$$\lambda=\sum_{k=1}^{r_\lambda}\lambda_i\beta_{j_k}$$

where each $\lambda_k\in E_1$. Similarly, each λ_k can be expressed as a unique F–linear combination of the α_i. Explicitly, we have

$$\lambda_k=\sum_{\ell=1}^{s_k}\tau_{\ell,k}\alpha_{k,i_\ell}$$

where $\tau_{\ell,k}\in F$. In particular, we see that

$$\lambda=\sum_{k=1}^{r_\lambda}\sum_{\ell=1}^{s_k}\tau_{\ell,k}\alpha_{k,i_\ell}\beta_{j_k}.$$

Hence, $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ is an F–spanning set. To see that $\{\alpha_i\beta_j\}$ is an F–linearly independent set, we will assume that we have an expression of the form

$$0=\sum_{k=1}^{r}\tau_k\alpha_{i_k}\beta_{j_k} \tag{2.2}$$

where $\tau_k\in F$. For each distinct β_j that occurs, we can combine all of the terms of the form $\tau_\star\alpha_\star\beta_j$. Relabeling our indices, we can rewrite (2.2) as

$$0=\sum_{j=1}^{s}\left(\sum_{i=1}^{r_j}\tau_{i,j}\alpha_{i,j}\right)\beta_j. \tag{2.3}$$

Since the β_j are E_1–linearly independent and $\sum_{i=1}^{r_j}\tau_{i,j}\alpha_{i,j}\in E_1$, for each j, we must have

$$\sum_{i=1}^{r_j}\tau_{i,j}\alpha_{i,j}=0.$$

Since the α_i are F–linearly independent, we must have $\tau_{i,j}=0$. Hence $\{\alpha_i\beta_j\}_{(i,j)\in\times I\times J}$ is F–linearly independent. ♠

***Scholium* 2.14.** *Let E_1/F and E_2/E_1 be finite extensions and let $\{\alpha_1,\ldots,\alpha_m\}$ be an F–basis for E_1 and $\{\beta_1,\ldots,\beta_n\}$ be an E_1–basis for E_2. Then $\{\alpha_1\beta_1,\alpha_2\beta_1,\ldots,\alpha_{m-1}\beta_n,\alpha_m\beta_n\}$ is an F–basis for E_2.*

Our interest will reside primarily with the concept of an algebraic extension of F.

Definition 2.21 (Algebraic Extension)**.** *We say that an extension of fields E/F is **algebraic** if each $\beta \in E$ is algebraic over F.*

Exercise 2.15. *Prove that if E/F is a finite extension, then E/F is algebraic.*

Definition 2.22 (Transcendental Extension)**.** *We say that an extension of fields E/F is **transcendental** if E/F is not algebraic.*

Lemma 2.15. *If E/F is a transcendental extension if and only if there exists an F–algebraically independent element $\beta \in E$.*

Exercise 2.16. *Prove Lemma 2.15.*

Exercise 2.17. *Prove that if F_1, F_2 are subfields of E, then $F_1 \cap F_2$ is a subfield of E.*

Given an extension of fields E/F and a subset $S \subseteq E$, we define $F(S)$ to be the smallest subfield of E that contains F and S. We call $F(S)$ is subfield of E **generated by** S **over** F. Since

$$F(S) = \bigcap_{\substack{E_0 \leq E, \\ F \leq E_0, \\ S \subseteq E_0}} E_0,$$

by Exercise 2.17, $F(S)$ is a subfield of E. Moreover, $F(S)$ is non-empty since $F \leq E$ and $S \subseteq E$.

Definition 2.23 (Finitely Generated Extension)**.** *We say that an extension E/F is **finitely generated** if there exists a finite subset $S \subseteq F$ such that $F(S) = E$.*

Definition 2.24 (Algebraically Independent)**.** *Given an extension of fields E/F, we say that $S \subseteq E$ is **algebraically independent over** F if for each subset $S_0 \subset S$ and each $\beta \in S - S_0$, we have that β is algebraically independent over $F(S_0)$.*

Definition 2.25 (Transcendence Degree)**.** *Given an extension of fields E/F, we define the **transcendence degree** of E/F to be the maximal cardinality of an algebraically independent subset $S \subset E$.*

Exercise 2.18. *Prove that if E/F is an extension of fields and S_1, S_2 are both maximal, algebraically independent subsets of E, then $|S_1| = |S_2|$. In particular, the transcendence degree of E is well defined [Hint: Compare this result with the concept of the dimension of a vector space and why dimension is well defined]*

Exercise 2.19. *Prove that if E/F is a finitely generated extension, then the transcendence degree of E/F is finite.*

Exercise 2.20. *Prove that if E/F is an extension of fields and $\beta \in E$ is such that $P(\beta) \neq 0$ for every $P \in F[t]$, then $F(\beta)/F$ has transcendence degree 1.*

Definition 2.26 (Composite). *Given a field F and subfields F_1, F_2 of F, the **composite** of F_1, F_2, denoted F_1F_2, is the smallest subfield of F that contains both F_1, F_2.*

Exercise 2.21. *Let E be a field with subfields $E_1, E_2 \leq E$. Prove that every element $\beta \in E_1E_2$ can be expressed as a finite sum of the form*

$$\beta = \sum_{i=1}^{n} \alpha_i \lambda_i$$

where $\alpha_i \in E_1$ and $\beta_i \in E_2$.

Exercise 2.22. *Let E/F be an extension of fields with $F \leq E_1, E_2 \leq E$. Prove there exists an F–basis for $\mathscr{B}$ given as follows. Let $\mathscr{B}_1$ be an F–basis for $E_1 \cap E_2$. Let $\mathscr{B}_2$ be an $(E_1 \cap E_2)$–basis for E_1 and let $\mathscr{B}_3$ be an $(E_1 \cap E_2)$–basis for E_2. Prove that*

$$\mathscr{B} = \{uv \,:\, u \in \mathscr{B}_1,\ v \in \mathscr{B}_2\} \cup \{uw \,:\, u \in \mathscr{B}_1,\ w \in \mathscr{B}_3\}$$

is an F–basis for E_1E_2.

Exercise 2.23. *Let E/F, E_1/F, and E_2/F be an extensions such that $E_1, E_2 \leq E$ and E_1/F and E_2/F are finite.*

(i) Prove that the composite E_1E_2/F is a finite extension.

(ii) Prove that $E_1 \cap E_2$ is an extension of F.

(iii) Prove that $[E_1E_2 : E_1] = [E_2 : E_1 \cap E_2]$ and $[E_1E_2 : E_2] = [E_1 : E_1 \cap E_2]$.

(iv) Prove that $[E_1E_2 : F] = \frac{[E_1:F][E_2:F]}{[E_1 \cap E_2:F]}$.

2.2.1 *Supplemental Material: Field of Fractions.**

In this supplemental section, we will discuss how to associate to an integral domain R, a field F that is minimal with respect to containing R. The basic, guiding example to consider is when $R = \mathbf{Z}$. In this case, the associated field for $\mathbf{Z}$ is the rationals $\mathbf{Q}$. In fact, the construction of the rational numbers from the integers generalizes to general integral domains. Informally, we want

$$F = \left\{ \frac{r}{s} \,:\, r, s \in R,\ s \neq 0_R \right\}.$$

Given $\frac{r_1}{s_1}, \frac{r_2}{s_2}$, it is natural to define our addition and multiplication operations via

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} \stackrel{\text{def}}{=} \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} \stackrel{\text{def}}{=} \frac{r_1 r_2}{s_1 s_2}.$$

The additive and multiplicative identities for F are 0_R and 1_R. Unfortunately, the elements $\frac{r}{s}$ do not represent unique elements in our field F. For instance, we want

$$r \cdot \frac{1}{r} = 1_R$$

and so

$$\frac{r}{r} = 1_R$$

for all $r \in R$. Additionally, we must have

$$0_R \cdot \frac{1}{r} = 0_R$$

and so

$$\frac{0_R}{r} = 0_R$$

for all $r \in R$. This should not be a surprise to the reader given their practical knowledge of $\mathbf{Q}$ and extensive experience working with fractions. We know that two "different" fractions can represent the same rational number. For instance,

$$\frac{1}{2} = \frac{-1}{-2} = \frac{2}{4} = \frac{-2}{-4} = \frac{3}{6} = \frac{-3}{-6} = \dots$$

We will introduce an equivalence relation on fractions and define the field F to be the set of equivalence classes.

Given an integral domain R, instead of thinking of fractions $\frac{r}{s}$, we will consider pairs $(r,s) \in R \times R$. Intuitively, (r,s) represents the fraction $\frac{r}{s}$ though we will not use fraction notation in what follows. To begin, we introduce an equivalence relation on $R \times R$. Specifically, we say that $(r_1,s_1) \sim (r_2,s_2)$ if $r_1 s_2 = r_2 s_1$. We define

$$[r,s] \stackrel{\text{def}}{=} \left\{ (r',s') \in R \times R \ : \ (r,s) \sim (r',s') \right\}$$

and let F be the set of equivalence classes $[r,s]$. We endow F with a field structure by defining our addition and multiplication operations via

$$[r,s] + [r',s'] \stackrel{\text{def}}{=} [rs' + r's, ss'], \quad [r,s] \cdot [r',s'] \stackrel{\text{def}}{=} [rr', ss'].$$

We set $0_F = [0_R, 1_R]$ and $1_F = [1_R, 1_R]$. We will first prove that $+, \cdot$ are well defined. Given $(r_1,s_1) \in [r,s]$ and $(r_2,s_2) \in [r',s']$, we must prove that

$$(r_1 s_2 + r_2 s_1, s_1 s_2) \sim (rs' + r's, ss'), \quad (r_1 r_2, s_1 s_2) \sim (rr', ss').$$

For the first equivalence, we must prove that

$$ss'(r_1s_2 + r_2s_1) = s_1s_2(rs' + r's).$$

By definition of $\sim$, we know that

$$r_1s = rs_1, \quad r_2s' = r's_2. \tag{2.4}$$

Using associativity, commutativity, the distributive law, and (2.4), we have

$$\begin{aligned} ss'(r_1s_2 + r_2s_1) &= ss'r_1s_2 + ss'r_2s_1 = (r_1s)(s's_2) + (r_2s')(ss_1) \\ &= (rs_1)(s's_2) + (r's_2)(ss_1) = s_1s_2rs' + s_1s_2r's \\ &= s_1s_2(rs' + r's). \end{aligned}$$

Similarly, for the second equivalence, we must prove that

$$r_1r_2ss' = rr's_1s_2.$$

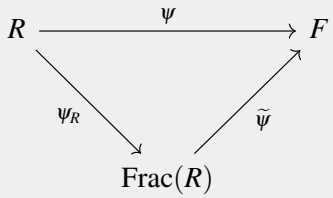
Using commutativity, the distributive law, and (2.4), we have

$$r_1r_2ss' = (r_1s)(r_2s') = (rs_1)(r's_2) = rr's_1s_2.$$

We leave it for the reader to verify that $(F, +, \cdot, 0_F, 1_F)$ satisfies all of the properties of a field.

Exercise 2.24. *Prove that $(F, +, \cdot, 0_F, 1_F)$ is a field.*

We call F the **field of fractions** of R and will denote it by $\mathrm{Frac}(R)$. We note that there is an injective ring homomorphism $\psi_R \colon R \to \mathrm{Frac}(R)$ given by $\psi_R(r) = [r, 1_R]$. Additionally, the field of fractions of R satisfies a universal mapping property. Given any injective ring homomorphism $\psi \colon R \to F$ where F is a field, there exists a unique injective field homomorphism $\widetilde{\psi} \colon \mathrm{Frac}(R) \to F$ such that for the diagram



(2.5)

we have $\psi = \widetilde{\psi} \circ \psi_R$; one often says that the diagram **commutes**.

Exercise 2.25. *Prove that if $\psi \colon R \to F$ is an injective ring homomorphism, then there exists a unique, injective field homomorphism $\widetilde{\psi} \colon \mathrm{Frac}(R) \to F$ such that (2.5) commutes.*

Aside from the basic example of $R = \mathbf{Z}$ and the associated field of fractions is $\mathbf{Q}$, we have the integral domain $F[t]$ of polynomials with coefficients in F. The associated field of fractions, which we denote by $F(t)$, is the **field of rational functions**. The elements of $F(t)$ are of the form

$$\sum_{i=1}^{m} \frac{P_i(t)}{Q_i(t)}$$

where $P_i, Q_i \in F[t]$ and each Q_i is non-zero.

Exercise 2.26. *Prove that $F(t)$ is not finitely generated over F. That is, given any finite subset S of $F(t)$, the field generated by S is a proper subfield of $F(t)$.*

Exercise 2.27. *Let R, R' be integral domains and $\psi\colon R \to R'$ an isomorphism of rings. Prove that there exists an isomorphism of fields $\widetilde{\psi}\colon \operatorname{Frac}(R) \to \operatorname{Frac}(R')$ such that the diagram*

$$\begin{array}{ccc} R & \xrightarrow{\psi} & R' \\ \downarrow{\scriptstyle \psi_R} & & \downarrow{\scriptstyle \psi_{R'}} \\ \operatorname{Frac}(R) & \xrightarrow[\widetilde{\psi}]{} & \operatorname{Frac}(R') \end{array} \tag{2.6}$$

commutes. [Hint: Exercise 2.25]

If we only insist that ψ be an injective ring homomorphism, we obtain an injective field homomorphism $\widetilde{\psi}\colon \operatorname{Frac}(R) \to \operatorname{Frac}(R')$ for which (2.6) commutes.

2.3 *Groups: Matrix Groups*

We will change our focus in this section and return to discuss groups. Our interest in this section will be in a special class of groups called linear groups or matrix groups. Given a field F and a pair of finite dimensional F–vector spaces V, W, we denote that $\operatorname{Hom}_F(V,W)$ the set of F–linear functions $L\colon V \to W$. The set $\operatorname{Hom}_F(V,W)$ can be endowed with an F–vector space structure by point-wise addition and point-wise scalar multiplication. Specifically, we have

$$(L_1 + L_2)(v) \stackrel{\text{def}}{=} L_1(v) + L_2(v), \quad (\lambda L)(v) = \lambda L(v).$$

Fixing an F–basis $\mathscr{B}_V = \{v_1, \ldots, m\}$ and $\mathscr{B}_W = \{w_1, \ldots, w_n\}$, where $m = \dim_F V$ and $n = \dim_F W$, we can associate to each $L \in \operatorname{Hom}_F(V,W)$ a matrix m by n matrix A_L with coefficients $a_{i,j}$ given by

$$L(v_j) = \sum_{j=1}^{n} a_{i,j} w_i.$$

When $V = W$, the F–vector space $\mathrm{Hom}_F(V,V)$ can also be endowed with a multiplication operation via composition of functions. Namely, $L_1 L_2 \stackrel{\text{def}}{=} L_1 \circ L_2$. One can verify that this endows $\mathrm{Hom}_F(V,V)$ with a ring with identity structure though the multiplication is not commutative unless $\dim_F V = 1$. The group of units for $\mathrm{Hom}_F(V,V)$ is precisely the subset of $L\colon V \to V$ that are bijective and will be denoted by $\mathrm{Aut}_{F-\mathrm{vec}}(V)$. Fixing a basis on V, we obtain a bijection $\mathrm{Hom}_F(V,V)$ with the set of m by m matrices with coefficients in F. Moreover, the addition, scalar multiplication, and multiplication operations on $\mathrm{Hom}_F(V,V)$ are compatible with the standard ones for m by m matrices. Note that $\mathrm{Hom}_F(V,V)$ has more structure than a typical ring and is an F–algebra with the operations of addition, F–scalar multiplication, and multiplication. For completeness, we give the definition of an F-algebra.

Definition 2.27 (F–algebra)**.** *Given a set A, an (associative) **F–algebra structure** on A is a F–vector space structure, a multiplication operation, and element $1_A \in A$ such that*

(a) For all $x,y \in A$, we have $\alpha(xy) = x(\alpha y) = (\alpha x)y$.

(b) For all $x,y,z \in A$, we have $x(yz) = (xy)z$.

(c) For all $x \in A$, we have $1_A x = x 1_A = x$.

Alternatively, A is a ring with identity, an F–vector space, and with these structures satisfying (a).

Exercise 2.28. *Let A be an F–algebra. Prove that the F–span of 1_A is a field and is isomorphic to F (as fields). Moreover, prove that it is an F–subalgebra of A (i.e. an F–linear subspace and a subring that satisfies (a), (b), and (c) in Definition 2.27). We will identity the F–span of 1_F with F and refer to it simply as $F \leq A$.*

Exercise 2.29. *Let F be a field and V be a finite dimensional F–vector space. Prove that $\mathrm{Hom}_F(V,V)$ is an F–algebra. Deduce that $\mathrm{Mat}(m,F)$, the set of m by m matrices with coefficients in F is an F–algebra with the usual matrix product and sum.*

We also will make brief use of the concept of a homomorphism of F–algebras.

Definition 2.28 (F–algebra homomorphism)**.** *Given two F–algebras A_1, A_2 and a function $\psi\colon A \to A$, we say that ψ is an **F–algebra homomorphism** if ψ is both an F–linear function and a ring homomorphism.*

We denote the F–algebra of m by m matrices with coefficients in F by $\mathrm{Mat}(m,F)$ and we denote the group of invertible elements or units by $\mathrm{GL}(m,F)$. The group $\mathrm{GL}(m,F)$ is called the **F–general linear group**. As an m by m matrix A is invertible if and only if $\det(A) \neq 0$, we see that

$$\mathrm{GL}(m,F) = \{A \in \mathrm{Mat}(m,F) \ : \ \det(A) \neq 0\}.$$

The identification of $\mathrm{Hom}_F(V,V)$ with $\mathrm{Mat}(m,F)$ afforded by fixing a basis $\mathscr{B}_V$ on V also identifies the groups $\mathrm{Aut}_{F-\mathrm{vec}}(V)$ with $\mathrm{GL}(m,F)$.

Exercise 2.30. *Let F be a field and $m \in \mathbf{N}$.*

(i) Prove that $\det\colon \mathrm{GL}(m,F) \to F^\times$ *is a homomorphism of groups.*

(ii) Let

$$\mathrm{SL}(m,F) = \{A \in \mathrm{Mat}(m,F) \ : \ \det(A) = 1\}.$$

Prove that $\mathrm{SL}(m,F)$ *is a normal subgroup of* $\mathrm{GL}(m,F)$. *The group* $\mathrm{SL}(m,F)$ *is called the* ***F–special linear group***. *[Hint: Use (i)]*

Given an extension E/F, for each $\beta \in E$, we define $L_\beta\colon E \to E$ by $L_\beta(\alpha) = \beta\alpha$. Viewing E as a 1–dimensional E vector space, the function L_β is an E–linear function.

Exercise 2.31. *Prove that* $L\colon E \to \mathrm{Hom}_E(E,E)$ *given by* $L(\beta) = L_\beta$ *is an isomorphism of F–algebras and the restriction of L to $E^\times$ gives an isomorphism of groups* $L\colon E^\times \to \mathrm{Aut}_{E\text{–}vec}(E)$.

Exercise 2.32. *Prove that* $L_\beta : E \to E$ *is an F–linear function when we view E as an F–vector space.*

By Exercise 2.32, for each $\beta \in E$, we obtain an F–linear function $L_\beta \in \mathrm{Hom}_F(E,E)$. Varying β, we obtain a function $L\colon E \to \mathrm{Hom}_F(E,E)$.

Exercise 2.33. *Prove that L is an injective F–linear function. Moreover, prove that L is a homomorphism of F–algebras.*

Example 2.5. *Let $E = \mathbf{C}$ and $F = \mathbf{R}$. We fix an $\mathbf{R}$–basis for $\mathbf{C}$, say $\{1,i\}$. Since $\mathbf{C}/\mathbf{R}$ is degree two, we can identify* $\mathrm{Hom}_{\mathbf{R}}(\mathbf{C},\mathbf{C})$ *with* $\mathrm{Mat}(2,\mathbf{R})$. *According to Exercise 2.33, we have an injective $\mathbf{R}$–linear function* $L\colon \mathbf{C} \to \mathrm{Mat}(2,\mathbf{R})$. *We now will explicitly determine this function in our basis $\{1,i\}$. To emphasize that we are working in a vector space, we will write $e_1 = 1$ and $e_2 = i$. Given $z = a+bi$, we want to write out the associated two by two real matrix for L_z. We see that*

$$L_z(e_1) = L_z(1) = z = a+bi = ae_1 + be_2$$

and

$$L_z(e_2) = L_z(i) = zi = -b+ai = -be_1 + ae_2.$$

Hence, the matrix associated to z is given by

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

In particular, we have an injective $\mathbf{R}$–linear function $L\colon \mathbf{C} \to \mathrm{Mat}(2,\mathbf{R})$ *given by*

$$L(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Recall that the ***modulus*** *of a complex number $z = a + bi$ is given by*

$$|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$$

where $\bar{z}$ is called the ***complex conjugate*** *of Z and is given by $\bar{z} = a - bi$. We see that $\det(L(z)) = |z|^2$ and so $L(\mathbf{C}^\times) \leq \mathrm{GL}(2, \mathbf{R})$. Additionally, if $|z| = 1$, we see that $\det(L(z)) = 1$. Moreover,*

$$L(z) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where $\theta = \tan^{-1}\left(\frac{b}{a}\right)$; geometrically this matrix is a clockwise rotation where the amount of rotation is θ. Notice that $L(\bar{z}) = (L(z))^T$, where $(L(z))^T$ denotes the ***transpose*** *matrix. Finally, given $z = a + bi$, we proved that z is the zero of the polynomial*

$$P_z(t) = t^2 - 2at + (a^2 + b^2).$$

Under L, we saw that

$$L(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

The ***characteristic polynomial*** *of $L(z)$ is given by*

$$c_{L(z)}(t) = \det(tI_2 - L(z)) = \det\left(\begin{pmatrix} t-a & b \\ -b & t-a \end{pmatrix}\right) = (t-a)^2 + b^2 = t^2 - 2at + a^2 + b^2.$$

In particular, $c_{L(z)}(t) = P_\beta(t)$. Moreover, by the ***Cayley–Hamilton Theorem****,*

$$c_{L(z)}(L(z)) = L(z)^2 + 2aL(z) + (a^2 + b^2)I_2 = 0_2$$

where 0_2 is the two by two zero matrix. We note also that for $z = a + bi$, we have

$$P_z(t) = t^2 - (z + \bar{z})t + z\bar{z}. \tag{2.7}$$

Exercise **2.34.** *Let $L\colon \mathbf{C} \to \mathrm{Mat}(2, \mathbf{R})$ be given as above.*

(i) Prove that if $z \in \mathbf{R}$, then

$$L(z) = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}.$$

(ii) Prove that $z, \bar{z}$ are eigenvalues for $L(z)$.

Remark **2.16.** *If $A \in \mathrm{Mat}(2, \mathbf{R})$ and λ_1, λ_2 are eigenvalues for A, then one can show that*

$$c_A(t) = t^2 - (\lambda_1 + \lambda_2)t + \lambda_1\lambda_2.$$

Given Exercise 2.34 (ii), our description of $P_z(t)$ given by (2.7) is less mysterious.

Example 2.6. *Let $E = \mathbf{Q}(\sqrt{2})$ and $F = \mathbf{Q}$. Since $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$, we can identify $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{2}))$ with $\mathrm{Mat}(2, \mathbf{Q})$. By Exercise 2.33 provides us with a $\mathbf{Q}$–linear injective function $L\colon \mathbf{Q}(\sqrt{2}) \to \mathrm{Mat}(2, \mathbf{Q})$. Fixing a $\mathbf{Q}$–basis for $\mathbf{Q}(\sqrt{2})$, say $\left\{1, \sqrt{2}\right\} = \{e_1, e_2\}$, for $z = a + b\sqrt{2}$, we see that*

$$L_z(e_1) = L_z(1) = z = ae_1 + be_2$$

and

$$L_z(e_2) = L_z(\sqrt{2}) = z\sqrt{2} = 2b + a\sqrt{2} = 2be_1 + ae_2.$$

Hence

$$L(z) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

As before, we saw that $z = a + b\sqrt{2}$ is a zero of the polynomial $P_z(t) = t^2 - 2at + (a^2 - 2b^2)$. We also have that the characteristic polynomial of $L(z)$ is given by

$$c_{L(z)}(t) = \det\left(\begin{pmatrix} t-a & -2b \\ -b & t-a \end{pmatrix}\right) = (t-a)^2 - 2b^2 = t^2 - 2at + a^2 - 2b^2.$$

In particular, $P_z(t) = c_{L(z)}(t)$. Finally, we can define a conjugation on $\mathbf{Q}(\sqrt{2})$ by

$$\bar{z} = \overline{a + b\sqrt{2}} = a - b\sqrt{2}.$$

We again see that

$$P_z(t) = t^2 - (z + \bar{z})t + z\bar{z}.$$

Given Remark 2.16, the reader should not be surprised by the fact that $z, \bar{z}$ are the eigenvalues for $L(z)$. Additionally, the reader can verify that $L(\bar{z}) = (L(z))^T$ as in the case of $\mathbf{C}/\mathbf{R}$.

Examples 2.5 and 2.6 are special cases of a more general fact. Given a finite extension E/F, the functions $L_\beta\colon E \to E$ given by $L_\beta(\alpha) = \beta\alpha$, where $\beta \in E$, are F–linear functions. This provides us with an injective F–algebra homomorphism $L\colon E \to \mathrm{Hom}_F(E, E)$. Fixing an F–basis $\{1, \beta_1, \ldots, \beta_{n-1}\}$ where $n = [E : F]$, we obtain an injective F–algebra homomorphism $L\colon E \to \mathrm{Mat}(n, F)$ with $L(E^\times) \leq \mathrm{GL}(n, F)$. For each $z \in E$, the characteristic polynomial of $c_{L(z)}$ is a monic, degree n polynomial with coefficients in F. That is, $c_{L(z)} \in F[t]$ and of the form

$$c_{L(z)}(t) = t^n + \sum_{\ell=0}^{n-1} a_\ell t^\ell.$$

By the Cayley–Hamilton Theorem, we know that $c_{L(z)}(L(z)) = 0_n$ where 0_n denotes the n by n zero matrix. Moreover, since L is an injective F–algebra homomorphism, it follows that $c_{L(z)}(z) = 0$. In particular, this gives another proof of Corollary 2.12.

