Math 503: Bridge To Algebra

Contents

A Few First Words

The primary purpose for these notes is to serve as the class textbook for a first graduate class in algebra. This class is designed to serve as a bridge between undergraduate and graduate algebra. Hence, the title of the notes! Typically a student enrolled in this class will take a standard first course in graduate algebra which also has a qualifying exam attached to it.

First, exercises will appear through the notes. A devoted reader should work as many of the exercises as possible to maximize understanding. At the end of some sections, additional reading material may appear. This material is not covered in the class lectures though. Additional reading material labeled with a * is considered essential reading will those without the * label should still be read but will not be tested on. Any text labeled **blue** will have a link attached to it. Typically, the links are to wikipedia pages or videos discussing the relevant concept or topic. In particular, I advise students to read the notes on a device with access to the internet.

Now to some more specifics about the mathematical content of this note. As this class sits in some sort of purgatory between undergraduate and graduate level mathematics, I have decided to experiment in the broad layout of the material. The notes will start with a brief review of some preliminary material on sets and functions. Some of the additional reading sections in this first chapter will be essential later in the notes. Next, we will introduce several different types of algebraic structures on sets. We will study subobjects and morphisms between objects in each of these different algebraic settings. We will also discuss quotients and various types of "isomorphism theorems". We end with a discussion on commutative diagrams and categories. This chapter is rather abstract and focuses on the commonalities between various types of algebraic structures. There are essentially no examples in this chapter, at least not without following the external links. The second chapter will investigate group actions on sets with a focus on basics and fundamental examples. The chapter will end with the Orbit–Stabilizer Theorem. The third chapter gives a thorough introduction to group theory with a focus on the general theory (as opposed the typical focus on finite groups). Free groups, generation of groups, and presentations of groups are covered along with Tietze transformations and decision problems. The chapter ends with three sections of finite groups, a section on finitely generated commutative groups, and two sections on infinite groups.

The third chapter focuses on rings and ideal theory. Finiteness conditions like Noetherian and Artinian are covered and the existence of maximal ideals is established. The fourth chapter studies polynomial rings with a focus on unique factorization and ideal theory. The fifth chapter gives a brief introduction to basic concepts from field theory. The last chapter gives an overview of some basic and fundamental results from the theory of algebras and Artin–Wedderburn Theory.

Chapter 0

Preliminaries

Contents

In this brief preliminary chapter, we record some basic facts from set theory and functions. We will also briefly review partial relations, equivalence relations, and quotient spaces. Additionally, we list some basic notation and terminology that we will make use of throughout this text.

0.1 *Sets*

Set theory is the area of mathematics that develops the concept of a set and the fundamental operations on sets. Sets are the most basic objects that one deals with in mathematics. For most topics, sets serve as a universe for developing mathematical concepts.

Informally, a **set** X is a collection of objects. When X is equipped with additional structure, like a metric or a topology, we often refer to the individual objects of a set X as points and we often refer to X as a space. When X is a vector space, we might refer to the elements of X as vectors. However, that language can be somewhat misleading as a set could be a collection of objects with no inherit meaning. For instance, one can have sets of sets, sets of functions, and so forth. From a physical viewpoint, we can view a set as the possible locations/places in our universe, which is the typical view when X is a metric space or topological space. When x is an element of X, we write $x \in X$.

The most basic set is the **empty set** that we denote by $\emptyset$. This set is the set with no objects. A set with a single object is referred to as a **singleton set**. If X is a singleton set, then we could write $X = \{x\}$, where $x \in X$ denotes the unique element in X. The symbol x has no inherit meaning aside from denoting this unique element. In this notation, the empty set could be written as $\emptyset = \{\,\}$.

***Remark* 0.1.** *The empty set and the set that contains the empty set are two different sets. One is empty and one is a singleton set. In particular,* $\emptyset \neq \{\emptyset\}$.

For our present purposes, there are several sets that we will make extensive use of.

1. **The Natural Numbers**[1]. The set $\mathbf{N}$ of natural numbers is defined to be $\mathbf{N} = \{1,2,3,4,\dots\}$. Note that we have a comparison relation on the set of natural numbers given by the numerical value of the elements. For example, $3 < 13$, $4 < 201$, and so forth. Given $a,b \in \mathbf{N}$, there is $c \in \mathbf{N}$ such that $a \leq c$ and $b \leq c$. The element c is not unique since $c+1$ would also satisfy these conditions, relative to a,b. However, we could just take $c = \max\{a,b\}$. The product and sum of finitely many natural numbers are also natural numbers.

2. **The Integers**. The set of integers $\mathbf{Z}$ is the set of all whole numbers, both positive and negative. We also include 0. Hence $\mathbf{Z} = \{0,\pm 1,\pm 2,\pm 3,\pm 4,\dots\}$. Products and sums of finitely many integers are integers. We have the same comparison relation $<$ on the integers as we did with the natural numbers.

3. **The Rational Numbers**. The rational numbers are the numbers given by m/n where $m,n \in \mathbf{Z}$. For example, $1/2$, $-10/21$, and 3 are all examples of rational numbers. The set of rational numbers is denoted by $\mathbf{Q}$. Again products and sums of finitely many rational numbers are rational numbers, something you have known since you first began working with fractions. For example,

$$\frac{1}{2} + \frac{1}{3} = \frac{3}{6} + \frac{2}{6} = \frac{5}{6}$$

and $\frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$. In fact, in the summation example, we used something that is both important and slightly subtle that rational numbers really represent sets of fractions. For instance, the rational number 1 has many expressions as a fraction:

$$[1] = \left\{1, \frac{-1}{-1}, \frac{2}{2}, \frac{-2}{-2}, \frac{3}{3}, \dots\right\}.$$

We say two fractions m_1/n_1 and m_2/n_2 are **equivalent** if $m_1 n_2 = m_2 n_1$. A rational number is then seen to be a collection of equivalent fractions. One convenient way to describe 1 as a collection of

[1] Whether or not one includes 0 in $\mathbf{N}$ is not uniform among mathematicians. There seems to be good reasons for each opinion and I have chosen the present convention arbitrarily. I will try to be consistent with this choice.

equivalent fractions is via

$$[1] = \left\{ \frac{m}{m} \ : \ m \in \mathbf{Z},\ m \neq 0 \right\}.$$

More generally, given $m_0, n_0 \in \mathbf{Z}$ with $n_0 \neq 0$, we have

$$\left[\frac{m_0}{n_0} \right] = \left\{ \frac{m}{n} \ : \ m_0 n = m n_0 \right\}.$$

The colon in the above two expressions should be read as "such that". An alternative for " : " is "|"

$$[1] = \left\{ \frac{m}{m} \mid m \in \mathbf{Z},\ m \neq 0 \right\}.$$

We have a comparison relation on rational numbers. Given $a, b \in \mathbf{Q}$, precisely one of the following:

$$a < b, \quad b < a, \quad a = b.$$

We will make use of these comparison relations throughout this text.

4. **The Real Numbers**. For now, we will simply define the real numbers to be the set of real numbers and denote this set by $\mathbf{R}$. As with the rational numbers, the real numbers are really collections of objects that all represent the "same thing". That said, you have seen the real numbers before and should think of them as you prefer. Examples of real numbers are the natural numbers, the integers, the rational numbers, and numbers like $\pi, e, \sqrt{5}$. As before, we have a comparison relation on the real numbers. Given $a, b \in \mathbf{R}$, we have precisely one of the following:

$$a < b, \quad b < a, \quad a = b.$$

We now return to our abstract discussion of sets. Given a set X, we say that a set A is a **subset** of X if for each element $a \in A$, we have $a \in X$. When A is a subset of X, we write $A \subseteq X$. The symbol $\subseteq$ is read as "a subset of with possible equality" whereas the symbol $\subset$ is read "as a proper subset". This is analogous to the less than or equal to symbol $\leq$ and the less than symbol $<$. Given a pair of subsets $A, B \subseteq X$, we can form the **intersection** and **union** of A and B. The intersection of A and B, which we denote by $A \cap B$, is defined to be

$$A \cap B \stackrel{\text{def}}{=} \{ x \in X \ : \ x \in A \text{ and } x \in B \}.$$

Informally, this subset of X is the subset of all elements of X that are elements of both A and B. The union of A and B, which we denote $A \cup B$, is defined to be

$$A \cup B \stackrel{\text{def}}{=} \{ x \in X \ : \ x \in A \text{ or } x \in B \}.$$

Informally, this subset of X is the subset of all elements of X that are elements of either A or B. The following lemma is left an an exercise.

Lemma **0.2.** *Let X be a set with $A,B,C \subseteq X$.*

(a) $A \cap B \subseteq A$, $A \cap B \subseteq B$.

(b) $A \subseteq A \cup B$, and $B \subseteq A \cup B$.

(c) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(d) If $C \subseteq A$ and $C \subseteq B$, then $C \subseteq A \cap B$.

(e) If $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.

Even the simplest statements can be difficult to prove when first starting mathematics. As the reader may not have any training in writing mathematical proofs, we will prove Lemma 0.2 (a).

Proof of Lemma 0.2 (a). To prove $A \cap B \subseteq A$, by definition of $\subseteq$, we must prove that for each $x \in A \cap B$, that $x \in A$. By definition of $A \cap B$, if $x \in A \cap B$, then $x \in A$ and $x \in B$. In particular, $x \in A$ and hence $A \cap B \subseteq A$. The proof of $A \cap B \subseteq B$ is logically identical. ♠

Remark **0.3.** *The standard method for showing $A \subseteq B$ is to prove that each $x \in A$ must satisfy $x \in B$. Without context, this does not have much content. However, this is precisely the method of proof we used in the above proof and is the method of proof for verifying Lemma 0.2.*

The other three subset containments are done similarly. Returning to our discussion of sets, we say that two subsets $A,B \subseteq X$ are **equal** if $A \subseteq B$ and $B \subseteq A$. In this case, we denote equality by $A = B$.

Remark **0.4.** *To show that two sets A,B are equal, the standard method of proof is to prove that $A \subseteq B$ and $B \subseteq A$. Again, without context, this does not mean much but it is a standard method from establishing set equality.*

We say that subsets $A,B \subseteq X$ are **disjoint** if $A \cap B = \emptyset$. Disjoint sets are as far away from being equal as a pair of sets can be in that they have no overlap or common element. Given $A \subseteq X$, if $x \in X$ is not an element of the subset A, we write $x \notin A$. The **complement** of A in X, denoted by $X - A$, is defined to be

$$X - A \stackrel{\text{def}}{=} \{x \in X \ : \ x \notin A\}.$$

Informally, $X - A$ is the subset of X of elements that are not elements of A (see this video for more on intersections, unions and complements). It is left as an exercise to prove the following:

- $A \cap (X - A) = \emptyset$

- $A \cup (X - A) = X$
- If $A \subseteq B$, the $X - B \subseteq X - A$.

The **power set** of X is the set $\mathscr{P}(X)$ of all subsets of X. Any subset $I \subset \mathscr{P}(X)$ is a collection of subsets of X. We can define the union and intersection of a collection of subsets $I \subseteq \mathscr{P}(X)$. Formally,

$$\bigcup_{A \in I} A \stackrel{\text{def}}{=} \{x \in X \ : \ x \in A \text{ for some } A \in I\}$$

and

$$\bigcap_{A \in I} A \stackrel{\text{def}}{=} \{x \in X \ : \ x \in A \text{ for all } A \in I\}.$$

The operations of intersection, union, and complements are related by **De Morgan's laws** (see this video on De Morgan's Laws).

***Proposition* 0.5** (De Morgan's Laws)**.** *Let X be a set and $I \subseteq \mathscr{P}(X)$.*

(a)

$$X - \left(\bigcup_{A \in I} A \right) = \bigcap_{A \in I} (X - A).$$

(b)

$$X - \left(\bigcap_{A \in I} A \right) = \bigcup_{A \in I} (X - A).$$

Proof. For (a), to prove $X - (\bigcup_{A \in I} A) = \bigcap_{A \in I} (X - A)$, we will prove

$$X - \left(\bigcup_{A \in I} A \right) \subseteq \bigcap_{A \in I} (X - A) \text{ and } \bigcap_{A \in I} (X - A) \subseteq X - \left(\bigcup_{A \in I} A \right).$$

By definition of set equality, if we verify both of these containments, we will prove (a). Given $x \in X - (\bigcup_{A \in I} A)$, by definition of the complement, $x \notin \bigcup_{A \in I} A$ and so $x \notin A$ for each $A \in I$. Since $x \in X$ and $x \notin A$, we see that $x \in X - A$ for each $A \in I$. Therefore, by definition of intersection, $x \in \bigcap_{A \in I} (X - A)$. For the reverse containment, let $x \in \bigcap_{A \in I} (X - A)$. By definition of intersections, $x \in X - A$ for each $A \in I$. By definition of complements, $x \in X$ and $x \notin A$ for each $A \in I$. Hence, by definition of union, $x \notin \bigcup_{A \in I} A$, and so $x \in X - \bigcup_{A \in I} A$.

For (b), we will proceed as we did in (a). In particular, it suffices to prove the set containment

$$X - \left(\bigcap_{A \in I} A \right) \subseteq \bigcup_{A \in I} (X - A) \text{ and } \bigcup_{A \in I} (X - A) \subseteq X - \left(\bigcap_{A \in I} A \right).$$

Given $x \in X - (\bigcap_{A \in I} A)$, we see that $x \in X$ and $x \notin \bigcap_{A \in I} A$. By definition of intersection, there exists some $A_0 \in I$ such that $x \notin A_0$. Since $x \in X$ and $x \notin A_0$, it follows by definition of complements that $x \in X - A_0$ for some $A_0 \in I$. Hence, by definition of unions, $x \in \bigcup_{A \in I} (X - A)$. For the second containment, given $x \in \bigcup_{A \in I} (X - A)$, by definition of union, $x \in X - A_0$ for some $A_0 \in I$. By definition of complements, $x \in X$ and $x \notin A_0$, and so by definition of intersections, we see that $x \notin \bigcap_{A \in I} A$. By definition of complements, we have $x \in X - (\bigcap_{A \in I} A)$. ♠

0.2 *Functions*

We now introduce the concept of a function (see Gowers' blog post on this topic). Given two sets X, Y, a **function** f from X to Y, denoted by $f : X \to Y$, associates to each $x \in X$, a unique $y \in Y$ that we denote by $f(x) = y$. We stress that each x is associated to exactly one $y \in Y$ though there could be another $x' \in X$ that is associated to the same y. We refer to X has the **domain** of f and we refer to Y as the **codomain**. The **image** of f, denoted by $f(X)$, is the subset of Y defined by

$$f(X) \stackrel{\text{def}}{=} \{ y \in Y \ : \ y = f(x) \text{ for some } x \in X \}.$$

This subset of Y is also referred to as the range of f. Given any subset $A \subseteq X$, we define

$$f(A) \stackrel{\text{def}}{=} \{ y \in Y \ : \ y = f(x) \text{ for some } x \in A \}.$$

For any subset $B \subseteq Y$, we define the **preimage** or **inverse image** of B by

$$f^{-1}(B) \stackrel{\text{def}}{=} \{ x \in X \ : \ f(x) \in B \}.$$

We stress that for a function $f : X \to Y$ with $A \subseteq X$ and $B \subseteq Y$, that $f(A) \subseteq Y$ and $f^{-1}(B) \subseteq X$.

***Lemma* 0.6.** *Let X, Y be sets and $f : X \to Y$ be a function.*

(a) For any subset $I \subseteq \mathscr{P}(X)$, we have

$$f\left(\bigcup_{A \in I} A \right) = \bigcup_{A \in I} f(A).$$

(b) For any subset $I \subseteq \mathscr{P}(X)$, we have

$$f\left(\bigcap_{A\in I} A\right) \subseteq \bigcap_{A\in I} f(A).$$

(c) For any subset $J \subseteq \mathscr{P}(Y)$, we have

$$f^{-1}\left(\bigcup_{B\in J} B\right) = \bigcup_{B\in J} f^{-1}(B).$$

(d) For any subset $J \subseteq \mathscr{P}(Y)$, we have

$$f^{-1}\left(\bigcap_{B\in J} B\right) = \bigcap_{B\in J} f^{-1}(B).$$

We leave the proof of Lemma 0.6 as an exercise. Given a function $f\colon X \to Y$ and $A \subseteq X$, we have an associated function $f_{|A}\colon A \to Y$ called the **restriction of f to A**. Formally, for each $a \in A$, we define $f_{|A}(a) \stackrel{\text{def}}{=} f(a)$. Given sets X, Y, Z and functions $f\colon X \to Y$, $g\colon Y \to Z$, we have the **composition** of f and g, denoted by $g \circ f$, which is a function $g \circ f\colon X \to Z$ defined by $(g \circ f)(x) \stackrel{\text{def}}{=} g(f(x))$.

***Definition* 0.1** (One-to-one)**.** *We say that a function $f\colon X \to Y$ is **one-to-one** or **injective** if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ for any pair $x_1, x_2 \in X$.*

***Definition* 0.2** (Onto)**.** *We say that a function $f\colon X \to Y$ is **onto** or **surjective** if for each $y \in Y$, there exists $x \in X$ such that $f(x) = y$.*

***Definition* 0.3** (Bijective)**.** *We say that a function is **bijective** if f is both one-to-one and onto.*

Examples: Below are some basic examples of functions.

- **Identity Function**. Given any set X, we define the identity function $\mathrm{Id}_X\colon X \to X$ by $\mathrm{Id}_X(x) = x$. This function is bijective.
- **Constant Function.** Given any sets X, Y and an element $y_0 \in Y$, we can define the constant function $f\colon X \to Y$ by $f(x) = y_0$. This function is one-to-one if and only if X is a singleton set. This function is onto if and only if Y is a singleton set.
- **Inclusion Function**. Given any set X and any subset $A \subseteq X$, we define the inclusion function $\iota_{A,X}\colon A \to X$ by $\iota_{A,X}(a) = a$. This function is always one-to-one, and is onto if and only if $A = X$.

- **Characteristic Function**. Given any set X and any subset $A \subseteq X$, we define the characteristic function or indicator function $\chi_{A,X}: X \to \{0,1\}$ of A in X by

$$\chi_{A,X}(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A. \end{cases}$$

  Note that $\chi_{A,X} \circ \iota_{A,X}$ is the constant function that assigns to each $a \in A$, the value 1.

If $f: X \to Y$ is a bijective function, then there exists a unique function $g: Y \to X$ such that $(g \circ f) = \mathrm{Id}_X$ and $(f \circ g) = \mathrm{Id}_Y$. We call the function g with these properties the **inverse of f** and denote it by f^{-1}. In more detail, we discuss the construction of the inverse. For each $y \in Y$, since f is onto, there exists $x \in X$ such that $f(x) = y$. Since f is one-to-one, we know that this x is unique. We define $f^{-1}(y) = x$ where $f(x) = y$.

Remark 0.7. *For any function $f: X \to Y$, we can try to implement the same ideas used in constructing f^{-1}. The function will only be defined on the image $f(X)$ of f. Given $y \in f(X)$, there exists $x \in X$ such that $f(x) = y$. Hence, we define $g: f(X) \to X$ by $g(y) = x$ where $f(x) = y$. We see that $(f \circ g) = \mathrm{Id}_{f(X)}$. However, $(g \circ f) \neq \mathrm{Id}_X$ unless f is one-to-one. In particular, when $f: X \to Y$ is 1-1, there exists an inverse function $f^{-1}: f(X) \to X$.*

We will often be dealing with **real-valued functions**. A real-valued function is a function $f: X \to \mathbf{R}$. We define the **support** of a real-valued function $f: X \to \mathbf{R}$ to be the subset $\mathrm{supp}(f) = \{x \in X \ : \ f(x) \neq 0\}$.

Given any pair of sets X, Y, the set of functions $f: X \to Y$ is denoted by $\mathrm{Fun}(X,Y)$. When either X or Y has additional structure (e.g. a topology, a binary operation, and so forth), the set $\mathrm{Fun}(X,Y)$ can often be endowed with additional structure as well. We will see some examples of this in the next section. Note that when $X = Y$, the set $\mathrm{Fun}(X,X)$ comes with an additional structure. Specifically, we have a binary operation given by composition of functions.

