Introduction to Higher Mathematics
Unit #5: Abstract Algebra

Joseph H. Silverman

Version Date: January 6, 2020

Contents

Chapter 1

Abstract Algebra — Lecture #1

1.1 What is Abstract Alegbra?

The overall theme of this unit is algebraic structures in mathematics. Roughly speaking, an algebraic structure consists of a set of objects and a set of rules that let you manipulate the objects. Here are some examples that will be familiar to you:

Example 1.1. The objects are the numbers $1, 2, 3, \ldots$. You already know two ways to manipulate these objects, namely addition $a + b$ and multiplication $a \cdot b$

Example 1.2. The objects are triangles in the plane, and we can be manipulate them by translation and by rotation and by reflection.

Example 1.3. The objects are functions $f : \mathbb{R} \to \mathbb{R}$, and we can manipulate them by addtion $f(x)+g(x)$, by multiplication $f(x)\cdot g(x)$, and also by composition $f\big(g(x)\big)$.

Our primary goal is to take examples of this sort and generalize them, or in mathematical terminology, *axiomatize them*. To do this, we strip away everything that is not essential and reduce down to an abstract description consisting of a set with operations (such as addition and multiplication) that are required to satisfy certain rules, also known as *axioms*.[1]

In this unit we will study three different types of objects and their associated rules:

Groups Rings Fields

Although groups, rings, and fields are not the same, they share common themes. In each case we use axioms to describe objects having an algebraic structure, and we study maps between these objects that preserve the structure. Roughly speaking, each topic is organized as follows, although the order may vary slightly from topic to topic:

[1] Axioms are also sometimes called "laws". For example, you're probably familiar with the "commutative law" for addition, which says that $a + b = b + a$. But this isn't really a law, debated and approved by a legislative body! Instead, addition is a rule that explains how to combine two numbers and get a third number, and the "commmutative law" is a property that we impose on the "addition rule".

- Give an example of a certain type of algebraic structure
- Give a formal definition, using axioms, of the algebraic structure.
- Prove a basic property directly from the definitions.
- Discuss what a map must do to "preserve the algebraic structure."
- Give additional examples.
- Investigate and prove a deeper property.

A Note on the Role of Definitions, Axioms, and Proofs in Higher Mathematics: Since at least the time of Euclid, circa 300 BC, the ultimate test of mathematical rigor lies in the construction of proofs of mathematical statements. Without getting into deep matters of philosophy, a proof is a sequence of steps that starts with a known fact and ends with the desired final statement. Each step is required to follow logically from a combination of one or more of the following:[2]

- Steps in the proof that have already been completed.
- Statements that have previously been proven.
- Axioms, which are statements that are assumed to be true.
- Definitions, which describe the properties possessed by objects.

Mini-Remark 1. **Further Remarks about Definitions**: There is nothing magical about a definition, and in principle there are no restrictions on what may be defined. For example, I might define a Zyglx to be a purple pig with wings. I could then potentially use that definition to prove that Zyglxes are able to fly, since they have wings. Is ths useful? No, since as far as I am aware, there is nothing in the real world to which I could apply "Zyglx Theory." So although definitions are, to some extent, arbitrary, the usefulness of a definition is determined by its applicability to a range of (realistic) situations. We will see many examples of such definitions, including especially the definitions of *groups*, *rings*, and *fields*. The primary goal of theoretical mathematics, and likewise of this course, is to formulate and prove interesting mathematical statements, which in our case means statements about groups, rings, etc. And the only way to get started is to have a soild understanding of the definitions of the objects that we want to study. This is why understanding and applying definitions is a crucial part of modern mathematics, and why you should spend time studying definitions when they're introduced and using definitions when you're trying to prove things.

Mini-Remark 2. **Further Remarks about Axioms**: In Greek mathematics, axioms were viewed as statements that are so self-evident, they must be true. The modern viewpoint is that in principle, one is free to use any set of axioms that one wants. However, not all axiom systems are equally interesting.[3] The best and most interesting axiom systems are those that start with very few axioms[4] and allow one to prove a very large number of useful and interesting and

[2] Axioms and definitions are discussed further in the Mini-Remarks in this section.

[3] Or, to misquote Orwell, "All axiom systems are created equal, but some are more equal than others."

[4] Although the sheep might initially bleat "Four axioms good, two axioms bad," eventually they are indoctrinated to follow the party line and proclaim "Four axioms good, two axioms better."

beautiful statements. The axioms for geometry that appear in Euclid's work are an example. But one of those axioms, the so-called *parallel postulate*, led to a revolution in mathematics. This axiom says that given a line L in the plane and a point P not lying on L, there is exactly one line L' that contains P and does not intersect L. Seems reasonable, but maybe not entirely self-evident, so mathematicians spent centuries trying to prove that it follows from Euclid's other axioms. All failed. Then, in the 19th century, it was discovered that if one changes the parallel postulate by replacing the words "exactly one line" with "infinitely many lines," or with "no lines," then one gets geometries that are as valid as Euclid's. These so-called non-Euclidean geometries have many uses in modern mathematics and physics, and indeed it is likely that the universe in which we live is actually an "infinitely many lines" space!

Important Note for Math 760: Unit 5: These notes are meant to supplement what we do in class. We will cover some of the material in these notes, and in class we will likely end up exploring material that is not in these notes. Our goal is to:

Explore Unfamiliar Terrain

Where that will take us remains to be seen!

1.2 Introduction to Groups

We start with a simple question. What are the different ways that we can rearrange the list of numbers $1, 2, 3, 4$? For example, we could send 1 to 2, send 2 to 3, send 3 to 4, and send 4 to 1. This is conveniently illustrated by the picture

$$1 \to 2, \qquad 2 \to 3, \qquad 3 \to 4, \qquad 4 \to 1. \tag{1.1}$$

Another way to rearrange them would be swap 1 and 2 and swap 3 and 4, illustrated by

$$1 \to 2, \qquad 2 \to 1, \qquad 3 \to 4, \qquad 4 \to 3. \tag{1.2}$$

The mathematical word for such a rearrangement is a *permutation*, so we have just described two different permutations of the set $\{1, 2, 3, 4\}$. A permutation of the set $\{1, 2, 3, 4\}$ is described by a rule that assigns to each element of the set $\{1, 2, 3, 4\}$ an element of the same set $\{1, 2, 3, 4\}$, with the added proviso that we don't use any element twice.

Mini-Remark 3. How many permutations are there of the set $\{1, 2, 3, 4\}$? We can assign 1 to any of $1, 2, 3, 4$, so there are 4 choices for 1, then we can assign 2 to any of the remaining 3 values, after which we can assign 3 to either of the remaining 2 values, and finally we have to assign 4 to the last remaining value. Thus there are $4 \cdot 3 \cdot 2 \cdot 1$, i.e., 24, different permutations of $\{1, 2, 3, 4\}$. More generally, Exercise #1.1 asks you to compute how many permutations there are of the set $\{1, 2, \ldots, n\}$.

Mini-Remark 4. If we have two permutations of $\{1, 2, 3, 4\}$, we can "compose" them by doing first one, and then the other. So for example, if we let σ be the permutation described in (1.1) and we let τ be the permutation described in (1.2), then $\sigma \circ \tau$ is the permutation having the following effect on the set $\{1, 2, 3, 4\}$:

$$1 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3, \qquad 2 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2, \qquad 3 \xrightarrow{\tau} 4 \xrightarrow{\sigma} 1, \qquad 4 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 4.$$

An interesting observation is that if we compose σ and τ in the other order, we get a different permutation. Thus

$$1 \xrightarrow{\sigma} 2 \xrightarrow{\tau} 1, \qquad 2 \xrightarrow{\sigma} 3 \xrightarrow{\tau} 4, \qquad 3 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 3, \qquad 4 \xrightarrow{\sigma} 1 \xrightarrow{\tau} 2.$$

In general, a *permutation* of a set X is a rule that "mixes up" the elements of X. Our first goal is to give a precise mathematical meaning to the notion of "a rule that mixes up a set."

We already have a mathematical name for "rules" that tell us how to take elements of a set X and assign them to elements of a set Y. These rules are called *functions with domain X and range Y*. So a permutation on a set X is a function whose domain and range are both the same set X, but with some added conditions to ensure that every image element comes from exactly one domain element.

Definition. A *permutation* of a set X is a bijective function[5] whose domain and range are X. In other words, a permutation of X is a function

$$\pi : X \longrightarrow X$$

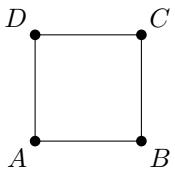
having the following property: For every element $x \in X$ there is exactly one element $x' \in X$ satisfying $\pi(x') = x$. This allows us to define the *inverse of* π to be the permutation

$$\pi^{-1} : X \longrightarrow X$$

determined by the rule that $\pi^{-1}(x)$ is equal to the unique element $x' \in X$ such that $\pi(x') = x$. Finally, we define the *identity permutation of* X to be the identity map,

$$e : X \longrightarrow X, \quad e(x) = x \quad \text{for all } x \in X.$$

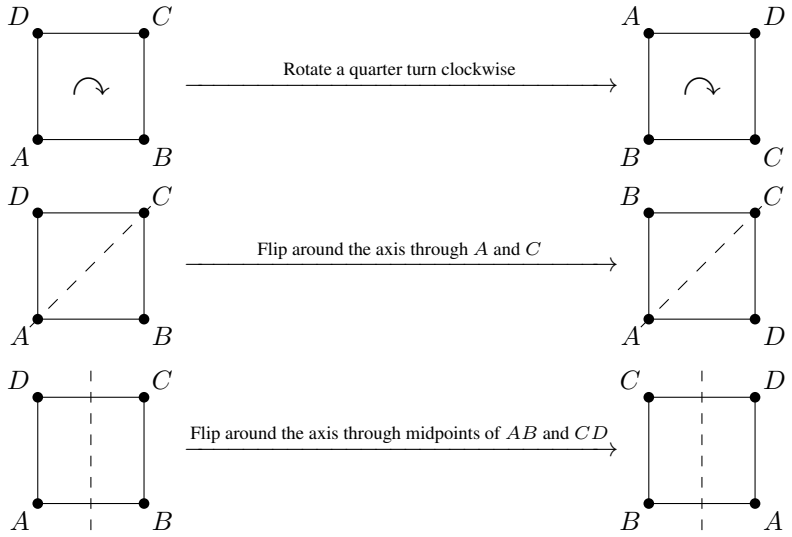
Example 1.4 (**Symmetries of a Square**). Next we consider a rigid square whose vertices are labeled A, B, C, D as in the following picture:



Suppose that we pick up the square and rotate or flip it[6] in some way, then put it back down. Here are three examples:

[5]Recall from Set Theory that a function $\phi : S \to T$ is *injective* if for every $t \in T$ there is at most one $s \in S$ satisfying $\phi(s) = t$, and that ϕ is *surjective* if for every $t \in T$ there is at least one $s \in S$ satisfying $\phi(s) = t$. A function that is both injective and surjective is said to be *bijective*. We also recall that another name for injective functions is *one-to-one*, and another name for surjective functions is *onto*.

[6]Many mathematicians prefer to say that we *reflect* the square, instead of using the more action-packed word *flip*.



The rotation and flips described in these pictures are permutations of the set $\{A, B, C, D\}$. Explicitly, if we call them Rot, Flip_1, and Flip_2,

Rot	Flip_1	Flip_2
$A \to D$	$A \to A$	$A \to B$
$B \to A$	$B \to D$	$B \to A$
$C \to B$	$C \to C$	$C \to D$
$D \to C$	$D \to B$	$D \to C$

But not all permutations of $\{A, B, C, D\}$ are permitted, since we're not allowed to bend or break the sides of the square. For example, there is no way to pick up the square and put it back down so that

$$A \to A, \quad B \to B, \quad C \to D, \quad D \to C,$$

without bending or breaking its sides. So the collection of symmetries of the square includes only some of the permutations of the set $\{A, B, C, D\}$. We leave it to you to check that among the 24 permutations of $\{A, B, C, D\}$, there are exactly 8 that are valid symmetries of the square.

1.3 Abstract Groups

Definition. A *group* consists of a set G together with a composition law

$$\begin{aligned} G \times G &\longrightarrow G, \\ (g_1, g_2) &\longmapsto g_1 \cdot g_2, \end{aligned}$$

satisfying the following axioms:

(a) (*Identity Axiom*) There is an element $e \in G$ such that

$$e \cdot g = g \cdot e = g \quad \text{for all } g \in G.$$

The element e is called the *identity element of* G.

(b) (*Inverse Axiom*) For every $g \in G$ there is an element $h \in G$ such that

$$g \cdot h = h \cdot g = e.$$

The element h is denoted g^{-1} and is called the *inverse of* g.

(c) (*Associative Law*) For all $g_1, g_2, g_3 \in G$, the *associative law* holds, that is,

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3.$$

(d) (*Commutative Law*) If in addition it is true that

$$g_1 \cdot g_2 = g_2 \cdot g_1 \quad \text{for all } g_1, g_2 \in G,$$

then G is said to be *commutative* or *abelian*.[7]

Remark 1.5. The key attribute of a group is that it includes a "rule" or "operation" or "law" (satisfying three axioms) for combining two elements of the group to create a third element. Depending on the context, you may find the group law being called "addition" or "multiplication" or "composition," but assigning a name to the group law is simply a linguistic convenience,[8] and if you prefer, you may make up some other name, say "xzyglpqz," for the group law in your favorite group.[9]

There are various basic properties of groups that follow from three group axioms. We list some of them here, prove one, and leave the others as exercises.

Proposition 1.6 (Basic Properties of Groups)**.** *Let G be a group.*

(a) *G has exactly one identity element.*

(b) *Each element of G has exactly one inverse.*

(c) *Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.*

(d) *Let $g \in G$. Then $(g^{-1})^{-1} = g$.*

Proof. We prove one part, and leave the others as exercises

(b) Let $g \in G$, and suppose that $h_1, h_2 \in G$ are both inverses for g. Then

$$\begin{aligned} h_1 &= h_1 \cdot e && \text{since } e \text{ is the identity element,} \\ &= h_1 \cdot (g \cdot h_2) && \text{since } h_2 \text{ is an inverse of } g, \\ &= (h_1 \cdot g) \cdot h_2 && \text{associative law,} \\ &= e \cdot h_2 && \text{since } h_1 \text{ is an inverse of } g, \\ &= h_2 && \text{since } e \text{ is the identity element.} \end{aligned}$$

This completes the proof. □

[7] The word "abelian" comes from Niels Henrik Abel (1802–1829), a Norwegian mathematician famous for many discoveries, including a proof that it is impossible to solve a general quintic equation using radicals. The Abel prize for mathematics, modeled after the Nobel prizes and awarded annually since 2002, is named in his honor.