Remark 2.17. *Since* $\deg(c_{L(z)}) = [E:F]$ *for every* $z \in E$*, it need not be the case that* $c_{L(z)} = P_z$*, where* P_z *is the minimal polynomial of* z *over* F*. For instance, if* $z \in F$*, then* $P_z(t) = t - z$ *while* $c_{L(z)}(t) = (t-z)^n$*. However, if* $n_z = n$ *(i.e.* $E = F(z)$*), then* $c_{L(z)}(t) = P_z(t)$*.*

Example 2.7. *Let* $E = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ *and* $F = \mathbf{Q}$*. A few words are required on precisely what* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ *is. First, we can take* E *to be the smallest subfield of* $\mathbf{R}$ *that contains both* $\sqrt{2}$ *and* $\sqrt{3}$*. The smallest subfield of* $\mathbf{R}$ *that contains* $\sqrt{2}$ *is* $\mathbf{Q}(\sqrt{2})$ *and can be described as all of the real numbers of the form* $a + b\sqrt{2}$ *where* $a, b \in \mathbf{Q}$*. Likewise, the smallest subfield of* $\mathbf{R}$ *that contains* $\sqrt{3}$ *is* $\mathbf{Q}(\sqrt{3})$ *and can be described as all of the real numbers of the form* $c + d\sqrt{3}$ *where* $c, d \in \mathbf{Q}$*. If* E *is the smallest subfield of* $\mathbf{R}$ *that contains both* $\sqrt{2}$ *and* $\sqrt{3}$*, we can instead view this as the smallest subfield of* $\mathbf{R}$ *that contains* $\sqrt{3}$ *and the subfield* $\mathbf{Q}(\sqrt{2})$*. Setting* $E_0 = \mathbf{Q}(\sqrt{2})$*, we can denote this field by* $E_0(\sqrt{3})$*. An* E_0*–basis for* $E_0(\sqrt{3})$ *is* $\{1, \sqrt{3}\}$ *and a* $\mathbf{Q}$*–basis for* E_0 *is* $\left\{1, \sqrt{2}\right\}$*. By Scholium 2.14,* $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ *is a* $\mathbf{Q}$*–basis for* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$*. Given* $z \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$*, we can write*

$$z = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}.$$

We see that

$$\begin{aligned} L_z(1) &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\ L_z(\sqrt{2}) &= 2b + a\sqrt{2} + 2d\sqrt{3} + c\sqrt{6} \\ L_z(\sqrt{3}) &= 3c + 3d\sqrt{2} + a\sqrt{3} + b\sqrt{6} \\ L_z(\sqrt{6}) &= 6d + 3c\sqrt{2} + 2b\sqrt{3} + a\sqrt{6}. \end{aligned}$$

Hence, in the basis $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$*, the* $\mathbf{Q}$*–linear function* $L(z)\colon \mathbf{Q}(\sqrt{2}, \sqrt{3}) \to \mathbf{Q}(\sqrt{2}, \sqrt{3})$ *is given by the matrix*

$$L(z) = \begin{pmatrix} a & 2b & 3c & 6d \\ b & a & 3d & 3c \\ c & 2d & a & 2b \\ d & c & b & a \end{pmatrix}.$$

We have three conjugations on the field $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ *and they are generated by two particular conjugations. One each of* $\mathbf{Q}(\sqrt{2})$ *and* $\mathbf{Q}(\sqrt{3})$*, we have*

$$\tau_1\colon a + b\sqrt{2} \longmapsto a - b\sqrt{2}, \quad \tau_2\colon c + d\sqrt{3} \longmapsto c - d\sqrt{3}.$$

Since $\sqrt{6} = \sqrt{2}\sqrt{3}$*, we see that* $\tau_1(\sqrt{6}) = \tau_2(\sqrt{6}) = -\sqrt{6}$*. We can also apply both* τ_1, τ_2 *together, which we will call* τ_3*. We see that* $\tau_3(\sqrt{2}) = -\sqrt{2}$*,* $\tau_3(\sqrt{3}) = -\sqrt{3}$*, and* $\tau_3(\sqrt{6}) = \sqrt{6}$*. Hence, we have*

$$\begin{aligned} \tau_0(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\ \tau_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ \tau_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\ \tau_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}. \end{aligned}$$

Finally, we set

$$\begin{aligned}
a_{z,0} &= \tau_0(z)\tau_1(z)\tau_2(z)\tau_3(z)\\
a_{z,1} &= \tau_0(z)\tau_1(z)\tau_2(z)+\tau_0(z)\tau_1(z)\tau_3(z)+\tau_0(z)\tau_2(z)\tau_3(z)+\tau_1(z)\tau_2(z)\tau_3(z)\\
a_{z,2} &= \tau_0(z)\tau_1(z)+\tau_0(z)\tau_2(z)+\tau_0(z)\tau_3(z)+\tau_1(z)\tau_2(z)+\tau_1(z)\tau_3(z)+\tau_2(z)\tau_3(z)\\
a_{z,3} &= \tau_0(z)+\tau_1(z)+\tau_2(z)+\tau_3(z).
\end{aligned}$$

We claim that

$$c_{L(z)}(t) = t^4 - a_{z,3}t^3 + a_{z,2}t^2 - a_{z,1}t + a_{z,0}.$$

We will not verify this claim; we cruelly leave this for the reader

Exercise 2.35. *For the problems below, we refer the reader to Example 2.7 for the notation.*

(i) Given $z \in \mathbf{Q}(\sqrt{2},\sqrt{3})$, prove that $z = \tau_1(z) = \tau_2(z) = \tau_3(z)$ if and only if $z \in \mathbf{Q}$.

(ii) Given $z \in \mathbf{Q}(\sqrt{2},\sqrt{3})$, prove that $z = \tau_1(z)$ if and only if $z \in \mathbf{Q}(\sqrt{2})$.

(iii) Given $z \in \mathbf{Q}(\sqrt{2},\sqrt{3})$, prove that $z = \tau_2(z)$ if and only if $z \in \mathbf{Q}(\sqrt{3})$.

(iv) Given $z \in \mathbf{Q}(\sqrt{2},\sqrt{3})$, prove that $z = \tau_3(z)$ if and only if $z \in \mathbf{Q}(\sqrt{6})$.

(v) Prove that $a_{z,3}, a_{z,2}, a_{z,1}, a_{z,0} \in \mathbf{Q}$. [Hint: Use (i)]

(vi) Prove that

$$c_{L(z)}(t) = t^4 - a_{z,3}t^3 + a_{z,2}t^2 - a_{z,1}t + a_{z,0}.$$

If the reader prefers something less demanding computationally, one should check that if

$$P_z(t) = t^4 - a_{z,3}t^3 + a_{z,2}t^2 - a_{z,1}t + a_{z,0},$$

then $P_z(z) = 0$. In fact, $P_z(\tau_i(z)) = 0$ for $i = 0,1,2,3$.

Exercise 2.36. *For the problems below, we refer the reader to Example 2.7 for the notation.*

(i) Prove that $\tau_i \colon E \to E$ are F–linear maps.

(ii) Prove that $\{\tau_0, \tau_1, \tau_2, \tau_3\}$ is a subgroup of $\mathrm{Hom}_F(E,E)$.

(iii) Write matrices for $\tau_0, \tau_1, \tau_2, \tau_3$ in the basis $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$.

Examples 2.5, 2.6, and 2.7 are all examples of Galois extensions; the fearful reader should note that we have yet to define this concept and will in the next chapter. In the case of $\mathbf{C}/\mathbf{R}$, complex conjugation is an example of a Galois automorphism of the extension $\mathbf{C}/\mathbf{R}$. Specifically, this is an $\mathbf{R}$–algebra automorphism $\sigma\colon \mathbf{C} \to \mathbf{C}$ such that $\sigma(x) = x$ for all $x \in \mathbf{R}$. The conjugation operation $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$ is a Galois automorphism of $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$. This is a $\mathbf{Q}$–algebra automorphism $\sigma\colon \mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{2})$ such that $\sigma(a) = a$ for all $a \in \mathbf{Q}$. Likewise, τ_1, τ_2, τ_3 are Galois automorphisms of $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$. Exercise 2.35 (i)–(iv) is part of what we will call the Galois correspondence that relates subgroups of the Galois group with subfields of the Galois extension.

2.4 *Fields/Rings: Maximal Ideals and Prime Fields*

Before discussing polynomial rings in some detail, we require a basic result on quotient rings associated to maximal ideals. We will also discuss the characteristic of a field and introduce the finite fields $\mathbf{F}_p$ of prime order p. Recall that if R is a ring and $\mathfrak{p}$ is an ideal in R, by Lemma 2.9, $\mathfrak{p}$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain. A similar characterization of maximal ideals can also be established.

***Lemma* 2.18.** *Let R be a commutative ring with identity and $\mathfrak{m} \lhd R$. Then $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.*

Proof. We first assume that $\mathfrak{m}$ is maximal. Given $r \in R - \mathfrak{m}$, we know that the ideal generated by $\mathfrak{m}$ and r is all of R. In particular, for some $r' \in R$, we just have $r'r + r'm = 1_R$. Hence, $rr' + \mathfrak{m} = 1_R + \mathfrak{m}$, and so $r + \mathfrak{m}$ is a unit in $R/\mathfrak{m}$. Thus, $R/\mathfrak{m}$ is a field.

Next, we assume $R/\mathfrak{m}$ is a field. Since every non-zero element of $R/\mathfrak{m}$ is a unit, by Lemma 2.3, it follows that $R/\mathfrak{m}$ has no non-zero, proper ideals. Hence, by the Third Isomorphism Theorem (Theorem 2.7), $\mathfrak{m}$ is maximal. ♠

Since fields are integral domains, we obtain an immediate corollary of Lemma 2.18.

***Corollary* 2.19.** *Let R be a commutative ring with identity and $\mathfrak{a} \lhd R$. If $\mathfrak{a}$ is maximal, then $\mathfrak{a}$ is prime.*

By Exercise 2.7, we know that $p\mathbf{Z}$ is a maximal ideal in $\mathbf{Z}$ if and only if p is a prime. Consequently, by Lemma 2.18, $\mathbf{Z}/p\mathbf{Z}$ is a field if and only if p is a prime. The cardinality of $\mathbf{Z}/p\mathbf{Z}$ is p and hence when p is prime, yields a finite field of cardinality p. We denote this field by $\mathbf{F}_p$.

***Exercise* 2.37.** *Prove that $\mathbf{F}_p^\times$ is a cyclic group.*

Exercise 2.38. *Let R, R' be commutative rings with identity and let $\psi\colon R \to R'$ be an isomorphism of rings.*

(i) If $\mathfrak{a} \lhd R$ is an ideal with $\mathfrak{a}' = \psi(\mathfrak{a})$, prove that there exists a ring isomorphism $\overline{\psi}\colon R/\mathfrak{a} \to R'/\mathfrak{a}'$ such that the diagram

$$\begin{array}{ccc} R & \xrightarrow{\psi} & R \\ {\scriptstyle \psi_{\mathfrak{a}}}\downarrow & & \downarrow{\scriptstyle \psi_{\mathfrak{a}'}} \\ R/\mathfrak{a} & \xrightarrow[\overline{\psi}]{} & R'/\mathfrak{a}' \end{array}$$

[Hint: Prove that $\psi_{\mathfrak{a}'} \circ \psi \circ \psi_{\mathfrak{a}}^{-1}$ is well-defined on $R/\mathfrak{a}$. That is independent of the choice of $\psi_{\mathfrak{a}}^{-1}$]

(ii) Prove that if $\mathfrak{p} \lhd R$ is a prime ideal, then $\psi(\mathfrak{p})$ is a prime ideal in R'. [Hint: Use (i) and Lemma 2.9]

(iii) Prove that if $\mathfrak{m} \lhd R$ is a maximal ideal, then $\psi(\mathfrak{m})$ is a maximal ideal in R'. [Hint: Use (i) and Lemma 2.18]

Since every field is a commutative ring with identity, we can define the characteristic of a field F by Definition 2.14.

Lemma 2.20. *Let F be a field of finite characteristic n.*

(a) If n is finite, then $n = p$ for some prime p.

(b) If F has finite characteristic p, then $F_p = \{n1_F \ : \ n \in \mathbf{N}\}$ is isomorphic to $\mathbf{F}_p$.

(c) If $F_0 \leq F$ is a subfield, then $F_p \leq F_0$.

Proof. For (a), define the function $\psi\colon \mathbf{Z} \to F$ by (see Exercise 1.27)

$$\psi(n) = n1_F \stackrel{\text{def}}{=} \underbrace{1_F + 1_F + \cdots + 1_F}_{n \text{ times}}.$$

To see that ψ is a ring homomorphism, note that $\psi(1) = 1_F$ by definition. By associativity of addition and the definition of ψ, we have

$$\begin{aligned} \psi(n+m) = (n+m)1_F &= \underbrace{(1_F + 1_F + \cdots + 1_F)}_{n+m \text{ times}} \\ &= \underbrace{(1_F + 1_F + \cdots + 1_F)}_{n \text{ times}} + \underbrace{(1_F + 1_F + \cdots + 1_F)}_{m \text{ times}} = \psi(n) + \psi(m). \end{aligned}$$

Finally, by associativity of addition, the distributive law, and the definition of ψ, we have

$$\begin{aligned}\psi(nm) = (nm)1_F &= \underbrace{(1_F + 1_F + \cdots + 1_F)}_{nm \text{ times}} \\ &= \underbrace{\underbrace{(1_F + \cdots + 1_F)}_{n \text{ times}} + \cdots + \underbrace{(1_F + \cdots + 1_F)}_{n \text{ times}}}_{m \text{ times}} \\ &= \underbrace{(1_F + \ldots 1_F)}_{n \text{ times}}\underbrace{(1_F + \ldots 1_F)}_{m \text{ times}} = \psi(n)\psi(m)\end{aligned}$$

Thus, ψ is a ring homomorphism and visibly, the kernel of ψ is $n\mathbf{Z}$. If n is not a prime, then $\psi(\mathbf{Z}) \leq F$ is not an integral domain and hence contains non-zero zero divisors. As such elements in F cannot be invertible, F would fail to be a field and so n must be a prime; see Exercise 2.39.

For (b), simply note that $\psi(\mathbf{Z}) = F_p$ and $\psi(\mathbf{Z}) \cong \mathbf{Z}/\ker\psi = \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ by the First Isomorphism Theorem for rings.

For (c), since F_0 is a subfield of F, we have $1_F \in F_0$ and so $F_p \leq F_0$. ♠

We give the following exercise which was implicitly used in the proof of Lemma 2.20 (a); specifically, that $\psi(\mathbf{Z})$ is an integral domain.

Exercise 2.39. *Let F be a field and $R \subseteq F$ a subring of F. Prove that R is an integral domain.*

Lemma 2.21. *Let F be a field of finite characteristic 0. Then the smallest field F_0 of F that contains 1_F is isomorphic to $\mathbf{Q}$.*

Proof. As in the proof of Lemma 2.20, we have a ring homomorphism $\psi\colon \mathbf{Z} \to F$ given by $\psi(n) = n1_F$. We can extend this to $\mathbf{Q}$ (see also Exercise 2.25) by setting

$$\psi\left(\frac{n}{m}\right) \stackrel{\text{def}}{=} \psi(n)\psi(m)^{-1}.$$

It follows that $\psi\colon \mathbf{Q} \to F$ is an injective homomorphism of fields and so $\psi(\mathbf{Q}) \cong \mathbf{Q}$. Since any subfield F' of F must contain 1_F, it follows that any subfield of F must contain $\psi(n)$ for any $n \in \mathbf{Z}$. Moreover, it must also contain $\psi(m)^{-1}$, and so $\psi(\mathbf{Q}) \leq F'$. ♠

Corollary 2.22. *Every field F contains a subfield that is isomorphic to precisely one of $\mathbf{F}_2, \mathbf{F}_3, \ldots,$ or $\mathbf{Q}$.*

We will call this minimal subfield the **prime subfield** of F.

Exercise 2.40. *Let F be a finite field. Prove that $|F| = p^\ell$ for some $\ell \in \mathbf{N}$ and prime p. [Hint: F is a finite dimensional vector space over $\mathbf{F}_p$ where $p = \text{char}(F)$]*

2.5 Rings: Polynomial Rings

The reader should hopefully appreciate that there is a connection between extension fields of F and polynomials over F. In the next three subsections, we will describe more explicitly this connection through the ideal theory of the polynomial ring $F[t]$ where F is a fixed field.

2.5.1 External View

We now begin our discussion of the ideal theory of polynomial rings. We note that given a commutative ring R with identity, we can approach the study of the ideals of R via two separate views which we loosely call the "internal view" and the "external view". From the internal view, we study ideals as subsets of R without reference outside of the ring R. From the external view, we study ideals in terms of ring homomorphisms $\psi\colon R \to R'$ where we vary the codomain ring R'. By the Isomorphism Theorems, we know every ideal is the kernel of a ring homomorphism and every kernel of a ring homomorphism is an ideal. In particular, both views, in theory, yield identical information. Both views have their own merits though we will start with the external view.

Given a field F, a polynomial ring $F[t]$ and an extension field E/F, we are afforded many natural ring homomorphisms $\mathrm{Eval}_\beta\colon F[t] \to E$. Specifically, given any element $\beta \in E$, we define $\mathrm{Eval}_\beta\colon F[t] \to E$ by $\mathrm{Eval}_\beta(P(t)) = P(\beta)$. For completeness, we will verify that Eval_β is a ring homomorphism. Indeed, Eval_β is an F–algebra homomorphism.

Exercise 2.41. *Prove that $F[t]$ is an F–algebra with the usual addition, multiplication, and F–scalar multiplication operations. Additionally, prove that $F[t]$ is an integral domain.*

First, note that the zero element and identity element in $F[t]$ are given by the constant polynomials

$$P_0(t) = 0_F, \quad P_1(t) = 1_F.$$

In particular, $\mathrm{Eval}_\beta(P_0) = 0_E = 0_F$ and $\mathrm{Eval}_\beta(P_1) = 1_E = 1_F$. Furthermore, we have

$$\mathrm{Eval}_\beta(P+Q) = (P+Q)(\beta) = P(\beta)+Q(\beta) = \mathrm{Eval}_\beta(P)+\mathrm{Eval}_\beta(Q)$$

and

$$\mathrm{Eval}_\beta(PQ) = (PQ)(\beta) = P(\beta)Q(\beta) = \mathrm{Eval}_\beta(P)\,\mathrm{Eval}_\beta(Q)$$

for all $P, Q \in F[t]$. Finally, we have

$$\mathrm{Eval}_\beta(\lambda P) = (\lambda P)(\beta) = \lambda P(\beta) = \lambda\,\mathrm{Eval}_\beta(P)$$

for all $P \in F[t]$ and $\lambda \in F$. Hence, Eval_β is an F–algebra homomorphism. We see that

$$\mathfrak{m}_\beta \stackrel{\text{def}}{=} \ker(\text{Eval}_\beta) = \{P(t) \in F[t] \ : \ P(\beta) = 0\}$$

is an ideal in $F[t]$. Since $\text{Eval}_\beta(F[t])$ is a subring of E, by Exercise 2.39 and Lemma 2.9, it follows that $\mathfrak{m}_\beta$ is a prime ideal. Our present goal is to show that $\mathfrak{m}_\beta$ is a maximal ideal and determine the image $\text{Eval}_\beta(F[t])$. To prove that $\mathfrak{m}_\beta$ is a maximal ideal, it is enough to show that for each $P \in F[t]$ with $\text{Eval}_\beta(P) = \alpha \neq 0_E$, that there exists $Q \in F[t]$ such that $\text{Eval}_\beta(Q) = \alpha^{-1}$. Equivalently, if $\text{Eval}_\beta(P) \neq 0_E$, we require $Q \in F[t]$ such that $\text{Eval}_\beta(PQ) = 1_E$. To find Q, we require an important property that polynomial ring $F[t]$ has. Namely, there is a division algorithm which endows $F[t]$ with the structure of a so-called Euclidean domain. We will take up this topic in the next section.

Before making our next observation, we have the following exercise.

Exercise 2.42. *Prove that if E is a field and $F \leq E$ is a subfield, then $F[t] \leq E[t]$ is a subring.*

The F–algebra homomorphism $\text{Eval}_\beta : F[t] \to E$ has an obvious extension to $E[t]$ which we denote also by Eval_β. Given $P \in E[t]$ with $\text{Eval}_\beta(P) \neq 0_E$, we claim that there exists $Q \in E[t]$ such that $\text{Eval}_\beta(PQ) = 1$. Setting $\alpha = P(\beta) = \text{Eval}_\beta(P)$, we define

$$Q(t) = \beta^{-1}t + (\alpha^{-1} - 1_E).$$

It follows that

$$\text{Eval}_\beta(Q) = Q(\beta) = \beta^{-1}\beta + \alpha^{-1} - 1_E = \alpha^{-1}.$$

In particular,

$$\mathfrak{M}_\beta \stackrel{\text{def}}{=} \{P \in E[t] \ : \ P(\beta) = 0\}$$

is a maximal ideal in $E[t]$ and $\text{Eval}_\beta(E[t]) = E$. Moreover, we have

$$\mathfrak{m}_\beta = \mathfrak{M}_\beta \cap F[t]. \tag{2.8}$$

Unfortunately, we cannot conclude that $\mathfrak{m}$ is a maximal ideal via (2.8) only.

Exercise 2.43. *Find an example of a ring R with subring R_0 and a maximal ideal $\mathfrak{m} \lhd R$ such that $\mathfrak{m}_0 = \mathfrak{m} \cap R_0$ is not a maximal ideal of R_0. Prove that $\mathfrak{m}_0$ is a prime ideal.*

Returning to our original homomorphism $\text{Eval}_\beta : F[t] \to E$, we note that if $\beta \notin F$, then $F \subset \text{Eval}_\beta(F[t])$ and this containment is proper (i.e. $F \neq \text{Eval}_\beta(F[t]) \neq F$). First, to see that $F \subset \text{Eval}_\beta(F[t])$, simply note that if $P = \alpha$ is a constant polynomial in $F[t]$, then $\text{Eval}_\beta(P) = \alpha$. Since for each $\alpha \in F$, we have such a constant polynomial in $F[t]$, we see that $F \subset \text{Eval}_\beta(F[t])$. Now, as $\beta \notin F$, we see that for $P(t) = t$ that $\text{Eval}_\beta(P) = \beta$ and so $F \neq \text{Eval}_\beta(F[t])$.

2.5.2 *Supplemental Material: Binomial Theorem.*⋆

Given a commutative ring R with identity, the **Binomial Theorem** can be extended to R. Specifically, if $r,s \in R$ and $n \in \mathbf{N}$, we have

$$(r+s)^n = \sum_{j=0}^{n} \binom{n}{j} r^{n-j} s^j \tag{2.9}$$

where

$$\binom{n}{j} \stackrel{\text{def}}{=} \frac{n!}{(n-j)!\,j!}$$

and

$$ma \stackrel{\text{def}}{=} \underbrace{a+a+\cdots+a}_{m \text{ times}}$$

for $a \in R$ and $m \in \mathbf{N}$.

***Exercise* 2.44.** *Prove (2.9) holds for any $r,s \in R$ and $n \in \mathbf{N}$.*

***Exercise* 2.45.** *Prove that if $\text{char}(R) = n$ and $r \in R$, then $nr = 0_R$.*

***Exercise* 2.46.** *Prove that if $\text{char}(R) = p$ and p is a prime, then*

$$(r+s)^p = r^p + s^p \tag{2.10}$$

*for any $r,s \in R$. In particular, if $R = \mathbf{F}_p$, then (2.10) holds. The equality (2.10) is sometimes referred to as the **Freshman's Dream**.*

2.5.3 *Internal View*

In this section, we consider the polynomial rings $F[t]$ via the "internal view". The bulk of the material in this section is devoted to the division algorithm in $F[t]$ and the Euclidean algorithm in $F[t]$ for determining great common divisors. Though somewhat elementary, these algorithms are also somewhat technically challenging. The guiding example for our algorithms of $F[t]$ are the analogs on the integers. Before we start this discussion on $F[t]$, we briefly review these algorithms in the ring $\mathbf{Z}$.

Given two elements $\alpha, \beta \in \mathbf{Z}$ with $\beta \neq 0$, there exist $q, r \in \mathbf{Z}$ such that $\alpha = q\beta + r$ where either $r = 0$ or $|r| < |\beta|$. For simplicity, we will assume that both $\alpha, \beta > 0$. To find q, r, we proceed as follows. There is a smallest integer q such that

$$q\beta \leq \alpha < (q+1)\beta.$$

In particular, $\alpha - q\beta = r \geq 0$ and $0 \leq r < \beta$.

Assuming still that $\alpha, \beta > 0$, the greatest common divisor of α, β is the largest positive integer d such that d divides a, b. It follows that any integer d' that divides α, β also divides d and that there exist $a, b \in \mathbf{Z}$ such that $a\alpha + b\beta = d$. Additionally, $\gcd(\alpha, \beta) \leq \min\{\alpha, \beta\}$. To determine the greatest common divisor of α, β, we proceed as follows. We will assume that $\beta \leq \alpha$. Using the above, there exists $q_1, r_1 \in \mathbf{Z}$ such that $\alpha = q_1\beta + r_1$ with $0 \leq r < \beta$. If $r_1 = 0$, we define $\gcd(\alpha, \beta) = \beta$. Note that $\beta + 0\alpha = \beta$ and that β divides both α, β. Otherwise, if $r_1 \neq 0$, we replace α with r_1. Using the division algorithm, there exist $q_1, r_2 \in \mathbf{Z}$ such that $\beta = q_2 r_1 + r_2$. If $r_2 = 0$, we set $\gcd(\alpha, \beta) = r_1$. In this case, r_1 divides β and since $\alpha = q_1\beta + r_1$, we see that r_1 also divides β. Furthermore, we have $r_1 = \alpha - q_1\beta$. If $r_2 \neq 0$, we replace β with r_2. By the division algorithm, there exist q_3, r_2 such that $r_1 = q_3 r_2 + r_3$. If $r_3 = 0$, we set $\gcd(\alpha, \beta) = r_2$. In this case, r_2 divides r_1 and since $\beta = q_2 r_1 + r_2$, we see that r_2 divides β. Similarly, since α equals $q_1\beta + r_1$, we see that r_2 divides β. Finally, we have

$$r_2 = \beta - q_2 r_1 = \beta + q_2(\alpha - q_1\beta) = (1 - q_1 q_2)\beta + q_2\alpha.$$

Continuing this process, we get a non-negative, strictly decreasing sequence of integers r_i such that

$$r_i = q_i r_{i-2} + r_{i-1}.$$

Eventually, there exists some $n \in \mathbf{N}$ such that $r_n = 0$ and we set $\gcd(\alpha, \beta) = r_{n-1}$. One can check that r_{n-1} divides both α, β and that there exist $a, b \in \mathbf{Z}$ such that $r_{n-1} = a\alpha + b\beta$.

The division and Euclidean algorithms on $\mathbf{Z}$ will be our models for these algorithms on $F[t]$. Our measurement of complexity in $\mathbf{Z}$ is the absolute value of the number. On $F[t]$, our measurement of complexity is given by the degree of the polynomial. We now review the division algorithm for polynomials in $F[t]$.

Given polynomials $P_1, P_2 \in F[t]$ with $P_2 \neq 0_F$, we assert that there exist polynomials $Q, R \in F[t]$ such that $P_1 = QP_1 + R$ where either $R = 0_F$ or $\deg(R) < \deg(P_2)$. We outline the division algorithm in $F[t]$.

Division Algorithm.