Supplemental Material: Disjoint Unions and Cartesian Products.*

Given a set I and a collection of sets $\{X_i\}_{i \in I}$, we can form the **disjoint union** of the sets X_i. Formally, the disjoint union is defined to be

$$\bigsqcup_{i \in I} X_i \stackrel{\text{def}}{=} \bigcup_{i \in I} \{(x,i) \ : \ x \in X_i\}.$$

We can identify X_i with the subset $X_i^* \subseteq \bigsqcup_i X_i$ given by $\{(x,i) \,:\, x \in X_i\}$. Informally, the disjoint union of the sets X_i is a set X that contains each X_i as a subset such that the following two properties hold:

$$X_i \cap X_j = \emptyset \text{ for } i \neq j, \quad X = \bigcup_{i \in I} X_i.$$

To see that the above formal construction of the disjoint union satisfies these two condition, we first note that the second condition follows from the definition; here we are identifying the sets X_i with the subsets X_i^*. The first condition is also obvious since $(x,k) \in X_i^*$ if and only if $k = i$ and $x \in X_i$. In particular, if $(x,i) \in X_i^*$, then $(x,i) \notin X_j^*$ for every $j \neq i$.

***Example* 0.1.** *Let $I = \{1,2\}$ and let $X_1 = \{a,b\}$ and $X_2 = \{c,d\}$. Then $\bigsqcup_{i=1}^2 X_i$ is formally the set given by $\{(a,1),(b,1),(c,2),(d,2)\}$. However, we could just view this set as $\{a,b,c,d\}$.*

***Definition* 0.4** (Cartesian Product)**.** *Given a set I and a collection of sets $\{X_i\}_{i \in I}$, the **Cartesian product** of the X_i by*

$$\prod_{i \in I} X_i \overset{def}{=} \left\{ f : I \to \bigsqcup_{i \in I} X_i \;:\; f(i) \in X_i^* \text{ for each } i \in I \right\}.$$

If $I = \{1,2\}$, we can view the Cartesian product of X_1, X_2 has pairs (x_1, x_2) where $x_1 \in X_1$ and $x_2 \in X_2$. With regard to our formal definition of the Cartesian product of X_1, X_2, an element of $X_1 \times X_2$ is a function $f : \{1,2\} \to X_1 \sqcup X_2$ such that $f(1) \in X_1^*$ and $f(2) \in X_2^*$. Informally, this function f picks an element x_i out of X_i for each i. We often think of the function as providing a list of these selections. That is $\{f(1), f(2)\} = \{(x_1,1),(x_2,2)\}$. For simplicity, we often drop the "second coordinate" and can think of the list as just (x_1, x_2). In particular, we can think of elements in $\prod_{i \in I} X_i$ all the possible choices we can make for these selections. Hence, a particular element in $\prod_{i \in I} X_i$ can be viewed as a list $(x_i)_{i \in I}$ where $x_i \in X_i$ represents the choice of the element in X_i that we picked.

***Example* 0.2.** *Let $I = \{1, \ldots, n\}$ and let $X_i = X$ for $i = 1, \ldots, n$. Then $\prod_{i=1}^n X_i$ is just n–tuples of elements in the set X. We often write $X^n = X \times X \times \cdots \times X$ to denote the Cartesian product of a set X with itself n times. Thus,*

$$X^n = \{(x_1, \ldots, x_n) \;:\; x_i \in X \text{ for all } i = 1, \ldots, n\}.$$

A concrete example of Cartesian product that you have seen before is $\mathbf{R}^n$. We view elements in $\mathbf{R}^n$ as n–dimensional vectors or as points with coordinates $(x_1, \ldots, x_n)$ where $x_i \in \mathbf{R}$ for each $i = 1, \ldots, n$. When $n = 2$, we have the plane $\mathbf{R}^2$ comprised of pairs of real numbers (x,y).

Cartesian products $\prod_{i \in I} X_i$ come with some natural functions called **projection functions** or **projection maps**. These are functions $\mathrm{P}_{i_0} : \prod_{i \in I} X_i \to X_{i_0}$ defined by

$$\mathrm{P}_{i_0}((x_i)_{i \in I}) = x_{i_0} \text{ or } \mathrm{P}_{i_0}(f) = f(i_0).$$

Informally, what the projection function P_{i_0} does is send our list (x_i) to the i_0–choice in the list or the i_0–coordinate. For our example X^n, we have $\mathrm{P}_i\colon X^n \to X$ given by

$$\mathrm{P}_i(x_1,\dots,x_{i-1},x_i,x_{i+1},\dots,x_n) = x_i.$$

For the concrete example $\mathbf{R}^2$, we have two projection functions $\mathrm{P}_1,\mathrm{P}_2\colon \mathbf{R}^2 \to \mathbf{R}$ given by $\mathrm{P}_1(x,y) = x$, $\mathrm{P}_2(x,y) = y$.

Supplemental Material: Cardinality.*

The concept of the size of a set X is fundamental to many areas of mathematics. Here, we briefly introduce the concept of cardinality of a set and the concept of two sets of the same cardinality. There are some nice YouTube videos on this topic; for instance, this video.

Given a set X, we denote the **cardinality** of X by $|X|$. Informality, $|X|$ represents the number of elements in X. The empty set has cardinality 0, a singleton set has cardinality 1, and so forth. We say that $|X| \leq |Y|$ if there exists a one-to-one function $f\colon X \to Y$. We say that $|X| = |Y|$ if there exists a bijective function $f\colon X \to Y$. It is a non-trivial result that $|X| \leq |Y|$ and $|Y| \leq |X|$ implies $|X| = |Y|$. This result is called the **Cantor–Schröder–Bernstein theorem** (here is a video with a proof).

***Theorem* 0.8.** *If X, Y are sets such that $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.*

For each natural number $n \in \mathbf{N}$, we have the finite set $X_n = \{1,\dots,n\}$ and we write $|X_n| = n$. We say that a set X is **finite** if $|X| = |X_n| = n$ for some $n \in N$ or if $X = \emptyset$. If $|X| \geq |X|_n$ for every $n \in \mathbf{N}$, we say that X is **infinite**.

Infinite sets come in an unimaginable number of flavors with regard to their cardinality; see **Russell's paradox** (here is a video on Russell's Paradox). Nevertheless, one can show:

***Lemma* 0.9.** *If X is an infinite set, then there is a subset $X_0 \subseteq X$ such that $|X_0| = |\mathbf{N}|$.*

Sketch of Proof. Since X is not finite, X is clearly non-empty and so there exists $x_1 \in X$. As X is infinite, it must be that $X \neq \{x_1\}$, and so there is an $x_2 \in X$ with $x_1 \neq x_2$. As before, since X is infinite, $X \neq \{x_1,x_2\}$ and so there is an $x_3 \in X$ with $x_3 \notin \{x_1,x_2\}$. Continuing this process, we obtain a subset $X_0 = \{x_1,\dots,x_n,\dots\} \subseteq X$. By construction, we have a bijective function $X_0 \to \mathbf{N}$ given by $x_i \mapsto i$ and so $|X_0| = |\mathbf{N}|$. ♠

Note that it follows, by definition of cardinality, that $|A| \leq |X|$ for any subset $A \subseteq X$; the inclusion function $\iota_{A,X} : A \to X$ is one-to-one . In particular, it follows from Lemma 0.9 that $|\mathbf{N}| \leq |X|$ for any infinite set X. We say that a set X is **countable** if either X is finite or $|X| = |\mathbf{N}|$. In particular, an infinite, countable set has the same cardinality as $\mathbf{N}$. If X is a set and is not countable, then we say that X is **uncountable**.

Exercise 0.1. *Prove that a set X is countable if and only if there exists finite subsets $\{X_i\}_{i\in\mathbf{N}}$ of X such that $X_i \subseteq X_{i+1}$ for each $i \in \mathbf{N}$ and $X = \bigcup_i X_i$.*

Exercise 0.2. *Prove that $|\mathbf{N}| = |\mathbf{Z}|$.*

Exercise 0.3. *Prove that $|\mathbf{N}| = |\mathbf{Q}|$. [Hint: Use Exercise 0.1]*

It may seem unnatural to have a notation of "size" for sets such that a set can have the same size as a proper subset. However, if you consider an infinite set X, how much does the size of X change if you add or remove a finite set? In a real sense, sets of the same cardinality are the same sets but with different ways of labeling them. The even numbers, the odd numbers, and the natural numbers are are infinite, countable sets. In what sense are they different as abstract sets?

It should be somewhat comforting to know that this cannot happen in the case of finite set.

Exercise 0.4. *Prove that if X is a finite set and $A \subset X$ is a proper subset, then $|X| \neq |A|$. [Hint: Use the **Pigeon Hole Principle**]*

The real numbers are not countable and this is not trivial to prove (check out this video or video for a proof).

Lemma 0.10. *$\mathbf{R}$ is uncountable.*

Exercise 0.5. *(i) If X is a set and $P \subseteq \mathscr{P}(X)$ is a partition of X such that P is countable and every $A \in P$ is countable, prove that X is countable.*

(ii) Prove that $\mathbf{R} - \mathbf{Q}$ is uncountable. [Hint: Use Lemma 0.10 and Part (a)]

As a result of the above exercise, we see that there are "more" irrational numbers than rational numbers. We will see later that for any two real numbers x, y with $x < y$, there exists a rational number α such that $x < \alpha < y$. The combination of these two facts is mildly disturbing though what it says that $\mathbf{R}$ is big but not too big.

Here are a few more exercises (check out this video of sets and power sets).

Exercise 0.6. *If X is a finite set, prove that $|\mathscr{P}(X)| = 2^{|X|}$. [Hint: Use the **Binomial Theorem** or **induction**]*

Exercise 0.7. *If X is any set, prove that $|X| \leq |\mathscr{P}(X)|$ and $|X| \neq |\mathscr{P}(X)|$.*

For more on the binomial theorem and induction, see [1]. Specifically, induction is cover in §1.3 of [1] and the binomial theorem is covers in §1.4 of [1].

Supplemental Material: Partitions and Equivalence Relations.*

Definition 0.5 (Partition)**.** *A **partition** of a set X is a collection of subsets $P \subseteq \mathscr{P}(X)$ that satisfies the following two properties:*

(i) For each pair $A, B \in P$, we have $A \cap B = \emptyset$ or $A = B$.

(ii) $X = \bigcup_{A \in P} A$.

Given a partition P of X, each element $x \in X$ is contained in exactly one of the sets in the partition P. In this way, a partition "cuts" X up into pieces. One natural example of a partition is the partitioning of the natural numbers into the even and odd numbers. We can partition the real numbers into three sets: the positive real numbers, the negative real numbers, and $\{0\}$. One might feel bad for 0 and instead partition the real numbers into two sets: the negative numbers and the non-negative numbers (or the positive numbers and the non-positive numbers). We could partition the unit interval $[0,1]$ into subsets $[0,\alpha_1], (\alpha_1,\alpha_2], (\alpha_2,\alpha_3], \ldots, (\alpha_n, 1]$ where

$$0 < \alpha_1 < \alpha_2 < \alpha_3 < \cdots < \alpha_n < 1.$$

There are lots of partitions, some of which are quite natural, some of which are rather unnatural. Typically one uses partitions in "divide-and-conquer" strategies. We will make extensive use of partitions in this class.

Partitions and equivalence relations on a set are related concepts.

Definition 0.6 (Equivalence Relation)**.** *An **equivalence relation** on a set X is a relation $\sim$ between elements in X that satisfies three properties:*

(i) $x \sim x$ for all $x \in X$.

(ii) If $x \sim y$, then $y \sim x$.

(iii) If $x \sim y$ and $y \sim z$, then $x \sim z$.

For an equivalence relation $\sim$ on X, for each $x \in X$, we define the **equivalence class of x** by

$$[x] \stackrel{\text{def}}{=} \{y \in X \ : \ x \sim y\}.$$

The reader can verify the set of equivalence class $\{[x]\} \subset \mathscr{P}(X)$ is a partition of X. Conversely, given a partition P of X, we can define the equivalence relation $x \sim y$ if and only if there exists $A \in P$ such that $x, y \in A$. Since P is a partition, each $x \in X$ is contained in exactly one set $A_x \in P$. The set A_x is the equivalence class of x relative to this equivalence relation.

Given two partitions $P_1, P_2 \subseteq \mathscr{P}(X)$, we say that P_1 is a **refinement** of P_2, if for each $A_1 \in P_1$, there exists a subset $A_2 \in P_2$ such that $A_1 \subseteq A_2$.

***Lemma* 0.11.** *If P_1 is a refinement of P_2, then for each $A_2 \in P_2$, there exists a subset $P_1(A_2) \subset P_1$ such that $P_1(A_2)$ is a partition of A_2.*

Specifically, if P_1 is a partition of P_2, then P_1 is derived from P_2 by selecting for each $A_2 \in P_2$, a partition I_{1,A_2} of A_2. Informally, refinements of partitions are obtained by taking partitions of the partitioning set in P_2.

Supplemental Material: The Pigeon Hole Principle.

The **Pigeon Hole Principle**, and some variants of it, is a basic tool in mathematics. See Theorem 1.6.1 in my class lecture notes for discrete math [1].

***Theorem* 0.12** (Pigeon Hole Principle)**.** *If $f\colon X \to Y$ is a function with X, Y finite and $|X| > |Y|$, then there exists $y \in Y$ such that $\left|f^{-1}(y)\right| > 1$.*

A useful variant of the Pigeon Hole Principle that involves infinite sets is the following.

***Theorem* 0.13** (Pigeon Hole Principle: Infinite Version)**.** *If $f\colon X \to Y$ is a function, X is an infinite set, and Y is a finite set, then there exists $y \in Y$ such that $f^{-1}(y)$ is an infinite set.*

To prove this, notice that a function $f\colon X \to Y$ gives us a partition on X. Specifically, we have $X = \bigcup_{y \in Y} f^{-1}(y)$.

Lemma 0.14. *If X is a set with a partition $P \subseteq \mathscr{P}$ such that P is finite and every $A \in P$ is finite, then X is finite. Moreover, $|X| = \sum_{A \in P} |A|$.*

For a proof of this fact, see [1, Lemma 1.5.4]. Returning to the proof of Theorem 0.13, we see that if for every $y \in Y$, the subset $f^{-1}(y) \subseteq X$ is finite, then X is finite. Hence, since X is infinite, we must have that $f^{-1}(y)$ is infinite for some $y \in Y$.

Exercise 0.8. *Prove that if X is an infinite set and P is a partition of X such that P is finite, then there exists $A_0 \in P$ such that $|A_0| = |X|$.*

Assuming this exercise, we obtain:

Theorem 0.15. *If $f : X \to Y$ is a function with X infinite, Y finite, then there exists $y \in Y$ such that $\left|f^{-1}(y)\right| = |X|$.*

Another refinement of the Pigeon Hole Principle is the following (see [1, Thm 1.6.2]).

Theorem 0.16 (Pigeon Hole Principle: Refined Version)**.** *If $f : X \to Y$ is a function, X, Y are finite sets, and $m < |X| / |Y|$, then there exists $y \in Y$ such that $\left|f^{-1}(y)\right| > m$.*

Supplemental Material: Partially Ordered and Directed Sets.

Definition 0.7 (Partial Ordering)**.** *A **partial ordering** on a set X is a binary relation $\leq$ that satisfies the following three conditions:*

(i) $x \leq x$.

(ii) *If* $x \leq y$, *then* $y \geq x$.

(iii) *If* $x \leq y$ *and* $y \leq z$, *then* $x \leq z$.

A set X with a fixed partial ordering $\leq$ is called a **partially ordered set** or poset for short. The most basic examples are $(\mathbf{N}, \leq)$, $(\mathbf{Q}, \leq)$, and $(\mathbf{R}, \leq)$. However, these examples are misleading as these are examples of **total orders**; you can read also about **well ordered sets**. Specifically, every pair of elements in a total order have relation. In a partially ordered set, there can exists $x, y \in X$ such that neither $x \leq y$ or $y \leq x$.

An example of a partially ordered set is $\mathscr{P}(X)$, the power set of a set X. The partial ordering on $\mathscr{P}(X)$ is given by subset containment. It is common to say that $\mathscr{P}(X)$ is partially ordered via containment in this case. For $A, B \in \mathscr{P}(X)$, we define the partial order by $A \leq B$ if and only if $A \subseteq B$. Note that in general, two subsets A, B of a set X are not related by the partial ordering as a typical pair of sets will not satisfy either $A \subseteq B$ or $B \subseteq A$. One can also partially order $\mathscr{P}(X)$ via reversion inclusion. This partial ordering is defined by $A \leq B$ if and only if $B \subseteq A$.

A **directed set** is a partially ordered set $(X, \leq)$ that satisfies the additional condition that given any $x, y \in X$, there exists $z \in X$ such that $x \leq z$ and $y \leq z$. Our example of $\mathscr{P}(X)$ partially ordered with respect to inclusion or reverse inclusion are both examples of directed sets. In the case of inclusion, we see that $A \leq A \cup B$ and $B \leq A \cup B$. In the case of reversion inclusion, we see that $A \leq A \cap B$ and $B \leq A \cap B$. (This video discusses directed sets).

Chapter 1

Algebraic Structures

Contents

In this first chapter, we will introduce different types of algebraic structures on sets. One can think of sets as something like unused memory. By themselves, sets do not provide enough structure to describe all of the different concepts of mathematics. Moreover, one essentially never uses an abstract set in either theoretical or applied matters. The point is that sets almost always come with some additional structure. The set could be labeled or ordered or partially ordered. There could be various binary operations on the set. Indeed, one of the main aims of mathematics broadly is the study of various types of structures on sets. The structures can be topological/geometric, analytic, or algebraic in practice. The real numbers $\mathbf{R}$ provide an example of a "concrete" set with a considerable amount of structure. Before starting off the chapter formally, we will discuss algebraic structures on $\mathbf{R}$ and some sets of functions associated to $\mathbf{R}$. In this discussion, we will see examples of commutative and non-commutative groups, rings with identity, commutative rings with identity, real vector spaces, real associative, commutative algebras, and real associative algebras. These structures play an essential role in all of mathematics including analysis, applied mathematics, and probability theory. One must accept that algebraic language is part of mathematics and welcome the wide array of concepts and tools that it can provide for present and future problem solving.

First, we have an addition operation $+$ that given any two real numbers $x, y \in \mathbf{R}$, outputs a real number $x+y$. We also have a multiplication operation $*$ that given any two real numbers $x, y \in \mathbf{R}$, outputs a real number $x*y$. Of course, we usually write xy instead of $x*y$. However, for future purposes, we will continue to use the bloated notation $x*y$ for multiplication. These two operations are examples of a more general type of operation called a binary operation. Specifically, any function $f\colon \mathbf{R}\times\mathbf{R}\to\mathbf{R}$ is called a **binary operation**. Addition and multiplication are two specific examples of binary operations on the real numbers. The two operations are nice and are also compatible. Recall, the following well known rules of arithmetic:

- **Existence of Additive Identity.** There exists $e_+ \in \mathbf{R}$ such that for any $x \in \mathbf{R}$, we have
$$x + e_+ = e_+ + x = x. \tag{1.1}$$
The number e_+ is typically denoted by 0 and is the unique number satisfying (1.1) for all $x \in \mathbf{R}$.
- **Existence of Additive Inverses.** For each $x \in \mathbf{R}$, there exists $y_x \in \mathbf{R}$ such that
$$x + y_x = y_x + x = 0. \tag{1.2}$$
The number y_x is typically denoted by $-x$ and is the unique number satisfying (1.2).
- **Associativity of Addition.** For every $x, y, z \in \mathbf{R}$, we have
$$x + (y + z) = (x + y) + z.$$

- **Commutativity of Addition.** For every $x, y \in \mathbf{R}$, we have

$$x + y = y + x.$$

- **Existence of Multiplicative Identity.** There exists $e_* \in \mathbf{R}$ such that for every $x \in \mathbf{R}$, we have

$$x * e_* = e_* * x = x. \tag{1.3}$$

  The number e_* is typically denoted by 1 and is the unique real number satisfying (1.3) for all $x \in \mathbf{R}$.

- **Existence of Multiplicative Inverses.** For each $x \in \mathbf{R}$ with $x \neq 0$, there exists $z_x \in \mathbf{R}$ such that

$$x * z_x = z_x * x = 1. \tag{1.4}$$

  The number z_x is typically denoted x^{-1} and is the unique real number satisfying (1.4).

- **Associativity of Multiplication.** For every $x, y, z \in \mathbf{R}$, we have

$$x * (y * z) = (x * y) * z.$$

- **Commutativity of Multiplication.** For every $x, y \in \mathbf{R}$, we have

$$x * y = y * x.$$

- **Distributive Law.** For every $x, y, z \in \mathbf{R}$, we have

$$x * (y + z) = (x * y) + (x * z).$$

The real numbers $\mathbf{R}$ together with these two operations $+, *$ give $\mathbf{R}$ an algebraic structure called a **field** structure. The addition operation gives $\mathbf{R}$ an algebraic structure called a **group** structure or more specifically a **commutative group** structure (also called an abelian group structure). If $\mathbf{R}^\times = \mathbf{R} - \{0\}$, then $\mathbf{R}^\times$ together with the $*$ operation gives $\mathbf{R}^\times$ a commutative group structure. A field structure is an extremely refined algebraic structure compared to only the commutative group structure coming from addition. Moreover, group structures will not necessarily be commutative (i.e. the commutative property might not hold for the binary operation).