[8] Or, as Juliet actually said to Romeo, "a group law by any other name would smell as sweet."

[9] Although in practice, people generally don't call a group law "addition" unless it is commutative.

Definition. The *order* of a group G, which we denote by $\#G$, is the cardinality of the set of elements of G, e.g., if G is finite, it is simply the number of elements in G.[10]

Definition. Let G be a group, and let $g \in G$. The *order* of the element g is the smallest integer $n \geq 1$ with the property that $g^n = e$. If no such n exists, then we say that g has infinite order.

Proposition 1.7. *Let G be a group, let $g \in G$, and let $n \geq 1$ be an integer such that $g^n = e$. Then the order of g divides n.*

Proof. Let m be the order of g, so m is the smallest positive integer satisfying $g^m = e$. Dividing n by m yields a quotient and remainder

$$n = mq + r \quad \text{with } 0 \leq r < m.$$

We use this equality and the fact that $g^n = g^m = e$ to compute

$$e = g^n = g^{mq+r} = (g^m)^q \cdot g^r = e^q \cdot g^r = g^r.$$

Thus $g^r = e$ and $0 \leq r < m$. But by definition, the smallest postive power of g that equals e is g^m. Therefore $r = 0$ and $n = mq$, which shows that m, which is the order of g, divides n. □

Exercises

1.1. Let n be a positive integer, and let G be the group of permutations of the set $\{1, 2, \ldots, n\}$. Prove that G is a finite group, and give a formula for the order of G.

1.2. (a) Let S be a finite set, and let $\phi : S \to S$ be a function. Prove that the following are equivalent:

(i) ϕ is injective. (ii) ϕ is surjective. (iii) ϕ is bijective.

(b) Give an example of an infinite set S and a function $\phi : S \to S$ such that ϕ is injective, but is not surjective.

(c) Give an example of an infinite set S and a function $\phi : S \to S$ such that ϕ is surjective, but is not injective.

1.3. Figure 1.1 shows various rotations and flips of a square. Fill in the boxes with the correct vertex labels for the indicated operations.

1.4. Let G be a group. In this exercise you will prove the remaining parts of Proposition 1.6. Be sure to justify each step using the group axioms or by reference to a previously proven fact.

(a) G has exactly one identity element.

[10] Other common notations for the order of a group, or more generally, for the cardinality of a set, include $o(G)$ and $|G|$.

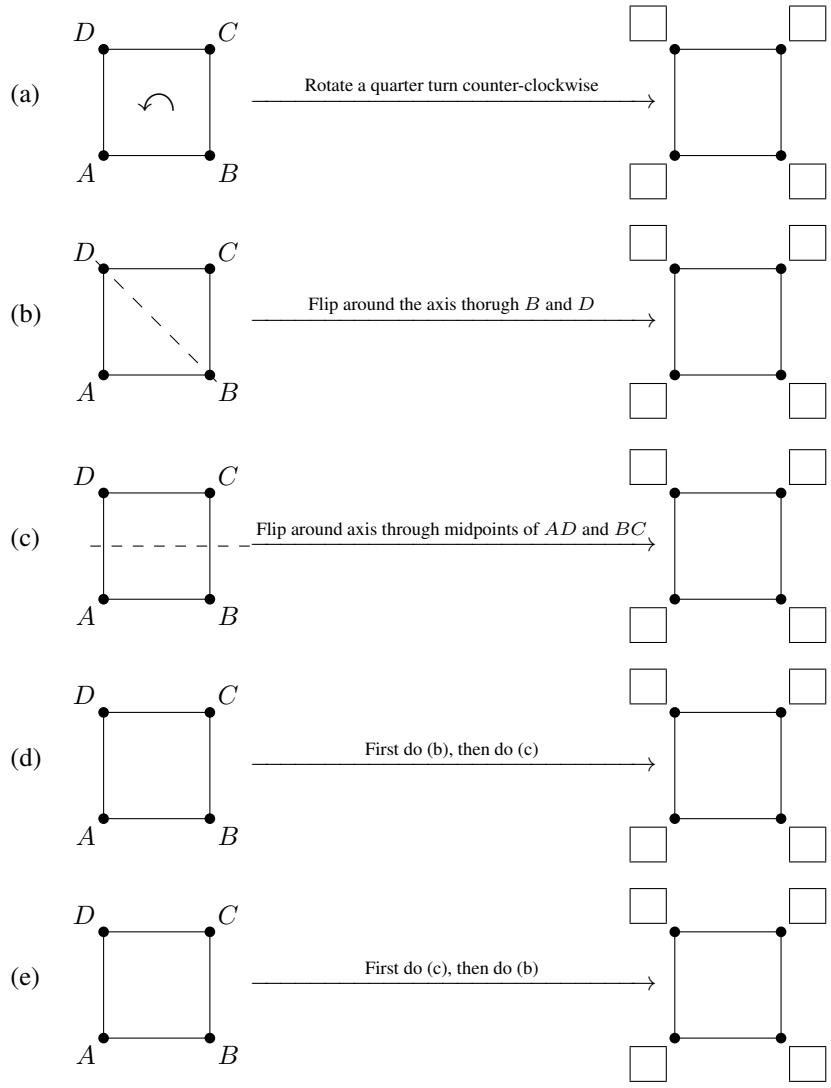


Figure 1.1: Motions of a Square for Exercise 1.3

(b) Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.
(c) Let $g \in G$. Then $(g^{-1})^{-1} = g$.

1.5. Let G be a group, let g and h be elements of G, and suppose that g has order n and h has order m.
(a) If G is an abelian group and if $\gcd(m, n) = 1$, prove that the order of gh is mn.
(b) Give an example of an abelian group showing that (a) need not be true if $\gcd(m, n) > 1$.
(c) Give an example a nonabelian group showing that (a) need not be true even if we retain the requirement that $\gcd(m, n) = 1$.

Chapter 2

Abstract Algebra — Lecture #2

2.1 Groups and More Groups: Examples

In Section 1.2 we saw a couple of groups. It's time to expand our repertoire.

Example 2.1 (**Group of Integers and Integers Modulo m**). The set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is a group if we use addition as the group law. It is an example of an *infinite group*, that is, a group having infinitely many elements. On the other hand, if we try to use multiplication as the group law, then $\mathbb{Z}$ is not a group. Do you see why not? The set $\mathbb{Z}/m\mathbb{Z}$ of integers modulo m forms a group with addition as the group law. It is a finite group of order m.

Example 2.2 (**Additive Group of Real, Rational, and Complex Numbers**). The set of real numbers $\mathbb{R}$ with addition is an infinite group, as is the set of rational numbers $\mathbb{Q}$ and the set of complex numbers $\mathbb{C}$.

Example 2.3 (**Multiplicative Group of Real Numbers**). The set of *non-zero* real numbers forms a group with mulitplication as the group law. The set of *positive* real numbers also forms a group using multiplication.

Definition. A group G is a *cyclic group* if there is an element $g \in G$ with the property that

$$G = \{\ldots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\}.$$

(Here g^{-k} is shorthand for the k-fold product $g^{-1} \cdot g^{-1} \cdots g^{-1}$.) The element g a *generator of* G, but note that cyclic groups may have more than one generator.

Example 2.4 (**Cyclic Groups**). We have already seen some examples of cyclic groups. The group of integers $(\mathbb{Z}, +)$ is an infinite cyclic group whose generators are 1 and -1. The group $(\mathbb{Z}/m\mathbb{Z}, +)$ of integers modulo m is a finite cyclic group of order m whose generators are precisely the elements $a \bmod m$ such that $\gcd(a, m) = 1$; see Exercise 2.1.

In general, for $n \geq 1$, we create an abstract cyclic group order n, which we denote $\mathcal{C}_n$, by taking the set

$$\mathcal{C}_n = \{g_0, g_1, g_2, \ldots, g_{n-1}\}$$

and using the composition rule

$$g_i \cdot g_j = \begin{cases} g_{i+j} & \text{if } i+j < n, \\ g_{i+j-n} & \text{if } i+j \ge n. \end{cases}$$

The identity element of $\mathcal{C}_n$ is the element g_0, and the inverse of an element g_i is the element g_{n-i}, except that the inveres of g_0 is g_0. We note that $\mathcal{C}_n$ is an abelian group, since $g_{i+j} = g_{j+i}$.

Example 2.5 (**Permutation Groups**). Let X be a set. We recall that a *permutation of* X is a bijective function

$$\pi : X \longrightarrow X.$$

The *symmetry group of* X is the collection of all of permutations of X, with the group law being composition of permutations. It is denoted $\mathcal{S}_X$. In the special case that $X = \{1, 2, \ldots, n\}$ consists of the integers from 1 to n, we write $\mathcal{S}_n$. We saw in Section 1.2 that the group $\mathcal{S}_4$ has order 24, and that it is nonabelian, since we described elements $\sigma, \tau \in \mathcal{S}_4$ with the property that $\sigma\tau \ne \tau\sigma$. Exercise 1.1 asks you to compute the order of the group $\mathcal{S}_n$.

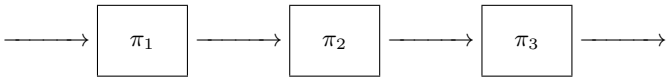
Mini-Remark 5. The identity element for the group $\mathcal{S}_X$ is the identity map $\pi_0(x) = x$, while the inverse of an element $\pi \in \mathcal{S}_X$ is the inverse map π^{-1}, which exists because π is bijective. But why does composition of permutations satisfy the associative law? The composition of two permutations $\pi_1, \pi_2 \in \mathcal{S}_X$ is defined by the formula

$$(\pi_1 \circ \pi_2)(x) = \pi_1\big(\pi_2(x)\big).$$

So we can formally compute

$$\begin{aligned} \big((\pi_1 \circ \pi_2) \circ \pi_3\big)(x) &= (\pi_1 \circ \pi_2)\big(\pi_3(x)\big) = \pi_1\big(\pi_2\big(\pi_3(x)\big)\big), \\ \big(\pi_1 \circ (\pi_2 \circ \pi_3)\big)(x) &= \pi_1\big((\pi_2 \circ \pi_3)(x)\big) = \pi_1\big(\pi_2\big(\pi_3(x)\big)\big). \end{aligned}$$

Alternatively, you may prefer to view a permutation as a function that takes in a value and spits out a value. Then the composition $\pi_1 \circ \pi_2 \circ \pi_3$, regardless of how you group the functions, is illustrated by the following picture:



Example 2.6 (**Matrix Groups**). Many of you will have learned how to multiply 2-by-2 matrices,

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}. \tag{2.1}$$

The following set of 2-by-2 matrices,

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\},$$

is a group using matrix multiplication as the group operation; see Exercise 2.6. Similarly, the set

$$\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z},\ ad-bc = \pm 1 \right\}$$

is a group. But the set

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z},\ ad-bc \neq 0 \right\}$$

not a group. Do you see why?

Example 2.7 (**Dihedral Groups**). Let P be a regular n-gon, with vertices labeled $1, 2, \ldots, n$. Figure 2.1 illustrates the case $n = 6$. Just as we did with the square in Section 1.2, we can permute the vertices $\{1, 2, \ldots, n\}$ of P by lifting up the n-gon, rotating and/or flipping it, and then putting it back down where it originally was. The group of all such permutations of the n-gon is called the *n'th dihedral group* and is denoted $\mathcal{D}_n$. There are exactly n rotations (if we treat no movement as the trivial rotation) and exactly n flips, so $\mathcal{D}_n$ is a group of order $2n$; see Exercise 2.3.

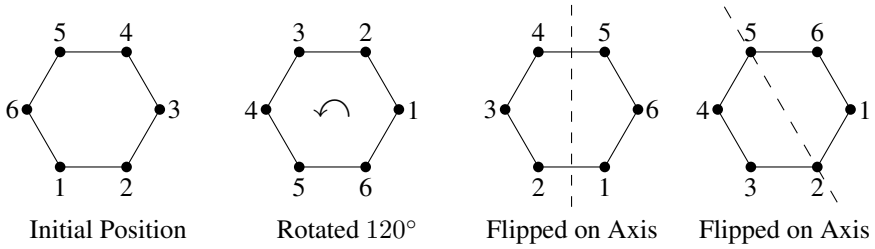


Figure 2.1: A rotation and two flips of a regular n-gon with $n = 6$

Example 2.8 (**Quaternion Group**). The *quaternion group* $\mathcal{Q}$ is a non-commutative group with eight elements,

$$\mathcal{Q} = \{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}.$$

The pluses and minuses work as usual with $(-1)^2 = 1$. The rules for multiplying the quantities $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ are determined by the formulas

$$\boldsymbol{i} \cdot \boldsymbol{i} = -1, \quad \boldsymbol{j} \cdot \boldsymbol{j} = -1, \quad \boldsymbol{k} \cdot \boldsymbol{k} = -1, \quad \boldsymbol{i} \cdot \boldsymbol{j} \cdot \boldsymbol{k} = -1.$$

From these rules one can prove, for example, that $\boldsymbol{j} \cdot \boldsymbol{i} = -\boldsymbol{i} \cdot \boldsymbol{j}$. See Exercise 2.7.

Example 2.9 (**Products of Groups**). Suppose that G_1 and G_2 are groups, with their own group laws. Consider the set of pairs

$$G_1 \times G_2 = \big\{(g_1, g_2) : g_1 \in G_1,\ g_2 \in G_2\big\}.$$

We can make $G_1 \times G_2$ into a group by defining

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2').$$

Do you see why this makes $G_1 \times G_2$ into a group? What is the identity element? What are inverse elements? Why is it associative?