To begin, if $\deg(P_1) < \deg(P_2)$, then we set $Q = 0_F$ and $R = P_1$. Assuming $\deg(P_1) \geq \deg(P_2)$, we write

$$P_1 = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0, \quad P_2 = b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0$$

where $a_n, b_m \neq 0_F$ and $n \geq m$. We define

$$Q_1(t) = \frac{a_n}{b_m} t^{n-m}$$

and note that

$$\begin{aligned} P_1 - Q_1P_2 &= a_nt^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 - a_nt^n - \frac{a_n}{b_m}b_{m-1}t^{n-1} - \cdots + \frac{a_n}{b_m}b_1t^{n-m+1} - \frac{a_n}{b_m}b_0t^{n-m} \\ &= \left(a_{n-1} - \frac{a_n}{b_m}b_{m-1}\right)t^{n-1} + \cdots + \left(a_{n-m+1} - \frac{a_n}{b_m}b_1\right)t^{n-m+1} \\ &\quad + \left(a_{n-m} - \frac{a_n}{b_m}b_0\right)t^{n-m} + a_{n-m-1}t^{n-m-1} + \cdots + a_1t + a_0 \end{aligned}$$

We replace P_1 with $P_{1,1} = P_1 - Q_1P_2$, noting that $\deg(P_{1,1}) < \deg(P_1)$. If $\deg(P_{1,1}) < \deg(P_2)$, we define

$$Q = Q_1, \quad R - P_{1,1}.$$

Otherwise, for notational simplicity, write

$$P_{1,1} = a_{1,n_1}t^{n_1} + \cdots + a_{1,1}t + a_{1,0}$$

where $a_{1,n_1} \neq 0_F$ and $n_1 \geq m$. We define

$$Q_2 = \frac{a_{1,n_1}}{b_m}t^{n_1-m}$$

and replace $P_{1,1}$ with $P_{2,1} = P_{1,1} - Q_2P_2$. As before, $\deg(P_{2,1}) < \deg(P_{1,1})$. If $\deg(P_{2,1}) < \deg(P_2)$, we define

$$Q = Q_1 + Q_2, \quad R = P_{2,1}.$$

Otherwise, we repeat this process, obtaining a sequence of polynomials Q_i and $P_{i,1}$ such that

$$P_{i+1,1} = P_{i,1} - Q_{i+1}P_2$$

and $\deg(P_{i+1,1}) < \deg(P_{i,1})$. Eventually $\deg(P_{i+1,1}) < \deg(P_2)$ and when this occurs, we set

$$Q = \sum_{j=1}^{i+1} Q_j, \quad R = P_{i+1,1}.$$

Theorem 2.23 (Division Algorithm: Polynomial Rings)**.** *Let F be a field and $P_1, P_2 \in F[t]$. Then there exist $Q, R \in F[t]$ such that $P_1(t) = Q(t)P_2(t) + R(t)$ with either $R(t) = 0_F$ or $\deg(R) < \deg(P_2)$. Moreover, Q, R are uniquely determined by this information*

Exercise 2.47. *Prove that $Q, R \in F[t]$ in Theorem 2.23 are unique.*

Given $P_1, P_2 \in F[t]$, we say that P_2 **divides** P_1 if $P_1 = QP_2$ for some $Q \in F[t]$.

We next use Theorem 2.23 to produce a **Euclidean algorithm** for computing the **greatest common divisor** $\gcd(P_1, P_2)$ of two polynomials $P_1, P_2 \in F[t]$. The greatest common divisor of P_1, P_2 should satisfy the following two conditions:

(a) $\gcd(P_1,P_2)$ divides P_1 and P_2.

(b) There exists $H_1,H_2 \in F[t]$ such that $\gcd(P_1,P_2) = H_1P_1 + H_2P_2$ and $\deg(H_1) < \deg(P_2)$ (provided $\deg(P_2) \neq 0$) and $\deg(H_2) < \deg(P_1)$ (provided $\deg(P_1) \neq 0$). In particular, if Q divides P_1,P_2, then Q divides $\gcd(P_1,P_2)$.

Exercise 2.48. *Let E/F be an extension of fields and $\beta \in E$ be algebraic. Prove that if $P \in F[t]$ is a non-zero polynomial such that $P(\beta) = 0$, then the minimal polynomial P_β of β over F divides P. In particular, the minimal polynomial of β is irreducible.*

Exercise 2.49. *Let E/F be a finite extension and $L\colon E \to \mathrm{Mat}(n,F)$ be an injective F–algebra homomorphism with $n = [E:F]$.*

(i) Prove that if $c_{L(\beta)}$ is the characteristic polynomial of $L(\beta)$, then P_β divides $c_{L(\beta)}$.

(ii) Prove that there exists an F–basis $\{\beta_1,\ldots,\beta_n\}$ of E such that for each $\beta \in E$, if we define the n by n matrix (A_β) to have (i,j) coefficient $(\alpha_{i,j})$ where $\alpha_{i,j}$ is defined by

$$\beta\beta_j = \sum_{i=1}^{n} \alpha_{i,j}\beta_i,$$

then $L(\beta) = A_\beta$.

Exercise 2.50. *Let E/F be a finite extension of degree n and $m \in \mathbf{N}$ with $m < n$. Prove that there cannot be an injective F–algebra homomorphism $L\colon E \to \mathrm{Mat}(m,F)$.*

Euclidean Algorithm.

Given $P_1,P_2 \in F[t]$, we will assume that $\deg(P_1) \geq \deg(P_2)$; if this is not the case, we can simply relabel P_1,P_2 so that it holds. By Theorem 2.23, there exist unique polynomials $Q_1,R_1 \in F[t]$ such that

$$P_1 = Q_1P_2 + R_1$$

where $\deg(R_1) < \deg(P_2)$ or $R_1 = 0_F$. If $R_1 = 0$, then we set $\gcd(P_1,P_2) = P_2$. Since $R_1 = 0$, we see that P_2 divides P_1,P_2 and that

$$P_2 = 0_RP_1 + 1_RP_2.$$

In particular, $H_1 = 0_R$ and $H_2 = 1_R$. Since $\deg(H_1) = \deg(H_2) = 0$, we see that $\deg(H_1) < \deg(P_2)$ (provided $\deg(P_2) \neq 0$) and $\deg(H_2) < \deg(P_1)$ (provided $\deg(P_1) \neq 0$).

If $R_1 \neq 0$, we replace P_1 with R_1. By Theorem 2.23, there exists $Q_2,R_2 \in F[t]$ such that

$$P_2 = Q_2R_1 + R_2$$

where either $R_2 = 0_F$ or $\deg(R_2) < \deg(R_1)$. If $R_2 = 0_F$, we set $\gcd(P_1, P_2) = R_1$. Note that

$$R_1 = P_1 - Q_1 P_2$$

and so we can take $H_1 = 1$ and $H_2 = Q_1$ in (b). It follows that $\deg(H_1) < \deg(P_2)$; note that if $\deg(P_2) = 0$, then $R_1 = 0$. By Exercise 2.13, we have $\deg(P_2) + \deg(Q_1) = \deg(P_1)$ and $\deg(P_2) > 0$, and so $\deg(H_2) < \deg(P_1)$. Finally, since $P_2 = Q_2 R_1$, we see that

$$P_1 = R_1 + Q_2 Q_1 R_1 = R_1(1 + Q_2 Q_1).$$

Hence R_1 divides both P_1, P_2 and so (a) holds.

If $R_2 \neq 0$, then we replace P_2 with R_2, by Theorem 2.23, there exist $Q_3, R_3 \in F[t]$ such that

$$R_1 = Q_3 R_2 + R_3$$

where $R_3 = 0$ or $\deg(R_3) < \deg(R_2)$. If $R_3 = 0$, we set $\gcd(P_1, P_2) = R_2$. We have

$$P_1 = Q_1 P_2 + R_1, \quad P_2 = Q_2 R_1 + R_2, \quad R_1 = Q_3 R_2.$$

Substituting, we see that

$$R_2 = P_2 - Q_2 R_1 = P_2 - Q_2(P_1 - Q_1 P_2) = (1_F - Q_2)P_1 + Q_1 Q_2 P_2.$$

By Exercise 2.13, $\deg(P_2) > \deg(Q_2) = \deg(1_F - Q_2)$. As $H_1 = 1_F - Q_2$, we see that $\deg(P_2) > \deg(H_1)$. Likewise,

$$\deg(P_1) = \deg(Q_1) + \deg(P_2) > \deg(Q_1) + \deg(Q_2) = \deg(Q_1 Q_2) = \deg(H_2).$$

Finally, since R_2 divides R_1 and $P_2 = Q_2 R_1 + R_2$, we see that R_2 divides P_2. Since $P_1 = Q_1 P_2 + R_1$, we see that R_2 also divides P_1.

We can continue this process, obtaining a sequence of polynomials $R_i \in F[t]$ with

$$R_i = Q_{i+2} R_{i+1} + R_{i+2}$$

and $\deg(R_{i+1}) < \deg(R_i)$. For some $n \in \mathbf{N}$, we will have $R_n = 0$ and $R_{n-1} \neq 0$. For such an n, we set $\gcd(P_1, P_2) = R_{n-1}$. We see that

$$R_i = R_{i-2} - Q_i R_{i-1} \tag{2.11}$$

for $i \geq 3$ and

$$R_1 = P_1 - Q_1 P_2, \quad R_2 = P_2 - Q_2 R_1. \tag{2.12}$$

Using (2.11) (many times) and (2.12), we obtain

$$\begin{aligned}
R_{n-1} &= R_{n-3} - Q_{n-1}R_{n-2} \\
&= R_{n-5} - Q_{n-3}R_{n-4} - Q_{n-1}(R_{n-4} - Q_{n-2}R_{n-3}) \\
&= R_{n-7} - Q_{n-5}Q_{n-6} - Q_{n-2}(R_{n-6} - Q_{n-4}R_{n-5}) - Q_{n-1}(R_{n-6} - Q_{n-4}R_{n-5}) - Q_{n-2}(R_{n-5} - Q_{n-3}R_{n-4}) \\
&\quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
&= H_1P_1 + H_2P_2.
\end{aligned}$$

Since R_{n-1} divides R_{n-2} and $R_{n-3} = R_{n-1} + Q_{n-1}R_{n-2}$, we see that R_{n-1} divides R_{n-3}. Arguing via induction, we conclude that R_{n-1} divides R_i for all $i \geq 1$ and so R_{n-1} divides both P_1, P_2 by (2.12).

Finally, we prove that $\deg(H_1) < \deg(P_2)$ and $\deg(H_2) < \deg(P_1)$ unless $\deg(P_1) = \deg(P_2) = 0$. If $\deg(H_1) \geq \deg(P_2)$, then by Theorem 2.23, there exists $Q, R \in F[t]$ such that $H_1 = QP_2 + R$ with $\deg(R) < \deg(P_2)$ or $R = 0$. For this, we obtain

$$P_1(QP_2 + R) + H_2P_2 = P_1R + (P_1Q + H_2)P_2 = \gcd(P_1, P_2).$$

If $R = 0$, we see that

$$\deg(\gcd(P_1, P_2)) \geq \deg(P_1) + \deg(P_2) + \deg(Q). \tag{2.13}$$

Since $\gcd(P_1, P_2)$ divides both P_1, P_2, we know that

$$\deg(\gcd(P_1, P_2)) \leq \min\{\deg(P_1), \deg(P_2)\}. \tag{2.14}$$

In particular, (2.13) contradicts (2.14) unless $\deg(P_1) = \deg(P_2) = \deg(Q) = \deg(H_1) = 0$. Hence, either $\deg(P_2) > \deg(H_1)$ or $\deg(P_1) = \deg(P_2) = 0$. If $R \neq 0$, since $\deg(R) < \deg(P_2)$, we again see that (2.13) holds. As before, (2.13) contradicts (2.14) unless $\deg(P_1) = \deg(P_2) = \deg(Q) = \deg(H_1) = 0$. In total, our assumption that $\deg(H_1) \geq \deg(P_2)$ leads to a contradiction unless $\deg(P_1) = \deg(P_2) = 0$. Thus, we conclude that $\deg(P_2) > \deg(H_1)$ or $\deg(P_1) = \deg(P_2) - 0$. The proof that $\deg(H_2) < \deg(P_1)$ or $\deg(P_1) = \deg(P_2) = 0$ is similar and left for the reader.

***Remark* 2.24.** *Given $P_1, P_2 \in F[t]$, the greatest common divisor $\gcd(P_1, P_2)$ is unique up to multiplication by a unit in $F[t]$. In a general commutative ring with identity R, we say that two elements $r_1, r_2 \in R$ are **associates** if there exists a unit $u \in R$ such that $ur_1 = r_2$. In particular, any two greatest common divisors of P_1, P_2 are associates. When we write $\gcd(P_1, P_2)$, we will assume that this is a monic polynomial and hence by Exercise 2.51 below, is unique under this additional condition.*

***Exercise* 2.51.** *Let $P_1, P_2 \in F[t]$. Prove that if $P \in F[t]$ divides $\gcd(P_1, P_2)$, then there exists an $\alpha \in F$ such that $P = \alpha \gcd(P_1, P_2)$.*

***Exercise* 2.52.** *Let $P_1, P_2 \in F[t]$. Prove that $\langle P_1 \rangle \langle P_2 \rangle = \langle \gcd(P_1, P_2) \rangle$.*

Exercise 2.53. *Let $m_1, \ldots, m_n \in \mathbf{N}$ and assume that $\gcd(m_i, m_j) = 1$ for all $i \neq j$.*

(i) Prove that

$$\bigcap_{i=1}^{n} m_i\mathbf{Z} = (m_1 \ldots m_n)\mathbf{Z}.$$

(ii) Prove that

$$\mathbf{Z}/\langle m_1 \ldots m_n \rangle \cong \prod_{i=1}^{n} \mathbf{Z}/m_i\mathbf{Z}.$$

*This is called the **Chinese Remainder Theorem**.*

(iii) Prove that if $s_1, \ldots, s_n \in \mathbf{N}$, then

$$\bigcap_{i=1}^{n} s_i\mathbf{Z} = \operatorname{lcm}(s_1, \ldots, s_n)\mathbf{Z}.$$

(iv) Prove that if $s, t \in \mathbf{N}$ and s divides t, then there exists a surjective ring homomorphism $\psi_{s,t} \colon \mathbf{Z}/t\mathbf{Z} \to \mathbf{Z}/s\mathbf{Z}$. [Hint: Try $a + t\mathbf{Z} \mapsto a + s\mathbf{Z}$.]

(v) If $s = \operatorname{lcm}(s_1, \ldots, s_n)$, prove that there exists an injective homomorphism

$$\psi \colon \mathbf{Z}/s\mathbf{Z} \to \prod_{i=1}^{n} \mathbf{Z}/s_i\mathbf{Z}$$

such that the index of $\psi(\mathbf{Z}/\operatorname{lcm}(s_1, \ldots, s_n)\mathbf{Z})$ in $\prod_{i=1}^{n} \mathbf{Z}/s_i\mathbf{Z}$ is $\gcd(s_1, \ldots, s_n)$. [Hint: Take the product of the ring homomorphisms $\psi_{s,s_i} \colon \mathbf{Z}/s\mathbf{Z} \to \mathbf{Z}/s_i\mathbf{Z}$.]

(vi) Deduce that if $s_1, \ldots, s_n \in \mathbf{N}$, then

$$s_1 \ldots s_n = \operatorname{lcm}(s_1, \ldots, s_n) \gcd(s_1, \ldots, s_n).$$

Exercise 2.54. *Let $P_1, \ldots, P_n \in F[t]$ and assume that $\gcd(P_i, P_j) = 1_F$ for $i \neq j$.*

(i) Prove that

$$\bigcap_{i=1}^{n} \langle P_i \rangle = \langle P_1 \ldots P_n \rangle .$$

(ii) Prove that

$$F[t]/\langle P_1 \ldots P_n \rangle \cong \prod_{i=1}^{n} F[t]/\langle P_i \rangle .$$

*This is a version of the **Chinese Remainder Theorem**.*

2.5.4 *Unified View*

We now utilize the previous subsection to further our understanding of ideals in $F[t]$. Our two main goals are to prove that prime ideals in $F[t]$ are maximal ideals and that every ideal in $F[t]$ is principal. Our focus will start with the "internal view" of ideals inside of $F[t]$. After establishing some fundamental results, we will connect the "internal" and "external" views.

***Definition* 2.29** (Principal Ideal Domain)**.** *We say that an integral domain D is a **principal ideal domain** if every proper, non-trivial ideal is principal.*

***Lemma* 2.25.** *If F is a field, then every proper, non-trivial ideal in $F[t]$ is principal. In particular, $F[t]$ is a principal ideal domain.*

Proof. Given an ideal $\mathfrak{a} \lhd F[t]$, we select $P \in \mathfrak{a}$ such that $\deg(P) \leq \deg(P')$ for any $P' \in \mathfrak{a}$. Provided $\mathfrak{a} \neq \{0_F\}$ or $F[t]$ (i.e. $\mathfrak{a}$ is proper and non-trivial), we must have $\deg(P) > 0$. Indeed, if $\deg(P) = 0$ and $P \neq 0_F$, then P is a unit and so $\mathfrak{a} = F[t]$ by Lemma 2.3. Given $P' \in \mathfrak{a}$, by Theorem 2.23, there exists $Q, R \in F[t]$ such that $P' = QP + R$ with either $R = 0_F$ or $\deg(R) < \deg(P)$. Since $\mathfrak{a}$ is an ideal and $P \in \mathfrak{a}$, we know that $QP \in \mathfrak{a}$. Also, since $P' \in \mathfrak{a}$, we know that $P' - QP \in \mathfrak{a}$. It follows then that $R \in \mathfrak{a}$ and so $R = 0_F$ by selection of P. Hence $P' = QP$ and $\mathfrak{a}$ is a principal ideal generated by P. ♠

***Exercise* 2.55.** *Let F be a field and $\mathfrak{a}$ be a non-zero, proper ideal in $F[t]$. Prove that if $P_1, P_2 \in \mathfrak{a}$ have minimal degree (among the non-zero elements), then there exists $\alpha \in F$ such that $\alpha P_1 = P_2$. In particular, if $P_1, P_2 \in \mathfrak{a}$ have minimal degree, then $\mathfrak{a} = \langle P_1 \rangle = \langle P_2 \rangle$. Deduce that for each non-zero ideal $\mathfrak{a}$, there exists a unique monic polynomial P of minimal degree and $\langle P \rangle = \mathfrak{a}$.*

***Exercise* 2.56.** *Let $P_1, \ldots, P_n \in F[t]$. If*

$$\langle P \rangle = \bigcap_{i=1}^{n} \langle P_i \rangle ,$$

*prove that if $Q \in F[t]$ and P_i divides Q for $i = 1, \ldots, n$, then P divides Q. Moreover, there is a unique monic polynomial P with this property. We call such a P the **least common multiple** of $P_1, \ldots, P_n$ and we denote it by $\operatorname{lcm}(P_1, \ldots, P_n)$.*

***Exercise* 2.57.** *Let $P_1, \ldots, P_n \in F[t]$. Prove that there exists $\alpha \in F$ such that*

$$P_1 \ldots P_n = \alpha \operatorname{lcm}(P_1, \ldots, P_n) \gcd(P_1, \ldots, P_n).$$

***Proposition* 2.26.** *If $\mathfrak{p}$ is a non-trivial, proper, prime ideal in $F[t]$, then $\mathfrak{p}$ is maximal.*

Proof. By Lemma 2.18, it is enough to show that $F[t]/\mathfrak{p}$ is a field. By Lemma 2.9, we know that $F[t]/\mathfrak{p}$ is an integral domain and so it is enough to prove that each non-zero element of $F[t]/\mathfrak{p}$ has a multiplicative

inverse. In particular, given $P_1 \in F[t] - \mathfrak{p}$, we show that there exists $P_2 \in F[t]$ such that $\psi_{\mathfrak{p}}(P_1 P_2) = 1$. We will find P_2 using the Euclidean algorithm.

By Lemma 2.25, we know that $\mathfrak{p} = \langle P \rangle$ for some $P \in F[t]$. We assert that if $P' \in F[t]$ divides P and $\deg(P') > 0$, then $P' = \alpha P$ for some $\alpha \in F$. To see this assertion, if P' divides P, then there exists $Q \in F[t]$ such that $P = QP'$. Since $\mathfrak{p}$ is a prime ideal, either $P' \in \mathfrak{p}$ or $Q \in \mathfrak{p}$. Now, by Exercise 2.13, we know that $\deg(P) = \deg(P') + \deg(Q)$. If $Q \in \mathfrak{p}$, since $\deg(P') > 0$, it follows that $\deg(Q) < \deg(P)$, contradicting the fact that P has minimal degree among the elements of $\mathfrak{p}$. Hence, $P' \in \mathfrak{p}$ and $\deg(Q) = 0$.

Given $P_1 \in F[t] - \mathfrak{p}$, by using Theorem 2.23, we can assume that $\deg(P_1) < \deg(P)$. To see this claim, note that if $\deg(P_1) \geq \deg(P)$, by Theorem 2.23, there exist $Q, R \in F[t]$ such that $P_1 = QP + R$ with either $R = 0$ or $\deg(R) < \deg(P)$. Since $P_1 \notin \mathfrak{p}$, it must be that $R \neq 0$. Moreover, we see that $\psi_{\mathfrak{p}}(P_1) = \psi_{\mathfrak{p}}(R)$ since $\psi_{\mathfrak{p}}(QP) = 0$. Setting $D = \gcd(P, P_1)$, since D divides P and

$$\deg(D) \leq \deg(P_1) = \min\{\deg(P_1), \deg(P)\},$$

we conclude that $D = 1_F$ from the previous paragraph. Indeed, from the previous paragraph, any divisor of P with degree strictly less than P must be an element of F and since D is monic and a divisor of P, it must be 1_F. By the Euclidean algorithm, there exist $H_1, H_2 \in F[t]$ such that $H_1 P + H_2 P_1 = 1_F$. Finally, we see that

$$\psi_{\mathfrak{p}}(H_1 P + H_2 P_1) = \psi_{\mathfrak{p}}(H_1 P) + \psi_{\mathfrak{p}}(H_2 P_1) = \psi_{\mathfrak{p}}(H_2 P_1) = 1.$$

♠

Proposition 2.27. *If $\mathfrak{m} \lhd F[t]$ is a maximal ideal, then $E_{\mathfrak{m}} = F[t]/\mathfrak{m}$ is a finite extension of F. Specifically, $\psi_{\mathfrak{m}} \colon F[t] \to E_{\mathfrak{m}}$ restricted to $F \leq F[t]$ is injective (and so $\psi_{\mathfrak{m}}(F) \leq E_{\mathfrak{m}}$ is isomorphic to F) and $E_{\mathfrak{m}}/\psi_{\mathfrak{m}}(F)$ is a finite extension.*

Proof. Given $\alpha \in F$, since $\mathfrak{m}$ is a proper ideal, by Lemma 2.3, we see that $\alpha \notin \mathfrak{m}$. If $\psi_{\mathfrak{m}}(\alpha_1) = \psi_{\mathfrak{m}}(\alpha_2)$ for $\alpha_1, \alpha_2 \in F$, we see that $\alpha_1 - \alpha_2 \in \mathfrak{m}$. Since $\alpha_1 - \alpha_2 \in F$ and $\alpha_1 - \alpha_2$ is not a unit by Lemma 2.3, we must have $\alpha_1 = \alpha_2$. Hence, $\psi_{\mathfrak{m}}$ restricted to F is injective and $\psi_{\mathfrak{m}} \colon F \to \psi_{\mathfrak{m}}(F) \leq E_{\mathfrak{m}}$ is an isomorphism of fields. Identifying $\psi_{\mathfrak{m}}(F)$ with F, we see that E/F is an extension.

To see that $E_{\mathfrak{m}}$ is a finite extension, by Lemma 2.25, we know that $\mathfrak{m} = \langle P \rangle$ for some polynomial $P \in F[t]$ with minimal degree in $\mathfrak{m}$. We assert that $[E_{\mathfrak{m}} : F] = \deg(P)$. Given $P' \in F[t] - \mathfrak{m}$ with $\deg(P') \geq \deg(P)$, by Theorem 2.23, there exist $Q, R \in F[t]$ such that $P' = QP + R$ with $\deg(R) < \deg(P)$ and $R \neq 0$. Since $\psi_{\mathfrak{m}}(P') = \psi_{\mathfrak{m}}(R)$, we see that

$$\psi_{\mathfrak{m}}(F[t]) = \left\{ \psi_{\mathfrak{m}}(P') \ : \ \deg(P') < \deg(P) \right\}. \tag{2.15}$$

Setting $m = \deg(P)$, we assert that $\mathscr{B} = \left\{\psi_{\mathfrak{m}}(1_F), \psi_{\mathfrak{m}}(t), \ldots, \psi_{\mathfrak{m}}(t^{m-1})\right\}$ is a basis for $E_{\mathfrak{m}}$ as an F–vector space. To see that $\mathscr{B}$ spans, given any $P' \in F[t]$ with $\deg(P') < m$, by definition, we have

$$P' = \sum_{i=0}^{m-1} \alpha_i t^i$$

where $\alpha_i \in F$. In particular,

$$\psi_{\mathfrak{m}}(P') = \sum_{i=0}^{m-1} \alpha_i \psi_{\mathfrak{m}}(t^i).$$

Therefore, $\psi_{\mathfrak{m}}(P')$ is in the F–span of $\mathscr{B}$ for every $P' \in F[t]$ with $\deg(P') < m$. Combining this with (2.15), we conclude that $\mathscr{B}$ spans $E_{\mathfrak{m}}$. To see that $\mathscr{B}$ is F–linearly independent, if

$$\sum_{i=0}^{m-1} \alpha_i \psi_{\mathfrak{m}}(t^i) = 0$$

for some $\alpha_i \in F$, we see that

$$\psi_{\mathfrak{m}}\left(\sum_{i=0}^{m-1} \alpha_i t^i\right) = 0.$$

Setting

$$P' = \sum_{i=0}^{m-1} \alpha_i t^i,$$

we conclude that $P' \in \mathfrak{m}$. Since $\deg(P') < \deg(P)$, we must have $P' = 0$ and so $\mathscr{B}$ is F–linearly independent. Finally, by definition of the degree of an extension, we have $[E_{\mathfrak{m}} : F] = |\mathscr{B}| = \deg(P)$. ♠

We will refer to $E_{\mathfrak{m}}$ as the **associated finite extension** of F. We have the following corollary of the proof of Proposition 2.27.

***Scholium* 2.28.** *Let $\mathfrak{m} = \langle P \rangle \lhd F[t]$ be maximal with associated extension $E_{\mathfrak{m}}$. Then $[E_{\mathfrak{m}} : F] = \deg(P)$. Moreover, $\left\{\psi_{\mathfrak{m}}(1_F), \psi_{\mathfrak{m}}(t), \ldots, \psi_{\mathfrak{m}}(t^{\deg(P)-1})\right\}$ is an F–basis for $E_{\mathfrak{m}}$.*

***Definition* 2.30** (Irreducible Polynomial)**.** *Let $P \in F[t]$ be non-constant. We say that P is **irreducible over F** if whenever $P = P_1 P_2$ for $P_1, P_2 \in F[t]$, we have either $\deg(P_1) = 0$ or $\deg(P_2) = 0$.*

We will often simply say that P is irreducible as "over F" is usually clear from the context.

***Exercise* 2.58.** *Let $P \in F[t]$ be non-constant. Prove the following are equivalent:*

(i) P is irreducible over F.

(ii) $\langle P \rangle$ *is a prime ideal in* $F[t]$.

In particular, by Proposition 2.26, a polynomial P *is irreducible if and only if* $\langle P \rangle \lhd F[t]$ *is maximal.*

Given an irreducible polynomial $P \in F[t]$, we know that $\langle P \rangle = \mathfrak{m}$ is a prime ideal by Exercise 2.58. Moreover, by Proposition 2.26, we know that $\mathfrak{m}$ is maximal. The associated extension $E_{\mathfrak{m}}$ is finite by Proposition 2.27. We assert that there exists $\beta \in E_{\mathfrak{m}}$ such that for

$$\mathfrak{m}_\beta = \left\{ P' \in F[t] \ : \ \mathrm{Eval}_\beta(P') = 0 \right\},$$

we have $\mathfrak{m} = \mathfrak{m}_\beta$. Let $\beta = \psi_{\mathfrak{m}}(t)$ and write

$$P(t) = \sum_{i=0}^{m} \alpha_i t^i.$$

Since

$$\sum_{i=0}^{m} \alpha_i \beta^i = \sum_{i=0}^{m} \alpha_i \psi_{\mathfrak{m}}(t)^i = \psi_{\mathfrak{m}} \left(\sum_{i=0}^{m} \alpha_i t^i \right) = \psi_{\mathfrak{m}}(P) = 0,$$

we see that $\mathrm{Eval}_\beta(P) = 0$, and so $P \in \mathfrak{m}_\beta$. In particular, $\mathfrak{m} \subseteq \mathfrak{m}_\beta$. As $\mathfrak{m}$ is maximal, we must have $\mathfrak{m} = \mathfrak{m}_\beta$. Moreover, since $\left\{1, \beta, \ldots, \beta^{m-1}\right\}$ is a basis for $E_{\mathfrak{m}}$ by Scholium 2.28, we see that $F(\beta) = E_{\mathfrak{m}}$.