This field structure on $\mathbf{R}$ is not the only structure we have. We have a notation of distance given by $|x - y|$ and this **distance function** gives $\mathbf{R}$ a **metric space** structure which in turn gives $\mathbf{R}$ a **topological structure**. With a topology, we can talk about concepts like **continuity of functions**, **limits of sequences**, .etc, and we can see that both the addition and multiplication operations are continuous. In particular, $\mathbf{R}$ with both the field structure and topological structure is an example of a **topological field**.

We also notice that these structures on $\mathbf{R}$ also give us algebraic and topological structures on sets of functions. For example, the set $\mathrm{Fun}(\mathbf{R},\mathbf{R})$ can be endowed with a real vector space structure. We have a pair of operations. First, we have a binary operation $+_{\mathrm{Fun}}$ on $\mathrm{Fun}(\mathbf{R},\mathbf{R})$ given by

$$(f \ +_{\mathrm{Fun}} \ g)(x) \stackrel{\mathrm{def}}{=} f(x)+g(x).$$

This binary operation is sometimes referred to as **point-wise addition**. We also have a scalar multiplication operation which formally is a function

$$\cdot_{\mathrm{Fun}} \colon \mathbf{R} \times \mathrm{Fun}(\mathbf{R},\mathbf{R}) \longrightarrow \mathrm{Fun}(\mathbf{R},\mathbf{R}).$$

The scalar multiplication operation $\cdot_{\mathrm{Fun}}$ is defined by

$$(\alpha \cdot_{\mathrm{Fun}} f)(x) \stackrel{\mathrm{def}}{=} \alpha * f(x).$$

We have the following properties for these two operations:

- **Existence of Additive Identity.** There exists a function $0_{\mathrm{Fun}} \in \mathrm{Fun}(\mathbf{R},\mathbf{R})$ such that for any function $f \in \mathrm{Fun}(\mathbf{R},\mathbf{R})$, we have

  $$f \ +_{\mathrm{Fun}} \ 0_{\mathrm{Fun}} = 0_{\mathrm{Fun}} \ +_{\mathrm{Fun}} \ f = f. \tag{1.5}$$

  The function 0_{Fun} is the unique function satisfying (1.5). Note that (1.5) is a family of numerical equalities $f(x)+0_{\mathrm{Fun}}(x) = f(x)$ and so $0_{\mathrm{Fun}}(x) = 0$ for all $x \in \mathbf{R}$. Alternatively, one can view 0_{Fun} as $\chi_{\emptyset}$ where given $S \subseteq \mathbf{R}$, we define

  $$\chi_S(x) \stackrel{\mathrm{def}}{=} \begin{cases} 1, & x \in S, \\ 0, & x \notin S. \end{cases}$$

- **Existence of Additive Inverses.** For each $f \in \mathrm{Fun}(\mathbf{R},\mathbf{R})$, there exists $g_f \in \mathrm{Fun}(\mathbf{R},\mathbf{R})$ such that

  $$f \ +_{\mathrm{Fun}} \ g_f = g_f \ +_{\mathrm{Fun}} \ f = 0_{\mathrm{Fun}}. \tag{1.6}$$

  The function g_f is denoted by $-f$ and is the unique function satisfying (1.6). Note that (1.6) is a family of numerical equalities given by $f(x)+g_f(x) = 0$ and so $g_f(x) = -f(x)$ for all $x \in \mathbf{R}$.

- **Associativity of Addition.** For every $f,g,h \in \mathrm{Fun}(\mathbf{R},\mathbf{R})$, we have

  $$f \ +_{\mathrm{Fun}} \ (g \ +_{\mathrm{Fun}} \ h) = (f \ +_{\mathrm{Fun}} \ g) \ +_{\mathrm{Fun}} \ h.$$

- **Commutativity of Addition.** For every $f,g \in \mathrm{Fun}(\mathbf{R},\mathbf{R})$, we have

  $$f \ +_{\mathrm{Fun}} \ g = g \ +_{\mathrm{Fun}} \ f.$$

- **Scalar Identity.** For every $f \in \text{Fun}(\mathbf{R},\mathbf{R})$, we have

$$1 \cdot_{\text{Fun}} f = f.$$

- **Scalar Compatibility.** For every $\alpha,\beta \in \mathbf{R}$ and every $f \in \text{Fun}(\mathbf{R},\mathbf{R})$, we have

$$\alpha \cdot_{\text{Fun}} (\beta \cdot_{\text{Fun}} f) = (\alpha * \beta) \cdot_{\text{Fun}} f.$$

- **Distributive Law, I.** For every $\alpha \in \mathbf{R}$ and every $f,g \in \text{Fun}(\mathbf{R},\mathbf{R})$, we have

$$\alpha \cdot_{\text{Fun}} (f \ +_{\text{Fun}} \ g) = (\alpha \cdot_{\text{Fun}} f) \ +_{\text{Fun}} \ (\alpha \cdot_{\text{Fun}} g).$$

- **Distributive Law, II.** For every $\alpha,\beta \in \mathbf{R}$ and every $f \in \text{Fun}(\mathbf{R},\mathbf{R})$, we have

$$(\alpha+\beta) \cdot_{\text{Fun}} f = (\alpha \cdot_{\text{Fun}} f) \ +_{\text{Fun}} \ (\beta \cdot_{\text{Fun}} f).$$

The set $\text{Fun}(\mathbf{R},\mathbf{R})$ with these two operations is a **real vector space** structure on the set $\text{Fun}(\mathbf{R},\mathbf{R})$. In fact, if X is *any* set, the set $\text{Fun}(X,\mathbf{R})$ can be given a real vector space structure as in our example $\text{Fun}(\mathbf{R},\mathbf{R})$, we only used the algebraic operations on the codomain. We will see shortly that one can define vector spaces over any field.

The multiplication operation on $\mathbf{R}$ also endows $\text{Fun}(\mathbf{R},\mathbf{R})$ (also $\text{Fun}(X,\mathbf{R})$) with another binary operation

$$(f \ *_{\text{Fun}} \ g)(x) \stackrel{\text{def}}{=} f(x) * g(x).$$

The two binary operations $+_{\text{Fun}}$ and $*_{\text{Fun}}$ satisfy the following properties:

- $\text{Fun}(\mathbf{R},\mathbf{R})$ is an commutative group with the operation $+_{\text{Fun}}$. Specifically, there exists an additive identity, there exist additive inverses, and the operation is both associative and commutative.
- **Existence of Multiplicative Identity.** There exists $1_{\text{Fun}} \in \text{Fun}(\mathbf{R},\mathbf{R})$ such that for every $f \in \text{Fun}(\mathbf{R},\mathbf{R})$, we have

$$f \ *_{\text{Fun}} \ 1_{\text{Fun}} = 1_{\text{Fun}} \ *_{\text{Fun}} \ f = f. \tag{1.7}$$

  The function 1_{Fun} is the unique function satisfying (1.7) for all $f \in \text{Fun}(\mathbf{R},\mathbf{R})$. As before, from (1.7), we obtain a family of numerical equalities $1_{\text{Fun}}(x) * f(x) = f(x)$. Note that since we can vary both x and f, we must have $1_{\text{Fun}}(x) = 1$ for all $x \in \mathbf{R}$.
- **Associativity of Multiplication.** For every $f,g,h \in \text{Fun}(\mathbf{R},\mathbf{R})$, we have

$$f \ *_{\text{Fun}} \ (g \ *_{\text{Fun}} \ h) = (f \ *_{\text{Fun}} \ g) \ *_{\text{Fun}} \ h.$$

- **Commutativity of Multiplication.** For every $f, g \in \mathrm{Fun}(\mathbf{R}, \mathbf{R})$, we have

$$f \ *_{\mathrm{Fun}} \ g = g \ *_{\mathrm{Fun}} \ f.$$

- **Distributive Law.** For every $f, g, h \in \mathrm{Fun}(\mathbf{R}, \mathbf{R})$, we have

$$f \ *_{\mathrm{Fun}} \ (g \ +_{\mathrm{Fun}} \ h) = f \ *_{\mathrm{Fun}} \ g \ +_{\mathrm{Fun}} \ f \ *_{\mathrm{Fun}} \ h.$$

The set $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ with these binary operations is a **commutative ring with identity** structure on $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$. In particular, for general rings, one does not always assume that a multiplicative identity exists.

If we combine the real vector space structure on $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ with operations $+_{\mathrm{Fun}}$ and $\cdot_{\mathrm{Fun}}$ with the **commutative ring with identity** structure on $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ with operations $+_{\mathrm{Fun}}$ and $*_{\mathrm{Fun}}$, we obtain a **commutative real algebra with identity** structure on $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ with operations $+_{\mathrm{Fun}}, *_{\mathrm{Fun}}$, and $\cdot_{\mathrm{Fun}}$.

There is another binary operation on $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ given by composition of functions. Specifically, we define

$$*_{\mathrm{comp}} \colon \mathrm{Fun}(\mathbf{R}, \mathbf{R}) \times \mathrm{Fun}(\mathbf{R}, \mathbf{R}) \to \mathrm{Fun}(\mathbf{R}, \mathbf{R})$$

given by

$$(f \ *_{\mathrm{comp}} \ g)(x) = f(g(x)).$$

The set $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ with the operations $+_{\mathrm{Fun}}$ and $*_{\mathrm{comp}}$ gives $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ a monoid structure. Specifically, we have the following properties:

- $\mathrm{Fun}(\mathbf{R}, \mathbf{R})$ with $+_{\mathrm{Fun}}$ is an commutative group.
- **Existence of Multiplicative Identity.** There exists $1_{\mathrm{comp}} \in \mathrm{Fun}(\mathbf{R}, \mathbf{R})$ such that for every $f \in \mathrm{Fun}(\mathbf{R}, \mathbf{R})$, we have

$$f \ *_{\mathrm{comp}} \ 1_{\mathrm{comp}} = 1_{\mathrm{comp}} \ *_{\mathrm{comp}} \ f = f. \tag{1.8}$$

  The function 1_{comp} is the unique function satisfying (1.8). Via (1.8), we obtain a family of numerical equalities $1_{\mathrm{comp}}(f(x)) = f(x)$ and $f(1_{\mathrm{comp}}(x)) = f(x)$ for all $x \in \mathbf{R}$ and $f \in \mathrm{Fun}(\mathbf{R}, \mathbf{R})$. From these equations, we deduce that $1_{\mathrm{comp}}(x) = x$ for all $x \in \mathbf{R}$. In particular, $1_{\mathrm{comp}} = \mathrm{Id}_{\mathbf{R}}$.

- **Associativity of Multiplication.** For every $f, g, h \in \mathrm{Fun}(\mathbf{R}, \mathbf{R})$, we have

$$f \ *_{\mathrm{comp}} \ (g \ *_{\mathrm{comp}} \ h) = (f \ *_{\mathrm{comp}} \ g) \ *_{\mathrm{comp}} \ h.$$

Note that unlike $*_{\text{Fun}}$, the operation $*_{\text{comp}}$ is not commutative. For a general $f \in \text{Fun}(\mathbf{R},\mathbf{R})$, there is no multiplicative inverse for either $*_{\text{Fun}}$ or $*_{\text{comp}}$. For $*_{\text{Fun}}$, we see that if there exists $g \in \text{Fun}(\mathbf{R},\mathbf{R})$ such that $f \ *_{\text{Fun}} \ g = 1_{\text{Fun}}$, then

$$f(x)g(x) = 1$$

for all $x \in \mathbf{R}$. In particular, $f(x) \neq 0$ for all $x \in \mathbf{R}$. Moreover, we see that if $f(x) \neq 0$ for all $x \in \mathbf{R}$, then $g(x) \stackrel{\text{def}}{=} (f(x))^{-1}$ is a multiplicative inverse for f with respect to $*_{\text{Fun}}$. The subset of $\text{Fun}(\mathbf{R},\mathbf{R})$ of those functions f which satisfy $f(x) \neq 0$ for all $x \in \mathbf{R}$ with the operation $*_{\text{Fun}}$ has the structure of a commutative group. This subset of $\text{Fun}(\mathbf{R},\mathbf{R})$ with this commutative ring with identity structure is called the **group of units** or group of invertible elements of the ring with identity.

The invertible elements $\text{Fun}(\mathbf{R},\mathbf{R})$ with the operation $*_{\text{comp}}$ are more complicated. For one, since $*_{\text{comp}}$ is not a commutative operation, we could have $f \ *_{\text{comp}} \ g = 1_{\text{comp}}$ but $g \ *_{\text{comp}} \ f \neq 1_{\text{comp}}$. In the case $f \ *_{\text{comp}} \ g = 1_{\text{comp}}$, we say that g is a **right inverse** of f or f is a **left inverse** of g. Given any injective function f, we can also find a left inverse g though g need not be defined on all of $\mathbf{R}$. In order to ensure that g is defined on all of $\mathbf{R}$, we also require that f be surjective. In particular, these invertible elements of $\text{Fun}(\mathbf{R},\mathbf{R})$ are the subset of bijective functions under the operation $*_{\text{comp}}$. Moreover, given any set X, the subset of bijective functions $\text{Sym}(X)$ of $\text{Fun}(X,X)$ is a group under composition. Specifically, we have the following properties:

- **Existence of Identity.** There exists $\text{Id}_X \in \text{Sym}(X)$ such that for every $f \in \text{Sym}(X)$, we have

  $$f \circ \text{Id}_X = \text{Id}_X \circ f = f. \tag{1.9}$$

  The identity function Id_X is the unique function satisfying (1.9) for all $f \in \text{Sym}(X)$.

- **Existence of Multiplicative Inverses.** For every $f \in \text{Sym}(X)$, there exists $g_f \in \text{Sym}(X)$ such that

  $$f \circ g_f = g_f \circ f = \text{Id}_X. \tag{1.10}$$

  The function g_f is typically denoted by f^{-1} and is the unique function satisfying (1.10).

- **Associativity of Multiplication.** For every $f,g,h \in \text{Sym}(X)$, we have

  $$f \circ (g \circ h) = (f \circ g) \circ h.$$

It turns out that the groups $\text{Sym}(X)$ are universal in the sense that every group can be realized as a subgroup of $\text{Sym}(X)$ for some X. When X is a finite set of size n, the group $\text{Sym}(X)$ is called the **symmetric group** on n objects or **permutation group** on n letters.

1.1 *Algebraic Structures*

In this section, we will introduce several different types of algebraic structures on sets. We will start with the least structured of these.

1.1.1 Magmas, Semigroups, Monoids, and Groups

We start our discussion of algebraic structures with the concept of a magma.

***Definition* 1.1** (Magma)**.** *A **magma** structure on a set M is a binary operation $\cdot\colon M \times M \to M$. Any set M equipped with a magma structure will be referred to as a magma.*

The concept of a magma is an odd one. On one hand, it is a certainty that every mathematician uses in some way the concept of a magma. On the other hand, these algebraic structures are so general that few things hold for all magmas. Before moving to a richer algebraic structure, we given an example of a magma.

***Example* 1.1** (Function Spaces)**.** *Given a set X, the set $\mathrm{Fun}(X,X)$ can be equipped with a magma structure via composition of functions. Specifically, we have the binary operation*

$$\circ\colon \mathrm{Fun}(X,X) \times \mathrm{Fun}(X,X) \to \mathrm{Fun}(X,X)$$

defined by

$$(f \circ g)(x) = f(g(x))$$

for all $x \in X$.

Just for contrast, we will give another magma structure on $\mathrm{Fun}(X,X)$. For example, we can define a binary operation of $\mathrm{Fun}(X,X)$ as follows. First, we fix $x_0 \in X$ and then define $(f \cdot g)(x) = f(g(x_0))$ for all $x \in X$. As far as I know, this magma structure on $\mathrm{Fun}(X,X)$ has never been mentioned before.

Returning to our introduction to algebraic structures, we next define a semigroup structure.

***Definition* 1.2** (Semigroup)**.** *A **semigroup** structure on a set S is a binary operation $\cdot\colon S \times S \to S$ satisfying the following property:*

- ***Associativity.*** *For all $s_1, s_2, s_3 \in S$, we have*

$$s_1 \cdot (s_2 \cdot s_3) = (s_1 \cdot s_2) \cdot s_3.$$

Any set S equipped with a semigroup structure will be called a semigroup.

One might rightfully call these structures **associative magmas** instead of semigroups. However, the (formal) concept of a semigroup predates magmas and so for historical reasons, we will call these semigroup structures.

The following exercise extends the associativity property, which is a relationship on triples, to a relationship on n–tuples.

***Exercise* 1.1.** *Let $(S,\cdot)$ be a semigroup and $s_1,\dots,s_n \in S$. Prove that*

$$s_1\cdot(s_2\cdot(\dots s_{n-2}\cdot(s_{n-1}\cdot s_n))) = ((\dots(s_1\cdot s_2)\cdot s_3)\dots)\cdot s_{n-1})\cdot s_n.$$

As a result of Exercise 1.1, the notation $s_1\cdot s_2\cdot\dots\cdot s_n$ is independent of how the terms are combined. Note that that does not mean that you can switch the order of the elements but only that you can combine any pair of them in any order you want. For instance,

$$s_1\cdot s_2\cdot s_3\cdot s_4 = (s_1\cdot s_2)\cdot(s_3\cdot s_4) = s_1\cdot(s_2\cdot s_3)\cdot s_4.$$

However, $s_1\cdot s_2 \neq s_2\cdot s_1$ in a general semigroup.

***Example* 1.2.** *The magma structure on* $\mathrm{Fun}(X,X)$ *given by composition of functions (see Example 1.1) is a semigroup as composition of functions is associative.*

Our next algebraic structure is a further refinement of magmas called monoids.

***Definition* 1.3** (Monoid)**.** *A **monoid** structure on a set M is a binary operation $\cdot$ and an element $e \in M$ such that the following properties hold:*

- ***Associativity.*** *For all $m_1,m_2,m_3 \in M$, we have*

$$m_1\cdot(m_2\cdot m_3) = (m_1\cdot m_2)\cdot m_3.$$

- ***Existence of an Identity.*** *For all $m \in M$, we have*

$$m\cdot e = e\cdot m = m.$$

Any set M equipped with a monoid structure will be referred to as a monoid.

***Example* 1.3.** *The semigroup structure on* $\mathrm{Fun}(X,X)$ *is also a monoid structure. The role of the identity element is played by the identity function.*

Example 1.4 (Natural Numbers)**.** *The set of natural numbers with zero (i.e.* $\mathbf{N} \cup \{0\}$*) with the binary operation given by addition is monoid. The identity element is given by* 0*.*

Example 1.5 (Natural Numbers)**.** *The set of natural numbers with the binary operation given by multiplication is a monoid. The identity element is given by* 1*.*

We now introduce the concept of a group which is a further refinement of a monoid structure.

Definition 1.4 (Group)**.** *A* ***group*** *structure on a set G is a binary operation $\cdot$ and an element $e \in G$ such that the following properties hold:*

- ***Associativity.*** *For all $g_1, g_2, g_3 \in G$, we have*
$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3.$$
- ***Existence of an Identity.*** *For all $g \in G$, we have $g \cdot e = e \cdot g = g$.*
- ***Existence of Inverses.*** *For each $g \in G$, there exist $g' \in G$ such that*
$$g \cdot g' = g' \cdot g = e.$$

Any set G equipped with a group structure will be called a group.

We will spend a considerable amount of time in these notes discuss groups further. For now, we give a few of exercises to help with the reader's understanding.

Exercise 1.2. *Let G be a group and let $g \in G$. Define the function $L_g \colon G \to G$ by $L_g(h) = g \cdot h$. Prove that L_g is 1-1 and onto.*

Exercise 1.3. *Find an example of a monoid M and an element $m \in M$ such that the function $L_m \colon M \to M$ given by $L_m(n) = mn$ is not 1-1. Find an example where L_m is not onto.*

Exercise 1.4. *Let G be a group and $g \in G$. Prove that if $h_1, h_2 \in G$ and*
$$g \cdot h_1 = h_1 \cdot g = h_2 \cdot g = g \cdot h_2 = e,$$
then $h_1 = h_2$.

As a result of Exercise 1.39, inverses are unique. We will typically denote inverses by g^{-1} or $-g$ depending on whether we use multiplicative or additive notation for our group binary operation.

Before giving some examples of groups, which will be a topic that we will study more extensively in the next few chapters, we introduce the concept of a commutative binary operation.

Definition* 1.5** (Commutative Binary Operation)**.** *We say that a binary operation $\cdot$ on a set X is* ***commutative *if the following holds:*

- ***Commutativity.*** *For each $x_1, x_2 \in X$, we have*

$$x_1 \cdot x_2 = x_2 \cdot x_1.$$

By a commutative magma, commutative semigroup, commutative monoid, or commutative group, we simply mean a set with a magma, semigroup, monoid, or group structure where the binary operation giving rise to the structure is commutative. In the case of groups, commutative groups are often referred to as **abelian groups** after the mathematician Abel.