2.2 Permutation Groups

We recall that

$$\mathcal{S}_n = \text{the group of permutations of the set } \{1, 2, \ldots, n\}.$$

Example 2.10. The group $\mathcal{S}_1 = \{e\}$ is the group with one element, while $\mathcal{S}_2 = \{e, \pi\}$ is a cyclic group of order 2. The group $\mathcal{S}_3$ is a non-abelian group of order 6 that is isomomorphic to the group $\mathcal{D}_3$ of symmetries of an equilateral triangle; see Exercise 3.3.

We start with two elementary, but important, properties of $\mathcal{S}_n$.

Proposition 2.11. (a) *The group $\mathcal{S}_n$ has order $n!$.*
(b) *For all $n \ge 3$, the group $\mathcal{S}_n$ is non-abelian.*

Proof. (a) Each $\pi \in \mathcal{S}_n$ is determined by what it does to each of $1, 2, \ldots, n$. The value of $\pi(1)$ can by any of the n values, then $\pi(2)$ can be any of the remaining $n-1$ values, then $\pi(3)$ can be any of the remaining $n-2$ values, and so on. Hence there are exactly $n \cdot (n-1) \cdots 2 \cdot 1$ possible permutations π. Hence $\mathcal{S}_n$ is a finite group of order $\#\mathcal{S}_n = n!$.
(b) We define elements $\pi_1, \pi_2 \in \mathcal{S}_n$ by having π_1 swap 1 and 2, and π_2 swap 2 and 3. In other words, we define π_1 and π_2 by the following rules:

$$\begin{aligned} &\pi_1(1) = 2, \quad &&\pi_1(2) = 1, \quad &&\pi_1(3) = 3, \quad &&\pi_1(k) = k \text{ for } k \ge 3. \\ &\pi_2(1) = 1, \quad &&\pi_2(2) = 3, \quad &&\pi_2(3) = 2, \quad &&\pi_2(k) = k \text{ for } k \ge 3. \end{aligned}$$

Then

$$\pi_1\pi_2(1) = \pi_1(1) = 2 \quad \text{and} \quad \pi_2\pi_1(1) = \pi_2(2) = 3.$$

So $\pi_1\pi_2$ and $\pi_2\pi_1$ are not the same permutation, and hence $\mathcal{S}_n$ is not commutative. □

2.2.1 Decomposing Permutations into Cycles

One way to analyze a permutation $\pi \in \mathcal{S}_n$ is to take some starting element of $\{1, 2, \ldots, n\}$ and see where it goes as we repeatedly apply π. For example, starting at 1, we would get

$$1,\ \pi(1),\ \pi^2(1),\ \pi^3(1), \ldots . \tag{2.2}$$

Of course, eventually we get a repeated value, since the set $\{1, \ldots, n\}$ is finite, and then the sequence starts repeating. Indeed, since some power of π is the identity permutation, the element will 1 eventually re-appear in the sequence.

We can characterize the list of elements (2.2) in another way. It is the orbit of 1 for the group $\langle\pi\rangle$ generated by π. This orbit might be all of $\{1, \ldots, n\}$, but then again, it might be smaller. In any case, it is convenient to write the distinct elements in the orbit as an ordered list. Thus if the the orbit of a contains k elements, we write the orbit as

$$\big(a, \pi(a), \pi^2(a), \ldots, \pi^{k-1}(a)\big),$$

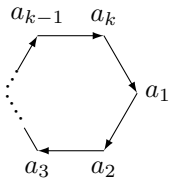
and we call this k-tuple the *π-cycle of a*. Thus if someone tells you that

$$(a_1, a_2, \ldots, a_k)$$

is a cycle for π, you would know that

$$a_1 \xrightarrow{\pi} a_2 \xrightarrow{\pi} a_3 \xrightarrow{\pi} \cdots \xrightarrow{\pi} a_{k-1} \xrightarrow{\pi} a_k \xrightarrow{\pi} a_1.$$

Notice how π "cycles" the last element around to the first element, which is why it is called a cycle. So although it's typographically convenient to write the cycle as $(a_1, \ldots, a_k)$, you should visualize this cycle as a picture that looks like



In particular, a cycle does not have a particular starting or ending element, just as a circle does not have a starting or ending point.

Definition. The number of elements in a cycle is called the *length of the cycle*. A cycle of length k is called a *k-cycle*. Two cycles $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_\ell)$ are said to be *disjoint* if

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_\ell\} = \emptyset.$$

Example 2.12. If $\pi(a) = a$, i.e., if the permutation π fixes a, then the π-cycle of a is simply (a).

Definition. Let $a_1, a_2, \ldots, a_k$ be distinct elements of $\{1, 2, \ldots, n\}$. We use this list to define a permutation $\pi \in \mathcal{S}_n$ by the rule

$$a_1 \xrightarrow{\pi} a_2 \xrightarrow{\pi} a_3 \xrightarrow{\pi} \cdots \xrightarrow{\pi} a_{k-1} \xrightarrow{\pi} a_k \xrightarrow{\pi} a_1 \quad \text{and} \quad b \xrightarrow{\pi} b \ \text{ for } b \notin \{a_1, \ldots, a_k\}.$$

In other words, the permutation π includes the cycle $(a_1, \ldots, a_k)$, and and every element of $\{1, \ldots, n\}$ that's not in the cycle is fixed by π. It is standard notation to denote this permutation by it's non-trivial cycle, i.e., we write[1]

$$(a_1, a_2, \ldots, a_k) \in \mathcal{S}_n.$$

Remark 2.13. Let σ_1 and σ_2 be cycles in $\mathcal{S}_n$. As we saw in Example 2.14, it may well happen that $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$. However, if the cycles σ_1 and σ_2 are disjoint, then they do commute:

$$\sigma_1 \text{ and } \sigma_2 \text{ are disjoint} \quad \Longrightarrow \quad \sigma_1\sigma_2 = \sigma_2\sigma_1.$$

We leave the proof of this elementary fact as an exercise; see Exercise 2.10.

Example 2.14. We work in $\mathcal{S}_4$. The cycles $(1,3)$ and $(1,4,2)$ correspond to the permutations

$$(1,3) : \begin{cases} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \\ 4 \to 4 \end{cases} \qquad \text{and} \qquad (1,4,2) : \begin{cases} 1 \to 4 \\ 2 \to 1 \\ 3 \to 3 \\ 4 \to 2 \end{cases}$$

We can compose cycle permutations, for example:

$$(1,3)(1,4,2) : \begin{cases} 1 \to 4 \\ 2 \to 3 \\ 3 \to 1 \\ 4 \to 2 \end{cases} \qquad \text{and} \qquad (1,4,2)(1,3) : \begin{cases} 1 \to 3 \\ 2 \to 1 \\ 3 \to 4 \\ 4 \to 2 \end{cases}$$

The rule for computing these is to input a number on the right, see where the rightmost cycle sends it, then see where the next cycle sends that, and so on. As it happens, both of these products are themselves cycles, but they are not the same cycle:

$$(1,3)(1,4,2) = (1,4,2,3) \quad \text{and} \quad (1,4,2)(1,3) = (1,3,4,2).$$

Definition. A permutation $\pi \in \mathcal{S}_n$ is called a *cycle* if it is equal to a single cycle $(a_1, a_2, \ldots, a_n)$.

Our next result says that every permutation can be uniquely written as a product of disjoint cycles. It plays the role in the study of permutation groups that unique factorization of integers plays in the study of $\mathbb{Z}$.

[1] So this is yet another meaning that we attach to a k-tuple. The meaning of $(a_1 \ldots, a_k)$ will usually be clear from context. But not always. For example, suppose that we let $\mathcal{S}_n$ act on points in $\mathbb{R}^n$ by permuting the coordinates of the points. Then $(1,2)$ could be the permutation whose effect on (x,y) is $(1,2) : (x,y) \mapsto (y,x)$. On the other hand, $(1,2)$ could be a point in $\mathbb{R}^2$, leading to the confusing formula $(1,2) : (1,2) \mapsto (2,1)$! The moral is that you need to be especially careful with notation if your permutation group is acting on n-tuples!

Theorem 2.15. *Let $\pi \in \mathcal{S}_n$. There is a unique collection of pairwise disjoint cycles $\sigma_1, \ldots, \sigma_k \in \mathcal{S}_n$ such that*

$$\pi = \sigma_1\sigma_2\cdots\sigma_k. \tag{2.3}$$

Proof. We first show that π is equal to a product of disjoint cycles. For each $a \in \{1, \ldots, n\}$, let

$$\mathcal{O}_\pi(a) = \bigl\{a, \pi(a), \pi^2(a), \pi^3(a), \ldots\bigr\}.$$

This is called the *orbit of a for the permutation π*. We are going to leave to you the proof of the following two statements:

(1) Every element of $\{1, \ldots, n\}$ is in some orbit of π.

(2) Distinct orbits have no elements in common. In other words, the sets $\mathcal{O}_\pi(a)$ and $\mathcal{O}_\pi(b)$ are either equal or disjoint.

These two facts mean that we can write $\{1, \ldots, n\}$ as a disjoint union of oribts,

$$\{1, 2, \ldots, n\} = \mathcal{O}_\pi(a_1) \cup \mathcal{O}_\pi(a_2) \cup \mathcal{O}_\pi(a_3) \cup \cdots \cup \mathcal{O}_\pi(a_r)$$
$$\text{with} \quad \mathcal{O}_\pi(a_i) \cap \mathcal{O}_\pi(a_j) = \emptyset \text{ for } i \neq j.$$

Writing $k_i = \#\mathcal{O}_\pi(a_i)$ for the size of the orbit $\mathcal{O}_\pi(a_i)$ of a_i, we see that the orbit is exactly

$$\mathcal{O}_\pi(a_i) = \bigl\{a_i, \pi(a_i), \pi^2(a_i), \ldots, \pi^{k_i-1}(a_i)\bigr\}.$$

In other words, the cycle σ_i defined by

$$\sigma_i = \bigl(a_i, \pi(a_i), \pi^2(a_i), \ldots, \pi^{k_i-1}(a_i)\bigr) \quad \text{is the } \pi\text{-cycle containing } a_i.$$

For $i \neq j$, the cycles σ_i and σ_j associated to the orbits $\mathcal{O}_\pi(a_i)$ and $\mathcal{O}_\pi(a_j)$ are disjoint, so if we multiply $\sigma_1, \ldots, \sigma_r$, we obtain a permutation that is equal to π,

$$\pi = \sigma_1\sigma_2\cdots\sigma_r.$$

This completes the proof that π is equal to a product disjoint cycles.

In order to show that the decomposition (2.3) into disjoint cycles is unique (up to rearranging the factors), we note that since the cycles are disjoint, every $a \in \{1, 2, \ldots, n\}$ must appear in exactly one of the cycles, and in that cycle, it must be followed by $\pi(a)$. There is thus only one way for the cycles to look. □

Example 2.16. Let $\pi \in \mathcal{S}_{10}$ be the permutation

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 7 & 2 & 10 & 9 & 4 & 5 & 6 & 8 \end{array}$$

In order to write π as a product of cycles, we start by computing the orbits:

$$1 \xrightarrow{\pi} 3 \xrightarrow{\pi} 7 \xrightarrow{\pi} 4 \xrightarrow{\pi} 2 \xrightarrow{\pi} 1, \qquad 5 \xrightarrow{\pi} 10 \xrightarrow{\pi} 8 \xrightarrow{\pi} 5, \qquad 6 \xrightarrow{\pi} 9 \xrightarrow{\pi} 6.$$

Thus π is a product of a 5-cycle, a 3-cycle, and a 2-cycle,

$$\pi = (1, 3, 7, 4, 2)(5, 10, 8)(6, 9).$$

2.2.2 Decomposing Permutations into Transpositions

The simplest non-trivial permutation is one that swaps two elements and leaves all of the other elements alone. We give these swap elements a special name.

Definition. An element $\pi \in \mathcal{S}_n$ is called a *transposition* if there are distinct $a, b \in \{1, 2, \ldots, n\}$ such that

$$\pi(a) = b, \quad \pi(b) = a, \quad \pi(i) = i \text{ for all } i \neq a, b.$$

In other words, using our cycle notation, the transpositions in $\mathcal{S}_n$ are the permutations (a, b) with $a \neq b$.

Just as with cycles, it turns out that every permutation can be written as a product of transpositions, although not in a unique way.

Proposition 2.17. *Let $\pi \in \mathcal{S}_n$. There are transpositions $\tau_1, \ldots, \tau_k \in \mathcal{S}_n$ so that*

$$\pi = \tau_1 \tau_2 \cdots \tau_k.$$

Proof. We know from Theorem 2.15 that π can be written as a product of (disjoint) cycles. So it suffices to write every cycle $\sigma = (a_1, a_2, \ldots, a_k)$ as a product of transpositions. We claim that the permutation

$$\nu = (a_k, a_1)(a_{k-1}, a_1) \cdots (a_3, a_1)(a_2, a_1) \tag{2.4}$$

is equal to σ. Since ν is visibly a product of transpositions, we just need to show that $\nu = \sigma$.

What is the value of $\nu(a_i)$? We consider three cases:

$\boxed{\nu(a_1)}$ When we apply ν to a_1, the first transposition (a_2, a_1) in ν sends a_1 to a_2, and then the other transpositions in ν have no effect on a_2. Hence $\nu(a_1) = a_2$.

$\boxed{\nu(a_i) \text{ with } 2 \le i \le k-1}$ The first transposition in ν to affect a_i is (a_i, a_1), and it sends a_i to a_1. Then the next transposion (a_{i+1}, a_1) sends a_1 to a_{i+1}, and the remaining transpositions have no effect on a_{i+1}. Hence $\nu(a_i) = a_{i+1}$.

$\boxed{\nu(a_k)}$ The only transposition in ν that affects a_k is the last one, which is (a_k, a_1) and sends a_k to a_1. Hence $\nu(a_k) = a_1$.

To recapitulate, we have shown that $\nu(a_i) = a_{i+1}$ for $1 \le i \le k-1$ and that $\nu(a_k) = a_1$. So ν is exactly the cycle $\sigma = (a_1, \ldots, a_k)$, which completes the proof that σ is a product of transpositions. □

Example 2.18. We use the idea described in the proof of Proposition 2.17 to write the cycle $(1, 2, 3, 4, 5)$ as a product of transpositions,

$$(1, 2, 3, 4, 5) = (5, 1)(4, 1)(3, 1)(2, 1).$$

But there are many other ways to write $(1, 2, 3, 4, 5)$ as a product of transpositions, for example,

$$\begin{aligned}(1,2,3,4,5) &= (5,2)(1,2)(5,2)(4,1)(3,1)(2,1)\\ &= (5,1)(4,3)(1,3)(4,3)(3,1)(2,5)(1,5)(2,5).\end{aligned}$$

We have thus written $(1,2,3,4,5)$ as a product of 4 transpositions, and as a product of 6 transpositions, and as a product of 8 transpositions.