Definition **2.31** (Simple Extension)**.** *We say that an extension* E/F *is* ***simple*** *if there exists* $\beta \in E$ *such that* $E = F(\beta)$.

From this discussion, we obtain the following result.

Corollary **2.29.** *Let* $\mathfrak{m} = \langle P \rangle$ *be a maximal ideal in* $F[t]$.

(a) There exists $\beta \in E_{\mathfrak{m}}$ *such that* $P(\beta) = 0$.

(b) $E_{\mathfrak{m}} = F(\beta)$. *That is,* $E_{\mathfrak{m}}$ *is a simple extension.*

(c) $\mathfrak{m} = \ker(\mathrm{Eval}_\beta) = \mathfrak{m}_\beta$.

(d) If $\beta' \in E_{\mathfrak{m}}$ *and* $P(\beta') = 0$, *then* $E_{\mathfrak{m}} = F(\beta')$.

Proof. Only (d) requires an argument as (a), (b), and (c) were established above. For (d), simply note that $\mathfrak{m} = \ker(\mathrm{Eval}_{\beta'}) = \mathfrak{m}_{\beta'}$ and so $F(\beta') = E_{\mathfrak{m}}$. ♠

In the sequel, we will require some additional terminology.

Definition 2.32 (Separable Polynomial)**.** *We say that a polynomial $P \in F[t]$ is **separable** if P has no repeated/multiple roots.*

Exercise 2.59. *Let $P \in F[t]$. Define*

$$dP(t) \stackrel{def}{=} \sum_{i=1}^{m} i\alpha_i t^{i-1}$$

where

$$P(t) = \sum_{i=0}^{m} \alpha_i t^i.$$

(i) Prove that $D\colon F[t] \to F[t]$ defined by $D(P) = dP$ is an F–linear function.

(ii) Prove that $P \in F[t]$ is separable if and only if $\gcd(P, dP) = 1_F$.

(iii) Prove that if $\mathrm{char}(F) = 0$, then every irreducible polynomial $P \in F[t]$ is separable. [Hint: Use (ii)]

(iv) Prove that if F is a field with $\mathrm{char}(F) = p \neq 0$ and $P \in F[t]$ is irreducible and not separable, then there exists $Q \in F[t]$ such that $P(t) = Q(t^p)$. [Hint: Use (ii)]

2.6 Fields: Factoring Polynomials and Splitting Fields

This section brings together of our work in the earlier sections of this chapter to establish several important results. One hopes that the reader will better understand why we spent a considerable amount of time and energy on polynomial rings. At any rate, in this section, we will discuss factorization of polynomials, spitting fields for polynomials, algebraically closed fields, and algebraic closures of fields. The focus will be on zeroes of polynomials which is equivalent to factorizing polynomials.

Given an ideal $\mathfrak{a}$ of $F[t]$, by Lemma 2.25, $\mathfrak{a}$ is principal and so $\mathfrak{a} = \langle P \rangle$ for some $P \in F[t]$. According to Exercise 2.58, $\mathfrak{a}$ is a maximal ideal if and only if P is irreducible. Of course, not every polynomial P in $F[t]$ is irreducible. We begin this section by discussing how P can be factored into a product of irreducible polynomials (see Theorem 2.30). The factorization of P will provide us with a factorization of the ideal $\mathfrak{a}$ (see Corollary 2.31). We will use the factorization of P to produce a finite extension of F such that every zero of P is an element of this extension (see Theorem 2.33). This is the so-called splitting field for P. Finally, we will produce an algebraic extension $\overline{F}$ of a field F such that every polynomial $P \in F[t]$ has a zero in $\overline{F}$ (see Theorem 2.38).

Factoring Polynomials.

Given $P \in F[t]$, if P is not irreducible, there exists $P_{0,1}, P_{0,2} \in F[t]$ such that $P = P_{0,1}P_{0,2}$ and

$$0 < \deg(P_{0,1}), \deg(P_{0,2}) < \deg(P).$$

If both $P_{0,1}$ and $P_{0,2}$ are irreducible, then we have expressed P as a product of irreducible polynomials. Otherwise, we can express $P_{0,i} = P_{1,i,1}P_{1,i,2}$ with $0 < \deg(P_{1,i,1}), \deg(P_{1,i,2}) < \deg(P_i)$. Continuing this process, since at each stage the polynomials have strictly decreasing degree, we see that it will terminate. Combining all of the factorizations of the smaller degree polynomials, we obtain

$$P = P_{0,1}P_{0,2} = (P_{1,1,1}P_{1,1,2})(P_{1,2,1}P_{1,2,2}) = \cdots = \prod_{i=0}^{r_P} P_i \tag{2.16}$$

where each P_i is irreducible over F and $0 < \deg(P_i) < \deg(P)$.

We next prove that the factorization of P given by (2.16) is unique up to permuting the factors P_i and multiply each factor P_i by a unit. We will prove this by induction on the number of factors r_P. If $r_P = 2$, then $P = P_1P_2$. We will assume that

$$P = \prod_{i=1}^{n} Q_i$$

where the Q_i are irreducible and $0 < \deg(Q_i) < \deg(P)$. Since $P = P_1P_2$, we see that $P \in \langle P_i \rangle$ for $i = 1, 2$. As $P = Q_1 \dots Q_n$ and $\langle P_1 \rangle$ is a prime ideal, we see that either $Q_i \in \langle P_1 \rangle$ for some $1 \leq i \leq n$. It follows that $\langle Q_i \rangle \leq \langle P_1 \rangle$. Since Q_i is irreducible, $\langle Q_i \rangle$ is a maximal ideal by Exercise 2.58. Hence, $\langle P_1 \rangle = \langle Q_i \rangle$. Since both P_1, Q_i have minimal degree in this ideal, we see that $\deg(P_1) = \deg(Q_i)$. In particular, by Exercise 2.55, there exists $\alpha \in F$ such that $\alpha P_1 = Q_i$. Now, we have

$$P = P_1P_2 = Q_1 \dots Q_{i-1}Q_iQ_{i+1} \dots Q_n = Q_1 \dots Q_{i-1}(\alpha P_1)Q_{i+1} \dots Q_n = P_1(\alpha Q_1 \dots Q_{i-1}Q_{i+1} \dots Q_n)$$

Since $F[t]$ is an integral domain, by the cancellation property, we see that

$$P_2 = \alpha Q_1 \dots Q_{i-1}Q_{i+1} \dots Q_n.$$

Since P_2 is irreducible, we must have $n = 2$ as otherwise P_2 cannot be irreducible. Hence, after relabeling the Q_j, we have $P = Q_1Q_2$ with $\alpha P_1 = Q_1$ and $P_2 = \alpha Q_2$.

For $r_P > 2$, we assume that we have two factorizations of P into a product of irreducible polynomials

$$P = P_1 \dots P_{r_P} = Q_1 \dots Q_n$$

where $n \geq r_P$. Since $P \in \langle P_1 \rangle$ and $\langle P_1 \rangle$ is a prime ideal, we must have $Q_i \in \langle P_1 \rangle$ for some $1 \leq i \leq n$. As before, since Q_i is irreducible, we deduce that there exists $\alpha \in F$ such that $\alpha P_1 = Q_i$. Relabeling the Q_j, we will assume that $i = 1$. Using the cancellation property, we have

$$P' = P_2 \dots P_{r_P} = \alpha Q_2 \dots Q_n.$$

By the induction hypothesis, $n-1 = r_P - 1$ and so $n = r_P$. Additionally, after relabeling the Q_j, we have $\alpha_i P_i = Q_i$ for $i > 2$ and $\alpha^{-1}\alpha_2 P_2 = Q_2$.

Theorem 2.30 (Factorization)**.** *Let F be a field $P \in F[t]$ with $\deg(P) > 0$. Then there exist irreducible polynomials $P_1, \dots, P_{r_P} \in F[t]$ with $0 < \deg(P_i) \leq \deg(P)$, and are unique up relabeling and multiplication by F, such that $P = P_1 \dots P_{r_P}$. Moreover, if $\deg(P) = \deg(P_i)$ for some i, then $r_P = 1$ and $P = P_1$. In particular, if P is not irreducible, $\deg(P_i) < \deg(P)$ for all i.*

We refer the reader to Exercise 2.5 for the definition of the ideal $\mathfrak{a}_1\mathfrak{a}_2$ for ideals $\mathfrak{a}_1, \mathfrak{a}_2$.

Corollary 2.31. *Given a non-trivial, proper ideal $\mathfrak{a} \lhd F[t]$, there exist unique (up to relabeling) prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_{r_\mathfrak{a}}$ such that $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_{r_\mathfrak{a}}$.*

Exercise 2.60. *Prove Corollary 2.31. [Hint: Use the fact that $\mathfrak{a}$ is principal and apply Theorem 2.30 to the generating polynomial.]*

Exercise 2.61. *Let F be a field.*

(i) Prove that if $P \in F[t]$ and $\deg(P) = 1$, then P is irreducible.

(ii) Prove that if $P \in F[t]$ and $\alpha \in F$ such that $P(\alpha) = 0$, then $P(t) = Q(t)(t-\alpha)$ for some $Q \in F[t]$.

(iii) Prove that if $P \in F[t]$ and $2 \leq \deg(P) \leq 3$, then P is irreducible over F if and only if $P(\alpha) \neq 0$ for all $\alpha \in F$.

(iv) Show that (ii) is false if $\deg(P) > 3$.

Definition 2.33 (Splitting Field)**.** *Let F be a field and $P \in F[t]$. We say that an extension E/F is a **splitting field** for P if $P = P_1 \dots P_n$ for $P_1, \dots, P_n \in E[t]$ with $\deg(P_i) = 1$. If E/F is a splitting field for P, we will say that P **splits** over E.*

We record the following lemma. We leave the proof to the reader.

Lemma 2.32. *Let F be a field and $P \in F[t]$. Then an extension E/F is a splitting field for P if and only if there exist $\alpha, \alpha_1, \dots, \alpha_{\deg(P)} \in E$ such that*

(a) $P(\alpha_i) = 0$ for $i = 1, \dots, \deg(P)$.

(b)

$$P(t) = \alpha \prod_{i=1}^{\deg(P)} (t - \alpha_i).$$

Exercise 2.62. *Prove Lemma 2.32.*

Theorem 2.33. *If F is a field and $P \in F[t]$ with $\deg(P) > 0$, then there exists a finite extension E/F such that E is a splitting field for P.*

Proof. We assume that $\deg(P) = n$. By Theorem 2.30, we can express $P = P_1 \dots P_{r_P}$ of irreducible polynomials $P_i \in F[t]$ and with $0 < \deg(P_i) \leq n$. If all of the P_i have degree 1, we set $E = F$. Otherwise, we select some P_j with $\deg(P_j) > 1$, we know that $\mathfrak{P}_j = \mathfrak{m}_j$ is a maximal ideal and $E_1 = E_{\mathfrak{m}_j} = F[t]/\mathfrak{m}_j$ is an extension of F of degree $\deg(P_j) \leq n$. By Corollary 2.29, there exists $\beta_1 \in E_1$ such that $P_i(\beta_1) = 0$. In particular, over E_1, we see that $P_i(t) = Q_i(t)(t - \beta_1)$. Applying Theorem 2.30 to P over the field E_1, we obtain

$$P = (t - \beta_1) \prod_{i=1}^{r_2} P_{1,i}$$

where $P_{1,i} \in E_1[t]$ are irreducible over E_1 and $0 < \deg(P_{1,i}) \leq n - 1$. If $\deg(P_{1,i}) = 1$ for all of the $P_{1,i}$, we can take $E = E_1$. Otherwise, we continue as in the first step and produce a finite extension E_2/E_1 such that

$$P = (t - \beta_1)(t - \beta_2) \prod_{i=1}^{r_2} P_{2,i}$$

where $\beta_2 \in E_2$, $P_{2,i} \in E_2[t]$ are irreducible over E_2, and $0 < \deg(P_{2,i}) \leq n - 2$. At the ℓ stage of this process, we will obtain an extension $E_\ell/E_{\ell-1}$ and a factorization

$$P = (t - \beta_1)(t - \beta_2) \dots (t - \beta_\ell) \prod_{i=1}^{r_\ell} P_{\ell,i}$$

where $\beta_j \in E_j$, $P_{\ell,i} \in E_\ell[t]$ are irreducible over E_ℓ, and $0 < \deg(P_{\ell,i}) \leq n - \ell$. Hence by the $n - 1$ stage, we will have an extension E_{n-1}/F that will be a splitting field for P. ♠

Taking $E_0 = F$ in the proof of Theorem 2.33, we see that $[E_{j+1}, E_j] \leq n - j$ and so

$$[E_{n-1} : F] = [E_{n-1} : E_0] = \prod_{j=0}^{n-2} [E_{j+1}, E_j] = \prod_{j=0}^{n-1} (n - j) = n!.$$

In fact, we have a more refined upper bound on this degree. If $P = P_1 \dots P_{r_P}$ where $P_i \in F[t]$ are irreducible over F and $\deg(P_i) = n_i \leq n!$, we have a splitting field E of P with

$$[E : F] \leq \prod_{i=1}^{r_P} n_i!.$$

We record this as a corollary as it can be useful in practice.

Corollary 2.34. *Let F be a field and $P \in F[t]$ such that $P = P_1 \dots P_{r_P}$ where $P_i \in F[t]$ and irreducible over F and $n_i = \deg(P_i)$. Then there exists a splitting field E/F of P such that*

$$[E : F] \leq \prod_{i=1}^{r_P} n_i!.$$

The following (tangential) exercises shows that our refinement in Corollary 2.34 is strictly better.

Exercise 2.63. *Let $n, n_1, \dots, n_j \in \mathbf{N}$ such that $n = \sum_{i=1}^{j} n_i$. Prove that $\prod_{i=1}^{j} n_i! \leq n!$ with equality if and only if $j = 1$.*

As an example, assume that we have a polynomial $P \in F[t]$ such that $P = P_1 P_2$ for irreducible $P_1, P_2 \in F[t]$ and with $\deg(P_1) = 2$ and $\deg(P_2) = 2$. In this case, $\deg(P) = \deg(P_1) + \deg(P_2) = 4$. According Corollary 2.34, we have a splitting field E/F of degree at most 4. However, for a general degree 4 polynomial, the minimal degree of a splitting field can be as large as $24 = 4!$. In fact, the minimal degree of a splitting field for P in the case $P = P_1 P_2$ and $\deg(P_1) = \deg(P_2)$ is either 2, or 4 under our assumption that P_1, P_2 are irreducible. For instance if $P = (t^2 - 2)(t^2 - 3)$ viewed as a polynomial in $\mathbf{Q}[t]$, the field $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field for P and has degree 4. However, $P = (t^2 - 2)(t^2 - 8)$ has $\mathbf{Q}(\sqrt{2})$ as a splitting field. The reason the degree is smaller in this second case is that both $t^2 - 2$ and $t^2 - 8$ have $\mathbf{Q}(\sqrt{2})$ as a splitting field. In our first example, the splitting fields of $t^2 - 2$ and $t^2 - 3$ are distinct.

Exercise 2.64. *Let $P_1(t) = t^2 - 2$, $P_2(t) = t^2 - 8$, and $P_3(t) = t^2 - 3$.*

(i) Prove that P_1, P_2, P_3 are irreducible over $\mathbf{Q}$.

(ii) Prove that $\mathbf{Q}(\sqrt{2})$ is a splitting field for P_1, P_2.

(iii) Prove that P_3 is irreducible over $\mathbf{Q}(\sqrt{2})$.

Exercise 2.65. *Let F be a field and $P \in F[t]$ with $\deg(P) = 2$ and $P(t) = at^2 + bt + c$ for $a, b, c \in F$.*

*(i) Prove that P is irreducible over F if and only if $b^2 - 4ac$ is not a square in F. That is, if $b^2 - 4ac \neq \alpha^2$ for some $\alpha \in F$. We call $b^2 - 4ac = \Delta(P)$ the **discriminant** of P. [Hint: **Completing the square**]*

(ii) Prove that if $P_1 \in F[t]$ is irreducible with $\deg(P_1) = 2$ and $\Delta(P_1) = \alpha^2 \Delta(P)$ for some $\alpha \in F$, then P_1 splits over an extension E/F if and only if P splits over E/F.

(iii) Prove that if E/F is degree two, then there exists $\alpha \in F$ such that α is not a square in F and $E = F(\sqrt{\alpha})$.

Exercise 2.66. *Let $P_1, P_2 \in F[t]$ be irreducible polynomials with $\deg(P_1) = \deg(P_2) = 2$.*

(i) *Prove that P_i splits over $F(\sqrt{\Delta(P_i)})$ and $[F(\sqrt{\Delta(P_i)}) : F] = 2$. [Hint: Exercise 2.65]*

(ii) *Prove that $P = P_1P_2$ has a splitting field E/F with $[E : F] = 2$ if and only if there exists an extension E'/F with $[E' : F] = 2$ such that E' is a splitting field for both P_1, P_2.*

(iii) *Prove that P_2 splits over the splitting field of P_1 if and only if $\sqrt{\Delta(P_2)}$ is a square in $F(\sqrt{\Delta(P_1)})$.*

***Remark* 2.35.** *The construction of the splitting field in the proof of Theorem 2.33 can be viewed as follows. We factor our polynomial P into a product of irreducible polynomials $P = P_1 \dots P_{r_P}$. For each P_i, we construct a splitting field E_i with the fields $E_{P_i} = F[t]/\langle P_i \rangle$; note we might need to take a series of extensions of this type for each P_i since E_{P_i} is not necessarily a splitting field for P_i. Finally, we can take E to be the composite field $E_1 \dots E_{r_P}$ as a splitting field for P.*

We note that once we have a finite extension E/F which is a splitting field for $P \in F[t]$, we can take $F_P = F(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n \in E$ are all of the roots of P. For future reference, we let $\text{Roots}(P) = \{\alpha_1, \dots, \alpha_n\}$. We postpone proving that F_P is unique until the next chapter when we will further investigate splitting fields of polynomials.

***Definition* 2.34** (Algebraically Closed Field)**.** *We say that a field E is **algebraically closed** if every $P \in E[t]$ splits over E.*

***Theorem* 2.36.** *Let E be a field. Then the following are equivalent:*

(a) *E is algebraically closed.*

(b) *If E'/E is an algebraic extension of fields, then $E = E'$.*

(c) *If E'/E is a finite extension of fields, then $E = E'$*

(d) *For each $P \in E[t]$ with $\deg(P) > 0$, there exists $\alpha \in E$ such that $P(\alpha) = 0$.*

Proof. For (a) implies (b), we will assume E is algebraically closed and need to prove that any algebraic extension E'/E is trivial. Given $\beta \in E'$, since E' is algebraic, there exists an integer $n \in \mathbf{N}$ such that $\{1, \beta, \beta^2, \dots, \beta^{n-1}\}$ is linearly independent but $\{1, \beta, \dots, \beta^n\}$ is linearly dependent. By definition of linear dependence, there exist $\lambda_0, \dots, \lambda_n \in E$ such that

$$\sum_{i=0}^{n} \lambda_i \beta^i = 0.$$

Let

$$P(t) = \sum_{i=0}^{n} \lambda_i t^i.$$

By (a), we see that

$$P(t) = \alpha(t-\alpha_1)(t-\alpha_2)\dots(t-\alpha_n)$$

for some $\alpha, \alpha_1, \dots, \alpha_n \in E$ with $\alpha \neq 0$. Since $P(\beta) = 0$, we see that

$$\alpha(\beta-\alpha_1)(\beta-\alpha_2)\dots(\beta-\alpha_n) = 0.$$

Since E is an integral domain, we must have $\beta - \alpha_i = 0$ for some i, and so $\beta = \alpha_i \in E$. As $\beta \in E'$ was arbitrary, we see that $E = E'$.

For (b) implies (c), by Exercise 2.15, every finite extension is algebraic, and so (c) follows from (b).

For (c) implies (d), we must show that any $P \in E[t]$ with $\deg(P) > 0$ has a zero in E. By Theorem 2.30, we have $P = P_1 \dots P_{r_P}$ where each $P_i \in E[t]$ is irreducible and $0 < \deg(P_i) \leq \deg(P)$. For each i, the field $E_i = E[t]/\langle P_i \rangle$ is an extension of degree $\deg(P_i)$ and so $E_i = E$ by (c). By Corollary 2.29, there exists $\beta_i \in E_i = E$ such that $P_i(\beta_i) = 0$. Hence $P(\beta_i) = 0$ and so P has a zero in E.

For (d) implies (a), given $P \in E[t]$, by Theorem 2.30, we have $P = P_1 \dots P_{r_P}$ such that $P_i \in E[t]$ are irreducible and $0 < \deg(P_i) \leq \deg(P)$. For each i, by our assumption (d), there exists $\beta_i \in E$ such that $P_i(\beta_i) = 0$ and so by Exercise 2.61, we have $P_i = (t-\beta_i)Q_i$. Since $\deg(t-\beta_i) = 1$, we must have $\deg(Q_i) = 0$ and so $\deg(P_i) = 1$. Hence, we see that (a) holds. ♠

We conclude this section with the construction of an algebraically closed extension E/F for any field E. Our construction will produce an extension $\overline{F}/F$ where $\overline{F}$ is called the algebraic closure of F. We will require the following result in our construction of the algebraic closure of F.

Proposition 2.37. *Let F be a field and E/F be an algebraic extension of F such that every polynomial $P \in F[t]$ splits over E. Then E is algebraically closed.*

Proof. By Theorem 2.36, will show that every polynomial $P \in E[t]$ has a zero in E. By Theorem 2.30, we have $P = P_1 \dots P_{r_P}$ such that $P_i \in E[t]$ are irreducible and $0 < \deg(P_i) \leq \deg(P)$. By Corollary 2.29, $E' = E[t]/\langle P_1 \rangle$ is a finite extension and there exists $\beta \in E'$ such that $P_1(\beta) = 0$. Writing

$$P_1(t) = \sum_{i=0}^{n_1} \lambda_i t^i$$

for $\lambda_i \in E$, since E/F is algebraic, we know that $F_1 = F(\lambda_0, \dots, \lambda_{n_1})$ is a finite extension of F and $P_1 \in F_1[t]$. Since P_1 is irreducible over E, it is irreducible over F_1. Taking $F_2 = F_1(\beta) = F_1[t]/\langle P_1 \rangle$, by Corollary 2.29, F_2/F_1 is a finite extension. As F_2/F_1 and F_1/F are finite extensions, F_2/F is a finite

extension and hence algebraic. Since $\beta \in F_2$, by Corollary 2.12, there exists a polynomial $Q \in F[t]$ such that $Q(\beta) = 0$. Since Q splits over E, we know that

$$Q = (t - \beta_1) \dots (t - \beta_m)$$

where $\beta_i \in E$. As β is a zero of Q, we conclude that $\beta = \beta_i$ for some i and so $\beta \in E$. In particular, P has a zero in E and so by Theorem 2.36, E is algebraically closed. ♠

An algebraically closed, algebraic extension E/F will be called an **algebraic closure** of F. Though we will not prove it here, it is unique up to field isomorphisms and so we will denote any such extension simply by $\overline{F}$. Using Proposition 2.37, we will now construct an algebraically closed, algebraic extension of F. Given F, if F is algebraically closed, we set $\overline{F} = F$. Otherwise, there exists a polynomial $P_1 \in F[t]$ which does not split over F. By Theorem 2.33, there exists a finite extension E_1/F such that P_1 splits over E_1. If every polynomial in $F[t]$ splits over E_1, we set $\overline{F} = E_1$. Otherwise, there exists a polynomial $P_2 \in F[t]$ which does not split over E_1. By Theorem 2.33, there exists a finite extension E_2/E_1 such that P_2 splits over E_2. If every polynomial in $F[t]$ splits over E_2, we set $\overline{F} = E_2$. Otherwise, we continue this process producing a sequence of algebraic extensions E_τ/F in which more and more polynomials in $F[t]$ split over E_τ. Using **Zorn's Lemma**, we can produce $\overline{F}$, an algebraic extension of F. Since every polynomial in $F[t]$ splits over $\overline{F}$, by Proposition 2.37, $\overline{F}$ is algebraically closed.

***Theorem* 2.38** (Algebraic Closure)**.** *Let F be a field. Then there exists an algebraic, algebraically closed extension $\overline{F}/F$ of F.*

By the **Fundamental Theorem of Algebra**, $\mathbf{C}$ is an algebraically closed field. $\mathbf{C}$ is the algebraic closure of $\mathbf{R}$ but is not the algebraic closure of $\mathbf{Q}$. Indeed, $\pi \in \mathbf{C}$ is not algebraic and so $\mathbf{C}/\mathbf{Q}$ is not an algebraic extension. The algebraic closure of $\mathbf{Q}$, denoted by $\overline{\mathbf{Q}}$, is a subfield of $\mathbf{C}$ but is considerably smaller than $\mathbf{C}$. In fact, $\overline{\mathbf{Q}}$ is countable while $\mathbf{C}$ is not!

***Exercise* 2.67.** *Let E/F be a finite extension. Prove that $\overline{F}$ is an algebraic closure for E. [Hint: Prove that there is a field homomorphism $E \to \overline{F}$]*

As a result of Exercise 2.67, when E/F is finite, we can take $\overline{E}$ to be $\overline{F}$.

Chapter 3

Fields: Galois Theory

In this chapter, we will introduce the concept of a Galois extension of a field F and its associated Galois group. Before laying out this topic rigorously, we delve into a special, well-known example. Given $P \in \mathbf{Q}[t]$ with $\deg(P) = 2$ and $P(t) = at^2 + bt + c$, we will assume that $\Delta(P) = b^2 - 4ac$ is not a square in $\mathbf{Q}$. In particular, by Exercise 2.65, P is irreducible over $\mathbf{Q}$. By the **quadratic formula**, we know that the zeroes of P are given by

$$\beta_{\pm} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b}{2a} \pm \frac{\sqrt{\Delta(P)}}{2a}.$$

Hence, $E = \mathbf{Q}(\sqrt{\Delta(P)})$ is the splitting field for P. Every element $\beta \in E$ can be expressed uniquely as $\alpha_1 + \alpha_2\sqrt{\Delta(P)}$. The function $\sigma\colon E \to E$ defined by

$$\sigma(\alpha_1 + \alpha_2\sqrt{\Delta(P)}) = \alpha_1 - \alpha_2\sqrt{\Delta(P)}$$

is an $\mathbf{Q}$–linear function. In fact, it is an $\mathbf{Q}$–algebra automorphism. To see this, we have

$$\begin{aligned}\sigma(\beta_1\beta_2) &= \sigma((\alpha_1 + \alpha_2\sqrt{\Delta(P)})(\alpha_3 + \alpha_4\sqrt{\Delta(P)})) = \sigma((\alpha_1\alpha_3 + \Delta(P)\alpha_3\alpha_4) + (\alpha_1\alpha_4 + \alpha_2\alpha_3)\sqrt{\Delta(P)}) \\ &= (\alpha_1\alpha_3 + \Delta(P)\alpha_2\alpha_4) - (\alpha_1\alpha_4 + \alpha_2\alpha_3)\sqrt{\Delta(P)} \\ &= (\alpha_1 - \alpha_2\sqrt{\Delta(P)})(\alpha_3 - \alpha_4\sqrt{\Delta(P)}).\end{aligned}$$

We see that $\sigma(\beta_{\pm}) = \beta_{\mp}$ and that $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbf{Q}$. In fact, if we have a $\mathbf{Q}$–algebra isomorphism $\sigma\colon E \to E$, we must have $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbf{Q}$ and $\sigma(\beta_{\pm}) = \beta_{\mp}$. In total, we see that $\{1, \sigma\}$, which is a group of order two, is a subgroup of $\mathrm{Aut}_{\mathbf{Q}\text{–alg}}(E) \leq \mathrm{Aut}_{\mathbf{Q}\text{–lin}}(E)$ and acts transitively on $\mathrm{Roots}(P)$. In fact, $\{1, \sigma\} = \mathrm{Aut}_{\mathbf{Q}\text{–alg}}(E)$ and $\left|\mathrm{Aut}_{\mathbf{Q}\text{–alg}}(E)\right| = [E : \mathbf{Q}]$.