For sets equipped with a single binary operation, there are many other types of structures. For completeness, we mention two of the more important ones:

- A **quasi-group** structure on a set Q is a binary operation such that the following property holds:
  - **Divisibility.** For each $q, q' \in Q$, there exist unique elements $\alpha, \beta \in Q$ such that

$$\alpha \cdot q = q', \quad q \cdot \beta = q'.$$

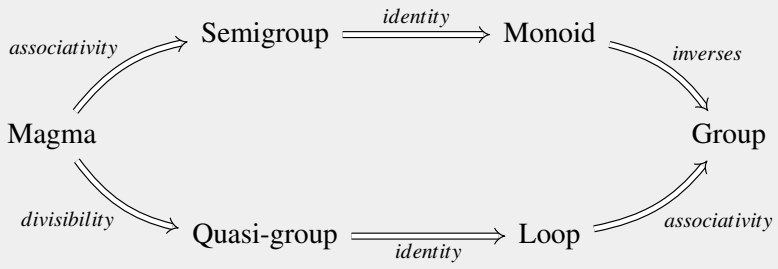
- A **loop** structure on a set L is a binary operation and an element $e \in L$ such that the following properties hold:
  - **Divisibility.** For each $\ell, \ell' \in L$, there exist unique elements $\alpha, \beta \in L$ such that

$$\alpha \cdot \ell = \ell', \quad \ell \cdot \beta = \ell'.$$

  - **Existence of an Identity.** For all $\ell \in L$, we have

$$\ell \cdot e = e \cdot \ell = \ell.$$

We have the following diagram indicating the various relationships between these algebraic structures (e.g. every magma is a quasi-group):



We end this subsection with a comment about notation.

1.1.2 Hemirings, Semirings, Rngs, Rings and Fields

In this subsection, we will introduce algebraic structures that use a pair of binary operations. We will utilize the language from the previous subsection in our definitions below; the previous subsection was deliberately repetitive.

***Definition* 1.6** (Semiring)**.** *Given a set S, a **semiring** structure on S is given by two binary operations $+,\cdot\colon S\times S\to S$ and a pair of elements $e_+, e.$ that satisfy the following properties:*

- *$(S,+,e_+)$ is a commutative monoid.*
- *$(S,\cdot,e.)$ is a monoid.*
- ***Left Distribution.*** *For all $s_1,s_2,s_3\in S$, we have*
$$s_1\cdot(s_2+s_3)=(s_1\cdot s_2)+(s_1\cdot s_3).$$
- ***Right Distribution.*** *For all $s_1,s_2,s_3\in S$, we have*
$$(s_2+s_3)\cdot s_1=(s_2\cdot s_1)+(s_3\cdot s_1).$$
- ***Multiplicative Annihilation By Zero.*** *For all $s\in S$, we have*
$$s\cdot e_+=e_+\cdot s=e_+.$$

We will denote the semiring structure by $(S,+,\cdot,e_+,e.)$. Semiring structures arise in several different areas of mathematics. The natural numbers with 0 (i.e. $\mathbf{N}\cup\{0\}$) and ordinary addition/multiplication form a semiring.

***Example* 1.6.** *The set of n by n real matrices with non-negative coefficients $\mathrm{Mat}_{\geq 0}(n,\mathbf{R})$ with ordinary matrix addition is a semiring with e_+ given by the zero matrix 0_n and $e.$ given by the identity matrix I_n.*

***Exercise* 1.5.** *Prove that $(\mathrm{Mat}_{\geq 0}(n,\mathbf{R}),+,\cdot,0_n,I_n)$ is a semiring.*

***Definition* 1.7** (Ring)**.** *Given a set R, a **ring** structure on R is given by two binary operations $+,\cdot\colon R\times R\to R$ and a pair of elements $e_+, e.$ that satisfy the following properties:*

- *$(R,+,e_+)$ is a commutative group.*

- $(R, \cdot, e.)$ *is a monoid.*
- ***Left Distribution.*** *For all* $r_1, r_2, r_3 \in R$*, we have*

$$r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3).$$

- ***Right Distribution.*** *For all* $r_1, r_2, r_3 \in R$*, we have*

$$(r_2 + r_3) \cdot r_1 = (r_2 \cdot r_1) + (r_3 \cdot r_1).$$

The reader should note that in the definition of a ring, we did not give the annihilation property that was given in the definition of a semiring. The following exercise shows that one can derive this property from the properties given in the definition of a ring.

Exercise 1.6. *Let* $(R, +, \cdot, e_+, e.)$ *be a ring. Prove that for all* $r \in R$*, we have*

$$r \cdot e_+ = e_+ \cdot r = e_+.$$

Deduce that every ring structure on a set also provides a semiring structure.

Exercise 1.7. *Let R be a ring. Prove that* $0_R r = 0_R$*. [Hint: consider* $r(0_R + 0_R)$*.]*

Definition 1.8 (Commutative Ring)**.** *Given a set R, a* ***commutative ring*** *structure on R is given by two binary operations* $+, \cdot : R \times R \to R$ *and a pair of elements* $e_+, e.$ *that satisfy the following properties:*

- $(R, +, e_+)$ *is a commutative group.*
- $(R, \cdot, e.)$ *is a commutative monoid.*
- ***Distribution.*** *For all* $r_1, r_2, r_3 \in R$*, we have*

$$r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3).$$

Our first example of a commutative ring is surely the most important example.

Example 1.7 (The Integers)**.** *The integers* $\mathbf{Z}$ *with ordinary addition/multiplication and with* $e_+ = 0$*,* $e. = 1$ *is a commutative ring. We will see a bit later that every commutative ring has a "piece" of* $\mathbf{Z}$ *inside of it.*

Our next example of a commutative ring is somewhat pathological.

Example 1.8 (Trivial Ring). *Let $R = \{r_0\}$ be a singleton set. We can define a commutative ring structure on S via*

$$r_0 + r_0 = r_0, \quad r_0 \cdot r_0 = r_0.$$

*We leave it for the reader to verify that $(\{r_0\}, +, \cdot, r_0, r_0)$ is a commutative ring. We call this ring the **trivial ring** or zero ring.*

Exercise 1.8. *Prove that $(\{r_0\}, +, \cdot, r_0, r_0)$ is a commutative ring where $r_0 + r_0 = r_0$ and $r_0 \cdot r_0 = r_0$.*

One reason the trivial ring is pathological is that $e_+ = e_\cdot$ in such a ring. This property is highly uncommon as seen via the following exercise.

Exercise 1.9. *Prove that if $(R, +, \cdot, e_+, e_\cdot)$ is a commutative ring and $|R| > 1$, then $e_+ \neq e_\cdot$.*

Definition 1.9 (Rng). *Given a set R, a **rng** structure on R is given by two binary operations $+, \cdot : R \times R \to R$ and a pair of elements $e_+, e_\cdot$ that satisfy the following properties:*

- *$(R, +, e_+)$ is a commutative group.*
- *$(R, \cdot, e_\cdot)$ is a semigroup.*
- ***Distribution.** For all $r_1, r_2, r_3 \in R$, we have*

$$r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3).$$

- ***Right Distribution.** For all $r_1, r_2, r_3 \in R$, we have*

$$(r_2 + r_3) \cdot r_1 = (r_2 \cdot r_1) + (r_3 \cdot r_1).$$

Rng structures are also called **pseudo-ring** structures or **non-unital ring** structures as the difference between a ring and a rng is the absence of a multiplicative identity; the removal of "i" is meant to remind one that the identity is missing.

Example 1.9 (Even Integers). *The subset of the integers $\mathbf{Z}$ of even integers $2\mathbf{Z}$ with ordinary addition/multiplication and with $e_+ = 0$ is an example of a rng.*

One can also weaken a semiring structure similarly.

Definition 1.10 (Hemiring). *Given a set H, a **hemiring** structure on H is given by two binary operations $+, \cdot : H \times H \to H$ and a pair of elements $e_+, e_\cdot$ that satisfy the following properties:*

- $(H, +, e_+)$ *is a commutative monoid.*
- $(H, \cdot, e_\cdot)$ *is a semigroup.*
- ***Left Distribution.*** *For all $h_1, h_2, h_3 \in H$, we have*

$$h_1 \cdot (h_2 + h_3) = (h_1 \cdot h_2) + (h_1 \cdot h_3).$$

- ***Right Distribution.*** *For all $h_1, h_2, h_3 \in H$, we have*

$$(h_2 + h_3) \cdot h_1 = (h_2 \cdot h_1) + (h_3 \cdot h_1).$$

- ***Multiplicative Annihilation By Zero.*** *For all $h \in H$, we have*

$$h \cdot e_+ = e_+ \cdot h = e_+.$$

We can also drop either one of the distributive laws from a hemiring structure. These give rise to structures called left pre-semirings (dropping the right distributive law) and right pre-semirings (dropping the left distributive law).

Definition **1.11** (Left pre-semiring)**.** *Given a set P, a **left pre-semiring** structure on P is given by two binary operations $+, \cdot : P \times P \to P$ and a pair of elements $e_+, e_\cdot$ that satisfy the following properties:*

- $(P, +, e_+)$ *is a commutative monoid.*
- $(P, \cdot, e_\cdot)$ *is a semigroup.*
- ***Left Distribution.*** *For all $p_1, p_2, p_3 \in P$, we have*

$$p_1 \cdot (p_2 + p_3) = (p_1 \cdot p_2) + (p_1 \cdot p_3).$$

- ***Multiplicative Annihilation By Zero.*** *For all $p \in P$, we have*

$$p \cdot e_+ = e_+ \cdot p = e_+.$$

Definition **1.12** (Right pre-semiring)**.** *Given a set P, a **right pre-semiring** structure on P is given by two binary operations $+, \cdot : P \times P \to P$ and a pair of elements $e_+, e_\cdot$ that satisfy the following properties:*

- $(P, +, e_+)$ *is a commutative monoid.*
- $(P, \cdot, e_\cdot)$ *is a semigroup.*

- ***Right Distribution.*** *For all $p_1, p_2, p_3 \in P$, we have*
$$(p_2 + p_3) \cdot p_1 = (p_2 \cdot p_1) + (p_3 \cdot p_1).$$
- ***Multiplicative Annihilation By Zero.*** *For all $p \in P$, we have*
$$p \cdot e_+ = e_+ \cdot p = e_+.$$

These structures are less used than ring and commutative ring structures which play a central role in basic algebra. We end this subsection with three structures that are important in basic algebra.

Definition 1.13 (Integral Domain)**.** *Given a set D, a **integral domain** structure on D is given by two binary operations $+, \cdot : D \times D \to D$ and a pair of elements $e_+, e.$ with $e_+ \neq e.$ that satisfy the following properties:*

- *$(D, +, e_+)$ is a commutative group.*
- *$(D - \{e_+\}, \cdot, e.)$ is a commutative monoid.*
- ***Distribution.*** *For all $d_1, d_2, d_3 \in D$, we have*
$$d_1 \cdot (d_2 + d_3) = (d_1 \cdot d_2) + (d_1 \cdot d_3).$$
- ***Cancellation.*** *If $\alpha, \beta, d \in D$ with $d \neq 0$ and $d \cdot \alpha = d \cdot \beta$, then $\alpha = \beta$.*

Definition 1.14 (Field)**.** *Given a set F, a **field** structure on F is given by two binary operations $+, \cdot : F \times F \to F$ and a pair of elements $e_+, e.$ with $e_+ \neq e.$ that satisfy the following properties:*

- *$(F, +, e_+)$ is a commutative group.*
- *$(F - \{e_+\}, \cdot, e.)$ is a commutative group.*
- ***Distribution.*** *For all $f_1, f_2, f_3 \in F$, we have*
$$f_1 \cdot (f_2 + f_3) = (f_1 \cdot f_2) + (f_1 \cdot f_3).$$

Example 1.10. *The set of rational numbers $\mathbf{Q}$, the set of real numbers $\mathbf{R}$, and the set of complex numbers $\mathbf{C}$ are all examples of fields.*

Example 1.11 (Field with Two Elements)**.** *Let $F = \{e_+, e.\}$ and define addition and multiplication by*

$$\begin{aligned} e_+ + e. &= e. + e_+ = e., & e_+ \cdot e. &= e. \cdot e_+ = e_+, \\ e_+ + e_+ &= e_+, & e_+ \cdot e_+ &= e_+, \\ e. + e. &= e_+, & e. \cdot e. &= e.. \end{aligned}$$

We leave it for the reader to verify that F is a field under these binary operations.

Exercise 1.10. *Let X be a set with $|X| = 6$. Prove that there is no field structure on X.*

Exercise 1.11. *Let $(F, +, \cdot, e_+, e_\cdot)$ be a field. Prove that F is an integral domain.*

Definition 1.15 (Division Ring)**.** *Given a set D, a **division ring** structure on D is given by two binary operations $+, \cdot : D \times D \to D$ and a pair of elements $e_+, e_\cdot$ with $e_+ \neq e_\cdot$ that satisfy the following properties:*

- *$(D, +, e_+)$ is a commutative group.*
- *$(D - \{e_+\}, \cdot, e_\cdot)$ is a group.*
- ***Distribution.*** *For all $d_1, d_2, d_3 \in D$, we have*

$$d_1 \cdot (d_2 + d_3) = (d_1 \cdot d_2) + (d_1 \cdot d_3).$$

Division rings are also called skew-fields. Perhaps the most famous example of a division ring that it not a field is Hamilton's quaternions. We will review this example at the end of this section.

Remark 1.1. *So far we have used notation that is not typically used when working with the various algebraic structures above. For instance, when we refer to a ring R, we will denote the additive and multiplicative identities by 0_R and 1_R. When working with a single ring R, it is common place to further reduce notation and simply denote the elements by 0 and 1. This notation is abusive but in most instance, the context provides the precise meaning for ambiguous notation. When work with a group G, it is common to denote the binary operation by multiplication instead of addition. However, when G is commutative, it is more common to denote the binary operation by $+$. For a ring R, since $(R, +, 0)$ is a commutative group, it is standard to denote the commutative operator by $+$. Regardless of when the second operation is commutative or not, it is standard to suppress the multiplicative operation and write $r_1 r_2$ for $r_1 \cdot r_2$. In particular, if $r_1, s_1, r_2, s_2 \in R$, we can write*

$$r_1 s_1 + r_2 s_2$$

for what is more formally

$$r_1 \cdot s_1 + r_2 \cdot s_2.$$

We can also summation and product notation, That is, given $r_1, \ldots, r_n \in R$, we write

$$\sum_{i=1}^{n} r_i = r_1 + r_2 + \cdots + r_n$$

and

$$\prod_{i=1}^{n} r_i = r_1 r_2 \ldots r_n.$$

We will also use power and additive notation:

$$r^n \stackrel{def}{=} \underbrace{rr\dots r}_{n \text{ times}} = \prod_{i=1}^{n} r,$$

$$nr \stackrel{def}{=} \underbrace{r+r+\dots+r}_{n \text{ times}} = \sum_{i=1}^{n} r.$$

We end with an exercise on opposite rings.

Exercise 1.12. *Let $(R,+,\cdot,0_R,1_R)$ be a ring and let $*\colon R\times R\to R$ be given by $r*s \stackrel{def}{=} s\cdot r$. Prove that $(R,+,*,0_R,1_R)$ is a ring. [This ring structure on the set R is called the **opposite** and is denoted R^{op}].*

Exercise 1.13. *Let R be a ring such that $r_1r_2 = r_2r_1$ for some $r_1,r_2\in R$; we say that r_1,r_2 commute in this case. Prove that r_1 commutes with $-r_2$ and r_2^{-1} (assuming it exists). Prove that if r_1 commutes with r_2,r_3, then r_1 commutes with r_2+r_3.*

1.1.3 Modules and Vector Spaces

In this subsection, we will discuss algebraic structures that require a new type of operation. This operation involves two sets instead of one and generalizes the scalar multiplication operation on vector spaces.

In this subsection and the next, we will have algebraic structures on two sets and thus must be careful in referring to the various types of identity elements. We will also initially use a rather labor intensive notation to distinguish between various binary operations and functions.

Definition 1.16 (Left R–module)**.** *Given a ring $(R,+_R,\cdot_R,0_R,1_R)$ and commutative group $(M,+_M,0_M)$, a **left R–module** structure on M is a function $\cdot_{R,M}\colon R\times M\to M$ that satisfies the following properties:*

- ***Distributive Law, I.*** *For each $r\in R$ and $m_1,m_2\in M$, we have*

$$r\cdot_{R,M}(m_1+_M m_2) = (r\cdot_{R,M} m_1)+_M(r\cdot_{R,M} m_2).$$

- ***Distributive Law, II.*** *For each $r_1,r_2\in R$ and each $m\in M$, we have*

$$(r_1+_R r_2)\cdot_{R,M} m = (r_1\cdot_{R,M} m)+_M(r_2\cdot_{R,M} m).$$

- ***Scalar Compatibility.*** *For each $r_1,r_2\in R$ and $m\in M$, we have*

$$(r_1\cdot_R r_2)\cdot_{R,M} m = r_1\cdot_{R,M}(r_2\cdot_{R,M} m).$$

- ***Scalar Identity.*** *For each $m \in M$, we have*

$$1_R \cdot_{R,M} m = m.$$

The reader will note that our use of the above notation surely prevents any ambiguity in what binary operation or function is being used. However, it is unnecessary since each of the other operations, aside from the scalar function $\cdot_{R,M}$, only applies when the elements are from the same set. We will rewrite the above definition in a more standard way:

Given a ring R and commutative group M, a left R–module structure on M is a function $R \times M \to M$ that satisfies the following properties:

- **Distributive Law, I.** For each $r \in R$ and $m_1, m_2 \in M$, we have

$$r(m_1 + m_2) = rm_1 + rm_2.$$

- **Distributive Law, II.** For each $r_1, r_2 \in R$ and each $m \in M$, we have

$$(r_1 + r_2)m = r_1 m + r_2 m.$$

- **Scalar Compatibility.** For each $r_1, r_2 \in R$ and $m \in M$, we have

$$(r_1 r_2)m = r_1(r_2 m).$$

- **Scalar Identity.** For each $m \in M$, we have

$$1_R m = m.$$

For completeness, we give the definition of a right R–module structure.

Definition **1.17** (Right R–module)**.** *Given a ring R and commutative group M, a **right R–module** structure on M is a function $M \times R \to M$ that satisfies the following properties:*

- ***Distributive Law, I.*** *For each $r \in R$ and $m_1, m_2 \in M$, we have*

$$(m_1 + m_2)r = m_1 r + m_2 r.$$

- ***Distributive Law, II.*** *For each $r_1, r_2 \in R$ and each $m \in M$, we have*

$$m(r_1 + r_2) = mr_1 + mr_2.$$

- ***Scalar Compatibility.*** *For each $r_1, r_2 \in R$ and $m \in M$, we have*
$$m(r_1 r_2) = (m r_1) r_2.$$
- ***Scalar Identity.*** *For each $m \in M$, we have*
$$m 1_R = m.$$

In the following exercise, we refer the reader to Exercise 1.12 for the definition of R^{op}.

Exercise 1.14. *Let R be a ring, M be a commutative group, and let $\cdot : R \times M \to M$ be a left R–module structure on M. Prove that the function $* : M \times R^{op} \to M$ given by $m * r \stackrel{def}{=} r \cdot m$. Prove that M with $*$ is a right R^{op}–module. [Hint: Scalar compatibility]*

When $R = F$ is a field, the concept of an F–module and an F–vector space coincide.

Definition 1.18 (F–vector space)**.** *Given a field F and a commutative group V, a **F–vector space** structure on V is a function $F \times V \to V$ that satisfies the following properties:*

- ***Distributive Law, I.*** *For each $\alpha \in F$ and $v_1, v_2 \in V$, we have*
$$\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2.$$
- ***Distributive Law, II.*** *For each $\alpha_1, \alpha_2 \in F$ and each $v \in V$, we have*
$$(\alpha_1 + \alpha_2) v = \alpha_1 v + \alpha_2 v.$$
- ***Scalar Compatibility.*** *For each $\alpha_1, \alpha_2 \in R$ and $v \in V$, we have*
$$(\alpha_1 \alpha_2) v = \alpha_1 (\alpha_2 v).$$
- ***Scalar Identity.*** *For each $v \in V$, we have*
$$1 v = v.$$

Below are two elementary properties for vector spaces:

Exercise 1.15. *Let F be a field and V an F–vector space.*

(a) Prove that $0_F v = 0_V$ for all $v \in V$.