2.2.3 The Sign of a Permutation

In general, there are many ways to write a permutation π as a product of transpositions, as illustrated in Example 2.18. A non-obvious, but very important, fact is that the parity of the number of transpositions depends only on π.

Theorem 2.19. *Let $\pi \in \mathcal{S}_n$, and suppose that we write π as a product of transpositions in two ways, say*

$$\pi = \tau_1\tau_2\cdots\tau_k = \sigma_1\sigma_2\cdots\sigma_\ell,$$

where $\tau_1,\ldots,\tau_k$ and $\sigma_1,\ldots,\sigma_\ell$ are transpositions. Then

$$k \equiv \ell \pmod 2.$$

Proof. Sadly, there are no easy proofs of Theorem 2.19, so we do not include one here. The most direct proof uses the action of $\mathcal{S}_n$ on a certain polynomial. □

Definition. Proposition 2.17 says that we can write any permutation $\pi \in \mathcal{S}_n$ as a product of transpositions,

$$\pi = \tau_1\tau_2\cdots\tau_k.$$

We define the *sign* of the permutation π to be the quantity

$$\operatorname{sign}(\pi) = (-1)^k.$$

Theorem 2.19 tells us that $\operatorname{sign}(\pi)$ is well-defined. We say that π is *even* if $\operatorname{sign}(\pi) = 1$ and that π is *odd* if $\operatorname{sign}(\pi) = -1$.

Example 2.20. We showed in Example 2.18 that the cycle $(1,2,3,4,5)$ is equal to a product of 4, 6, and 8 transpositions. In particular,

$$\operatorname{sign}\bigl((1,2,3,4,5)\bigr) = (-1)^4 = 1.$$

Exercises

2.1. Let G be a finite cyclic group of order n, and let g be a generator of G. Prove that g^k is a generator of G if and only if $\gcd(k,n) = 1$.

2.2. Figure 2.2 shows a hexagon in its initial and three subsequent positions. It thus illustrates four elements e, r_1, f_1, f_2 of the dihedral group $\mathcal{D}_6$, where e is the identiy element, r_1 is a rotation, and f_1 and f_2 are flips about the indicated axes. We mention that the flips are the same as those given in Figure 2.1, but the rotation is different.

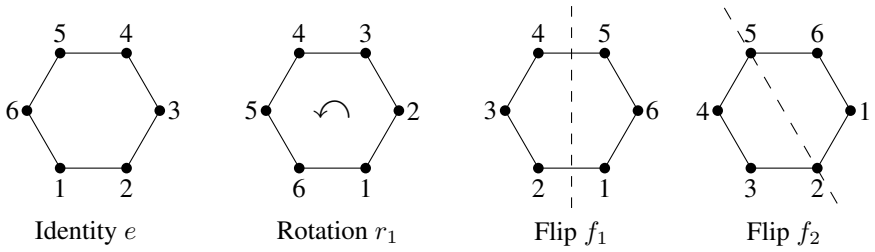


Figure 2.2: A rotation and two flips of a regular hexagon

(a) Write down and give names to the other 8 ways to rotate and/or flip the hexagon. The 12 pictures illustrate the 12 elements of the dihedral group $\mathcal{D}_6$.
(b) What is the smallest power of each of r_1, f_1, and f_2 that is equal to the identity transformation e?
(c) Write down the hexagon configurations that correspond to the compositions $r_1 f_1$, $f_1 r_1$, $r_1 f_2$, and $f_2 r_1$. Does r_1 commute with f_1 or f_2.
(d) Write down the hexagon configurations that correspond to the $f_1 f_2$ and $f_2 f_1$. Show that each of them is equal to a power of the rotation r_1, i.e., the compositions of these two flips gives a rotation.
(e) Prove that every rotation is equal to some power of r_1.
(f) Prove that every flip is equal the composition of f_1 and some power of r_1.
(g) Using (e) and (f), prove that the entire group $\mathcal{D}_6$ consists of the 12 elemenets

$$\{f_1^i r_1^j : 0 \le i \le 1 \text{ and } 0 \le j \le 5\}.$$

(h) Express $r_1 f_1$ in the form $f_1^i r_1^j$.
(i) More generally, describe one or more formulas that explain how to write the product $(f_1^k r_1^\ell)(f_1^m r_1^n)$ in the form $f_1^i r_1^j$.

2.3. Prove that the dihedral group $\mathcal{D}_n$, as described in Example 2.7, has exactly $2n$ elements.

2.4. (a) Let $\mathbb{Q}^*$ be the set of non-zero rational numbers, with the group law being multiplication. Prove that $\mathbb{Q}^*$ is a group.
(b) Let p be a prime number. Prove that the non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ form a group using multiplication as the group law.
(c) Let $m \ge 4$ be an integer that is not a prime number. Prove that the non-zero elements of $\mathbb{Z}/m\mathbb{Z}$ do not form a group using multiplication as the group law. (Try it first with $m = 4$ and $m = 6$ to see what's going on.)
(d) Let $m \ge 2$ be any integer, and define

$$(\mathbb{Z}/m\mathbb{Z})^* = \big\{a \in \mathbb{Z}/m\mathbb{Z} : \gcd(a, m) = 1\big\}.$$

Prove that $(\mathbb{Z}/m\mathbb{Z})^*$ forms a group using multiplication as the group law.

2.5. Let $\mathbb{C}$ be the set of complex numbers, that is, the set of numbers of the form $x + yi$, where $x, y \in \mathbb{R}$ and $i^2 = -1$.
(a) We make $\mathbb{C}$ into a group using addition. What is the identity element? What is the inverse of an element $z \in \mathbb{C}$?

(b) Let $\mathbb{C}^*$ be the set of non-zero complex numbers. We make $\mathbb{C}^*$ into a group using multiplication. What is the identity element? What is the inverse of an element $z \in \mathbb{C}^*$? Be sure to write your answers as a real number added to i times another real number.

2.6. (a) Let

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R},\ ad - bc \neq 0 \right\}.$$

be the indicated set of 2-by-2 matrices, with composition law being matrix multiplication, as described in Example 2.6. Prove that $\mathrm{GL}_2(\mathbb{R})$ is a group.

(b) Let $\mathrm{SL}_2(\mathbb{R})$ be the set of 2-by-2 matrices

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R},\ ad - bc = 1 \right\}.$$

Prove that $\mathrm{SL}_2(\mathbb{R})$ is a group, where the group law is again matrix multiplication.

(c) This part is for those who have studied n-dimensional linear algebra. Fix an integer $n \geq 1$. Generalize (a) and (b) by proving that each of the following sets of n-by-n matrices is a group using matrix multiplication for the group law:

$$\mathrm{GL}_n(\mathbb{R}) = \left\{ n\text{-by-}n \text{ matrices } A \text{ with real entries satisfying } \det(A) \neq 0 \right\},$$
$$\mathrm{SL}_n(\mathbb{R}) = \left\{ n\text{-by-}n \text{ matrices } A \text{ with real entries satisfying } \det(A) = 1 \right\}.$$

The group $\mathrm{GL}_n(\mathbb{R})$ is called the *general linear group*, and the group $\mathrm{SL}_n(\mathbb{R})$ is called the *special linear group*.

2.7. Let $\mathcal{Q} = \{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}$ be the group of quaternions as describe in Example 2.8. We claimed there that the group law for $\mathcal{Q}$ is determined by the formulas

$$\boldsymbol{i} \cdot \boldsymbol{i} = -1, \qquad \boldsymbol{j} \cdot \boldsymbol{j} = -1, \qquad \boldsymbol{k} \cdot \boldsymbol{k} = -1, \qquad \boldsymbol{i} \cdot \boldsymbol{j} \cdot \boldsymbol{k} = -1.$$

Use these formulas to prove the following formulas, which completely determine the group operations on $\mathcal{Q}$:

$$\begin{aligned} &\boldsymbol{i} \cdot \boldsymbol{j} = \boldsymbol{k}, && \boldsymbol{j} \cdot \boldsymbol{k}, = \boldsymbol{i} && \boldsymbol{k} \cdot \boldsymbol{i} = \boldsymbol{j}, \\ &\boldsymbol{j} \cdot \boldsymbol{i} = -\boldsymbol{k}, && \boldsymbol{k} \cdot \boldsymbol{j}, = -\boldsymbol{i} && \boldsymbol{i} \cdot \boldsymbol{k} = -\boldsymbol{j}. \end{aligned}$$

2.8. We can form groups of matrices whose entries are in any algebraic system where we can add, subtract, and multply. For example, let $m \geq 2$ be an integer, and define

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/m\mathbb{Z},\ ad - bc = 1 \right\}.$$

Prove that matrix multiplication (2.1) makes $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ into a non-commutative group.

2.9. Let $\sigma = (2, 4, 3)$ and $\tau = (1, 3, 5)$ be cycles in $\mathcal{S} - 5$. Describe the associated permutations and the composition $\sigma\tau$ and $\tau\sigma$ as was done in Example 2.14. Are $\sigma\tau$ and/or $\tau\sigma$ themselves cycles?

2.10. If σ_1 and σ_2 are disjoint cycles in $\mathcal{S}_n$, prove that $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

2.11. Let $\pi \in \mathcal{S}_{10}$ be the permutation

1	2	3	4	5	6	7	8	9	10
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
5	8	2	3	10	9	6	4	7	1

(a) Write π as a product of disjoint cycles.
(b) Compute $\operatorname{sign}(\pi)$. (*Hint*. If you prefer not to explicitly write π as a product of transpositions, you could use (a) and Example 3.7.)

2.12. (a) Let π be the cycle $\pi = (1, 2, 3, 4, 5, 6)$. Write each of $\pi^2, \pi^3, \ldots, \pi^6$ as a product of disjoint cycles. In each case, write down the number of cycles and their sizes.
(b) Let σ be a k-cycle. If we write σ^m as a product of disjoint cycles, how many cycles are there, and what are their sizes? (*Hint*. The data from (a) might help you to guess the answer, and it's always easier to prove soemthing if you know exactly what you're trying to prove.)

2.13. Let $\pi \in \mathcal{S}_n$. Then the group $\langle \pi \rangle$ acts transitively on $\{1, 2, \ldots, n\}$ if and only if every π-cycle has length n.

2.14. (a) If a and b are distinct, prove that for all c, the transposition (a, b) can be written as the following product:

$$(a, b) = (a, c)(b, c)(a, c).$$

(b) Write the cycle $(1, 2, 3, 4) \in \mathcal{S}_4$ as a product of 3 transpositions.
(c) Write the cycle $(1, 2, 3, 4) \in \mathcal{S}_4$ as a product of 5 transpositions.
(d) Write the cycle $(1, 2, 3, 4) \in \mathcal{S}_4$ as a product of 7 transpositions.

Chapter 3

Abstract Algebra — Lecture #3

3.1 Group Homomorphisms

Suppose that G and G' are groups, and suppose that ϕ is a function

$$\phi : G \longrightarrow G'$$

from the elements of G to the elements of G'. There are many such functions, but since G and G' are groups, we want to concentrate on functions ϕ that respect the "*group-i-ness*" of G and G'.

Question: What makes a group a group?
Answer: Groups have a composition law and identity elements and inverses.

So we should require that the function $\phi : G \to G'$ have the following properties:

- $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$ for all $g_1, g_2 \in G$.
- $\phi(e) = e'$, where e and e' are, respectively, the identtity elements on G and G'.
- $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.

Important Observation: Did you notice that the two "dots" in the formula

$$\begin{array}{c} \phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) \\ \uparrow \qquad\qquad \uparrow \\ \boxed{G \text{ group law}} \quad \boxed{G' \text{ group law}} \end{array} \tag{3.1}$$

are not the same dot?!! That's because the dot in $\phi(g_1 \cdot g_2)$ means that g_1 and g_2 are being combined using the composition law on the group G, while the dot in $\phi(g_1) \cdot \phi(g_2)$ means that $\phi(g_1)$ and $\phi(g_2)$ are being combined using the composition law on the group G'. So the formula (3.1) says that ϕ cleverly intertwines the group laws on G and G'. It turns out that this is enough to force the other two properties to be true, which leads to the following fundamental definition.

Definition. Let G and G' be groups. A *homomorphism from G to G'* is a function $\phi : G \to G'$ satisfying

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) \quad \text{for all} \quad g_1, g_2 \in G.$$

We'll now check that this is enough to get the other two properties that we want.

Proposition 3.1. *Let $\phi : G \to G'$ be a homomorphism of groups.*
(a) *Let $e \in G$ be the identity element of G. Then $\phi(e)$ is the identity element of G'.*
(b) *Let $g \in G$. Then $\phi(g^{-1})$ is the inverse of $\phi(g)$.*

Proof. (a) We use the fact that $e \cdot e = e$ and the fact that ϕ is a homomorphism to compute

$$\phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e). \tag{3.2}$$

We now apply $\phi(e)^{-1}$ to both sides to obtain

$$\begin{aligned}
e' &= \phi(e) \cdot \phi(e)^{-1} && \text{since } \phi(e)^{-1} \text{ is the inverse of } \phi(e),\\
&= \big(\phi(e) \cdot \phi(e)\big) \cdot \phi(e)^{-1} && \text{using (3.2)},\\
&= \phi(e) \cdot \big(\phi(e) \cdot \phi(e)^{-1}\big) && \text{associative law},\\
&= \phi(e) \cdot e' && \text{since } \phi(e)^{-1} \text{ is the inverse of } \phi(e),\\
&= \phi(e) && \text{since } e' \text{ is the identity element of } G'.
\end{aligned}$$

(b) We need to show that $\phi(g^{-1})$ has the property to be the inverse of $\phi(g)$. So we compute

$$\begin{aligned}
\phi(g^{-1}) \cdot \phi(g) &= \phi(g^{-1} \cdot g) && \text{since } \phi \text{ is a homomorphism},\\
&= \phi(e) && \text{since } g^{-1} \text{ is the inverse of } g,\\
&= e' && \text{from what we proved in (a)}.
\end{aligned}$$

The proof that $\phi(g) \cdot \phi(g^{-1}) = e'$ is similar, which completes the proof that $\phi(g^{-1})$ is the inverse of $\phi(g)$. □

Example 3.2. Recall from Example 2.7 the the dihedral group $\mathcal{D}_n$ is the collections of rotations and flips of an n-sided polygon. It is a group with $2n$ elements, half of which are rotations. We can define a homomorphism from $\mathcal{D}_n$ to the two-element group $\{\pm 1\}$ by the rule

$$\phi : \mathcal{D}_n \longrightarrow \{\pm 1\}, \quad \phi(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is a rotation,} \\ -1 & \text{if } \sigma \text{ is a flip.} \end{cases}$$

In order to check that ϕ is a homomorphism, one needs to check

$$\begin{aligned}
\text{Rotation} \circ \text{Rotation} &= \text{Rotation}, \quad \text{Rotation} \circ \text{Flip} = \text{Flip},\\
\text{Flip} \circ \text{Rotation} &= \text{Flip}, \qquad \text{Flip} \circ \text{Flip} = \text{Rotation},
\end{aligned} \tag{3.3}$$

a task which we leave to you (Exercise 3.2).