Unfortunately, this does not extend to every finite extension $E/\mathbf{Q}$. For instance, $E = \mathbf{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbf{Q}$. The main issue with this extension E is that it does not contain all of the zeroes of $P(t) = t^3 - 2$. In fact, it contains only $\sqrt[3]{2}$ and so any F–algebra automorphism of E must fix $\sqrt[3]{2}$.

3.1 *Extension Fields: Automorphisms of Extensions*

The main focus of this section is the group of F–algebra automorphisms of an extension E/F. Typically, this group is viewed as the field automorphisms of E that fix F point-wise. As these automorphisms are precisely the F–algebra automorphisms of E, we have opted for the latter view.

***Definition* 3.1.** *Let F be a field and E/F an extension of fields. We define $\mathrm{Aut}_{F-alg}(E)$ to be the group of F–algebra automorphisms of E.*

By definition of an F–algebra homomorphism, we see that $\mathrm{Aut}_{F-\mathrm{alg}}(E) \leq \mathrm{Aut}_{F-\mathrm{lin}}(E)$.

***Exercise* 3.1.** *Prove that $\mathrm{Aut}_{F-alg}(E)$ is a group with group operation given by composition. Specifically, prove that the composition of F–algebra automorphisms of E is an F–algebra automorphism of E and that the inverse function of an F–algebra automorphism of E is also an F–algebra automorphism.*

Our first observation is the following.

***Lemma* 3.1.** *Let $\sigma \in \mathrm{Aut}_{F-alg}(E)$. Then $\sigma(\alpha) = \alpha$ for all $\alpha \in F$.*

Proof. Given an F–algebra automorphism σ of E, we know that $\sigma(1) = 1$ and $\sigma(\alpha\beta) = \alpha\sigma(\beta)$ for every $\alpha \in F$ and $\beta \in E$. Since $\sigma(\alpha) = \sigma(\alpha 1) = \alpha\sigma(1) = \alpha$ for any $\alpha \in F$, we see the lemma holds. ♠

***Lemma* 3.2.** *Let E/F be an extension and $\beta \in E$ be a zero of a polynomial $P \in F[t]$. If $\sigma \in \mathrm{Aut}_{F-alg}(E)$, then $\sigma(\beta)$ is also a zero of P.*

Proof. Let

$$P(t) = \sum_{i=0}^{n} \lambda_i t^i$$

where $\lambda_i \in F$. Since σ is an F–algebra homomorphism and fixes F point-wise, we see that

$$P(\sigma(\beta)) = \sum_{i=0}^{n} \lambda_i \sigma(\beta)^i = \sigma\left(\sum_{i=0}^{n} \lambda_i \beta^i\right) = \sigma(P(\beta)) = 0.$$

Hence $\sigma(\beta) \in \mathrm{Roots}(P)$. ♠

Lemma 3.2 is a big reason for having an interest in the group $\mathrm{Aut}_{F\text{–alg}}(E)$.

***Lemma* 3.3.** *Let E/F be a finite extension. Then $\mathrm{Aut}_{F\text{–}alg}(E)$ is a finite group.*

Proof. Since E/F is finite, there exists a finite F–linear basis $\mathscr{B} = \{1, \beta_2, \ldots, \beta_n\}$. For each β_i, by Corollary 2.12, there exists a monic polynomial $P_i \in F[t]$ such that $P_i(\beta_i) = 0$. Since $\mathscr{B}$ is an F–linear basis, any $\sigma \in \mathrm{Aut}_{F\text{–alg}}(E)$ is uniquely determined by the values $\sigma(\beta_i) \in E$. By Lemma 3.2, we know that $\sigma(\beta_i) \in \mathrm{Roots}(P_i)$ and that $\mathrm{Roots}(P_i)$ is finite. In particular, we see that

$$\mathrm{Aut}_{F\text{–alg}}(E) \leq \prod_{i=2}^{n} \mathrm{Aut}_{\mathrm{set}}(\mathrm{Roots}(P_i)) = \prod_{i=2}^{n} \mathrm{Sym}(\mathrm{Roots}(P_i))$$

and so by Exercise 1.25 and Exercise 1.29, we have

$$\left|\mathrm{Aut}_{F\text{–alg}}(E)\right| \leq \prod_{i=2}^{n} |\mathrm{Roots}(P_i)|! = \prod_{i=2}^{n} (\deg(P_i))!.$$

♠

***Lemma* 3.4.** *Let E/F be an extension of fields and $H \leq \mathrm{Aut}_{F\text{–}alg}(E)$ be a subgroup. If*

$$E^H \stackrel{def}{=} \{\beta \in E \ : \ \sigma(\beta) = \beta \text{ for all } \sigma \in H\},$$

then E^H is a field and E^H/F is an extension.

Proof. According to Lemma 3.1, we know that $F \subset E^H$ and so it suffices to prove that E^H is a field. Given $\beta, \beta_1, \beta_2 \in E^H$, we must prove that $\beta^{-1} \in E^H$ and $\beta_1 + \beta_2 \in E^H$. For the former, for any $\sigma \in H$, we have

$$\sigma(\beta^{-1}) = (\sigma(\beta))^{-1} = \beta^{-1}.$$

Hence, $\sigma(\beta^{-1}) = \beta^{-1}$ and so by definition of E^H, we have $\beta^{-1} \in E^H$. For the latter, for any $\sigma \in H$, we have

$$\sigma(\beta_1 + \beta_2) = \sigma(\beta_1) + \sigma(\beta_2) = \beta_1 + \beta_2.$$

Hence, $\sigma(\beta_1 + \beta_2) = \beta_1 + \beta_2$ and so by definition of E^H, we have $\beta_1 + \beta_2 \in E^H$. ♠

Given an extension of fields E/F, a subfield K of E that contains F will be called an **intermediate field**. Note that K/F and E/K are extensions of fields.

***Lemma* 3.5.** *Let E/F be an extension of fields and $E \leq K \leq E$ be an intermediate field. If*

$$H_K \stackrel{def}{=} \left\{\sigma \in \mathrm{Aut}_{F\text{–}alg}(E) \ : \ \sigma(\lambda) = \lambda \text{ for all } \lambda \in K\right\},$$

then $H_K \leq \mathrm{Aut}_{F\text{–}alg}(E)$ is a subgroup.

Proof. First, the identity function $\mathrm{Id}_E : E \to E$ is the identity element in $\mathrm{Aut}_{F\text{–alg}}(E)$ and $\mathrm{Id}_E(\lambda) = \lambda$ for all $\lambda \in E$. Hence $\mathrm{Id}_E \in H_K$. Given $\sigma, \sigma_1, \sigma_2 \in H_K$, we must prove that $\sigma^{-1} \in H_K$ and $\sigma_1\sigma_2 \in E_H$. For the former, since $\sigma \in H_K$, for any $\lambda \in K$, we see that

$$\sigma^{-1}(\lambda) = \sigma^{-1}(\sigma(\lambda)) = \lambda.$$

Likewise, we have

$$\sigma_1(\sigma_2(\lambda)) = \sigma_1(\lambda) = \lambda.$$

Hence, H_K is a subgroup of $\mathrm{Aut}_{F\text{–alg}}(E)$. ♠

The following exercise shows that H_K is, in fact, nothing more than $\mathrm{Aut}_{K\text{–alg}}(E)$.

Exercise 3.2. *Let E/F be an extension and $F \leq K \leq E$.*

(i) Prove that if $\sigma \in H_K$, then σ is a K–algebra automorphism of E. In particular, we have a group homomorphism $\psi : H_K \to \mathrm{Aut}_{K\text{–}alg}(E)$.

(ii) Prove that ψ is injective.

(iii) Prove that ψ is surjective.

We will largely use our notation H_K instead of $\mathrm{Aut}_{K\text{–alg}}(E)$ though it may be helpful for the reader at points to remember that these two groups are the same.

Lemma 3.6. *Let E/F be an extension of fields.*

(a) If $H_1 \leq H_2 \leq \mathrm{Aut}_{F\text{–}alg}(E)$, then $E^{H_2} \leq E^{H_1}$.

(b) If K_1, K_2 are intermediate fields with $K_1 \leq K_2$, then $H_{K_2} \leq H_{K_1}$.

Proof. For (a), given $\beta \in E^{H_2}$, by definition, for each $\sigma \in H_2$, we have $\sigma(\beta) = \beta$. Since $H_1 \leq H_2$, we see that $\beta \in E^{H_1}$. For (b), given $\sigma \in H_{K_2}$, by definition, for each $\lambda \in K_2$, we have $\sigma(\lambda) = \lambda$. Since $K_1 \leq K_2$, we see that $\sigma \in H_{K_1}$. ♠

3.2 *Extension Fields: Automorphisms of Splitting Fields*

Before proceeding to a rather general setting where we will discuss in more detail the correspondences above, we consider a fairly concrete class of examples arising from splitting fields of polynomials.

Though somewhat specific, we will see that these examples are central to Galois theory. Indeed, Galois extensions are precisely the splitting fields of a collection of polynomials; this will be one of the main results of this chapter.

Our present goal is to prove the following:

Theorem 3.7. *Let F be a field, $P \in F[t]$ an irreducible polynomial and E/F be a splitting field for P. Then given $\beta_1, \beta_2 \in \text{Roots}(P)$, there exists $\sigma \in \text{Aut}_{F-alg}(E)$ such that $\sigma(\beta_1) = \beta_2$.*

We will need to establish some preliminary results in order to prove Theorem 3.7. Given an irreducible polynomial $P \in F[t]$ and an extension E/F where P splits over E, we will prove that if $\beta_1, \beta_2 \in \text{Roots}(P) \subset E$, then $F(\beta_1), F(\beta_2)$ are isomorphic as F–algebras.

Lemma 3.8. *Let $P \in F[t]$ be irreducible over F and E/F be an extension of fields such that P splits over E. If $\beta_1, \beta_2 \in \text{Roots}(P) \subset E$, then there exists an F–algebra isomorphism $\psi\colon F(\beta_1) \to F(\beta_2)$.*

Proof. Since P is the minimal polynomial of β_1, β_2 over F, we see that

$$\mathfrak{m}_1 = \{Q \in F[t] \ : \ Q(\beta_1) = 0\} = \langle P \rangle$$

and

$$\mathfrak{m}_2 = \{Q \in F[t] \ : \ Q(\beta_2) = 0\} = \langle P \rangle .$$

Since $\mathfrak{m}_i = \ker(\text{Eval}_{\beta_i})$, by the First Ring Isomorphism, we have $F[t]/\ker(\text{Eval}_{\beta_1}) \cong F[t]/\ker(\text{Eval}_{\beta_2})$. Of course $\text{Eval}_{\beta_i}(F[t]) = F(\beta_i)$ and so $F(\beta_1) \cong F(\beta_2)$. By Scholium 2.28, we know that $\left\{1, \beta_1, \ldots, \beta_1^{m-1}\right\}$ and $\left\{1, \beta_2, \ldots, \beta_2^{m-1}\right\}$ are F–bases for $F(\beta_1)$ and $F(\beta_2)$, respectively, where $m = \deg(P)$. In particular, every element $\beta \in F(\beta_j)$ can be expressed uniquely by

$$\beta = \sum_{i=0}^{m-1} \alpha_i \beta_j^i$$

where $\alpha_i \in F$. It is straightforward to prove that $\psi\colon F(\beta_1) \to F(\beta_2)$ given by

$$\psi\left(\sum_{i=0}^{m-1} \alpha_i \beta_1^i\right) = \sum_{i-0}^{m-1} \alpha_i \beta_2^i$$

is an isomorphism of F–algebras. ♠

We need a more general version of Lemma 3.8. We leave the deduction of this result to the reader in the following guided exercise.

Exercise 3.3. *Given a pair of fields F, F' and an isomorphism of fields $\psi\colon F \to F'$, we define $\psi_*\colon F[t] \to F'[t]$ by*

$$\psi_*\left(\sum_{i=0}^{m} \alpha_i t^i\right) = \sum_{i=0}^{m} \psi(\alpha_i) t^i.$$

(i) Prove that ψ_* is an isomorphism of F–algebras.

(ii) Identifying $F, F' \leq F[t], F'[t]$ as the field of constant functions, prove that the restriction of ψ_* to F is equal to ψ. That is

$$\begin{array}{ccc} F[t] & \xrightarrow{\psi_*} & F'[t] \\ {\scriptstyle \iota_F}\uparrow & & \uparrow{\scriptstyle \iota_{F'}} \\ F & \xrightarrow[\psi]{} & F' \end{array}$$

is a commutative diagram where $\iota_F, \iota_{F'}$ are isomorphisms with the fields of constant polynomials.

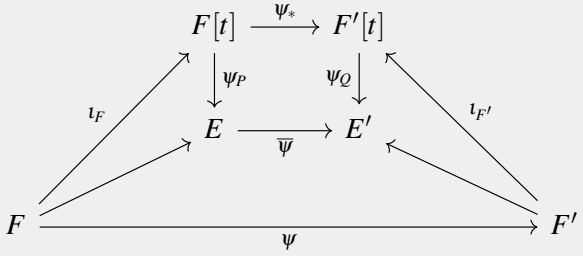
(iii) Prove that if $P \in F[t]$ is irreducible, then $\psi_*(P) \in F'[t]$ is irreducible.

(iv) Given $P \in F[t]$ with $Q = \psi_*(P)$, prove that there exists a ring isomorphism $\overline{\psi}\colon F[t]/\langle P\rangle \to F'[t]/\langle Q\rangle$ such that the diagram

$$\begin{array}{ccc} F[t] & \xrightarrow{\psi_*} & F'[t] \\ {\scriptstyle \psi_P}\downarrow & & \downarrow{\scriptstyle \psi_Q} \\ F[t]/\langle P\rangle & \xrightarrow[\overline{\psi}]{} & F'[t]/\langle Q\rangle \end{array}$$

where ψ_P and ψ_Q are the canonical homomorphisms (i.e. quotient homomorphisms). [Hint: Exercise 2.38]

(v) Let $P \in F[t]$ be irreducible, $Q = \psi_*(P) \in F'[t]$, $E = F[t]/\langle P\rangle$ and $E' = F'[t]/\langle Q\rangle$. Prove that there exists a field isomorphism $\widetilde{\psi}\colon E \to E'$ such that $\widetilde{\psi}$ restricted to $F \leq E$ is ψ. In particular, we have the commutative diagram



We next prove a fairly general result that we will use to prove Theorem 3.7.

Theorem 3.9. *Let F, F' be fields and $\psi\colon F \to F'$ an isomorphism of fields. If $P \in F[t]$, $Q = \psi_*(P)$, and E/F, E'/F' are splitting fields for P, Q, respectively, then there exists an isomorphism $\widetilde{\psi}\colon E \to E'$ such that the restriction of $\widetilde{\psi}$ to F is ψ.*

Proof. We will prove this via induction on $[E : F]$. If $[E : F] = 1$, then P splits over F. It follows that Q splits over F' and we can take $\widetilde{\psi} = \psi$. We will assume that the result holds for all fields F and all polynomials $P \in F[t]$ with $[E : F] < n$. We must show that the result holds when $[E : F] = n$. Factoring P in $F[t]$, we have $P = P_1 \dots P_{r_P}$ with associated factorization $Q = Q_1 \dots Q_{r_P}$, where $\psi_*(P_i) = Q_i$. Since $n > 1$, we know that at least one of the P_i must have degree strictly larger than 1. Relabelling the P_i if necessary, we will assume that P_1 has degree greater than 1. By Exercise 3.3, there exists an isomorphism $\psi_1\colon F(\beta) \to F'(\beta')$ where $\beta \in \text{Roots}(P_1)$ and $\beta' \in \text{Roots}(Q_1)$ that extends ψ. Viewing $P \in F(\beta)[t]$, since $[E : F] = [E : F(\beta)][F(\beta) : F]$ and $[F(\beta) : F] = \deg(P_1)$, we see that $[E : F(\beta)] < [E : F]$. Applying our induction hypothesis for $E/F(\beta)$, we obtain the desired isomorphism $\widetilde{\psi}$. Since $\widetilde{\psi}$ extends ψ_1 which is an extension of ψ, we see that $\widetilde{\psi}$ extends ψ. ♠

Taking $F = F'$ and $\psi = \text{Id}_F$, we see that the splitting field of P is unique.

Proof of Theorem 3.7. We take $F = F'$ and $\psi = \text{Id}_F$. Given $\beta_1, \beta_2 \in \text{Roots}(P)$, by Lemma 3.8, there exists an isomorphism $\psi\colon F(\beta_1) \to F(\beta_2)$ that is the identity on F with $\psi(\beta_1) = \beta_2$. By Theorem 3.9, there is an extension $\widetilde{\psi}\colon E \to E$. Taking $\sigma = \widetilde{\psi}$ completes the proof. ♠

An immediate corollary of Theorem 3.7 is the following.

Corollary 3.10. *Let F be a field, $P \in F[t]$ an irreducible polynomial, and E/F the splitting field of P. Then $\text{Aut}_{F-alg}(E)$ acts transitively on $\text{Roots}(P)$.*

We also have another corollary of Theorem 3.7.

Corollary 3.11. *Let F be a field, $P \in F[t]$ an irreducible polynomial, and E/F the splitting field of P. Then there exists an injective group homomorphism $\psi\colon \text{Aut}_{F-alg}(E) \to \text{Sym}(\text{Roots}(P))$ such that the image is a transitive subgroup of $\text{Sym}(\text{Roots}(P))$.*

Proof. Since $E = F(\text{Roots}(P))$, we see that if $\sigma \in \text{Aut}_{F-\text{alg}}(E)$ and $\sigma(\beta) = \beta$ for all $\beta \in \text{Roots}(P)$, then $\sigma = \text{Id}_E$. The action of $\text{Aut}_{F-\text{alg}}(E)$ on $\text{Roots}(P)$ induces a group homomorphism $\psi\colon \text{Aut}_{F-\text{alg}}(E)$ and ψ is injective by the previous sentence. ♠

3.3 *Extension Fields: Galois Connections, I*

From the first section of this chapter, we have a correspondence between intermediate fields $F \leq K \leq E$ and subgroups of $\mathrm{Aut}_{F\text{–alg}}(E)$. Set $\mathscr{L}_{\mathrm{sub}}(E/F)$ to be the set of subgroups of $\mathrm{Aut}_{F\text{–alg}}(E)$ and $\mathscr{L}_{\mathrm{int}}(E/F)$ to be the set of intermediate subfields of E/F. Both of these sets are partially ordered via set containment. Both of these sets also have two operations:

$$\wedge, \vee \colon \mathscr{L}_{\mathrm{sub}}(E/F) \times \mathscr{L}_{\mathrm{sub}}(E/F) \longrightarrow \mathscr{L}_{\mathrm{sub}}(E/F)$$
$$\wedge, \vee \colon \mathscr{L}_{\mathrm{int}}(E/F) \times \mathscr{L}_{\mathrm{int}}(E/F) \longrightarrow \mathscr{L}_{\mathrm{int}}(E/F)$$

given by

$$H_1 \vee H_2 \stackrel{\mathrm{def}}{=} H_1 H_2, \quad H_1 \wedge H_2 \stackrel{\mathrm{def}}{=} H_1 \cap H_2$$
$$K_1 \vee K_2 \stackrel{\mathrm{def}}{=} K_1 K_2, \quad K_1 \wedge K_2 \stackrel{\mathrm{def}}{=} K_1 \cap K_2.$$

We have functions

$$\mathscr{F}^\star \colon \mathscr{L}_{\mathrm{int}}(E/F) \to \mathscr{L}_{\mathrm{sub}}(E/F), \quad \mathscr{F}_\star \colon \mathscr{L}_{\mathrm{sub}}(E/F) \to \mathscr{L}_{\mathrm{int}}(E/F).$$

Explicitly, we have

$$\mathscr{F}^\star(K) = H_K = \mathrm{Aut}_{K\text{–alg}}(E), \quad \mathscr{F}_\star(H) = E^H.$$

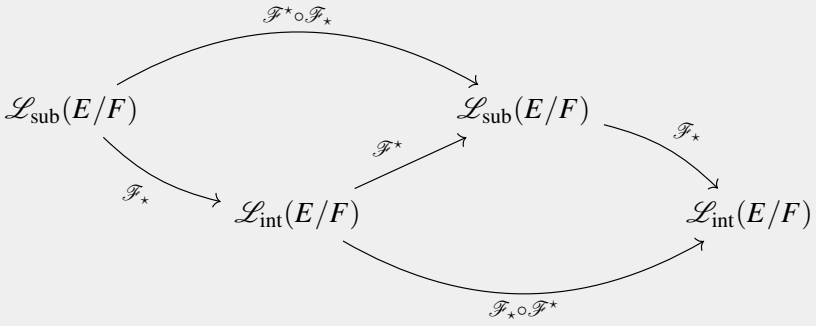
By Lemma 3.6, we see that if $H_1, H_2 \leq \mathrm{Aut}_{F\text{–alg}}(E)$ with $H_1 \leq H_2$, then

$$\mathscr{F}^\star(\mathscr{F}_\star(H_1)) \leq \mathscr{F}^\star(\mathscr{F}_\star(H_2)).$$

Likewise, by Lemma 3.6, if $F \leq K_1 \leq K_2 \leq E$, then

$$\mathscr{F}_\star(\mathscr{F}^\star(K_1)) \leq \mathscr{F}_\star(\mathscr{F}^\star(K_2)).$$

We can encode this more succinctly in the following diagram:



In particular,

$$\mathscr{F}^\star \circ \mathscr{F}_\star \colon \mathscr{L}_{\text{sub}}(E/F) \to \mathscr{L}_{\text{sub}}(E/F), \quad \mathscr{F}_\star \circ \mathscr{F}^\star \colon \mathscr{L}_{\text{int}}(E/F) \to \mathscr{L}_{\text{int}}(E/F)$$

are functions that preserve the partial orders of $\mathscr{L}_{\text{sub}}(E/F)$ and $\mathscr{L}_{\text{int}}(E/F)$, respectively. These functions give a correspondence between $\mathscr{L}_{\text{sub}}(E/F)$ and $\mathscr{L}_{\text{int}}(E/F)$ that is the prototypical example of what is often referred to as a **Galois connection**. We will refer to the package $(E/F, \mathscr{L}_{\text{sub}}(E/F), \mathscr{L}_{\text{int}}(E/F), \mathscr{F}_\star, \mathscr{F}^\star)$ as a Galois connection.

One of the main goals of this chapter is to find a necessary and sufficient condition for the functions $\mathscr{F}_\star, \mathscr{F}^\star$ to be bijective; when these functions are bijections, then this Galois connection is often called a **Galois correspondence**. We will prove that these functions are always bijective on certain subsets of $\mathscr{L}_{\text{sub}}(E/F)$ and $\mathscr{L}_{\text{int}}(E/F)$. We will see that these functions intertwine the operations $\vee, \wedge$ and also are non-increasing with respect to index, degree on $\mathscr{L}_{\text{sub}}(E/F)$ and $\mathscr{L}_{\text{int}}(E/F)$, respectively.

We start by showing that $\mathscr{F}_\star$ and $\mathscr{F}^\star$ are **quasi-inverses**.

***Lemma* 3.12.** *With $\mathscr{F}_\star$ and $\mathscr{F}^\star$ defined as above, we have*

$$\mathscr{F}_\star \circ \mathscr{F}^\star \circ \mathscr{F}_\star = \mathscr{F}_\star, \quad \mathscr{F}^\star \circ \mathscr{F}_\star \circ \mathscr{F}^\star = \mathscr{F}^\star.$$

Proof. Let $H \in \mathscr{L}_{\text{sub}}(E/F)$ and $E^H = \mathscr{F}_\star(H)$. We must prove that $E^H = \mathscr{F}_\star \circ \mathscr{F}^\star(E^H)$. By definition,

$$\mathscr{F}^\star(E^H) = \left\{\tau \in \text{Aut}_{F\text{–alg}}(E) \ : \ \tau(\lambda) = \lambda \text{ for all } \lambda \in E^H\right\},$$

and so it follows that $H \leq \mathscr{F}^\star(E^H)$. Hence, $\mathscr{F}_\star \circ \mathscr{F}^\star(E^H) \leq E^H$ by Lemma 3.6 (a). For the reverse inclusion, by definition of $\mathscr{F}_\star$, we have

$$\mathscr{F}_\star(\mathscr{F}^\star(E^H)) = \left\{\lambda \in E \ : \ \tau(\lambda) = \lambda \text{ for all } \tau \in \mathscr{F}^\star(E^H)\right\}.$$

Additionally, by definition of $\mathscr{F}^\star$, we have

$$\mathscr{F}^\star(E^H) = \left\{\tau \in \text{Aut}_{F\text{–alg}}(E) \ : \ \tau(\lambda) = \lambda \text{ for all } \lambda \in E^H\right\}.$$

In particular, we see that $E^H \leq \mathscr{F}_\star(\mathscr{F}^\star(E^H))$.