(b) Prove that $(-1_F)v = -v$ where -1_F denotes the additive inverse of 1_F and $-v$ is the additive inverse of v.

The focus in this class will reside mostly with groups, rings, and fields. However, we will use vector spaces both to serve as motivation as well as in our treatment of elementary field theory.

1.1.4 Algebras

In this final subsection, we introduce one of the richest algebraic structures called algebras. Loosely, given a commutative ring R, R–algebras are both R–modules and rings where these structures satisfy a compatibility condition

Definition **1.19** (R–algebra)**.** *Given a commutative ring R and a left R–module A that is also endowed with a rng structure, an **left R–algebra** structure on A satisfies the following property:*

- ***Scalar/Ring Multiplicative Compatibility.*** *For each $r \in R$ and for each $a_1, a_2 \in A$, we have*

$$r(a_1 a_2) = (ra_1)a_2 = a_1(ra_2).$$

We note that the algebra A need not have a multiplicative identity since we merely assumed that A is a rng.

Definition **1.20** (Unital R–algebra)**.** *We say that a left R–algebra A is **unital** if A is a ring.*

Definition **1.21** (Commutative R–algebra)**.** *We say that a left R–algebra is **commutative** if A is a commutative rng.*

Definition **1.22** (R–division algebra)**.** *We say that a left R–algebra is a **R–division algebra** if A is a division ring.*

Example **1.12** (Hamilton's Quaternions)**.** *We will view $\mathbf{R}^4$ has a real vector space with basis u, x, y, z. In particular, every element $\lambda \in \mathbf{R}^4$ has a unique expression*

$$\lambda = \lambda_1 u + \lambda_2 x + \lambda_3 y + \lambda_4 z$$

with $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbf{R}$. We define multiplication by the rules

$$x^2 = -1, \quad y^2 = -1, \quad xy = z, \quad yx = -xy.$$

Additionally, we insist that $u\lambda = \lambda u = \lambda$ for all $\lambda \in \mathbf{R}^4$. We extend multiplication to general pairs as follows. Given

$$\lambda = \lambda_1 u + \lambda_2 x + \lambda_3 y + \lambda_4 z$$
$$\tau = \tau_1 u + \tau_2 x + \tau_3 y + \tau_4 z,$$

we have

$$\begin{aligned}\lambda\tau &= (\lambda_1 u+\lambda_2 x+\lambda_3 y+\lambda_4 z)(\tau_1 u+\tau_2 x+\tau_3 y+\tau_4 z)\\ &= \lambda_1 u\tau_1 u+\lambda_1 u\tau_2 x+\lambda_1 u\tau_3 y+\lambda_1 u\tau_4 z+\lambda_2 x\tau_1 u+\lambda_2 x\tau_2 x+\lambda_2 x\tau_3 y+\lambda_2 x\tau_4 z\\ &\quad+\lambda_3 y\tau_1 u+\lambda_3 y\tau_2 x+\lambda_3 y\tau_3 y+\lambda_3 y\tau_4 z+\lambda_4 z\tau_1 u+\lambda_4 z\tau_2 x+\lambda_4 z\tau_3 y+\lambda_4 z\tau_4 z\\ &= (\lambda_1\tau_1-\lambda_2\tau_2-\lambda_3\tau_3-\lambda_4\tau_4)u+(\lambda_1\tau_2+\lambda_2\tau_1+\lambda_3\tau_4-\lambda_4\tau_3)x\\ &\quad+(\lambda_1\tau_3-\lambda_2\tau_4+\lambda_3\tau_1+\lambda_4\tau_2)y+(\lambda_1\tau_4+\lambda_2\tau_3-\lambda_3\tau_2+\lambda_4\tau_1)z.\end{aligned}$$

With these algebraic operations, $\mathbf{R}^4$ *is a non-commutative unital* $\mathbf{R}$*–algebra and is denoted by* $\mathbb{H}$*. We call this algebra the real quaternion algebra.*

Exercise 1.16. *Prove that* $\mathbb{H}$ *is a division algebra.*

Of course, $\mathbf{R}$, $\mathbf{C}$ are both commutative, unital $\mathbf{R}$–algebras. Additionally, the set of n by n real matrices $\mathrm{Mat}(n,\mathbf{R})$ with the usual $\mathbf{R}$–vector space structure and the usual matrix addition/multiplication is a non-commutative (if $n>1$), unital $\mathbf{R}$–algebra.

Exercise 1.17. *Prove that* $\mathrm{Mat}(n,\mathbf{R})$ *is a division algebra if and only if* $n=1$*. [Hint: Find an element that cannot be inverted]*

1.2 *Algebraic Subobjects*

In this section, we will introduce various concepts of subobjects. Before starting formally with subgroups of groups, we will discuss a bit of the philosophy of what a subobject should be via vector spaces.

In a set X, the interesting subobjects are all subsets of the given set and so yield the power set $\mathscr{P}(X)$. In a **topological space**, the open subsets (or alternatively the closed subsets) comprise the subsets that encode all of the information provided via the topology. This is a proper subset of the power set provide the topology is not the **discrete topology**. In particular, the richer/more restrictive the structure, the smaller the subset of the power set the subsets of interest become. We will see a similar phenomenon which we consider suitable functions between sets equipped with algebraic structures. Moreover, for a certain class of subobjects, we will associate to each one, a unique function compatible the algebraic structure.

Before starting our discussion of subobjects formally, we will first recall this concept in a vector space. For concreteness, we will take $\mathbf{R}^n$ to be our vector space over $\mathbf{R}$. Recall that a non-empty subset $W\subseteq\mathbf{R}^n$ is a (real) vector subspace of $\mathbf{R}^n$ if W is closed under both addition and scalar multiplication. That is, given $w_1,w_2\in W$ and $\alpha,\beta\in\mathbf{R}$, we must have $\alpha w_1+\beta w_2\in W$. As a result of this condition, we

know that if we restrict the binary function $+\colon \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}^n$ to the subset $W \times W \subseteq \mathbf{R}^n \times \mathbf{R}^n$, then $+_{|W\times W}\colon W \times W \to W$. Note that for a general subset $S \subseteq \mathbf{R}^n$, we can restrict $+$ to the subset $S \times S$. However, the image of $S \times S$ under this function need not be contained in S. Likewise, we can restrict the function $\cdot\colon \mathbf{R} \times \mathbf{R}^n \to \mathbf{R}^n$ to $\mathbf{R} \times W$ and by our assumption on W, we see that $\cdot_{|\mathbf{R}\times W}\colon \mathbf{R} \times W \to W$. Again, for a general subset S of $\mathbf{R}^n$, there is no reason that the image of $\mathbf{R} \times S$ under $\cdot$ will be contained in S. Since W is non-empty, we know that there is some $w_0 \in W$. If $w_0 = 0_{\mathbf{R}^n}$, then we see that $0_{\mathbf{R}^n} \in W$. Otherwise, if $w_0 \neq 0_{\mathbf{R}^n}$, then since $w_0 - w_0 \in W$, we again see that $0_{\mathbf{R}^n} \in W$.

We now summarize this discussion. Given a vector subspace $W \subseteq \mathbf{R}^n$, we see that W is itself a vector space with the binary operation $+$ restricted to $W \times W$ and the scalar multiplication function restricted to $\mathbf{R} \times W$. Indeed, as $+, \cdot$ satisfy all of the properties needed to be a real vector space, we see that W does as well. Moreover, any non-empty subset W of $\mathbf{R}^n$ for which the operations $+, \cdot$ restrict to W to give functions $W \times W \to W$ and $\mathbf{R} \times W \to W$ is a vector subspace of $\mathbf{R}^n$. In particular, vector subspaces are just subsets of the vector space for which the vector space structure restricts to the subset to endow it with vector space structure.

1.2.1 Subgroups

Throughout this subsection, G will denote a group. We will use juxtaposition to denote the binary operation and we will denote the identity element in G by 1_G. In the event our group is commutative, we will often switch to an additive binary operation and then we will denote the identity element by 0_G. Given an element $g \in G$, we will denote the inverse of g by g^{-1}.

Definition 1.23 (Subgroup)**.** *We say that $H \subseteq G$ of a group G is a **subgroup** if H satisfies the following properties:*

- ***Non-empty.*** *H is non-empty.*
- ***Closed Under Multiplication.*** *For each $h_1, h_2 \in H$, we have $h_1 h_2 \in H$.*
- ***Closed Under Inverses.*** *For each $h \in H$, we have $h^{-1} \in H$.*

When H is a subgroup of G, we will write $H \leq G$.

We state a few basic exercises on subgroups.

Exercise 1.18. *Prove that the following are equivalent for a subset H of a group G:*

(a) H is a subgroup of G.

(b) *H is non-empty and for each $h_1, h_2 \in H$, we have $h_1 h_2^{-1} \in H$.*

For our next exercise, we require an additional piece of notation. Given a group G, we define a function $\iota_G \colon G \to G$ by $\iota_G(g) \stackrel{\text{def}}{=} g^{-1}$. This function is sometimes called the inversion map.

Exercise 1.19. *Let G be a group with associated binary operation $\cdot$, inversion map ι_G, and identity element 1_G. Given a subgroup $H \leq G$, prove the following:*

(i) *$1_G \in H$.*

(ii) *The image of the restriction of $\cdot$ to $H \times H$ is contained in H.*

(iii) *The image of the restriction of ι_G to H is contained in H.*

(iv) *H is a group with the binary operation $\cdot_{|H\times H} \colon H \times H \to H$ and identity 1_G.*

As a result of Exercise 1.19, we can view subgroups of a group as groups.

Exercise 1.20. *Let G be a group with a subgroup H and let K be a subgroup of H. Prove that K is a subgroup of G.*

Exercise 1.21. *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*

(ii) *Prove that $\{1_G\}$ 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 $s_1 s_2 \dots s_\ell$ where for each $i = 1, \dots, \ell$, 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,*

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

We will now give several different examples of subgroups of groups. 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 $[g_1, g_2] = 1_G$.

Exercise 1.22. *Let $g_1, g_2 \in G$.*

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

(ii) Prove that $g_1 g_2 = g_2 g_1$ if and only if $[g_1, g_2] = 1_G$.

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

$$Z(G) = \{g_0 \in G \,:\, [g, g_0] = 1_G \text{ for all } g \in G\}.$$

Exercise 1.23. *Let G be a group. Prove that $Z(G)$ is a subgroup of G.*

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

$$C_G(g) = \{g_0 \in G \,:\, [g, g_0] = 1_G\}.$$

Exercise 1.24. *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

$$C_G(H) = \{g_0 \in G \,:\, [h, g_0] = 1_G \text{ for all } h \in H\}.$$

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 1.25. *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 $C_G(H) \leq N_G(H)$.

Remark 1.2. *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 1.26. *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 1.27. *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 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.

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 1.28. *Let G be a group. Prove that $G_{i+1} \leq G_i$ 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 1.29. *Let G be a group.*

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

(ii) Prove that $G^i \leq G_i$ for all $i \geq 0$.

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

Exercise 1.30. *Let G be a group and let $H_1, H_2, H_3 \leq G$ with $H_1 \leq H_2$. Prove that if $H_1 \cap H_3 = H_2 \cap H_3$ and $H_1H_3 = H_2H_3$, then $H_1 = H_2$. Here*

$$H_iH_j \stackrel{def}{=} \{h_ih_j \ : \ h_i \in H_i, \ h_j \in H_j\}.$$

Exercise 1.31. *Let G be a group and $H_1, H_2, H_3 \leq G$ with $H_1 \leq H_2$. Prove that $H_1H_2 \cap H_3 = H_1(H_2 \cap H_3)$.*

Exercise 1.32. *Let G be a group and $H_1, H_2 \leq G$. Prove that H_1H_2 is a subgroup of G if and only if $H_1H_2 = H_2H_1$.*

1.2.2 Subrings

In this short subsection, we will introduce the concept of a subring.

Definition 1.24 (Subring)**.** *Given a ring R and a subset $S \subseteq R$, we say that S is a **subring** if S satisfies the following properties:*

- ***Non-empty.*** $1_R \in S$.
- ***Closed Under Addition.*** *For each $s_1, s_2 \in S$, we have $s_1 + s_2 \in S$.*
- ***Closed Under Additive Inverses.*** *For each $s \in S$, we have $-s \in S$.*
- ***Closed Under Multiplication.*** *For each $s_1, s_2 \in S$, we have $s_1s_2 \in S$.*

When S is a subring of R, we write $S \leq R$.

When R is a ring and $S \leq R$ is a subring, it is common to refer to R as an extension ring of S.

Exercise 1.33. *Let R be a ring and define $\mathrm{Mat}(n,R)$ to be the set of n by n matrices with coefficients in R.*

(i) Prove that if $S \leq R$ is a subring, then $\mathrm{Mat}(n,S) \leq \mathrm{Mat}(n,R)$ is a subring.

(ii) Prove that $A \in \mathrm{Mat}(n,R)$ is invertible if and only if $\det(A)$ is a unit in R.

Exercise 1.34. *For each prime p, define R_p to be the subset of $\mathbf{Q}$ of rational numbers $\frac{a}{b}$ such that a, b are relatively prime and b, p are relatively prime.*

(i) Prove that R_p is a subring of $\mathbf{Q}$.

(ii) Prove that if $m \in \mathbf{Z} \leq R_p$ is invertible in R_p if and only if m is relatively prime with p.

Exercise 1.35. *Let R be a ring with a subring $S \leq R$ and let X be a set. Endow $\mathrm{Fun}(X,R)$ with a ring structure via point-wise addition and multiplication. Prove that the subset*

$$\{f \in \mathrm{Fun}(X,R) \ : \ f(x) \in S \text{ for all } x \in X\}$$

is a subring of $\mathrm{Fun}(X,R)$.

Exercise 1.36. *Let $C(a,b)$ be the set of continuous functions $f\colon [a,b] \to \mathbf{R}$. Prove that $C(a,b)$ is a subring of $\mathrm{Fun}([a,b],\mathbf{R})$.*

Exercise 1.37. *Let R be a ring and define*

$$Z(R) \stackrel{def}{=} \left\{r \in R \ : \ rr' = r'r \text{ for all } r' \in R\right\}.$$

Prove that $Z(R)$ is a subring of R.

1.3 *Morphisms*

Broadly, morphisms between sets equipped with algebraic structures are functions which are compatible with the algebraic structures. Perhaps the first example of a morphism is the concept of a linear function $L\colon V \to W$ between two real vector spaces. Recall, that L is linear if L satisfies the properties:

- **Compatible Under Addition.** For each $v_1, v_2 \in V$, we have
$$L(v_1 + v_2) = L(v_1) + L(v_2).$$
- **Compatible Under Scalar Multiplication.** For each $\alpha \in \mathbf{R}$ and $v \in V$, we have
$$L(\alpha v) = \alpha L(v).$$

We will review the concept of a morphisms with a focus on morphisms between groups and rings.

1.3.1 Groups Homomorphisms

Definition 1.25 (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 $\psi(g_1 g_2) = \psi(g_1)\psi(g_2)$ for all $g_1, g_2 \in G$.*

Note that in Definition 1.25, 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 1.38. *Prove that if $\psi\colon G \to H$ is a homomorphism of groups, then the following holds:*

(i) $\psi(1_G) = 1_H$ *where $1_G \in G$ and $1_H \in H$ are the identity elements.*

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

Exercise 1.39. *Let G be a group and $g \in G$. Prove that $\mathrm{Ad}_g\colon G \to G$ defined by $\mathrm{Ad}_g(h) \overset{def}{=} g^{-1}hg$ is a 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 1.26 (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.*

Exercise 1.40. *Prove that if $\psi\colon G_1 \to G_2$ is an isomorphism, then $\psi^{-1}\colon G_2 \to G_1$ is an isomorphism.*

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

$$\ker\psi = \{g \in G \ :\ \psi(g) = 1_H\}$$

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**.

If M_1, M_2 are monoids and $\psi\colon M_1 \to M_2$ is a function, we say ψ is a **monoid homomorphism** if the following properties hold:

- For all $m_1, m_1' \in M_1$, we have $\psi(m_1 m_1') = \psi(m_1)\psi(m_1')$.
- $\psi(1_{M_1}) = 1_{M_2}$.

If M_1, M_2 were semigroups, then we would only insist on the first condition in the definition of a **semigroup homomorphism** or a magma homomorphism.

Exercise 1.41. *Let G_1, G_2 be groups and $\psi\colon G_1 \to G_2$ be a group homomorphism. Prove that ψ is injective if and only if $\ker\psi = \{1_{G_1}\}$.*

Exercise 1.42. *Let M be a magma and define*

$$\mathrm{Hom}(M,M) \stackrel{def}{=} \{\psi\colon M \to M \ : \ \psi \text{ is a magma homomorphism}\}.$$

Prove that $\mathrm{Hom}(M,M)$ is a monoid with binary operation given by composition of functions and with the identity being the identity function.

Exercise 1.43. *Let M be a magma and define*

$$\mathrm{Aut}(M) \stackrel{def}{=} \{\psi \in \mathrm{Hom}(M,M) \ : \ \psi \text{ is bijective}\}.$$

Prove that $\mathrm{Aut}(M)$ is a submonoid of $\mathrm{Hom}(M,M)$. Prove that $\mathrm{Aut}(M)$ is, in fact, a group.

Exercise 1.44. *Let X be a set and M be a magma. Prove that $\mathrm{Fun}(X,M)$ is a magma where the binary operation is given by point-wise multiplication.*

Exercise 1.45. *Let M be a set, $m_0 \in M$, and define $M \times M \to M$ via*

$$(m_1, m_2) \longmapsto m_0.$$

Prove that M is a semigroup under this binary operation and prove that $\mathrm{Aut}(M) = \mathrm{Sym}(M) \subseteq \mathrm{Fun}(M,M)$.

Exercise 1.46. *Let G be a group and let $\mathrm{Hom}(\mathbf{Z}, G)$ denote the set of group homomorphisms $\psi\colon \mathbf{Z} \to G$.*

(i) Let $g_0 \in G$. Define $\psi_{g_0} : \mathbf{Z} \to G$ by $\psi(n) = g_0^n$. Prove that ψ_{g_0} is a homomorphism of groups.

(ii) Define Eval$:\ \mathrm{Hom}(\mathbf{Z}, G) \to G$ *by* $\mathrm{Eval}(\psi) = \psi(1)$. *Prove thet* Eval *is a bijection.*

(iii) Define a binary operation $*:\ \mathrm{Hom}(\mathbf{Z}, G) \times \mathrm{Hom}(\mathbf{Z}, G) \to \mathrm{Hom}(\mathbf{Z}, G)$ *by*

$$\rho_1 * \rho_2 \stackrel{def}{=} \mathrm{Eval}^{-1}(\mathrm{Eval}(\rho_1)\,\mathrm{Eval}(\rho_2))$$

where $\mathrm{Eval}(\rho_1)\mathrm{Eval}(\rho_2)$ *denotes the product of* $\mathrm{Eval}(\rho_1)$ *and* $\mathrm{Eval}(\rho_2)$ *via the group structure on G. Prove that* $\mathrm{Hom}(\mathbf{Z}, G)$ *is a group with this binary operation and with identity* ρ_0 *where* $\rho_0(n) = 1_G$.

(iv) Prove that the function Eval$:\ \mathrm{Hom}(\mathbf{Z}, G) \to G$ *is an isomorphism of groups where* $\mathrm{Hom}(\mathbf{Z}, G)$ *is given the group structure from (c).*

Exercise 1.47. *Let G_1, G_2, G be groups and let $\psi : G_1 \to G_2$ be a group homomorphism.*

(i) Define $\psi^\star : \mathrm{Hom}(G_2, G) \to \mathrm{Hom}(G_1, G)$ by $\psi^\star(\tau) = \tau \circ \psi$. Prove that if ψ is an isomorphism, then $\psi^\star$ is a bijection.

(ii) Find an example where ψ is not bijective but $\psi^\star$ is a bijection.

Exercise 1.48. *Let G_1, G_2, G be groups and let $\psi : G_1 \to G_2$ be a group homomorphism.*

(i) Define $\psi_\star : \mathrm{Hom}(G, G_1) \to \mathrm{Hom}(G, G_2)$ by $\psi_\star(\tau) = \psi \circ \tau$. Prove that if ψ is an isomorphism, then $\psi_\star$ is a bijection.

(ii) Find an example where ψ is not bijective but $\psi_\star$ is a bijection.