Example 3.3. For any integers $n \ge m \ge 1$, there is an injective homomorphism

$$\phi : \mathcal{S}_m \longrightarrow \mathcal{S}_n \quad \text{given by the rule} \quad \phi(\pi)(k) = \begin{cases} \pi(k) & \text{if } 1 \le k \le m, \\ k & \text{if } m < k \le n. \end{cases}$$

In other words, if π is a permutation of $\{1, 2, \dots, m\}$, then we view π as a permutation of $\{1, 2, \dots, n\}$ by letting it permute $1, 2, \dots, m$ and having it fix $m+1, m+2, \dots, n$.

Example 3.4. You already know a very important group homomorphism, namely the logarithm function (to any base), which gives a homomorphism

$$\log : \{\text{positive real numbers with } \times\} \longrightarrow \{\text{real numbers with } +\}.$$

The logarithm function is a homomorphism because it converts multiplication to addition,[1]

$$\log(ab) = \log(a) + \log(b).$$

Definition. Two groups G_1 and G_2 are said to be *isomorphic* if there is a bijective homomorphism

$$\phi : G_1 \longrightarrow G_2.$$

The map ϕ is called an *isomorphism* from G_1 to G_2. Isomorphic groups are really the same group, but their elements have been given different names.[2]

Example 3.5. The groups $\mathcal{C}_2$ and $\mathcal{S}_2$ are isomorphic, as are the group $\mathcal{D}_3$ and $\mathcal{S}_3$. If p is a prime number, then every group with exactly p elements is isomorphic to $\mathcal{C}_p$. The logarithm map (Example 3.4) is an isomorphism from the group of positive real numbers with multiplication to the group of real numbers with addition. You will get to prove these assertions in the exercises.

We recall that every permutation $\pi \in \mathcal{S}_n$ has an associated sign $\operatorname{sign}(\pi) \in \{\pm 1\}$ defined by writing $\pi = \tau_1 \tau_2 \cdots \tau_k$ for transpositions $\tau_1, \dots, \tau_k$ and then setting $\operatorname{sign}(\pi) = (-1)^k$.

Proposition 3.6. *The map*

$$\operatorname{sign} : \mathcal{S}_n \longrightarrow \{\pm 1\}$$

is a homomorphism of groups.

Proof. Let $\pi, \pi' \in \mathcal{S}_n$ be permutations. We use Proposition 2.17 to write π and π' as products of transpositions, say

$$\pi = \tau_1 \tau_2 \cdots \tau_k \quad \text{and} \quad \pi' = \tau_1' \tau_2' \cdots \tau_m'.$$

[1] Logarithms were discovered by John Napier (1550–1617). Back in "ancient days" when computations were done by hand, tables of logarithm were used extensively to speed numerical calculations in astronomy, engineering, and physics.

[2] The group you are about to study is true. Only the names of its elements have been changed to protect the innocent. . . . Cue *Dragnet* theme.

Then $\operatorname{sign}(\pi) = (-1)^k$ and $\operatorname{sign}(\pi') = (-1)^m$ by definition of sign. Taking the product,

$$\pi\pi' = (\underbrace{\tau_1\tau_2\cdots\tau_k}_{k \text{ transpositions}})(\underbrace{\tau_1'\tau_2'\cdots\tau_m'}_{m \text{ transpositions}}) = \underbrace{\tau_1\tau_2\cdots\tau_k\tau_1'\tau_2'\cdots\tau_m'}_{k+m \text{ transpositions}},$$

we see that $\pi\pi'$ is equal to a product of $k+m$ transpositions. Hence

$$\operatorname{sign}(\pi\pi') = (-1)^{k+m} = (-1)^k \cdot (-1)^m = \operatorname{sign}(\pi) \cdot \operatorname{sign}(\pi'),$$

which completes the proof that sign is a group homomorphism. □

Example 3.7. Let $\pi \in \mathcal{S}_n$ be a k cycle, say

$$\pi = (a_1, a_2, \ldots, a_k) \in \mathcal{S}_n.$$

During the proof of Proposition 2.17, we showed that π is equal to the following product of transpositions:

$$\pi = (a_k, a_1)(a_{k-1}, a_1)\cdots(a_3, a_1)(a_2, a_1).$$

There are $k-1$ transpositions in this product, so

$$\operatorname{sign}(k\text{-cycle}) = (-1)^{k-1}.$$

Since every permutation is a product of cycles, and Proposition 3.6 says that $\operatorname{sign} : \mathcal{S}_n \to \{\pm 1\}$ is a group homomorphism, this gives a quick way to compute the sign of a permutation:

$$\pi = (k_1\text{-cycle})(k_2\text{-cycle})\cdots(k_r\text{-cycle}) \quad \Longrightarrow \quad \operatorname{sign}(\pi) = (-1)^{k_1+k_2+\cdots+k_r-r}.$$

Definition. Let $n \geq 1$. The *alternating group*, denoted $\mathcal{A}_n$, is the group of even permutations. Equivalently,

$$\mathcal{A}_n = \ker(\operatorname{sign}) = \big\{\pi \in \mathcal{S}_n : \operatorname{sign}(\pi) = 1\big\}.$$

3.2 Subgroups

A guiding principle in mathematics when attempting to analyze a complicated object may be summarized by the following three steps:

Step 1 (Deconstruction): Break your object into smaller and simpler pieces.

Step 2 (Analysis): Analyze the smaller, simpler pieces.

Step 3 (Reconstruction): Fit the pieces back together.

For a group G, a natural way to form a "smaller and simpler piece" is by taking subsets H that are themselves groups. This prompts the following definition.

Definition. Let G be a group. A *subgroup of* G is a subset $H \subset G$ that is itself a group using G's group law. Explicitly, H needs to satisfy:[3]

(i) For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2$ is in H.

(ii) The identity element e is in H.

(iii) For every $h \in H$, the inverse h^{-1} is in H.

Note that since H uses the same group law as G, the elements of H automatically satisfy the associative law, so we do not need to add that as a requirement. If H is finite, we define the *order of* H to be the number of elements in H.

Example 3.8. Every group G has at least two subgroups, namely the *trivial subgroup* $\{e\}$ consisting of only the identity element, and the entire group G. Most groups have other subgroups; see Exercise 4.6.

Example 3.9. Let G be a group, and let $g \in G$. Then the *cyclic subgroup of* G *generatedy by* g, denoted $\langle g \rangle$, is the set

$$\langle g \rangle = \{\ldots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\}.$$

If g has order n, then

$$\langle g \rangle = \{e, g, g^2, g^3, \ldots, g^{n-1}\}$$

is isomorphic to the cyclic group $\mathcal{C}_n$, while if g has infinite order, then $\langle g \rangle$ is isomorphic to $\mathbb{Z}$.

Every group homomorphism has an associated subgroup, called its kernel, which can be used to give a convenient criterion for checking if the homomorphism is injective.

Definition. Let $\phi : G \to G'$ be a group homomorphism. The *kernel of* ϕ is the set of elements of G that are sent to the identity element of G',

$$\ker(\phi) = \big\{g \in G : \phi(g) = e'\big\}.$$

Proposition 3.10. *Let $\phi : G \to G'$ be a group homomorphism.*
(a) $\ker(\phi)$ *is a subgroup of* G.
(b) ϕ *is injective if and only if* $\ker(\phi) = \{e\}$.

Proof. (a) Proposition 3.1(a) says $\phi(e) = e'$, so $e \in \ker(\phi)$. Next let $g_1, g_2 \in \ker(\phi)$. Then the homomorphism property of ϕ gives $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) = e' \cdot e'$, so $g_1 \cdot g_2 \in \ker(\phi)$. Finally, for $g \in \ker(\phi)$, Proposition 3.1(b) says $\phi(g^{-1}) = \phi(g)^{-1}) = e'^{-}1 = e'$, so $g^{-1} \in \ker(\phi)$. This completes the proof that $\ker(\phi)$ is a subgroup of G.
(b) We know from Proposition 3.1(a) that $e \in \ker(\phi)$. If ϕ injective, then there is at most one element $g \in G$ satisfying $\phi(g) = e'$, so we must have $\ker(\phi) = \{e\}$

[3] In order to prove that a subset H is a subgroup, it suffices to check that $H \neq \emptyset$ and that for every $h_1, h_2 \in H$, the element $h_1 h_2^{-1}$ is in H. See Exercise 3.7.

Next we suppose that $\ker(\phi) = \{e\}$. Let $g_1, g_2 \in G$ satisfy $\phi(g_1) = \phi(g_2)$. Again using the homomorphism property and Proposition 3.1(b), we find that

$$\phi(g_1 \cdot g_2^{-1}) = \phi(g_1) \cdot \phi(g_2^{-1}) = \phi(g_1) \cdot \phi(g_2)^{-1} = e' \cdot e'^{-1} = e'.$$

Thus $g_1 \cdot g_2^{-1} \in \ker(\phi) = \{e\}$, so $g_1 = g_2$. This proves that ϕ is injective. □

Example 3.11. Let $d \in \mathbb{Z}$, then we can form a subgroup of $\mathbb{Z}$ using the multiples of d,

$$d\mathbb{Z} = \{dn : n \in \mathbb{Z}\}.$$

Example 3.12. The set of rotations in the dihedral group $\mathcal{D}_n$ is a subgroup of $\mathcal{D}_n$.

Example 3.13. The set of elements of the symmetric group $\mathcal{S}_n$ that fix n form a subgroup of $\mathcal{S}_n$. This subgroup is naturaly isomorphic to $\mathcal{S}_{n-1}$, since its elements are the permutations of $1, 2, \ldots, n-1$.

Exercises

3.1. Recall that two groups G_1 and G_2 are said to be *isomorphic* if there is a bijective homomorphism

$$\phi : G_1 \longrightarrow G_2.$$

The fact that ϕ is bijective means that the inverse map $\phi^{-1} : G_2 \to G_1$ exists. Prove that ϕ^{-1} is a homomorphism from G_2 to G_1.

3.2. Complete the proof that the map $\mathcal{D}_n \to \{\pm 1\}$ in Example 3.2 is a homomorphism by showing that compositions of rotations and flips satisfy the rules shown in equation 3.3.

3.3. In this exercise, $\mathcal{C}_n$ is a cyclic group of order n, $\mathcal{D}_n$ is the n'th dihedral group, and $\mathcal{S}_n$ is the n'th symmetric group.

(a) Prove that $\mathcal{C}_2$ and $\mathcal{S}_2$ are isomorphic.
(b) Prove that $\mathcal{D}_3$ is isomorphic to $\mathcal{S}_3$.
(c) Let $m \ge 3$. Prove that for every n, the groups $\mathcal{C}_m$ and $\mathcal{S}_n$ are not isomorphic.
(d) Prove that for every $n \ge 4$, the groups $\mathcal{D}_n$ and $\mathcal{S}_n$ are not isomorphic.
(e) More generally, let $m \ge 4$ and let $n \ge 4$. Prove the groups $\mathcal{D}_m$ and $\mathcal{S}_n$ are not isomorphic.
(f) The dihedral group $\mathcal{D}_4$ (Example 2.7) and the quaternion group $\mathcal{Q}$ (Example 2.8) are non-abelian groups of order 8. Prove that they are not isomorphic. (*Hint*. How many elements of order 2 and order 4 are there in $\mathcal{D}_4$ and $\mathcal{Q}$?)

3.4. Let $\mathrm{GL}_2(\mathbb{R})$ be the general linear group as described in Example 2.6 and Exercise 2.6(a). Prove or disprove that each of the following subsets of $\mathrm{GL}_2(\mathbb{R})$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. In the case of non-subgroups, indicate which of the subgroup conditions fail.

(a) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : ad - bc = 2 \right\}$.
(b) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : ad - bc \in \{-1, 1\} \right\}$.
(c) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : c = 0 \right\}$.

(d) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : d = 0 \right\}$.

(e) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : a = d = 1 \text{ and } c = 0 \right\}$.

3.5. Let $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ be the group that we defined in Exercise 2.8.

(a) Prove that $\#\,\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = 6$.

(b) Prove that $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to the symmetric group $\mathcal{S}_3$. (*Hint*. Show that the matrices in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ permute the vectors in the set $\big\{(1,0),(0,1),(1,1)\big\}$, where the coordinates of the vectors are viewed as numbers modulo 2.)

3.6. Let G be a cyclic group of order n, and let d be an integer that divides n. Prove that G has a subgroup of order d.

3.7. Let G be a group, and let $H \subset G$ be a subset of G. Prove that H is a subgroup if and only if it has the following two properties:

(1) $H \neq \emptyset$

(2) For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2^{-1}$ is in H.