Let $K \in \mathscr{L}_{\text{int}}(E/F)$ and $H_K = \mathscr{F}^\star(K)$. We must prove that $H_K = \mathscr{F}^\star \circ \mathscr{F}_\star(H_K)$. By definition,

$$\mathscr{F}_\star(H_K) = \{\lambda \in E \ : \ \tau(\lambda) = \lambda \text{ for all } \tau \in H_K\}$$

and so it follows that $K \leq \mathscr{F}_\star(H_K)$. Hence, $\mathscr{F}^\star \circ \mathscr{F}_\star(H_K) \leq H_K$ by Lemma 3.6 (b). For the reverse inclusion, by definition of $\mathscr{F}^\star$, we have

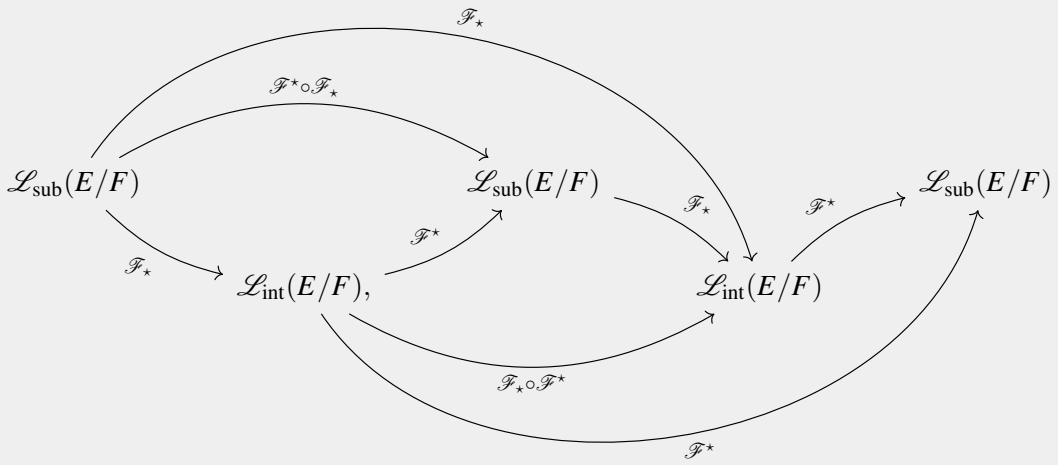
$$\mathscr{F}^\star(\mathscr{F}_\star(H_K)) = \left\{\tau \in \text{Aut}_{F\text{–alg}}(E) \ : \ \tau(\lambda) = \lambda \text{ for all } \lambda \in \mathscr{F}_\star(H_K)\right\}.$$

Additionally, by definition of $\mathscr{F}_\star$, we have

$$\mathscr{F}_\star(H_K) = \{\lambda \in E \,:\, \tau(\lambda) = \lambda \text{ for all } \tau \in H_K\}.$$

In particular, we have $H_K \leq \mathscr{F}^\star(\mathscr{F}_\star(H_K))$. ♠

As a result of Lemma 3.12, the following diagram is commutative:



One views the assignments

$$H \longmapsto \mathscr{F}^\star(\mathscr{F}_\star(H)), \quad K \longmapsto \mathscr{F}_\star(\mathscr{F}^\star(K))$$

as a type of "closure". For comparison, if X is subset of $\mathbf{R}$, we can define $\overline{X}$ as the set of all limits of sequences $\{x_n\}$ where $x_n \in X$. This is often referred to as the closure of X. We see that $X \subseteq \overline{X}$, $\overline{\overline{X}} = \overline{X}$. More generally, we say that X is closed if $\overline{X} = X$. In mathematics, there is a wide variety of settings where one has a **"closure"** procedure. The reader should view our setting as such a case. Indeed, we will even use the adjective "closed" to describe a certain subset of $\mathscr{L}_{\text{sub}}(E/F)$ and $\mathscr{L}_{\text{int}}(E/F)$, respectively, where the functions $\mathscr{F}_\star$ and $\mathscr{F}^\star$ are well behaved.

We now establish several basic results for the functions $\mathscr{F}_\star$ and $\mathscr{F}^\star$.

***Lemma* 3.13.** *Let E/F be an extension of fields.*

(a) *For any* $H \in \mathscr{L}_{sub}(E/F)$, *we have* $H \leq \mathscr{F}^{\star}(\mathscr{F}_{\star}(H))$.

(b) *For any* $K \in \mathscr{L}_{int}(E/F)$, *we have* $K \leq \mathscr{F}_{\star}(\mathscr{F}^{\star}(K))$.

Proof. For (a), given $\tau \in H$, by definition, τ fixes every element of $\mathscr{F}_{\star}(H)$. In particular, $\tau \in \mathscr{F}^{\star}(\mathscr{F}_{\star}(H))$ since $\mathscr{F}^{\star}(\mathscr{F}_{\star}(H))$ is the subgroup of $\mathrm{Aut}_{F-\mathrm{alg}}(E)$ that fix each element of $\mathscr{F}_{\star}(H)$. For (b), given $\beta \in K$, by definition, we know that β is fixed by every element of $\mathscr{F}^{\star}(K)$. In particular, $\beta \in \mathscr{F}_{\star}(\mathscr{F}^{\star}(K))$ since $\mathscr{F}_{\star}(\mathscr{F}^{\star}(K))$ is the subfield of elements of E that are fixed by each element of $\mathscr{F}^{\star}(K)$. ♠

We will say that $H \in \mathscr{L}_{\mathrm{sub}}(E/F)$ is **closed** if $\mathscr{F}^{\star}(\mathscr{F}_{\star}(H)) = H$ and we will say that $K \in \mathscr{L}_{\mathrm{int}}(E/F)$ is **closed** if $\mathscr{F}_{\star}(\mathscr{F}^{\star}(K)) = K$. We denote the set of closed subgroups of $\mathscr{L}_{\mathrm{sub}}(E/F)$ by $\mathscr{L}_{\mathrm{sub}}^{\mathrm{closed}}(E/F)$ and the set of closed subfields E/F by $\mathscr{L}_{\mathrm{int}}^{\mathrm{closed}}(E/F)$.

***Lemma* 3.14.** *Let* E/F *be an extension of fields.*

(a) *If* $H \in \mathscr{L}_{sub}(E/F)$, *then* $\mathscr{F}_{\star}(H) \in \mathscr{L}_{int}^{closed}(E/F)$.

(b) *If* $K \in \mathscr{L}_{int}(E/F)$, *then* $\mathscr{F}^{\star}(K) \in \mathscr{L}_{sub}^{closed}(E/F)$.

Proof. Given $H \in \mathscr{L}_{\mathrm{sub}}(E/F)$, by Lemma 3.12, we know that

$$\mathscr{F}_{\star}(H) = \mathscr{F}_{\star}(\mathscr{F}^{\star}(\mathscr{F}_{\star}(H))).$$

Hence $\mathscr{F}_{\star}(H)$ is closed. Likewise, given $K \in \mathscr{L}_{\mathrm{int}}(E/F)$, by Lemma 3.12, we know that

$$\mathscr{F}^{\star}(K) = \mathscr{F}^{\star}(\mathscr{F}_{\star}(\mathscr{F}^{\star}(K))).$$

Hence $\mathscr{F}^{\star}(K)$ is closed. ♠

We now prove that $\mathscr{F}_{\star}$ and $\mathscr{F}^{\star}$ are inverses on the subsets $\mathscr{L}_{\mathrm{sub}}^{\mathrm{closed}}(E/F)$ and $\mathscr{L}_{\mathrm{int}}^{\mathrm{closed}}(E/F)$.

***Proposition* 3.15.** *Let* E/F *be an extension of fields. Then*

$$\mathscr{F}_{\star}\colon \mathscr{L}_{sub}^{closed}(E/F) \longrightarrow \mathscr{L}_{int}^{closed}(E/F)$$

and

$$\mathscr{F}^{\star}\colon \mathscr{L}_{int}^{closed}(E/F) \longrightarrow \mathscr{L}_{sub}^{closed}(E/F)$$

are bijective functions.

Proof. That $\mathscr{F}_\star$ and $\mathscr{F}^\star$ are bijections upon restricting them to $\mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$ and $\mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$, respectively follows immediate from the fact that

$$\mathscr{F}^\star \circ \mathscr{F}_\star = \text{Id}_{\mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)}, \quad \mathscr{F}_\star \circ \mathscr{F}^\star = \text{Id}_{\mathscr{L}_{\text{int}}^{\text{closed}}(E/F)}.$$

In particular, $(\mathscr{F}^\star)^{-1} = \mathscr{F}_\star$ and so both are bijections since they are inverses of one another. ♠

We next show that $\mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$ and $\mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$ are closed under intersections. We only prove this for intersections of pairs though it holds for arbitrary intersections.

***Lemma* 3.16.** *Let E/F be an extension of fields.*

(a) Let $H_1, H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$. Then $H_1 \cap H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$.

(b) Let $K_1, K_2 \in \mathscr{L}_{int}^{closed}(E/F)$. Then $K_1 \cap K_2 \in \mathscr{L}_{int}^{closed}(E/F)$.

Proof. For (a), given $H_1, H_2 \in \mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$, we must prove that $H_1 \cap H_2 \in \mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$. Given any subgroup $H \leq H_1, H_2$, by Lemma 3.6 (a), we know that $\mathscr{F}_\star(H_1), \mathscr{F}_\star(H_2) \leq \mathscr{F}_\star(H)$. By Lemma 3.6 (b), we know that $\mathscr{F}^\star(\mathscr{F}_\star(H)) \leq \mathscr{F}^\star(\mathscr{F}_\star(H_1)), \mathscr{F}^\star(\mathscr{F}_\star(H_2))$. In particular, since H_1, H_2 are closed, we see that if $H \leq H_1, H_2$, then

$$\mathscr{F}^\star(\mathscr{F}_\star(H)) \leq H_1 \cap H_2.$$

Taking $H = H_1 \cap H_2$, we see that

$$\mathscr{F}^\star(\mathscr{F}_\star(H_1 \cap H_2)) \leq H_1 \cap H_2.$$

By Lemma 3.13 (a), we have

$$H_1 \cap H_2 \leq \mathscr{F}^\star(\mathscr{F}_\star(H_1 \cap H_2)),$$

and so $H_1 \cap H_2 = \mathscr{F}^\star(\mathscr{F}_\star(H_1 \cap H_2)$. Thus, by definition of closed, we have $H_1 \cap H_2 \in \mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$.

For (b), given $K_1, K_2 \in \mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$, we must prove that $K_1 \cap K_2 \in \mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$. Given K with $K \leq K_1, K_2$, by Lemma 3.6 (b), we know that $\mathscr{F}^\star(K_1), \mathscr{F}^\star(K_2) \leq \mathscr{F}^\star(K)$. By Lemma 3.6 (a) and the fact that K_1, K_2 are closed, we see that

$$\mathscr{F}_\star(\mathscr{F}^\star(K)) \leq K_1 \cap K_2.$$

Taking $K = K_1 \cap K_2$, we obtain

$$\mathscr{F}_\star(\mathscr{F}^\star(K_1 \cap K_2)) \leq K_1 \cap K_2.$$

As the reverse inclusion follows from Lemma 3.13 (b), we obtain

$$K_1 \cap K_2 = \mathscr{F}_\star(\mathscr{F}^\star(K_1 \cap K_2)),$$

and so $K_1 \cap K_2 \in \mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$. ♠

Exercise 3.4. *Prove that if $\{H_i\}$ is an arbitrary collection of subgroups in $\mathscr{L}_{sub}^{closed}(E/F)$, then $\cap H_i \in \mathscr{L}_{sub}^{closed}(E/F)$.*

Exercise 3.5. *Prove that if $\{K_i\}$ is an arbitrary collection of subfields in $\mathscr{L}_{int}^{closed}(E/F)$, then $\cap K_i \in \mathscr{L}_{int}^{closed}(E/F)$.*

3.4 *Extension Fields: Galois Connections, II*

For our next result, the reader should recall our rarely used notation:

$$H_1 \vee H_2 \stackrel{\text{def}}{=} H_1 H_2, \quad H_1 \wedge H_2 \stackrel{\text{def}}{=} H_1 \cap H_2$$
$$K_1 \vee K_2 \stackrel{\text{def}}{=} K_1 K_2, \quad K_1 \wedge K_2 \stackrel{\text{def}}{=} K_1 \cap K_2.$$

In this notation and viewing $\mathscr{F}_\star$ and $\mathscr{F}^\star$ as "complementary/negation" procedures, we can view it as a sort of **De Morgan's Law**.

***Lemma* 3.17** (De Morgan's Law: Galois Connections)**.** *Let E/F be an extension of field.*

(a) If $H_1, H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$, then $\mathscr{F}_\star(H_1 H_2) = \mathscr{F}_\star(H_1) \cap \mathscr{F}_\star(H_2)$.

(b) If $K_1, K_2 \in \mathscr{L}_{int}^{closed}(E/F)$, then $\mathscr{F}^\star(K_1 K_2) = \mathscr{F}^\star(K_1) \cap \mathscr{F}^\star(K_2)$.

(c) If $H_1, H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$, then $\mathscr{F}_\star(H_1 \cap H_2) = \mathscr{F}_\star(H_1)\mathscr{F}_\star(H_2)$.

(d) If $K_1, K_2 \in \mathscr{L}_{int}^{closed}(E/F)$, then $\mathscr{F}^\star(K_1 \cap K_2) = \mathscr{F}^\star(K_1)\mathscr{F}^\star(K_2)$.

Proof. For (a), as $H_1, H_2 \leq H_1 H_2$, by Lemma 3.6 (a), we know $\mathscr{F}_\star(H_1 H_2) \leq \mathscr{F}_\star(H_1) \cap \mathscr{F}_\star(H_2)$. Hence, it suffices to prove that $\mathscr{F}_\star(H_1) \cap \mathscr{F}_\star(H_2) \leq \mathscr{F}_\star(H_1 H_2)$. To that end, let $K_i = \mathscr{F}_\star(H_i)$ for $i = 1, 2$. By definition, K_i is the subfield of elements of E that are fixed by all of the elements of H_i. Given an element $\beta \in K_1 \cap K_2$, we must show that β is fixed by every element of $H_1 H_2$. Since $\beta \in K_1 \cap K_2$, we know that β is fixed by every element of H_1 and H_2. As every element in $H_1 H_2$ can be expressed as a product of the form $\sigma_1 \tau_1 \ldots \sigma_n \tau_n$ where $\sigma_i \in H_1$ and $\tau_i \in H_2$, we see that β is fixed by every element of $H_1 H_2$.

For (b), as $K_1, K_2 \leq K_1 K_2$, by Lemma 3.6 (b), we know that $\mathscr{F}^\star(K_1 K_2) \leq \mathscr{F}^\star(K_1) \cap \mathscr{F}^\star(K_2)$. Hence, it suffices to prove that $\mathscr{F}^\star(K_1) \cap \mathscr{F}^\star(K_2) \leq \mathscr{F}^\star(K_1 K_2)$. Given $\sigma \in \mathscr{F}^\star(K_1) \cap \mathscr{F}^\star(K_2)$, by definition σ fixes every element of K_1 and K_2. Since every element of $K_1 K_2$ can be expressed as a finite sum of the form (see Exercise 2.21)

$$\beta = \sum_{i=1}^{n} \alpha_i \lambda_i$$

where $\alpha_i \in K_1$ and $\lambda_i \in K_2$, we see that σ fixes every element of K_1K_2. Hence $\sigma \in \mathscr{F}^\star(K_1K_2)$ as needed.

For (c), as $H_1 \cap H_2 \leq H_1, H_2$, by Lemma 3.6 (a), we know that $\mathscr{F}_\star(H_1)\mathscr{F}_\star(H_2) \leq \mathscr{F}_\star(H_1 \cap H_2)$. Hence, it suffices to prove that $\mathscr{F}_\star(H_1 \cap H_2) \leq \mathscr{F}_\star(H_1)\mathscr{F}_\star(H_2)$. If $K \in \mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$ with $\mathscr{F}_\star(H_i) \leq K$ for $i = 1,2$, by Lemma 3.6 (b), we know that $\mathscr{F}^\star(K) \leq H_i$ for $i = 1,2$. Hence, $\mathscr{F}^\star(K) \leq H_1 \cap H_2$ and so $\mathscr{F}_\star(H_1 \cap H_2) \leq K$. Taking $K = \mathscr{F}_\star(H_1)\mathscr{F}_\star(H_2)$, we obtain the desired reverse inclusion.

For (d), as $K_1 \cap K_2 \leq K_1, K_2$, by Lemma 3.6 (b), we know that $\mathscr{F}^\star(K_1)\mathscr{F}^\star(K_2) \leq \mathscr{F}^\star(K_1 \cap K_2)$. Hence, it suffices to prove that $\mathscr{F}^\star(K_1 \cap K_2) \leq \mathscr{F}^\star(K_1)\mathscr{F}^\star(K_2)$. If $H \in \mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$ with $\mathscr{F}^\star(K_1), \mathscr{F}^\star(K_2) \leq H$, then by Lemma 3.6 (b), we have $\mathscr{F}_\star(H) \leq K_1 \cap K_2$ since K_1, K_2 are closed. Thus, $\mathscr{F}^\star(K_1 \cap K_2) \leq H$. Taking $H = \mathscr{F}^\star(K_1)\mathscr{F}^\star(K_2)$, we obtain the desired reverse inclusion. ♠

Corollary 3.18. *Let E/F be an extension of field.*

(a) If $H_1, H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$, then $H_1H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$.

(b) If $K_1, K_2 \in \mathscr{L}_{int}^{closed}(E/F)$, then $K_1K_2 \in \mathscr{L}_{int}^{closed}(E/F)$.

Proof. For (a), applying parts (a), (d) of Lemma 3.16 and the fact that H_1, H_2 are closed, we see that

$$\begin{aligned}\mathscr{F}^\star(\mathscr{F}_\star(H_1H_2)) &= \mathscr{F}^\star(\mathscr{F}_\star(H_1) \cap \mathscr{F}_\star(H_2)) \\ &= \mathscr{F}^\star(\mathscr{F}_\star(H_1))\mathscr{F}^\star(\mathscr{F}_\star(H_2)) = H_1H_2.\end{aligned}$$

Hence $H_1H_2 \in \mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$. For (b), applying parts (c), (b) of Lemma 3.16 and the fact that K_1, K_2 are closed, we see that

$$\mathscr{F}_\star(\mathscr{F}^\star(K_1K_2)) = \mathscr{F}_\star(\mathscr{F}^\star(K_1) \cap \mathscr{F}^\star(K_2)) = \mathscr{F}_\star(\mathscr{F}^\star(K_1))\mathscr{F}_\star(\mathscr{F}^\star(K_2)) = K_1K_2.$$

Hence $K_1K_2 \in \mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$. ♠

The main goal of this section is to establish results relating index and degree under the functions $\mathscr{F}_\star$ and $\mathscr{F}^\star$. We will show that $\mathscr{F}_\star$ and $\mathscr{F}^\star$ preserve index/degree on $\mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$ and $\mathscr{L}_{\text{int}}^{\text{closed}}(E/F)$. Specifically, we have the following.

Proposition 3.19. *Let E/F be an extension of fields.*

(a) If $H_1, H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$ and $H_1 \leq H_2$, then $[H_2 : H_1] = [\mathscr{F}_\star(H_1) : \mathscr{F}_\star(H_2)]$.

(b) If $K_1, K_2 \in \mathscr{L}_{int}^{closed}(E/F)$ and $K_1 \leq K_2$, then $[K_2 : K_1] = [\mathscr{F}^\star(K_1) : \mathscr{F}^\star(K_2)]$.

Proposition 3.19 will be derived as a special case of a more general result that shows that $\mathscr{F}_\star$ and $\mathscr{F}^\star$, respectively, are non-increase with respect to degree and index. Specifically, we will prove:

Theorem 3.20. *Let E/F be an extension of fields.*

(a) If $H_1, H_2 \in \mathscr{L}_{sub}(E/F)$ with $H_1 \leq H_2$, then $[\mathscr{F}_\star(H_1) : \mathscr{F}_\star(H_2)] \leq [H_2 : H_1]$.

(b) If $K_1, K_2 \in \mathscr{L}_{int}(E/F)$ with $K_1 \leq K_2$, then $[\mathscr{F}^\star(K_1) : \mathscr{F}^\star(K_2)] \leq [K_2 : K_1]$.

Proposition 3.19 follows easily from Theorem 3.20. The proof of Theorem 3.20 is more involved and will require us to establish some important results of independent utility. Consequently, assuming Theorem 3.20 for the moment, we derive Proposition 3.19.

Proof of Proposition 3.19. Given $H_1, H_2 \in \mathscr{L}_{\text{sub}}^{\text{closed}}(E/F)$, applying Theorem 3.20 twice, we see that

$$[H_2 : H_1] = [\mathscr{F}^\star(\mathscr{F}_\star(H_2)) : \mathscr{F}^\star(\mathscr{F}_\star(H_1))] \leq [\mathscr{F}_\star(H_1) : \mathscr{F}_\star(H_2)] \leq [H_2 : H_1].$$

Hence (a) follows. The derivation of (b) is logically identical. ♠

The remainder of this section is devoted to the proof of Theorem 3.20. To begin, in Theorem 3.20, we will restrict to the case when the index/degree is finite; disregarding cardinal numbers, when either $[H_2 : H_1]$ or $[K_2 : K_1]$ is infinite, the inequalities in Theorem 3.20 follow trivially. The proof of Theorem 3.20 requires some preliminary work. We prove each part of Theorem 3.20 separately, starting with (a).

Let E/F be an extension of fields and $H \leq \text{Aut}_{F\text{–alg}}(E)$ a subgroup. For each $\beta \in E$, we define a function $\text{Eval}_{H,\beta} : H \to E$ by $\text{Eval}_{H,\beta}(\sigma) \stackrel{\text{def}}{=} \sigma(\beta)$. If $\beta \in \mathscr{F}_\star(H) = E^H$, then $\text{Eval}_{H,\beta}(\sigma) = \beta$ is a constant function. In particular, if $\beta' = \alpha\beta$ for $\alpha \in E^H$, we see that $\text{Eval}_{H,\beta'} = \alpha\,\text{Eval}_{H,\beta}$. In addition, we have

$$\text{Eval}_{H,\beta_1+\beta_2} = \text{Eval}_{H,\beta_1} + \text{Eval}_{H,\beta_2}.$$

Viewing $\text{Fun}(H,E)$ as a E^H–vector space, we have a E^H–linear function $L_H : E \to \text{Fun}(H,E)$ given by $L_H(\beta) = \text{Eval}_{H,\beta}$.

Exercise 3.6. *Let E/F be an extension and $H \leq \text{Aut}_{F-alg}(E)$ be a subgroup. For $\alpha \in E$, define*

$$\text{Eval}_{H,\alpha} : H \longrightarrow E$$

to be $\text{Eval}_{H,\beta}(\sigma) = \sigma(\beta)$. Prove that $L_H : E \to \text{Fun}(H,E)$ defined by $L_H(\beta) = \text{Eval}_{H,\beta}$ is an E^H–linear function.

We can also view $\mathrm{Fun}(H,E)$ as an E–vector space. The following proposition will be useful in proving Theorem 3.20 (a).

Proposition 3.21. *Given $\beta_1,\dots,\beta_n \in E$, the functions $\mathrm{Eval}_{H,\beta_1},\dots,\mathrm{Eval}_{H,\beta_n} \in \mathrm{Fun}(H,E)$ are E–linearly independent if and only if $\beta_1,\dots,\beta_n$ are E^H–linearly independent.*

In the proof of Proposition 3.21, we will assume that $\mathrm{char}(F)=0$ and that H is finite. The result holds without either of these assumptions; we can remove our assumption that $\mathrm{char}(F)=0$ using Exercise 3.8. We have opted for the proof below as it utilizes a basic method when working with groups (especially finite or compact ones). Specifically, we will employ an averaging process (see (3.3) below) in the proof of the"harder" direction of Proposition 3.21.

Proof. We will prove the contrapositive. Namely, $\mathrm{Eval}_{H,\beta_1},\dots,\mathrm{Eval}_{H,\beta_n}$ are E–linearly dependent if and only if $\beta_1,\dots,\beta_n$ are E^H–linearly dependent. We will prove the harder of these two implications, the direct implication, first. For the direct implication, we will assume that $\mathrm{Eval}_{H,\beta_1},\dots,\mathrm{Eval}_{H,\beta_n}$ are E–linearly dependent. By definition of E–linear dependence, there exists $\lambda_1,\dots,\lambda_n \in E$ such that

$$\sum_{i=1}^{n} \lambda_i \,\mathrm{Eval}_{H,\beta_i} = 0 \tag{3.1}$$

where not all of the $\lambda_i = 0$. After relabelling if necessary, we can assume that $\lambda_1 \neq 0$. Multiplying (3.1) by λ_1^{-1}, we can assume that $\lambda_1 = 1$. It follows from (3.1) that for all $\sigma \in H$, we have

$$\sum_{i=1}^{n} \lambda_i \sigma(\beta_i) = 0.$$

Applying σ^{-1}, we see that

$$\sigma^{-1}\left(\sum_{i=1}^{n} \lambda_i \sigma(\beta_i)\right) = \sum_{i=1}^{n} \sigma^{-1}(\lambda_i)\beta_i = 0. \tag{3.2}$$

As we have (3.2) for each $\sigma \in H$, we can take the sum over all $\sigma \in H$. This yields

$$\sum_{\sigma\in H}\left(\sum_{i=1}^{n} \sigma^{-1}(\lambda_i)\beta_i\right) = 0. \tag{3.3}$$

Interchanging the sums in (3.3), we obtain

$$\sum_{\sigma\in H}\left(\sum_{i=1}^{n} \sigma^{-1}(\lambda_i)\beta_i\right) = \sum_{i=1}^{n}\left(\sum_{\sigma\in H} \sigma^{-1}(\lambda_i)\beta_i\right) = 0. \tag{3.4}$$

Since β_i does not depend on σ in the inner sum of the right hand side of (3.4), we see that

$$\sum_{\sigma\in H}\left(\sum_{i=1}^{n}\sigma^{-1}(\lambda_i)\beta_i\right)=\sum_{i=1}^{n}\left(\sum_{\sigma\in H}\sigma^{-1}(\lambda_i)\right)\beta_i=0.$$

Setting

$$\alpha_i=\sum_{\sigma\in H}\sigma^{-1}(\lambda_i),$$

we see that $\tau(\alpha_i)=\alpha_i$ for all $\tau\in H$ and so $\alpha_i\in E^H$; see Exercise 3.7. In particular,

$$\sum_{i=1}^{n}\alpha_i\beta_i=0.$$

It remains to prove that not all of the $\alpha_i=0$. Since $\lambda_1=1$ and $\sigma(1)=1$ for all $\sigma\in H$, we have $\alpha_1=|H|\,\lambda_1\neq 0$; see Exercise 3.8 below.

For the reverse implication, we will assume that $\beta_1,\ldots,\beta_n$ are E^H–linearly dependent and must prove that $\mathrm{Eval}_{H,\beta_1},\ldots,\mathrm{Eval}_{H,\beta_n}$ are E–linearly dependent. By definition of E^H–linear dependence, there exists $\alpha_1,\ldots,\alpha_n\in E^H$ such that

$$\sum_{i=1}^{n}\alpha_i\beta_i=0$$

with not all of the $\alpha_i=0$. Since $L_H\colon E\to\mathrm{Fun}(H,E)$ is E^H–linear by Exercise 3.6, we see that

$$L_H\left(\sum_{i=1}^{n}\alpha_i\beta_i\right)=\sum_{i=1}^{n}\alpha_iL_H(\beta_i)=\sum_{i=1}^{n}\alpha_i\,\mathrm{Eval}_{H,\beta_i}=0.$$

Hence, $\mathrm{Eval}_{H,\beta_1},\ldots,\mathrm{Eval}_{H,\beta_n}$ are E–linearly dependent (in fact, they are E^H–linearly dependent). ♠

Exercise 3.7. *Let E/F be an extension of fields and $H\leq\mathrm{Aut}_{F-alg}(E)$ be a finite subgroup. Prove that if $\lambda\in E$, then*

$$\alpha_\lambda\stackrel{def}{=}\sum_{\sigma\in H}\sigma(\lambda)$$

is invariant under H. That is, for each $\sigma'\in H$, we have $\sigma'(\alpha_\lambda)=\alpha_\lambda$.

Using the following, we can remove our assumption that $\mathrm{char}(F)=0$ in our proof of Proposition 3.21.

Exercise 3.8. *Let E/F be an extension and let $H\leq\mathrm{Aut}_{F-alg}(E)$ be a finite group. Prove that if $\lambda\in E$ and $\lambda\neq 0$, then there exists $\lambda'\in E$ such that*

$$\sum_{\sigma\in H}\sigma(\lambda'\lambda)\neq 0.$$

We now prove Theorem 3.20 (a).