(iii) If $G = \mathbf{Z}$ and $\varphi = \psi_{g_1} \in \mathrm{Hom}(\mathbf{Z}, G_1)$ where ψ_{g_1} is as in Exercise **??**, *then $\psi_\star(\psi_{g_1}) = \psi_{\psi(g_1)}$.*

Exercise 1.49. *Let G be a group such that for each $g_1, g_2 \in G$, we have $(g_1 g_2)^2 = g_1^2 g_2^2$. Prove that G is commutative.*

Exercise 1.50. *Let $\psi : G \to G'$ be a homomorphism of groups and let $H' \leq G'$. Prove that $\psi^{-1}(H')$ is a subgroup of G and $\ker\psi \leq \psi^{-1}(H')$.*

Exercise 1.51. *Let $\psi : G \to G'$ be a homomorphism of groups and let $H \leq G$. Prove that*

$$\psi^{-1}(\psi(H)) = H \ker\psi.$$

1.3.2 Ring Homomorphisms

The analog of a homomorphism in the ring setting is a ring homomorphism.

Definition 1.27 (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 $r_1, r_2, r_3, r_4 \in R$.*

As with a group homomorphism, given a homomorphism of rings $\psi\colon R \to R'$, we define the **kernel** of ψ to be

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

and the image of ψ to be

$$\psi(R) = \left\{r' \in R \ : \ \psi(r) = r' \text{ for some } r \in R\right\}.$$

Exercise 1.52. *Let $\psi\colon R \to R'$. Is $\ker \psi$ a subring of R? Is $\psi(R)$ a subring of R'?*

Exercise 1.53. *Let $\iota_{\mathbf{N}}\colon \mathbf{N} \cup \{0\} \to \mathbf{Z}$ be the inclusion function $\iota_{\mathbf{N}}(n) = n$. Prove that if G is a group and $\psi\colon \mathbf{N} \cup \{0\} \to G$ is a monoid homomorphism, then there exists a unique group homomorphism $\Psi\colon \mathbf{Z} \to G$ such that $\Psi(\iota_{\mathbf{N}}(n)) = \psi(n)$ for all $n \in \mathbf{N} \cup \{0\}$.*

Exercise 1.54. *Let R be a ring and define $\psi_R\colon \mathbf{Z} \to R$ by*

$$\psi_R(n) = \sum_{i=1}^{n} 1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}}.$$

Prove that ψ_R is a ring homomorphism.

Exercise 1.55. *Let $C(a,b)$ be as in Exercise 1.36. Let $f \in C(a,b)$ and define $T_f\colon C(a,b) \to \mathbf{R}$ by*

$$T_f(g) = \int_a^b fg.$$

Prove that T_f is an $\mathbf{R}$–linear function. Is T_f a ring homomorphism?

Exercise 1.56. *Let R_1, R_2, R_3 be rings and let $\psi_1\colon R_1 \to R_2$, $\psi_2\colon R_2 \to R_3$ be ring homomorphisms. Prove that $\psi_2 \circ \psi_1$ is a ring homomorphisms.*

Exercise 1.57. *Let R, R_1, R_2 be rings and $\psi_i\colon R \to R_i$ be ring homomorphisms for $i = 1, 2$. Prove that $\psi\colon R \to R_1 \times R_2$ given by $\psi(r) = (\psi_1(r), \psi_2(r))$ is a ring homomorphism and determine $\ker \psi$.*

Exercise 1.58. *Let R_1, R_2 be rings and $\psi\colon R_1 \to R_2$ be a ring homomorphism. Let $\mathrm{Mat}(n,R)$ denote the ring of n by n matrices with coefficients in R and for each $A \in \mathrm{Mat}(n,R)$, we will denote the i,j coefficient of A by $A_{i,j}$. Define $\tau\colon \mathrm{Mat}(n,R_1) \to \mathrm{Mat}(n,R_2)$ by $\tau(A) = B$ where $B_{i,j} = \psi(A_{i,j})$. Prove that τ is a ring homomorphism.*

1.4 *Quotient Spaces*

1.4.1 Quotients of Groups and Normal Subgroups

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 1.28 (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 $H \lhd G$.*

Before discussing quotients of groups by subgroups and normal subgroups, we give some exercises for further the reader's understanding on normal subgroups.

Exercise 1.59. *Let G be a group and $H \leq G$ a subgroup. Prove the following are equivalent:*

(a) H is normal.

(b) For each $g \in G$, we have

$$gH = Hg$$

where

$$gH = \{gh \ : \ h \in H\}, \quad Hg = \{hg \ : \ h \in H\}.$$

Exercise 1.60. *Let G be a group and $H \leq G$.*

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

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

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

Exercise 1.61. *Let G be a group and $[G,G]$ be the commutator subgroup. Prove that $[G,G]$ is a normal subgroup of G.*

Exercise 1.62. *Let G be a group and let G_i, G^i denote the lower central and derived series of G (see*

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

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

Exercise 1.63. *Let G be a group. Prove that $Z(G)$ is normal in G.*

Exercise 1.64. *Let G be a group, let $[G,G]$ be the commutator subgroup, and $H \leq G$ with $[G,G] \leq H$. Prove that $H \lhd G$.*

Lemma 1.3. *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 1.38 (i), we know that $e_G \in \ker\psi$. Given $g_1, g_2 \in \ker\psi$, by Exercise 1.21 (i), it suffices to prove that $g_1 g_2^{-1} \in \ker\psi$. To that end, we have

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

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

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

Next, we prove that $\psi(G)$ is a subgroup of H. By Exercise 1.38 (i), $\psi(1_G) = 1_H$, and so $1_H \in \psi(G)$. Hence, by Exercise 1.21 (i), it suffices to prove that if $h_1, h_2 \in \psi(G)$, then $h_1 h_2^{-1} \in \psi(G)$. 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

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

♠

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

Lemma 1.4. *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 1.65. *Prove Lemma 1.4*

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 1.7 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 1.29 (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*

$$gH = \{gh \ : \ h \in H\}$$

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

$$Hg = \{hg \ : \ h \in H\}.$$

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 1.66. *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 $g_1 H = g_2 H$ or $g_1 H \cap g_2 H = \emptyset$. [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 1.66, 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 1.30 (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 $[G:H]$.*

Below is a list of problems on indices of subgroups.

Exercise 1.67. *Let G be a group and let $H, K \leq G$ be finite index subgroups. Prove the following:*

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

(ii) *Assuming G is finite, prove that*

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

*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 $[HK : H] = [K : H \cap K]$.*

If H is a normal subgroup, the set G/H can be equipped with a group structure as follows. We define $\overline{1_G} = 1_G H = H$ and given $g_1 H, g_2 H \in G/H$, we define $*\colon G/H \times G/H \to G/H$ by

$$g_1 H * g_2 H \stackrel{\text{def}}{=} (g_1 g_2) H.$$

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

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

and

$$(g_1g_2)H \subseteq (k_1k_2)H.$$

To that end, let $g \in (k_1k_2)H$. By definition, there exists $h_1 \in H$ such that $g = k_1k_2h_1$. Since $k_1 \in g_1H$, there exists $h_2 \in H$ such that $k_1 = g_1h_2$. Likewise, since $k_2 \in g_2H$, there exists $h_3 \in H$ such that $k_2 = g_2h_3$. In particular, we have

$$g = g_1h_2g_2h_3h_1. \tag{1.11}$$

Now, $h_2g_2 \in Hg_2$ and by Exercise 1.66 (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 $h_2g_2 = g_2h_4$. Replacing h_2g_2 with g_2h_4 in (1.11), we obtain

$$g = g_1g_2h_4h_3h_1.$$

Since H is a subgroup, we know that $h_4h_3h_1 \in H$. Setting $h_5 = h_4h_3h_1$, we obtain

$$g = g_1g_2h_5 \in (g_1g_2)H.$$

Thus, we conclude that $(k_1k_2)H \subseteq (g_1g_2)H$.

For the reverse implication, which is logically identical, we start with $g \in (g_1g_2)H$. By definition, there exists $h_6 \in H$ such that $g = g_1g_2h_6$. Since $g_1 \in k_1H$ and $g_2 \in k_2H$, there exist $h_7, h_8 \in H$ such that $g_1 = k_1h_7$ and $g_2 = k_2h_8$. Hence

$$g = k_1h_7k_2h_8h_6 \tag{1.12}$$

Since H is normal, we know that $k_2H = Hk_2$ and so there exists $h_9 \in H$ such that $h_7k_2 = k_2h_9$. Replacing h_7k_2 with k_2h_9 in (1.12) yields

$$g = k_1k_2h_9h_8h_6.$$

Finally, setting $h_{10} = h_9h_8h_6 \in H$, we see that

$$g = k_1k_2h_{10} \in (k_1k_2)H.$$

Hence, $(g_1g_2)H \subseteq (k_1k_2)H$.

It remains to prove that $*$ with $\overline{1_G}$ is a group structure on G/H. By definition of $*$, we see that

$$1_GH * gH = (1_Gg)H = gH, \quad gH * 1_GH = (g1_GG)H = gH.$$

Hence, 1_GH 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 $*$, we have

$$gH * g^{-1}H = (gg^{-1})H = 1_GH, \quad g^{-1}H * gH = (g^{-1}g)H = 1_GH.$$

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

$$g_1H * (g_2H * g_3H) = (g_1H * g_2H) * g_3H.$$

To that end, we have

$$\begin{aligned} g_1H * (g_2H * g_3H) &= g_1H * (g_2g_3)H = (g_1(g_2g_3))H \\ &= ((g_1g_2)g_3)H = (g_1 \cdot g_2)H * g_3H \\ &= (g_1H * g_2H) * g_3H. \end{aligned}$$

We now summarize the above construction in the following definition.

Definition 1.31 (Quotient Group)**.** *Given a group G and normal subgroup $H \lhd G$, we call the set G/H with the group structure $*$ and $\overline{1_G}$ 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 $\psi_H(g_1g_2) = \psi_H(g_1)\psi_H(g_2)$. For that, simply note that

$$\psi_H(g_1g_2) = (g_1g_2)H = g_1Hg_2H = \psi_H(g_1)\psi_H(g_2).$$

We again summarize the above observation in the following definition.

Definition 1.32 (Canonical Homomorphism)**.** *Given a group G and normal subgroup H, the homomorphism $\psi_H \colon G \to G/H$ is called the **canonical homomorphism**.*

Exercise 1.68. *Let G be a group and $H \leq G$ with $[G : H] = 2$. Prove that H is a normal subgroup.*

Exercise 1.69. *Find an example of a group G such that $H \lhd G$ and $K \lhd H$ but K is not a normal subgroup of G.*

Supplemental Material: Special Groups.*

We say that a group G is **commutative** if $[G,G] = \{1_G\}$. The following exercise shows that this matches our previous definition of a commutative group.

Exercise 1.70. *Prove that G is commutative if and only if every pair $g, g' \in G$ commute.*

Exercise 1.71. *Let G be an commutative group.*

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

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

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

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

Exercise 1.72. *Prove that commutative groups are precisely the nilpotent groups of step size 1.*

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

Exercise 1.73. *Prove that commutative groups are precisely the solvable groups of step size 1.*

Exercise 1.74. *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 1.75. *Prove that cyclic groups are commutative. Prove that if G_1, G_2 are finite cyclic groups and $|G_1| = |G_2|$, then G_1, G_2 are isomorphic.*

Exercise 1.76. *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 commutative 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 commutative 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 $\not\in = (1_{G_\alpha})_{\alpha\in I}$ 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 1.77. *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 commutative, then $\prod_\alpha G_\alpha$ is commutative.

(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 1.78. *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 commutative, then H is commutative.

(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 1.79. *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*

$$g^n \stackrel{def}{=} \underbrace{gg\ldots g}_{n\text{ times}}.$$

(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.*

Exercise 1.80. *Let $\mathbf{Q}$ be the rational numbers which we view as a group under addition. Prove that if $G\leq\mathbf{Q}$ is a finitely generated subgroup, then there exists $g\in G$ such that $\langle g\rangle = G$.*

1.4.2 Quotients of Rings and Ideals

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

***Definition* 1.33** (Ideal)**.** *Let R be a commutative ring. A subrng $\mathfrak{a}$ 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 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* 1.34** (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* 1.81.** *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* 1.82.** *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 $\mathbf{Z}$?*

***Exercise* 1.83.** *Let $\psi \colon R \to R'$ be a ring homomorphism and let $U_R, U_{R'}$ denote the group of units of R, R', respectively.*

(i) Prove that $\psi(U_R) \subseteq U_{R'}$.

(ii) Prove that $\psi_{|U_R}: U_R \to U_{R'}$ is a homomorphism of groups.

As a consequence of Exercise 1.81, 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 1.7.

The following basic lemma will be useful later.

Lemma 1.5. *Let R be a commutative ring 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 1.71 (i). Moreover, R/S is an commutative group by Exercise 1.71 (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* 1.35** (Quotient Ring)**.** *Let R be a commutative ring 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* 1.84.** *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* 1.85.** *Let R be a commutative ring 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 1.6. *Let R, R' be commutative rings and $\psi\colon R \to R'$ be a ring homomorphism. Then $\psi(R)$ is a subring of R' and $\ker\psi$ is an ideal of R.*

Proof. By Lemma 1.3, 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 1.3, 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 1.7 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. ♠

We end this subsection with the definition of a ring isomorphism.

Definition 1.36 (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 $R \cong R'$.*

Exercise 1.86. *Let $\psi\colon R \to R'$ be an isomorphism of rings. Prove that $\psi_{|U_R}\colon U_R \to U_{R'}$ is an isomorphism of groups.*

Exercise 1.87. *Let X be a set, $x \in X$, and equip $\mathrm{Fun}(X, \mathbf{R})$ with a ring structure via point-wise addition and multiplication. Define*

$$\mathrm{Eval}_x\colon \mathrm{Fun}(X, \mathbf{R}) \longrightarrow \mathbf{R}$$

by $\mathrm{Eval}_x(f) = f(x)$.

(i) Prove that Eval_x is a ring homomorphism.

(ii) Prove that Eval_x is surjective.

Exercise 1.88. *Let R be a commutative ring and $r_0 \in R$. Prove that*

$$\langle r_0 \rangle = \{r_0 r \ : \ r \in R\}$$

is an ideal. [These ideals are called principal ideals]

Exercise 1.89. *Let R be a commutative ring and let $\mathfrak{a}$ be an ideal in R.*

(i) Prove that

$$\{r \in R \ : \ ra = 0 \text{ for all } a \in \mathfrak{a}\}$$

is an ideal.

(ii) Let M be an R–module and set

$$\text{Ann}(M) = \{r \in R \ : \ rm = 0 \text{ for all } m \in M\}.$$

Prove that $\text{Ann}(M)$ is an ideal in R.

1.5 *Isomorphism Theorems*

One of the foundational results in algebraic structures is called the Isomorphism Theorems. This suite of results relates the study of group/ring homomorphisms with the study of the normal subgroups/ideals. Our focus will be with these results for groups, where we will give detail proofs of these theorems. In the setting of rings, as the proofs of logically identical, we will merely state the results and trust that the motivated reader can work them out in private.

1.5.1 Isomorphism Theorem: Groups

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

Theorem 1.7 (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 $g' = gg_1$. In particular,

$$\psi(g') = \psi(gg_1) = \psi(g)\psi(g_1) = \psi(g)1_H = \psi(g).$$

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

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

To that end, we have

$$\begin{aligned}\overline{\psi}(g_1\ker\psi g_2\ker\psi) &= \overline{\psi}((g_1g_2)\ker\psi) = \psi(g_1g_2)\\ &= \psi(g_1)\psi(g_2) = \overline{\psi}(g_1\ker\psi)\overline{\psi}(g_2\ker\psi).\end{aligned}$$

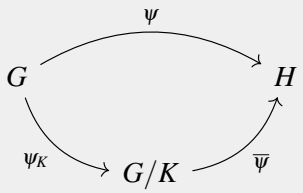
For (3), to show that $\overline{\psi}$ is injective, we must prove that for any $g_1\ker\psi, g_2\ker\psi \in G/\ker\psi$ with $g_1\ker\psi \neq g_2\ker\psi$, we have $\overline{\psi}(g_1\ker\psi) \neq \overline{\psi}(g_2\ker\psi)$. By Exercise 1.66 (i) and (ii), we know that $g_1g_2^{-1} \notin \ker\psi$. By definition of $\ker\psi$, we must have $\psi(g_1g_2^{-1}) \neq e_H$ 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 1.8. *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 1.9 (Second Isomorphism Theorem)**.** *Let G be a group, $K \leq G$, and $H \lhd G$. Then*

(a) The set

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

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 $h_1k_1, h_2k_2 \in HK$, we see that

$$h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}.$$

Since H is normal, we know that $(k_1k_2^{-1})H = H(k_1k_2^{-1})$. Hence, there exists $h_3 \in H$ such that $k_1k_2^{-1}h_2 = h_3k_1k_2^{-1}$. Therefore,

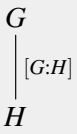
$$h_1k_1k_2^{-1}h_2^{-1} = h_1h_3k_1k_2^{-1}.$$

Since H, K are subgroups, $h_1h_3 \in H$ and $k_1k_2^{-1} \in K$. In particular, $h_1h_3k_1k_2^{-1} \in HK$ and so $h_1k_1(h_2k_2)^{-1} \in HK$. It now follows that HK is a subgroup by Exercise 1.21.

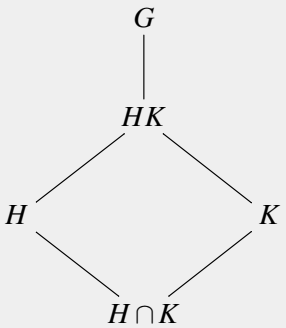
For (b), by Exercise 1.21 (-i), we know that $H \cap K$ is a subgroup of G and so we need only verify that it is normal. For that, given $h \in H \cap K$ and $k \in K$, we must prove that $k^{-1}hk \in H \cap K$. Since H is normal in G and $h \in H$, it follows that $k^{-1}hk \in H$. Since K is a subgroup of G and $h, k \in K$, it follows that $k^{-1}hk \in K$. Thus, $k^{-1}hk \in H \cap K$.

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 1.4, 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 1.7, 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 $k = h_1k_1$ for $h_1\in H$ and $k_1\in K$. Since H is normal, we know that $k_1H = Hk_1$ and so $h_1k_1 = k_1h_2$ for some $h_2\in H$. In particular, we see that $k = k_1h_2$ and so $kk_1^{-1}\in H$. Hence, $kH = k_1H$ by Exercise 1.66. By definition of ψ_H, we have $\psi_H(k_1) = k_1H = kH$. Therefore, $\psi_H(K) = HK/H$ and so $K/(H\cap K)$ and HK/H are isomorphic. ♠

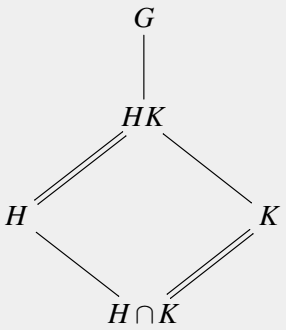
When $H\leq G$, it is common to associate to G,H a diagram



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



By (c) in Theorem 1.9 the opposite sides of the diamond



are the "same". Theorem 1.9 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* 1.10** (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 $\psi_H : G \to G/H$ to K. The image $\psi_H(K) = K/H$ and by Lemma 1.4, $\psi_H(K) \leq G/H$.

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 1.21, we have $\ell_1 \ell_2^{-1} \in L$. Additionally, we have

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

Hence $g_1 g_2^{-1} \in \psi_H^{-1}(L)$ and so by Exercise 1.21, $\psi_H^{-1}(L)$ 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 $(gH)^{-1} kHgH \in K/H$. Since K is normal, we know that $g^{-1}kg = k_1 \in K$. As $\psi_H(k) = kH$ and $\psi_H(g) = gH$, we see that

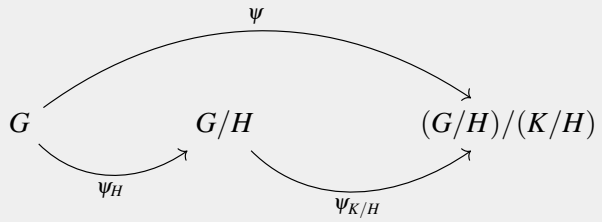
$$(gH)^{-1} kHgH = (\psi_H(g))^{-1} \psi_H(k) \psi_H(g) = \psi_H(g^{-1}kg) = \psi_H(k_1) \in K/H.$$

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 $g^{-1} g_0 g \in \psi_H^{-1}(L)$. 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

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

since L is normal. Hence, $g^{-1}g_0g \in \psi_H^{-1}(L)$. 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 1.7, 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 $(\cdot, 1_G)$. Specifically, if G is a group and $g_1, g_2 \in G$, we will write $g_1 \cdot g_2 = g_1g_2$.

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 1.10 asserts that

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

Exercise 1.90. *Let* $\mathbf{C}$ *be the complex numbers and* $\mathbf{R}$ *the real numbers. We view both as groups under addition. Prove that* $\mathbf{C}/\mathbf{R} \cong \mathbf{R}$.