Chapter 4

Abstract Algebra — Lecture #4

4.1 Equivalence Relations

Review of Material From Math 750 Unit #1

It is often convenient to split a set into a union of disjoint subsets, and then to view the elements in each subset as being "identical" or "equivalent". For example, consider the set of animals

$$S = \{\text{cat, lizard, dog, ant, elephant, whale, trout, mosquito, eagle}\}.$$

We can write S as a disjoint union

$$S = \underbrace{\{\text{cat, dog, elephant, whale, eagle}\}}_{\text{mammal}} \cup \underbrace{\{\text{lizard, ant, trout, mosquito}\}}_{\text{non-mammal}}.$$

For some purposes it might be convenient to treat the elements of each subset as being identical. This gives a new set whose elements are "equivalence classes" of elements of the original set,

$$\{\text{mammal, non-mammal}\},$$

where "mammal" is iteslf a set containing 5 elements and "non-mammal" is a set containing 4 elements. Note that there are other decomposition, for example we could decompose S as

$$S = \underbrace{\{\text{eagle, mosquito}\}}_{\text{flyer}} \cup \underbrace{\{\text{cat, dog, elephant, lizard, ant}\}}_{\text{walker}} \cup \underbrace{\{\text{whale, trout}\}}_{\text{swimmer}},$$

leading to the set of equivalence classes

$$\{\text{flyers, walkers, swimmers}\}.$$

We formalize this idea, which leads to a key concept that will be frequently used in the remainder of this book.

Definition. Let S be a set, and let $S_1, \ldots, S_n$ be subsets of S. We say that S is the *disjoint union of* $S_1, \ldots, S_n$ if

$$S = S_1 \cup \cdots \cup S_n \quad \text{and} \quad S_i cap S_j = \emptyset \text{ for every } i \neq j.$$

In other words, the set S is the disjoint union of the subsets $S_1, \ldots, S_n$ if every element of S is in exactly one of the subsets.

As described earlier, if S is the disjoint union of $S_1, \ldots, S_n$, then it is then often convenient to view the elements in each S_i as being equivalent to one another. Turning this around, we start with a set S and describe properties that "equivalence" should have.

Definition. Let S be a set. An *equivlaence relation on* S is a map

$$R : S \times S \longrightarrow \{0, 1\}$$

satisfying certain axioms that we'll get to in a minute. But the intuition is that elements $a, b \in S$ are "equivalent" if $R(a, b) = 1$, and they are "inequivalent" (not equivalent) if $R(a, b) = 0$, so R should be viewed as a test function that checks whether a and b are equivalent. We write

$$\begin{aligned} a \sim b \quad &\text{if } R(a, b) = 1, \\ a \not\sim b \quad &\text{if } R(a, b) = 0. \end{aligned}$$

With this $\sim$ notation, the three axioms that are required for R to be an equivalence relation are as follows:

$a \sim a$ for all $a \in S$.	**Reflexive Property**
$a \sim b \Longleftrightarrow b \sim a$ for all $a, b \in S$.	**Symmetry Property**
$a \sim b$ and $b \sim c \Longrightarrow a \sim c$ for all $a, b, c \in S$.	**Transitive Property**

Example 4.1. Let $m \geq 1$ be an integer. We define a relation on the set of integers by saying that

$$a \sim b \quad \text{if } a - b \text{ is an integer multiple of } m.$$

We claim that this is an equivalence relation. The reflexive property is easy, since $a - a = 0 \cdot m$. The symmetry property is also easy, since if $a \sim b$, then $a - b = k \cdot m$ for some integer k, so $b - a = (-k) \cdot m$ is also a multiple of m, and hence $b \sim a$. Finally, to check the transitive property, we suppose that $a \sim b$ and $b \sim c$. This means that $a - b = k \cdot m$ and $b - c = j \cdot m$ for some integers j and k. Adding these equations gives

$$a - c = (a - b) + (b - c) = k \cdot m + j \cdot m = (k + j) \cdot m,$$

which shows that $a \sim c$.

The following result is **very important**. It is used in a myriad of situations to count the size of a set, sometimes in more than one way.

Theorem 4.2. *Let S be a set and let $\sim$ be an equivalence relation on S. For each $a \in S$, let S_a be the set of elements that are equivalent to a, i.e.,*

$$S_a = \{b \in S : b \sim a\}.$$

We say that the set S_a is the equivalence class of a.

(a) *Let $a_1, a_2 \in S$. Then either*

$$S_{a_1} = S_{a_2} \quad \textit{or} \quad S_{a_1} \cap S_{a_2} = \emptyset.$$

(b) *Let $a_1, \ldots, a_n \in S$ be elements so that the equivalence classes $S_{a_1}, \ldots, S_{a_n}$ are pairwise disjiont, i.e., $S_{a_i} \cap S_{a_j} = \emptyset$ for all $i \neq j$. Then*

$$S = S_{a_1} \cup \cdots \cup S_{a_n} \quad \textit{is a disjoint union.}$$

In particular, if S is finite, then

$$\#S = \#S_{a_1} + \cdots + \#S_{a_n}.$$

Proof. (a) If $S_{a_1} \cap S_{a_2} = \emptyset$, then we're done, so we may assume that there is at least one element

$$b \in S_{a_1} \cap S_{a_2}.$$

The fact that $b \in S_{a_1}$ means that b is equivalent to a_1, and similarly the fact that $b \in S_{a_2}$ means that b is equivalent to a_2. This allows us to make the following chain of deductions to show that a_1 is equivalent to a_2:

$$\begin{aligned} b \sim a_1 \text{ and } b &\sim a_2 && \text{since } b \in S_{a_1} \text{ and } b \in S_{a_2}, \\ a_1 \sim b \quad \text{and } b &\sim a_2 && \text{symmetry property}, \\ a_1 &\sim a_2 && \text{transitive property}. \end{aligned}$$

Our next goal is to show that $S_{a_1} \subseteq S_{a_2}$, so we take an arbitrary element $c \in S_{a_1}$ and we need to prove that $c \in S_{a_2}$. We prove this as follows:

$$\begin{aligned} c &\in S_{a_1} && \text{starting assumption}, \\ c &\sim a_1 && \text{since } c \in S_{a_1}, \\ a_1 &\sim a_2 && \text{we proved this earlier}, \\ c &\sim a_2 && \text{transitive property using previous two lines}, \\ c &\in S_{a_2} && \text{from the definition of } S_{a_2}. \end{aligned}$$

This completes the proof of the inclusion $S_{a_1} \subseteq S_{a_2}$. And we can prove the opposite inclusion $S_{a_2} \subseteq S_{a_1}$ by reversing the roles of a_1 and a_2 in the above proof. Therefore $S_{a_2} = S_{a_1}$, which completes the proof of (a).

(b) Let $c \in S$. The reflexive property says that $c \sim c$, so $c \in S_c$, which shows that every $c \in S$ is in at least one equivalence class. But (a) says that c cannot be in more than one equivalence class, since if $c \in S_{a_1} \cap S_{a_2}$, then S_{a_1} and S_{a_2} have a common element, so (a) tells us that $S_{a_1} = S_{a_2}$. Hence every $c \in S$ is in exactly one equivalence class, which is just another way of saying that S is equal to the disjoint union of the distinct equivalence classes. This proves the first part of (b), and the second part follows immediately, since the number of elements in a disjoint union of finite sets is the sum of the number of elements in each set. □

4.2 Cosets and Lagrange's Theorem

We are going to use a subgroup H of G to break G into pieces that are called cosets of H.

Definition. Let G be a group, and let $H \subset G$ be a subgroup of G. For each $g \in G$, the (left) *coset of H attached to g* is the set

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

In other words, gH is the set that we get when we multiply g by every element of H.

We now prove several properties of cosets which help explain why they're important.

Proposition 4.3. *Let G be a finite group, and let $H \subset G$ be a subgroup of G.*
(a) *Every element of G is in some coset of H.*
(b) *Every coset of H has the same number of elements.*
(c) *Let $g_1, g_2 \in G$. Then the cosets g_1H and g_2H satisfy either*

$$g_1H = g_2H \quad \textit{or} \quad g_1H \cap g_2H = \emptyset.$$

Using set-theoretic terminology, this says that cosets of H are either equal or disjoint

Proof. (a) This is easy. Let $g \in G$. The subgroup H contains the identity element e, so the coset gH contains $g \cdot e = g$.
(b) Let $g \in G$. We are going to prove that the cosets gH and H have the same number of elements by proving that the map

$$F : H \longrightarrow gH, \quad F(h) = gh,$$

is a bijective map from H to gH.

We first check that F is injective. Suppose that $h_1, h_2 \in H$ satisfy $F(h_1) = F(h_2)$. This means that $gh_1 = gh_2$, and multiplying by g^{-1} on the left shows that $h_1 = h_2$. Hence F is injective.

We next check that F is surjective. Every element of gH looks like gh for some $h \in H$, and $F(h) = gh$, so every element of gH is the image of an element of H. Hence F is surjective.

We have now proven that $F : H \to gH$ is bijective, so in particular H and gH have the same number of elements. Since this is true for every $g \in G$, we conclude that every coset of H has the same number of elements.
(c) If $g_1H \cap g_2H = \emptyset$, we are done, so assume the two cosets are not disjoint. This means we can find elements $h_1, h_2 \in H$ satisfying $g_1h_1 = g_2h_2$. We rewrite this as $g_1 = g_2h_2h_1^{-1}$. Now take any element $g \in g_1H$. We need to show that g is also in g_2H. We write g as $g = g_1h$ for some $h \in H$. Then

$$g = g_1h = g_2h_2h_1^{-1}h \in g_2H,$$

since the assumption that H is a subgroup ensures that the product $h_2h_1^{-1}h$ is in H. This shows that every element of g_1H is in g_2H, and a similar argument shows the reverse inclusion. Alternatively, we can use the fact from (b) that g_1H and g_2H have the same number of elements, so if one is a subset of the other, they must be equal. □

We are now going to use the properties of cosets proven in Proposition 4.3 to derive a fundamental divisibility property for the orders of subgroups.

Theorem 4.4 (Lagrange's Theorem)**.** *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.*

Proof. We start by choosing elements $g_1, \ldots, g_k \in G$ so that $g_1H, \ldots, g_kH$ is a list of all of the different cosets of H. Proposition 4.3(a) tells us that every element of G is in some coset of H, so G is equal to the union

$$G = g_1H \cup g_2H \cup \cdots \cup g_kH. \tag{4.1}$$

On the other hand, Proposition 4.3(c) tells us that distinct cosets have no elements in common, i.e., if $i \neq j$, then $g_iH \cap g_jH = \emptyset$. Thus the union in (4.1) is a disjoint union, so the number of elements in G is the sum of the number of elements in the cosets,

$$\#G = \#g_1H + \#g_2H + \cdots + \#g_kH. \tag{4.2}$$

We next invoke Proposition 4.3(b), which tells us that every coset has the same number of elements, so in particular, $\#g_iH = \#eH = \#H$. Using this fact in (4.2) yields

$$\#G = k\#H.$$

Thus the order of G is a multiple of the order of H, which completes the proof of Lagrange's theorem. □

Corollary 4.5. *Let G be a finite group, and let $g \in G$. Then the order of g divides the order of G.*

Proof. The order of the subgroup $\langle g \rangle$ generated by G is equal to the order of the element g, and Theorem 4.4 tells us that the order of $\langle g \rangle$ divides the order of G. □

We give one application of Lagrange's theorem. It marks the starting line of a long and ongoing mathematical journey that strives to classify finite groups according to their orders.

Proposition 4.6. *Let p be a prime, and let G be a finite group of order p. Then G is isomorphic to the cyclic group $\mathcal{C}_p$.*

Proof. Since $p \geq 2$, we know that G contains more than just the identity element, so we choose some non-identity element $g \in G$. Lagrange's theorem (Theorem 4.4) tells us that the order of the subgroup $\langle g \rangle$ generated by g divides the order of G. But $\#G = p$ is prime, so $\#\langle g \rangle$ equals 1 or p, and we know that it doesn't equal 1,

since $\langle g\rangle$ contains e and g. Hence $\#\langle g\rangle = p = \#G$. Thus the subgroup has the same number of elements as the full group, so they are equal, $G = \langle g\rangle$. Writing the cyclic group $\mathcal{C}_p$ as $\mathcal{C}_p = \{g_0, g_1, g_2, \ldots, g_{p-1}\}$, with group law as described in Example 2.4, we obtain an isomorphism

$$\mathcal{C}_p \longrightarrow G, \quad g_i \longmapsto g^i.$$

This completes the proof of the proposition. □

Mini-Remark 6. The vast theory of finite groups includes many fascinating, and frequently unexpected, results whose proofs are unfortunately beyond the scope of these notes. To whet your appetite for studying more group theory, we state two such theorems.

Theorem 4.7. *Let p be a prime number, and let G be a group of order p^2. Then G is an abelian group.*

On the other hand, we know that there exist non-abelian groups of order p^3. For example, the dihedral group $\mathcal{D}_4$ (Example 2.7) and the quaternion group $\mathcal{Q}$ (Example 2.8) are non-abelian groups of order 8. The next result is an important partial converse to Lagrange's theorem.

Theorem 4.8 (Sylow's Theorem)**.** *Let G be a group, let p be a prime, and suppose that p^n divides $\#G$ for some power $n \ge 1$. Then G has a subgroup of order p^n.*

One might hope, more generally, that if d is any number that divides the order of G, then G has a subgroup of order d. Unfortunately, this is not true, although we have not yet seen a group that is a counterexample.

Exercises

4.1. Rewrite the three axioms for an equivalence relation (Definition 4.1) in terms of the map $R : S \times S \to \{0, 1\}$.

4.2. Which of the following are equivalence relations on the set of integers $\mathbb{Z}$? For the equivalence relations, describe the distinct equivalence classes, and for the non-equivalence relations, explain which of the three properties of an equivalence relation fail.

(a) $a \sim b$ if $a - b$ is a multiple of 5.
(b) $a \sim b$ if $a + b$ is a multiple of 5.
(c) $a \sim b$ if $a^2 - b^2$ is a multiple of 5.
(d) $a \sim b$ if $a - b^2$ is a multiple of 5.
(e) $a \sim b$ if $a - b$ is purple.

4.3. Let S be the set $S = \{1, 2, 3, 4, 6, 8, 9\}$, and define an equivalence relation on S by the rule

$$a \sim b \quad \text{if and only if} \quad a - b \text{ is even.} \tag{4.3}$$

(a) Prove that (4.3) is an equivalence relation on S. More generally, prove that it is an equivalence relation on $\mathbb{Z}$.