Proof of Theorem 3.20 (a). Given $H_1, H_2 \in \mathscr{L}_{\text{sub}}(E/F)$ with $H_1 \leq H_2$, we must show that

$$[\mathscr{F}_\star(H_1) : \mathscr{F}_\star(H_2)] \leq [H_2 : H_1].$$

We select a complete set of H_1–coset representatives $\sigma_1, \ldots, \sigma_m$ in H_2. Setting $K_i = \mathscr{F}_\star(H_i)$, we select a K_2–basis for K_1, say $\{\beta_1, \ldots, \beta_n\}$ and must show that $n \leq m$. For each σ_i, we have the the linear equation

$$\sum_{j=1}^{n} s_j \operatorname{Eval}_{H_2,\beta_j}(\sigma_i) = 0$$

where we view $s_1, \ldots, s_n$ as variables which can take values in K_1. In total, we obtain the homogeneous linear system (with coefficients in K_1)

$$\begin{array}{cccc}
s_1 \operatorname{Eval}_{H_2,\beta_1}(\sigma_1) + s_2 \operatorname{Eval}_{H_2,\beta_2}(\sigma_1) + \cdots + s_n \operatorname{Eval}_{H_2,\beta_n}(\sigma_1) = 0 \\
s_1 \operatorname{Eval}_{H_2,\beta_1}(\sigma_2) + s_2 \operatorname{Eval}_{H_2,\beta_2}(\sigma_2) + \cdots + s_n \operatorname{Eval}_{H_2,\beta_n}(\sigma_2) = 0 \\
\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
s_1 \operatorname{Eval}_{H_2,\beta_1}(\sigma_m) + s_2 \operatorname{Eval}_{H_2,\beta_2}(\sigma_m) + \cdots + s_n \operatorname{Eval}_{H_2,\beta_n}(\sigma_m) = 0.
\end{array}$$

This is a system of m equations in n unknowns. If $n > m$, the system is undetermined and so we have a non-trivial solution, say $\lambda_1, \ldots, \lambda_n \in K_1$. In particular,

$$\sum_{j=1}^{n} \lambda_j \operatorname{Eval}_{H_2,\beta_j}(\sigma_i) = 0$$

for all $i = 1, \ldots, m$. For any $\sigma \in H_2$, we know that $\sigma = \sigma_i \tau$ for some $\tau \in H_1$. In particular,

$$\operatorname{Eval}_{H_2,\beta_j}(\sigma) = \operatorname{Eval}_{H_2,\beta_j}(\sigma_i\tau) = \sigma_i(\tau(\beta_j)) = \sigma_i(\beta) = \operatorname{Eval}_{H_2,\beta_j}(\sigma_i).$$

Hence

$$\sum_{j=1}^{n} \lambda_j \operatorname{Eval}_{H_2,\beta_j}(\sigma) = 0$$

for all $\sigma \in H_2$. In particular, $\operatorname{Eval}_{H_2,\beta_1}, \ldots, \operatorname{Eval}_{H_2,\beta_n}$ are K_1–linearly dependent. By Proposition 3.21, this implies that $\beta_1, \ldots, \beta_n$ are K_2–linearly dependent. As this is impossible by our selection of the β_i, we conclude that $n \leq m$. ♠

***Remark* 3.22.** *We note that since we assumed $[H_2 : H_1] < \infty$ in our proof of Theorem 3.20, we only require Proposition 3.21 in the case when H is finite.*

3.5 *Extension Fields: Galois Connections, III*

To prove Theorem 3.20 (b), we require a preliminary result that is more general than what we require. However, as this preliminary result is important in the study of field extensions, we have included it.

Given a finite extension E/F, we can view both E/F and $\overline{F}/F$ as F–algebras where $\overline{F}$ is the algebraic closure of F. Since E/F is finite, it follows that E/F is algebraic, and so there exists an injective F–algebra homomorphism $\psi\colon E \to \overline{F}$. Our present interest is on the size of $\text{Hom}_{F\text{–alg}}(E,\overline{F})$. Note that because E is a field, any $\psi \in \text{Hom}_{F\text{–alg}}(E,\overline{F})$ is injective; we must have $\psi(1) = 1$. In particular, we only need to determine the number of injective ψ. We will first consider the case when E is a simple extension.

***Lemma* 3.23.** *Let E/F be a finite, simple extension and E/F is separable. Then*

$$\left|\text{Hom}_{F\text{–}alg}(E,\overline{F})\right| = [E:F].$$

Proof. Since E/F is a simple extension, there exists $\beta \in E$ such that $E = F(\beta)$. Taking $P = P_\beta$ to be the minimal polynomial for β over F, since $\overline{F}$ is algebraically closed, we know that $\text{Roots}(P) \subset \overline{F}$. Given an injective homomorphism $\psi\colon E \to \overline{F}$, it must be that $\psi(\beta) \in \text{Roots}(P)$. Moreover, any F–algebra homomorphism $\psi\colon E \to \overline{F}$ is completely determined by $\psi(\beta)$. Hence, the number of F–algebra homomorphisms $\psi\colon E \to \overline{F}$ is at most $|\text{Roots}(P)| = \deg(P) = [E:F]$. By Theorem 3.7, for each $\beta_i \in \text{Roots}(P)$, there exists a homomorphism $\psi\colon E \to \overline{F}$ such that $\psi(\beta) = \beta_i$. Hence, the number of F–algebra homomorphisms $\psi\colon E \to \overline{F}$ is precisely $[E:F]$. ♠

Before extending Lemma 3.23, we require a few definitions.

***Definition* 3.2** (Separable Element)**.** *Given an algebraic extension E/F, we say that $\beta \in E$ is **separable** if β is the zero of a separable polynomial.*

Some mathematicians allow for β to be transcendental in the definition of a separable element. As our interests are on algebraic extensions (almost exclusively), we have opted to assume that E/F is algebraic.

***Remark* 3.24.** *If $\beta \in E$ is algebraic, by Exercise 2.48, the minimal polynomial $P_\beta \in F[t]$ is irreducible and if $\text{char}(F) = 0$, by Exercise 2.59 (iii), we know that P_β is separable. In particular, every element $\beta \in E$ is separable when $\text{char}(F) = 0$ and E/F is algebraic.*

***Definition* 3.3** (Separable Extension)**.** *We say an extension E/F is **separable** if every algebraic element $\beta \in E$ is separable.*

***Proposition* 3.25.** *Let E/F be a finite, separable extension. Then $\left|\text{Hom}_{F\text{–}alg}(E,\overline{F})\right| = [E:F]$.*

Proof. As E/F is finite and separable, $E = F(\beta_1, \ldots, \beta_n)$ where the minimal polynomial of each β_i is separable. We will assume that each β_i is not contained in $F(\beta_1, \ldots, \beta_{i-1})$ as otherwise we can remove it from the generating set. We first note that any $\psi\colon E \to \overline{F}$ is determined by $\psi(\beta_1), \ldots, \psi(\beta_n)$. Letting P_1 be the minimal polynomial for β_1, we have $\text{Roots}(P_1)$ choices for β_1. Taking P_2 to be the minimal polynomial for β_2 over the splitting field of P_1 over F, we have $\deg(P_2)$ choices for β_2. Note that $[F(\beta_1, \beta_2) : F(\beta_1)] = \deg(P_2)$. Continuing, for P_i, the minimal polynomial for β_i over $F(\beta_1, \ldots, \beta_{i-1})$, we have $\deg(P_i)$ choices for the image of β_i. As before, $[F(\beta_1, \ldots, \beta_i) : F(\beta_1, \ldots, \beta_{i-1})] = \deg(P_i)$. In total, we have

$$\deg(P_1)\deg(P_2)\ldots\deg(P_n) = [F(\beta_1) : F][F(\beta_1, \beta_2) : F(\beta_1)]\ldots[E : F(\beta_1, \ldots, \beta_{n-1}] = [E : F]$$

F–algebra homomorphisms $\psi\colon E \to \overline{F}$. ♠

As the proof of Proposition 3.25 is short on precise details, we expound further on it. Given any F–algebra homomorphism $\psi\colon E \to \overline{F}$, the restriction to $F(\beta_1)$ gives an F–algebra homomorphism $F(\beta_1) \to \overline{F}$. By Lemma 3.23, we know that there are precisely $[F(\beta_1) : F]$ such homomorphisms and that any ψ is an extension of one of these. Each extension gives rise to an $F(\beta_1)$–algebra homomorphism $F(\beta_1, \beta_2) \to \overline{F(\beta_1)} = \overline{F}$. Hence, the number of extensions is equal to $[F(\beta_1, \beta_2) : F(\beta_1)]$ for each F–algebra homomorphism $F(\beta_1) \to \overline{F}$. Thus, we have $[F(\beta_1, \beta_2) : F] = [F(\beta_1, \beta_2) : F(\beta_1)][F(\beta_1) : F]$ such mappings. Continuing this argument over the β_i yields the desired count.

Remark 3.26. *If E/F is not separable, then we will have fewer elements in* $\text{Roots}(P_i)$ *in the above argument since some of the P_i will have multiple/repeated roots. In particular, in this case, we have* $\left|\text{Hom}_{F-alg}(E, \overline{F})\right| \leq [E : F]$. *The number* $\left|\text{Hom}_{F-alg}(E, \overline{F})\right|$ *is called the* ***separable degree*** *of the extension E/F and is denoted by $[E : F]_s$. The above argument shows, in fact, that $[E : F]_s$ divides $[E : F]$.*

Exercise 3.9. *Let E/F be a finite extension. Prove that $[E : F]_s$ divides $[E : F]$.*

Exercise 3.10. *Let E/F and K/E be finite extensions. Prove that $[K : F]_s = [K : E]_s[E : F]_s$. That is,*

$$\left|\text{Hom}_{F-alg}(K, \overline{F})\right| = \left|\text{Hom}_{E-alg}(K, \overline{F})\right| \left|\text{Hom}_{F-alg}(E, \overline{F})\right|.$$

We record the following application of Proposition 3.25 and Remark 3.26.

Corollary 3.27. *If K_1/F, K_2/K_1, and E/K_2 are algebraic extensions such that K_2/K_1 is finite, then*

$$\left|\text{Hom}_{K_1-alg}(K_2, E)\right| \leq [K_2 : K_1].$$

Exercise 3.11. *Prove Corollary 3.27. [Hint: View $E \leq \overline{F}$ and note that roots must still map to roots.]*

Exercise 3.12. *If K_1/F, K_2/K_1, and E/K_2 are algebraic extensions such that K_2/K_1 is finite, prove that*

$$\left|\text{Hom}_{K_1-alg}(K_2, E)\right| = [K_2 : K_1]_s.$$

We now prove Theorem 3.20 (b).

Proof of Theorem 3.20 (b). Given $K_1, K_2 \in \mathscr{L}_{\text{int}}(E/F)$ with $K_1 \leq K_2$, we must show that

$$[\mathscr{F}^\star(K_1) : \mathscr{F}^\star(K_2)] \leq [K_2 : K_1].$$

For $\sigma_1, \sigma_2 \in \mathscr{F}^\star(K_1)$, if $\sigma_1(\beta) = \sigma_2(\beta)$ for all $\beta \in K_2$, then $\sigma_1^{-1}\sigma_2 \in \mathscr{F}^\star(K_2)$. Therefore, we see that $\sigma_1\mathscr{F}^\star(K_2) = \sigma_2\mathscr{F}^\star(K_2)$ and so each coset $\sigma\mathscr{F}^\star(K_2)$ represents a distinct K_1–algebra homomorphism $K_2 \to E$. It follows from Corollary 3.27 that the number of such homomorphisms is at most $[K_2 : K_1]$. Hence, $[\mathscr{F}^\star(K_1) : \mathscr{F}^\star(K_2)] \leq [K_2 : K_1]$ as desired. ♠

As an application of Theorem 3.20, we have the following lemma.

***Lemma* 3.28.** *Let E/F be an extension of fields.*

(a) If $H_1 \in \mathscr{L}_{sub}^{closed}(E/F)$, $H_2 \in \mathscr{L}_{sub}(E/F)$, $H_1 \leq H_2$, and $[H_2 : H_1] < \infty$, then $H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$.

(b) If $K_1 \in \mathscr{L}_{int}^{closed}(E/F)$, $K_2 \in \mathscr{L}_{int}^{closed}(E/F)$, $K_1 \leq K_2$, and $[K_2 : K_1] < \infty$, then $K_2 \in \mathscr{L}_{int}^{closed}(E/F)$.

Proof. For (a), by Theorem 3.20 (a) and (b), we have

$$[\mathscr{F}^\star(\mathscr{F}_\star(H_2)) : \mathscr{F}^\star(\mathscr{F}_\star(H_1))] \leq [\mathscr{F}_\star(H_1) : \mathscr{F}_\star(H_2)] \leq [H_2 : H_1].$$

Since H_1 is closed, this yields

$$[\mathscr{F}^\star(\mathscr{F}_\star(H_2)) : H_1] \leq [H_2 : H_1].$$

Since $H_2 \leq \mathscr{F}^\star(\mathscr{F}_\star(H_2)$, we see that

$$[\mathscr{F}^\star(\mathscr{F}_\star(H_2)) : H_1] = [\mathscr{F}^\star(\mathscr{F}_\star(H_2)) : H_2][H_2 : H_1].$$

In particular, we conclude that

$$[\mathscr{F}^\star(\mathscr{F}_\star(H_2)) : H_2][H_2 : H_1] \leq [H_2 : H_1].$$

Since $[H_2 : H_1] < \infty$, this implies that $[\mathscr{F}^\star(\mathscr{F}_\star(H_2)) : H_2] \leq 1$ and hence $H_2 = \mathscr{F}^\star(\mathscr{F}_\star(H_2))$. The proof of (b) is logically identical. ♠

An immediate corollary of Lemma 3.28 is the following. In the statement, $\{e\}$ denotes the trivial subgroup in $\text{Aut}_{F\text{–alg}}(E)$.

***Corollary* 3.29.** *Let E/F be an algebraic extension.*

(a) *If* $\{e\} \in \mathscr{L}_{sub}^{closed}(E/F)$ *and* E/F *is finite, then* $\mathscr{L}_{sub}(E/F) = \mathscr{L}_{sub}^{closed}(E/F)$.

(b) *If* $F \in \mathscr{L}_{int}^{closed}(E/F)$ *and* E/F *is finite, then* $\mathscr{L}_{int}(E/F) = \mathscr{L}_{int}^{closed}(E/F)$.

Exercise 3.13. *Prove Corollary 3.29*

We now summarize our work from this and previous sections with the following result which lists the properties of our Galois connection $(E/F, \mathscr{L}_{\text{sub}}(E/F), \mathscr{L}_{\text{int}}(E/F), \mathscr{F}_\star, \mathscr{F}^\star)$.

Theorem 3.30 (Fundamental Theorem: Galois Connections)**.** *Let* E/F *be an algebraic extension,* $\mathscr{L}_{sub}(E/F)$ *the set (lattice) of subgroups of* $\text{Aut}_{F-alg}(E)$, $\mathscr{L}_{int}(E/F)$ *the set (lattice) of intermediate fields for* E/F, *and*

$$\mathscr{F}_\star \colon \mathscr{L}_{sub}(E/F) \to \mathscr{L}_{int}(E/F), \quad \mathscr{F}^\star \colon \mathscr{L}_{int}(E/F) \to \mathscr{L}_{sub}(E/F)$$

given by

$$\mathscr{F}_\star(H) = \{\beta \in E \ : \ \sigma(\beta) = \beta \text{ for all } \sigma \in H\} = E^H$$

and

$$\mathscr{F}^\star(K) = \left\{\sigma \in \text{Aut}_{F-alg}(E) \ : \ \sigma(\beta) = \beta \text{ for all } \beta \in K\right\} = \text{Aut}_{K-alg}(E).$$

Then we have the following:

(a) *We have* $\mathscr{F}_\star = \mathscr{F}_\star \circ \mathscr{F}^\star \circ \mathscr{F}_\star$ *and* $\mathscr{F}^\star = \mathscr{F}^\star \circ \mathscr{F}_\star \circ \mathscr{F}^\star$. *Moreover,* $\mathscr{F}_\star$ *and* $\mathscr{F}^\star$ *are inverse functions on* $\mathscr{L}_{sub}^{closed}(E/F)$ *and* $\mathscr{L}_{int}^{closed}(E/F)$.

(b) *For all* $H \in \mathscr{L}_{sub}(E/F)$ *and* $K \in \mathscr{L}_{int}(E/F)$, *we have*

$$H \leq \mathscr{F}^\star(\mathscr{F}_\star(H)), \quad K \leq \mathscr{F}_\star(\mathscr{F}^\star(K))$$

with equality if and only if $H \in \mathscr{F}_{sub}^{closed}(E/F)$ *and* $K \in \mathscr{L}_{int}^{closed}(E/F)$.

(c) *For all* $H_1, H_2 \in \mathscr{L}_{sub}(E/F)$ *with* $H_1 \leq H_2$ *and all* $K_1, K_2 \in \mathscr{L}_{int}(E/F)$, *we have*

$$[\mathscr{F}_\star(H_1) : \mathscr{F}_\star(H_2)] \leq [H_2 : H_1], \quad [\mathscr{F}^\star(K_1) : \mathscr{F}^\star(K_2)] \leq [K_2 : K_1].$$

If $H_1, H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$ *and* $K_1, K_2 \in \mathscr{L}_{int}^{closed}(E/F)$, *then we have equality.*

(d) *If* $H_1, H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$ *and* $K_1, K_2 \in \mathscr{L}_{int}^{closed}(E/F)$, *then* $H_1 \cap H_2, H_1 H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$ *and* $K_1 \cap K_2, K_1 K_2 \in \mathscr{L}_{int}^{closed}(E/F)$.

(e) *If* $H_1 \in \mathscr{L}_{sub}^{closed}(E/F)$, $H_2 \in \mathscr{L}_{sub}(E/F)$, $H_1 \leq H_2$, *and* $[H_2 : H_1] < \infty$, *then* $H_2 \in \mathscr{L}_{sub}^{closed}(E/F)$.

(f) *If* $K_1 \in \mathscr{L}_{int}^{closed}(E/F)$, $K_2 \in \mathscr{L}_{int}(E/F)$, $K_1 \leq K_2$, *and* $[K_2 : K_1] < \infty$, *then* $K_2 \in \mathscr{L}_{int}^{closed}(E/F)$.

(g) *If* $F \in \mathscr{L}_{int}^{closed}(E/F)$ *and* E/F *is finite, then* $\mathscr{L}_{int}(E/F) = \mathscr{F}_{int}^{closed}(E/F)$. *Likewise, if* $\{e\} \in \text{Aut}_{F-alg}(E)$ *is closed and* E/F *is finite, then* $\mathscr{L}_{sub}(E/F) = \mathscr{L}_{sub}^{closed}(E/F)$.

3.6 *Extension Fields: Galois Extensions*

Before introducing the fundamental concepts of normal and Galois extensions, we briefly discuss the concept of a separable extensions further. The following exercise shows that separability is preserved under passing to intermediate fields.

Exercise 3.14. *Let E/F be a separable extension and $F \leq K \leq E$. Prove that E/K and K/F are separable extensions.*

The following lemma is an immediate consequence of Remark 3.24.

Lemma 3.31. *If E/F is algebraic and $\text{char}(F) = 0$, then E/F is separable.*

Fields with the property that every finite extension is separable are a nice class of fields and have been given a special name.

Definition 3.4 (Perfect Field)**.** *We say that a field F is **perfect** if every finite extension E/F is separable.*

We again see that characteristic zero fields are perfect.

Lemma 3.32. *If F is a field with $\text{char}(F) = 0$, then F is perfect.*

As Lemma 3.32 is straightforward, we leave it as an exercise for the reader.

Exercise 3.15. *Prove Lemma 3.32. [Hint: Use Exercise 2.15 and Lemma 3.31]*

Exercise 3.16. *Prove that if F is a field with $\text{char}(F) = p$ with $p \neq 0$, then F if perfect if and only if for every $\alpha \in F$, there exists $\beta \in F$ such that $\beta^p = \alpha$.*

Under our Galois connection, we saw that closed subfields and closed subgroups satisfy several nice properties with regard to our functions $\mathscr{F}_\star$ and $\mathscr{F}^\star$. Our next condition on fields will ensure that in an extension E/F that F is closed.

Definition 3.5 (Normal Extension)**.** *We say that an algebraic extension E/F is **normal** if*

$$\mathscr{F}_\star(\text{Aut}_{F-alg}(E)) = F.$$

Exercise 3.17. *Prove that if E/F is a normal extension and $F \leq K \leq E$, then E/K is normal.*

Lemma 3.33. *If E/F is normal, then $F \in \mathscr{L}_{int}^{closed}(E/F)$.*

Proof. By definition of $\mathrm{Aut}_{F-\mathrm{alg}}(E)$, we have $\mathscr{F}^\star(F) = \mathrm{Aut}_{F-\mathrm{alg}}$. Since E/F is normal, we have

$$\mathscr{F}_\star(\mathrm{Aut}_{F-\mathrm{alg}}(E)) = F.$$

Hence $\mathscr{F}_\star(\mathscr{F}^\star(F)) = F$ and so $F \in \mathscr{L}_{\mathrm{int}}^{\mathrm{closed}}(E/F)$. ♠

Combining 3.33 and Corollary 3.29, we obtain the following.

Corollary 3.34. *If E/F is normal and finite, then $\mathscr{L}_{int}(E/F) = \mathscr{L}_{int}^{closed}(E/F)$.*

We next turn our attention to which subgroups of $\mathrm{Aut}_{F-\mathrm{alg}}(E)$ are closed. The following lemma establishes that all finite subgroups are closed.

Lemma 3.35. *Let E/F be an algebraic extension. If $H \leq \mathrm{Aut}_{F-alg}(E)$ is finite, then $H \in \mathscr{L}_{sub}^{closed}(E/F)$.*

The validity of Lemma 3.35 follows immediately from Corollary 3.29 and the following exercise.

Exercise 3.18. *Prove that if E/F is algebraic, then $\{e\} \in \mathscr{L}_{sub}^{closed}(E/F)$.*

As an application of Lemma 3.35, we have the following corollary.

Corollary 3.36. *Let E/F be a finite extension.*

(a) $\mathscr{L}_{sub}(E/F) = \mathscr{L}_{sub}^{closed}(E/F)$.

(b) $\mathscr{F}_\star$ *is injective.*

(c) $\mathscr{F}^\star$ *is surjective.*

Proof. (a) follows immediately from Lemma 3.35. For (b), we know that $\mathscr{F}^\star(\mathscr{F}_\star(H)) = H$ for all $H \in \mathscr{L}_{\mathrm{sub}}(E/F)$ by (a). In particular, if $H_1 \neq H_2$, we see that $\mathscr{F}^\star(\mathscr{F}_\star(H_1)) \neq \mathscr{F}^\star(\mathscr{F}_\star(H_2))$. Hence, $\mathscr{F}_\star(H_1) \neq \mathscr{F}_\star(H_2)$. For (c), we know that $\mathscr{F}^\star$ is a bijection between $\mathscr{L}_{\mathrm{int}}^{\mathrm{closed}}(E/F)$ and $\mathscr{L}_{\mathrm{sub}}^{\mathrm{closed}}(E/F)$. In particular, $\mathscr{F}^\star$ maps onto $\mathscr{L}_{\mathrm{sub}}^{\mathrm{closed}}$. Hence, by (a), we see that $\mathscr{F}^\star$ is onto. ♠

We see from Corollary 3.36 that if E/F is finite and $H_1 \leq H_2 \leq \mathrm{Aut}_{F-\mathrm{alg}}(E)$, then $[H_2 : H_1] = [E^{H_1} : E^{H_2}]$. We now introduce one of the central concepts of these notes, namely the concept of a Galois extension.

Definition 3.6 (Galois Extension)**.** *We say that E/F is **Galois** if E/F is a normal, separable extension.*

It is common practice to replace, notationally, $\mathrm{Aut}_{F\text{–alg}}(E)$ with $\mathrm{Gal}(E/F)$ when E/F is Galois. When E/F is Galois, we call $\mathrm{Gal}(E/F)$ the associated **Galois group**.

Exercise 3.19. *Prove that if E/F is Galois and $F \leq K \leq E$, then E/K is Galois.*

As a result of Exercise 3.19, we see that if E/F is Galois, then E/K is Galois. Consequently, we will replace, notationally, $\mathscr{F}^\star(K)$ with $\mathrm{Gal}(E/K)$ when E/F is Galois. The next two exercises establish that being Galois is lifts under taking composites with an arbitrary extension and is preserved under composite/intersection with other Galois extensions.

Exercise 3.20. *Let E/F be Galois and K/F an extension. Prove that EK/K is Galois. [Hint: Use the definition of Galois]*

Exercise 3.21. *Let E_i/F be a collection of Galois extensions of F. Prove that the composite of the E_i is Galois over F and the intersection of the E_i is Galois over F. [Hint: Use the definition of Galois]*

As an application of our work, we have the following result which is often called the **Fundamental Theorem of Galois Theory**. In the statement of the theorem, we will not use the $\mathscr{F}_\star, \mathscr{F}^\star$ notation and will instead use the more traditional notation $\mathscr{F}_\star(H) = E^H$ and $\mathscr{F}^\star(K) = \mathrm{Gal}(E/K)$.

Theorem 3.37 (Fundamental Theorem: Galois Correspondence)**.** *Let E/F be a finite Galois extension.*

(a) *The assigments*
$$H \longmapsto E^H, \quad K \longmapsto \mathrm{Gal}(E/K)$$
are bijective functions between the subgroups of $\mathrm{Gal}(E/F)$ and the intermediate subfields of E/F. Moreover, these bijections are inclusion reversing and inverses.

(b) *If $H \leq \mathrm{Gal}(E/F)$ and $F \leq K \leq E$, then $H = \mathrm{Gal}(E/E^H)$ and $K = E^{\mathrm{Gal}(E/K)}$.*

(c) *For all $F \leq K_1 \leq K_2 \leq E$, we have*
$$[\mathrm{Gal}(E/K_1) : \mathrm{Gal}(E/K_2)] = [K_2 : K_1].$$
In particular, for any $F \leq K \leq E$, we have
$$[K : F] = [\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)], \quad [E : K] = |\mathrm{Gal}(E/K)|.$$

(d) *For all $H_1 \leq H_2 \leq \mathrm{Gal}(E/F)$, we have $[H_2 : H_1] = [E^{H_1} : E^{H_2}]$. In particular, for any $H \leq \mathrm{Gal}(E/F)$, we have*
$$[\mathrm{Gal}(E/F) : H] = [E^H : F], \quad |H| = [E : \mathrm{Gal}(E/E^H)]$$

(e) If $H_1, H_2 \leq \mathrm{Gal}(E/F)$ and $F \leq K_1, K_2 \leq E$, then

$$E^{H_1 \cap H_2} = E^{H_1} E^{H_2}, \qquad E^{H_1 H_2} = E^{H_1} \cap E^{H_2}$$
$$\mathrm{Gal}(E/(K_1 \cap K_2)) = \mathrm{Gal}(E/K_1)\,\mathrm{Gal}(E/K_2) \qquad \mathrm{Gal}(E/K_1K_2) = \mathrm{Gal}(E/K_1) \cap \mathrm{Gal}(E/K_2).$$

Thus far, we have established several properties pertaining to Galois connections and Galois correspondences. What is lacking now is a characterization of Galois extensions in terms of zeroes of polynomials. We will establish a characterization of Galois extension in terms of splitting fields and then use this characterization to connect normal intermediate fields of E/F with normal subgroups of $\mathrm{Gal}(E/F)$.

Theorem 3.38 (Characterization of Galois Extensions)**.** *Let E/F be an extension. Then the following are equivalent:*

(a) E/F is a Galois extension.

(b) If $P \in F[t]$ is any irreducible polynomial such that there exists $\beta \in E$ with $P(\beta) = 0$, then P is separable and splits over E.

(c) E is the splitting field of a collection of irreducible, separable polynomials $\{P_i\} \subset F[t]$.

It is important to extract the roles that normality and separability play in the proof of Theorem 3.38. For that, we will prove a preliminary result before proving Theorem 3.38.

Proposition 3.39. *Let E/F be a normal extension.*

(a) If $\beta \in E$, then P_β splits over E.

(b) E is the splitting field of a collection of polynomials.