Exercise 1.91. *Let* G_1, G_2 *be finite groups with* $|G_1| = |G_2|$ *and let* $\psi\colon G_1 \to G_2$ *be a group homomorphism. Prove the following are equivalent:*

(i) ψ *is a bijection.*

(ii) ψ *is injective.*

(iii) ψ *is surjective.*

Exercise 1.92. *Prove that every surjective homomorphism* $\psi\colon \mathbf{Z} \to \mathbf{Z}$ *is injective.*

Exercise 1.93. *Prove that every surjective homomorphism* $\psi\colon \mathbf{Z}^n \to \mathbf{Z}^n$ *is injective.*

Exercise 1.94. *Find a group* G *and a surjective homomorphism* $\psi\colon G \to G$ *that is not injective.*

Exercise 1.95. *Find a group such that* $G \cong G \times G$*? Explain why* G *must be infinite.*

1.5.2 Isomorphism Theorem: Rings

Theorem 1.11 (First Isomorphism Theorem)**.** *Let R, R' be commutative rings 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 1.12 (Second Isomorphism Theorem)**.** *Let R be a commutative ring, $S \leq R$ a subring, 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 1.13 (Third Isomorphism Theorem)**.** *Let R be a commutative ring 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 1.11, Theorem 1.12, and Theorem 1.13 are quite similar to the proofs of Theorem 1.7, Theorem 1.9, and Theorem 1.10, we have omitted them from the notes.

Exercise 1.96. *Let R be a ring and let $\psi_R\colon \mathbf{Z} \to R$ be given as in Exercise 1.54.*

(i) Prove that $\ker\psi_R = n_R\mathbf{Z}$ for some $n_R \in \mathbf{N}$.

(ii) Prove that $\psi_R(\mathbf{Z})$ is isomorphic to $\mathbf{Z}/n_R\mathbf{Z}$. [We call n_R the characteristic on R].

1.6 *Commutative Diagrams*

blah

1.6.1 Exact Sequences

1.6.2 Commutative Diagrams

1.6.3 Chain and Cochain Complexes

Chapter 2

Group Actions

Contents

In this chapter we begin to focus our views and start with the theory of group actions on sets.

2.1 *Basics*

***Definition* 2.1** (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* 2.1.** *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 bijective function $\lambda : X\to X$.*

(i) Prove that $\mathrm{Aut}_{\mathrm{set}}(X)$ *is a group where the identity element is given by the function* $\mathrm{Id}_X : X \to X$ *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* $\varphi_g : X \to X$ *by* $\varphi_g(x) = \varphi(g,x)$*. Prove that* $\varphi_g \in \mathrm{Aut}_{\mathrm{set}}(X)$*.*

(iii) Define the function $\Phi : G \to \mathrm{Aut}_{\mathrm{set}}(X)$ *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 2.2. *Prove that if* X *is finite, then* $|\mathrm{Aut}_{set}(X)| = |\mathrm{Sym}(X)| = |X|!$.

Exercise 2.3. *Prove that if* $\Phi : G \to \mathrm{Sym}(X)$ *is a homomorphism, then the function* $\varphi : G \times X \to X$ *given by* $\varphi(g,x) = \Phi(g)(x)$ *is a group action of* G *on* X*.*

In summary, Exercise 2.1 and Exercise 2.3 show that a group action of G on X is equivalent to a homomorphism $\Phi : G \to \mathrm{Sym}(X)$. Consequently, when we have a group action $\varphi : G \times X \to X$, 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 2.1 (Symmetry Groups of Sets)**.** *Given a set* X*, the group* $\mathrm{Sym}(X)$ *of bijective functions* $\lambda : X \to X$ *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 2.1; 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 2.1. *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 2.1 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 2.2 (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*

$$(g \cdot f)(x) = f(g^{-1} \cdot x) \tag{2.1}$$

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 **2.2.** *For additional clarity, we discuss further why we must define the contragradient action as we did. If we replace (2.1) with*

$$(g \cdot f)(x) = f(g \cdot x), \tag{2.2}$$

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, (2.2) does not in general satisfy (b) in Definition 2.1.*

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 (2.1).

Remark **2.3.** *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 **2.4.** *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 **2.2** (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 $\mathrm{Sym}(X)$ 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 $\sigma \in \mathrm{Sym}(X)$ such that $\sigma(S_1) = S_2$. One the other hand, if we take the subgroup of $\mathrm{Sym}(X)$ of all elements that fix $x_0 \in X$ (i.e. $\sigma(x_0) = x_0$), this subgroup of $\mathrm{Sym}(X)$ does not act transitively on X; it does act transitively on $X - \{x_0\}$.

Exercise 2.5. *Prove that if $S_1, S_2 \subset X$ and $|S_1| = |S_2|$, then there exists $\sigma \in \mathrm{Sym}(X)$ 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 2.3 (Affine Group)**.** *The group $\mathrm{Aff}(\mathbf{R}^n) \stackrel{def}{=} \mathbf{R}^n \rtimes \mathrm{GL}(n,\mathbf{R})$ is called the **n–dimensional affine group**. It consists of pairs (v,A) where $v \in \mathbf{R}^n$ and $A \in \mathrm{GL}(n,\mathbf{R})$; the group $\mathrm{GL}(n,\mathbf{R})$ is comprised of the n by n matrices of non-zero determinant. Being a semi-direct product (see Remark 2.6 below for more on semi-direct products), the group operation on $\mathbf{R}^n \rtimes \mathrm{GL}(n,\mathbf{R})$ is defined by*

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

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

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

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

Exercise 2.6. *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 2.3 (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 2.4. *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 2.4 as an exercise.

Exercise **2.7.** *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 2.4.*

As a consequence of Lemma 2.4, 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 **2.8.** *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

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

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

Exercise **2.9.** *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 **2.4** (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 2.10. *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 2.11. *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 2.5 (Orbit-Stabilizer Theorem)**.** *Let G be a group, X a set with a G–action, and $x \in X$.*

(a) For each $x_1, x_2 \in \mathscr{O}_x$, 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 $\lambda\colon G/\mathrm{Stab}_G(x) \to \mathscr{O}_x$.

(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 $x_1, x_2 \in \mathscr{O}_x$, 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

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

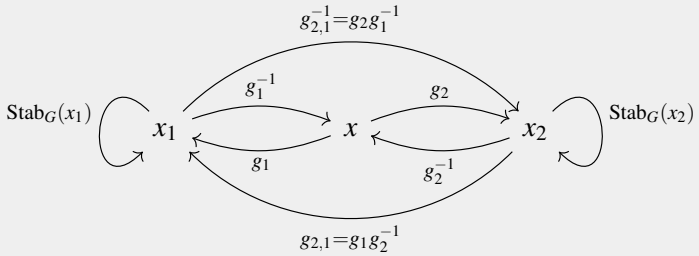
Hence, $g \in \mathrm{Stab}_G(x_2)$. Given $g \in \mathrm{Stab}_G(x_2)$, it follows that

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

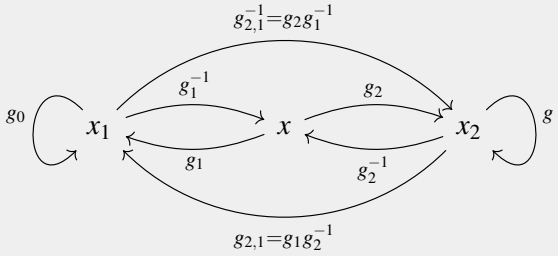
We assert that $g_{2,1} g g_{2,1}^{-1} \in \mathrm{Stab}_G(x_1)$. To see this, we have

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

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



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 $\lambda(g \operatorname{Stab}_G(x)) = g \cdot x$. To show that λ is well defined, we must show that if $g' \in g \operatorname{Stab}_G(x)$, then $g' \cdot x = g \cdot x$. By definition, $g' = g g_0$ where $g_0 \in \operatorname{Stab}_G(x)$. 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 $\lambda(g \operatorname{Stab}_G(x)) = \lambda(g' \operatorname{Stab}_G(x))$, we must show that $g \operatorname{Stab}_G(x) = g' \operatorname{Stab}_G(x)$. By definition, we have

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

In particular, $g' g^{-1} \cdot x = x$ and so $g' g^{-1} \in \operatorname{Stab}_G(x)$. Hence $g \operatorname{Stab}_G(x) = g' \operatorname{Stab}_G(x)$ by Exercise 1.66. For surjectivity, given $x' \in \mathcal{O}_x$, we must find $g \operatorname{Stab}_G(x) \in G/\operatorname{Stab}_G(x)$ such that $\lambda(g \operatorname{Stab}_G(x)) = x'$. Since $x' \in \mathcal{O}_x$, there exists $g \in G$ such that $g \cdot x = x'$. By definition of λ, we see that $\lambda(g \operatorname{Stab}_G(x)) = x'$.

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

Exercise 2.12. *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 $H \leq \operatorname{Sym}(X)$ acts freely and transitively on the set X. Prove that H is a cyclic group and $|H| = |X|$. Deduce that $\operatorname{Sym}(X)$ is not cyclic provided $|X| \geq 3$.

Exercise 2.13. *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 $\mathcal{O}_x$.

(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

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

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

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

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

Given sets X, Y, each with a G–action, we say that a function $f : X \to Y$ 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 $G/\operatorname{Stab}_G(x) \to \mathcal{O}_x$ is a G–equivariant map.

2.2 *Fundamental Examples*

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 $\operatorname{Aut}_{\text{set}}(X)$. 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 $\operatorname{Aut}_{\text{group}}(G)$ for the group of bijective group homomorphisms $\lambda : G \to G$. However, we will instead write simply $\operatorname{Aut}(G)$; 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 2.4 (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 2.1,* $\mathrm{Aut}(G)$ *acts on G.*

Remark 2.6. *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 $\Phi : H \to \mathrm{Aut}(G)$, 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 2.14. *Prove that $G \rtimes_\Phi H$ is a group.*

Exercise 2.15. *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 2.5 (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 **2.16.** *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 **2.6** (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*:*

$$|G| = \sum_{i=1}^{r_G} \frac{|G|}{|C_G(g_i)|} \tag{2.3}$$

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* (2.3)*, we obtain the following alternative form for the class equation:*

$$\sum_{i=1}^{r_G} \frac{1}{|C_G(g_i)|} = 1. \tag{2.4}$$

By Exercise 1.67 (ii), we can also rewrite (2.3) *as follows:*

$$|G| = \sum_{i=1}^{r_G} [G : C_G(g_i)]. \tag{2.5}$$

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

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{r_G} [G : C_G(g_i)]. \tag{2.6}$$

Each of the equations (2.3), (2.4), (2.5), or (2.6) 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 2.17. *Prove that the conjugate action of G on G is free if and only if G is the trivial group.*

Exercise 2.18. *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 $\mathrm{Aut}(G)/\mathrm{Ad}_G(G) \stackrel{def}{=} \mathrm{Out}(G)$ is called the group of outer automorphisms.*

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

Example 2.7 (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*

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

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 2.5), 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 $\Phi_H \colon G \to \mathrm{Sym}(G/H)$ 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 2.7. *The bijective function given in Theorem 2.5 (ii) is G–equivariant where G acts on* $G/\operatorname{Stab}_G(x)$ *as in Example 2.7.*

Exercise 2.19. *Let G be a group and* $H \leq G$.

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

(ii) Prove that if $H_0 \lhd G$ *and* $H_0 \subseteq H$, *then* $H_0 \subseteq \operatorname{Core}_G(H)$. *In particular,* $\operatorname{Core}_G(H)$ *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 2.8 (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* $\operatorname{Ad}_G(g)(H) = H$ *and so we obtain* $\operatorname{Ad}_{G,H} \colon G \to \operatorname{Aut}(H)$ *given by*

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

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

Exercise 2.20. *Let G be a group and* $H \leq G$.

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

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

Chapter 3

Group Theory

Contents

3.1 *Groups by Size and Universal Examples*

3.1.1 Finite, Countable, and Otherwise

3.1.2 Free Vector Spaces on Sets

3.1.3 Free Groups on Sets

Given a set X, the **free group on the set X** is the unique group (up to isomorphism) $F(X)$ with $X \subset F(X)$ and satisfying the following universal mapping property: if $f\colon X \to G$ is any function where G is a group, then there exists a unique homomorphism $\varphi_f\colon F(X) \to G$ such that the restriction of φ_f to X is f. The existence of such a group can be done constructively in the same spirit as the construction of a vector space or free commutative group associated to a set. We briefly outline the approach.

We start by forming a set $\mathscr{A} = \{x\}_{x\in X} \cup \left\{x^{-1}\right\}_{x\in X}$ that we will call an **alphabet**. A **word** in the alphabet $\mathscr{A}$ is a finite ordered subset $w \subset \mathscr{A}$. By definition, $w = \left\{x_1^{\varepsilon_1}, \ldots, x_m^{\varepsilon_m}\right\}$ where $x_i \in X$ and $\varepsilon_i = \pm 1$. We can combine words $w_1 = \left\{x_1^{\varepsilon_1}, \ldots, x_m^{\varepsilon_m}\right\}$ and $w_2 = \left\{y_1^{\varepsilon_1'}, \ldots, y_n^{\varepsilon_n'}\right\}$ to form a new word $w_1 w_2 \subset \mathscr{A}$ given by

$$w_1 w_2 = \left\{x_1^{\varepsilon_1}, \ldots, x_m^{\varepsilon_m}, y_1^{\varepsilon_1'}, \ldots, y_n^{\varepsilon_n'}\right\}.$$

We say that a word $w = \left\{x_i^{\varepsilon_i}\right\}_{i=1}^m$ is **reducible** if there exists an index $i \in \{1, \ldots, n-1\}$ such that $x_i = x_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$, and we say w is **irreducible** otherwise. Given a reducible word $w \subset \mathscr{A}$ with $i \in \{1, \ldots, n-1\}$ such that $x_i = x_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$, we can perform a reduction operation on w. Formally, we define a new word

$$\mathrm{R}_i(w) = \left\{x_1^{\varepsilon_1}, \ldots, x_{i-1}^{\varepsilon_{i-1}}, x_{i+2}^{\varepsilon_{i+2}}, \ldots, x_n^{\varepsilon_n}\right\}.$$

After applying finitely many reduction operations $R_{i_1}, \ldots, R_{i_m}$ on the reducible word w, we obtain a unique irreducible word w_{irr}. We define $\mathscr{W}_X$ to be the set of irreducible words in the alphabet $\mathscr{A}$. We have a binary operation $*\colon \mathscr{W}_X \times \mathscr{W}_X \to \mathscr{W}_X$ given by $w_1 * w_2 = (w_1 w_2)_{irr}$. We also have an involution $\iota\colon \mathscr{W}_X \to \mathscr{W}_X$ given by

$$\iota(w) = \iota\left(\left\{x_i^{\varepsilon_i}\right\}_{i=1}^n\right) = \left\{x_{n-i+1}^{-\varepsilon_{n-i+1}}\right\}_{i=1}^n.$$

Setting $1_{\mathscr{W}_X} = \emptyset$, we see that $(\mathscr{W}_X, *, \iota, 1_{\mathscr{W}_X})$ is a group with multiplication operation $*$, inverse operation ι, and identity $1_{\mathscr{W}_X}$. Given any group G and any function $f\colon X \to G$, we define $\varphi_f\colon \mathscr{W}_X \to G$ by

$$\varphi_f(w) = \prod_{i=1}^n f(x_i)^{\varepsilon_i}, \quad w = \left\{x_i^{\varepsilon_i}\right\}_{i=1}^n.$$

It is straightforward to check that φ_f is a homomorphism with $f(x) = \varphi_f(x)$ for all $x \in X$.

Exercise 3.1. *Prove that φ_f is unique.*

Exercise 3.2. *Prove $F(X) \cong F(Y)$ if and only if there exists a bijective function $X \to Y$.*

Lemma 3.1. *If Γ is a group, then there exists a free group F and a surjective homomorphism $F \to \Gamma$.*

Proof. Take $X = \Gamma$, $F = F(X)$, $f\colon X \to \Gamma$ to be the identity, and apply the universal mapping property. ♠

Exercise 3.3. *Let G be a group, let F_r be a free group on the set $\{x_1, \ldots, x_r\}$, and let $\mathrm{Hom}(F_r, G)$ denote the set of group homomorphisms $\psi\colon F_r \to G$.*

(i) Given $(g_1, \ldots, g_r) \in G^r$, prove that there exists a unique group homomorphisms $\psi_{(g_1,\ldots,g_r)}\colon F_r \to G$ such that $\psi_{(g_1,\ldots,g_r)}(x_i) = g_i$ for $i = 1, \ldots, n$.

(ii) For each $i \in \{1, \ldots, r\}$, define $\mathrm{Eval}_i\colon \mathrm{Hom}(F_r, G) \to G$ by $\mathrm{Eval}_i(\psi) = \psi(x_i)$ and define $\mathrm{Eval}\colon \mathrm{Hom}(F_r, G) \to G^r$ by

$$\mathrm{Eval}(\psi) \stackrel{def}{=} (\mathrm{Eval}_1(\psi), \ldots, \mathrm{Eval}_r(\psi)).$$

Prove that Eval *is a bijection.*

(iii) Define a binary operation $*\colon \mathrm{Hom}(F_r, G) \times \mathrm{Hom}(F_r, G) \to \mathrm{Hom}(F_r, G)$ by

$$\rho_1 * \rho_2 \stackrel{def}{=} \mathrm{Eval}^{-1}(\mathrm{Eval}(\rho_1)\,\mathrm{Eval}(\rho_2))$$

where $\mathrm{Eval}(\rho_1)\,\mathrm{Eval}(\rho_2)$ denotes the product of $\mathrm{Eval}(\rho_1)$ and $\mathrm{Eval}(\rho_2)$ via the group structure on G^r. Prove that $\mathrm{Hom}(F_r, G)$ is a group with this binary operation and with identity ρ_0 where $\rho_0(x) = 1_G$ for all $x \in F_r$.

(iv) Prove that the function Eval$\colon \mathrm{Hom}(\mathbf{Z}, G) \to G$ *is an isomorphism of groups where $\mathrm{Hom}(\mathbf{Z}, G)$ is given the group structure from (c).*

3.1.4 Products and Induced Algebraic Structures

3.2 *Generating Sets and Presentations*

3.2.1 Generating Sets

3.2.2 Presentations

3.2.3 Finite Generation and Finitely Presented Groups

3.2.4 Tietze Transformations

3.2.5 Decision Problems

3.3 *Finite Groups*

blah

3.3.1 Part 1: The Standard Examples

blah

Exercise 3.4. *Let G be a finite group and let H be a proper subgroup. Prove that*

$$G \neq \bigcup_{g \in G} g^{-1} H g.$$

3.3.2 Part 2: The Sylow Theorems

blah

3.3.3 Part 3: Simple Groups

blah

3.4 *Finitely Generated Commutative Groups*

blah

3.5 *Infinite Groups*

blah

3.5.1 Part 1: Matrix Groups

blah

3.5.2 Part 2

blah

Exercise 3.5. *Let G be a group and let H be a finite index subgroup. Prove that there exists a finite index, normal subgroup $N \lhd G$ with $N \subseteq H$.*

Exercise 3.6. *Let G be a group.*

(i) Let $H_1, H_2 \leq G$ be finite index subgroups. Prove that if $[G : H_1]$ and $[G : H_2]$ are relatively prime, then $G = H_1H_2$.

(ii) Let $H \leq G$ be finite index and let $N \lhd G$ be a finite, normal subgroup. Prove that if $[G : H]$ and $|N|$ are relatively prime, then $N \subseteq H$.

Chapter 4

Ring Theory

Contents

4.1 *Basics*

4.2 *Ideals*

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 **4.1** (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 **4.2** (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* 4.3** (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* 4.4** (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* 4.1** (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* 4.2.** *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* 4.1.** *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 4.1, $R/\mathfrak{a}$ 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 4.1, 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* 4.2.** *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 1.79)

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

Definition **4.5** (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 **4.3.** *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 **4.3.** *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

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

Exercise 4.4. *Let R be a commutative ring. Prove that an ideal $\mathfrak{p}$ of R is prime if and only if $R-\mathfrak{p}$ is closed under multiplication.*

Exercise 4.5. *Let R be a commutative ring. Prove that an ideal $\mathfrak{p}$ of R is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain. Deduce that maximal ideals are prime ideals.*

Exercise 4.6. *Let X be a set and for each $x \in X$, let*

$$\mathfrak{m}_x \stackrel{def}{=} \{f \in \mathrm{Fun}(X,\mathbf{R}) \ : \ f(x) = 0\}.$$

(i) Prove that $\mathfrak{m}_x$ is a maximal ideal in $\mathrm{Fun}(X,\mathbf{R})$. [Hint: Exercise 1.87]

(ii) Prove that $\mathrm{Fun}(X,\mathbf{R})/\mathfrak{m}_x \cong \mathbf{R}$.