(b) Write S as a disjoint union of the equivalence classes for the equivalence relation (4.3).

4.4. This exercise provides a converse to Theorem 4.2. Let S be a set, and suppose that we have written $S = S_1 \cup S_2 \cup \cdots \cup S_n$ as a disjoint union of subsets. For $a, b \in S$, define

$$a \sim b \quad \text{if } a \text{ and } b \text{ are in the same } S_i.$$

(a) Prove that $\sim$ is an equivalence relation.
(b) Since $\sim$ is an equivalence relation, Theorem 4.2 says that it decomposes S into a disjoint union of subsets. Show that this is exactly the disjoint union that we started with.

4.5. This exercise explains when two elements of G determine the same coset of H. Let G be a group, let H be a subgroup of G, and let $g_1, g_2 \in G$. Prove that the following three statements are equivalent:
(1) $g_1H = g_2H$.
(2) There is an element $h \in H$ such that $g_1 = g_2h$.
(3) $g_2^{-1}g_1 \in H$.

4.6. Let G be a finite group whose only subgroups are $\{e\}$ and G. Prove that either $G = \{e\}$, or else G is a cyclic group whose order is a prime.

4.7. Let G be a group and $H \subset G$ a subgroup. The *index of H in G*, which is denoted by $(G : H)$, is the quantity $\#G/\#H$.
(a) Prove that $(G : H)$ is the number of distinct cosets of H.
(b) Suppose that $K \subset H$ is a subgroup of H, so we may also view K as a subgroup of G. In other words, $K \subset H \subset G$ is a chain of subgroups. Prove the *Index Multiplication Rule*

$$(G : K) = (G : H)(H : K).$$

(*Hint*. Count cosets.)

Chapter 5

Abstract Algebra — Lecture #5

5.1 Normal Subgroups and Quotient Groups

Let G be a group, and let H be a subgroup of G. We have seen in Section 4.2 that it is interesting and useful to decompose G into a disjoint union of cosets

$$G = C_1 \cup C_2 \cup \cdots \cup C_k,$$

where each C_i has the form $C_i = g_i H$. But we have written the cosets using the notation C_i, because for a given coset C, there are lots of different elements $g \in G$ with $C = gH$. Indeed, one can easily check that if C is a coset of H, then

$$C = gH \quad \Longleftrightarrow \quad g \in C.$$

Here's an interesting thought. Suppose that we try to turn the collection of cosets $\{C_1, \ldots, C_k\}$ into a group! How should we define the product of two cosests C_i and C_j? The obvious choice is to take the coset for the product of an element from C_i and an element of C_j.

Definition. Let G be a group, let H be a subgroup of G, and let C_1 and C_2 be cosets of H. Define the *product of* C_1 *and* C_2 by the rule

$$C_1 \cdot C_2 = g_1 g_2 H, \quad \text{where we take any } g_1 \in C_1 \text{ and any } g_2 \in C_2.$$

Is this a good definition? The following example says that it is not!

Example 5.1. Let $G = \mathcal{S}_3$, and let $H = \big\{e, (1,2)\big\}$. The cosets of H are

$$\begin{aligned} C_1 &= H, \\ C_2 &= (1,3)H = \big\{(1,3), (1,2,3)\big\}, \\ C_3 &= (2,3)H = \big\{(2,3), (1,3,2)\big\}. \end{aligned}$$

So to "multiply" the cosets C_2 and C_3 using Definition 5.1, we could choose $(1,3) \in C_2$ and $(2,3) \in C_3$ to get the product

$$(1,3)\cdot(2,3) = (1,3,2) \in C_3, \quad \text{so} \quad C_2 \cdot C_3 = C_3.$$

But if we instead choose $(1,2,3) \in C_2$ and $(1,3,2) \in C_3$, then we get

$$(1,2,3)\cdot(1,3,2) = (1)(2)(3) = e \in H, \quad \text{so} \quad C_2 \cdot C_3 = C_1.$$

Oops! The rule given in Definition 5.1 for computing the product of C_1 and C_2 is not well-defined, since different choices of $g_1 \in C_1$ and $g_2 \in C_2$ may lead to different product cosets g_1g_2H. That's annoying!

However, you can check that the rule does work if we use the cosets of $H = \big\{e, (1,2,3), (1,3,2)\big\} \subset \mathcal{S}_3$. So the definition seems to work for some subgroups, but not for others. How can we distinguish which are the "good" subgroups?

We want the group G and subgroup H to have the following property:

> Let C_1 and C_2 be cosets of H, let $g_1, g_1' \in C_1$, and let $g_2, g_2' \in C_2$. Then
> $$g_1g_2H = g_1'g_2'H.$$

The assumption that g_1 and g_1' are in the same coset C_1 of H means that there is some $h_1 \in H$ with $g_1' = g_1h_1$, and similarly $g_2' = g_2h_2$ for some $h_2 \in H$. So we want

$$g_1' = g_1h_1 \quad \text{and} \quad g_2' = g_2h_2 \quad \Longrightarrow \quad g_2^{-1}g_1^{-1}g_1'g_2' \in H.$$

Substituting the values of g_1' and g_2', we want

$$g_2^{-1}g_1^{-1}g_1h_1g_2h_2 \in H \quad \text{for all } g_1, g_2 \in G \text{ and all } h_1, h_2 \in H.$$

Happily, there's a bit of cancelation, so we want

$$g_2^{-1}h_1g_2h_2 \in H \quad \text{for all } g_2 \in G \text{ and all } h_1, h_2 \in H.$$

But we know that $gh_2 \in H$ if and only if $g \in H$, so we end up with

$$g_2^{-1}h_1g_2 \in H \quad \text{for all } g_2 \in G \text{ and all } h_1 \in H.$$

Dropping the subscripts, we have been lead naturally to the following definition.

Definition. Let G be a group, let $H \subset G$ be a subgroup, and let $g \in G$. The *g-conjugate of H* is the subgroup

$$g^{-1}Hg = \{g^{-1}hg : g \in G\}.$$

We say that H is a *normal subgroup of G* if it satisfies

$$g^{-1}Hg = H \quad \text{for every } g \in G.$$

Proposition 5.2. *Let G be a group, let $H \subset G$ be a subgroup, and let $g \in G$.*
(a) *The conjugate $g^{-1}Hg$ is a subgroup of G*

(b) *The map $H \to g^{-1}Hg$ defined by $h \mapsto g^{-1}hg$ is an group isomorphism.*

Proof. Left as an exercise. □

Proposition 5.3. *Let $\phi : G \to G'$ be a homomorphism of groups. Then $\ker(\phi)$ is a normal subgroup of G.*

Proof. We already know from Proposition 3.10(a) that $\ker(\phi)$ is a subgroup of G. Let $h \in \ker(\phi)$ and $g \in G$. Then

$$\begin{aligned}
\phi(g^{-1} \cdot h \cdot g) &= \phi(g^{-1}) \cdot \phi(h) \cdot \phi(g) && \text{homomorphism property of } \phi,\\
&= \phi(g)^{-1} \cdot \phi(h) \cdot \phi(g) && \text{Proposition 3.1(b)},\\
&= \phi(g)^{-1} \cdot \phi(g) && \text{since } h \in \ker(\phi),\\
&= e'.
\end{aligned}$$

Hence $g^{-1} \cdot h \cdot g \in \ker(\phi)$. We have proven that this is true for all $h \in \ker(\phi)$ and all $g \in G$, which completes the proof that $\ker(\phi)$ is a normal subgroup of G. □

We now turn Proposition 5.3 on its head and use a given normal subgroup $H \subset G$ to create a group G' and a group homomorphism $\phi : G \to G'$ with the property that $\ker(\phi) = H$. We do this as indicated earlier using the (left) cosets of H, i.e., the sets of the form

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

It is convenient to have a notation for the set of cosets.

Definition. Let G be a group, and let H be a subgroup of G. We denote the set of cosets of G by

$$G/H = \{\text{cosets of } H\}.$$

Definition 5.1 gives the natural way try to make G/H into a group, namely by defining a group law on cosets via the rule

$$g_1H \cdot g_2H = g_1g_2H. \tag{5.1}$$

But as we have seen, there is a serious potential problem, since although every coset of H has the form gH, there are lots of choices for g that give the same coset. Indeed, if $h \in H$ is any element of H, then $hH = H$, so $ghH = gH$.[1] So in (5.1), if we choose different elements g_1 and g_2 of G that give the same cosets, how do we know that we get the same product coset? The answer is that in general, we do not get the same product. ☹ However, if H is a *normal* subgroup of G, then darkness turns to light ☺, and we do get the same product coset, as we now verify.

[1] Exercise 4.5 says that the converse is also true, i.e., if $g_1H = g_2H$, then there is an $h \in H$ such that $g_1 = g_2h$.

Lemma 5.4. *Let G be a group, and let H be a normal subgroup of G. Let $g_1, g_1', g_2, g_2' \in G$ be elements of G satisfying*

$$g_1'H = g_1H \quad \textit{and} \quad g_2'H = g_2H.$$

Then

$$g_1'g_2'H = g_1g_2H.$$

Proof. The assumption that $g_1'H = g_1H$ implies that there is an $h_1 \in H$ such that $g_1' = g_1h_1$. (This assertion is part of Exercise 4.5, but it is very easy. Here is the short proof: $g_1' = g_1' \cdot e \in g_1'H = g_1H$.) Similarly the assumption that $g_2'H = g_2H$ implies that there is an $h_2 \in H$ such that $g_2' = g_2h_2$.

Let $g_1'g_2'h$ be an element of $g_1'g_2'H$. We want to show that $g_1'g_2'h$ is in g_1g_2H. To do this, we compute

$$\begin{aligned}
g_1'g_2'h &= g_1h_1g_2h_2h && \text{since } g_1' = g_1h_1 \text{ and } g_2' = g_2h_2,\\
&= g_1(g_2g_2^{-1})h_1g_2h_2h && \text{inserting } g_2g_2^{-1} = e \text{ doesn't change the value,}\\
&= g_1g_2(g_2^{-1}h_1g_2)h_2h && \text{associative law of group multiplication,}\\
&\in g_1g_2H && \text{the normality of } H \text{ tells us that } g_2^{-1}h_1g_2 \in H, \text{ so}\\
& && g_2^{-1}h_1g_2 \cdot h_2 \cdot h \text{ is a product of three elements of}\\
& && H, \text{ and thus is in } H.
\end{aligned}$$

Since this is true for every $h \in H$, we have proven that

$$g_1'g_2'H \subseteq g_1g_2H.$$

Reversing the roles of g_1, g_2 and g_1', g_2' gives the opposite inclusion. This completes the proof that $g_1'g_2'H = g_1g_2H$. □

The content of Lemma 5.4 is that the multiplication rule $g_1H \cdot g_2H = g_1g_2H$ on cosets of H is well-defined provided we take H to be a normal subgroup of G. The following properties of coset multiplication then follow directly from the corresponding properties of the group operation on G:

$$\begin{aligned}
eH \cdot gH = gH \cdot eH = gH,\\
gH \cdot g^{-1}H = g^{-1}H \cdot gH = eH,\\
(g_1H \cdot g_2H) \cdot g_3H = g_1H \cdot (g_2H \cdot g_3H).
\end{aligned}$$

We have proven the first part the following important theorem.

Theorem 5.5. *Let G be a group, and let H be a normal subgroup of G.*

(a) *The collection of cosets G/H is a group via the well-defined group operation*

$$g_1H \cdot g_2H = g_1g_2H. \tag{5.2}$$

(b) *The map*

$$\phi : G \longrightarrow G/H, \quad \phi(g) = gH,$$

is a homomorphism whose kernel is $\ker(\phi) = H$.

(c) *Let*

$$\psi : G \longrightarrow G'$$

be a homomorphism with the property that $H \subset \ker(\psi)$*. Then there is a unique homomorphism*

$$\lambda : G/H \longrightarrow G' \quad \textit{satisfying} \quad \lambda(gH) = \psi(g).$$

Proof. (a) The fact that the group operation (5.2) is well-defined is exactly what Lemma 5.4 says, and as we noted earlier, the group axioms for G/H follow immediately from the groups axioms for G.
(b) In order to check that ϕ is a homomorphism, we compute

$$\phi(g_1)\phi(g_2) = g_1H \cdot g_2H = g_1g_2H = \phi(g_1g_2).$$

The kernel of ϕ is

$$\ker(\phi) = \big\{g \in G : \phi(g) = eH\big\} = \big\{g \in G : gH = H\big\} = H.$$

(c) We would like to define $\lambda : G/H \to G'$ by the following three-step algorithm:

(1) Let $C \in G/H$ be a coset.

(2) Choose some $g \in G$ with $C = gH$

(3) Define $\lambda(C)$ to be $\psi(g)$.

However, there is a potential problem, since there are usually lots of choices for g in Step (2). So we need to prove the following assertion:

$$\text{If} \quad g'H = gH, \quad \text{then} \quad \psi(g') = \psi(g). \tag{5.3}$$

The assumption that $g'H = gH$ means that $g' = gh$ for some $h \in H$. This allows us to compute

$$\begin{aligned}
\psi(g') &= \psi(gh) && \text{since } g' = gh,\\
&= \psi(g) \cdot \psi(h) && \text{since } \psi \text{ is a group homomorphism,}\\
&= \psi(g) \cdot e' && \text{since } h \in H \text{ and } H \subset \ker(\psi),\\
&= \psi(g).
\end{aligned}$$

This proves assertion (5.3), so our three-step algorithm gives a well-defined map $\lambda : G/H \to G'$. And now that we know that λ is well-defined, it's easy to check that it is a homomorphism,

$$\lambda(g_1g_2H) = \psi(g_1g_2) = \psi(g_1) \cdot \psi(g_2) = \lambda(g_1H) \cdot \lambda(g_2H).$$

Finally for a given homomorphism ψ, it is clear that there is only one map λ satisfying $\psi(g) = \lambda(gH)$, since this equality completely determines the values of λ in terms of the values of ψ. □

Exercises

5.1. (a) Let H be the subgroup of $\mathcal{S}_3$ generated by $\pi = (1,2,3)$. Write down the elements of H. Describe the conjugate subgroups $g^{-1}Hg$ of H. How many are there? Is H a normal subgroup?
(b) Same question for the subgroup of $\mathcal{S}_3$ generated by $\pi = (1,2)$.
(c) Same question for the subgroup of $\mathcal{S}_4$ generated by $\pi = (1,2,3,4)$.
(d) Same question for the subgroup of $\mathcal{S}_4$ generated by $\pi = (1,2)(3,4)$.