Proof. For (a), given $\beta \in E$, we can assume that $P_\beta \in F[t]$, the minimal polynomial of β over F, is at least of degree 2 as otherwise the result is trivial. We take $\mathcal{O}_\beta$ to be the orbit of β under the action of $\mathrm{Aut}_{F-\mathrm{alg}}(E)$. Since every $\beta' \in \mathcal{O}_\beta$ is in $\mathrm{Roots}(P_\beta)$, we know that $\left|\mathcal{O}_\beta\right| \leq \deg(P_\beta)$. We define

$$Q(t) = \prod_{\beta' \in \mathcal{O}_\beta} (t - \beta').$$

Since $\sigma(Q) = Q$ for all $\sigma \in \mathrm{Aut}_{F-\mathrm{alg}}(E)$ and E/F is normal, we deduce that $Q \in F[t]$. As $Q(\beta) = 0$, we know that P_β divides Q. In particular, since $\deg(Q) \leq \deg(P_\beta)$, both polynomials are monic, and P_β is irreducible, it follows that $P_\beta = Q$. Finally, by construction Q splits over E and so P splits over E.

For (b), we know that $E = F(S)$ for some $S \subset E$. Let $\{P_\beta\}_{\beta \in S}$ be the associated minimal polynomials. By (a), we know that each P_β splits over E. As E is generated by S, we know that E is the minimal field for which each polynomial P_β splits, and so E is the splitting field for the collection $\{P_\beta\}_{\beta \in S} \subset F[t]$. ♠

We leave the reader to write out completely why $\sigma(Q) = Q$ for all $\sigma \in \mathrm{Aut}_{F-\mathrm{alg}}(E)$.

Exercise 3.22. *Let E/F be a normal extension, $\beta \in E$, and $\mathcal{O}_\beta = \{\sigma(\beta) : \sigma \in \mathrm{Aut}_{F-alg}(E)\}$. Define*

$$Q(t) = \prod_{\beta' \in \mathcal{O}_\beta} (t - \beta') = \sum_{i=0}^{|\mathcal{O}_\beta|} \alpha_i t^i.$$

Prove that for each $\sigma \in \mathrm{Aut}_{F-alg}(E)$ and each α_i, we have $\sigma(\alpha_i) = \alpha_i$. Deduce that $\alpha_i \in F$ for each i and so $Q \in F[t]$.

Proof of Theorem 3.38. That (a) implies (b) follows from Proposition 3.39. Specifically, given an irreducible polynomial $P \in F[t]$ with root in $\beta \in E$, since P is irreducible, we know that $P = \lambda P_\beta$ for some $\lambda \in F$. By Proposition 3.38, P_β splits over E and so P splits over E. Finally, since E/F is separable, by definition, P must be separable.

For (b) implies (c), note that $E = F(S)$ for some subset $S \subset E$. Setting $\{P_\beta\}_{\beta \in S}$, by assumption each P_β splits over E. Since S generates E, we see that E is the splitting field for the collection of polynomials $\{P_\beta\} \subset F[t]$.

For (c) implies (a), we assume that E is the splitting field for a collection of separable polynomials $\{P_i\}_{i \in I}$ where I is an indexing set for the collection. We can assume that each P has degree at least two as otherwise we can discard it from our collection. By Corollary 3.10, we know that $\mathrm{Aut}_{F-\mathrm{alg}}(E)$ acts transitively on $\mathrm{Roots}(P_i)$ for each i. Since E is the splitting field for the collection $\{P_i\}$, it follows that the only $\mathrm{Aut}_{F-\mathrm{alg}}(E)$–invariant elements of E are in F. Hence, E/F is a normal extension. Since the polynomials P_i are separable, E/F is separable as well, and so by definition of Galois, E/F is a Galois extension. ♠

The concept of a normal extension is directly related to normality of subgroups in a group as we show with our next result.

Proposition 3.40. *Let E/F be a Galois extension.*

(a) If $F \leq K \leq E$ and K/F is normal, then for each $\sigma \in \mathrm{Gal}(E/F)$, we have $\sigma(K) = K$.

(b) If $F \leq K \leq E$ and K/F is normal, then K/F is Galois and $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.

(c) *If* $F \leq K \leq E$ *and* $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$, *then* K/F *is normal.*

Proof. For (a), given $\beta \in K$ and $\sigma \in \mathrm{Gal}(E/F)$, we must show that $\sigma(\beta) \in K$. Since K/F is normal, by Proposition 3.39, we know that P_β splits over K and so $\mathrm{Roots}(P_\beta) \subset K$. By Lemma 3.2, we know that $\sigma(\beta) \in \mathrm{Roots}(P_\beta)$, and so $\sigma(\beta) \in K$.

For (b), since E/F is separable, K/F is separable by Exercise 3.14. As K/F is normal, by definition of Galois, K/F is Galois. By (a), any $\sigma \in \mathrm{Gal}(E/F)$ satisfies $\sigma(K) = K$. In particular, we have a homomorphism $\psi\colon \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ given by $\psi(\sigma) = \sigma_{|K}$. Since every $\tau \in \mathrm{Gal}(K/F)$ can be extended to E by Theorem 3.9, we deduce that ψ is surjective. By definition of ψ, we see that $\ker\psi = \mathrm{Gal}(E/K)$. Hence, by the First Isomorphism Theorem for groups, $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.

For (c), we first argue that $\sigma(K) = K$ for all $\sigma \in \mathrm{Gal}(E/F)$. First, for any $\tau \in \mathrm{Gal}(E/K)$, since $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$, we know that $\sigma^{-1}\tau\sigma = \theta_{\sigma,\tau}$ for some $\theta_{\sigma,\tau} \in \mathrm{Gal}(E/K)$. In particular, $\tau\sigma = \sigma\theta_{\sigma,\tau}$. Given $\beta \in K$, we see that

$$\tau(\sigma(\beta)) = \sigma(\theta_{\sigma,\tau}(\beta)) = \sigma(\beta).$$

In particular, τ fixes $\sigma(\beta)$ for all $\tau \in \mathrm{Gal}(E/K)$. Since E/K is Galois, we have $E^{\mathrm{Gal}(E/K)} = K$ and so $\sigma(\beta) \in K$. Hence, $\sigma(K) = K$ as claimed. To prove that K/F is normal, we will prove K/F Galois. Given an irreducible $P \in F[t]$ with $P(\beta) = 0$ for some $\beta \in K$, since $K \subset E$ and E/F is Galois, we know that P is separable and splits over E by Theorem 3.38. By Lemma 3.2, we know that $\sigma(\beta) \in \mathrm{Roots}(P)$ for each $\beta \in \mathrm{Roots}(P)$ and each $\sigma \in \mathrm{Gal}(E/F)$. As $\sigma(\beta) \in K$ and $\mathrm{Gal}(E/F)$ acts transitively on $\mathrm{Roots}(P)$ by Corollary 3.10, we deduce that $\mathrm{Roots}(P) \subset K$. In particular, P splits over K. Thus, K/F is Galois by Theorem 3.38. As K/F is Galois, by definition, K/F is normal. ♠

We end this section with a corollary of Proposition 3.40 and its proof.

Scholium **3.41.** *Let* E/F *be a Galois extension and* $F \leq F \leq E$. *Then the following are equivalent:*

(a) K/F *is Galois.*

(b) K/F *is normal.*

(c) *For each* $\sigma \in \mathrm{Gal}(E/F)$, *we have* $\sigma(K) = K$.

(d) $\mathrm{Gal}(E/K)$ *is normal in* $\mathrm{Gal}(E/F)$.

3.7 *Extension Fields: Loose Ends*

In this final section of this chapter, we tie up several loose ends. We will prove that finite extensions E/F are simple when $\text{char}(F) = 0$. We will discuss solvability by radicals of polynomials. We will introduce the Galois closure of an algebraic extension. Finally, we will conclude with a brief discussion of the norm and trace maps on a finite Galois extension E/F. Aside from the proof of the Primitive Element Theorem, Theorem 3.42, this section is expository with all of the details either omitted or relegated to exercises for the reader.

Simple Extensions

Our first general result of this section is sometimes referred to as the **Primitive Element Theorem**.

***Theorem* 3.42** (Primitive Element Theorem)**.** *Let E/F be a finite extension and* $\text{char}(F) = 0$*. Then E/F is a simple extension. Specifically, there exists $\beta \in E$ such that $E = F(\beta)$.*

Our proof of Theorem 3.37 is borrowed from the literature. As the method of proof for this result seems to be rather uniform among texts on this topic, it seems unfair to reference a specific one. That said, the argument is clever and one should appreciate that aspect in reading my rendition.

Proof. Since E/F is a finite extension, we know that there exist $\beta_1 \ldots, \beta_r \in E$ such that $E = F(\beta_1, \ldots, \beta_r)$. We will prove the result via induction on r. For $r = 2$, we have $E = F(\beta_1, \beta_2)$ and we let $P_1, P_2 \in F[t]$ be the minimal polynomials for β_1, β_2, respectively. To begin, we select a finite extension E_0/E in which both P_1, P_2 split. Since $\text{char}(F) = 0$, by Lemma 3.31, we know that both P_1, P_2 have distinct zeroes, and we denote these sets by

$$\text{Roots}(P_1) = \{\beta_1, \gamma_2, \ldots, \gamma_{r_1}\}, \quad \text{Roots}(P_2) = \{\beta_2, \theta_2, \ldots, \theta_{r_2}\}.$$

For each $i = 2, \ldots, r_1$ and $j = 2, \ldots r_2$, there is a unique $\lambda_{i,j} \in E_0$ such that

$$\beta_1 + \lambda_{i,j}\beta_2 = \gamma_i + \lambda_{i,j}\theta_j.$$

Specifically,

$$\lambda_{i,j} = \frac{\gamma_i - \beta_1}{\beta_2 - \theta_j}.$$

By Lemma 2.21, we know that F is infinite and so there exists $\lambda \in F$ such that

$$\beta_1 + \lambda\beta_2 \neq \gamma_i + \lambda\theta_j$$

for all $i = 2, \ldots, r_1$ and $j = 2, \ldots, r_2$. Setting $\beta = \beta_1 + \lambda\beta_2$, we assert that $F(\beta) = F(\beta_1, \beta_2)$; for notational simplicity, set $F_\beta = F(\beta)$. By definition of β, we see that $\beta \in F(\beta_1, \beta_2)$ and so $F_\beta \leq F(\beta_1, \beta_2)$. For the

reverse inclusion, it suffices to show that $\beta_1, \beta_2 \in F_\beta$. Note that if $\beta_2 \in F(\beta)$, since $\beta = \beta_1 + \gamma\beta_2$ with $\gamma \in F$, we see that $\beta_1 = \beta - \gamma\beta_2 \in F_\beta$. In particular, it suffices to show that $\beta_2 \in F_\beta$.

To that end, define $Q(t) = P_1(\beta - \gamma t)$ and note that $Q(t) \in F_\beta[t]$ and that

$$Q(\beta_2) = P_1(\beta - \gamma\beta_1) = P_1(\beta_1) = 0.$$

It follows that $t - \beta_2$ is a common divisor of both P_2, Q over E_0. We assert that $\gcd(P_2, Q) = (t - \beta_2)$. To see this claim, note that since P_2 is separable, $(t - \beta_2)^2$ cannot divide P_2. By selection of γ, we know that no factors $(t - \theta_j)$ can divide Q. Consequently, $\gcd(P_2, Q) = (t - \beta_2)$ over E_0. Since both $P_2, Q \in F_\beta[t]$, it follows that $\gcd(P_2, Q) \neq 1$ over F_β (see Exercise 3.23 below). Since $t - \beta_2$ is degree 1, we conclude that $\gcd(P_2, Q) = t - \beta_2$ in $F_\beta[t]$. In particular, $t - \beta_2 \in F_\beta[t]$ and so $\beta_2 \in F_\beta$.

For the general case, given $E = F(\beta_1, \ldots, \beta_r)$, we apply the base case to deduce that $F(\beta_1, \beta_2) = F(\beta)$ for some $\beta \in F(\beta_1, \beta_2)$. Hence, $E = F(\beta, \beta_3, \ldots, \beta_r)$ and so by the induction hypothesis, we conclude that there exists $\beta' \in E$ such that $E = F(\beta')$. ♠

Exercise 3.23. *Prove that if $P, Q \in F[t]$ have $\gcd(P, Q) = 1$, then for any finite extension E/F, we have $\gcd(P, Q) = 1$ where $P, Q \in E[t]$.*

Exercise 3.24. *Find $\beta \in E$ such that $E = F(\beta)$ for the examples below:*

(i) $F = \mathbf{Q}$ *and* $E = \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

(ii) $F = \mathbf{Q}(\sqrt{2})$ *and* $E = F(\sqrt{3}, \sqrt{11})$.

Radical Extensions

Given a finite extension E/F, we write $E = F(\sqrt[n]{\alpha})$ or $F(\alpha^{1/n})$ if there exists a $\beta \in E$ such that $\beta^n = \alpha$ and $E = F(\beta)$. We say that β is an n**th root** of α in this case. Given an nth root of α, say β, it follows that β is a zero of the polynomial $t^n - \alpha$, which is in $F[t]$.

Definition 3.7 (Extension by Radicals)**.** *We say that a finite extension E/F is a* ***extension by radicals*** *or* ***radical extension*** *if there exists a sequence of extensions E_i/E_{i-1} for $i = 1, \ldots, m$ such that $E_0 = F$, $E = E_m$, and $E_i = E_{i-1}(\alpha^{1/\ell_i})$ where $\ell_i > 1$ and $\alpha \in E_{i-1}$.*

Definition 3.8 (Solvable by Radicals)**.** *We say that a polynomial $P \in F[t]$ is* ***solvable by radicals*** *if the splitting field for P over F is an extension by radicals.*

One of the striking achievements of Galois theory is that there is a characterization of when a polynomial is solvable by radicals in terms of the structure of the Galois group of the splitting field for the polynomial.

Prior to this characterization given by **Galois**, there where already examples of degree 5 polynomials that were not solvable by radical; see the **Abel–Ruffini Theorem**. We record here a simple consequence of Exercise 2.66 that says that a degree 2 polynomial is always solvable by radicals.

***Lemma* 3.43.** *If $P \in F[t]$ has degree two, then P is solvable by radicals. Indeed, the splitting field of P is given by $F(\sqrt{\Delta(P)})$ where $\Delta(P)$ is the discriminant of P.*

Polynomials of degree 3 and 4 are always solvable by radicals. This is classical and the formulas for the cubic can be found **here** while the formula for the quartic can be found **here**. These formulas make use of roots of unity, which we now discuss.

***Definition* 3.9** (Roots of Unity)**.** *Given an integer $n \in \mathbf{N}$ and a field F, we say that $\beta \in \overline{F}$ is an **nth root of unity** if $\beta \in \text{Roots}(t^n - 1)$.*

If $F = \mathbf{Q}$, we see that a second root of unity is a zero of the polynomial $t^2 - 1$ and so must be ± 1. A fourth root of unity is a solution to

$$t^4 - 1 = (t^2 - 1)(t^2 + 1)$$

and so the fourth roots of unity are $\{1, -1, i, -i\}$.

***Exercise* 3.25.** *Let $n \in \mathbf{N}$ and F be a field. If $\zeta_n \in F$ is an nth root of unity, prove that ζ_n^ℓ is an nth root of unity for any $\ell = 1, \ldots, n$.*

***Exercise* 3.26.** *Prove that if $m, n \in \mathbf{N}$ and m divides n, then $t^m - 1$ divides $t^n - 1$. Deduce that if ζ_m is an mth root of unity, then ζ_m is an nth root of unity for any n such that m divides n.*

***Exercise* 3.27.** *Prove that if $n \in \mathbf{N}$ and $\text{char}(F) = 0$, then there exists an nth root of unity ζ_n that is not an mth root of unity for any m that divides n. We call any nth root of unity with this property a **primitive root of unity**.*

***Exercise* 3.28.** *Let $n \in N$, $\text{char}(F) = 0$, and ζ_n be a primitive nth root of unity. Prove that if ζ is an nth root of unity, then $\zeta = \zeta_n^\ell$ for some $\ell = 1, \ldots, n$. Deduce that $\text{Roots}(t^n - 1) = \{\zeta_n, \zeta_n^2, \ldots, \zeta_n^n\}$.*

***Exercise* 3.29.** *Let F be a field with $\text{char}(F) = 0$. Prove that if $\zeta_n \in F$ is an nth root of unity, then $\zeta_n \in \overline{\mathbf{Q}}$. In particular, when studying roots of unity over characteristic zero fields, it suffices to use $F = \mathbf{Q}$.*

Roots of unity are important in the study of Galois extensions E/F such that $\text{Gal}(E/F)$ is an abelian groups; the study of such extensions is often called **Kummer theory**. The relevance of roots of unity in our current discuss can be seen by the following example.

***Example* 3.1.** *Let $P(t) = t^3 - \alpha$ for $\alpha \in F$ with $\text{char}(F) = 0$. We see that if $\beta \in \text{Roots}(P)$ and $\zeta_3 \in \overline{F}$ is a 3rd root of unity, then $\zeta_3\beta \in \text{Roots}(P)$. Moreover, if ζ_3 is a primitive 3rd root of unity, then $\text{Roots}(P) = \{\beta, \zeta_3\beta, \zeta_3^2\beta\}$.*

Roots of unity appear in the formulas for the zeros of a polynomial of degree 3 and 4 over $\mathbf{Q}$ (or any field F with $\text{char}(F) = 0$).

We now state the characterization of polynomials which are solvable by radicals.

Theorem 3.44 (Solvable by Radicals)**.** *If $P \in F[t]$ and F_P is the splitting field for P over F, then the following are equivalent:*

(a) P is solvable by radicals.

(b) $\text{Gal}(F_P/F)$ is a solvable group.

We will not prove Theorem 3.44 despite its historical importance. However, we will briefly discuss why polynomials of degree at most 4 are always solvable by radicals using Theorem 3.44. Recall, if P is an irreducible polynomial of degree n, then there is an injective homomorphism $\text{Gal}(F_P/F) \to \text{Sym}(n)$, where $\text{Sym}(n)$ is the symmetric group on a set of size n. The symmetric group $\text{Sym}(2)$ is an abelian group of order 2 and when P has degree two and is separable, we see that $\text{Gal}(F_P/F) = \text{Sym}(2)$. If $\deg(P) = 3$, we can view $\text{Gal}(F_P/F)$ as a subgroup of $\text{Sym}(3)$, which is a solvable group of order 6. Assuming P is irreducible and separable, $\text{Gal}(F_P/F)$ is either $\text{Sym}(3)$ or the order 3 subgroup generated by the element (123). Either way, since subgroups of solvable groups are solvable, $\text{Gal}(F_P/F)$ is solvable.

Exercise 3.30. *Let $F = \mathbf{Q}$, $P \in \mathbf{Q}[t]$, and F_P be the splitting field for P.*

(i) Prove that if $P = t^3 - 1$, then $\text{Gal}(F_P/\mathbf{Q})$ is a cyclic group of order three. [Hint: Prove that if ζ_3 is a primitive 3rd root of unity, then $F_P = \mathbf{Q}(\zeta_3)$ and $\zeta_3 \to \zeta_3^2$ generates $\text{Gal}(F_P/\mathbf{Q})$]

(ii) Prove that if $P = t^3 - 2$, then $\text{Gal}(F_P/\mathbf{Q}) = \text{Sym}(3)$. [Hint: It is enough to prove that $[F_P : \mathbf{Q}] = 6$]

(iii) List the subgroups of $\text{Sym}(3)$ and the associate subfields of F_P in (ii) under the Galois correspondence.

For $\deg(P) = 4$, we again have an injective homomorphism $\text{Gal}(F_P/F) \to \text{Sym}(4)$. It turns out that $\text{Sym}(4)$ is also solvable and so $\text{Gal}(F_P/F)$ is solvable. There are more possibilities for $\text{Gal}(F_P/F)$ when $\deg(P) = 4$. As $\text{Gal}(F_P/F)$ acts transitively, this reduces the possibilities to the subgroups of $\text{Sym}(4)$ that act transitively on $\{1,2,3,4\}$; one typically replaces the set of size 4 with the set $\{1,2,3,4\}$.

Given that $\text{Sym}(2), \text{Sym}(3)$, and $\text{Sym}(4)$ are all solvable, one might expect this to hold for higher n. In fact, it fails for all $n > 4$. Specifically, $\text{Sym}(n)$ is not solvable for any $n \geq 5$. Moreover, $\text{Sym}(n)$ is quite far from being solvable since it has precisely one normal subgroup $\text{Alt}(n)$, which has index 2. The

subgroup $\mathrm{Alt}(n)$ is a simple group (i.e. it has no non-trivial, proper normal subgroups) and simple groups are, in some sense, as far from being solvable as possible.

Given a random irreducible polynomial $P \in \mathbf{Q}[t]$ of degree n, the expectation is that $\mathrm{Gal}(F_P/\mathbf{Q})$ is either $\mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$. In particular, one expects that a typical polynomial is not solvable by radicals. Oddly enough, a random finite group is typically solvable. A deep result of Feit–Thompson states that any finite group with odd order is solvable; the first proof of this "fact" was longer than these notes (see **here** for more on this). The somewhat contradictory nature of these two claims is rectified by the fact that for a random polynomial, the Galois group of the splitting field tends to be as large as possible. So despite the fact that most finite groups are solvable, most polynomials are not solvable by radicals.

Whether or not every every finite group G is the Galois group of a Galois extension $E/\mathbf{Q}$ is an open question and is referred to as the **inverse Galois problem**. It is known by work of Shafarevich that every finite solvable group arises as the Galois group of a Galois extension of $\mathbf{Q}$.

Galois Closure

Given a finite extension E/F (or more generally, an algebraic extension), we know that there exists an (injective) F–algebra homomorphism $\psi\colon E \to \overline{F}$. Given ψ, we can take a Galois closure of E by setting

$$E_{\psi,\mathrm{Gal}} = \bigcap_{\substack{E \leq L \leq \overline{F} \\ L/F \text{ Galois}}} L.$$

The extension $E_{\psi,\mathrm{Gal}}/F$ is Galois and is the smallest subfield of $\overline{F}$ that contains $\psi(E)$ and is Galois over F.

Exercise **3.31.** *Prove that if $\psi_1, \psi_2 \in \mathrm{Hom}_{F-alg}(E, \overline{F})$, then $E_{\psi_1,\mathrm{Gal}} = E_{\psi_2,\mathrm{Gal}}$.*

As a result of Exercise 3.31, we see that $E_{\psi,\mathrm{Gal}}$ is independent of the choice of ψ and so we define the **Galois closure** of E/F, which we denote simply by E_{Gal}, to be $E_{\psi,\mathrm{Gal}}$ for any $\psi \in \mathrm{Hom}_{F-\mathrm{alg}}(E, \overline{F})$.

Exercise **3.32.** *Prove that if E/F is a finite extension, then E_{Gal}/F is a finite extension.*

In practice, one sometimes passes to E_{Gal} when trying to understand an extension E/F as one is afforded many nice properties that otherwise might not hold in E/F.

Norm and Trace

Given a finite Galois extension E/F, we define a pair of function

$$\mathrm{Tr}_{E/F}\colon E \to F, \quad \mathrm{N}_{E/F}\colon E \to F$$

defined by

$$\mathrm{Tr}_{E/F}(\beta) = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\beta), \quad \mathrm{N}_{E/F}(\beta) = \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\beta).$$

The function $\mathrm{N}_{E/F}$ is referred to as the **norm** and the function $\mathrm{Tr}_{E/F}$ is referred to as the **trace**. We leave the reader the task of proving that these function take values in F.

Exercise 3.33. *Prove that* $\mathrm{Tr}_{E/F}(\beta), \mathrm{N}_{E/F}(\beta) \in F$. *[Hint: Use normality]*

Using the trace function, we can form endow E with a bilinear form. Namely, the function

$$B_{E/F} \colon E \times E \to F$$

given by $B_{E/F}(\beta_1, \beta_2) = \mathrm{Tr}_{E/F}(\beta_1 \beta_2)$.

Definition 3.10 (Bilinear Form)**.** *Given an F–vector space V and a function $B \colon V \times V \to F$, we say that B is a **F–bilinear form** if B satisfies the following properties:*

(a) For all $u, v, w \in V$, we have

$$B(u, v+w) = B(u,v) + B(u,w), \quad B(u+v, w) = B(u,w) + B(v,w).$$

(b) For all $u, v \in V$ and $\alpha \in F$, we have

$$B(\alpha u, v) = B(u, \alpha v) = \alpha B(u,v).$$

*We say that B is **symmetric** if in addition, we have*

(c) For all $u, v \in V$, we have

$$B(u,v) = B(v,u).$$

*Finally, we say B is **non-degenerate** if we have the following property:*

(d) For each $u \in V$ with $u \neq 0$, there exists $v_u \in V$ such that $B(u, v_u) \neq 0$.

Exercise 3.34. *Prove that $B_{E/F}$ is a symmetric, F–bilinear form.*

Given any finite dimensional F–vector space V and any F–bilinear form B on V, the **B–orthogonal group** is defined to be

$$\mathrm{O}(V,B) \stackrel{\text{def}}{=} \{L \in \mathrm{Hom}_{F\text{–lin}}(V,V) \ : \ B(L(v), L(w)) = B(v,w) \text{ for all } v, w \in V\}.$$

Exercise 3.35. *Prove that if B is non-degenerate, then $\mathrm{O}(V,B)$ is a subgroup of $\mathrm{Aut}_{F\text{–}lin}(V)$.*

Exercise 3.36. *Let $B_{E/F}$ be as in Exercise 3.34. Prove that if $\sigma \in \mathrm{Gal}(E/F)$ and $\beta_1, \beta_2 \in E$, then*

$$B_{E/F}(\sigma(\beta_1), \sigma(\beta_2)) = B_{E/F}(\beta_1, \beta_2).$$

Since E/F is an F–vector space and $B_{E/F}$ is an (non-degenerate; see Exercise 3.8) F–bilinear form on E, by Exercise 3.36, we see that $\mathrm{Gal}(E/F)$ can be viewed as a subgroup of $\mathrm{O}(E, B_{E/F})$.

Exercise 3.37. *Prove that*

$$E^1 = \left\{\beta \in E \ : \ \mathrm{N}_{E/F}(\beta) = 1\right\}$$

is a group under multiplication.

The group E^1 is called the group of norm 1 elements as one refers to $\mathrm{N}_{E/F}(\beta)$ as the norm of β.

Exercise 3.38. *Let $F \leq K \leq E$ with K/F and E/K finite Galois extensions. Prove that*

$$\mathrm{N}_{K/F} \circ \mathrm{N}_{E/K} = \mathrm{N}_{E/F}, \quad \mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{E/K} = \mathrm{Tr}_{E/F}.$$

Exercise 3.39. *Let E/F be a finite Galois extension with $[E:F] = m$. Recall that we have $L\colon E \to \mathrm{Mat}(m,F)$. Given $\beta \in E$, prove that*

$$\mathrm{Tr}(L(\beta)) = \mathrm{Tr}_{E/F}(\beta) = [E : F(\beta)] \left(\sum_{\beta' \in \mathrm{Roots}(P_\beta)} \beta' \right)$$

$$\det(L(\beta)) = \mathrm{N}_{E/F}(\beta) = \left(\prod_{\beta' \in \mathrm{Roots}(P_\beta)} \beta' \right)^{[E:F(\beta)]}$$

where P_β is the minimal polynomial for β over F.

Bibliography

[1] D. B. McReynolds, *Discrete Math*, Class Notes.

[2] D. B. McReynolds, *Linear Algebra*, Class Notes.

[3] D. B. McReynolds, *Real Analysis*, Class Notes.