(iii) Prove that if $\mathfrak{a}$ is a proper ideal in $\mathrm{Fun}(X,\mathbf{R})$, then there exists $x_0 \in X$ such that $f(x_0) = 0$ for all $f \in \mathfrak{a}$.

Exercise 4.7. *Prove that if R is an integral domain with $|R| < \infty$, then R is a field.*

Exercise 4.8. *Prove that if R is a commutative ring, then the following are equivalent:*

(i) R is a field.

(ii) Given any ring homomorphism $\psi\colon R \to R'$, either $\ker\psi = R$ or $\ker\psi = \{0_R\}$.

(iii) R and $\{0\}$ are the only ideals in R.

Exercise 4.9. *Let D be an integral domain and $R \leq D$ a subring. Prove that R is an integral domain.*

Exercise 4.10. *Let R be an integral domain with finite characteristic $\mathrm{char}(R)$. Prove that $\mathrm{char}(R)$ is a prime number. [Hint: Exercise 4.9]*

Exercise 4.11. *Let R be a ring such that for each $r \in R$, we have $r^2 = r$. Prove that R is commutative.*

Exercise 4.12. *Let R be a ring and assume that $r_1, r_2 \in R$ such that $1 - r_1 r_2$ is unit in R. Prove that $1 - r_2 r_1$ is a unit.*

Exercise 4.13. *Let R be a ring such that for $r_1, r_2 \in R$, we have that r_1, r_2, and $r_1 r_2 - 1$ are units. Prove that $r_1 - r_2^{-1}$ and $(r_1 - r_2^{-1})^{-1} - r_1^{-1}$ are units and that*

$$((r_1 - r_2^{-1})^{-1} - r_1^{-1})^{-1} = r_1 r_2 r_1 - r_1.$$

Exercise 4.14. *Let R be a commutative ring. We say that $r \in R$ is **nilpotent** if $r^n = 0$ from some $n \in \mathbf{N}$. Prove that the set of nilpotent elements in R is an ideal.*

Exercise 4.15. *Determine all of the maximal ideals of* $\mathbf{R} \times \mathbf{R}$.

Exercise 4.16. *Let R be a commutative ring and let $r \in R$ be nilpotent. Prove that $1 + r$ is a unit.*

Exercise 4.17. *Let R be a commutative ring, let $r \in R$ be nilpotent, and let $s \in R$ be a unit. Prove that $s + r$ is a unit.*

Exercise 4.18. *Let R be a commutative ring and define $\mathrm{Hom}_{add}(R,R)$ be the set of group homomorphisms $(R,+) \to (R,+)$ where R is viewed as a group with addition. Prove that $\mathrm{Hom}_{add}(R,R)$ is a ring under pointwise addition and composition of functions. Prove that the group of units of $\mathrm{Hom}_{add}(R,R)$ is $\mathrm{Aut}(R,+)$, the group of automorphisms of R as an additive group.*

Exercise 4.19. *Let R be a commutative ring and $\mathfrak{a}, \mathfrak{b} \lhd R$ be ideals. Prove that $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.*

Exercise 4.20. *Let R be a commutative ring and $\mathfrak{a}, \mathfrak{b} \lhd R$ be ideals such that $\mathfrak{a} + \mathfrak{b} = R$. Prove that $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.*

Exercise 4.21. *Let R be a commutative ring with $\mathrm{char}(R) = p$ where p is prime. Prove that $(r_1 + r_2)^p = r_1^p + r_2^p$ for any $r_1, r_2 \in R$.*

Exercise 4.22. *Let R be an integral domain with $r_1, r_2 \in R$. Prove that $\langle r_1 \rangle = \langle r_2 \rangle$ if and only if there exists a unit $r \in R$ with $rr_1 = r_2$.*

Exercise 4.23. *Let R be a commutative ring with ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{p}$. Prove that if $\mathfrak{p}$ is prime and $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, then $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.*

Exercise 4.24. *Let R be a finite, commutative ring and let $\mathfrak{p}$ be a prime ideal in R. Prove that $\mathfrak{p}$ is maximal. [Hint: Exercise 4.7]*

Exercise 4.25. *Let R be a commutative ring and let $\mathfrak{a}$ be an ideal in R. Define*

$$\mathrm{Rad}(\mathfrak{a}) \stackrel{def}{=} \{r \in R \ : \ r^n \in \mathfrak{a} \text{ for some } n \in \mathbf{N}\}.$$

Prove that $\mathrm{Rad}(\mathfrak{a})$ is an ideal and $\mathfrak{a} \subseteq \mathrm{Rad}(\mathfrak{a})$.

Exercise 4.26. *Let R be a commutative ring and let $\mathfrak{p}$ be a prime ideal. Prove that $\mathrm{Rad}(\mathfrak{p}) = \mathfrak{p}$.*

Exercise 4.27. *Let R be a commutative ring and let $\mathscr{M}_R$ be the collection of maximal ideals in R. Given an ideal $\mathfrak{a} \lhd R$, we define*

$$\mathrm{Jac}(\mathfrak{a}) \stackrel{def}{=} \bigcap_{\substack{\mathfrak{m} \in \mathscr{M}_R, \\ \mathfrak{a} \subseteq \mathfrak{m}}} \mathfrak{m}.$$

Prove that $\mathrm{Jac}(\mathfrak{a})$ is an ideal and $\mathrm{Rad}(\mathfrak{a}) \subseteq \mathrm{Jac}(\mathfrak{a})$.

Exercise 4.28. *Let R be a commutative ring and let $\mathfrak{a} = \langle S \rangle$ where $S \subseteq R$ is finite. Prove that there is an ideal $\mathfrak{b}$ in R is is maximal with respect to not containing $\mathfrak{a}$.*

Exercise 4.29. *Let R be a commutative ring. We say that an ideal $\mathfrak{a}$ of R is **primary** if whenever $r_1 r_2 \in \mathfrak{a}$ with $r_1 \notin \mathfrak{a}$, then $r_2^n \in \mathfrak{a}$ for some $n \in \mathbf{N}$. Prove that $\mathrm{Rad}(\mathfrak{a})$ is a prime ideal when $\mathfrak{a}$ is primary.*

Exercise 4.30. *Let R be a commutative ring. We say that R is a **local ring** if R has a unique maximal ideal $\mathfrak{m}$. Prove that every $r \in R - \mathfrak{m}$ is a unit.*

Exercise 4.31. *Let R be a commutative ring such that the set of non-unit elements $\mathfrak{m}$ of R is an ideal. Prove that R is a local ring with unique maximal ideal $\mathfrak{m}$.*

Exercise 4.32. *Let R be a commutative ring and let $\mathscr{P}_R$ denote the set of all prime ideals in R. Prove that if $\mathfrak{a} \lhd R$, then*

$$\mathrm{Rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{p} \in \mathscr{P}_R, \\ \mathfrak{a} \subseteq \mathfrak{p}}} \mathfrak{p}.$$

Deduce that $\mathrm{Rad}(\mathfrak{a}) \subseteq \mathrm{Jac}(\mathfrak{a})$; see Exercise 4.27.

Exercise 4.33. *Let R be a commutative ring. Prove that*

$$\mathrm{nil}(R) \stackrel{def}{=} \bigcap_{\mathfrak{p} \in \mathscr{P}_R} \mathfrak{p}$$

is the set of all nilpotent elements in R.

We say that a commutative ring R is **reduced** if R has no non-trivial nilpotent elements.

Exercise 4.34. *Let R be a commutative ring and let $\psi\colon R \to R'$ be a ring homomorphism with R' reduced.*

(i) Prove that $R/\mathrm{nil}(R)$ is reduced.

(ii) If ψ_R is the canonical homomorphism $\psi_R\colon R \to R/\mathrm{nil}(R)$, prove that there exists a unique ring homomorphism $\tau\colon R/\mathrm{nil}(R) \to R'$ such that $\psi = \tau \circ \psi_R$.

4.3 *Finiteness Conditions: Artinian and Noetherian Rings*

4.4 *The Spectrum of a Ring*

Chapter 5

Polynomial Rings

Contents

5.1 *Division Algorithm and Euclidean Algorithm*

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

$$\begin{aligned} P_1 - Q_1 P_2 &= a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 - a_n t^n - \frac{a_n}{b_m} b_{m-1} t^{n-1} - \cdots + \frac{a_n}{b_m} b_1 t^{n-m+1} - \frac{a_n}{b_m} b_0 t^{n-m} \\ &= \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) t^{n-1} + \cdots + \left(a_{n-m+1} - \frac{a_n}{b_m} b_1\right) t^{n-m+1} \\ &\quad + \left(a_{n-m} - \frac{a_n}{b_m} b_0\right) t^{n-m} + a_{n-m-1} t^{n-m-1} + \cdots + a_1 t + a_0 \end{aligned}$$

We replace P_1 with $P_{1,1} = P_1 - Q_1 P_2$, 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* 5.1** (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* 5.1.** *Prove that $Q, R \in F[t]$ in Theorem 5.1 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 5.1 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* 5.2.** *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 5.3. *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 5.4. *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 5.1, 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

$$P_2 = 0_R P_1 + 1_R P_2.$$

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 5.1, 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

$$R_1 = P_1 - Q_1P_2$$

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 6.3, 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 $P_2 = Q_2R_1$, we see that

$$P_1 = R_1 + Q_2Q_1R_1 = R_1(1 + Q_2Q_1).$$

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 5.1, 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 6.3, $\deg(P_2) > \deg(Q_2) = \deg(1_F - Q_2)$. 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

$$R_i = R_{i-2} - Q_i R_{i-1} \tag{5.1}$$

for $i \geq 3$ and

$$R_1 = P_1 - Q_1 P_2, \quad R_2 = P_2 - Q_2 R_1. \tag{5.2}$$

Using (5.1) (many times) and (5.2), we obtain

$$\begin{aligned}
R_{n-1} &= R_{n-3} - Q_{n-1} R_{n-2} \\
&= R_{n-5} - Q_{n-3} R_{n-4} - Q_{n-1}(R_{n-4} - Q_{n-2} R_{n-3}) \\
&= R_{n-7} - Q_{n-5} Q_{n-6} - Q_{n-2}(R_{n-6} - Q_{n-4} R_{n-5}) - Q_{n-1}(R_{n-6} - Q_{n-4} R_{n-5}) - Q_{n-2}(R_{n-5} - Q_{n-3} R_{n-4}) \\
&\quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
&= H_1 P_1 + H_2 P_2.
\end{aligned}$$

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 (5.2).

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 5.1, 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

$$\deg(\gcd(P_1, P_2)) \geq \deg(P_1) + \deg(P_2) + \deg(Q). \tag{5.3}$$

Since $\gcd(P_1, P_2)$ divides both P_1, P_2, we know that

$$\deg(\gcd(P_1, P_2)) \leq \min\{\deg(P_1), \deg(P_2)\}. \tag{5.4}$$

In particular, (5.3) contradicts (5.4) 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 (5.3) holds. As before, (5.3) contradicts (5.4) 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 5.2. *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 5.5 below, is unique under this additional condition.*

Exercise 5.5. *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 5.6. *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 5.7. *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* $\psi_{s,t} : \mathbf{Z}/t\mathbf{Z} \to \mathbf{Z}/s\mathbf{Z}$*. [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*

$$\psi : \mathbf{Z}/s\mathbf{Z} \to \prod_{i=1}^{n} \mathbf{Z}/s_i\mathbf{Z}$$

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* $\psi_{s,s_i} : \mathbf{Z}/s\mathbf{Z} \to \mathbf{Z}/s_i\mathbf{Z}$*.]*

(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 5.8. *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****.*

5.2 Ideals

Definition 5.1 (Principal Ideal Domain)**.** *We say that an integral domain* D *is a* ***principal ideal domain*** *if every proper, non-trivial ideal is principal.*

Lemma 5.3. *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 1.5. Given $P' \in \mathfrak{a}$, by Theorem 5.1, 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 5.9. *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 5.10. *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 5.11. *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 5.4. *If $\mathfrak{p}$ is a non-trivial, proper, prime ideal in $F[t]$, then $\mathfrak{p}$ is maximal.*

Proof. By Lemma **??**, it is enough to show that $F[t]/\mathfrak{p}$ is a field. By Lemma 4.2, 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 5.3, 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 6.3, 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 5.1, we can assume that $\deg(P_1) < \deg(P)$. To see this claim, note that if $\deg(P_1) \geq \deg(P)$, by Theorem 5.1, 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 $H_1P + H_2P_1 = 1_F$. Finally, we see that

$$\psi_{\mathfrak{p}}(H_1P + H_2P_1) = \psi_{\mathfrak{p}}(H_1P) + \psi_{\mathfrak{p}}(H_2P_1) = \psi_{\mathfrak{p}}(H_2P_1) = 1.$$

♠

Chapter 6

Fields

Contents

6.1 *Basics*

Definition 6.1 (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 6.2 (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 6.1. *Let E/F be an extension of fields. Prove that E is an F–vector space.*

Definition 6.3 (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 6.1. *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 6.2. *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 6.1 and Example 6.2, 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 $B_n = \{\beta^i\}_{i=0}^n$. 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 **6.4** (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

$$\sum_{i=0}^{n_\beta} \alpha_i \beta^i = 0. \tag{6.1}$$

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 (6.1) by $\alpha_{n_\beta}^{-1}$. Consequently, we can assume that $\alpha_{n_\beta} = 1_F$ in (6.1). 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 **6.2.** *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 **6.3.** *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 **6.1.** *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 6.4. *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 6.1

Corollary 6.2. *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 6.3. *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

$$0 = \sum_{k=1}^{r} \tau_k \alpha_{i_k} \beta_{j_k} \tag{6.2}$$

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 (6.2) as

$$0 = \sum_{j=1}^{s} \left(\sum_{i=1}^{r_j} \tau_{i,j} \alpha_{i,j} \right) \beta_j. \tag{6.3}$$

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 $\left\{\alpha_i\beta_j\right\}_{(i,j)\in\times I\times J}$ is F–linearly independent. ♠

***Scholium* 6.4.** *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* 6.5** (Algebraic Extension)**.** *We say that an extension of fields E/F is **algebraic** if each $\beta \in E$ is algebraic over F.*

***Exercise* 6.5.** *Prove that if E/F is a finite extension, then E/F is algebraic.*

***Definition* 6.6** (Transcendental Extension)**.** *We say that an extension of fields E/F is **transcendental** if E/F is not algebraic.*

***Lemma* 6.5.** *If E/F is a transcendental extension if and only if there exists an F–algebraically independent element $\beta \in E$.*

***Exercise* 6.6.** *Prove Lemma 6.5.*

***Exercise* 6.7.** *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 6.7, $F(S)$ is a subfield of E. Moreover, $F(S)$ is non-empty since $F \leq E$ and $S \subseteq E$.

***Definition* 6.7** (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* 6.8** (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 6.9 (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 6.8. *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 6.9. *Prove that if E/F is a finitely generated extension, then the transcendence degree of E/F is finite.*

Exercise 6.10. *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 6.10 (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 6.11. *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 6.12. *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 6.13. *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 $[E_1E_2 : F] = \frac{[E_1:F][E_2:F]}{[E_1 \cap E_2:F]}$.

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

$$(r_1s_2 + r_2s_1, s_1s_2) \sim (rs'+r's, ss'), \quad (r_1r_2, s_1s_2) \sim (rr', ss').$$

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

$$r_1s = rs_1, \quad r_2s' = r's_2. \tag{6.4}$$

Using associativity, commutativity, the distributive law, and (6.4), 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

$$r_1r_2ss' = rr's_1s_2.$$

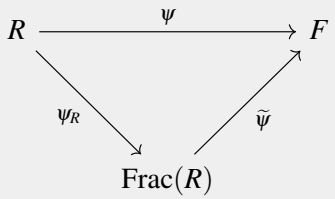
Using commutativity, the distributive law, and (6.4), we have

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

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

Exercise 6.14. *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



(6.5)

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

Exercise 6.15. *Prove that if $\psi\colon R \to F$ is an injective ring homomorphism, then there exists a unique, injective field homomorphism $\widetilde{\psi}\colon \operatorname{Frac}(R) \to F$ such that (6.5) 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 6.16. *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 6.17. *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*

$$\begin{array}{ccc} R & \xrightarrow{\psi} & R' \\ {\scriptstyle \psi_R}\downarrow & & \downarrow{\scriptstyle \psi_{R'}} \\ \operatorname{Frac}(R) & \xrightarrow[\widetilde{\psi}]{} & \operatorname{Frac}(R') \end{array} \tag{6.6}$$

commutes. [Hint: Exercise 6.15]

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 (6.6) commutes.

6.2 *Roots, Splitting Fields and Algebraic Closures*

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 5.3, $\mathfrak{a}$ is principal and so $\mathfrak{a} = \langle P \rangle$ for some $P \in F[t]$. According to Exercise **??**, $\mathfrak{a}$ 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 6.6). The factorization of P will provide us with a factorization of the ideal $\mathfrak{a}$ (see Corollary 6.7). 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 6.9). 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 6.14).

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

$$P = P_{0,1}P_{0,2} = (P_{1,1,1}P_{1,1,2})(P_{1,2,1}P_{1,2,2}) = \cdots = \prod_{i=0}^{r_P} P_i \tag{6.7}$$

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 (6.7) 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 **??**. 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 5.9, 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 6.6 (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 1.85 for the definition of the ideal $\mathfrak{a}_1\mathfrak{a}_2$ for ideals $\mathfrak{a}_1, \mathfrak{a}_2$.

Corollary 6.7. *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 6.18. *Prove Corollary 6.7. [Hint: Use the fact that $\mathfrak{a}$ is principal and apply Theorem 6.6 to the generating polynomial.]*

Exercise 6.19. *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 6.11 (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 6.8. *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 $\alpha, \alpha_1, \ldots, \alpha_{\deg(P)} \in E$ such that*

(a) $P(\alpha_i) = 0$ *for* $i = 1, \ldots, \deg(P)$.

(b)

$$P(t) = \alpha \prod_{i=1}^{\deg(P)} (t - \alpha_i).$$

Exercise 6.20. *Prove Lemma 6.8.*

Theorem 6.9. *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 6.6, we can express $P = P_1 \ldots P_{r_P}$ 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 **??**, 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 6.6 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

$$P = (t - \beta_1)(t - \beta_2) \ldots (t - \beta_\ell) \prod_{i=1}^{r_\ell} P_{\ell,i}$$

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 6.9, 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 6.10. *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 6.10 is strictly better.

Exercise 6.21. *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 6.10, 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 6.22. *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 6.23. *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 6.24. *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 6.23]*

(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 6.11. *The construction of the splitting field in the proof of Theorem 6.9 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 6.12 (Algebraically Closed Field)**.** *We say that a field E is **algebraically closed** if every $P \in E[t]$ splits over E.*

Theorem 6.12. *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

$\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ is linearly independent but $\{1, \beta, \ldots, \beta^n\}$ is linearly dependent. By definition of linear dependence, there exist $\lambda_0, \ldots, \lambda_n \in E$ 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

$$P(t) = \alpha(t - \alpha_1)(t - \alpha_2)\ldots(t - \alpha_n)$$

for some $\alpha, \alpha_1, \ldots, \alpha_n \in E$ with $\alpha \neq 0$. Since $P(\beta) = 0$, we see that

$$\alpha(\beta - \alpha_1)(\beta - \alpha_2)\ldots(\beta - \alpha_n) = 0.$$

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 6.5, 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 6.6, we have $P = P_1 \ldots P_{r_P}$ 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 **??**, 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 6.6, we have $P = P_1 \ldots P_{r_P}$ 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 6.19, 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 6.13. *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 6.12, will show that every polynomial $P \in E[t]$ has a zero in E. By Theorem 6.6, we have $P = P_1 \ldots P_{r_P}$ such that $P_i \in E[t]$ are irreducible and $0 < \deg(P_i) \leq \deg(P)$. By Corollary **??**,

$E' = E[t]/\langle P_1\rangle$ 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 $F_1 = F(\lambda_0, \ldots, \lambda_{n_1})$ 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 **??**, 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 6.2, there exists a polynomial $Q \in F[t]$ such that $Q(\beta) = 0$. Since Q splits over E, we know that

$$Q = (t - \beta_1)\ldots(t - \beta_m)$$

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 6.12, 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 6.13, 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 6.9, 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 6.9, 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 6.13, $\overline{F}$ is algebraically closed.

Theorem 6.14 (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 6.25. *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 6.25, when E/F is finite, we can take $\overline{E}$ to be $\overline{F}$.

Chapter 7

Algebras

Contents

7.1 *Matrix Algebras*

7.2 *Group Algebras*

7.3 *Artin–Wedderburn Theory*

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.