5.2. Let $\psi : G \to G'$ be a homomorphism of groups.
(a) Prove that the image $\psi(G) = \big\{\psi(g) : g \in G\big\}$ is a subgroup of G'.
(b) Suppose that G is a finite group. Prove that

$$\#G = \#\psi(G) \cdot \#\ker(\psi).$$

5.3. In the dihedral group $\mathcal{D}_n$, let R be a clockwise rotation by $2\pi/n$ radians, and let F be a flip.
(a) Prove that the subgroup $\{e, R, R^2, \ldots, R^{n-1}\}$ is a normal subgroup of $\mathcal{D}_n$
(b) Prove that the subgroup $\{e, F\}$ is not a normal subgroup.

5.4. Let $\mathcal{Q} = \{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}$ be the group of quaternions; see Example 2.8. Prove that every subgroup of $\mathcal{Q}$ is a normal subgroup.

5.5. Let G be a group, and let $H \subset G$ be a subgroup of index 2, i.e., there are exactly two cosets of H. Prove that H is a normal subgroup of G. (*Hint*. For every $g \in G$, prove that the left coset gH is equal to the right coset Hg.)

5.6. Let G be a group, let $H \subset G$ and $K \subset G$ be subgroups, and assume that K is a normal subgroup of G.
(a) Prove that $HK = \{hk : h \in H,\ k \in K\}$ is a subgroup of G.
(b) Prove that $H \cap K$ is a normal subgroup of H, and that K is a normal subgroup of HK.
(c) Prove that HK/K is isomorphic to $H/(H \cap K)$. (*Hint*. What is the kernel of the surjective homoorphism $H \to HK/K$?)
(d) Rather than assuming that K is a normal subgroup, suppose that we only assume that $H \subset N(K)$, i.e., we assume that H is contained in the normalizer of K. Prove that (a), (b), and (c) are true.

5.7. Let G be a group, let $K \subseteq H \subseteq G$ be subgroups, and assume that K is a normal subgroup of G.
(a) Prove that H/K is naturally a subgroup of G/K.
(b) Conversely, prove that every subgroup of G/K looks like H/K for some subgroup H satisfying $K \subseteq H \subseteq G$.
(c) Prove that H is a normal subgroup of G if and only if H/K is a normal subgroup of G/K.
(d) If H is a normal subgroup of G, prove that

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

(*Hint*. What is the kernel of the surjective homomorphism $G/K \to G/H$?)

Chapter 6

Abstract Algebra — Lecture #6

6.1 Introduction to Rings

When we introduced groups in Section 1.2, they were probably unfamiliar to most of you. In this chapter we introduce another fundamental type of algebraic object, called a *ring*. The good news is that you are already familiar with many rings. Here are some examples:

- The integers $\mathbb{Z}$ are a ring.
- The rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are rings. (They are a special type of ring, called a field, but that's a topic for a later.)
- The set of mod m integers $\mathbb{Z}/m\mathbb{Z}$ that you studied in the Number Theory Unit forms a ring.

What do these examples have in common? They each have two operations, addition and multiplication. These operations, individually, satisfy some axioms, and the two operations interact via one further axiom, the great and powerful distributive law,

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

In general, a ring is a set with two operations satisfying a bunch of axioms that are modeled after the properties satisfied by addition and multiplication of integers.

6.2 Abstract Rings and Ring Homomorphisms

Definition. A *ring* R is a set with two operations, generally called *addition* and *multiplication* and written

$$\underbrace{a+b}_{\text{addition}} \quad \text{and} \quad \underbrace{a \cdot b \text{ or } ab}_{\text{multiplication}},$$

satisfying the following axioms:

(1) The set R with its addition law $+$ is an abelian group. The identity element of this group is denoted 0 or 0_R.
(2) The set R with its multiplication law $\cdot$ is almost a group, but its elements are not required to have inverses.[1] Explicitly, the multiplication law of a ring satisfies:
   - There is an element $1_R \in R$ satisfying[2]
$$1_R \cdot a = a \cdot 1_R = a \quad \text{for all } a \in R.$$
   - The associative law holds,
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{for all } a, b, c \in R.$$
(3) [Distributive Law] For all $a, b, c \in R$ we have
$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$
(4) If further $a \cdot b = b \cdot a$ for all $a, b \in R$, then the ring is said to be *commutative*.

Your long experience with the ring of integers $\mathbb{Z}$ might lead you to assume that various "obvious" formulas are true in every ring. For example, the formulas
$$0_R \cdot a = 0_R \quad \text{and} \quad (-a) \cdot (-b) = a \cdot b$$
must be true, right? But why should they be true? The definition of 0_R is as the identity element for *addition*, i.e., $a + 0_R = 0_R + a = a$ for every $a \in R$, so why should that tell us anything about 0_R when we switch to *multiplication*? Similarly, the defintion of $-a$ is as the element that gives 0_R when it is *added* to a, which seems to tell us very little about the *product* of $-a$ with other elements of R. The only hope of proving multiplication properties for 0_R and $-a$ lies in the distributive law, which intertwines addition and multiplication. Study closely the use of the distributive law in the following proof that $0_R \cdot a = 0_R$.

Proposition 6.1. *Let R be a ring.*
(a) $0_R \cdot a = 0_R$ *for all $a \in R$.*
(b) $(-a) \cdot (-b) = a \cdot b$ *for all $a, b \in R$. In particular, we have $(-1_R) \cdot a = -a$.*

Proof. (a) We start with $1_R = 1_R + 0_R$, which is true because 0_R is the identity for addition. We multiply both sides by a and compute

$$\begin{aligned}
a &= a \cdot 1_R && \text{since } 1_R \text{ is the identity for multiplication,} \\
&= a \cdot (1_R + 0_R) && \text{since } 0_R \text{ is the identity for addition,} \\
&= a \cdot 1_R + a \cdot 0_R && \text{distributive law,} \\
&= a + a \cdot 0_R && \text{since } 1_R \text{ is the identity for multiplication.}
\end{aligned}$$

[1] For those who are interested, algebraic objects that are like groups except that not every element needs to have an inverse also have a name; they are called *monoids*.

[2] To avoid the trivial ring consisting of a single element, we also include the requirement that $1_R \neq 0_R$.

We now "subtract" a from both sides. But this one time we will spell out every detail so that you can see how the different ring axioms come into play:

$$\begin{aligned}
0_R &= (-a) + a && \text{definition of inverse for addition,}\\
&= (-a) + (a + a \cdot 0_R) && \text{from our earlier calculation,}\\
&= \big((-a) + a\big) + a \cdot 0_R && \text{associativity of addition,}\\
&= 0_R + a \cdot 0_R && \text{definition of inverse for addition,}\\
&= a \cdot 0_R && \text{since } 0_R \text{ is the identity for addition.}
\end{aligned}$$

(b) We leave this part for you to do; see Exercise 6.1. □

Just as we did with groups, we want to look at maps

$$\phi : R \to R'$$

between rings that respects the "*ring-i-ness*" of R and R'. Rings are characterized by their addition and multiplication laws, leading to the following definition.

Definition. Let R and R' be rings. A *ring homomorphism from R to R'* is a function $\phi : R \to R'$ satisfying

$$\begin{aligned}
\phi(1_R) &= 1_{R'},\\
\phi(a+b) &= \phi(a) + \phi(b) \quad \text{for all } a, b \in R,\\
\phi(a \cdot b) &= \phi(a) \cdot \phi(b) \quad \text{for all } a, b \in R.
\end{aligned}$$

The *kernel of ϕ* is the set of elements that is sent to 0,,

$$\ker(\phi) = \big\{a \in R : \phi(a) = 0\big\}.$$

(The zero here is, of course, the zero element in R'.)

As with groups, we say that R and R' are *isomorphic* if there is a bijective homomorphism $\phi : R \to R'$, and we call such a map ϕ an *isomorphism*.

In the next section, after we have a few more examples of ring, we will give some examples of ring homomorphisms.

Remark 6.2. The axiom $\phi(1_R) = 1_{R'}$ is included to rule out the boring and trivial map $\phi(a) = 0_{R'}$ that sends every $a \in R$ to zero.

6.3 Ring and More Rings: Examples

Example 6.3 ($\mathbb{Z}$**,** $\mathbb{Q}$**,** $\mathbb{R}$**,** $\mathbb{C}$**: Four rings that you already know**). The integers, rational numbers, real numbers, and complex numbers are rings, and they fit one into another, sort of like Russian stacking dolls:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

We say that $\mathbb{Z}$ is a *subring* of $\mathbb{Q}$, and similarly for the others.

Example 6.4 (**The RIng $\mathbb{Z}/\mathbb{Z}$ of Integers Modulo m**). The other ring that we mentioned in the introduction is $\mathbb{Z}/m\mathbb{Z}$, the ring of integers modulo m. The ring $\mathbb{Z}/m\mathbb{Z}$ is not a subring of $\mathbb{C}$, but there is a homomorphism

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad \phi(a) = a \bmod m,$$

called naturally enough the *reduction mod m homomorphism*. This homomorphism sends an integer to its congruence class modulo m, and its kernel is the set of all multiples of m. The fact that ϕ is a homomorphism means checking that reduction modulo m behaves well for addition and multiplication, facts that you saw in the Number Theory Unit.

Example 6.5 (**Gaussian Integers $\mathbb{Z}[i]$**). Here is another interesting subring of $\mathbb{C}$. It is called the *ring of Gaussian integers*.

$$\mathbb{Z}[i] = \bigl\{a + bi : a, b \in \mathbb{Z}\bigr\}.$$

The quantity i is, as usual, a symbol that represents a square root of -1. Addition and multiplication of elements in $\mathbb{Z}[i]$ follow the usual rules for adding and multiplying complex numbers,

$$\begin{aligned}(a_1 + b_1 i) + (a_2 + b_2 i) &= (a_1 + a_2) + (b_1 + b_2)i,\\ (a_1 + b_1 i) \cdot (a_2 + b_2 i) &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i.\end{aligned}$$

Note that if we allowed a and b to be real numbers, then we would get the entire ring of complex numbers; but we're restricting a and b to be integers.

Example 6.6 (**Polynomial Rings $R[x]$**). Polynomial rings are a way to create a bigger (and better?) ring from a given ring. Thus for any commutative ring R, we use R to build the *ring of polynomials over R*,

$$R[x] = \left\{\begin{matrix}\text{polynomials } a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \text{ of all}\\ \text{degrees with coefficients } a_0, a_1, \ldots, a_d \in R\end{matrix}\right\}.$$

You've undoubtedly seen polynomials whose coefficients are real numbers, but the rules that you learned to add and multiply polynomials work with coefficients in any commutative ring. Indeed, the rule for multiplying polynomials is forced on you by the distributive law. Here's a simple example:

$$\begin{aligned}&(a_0 + a_1 x + a_2 x^2) \cdot (b_0 + b_1 x)\\ &\qquad = a_0 \cdot (b_0 + b_1 x) + a_1 x \cdot (b_0 + b_1 x) + a_2 x^2 \cdot (b_0 + b_1 x)\\ &\qquad = (a_0 b_0 + a_0 b_1 x) + (a_1 b_0 x + a_1 b_1 x^2) + (a_2 b_0 x^2 + a_2 b_1 x^3)\\ &\qquad = a_0 b_0 + (a_1 b_1 + a_1 b_0)x + (a_1 b_1 + a_2 b_0)x^2 + (a_2 b_1)x^3.\end{aligned}$$

Definition (The Degree of a Polynomial). Let $f(x) \in R[x]$ be a non-zero polynomial. If we write $f(x)$ as

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \quad \text{with } a_d \neq 0,$$

then the *degree of* $f(x)$ is d. In other words,

$$\deg(f) = \text{exponent of the largest power of } x \text{ appearing in } f(x).$$

Notice that the non-zero elements of R have degree 0, while $0 \in R$ is not assigned a degree.[3]

Example 6.7 (**The Evaluation Homomorphism**). Let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d \in R[x]$$

be a polynomial. Then for any element $c \in R$, we can *evaluate* f *at* c simply by substituting c for x. Thus

$$f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_dc^d \in R.$$

In other classes you probably took a polynomial $f(x)$ and evaluated it at lots of different values. In other words, you viewed $f(x)$ as defining a function

$$f : R \to R.$$

Although this function can be interesting, it function is almost never a ring homomorphism!

We are going to take a different approach. We choose one particular element $c \in R$ and use it to define a function from the ring of polynomials $R[x]$ to the ring R. We denote this function E_c and call it the *evalaution at* c *map*. It is defined exactly as its name suggests,

$$E_c : R[x] \longrightarrow R, \quad E_c(f) = f(c).$$

The evaluation by c map is a ring homomorphism, as you will verify in Exercise 6.8, and its kernel is exactly the set of polynomials that have a factor of $x - c$.

Example 6.8 (**Ring of Quarternions** $\mathbb{H}$). We next describe a famous non-commutative ring, called the *ring of quaternions*,[4]

$$\mathbb{H} = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} : a, b, c, d \in \mathbb{R}\}.$$

The quantities $\boldsymbol{i}$, $\boldsymbol{j}$, and $\boldsymbol{k}$ are three different square roots of -1, and although we specify that they commute with elements of $\mathbb{R}$, they do not commute with one another. More precisely, the rule for multipying two quaternions is to use the distributative law to reduce to multiplying pairs of $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$, and then applying the following rules:

$$\boldsymbol{i}^2 = -1, \quad \boldsymbol{j}^2 = -1, \quad \boldsymbol{k}^2 = -1, \quad \boldsymbol{i} \cdot \boldsymbol{j} = \boldsymbol{k}, \quad \boldsymbol{j} \cdot \boldsymbol{k} = \boldsymbol{i}, \quad \boldsymbol{k} \cdot \boldsymbol{i} = \boldsymbol{j}.$$

To see that $\mathbb{H}$ is a noncommutative ring, we compute

[3] Sometimes people say that $\deg(0) = -\infty$, which is a quantity that is smaller than very real number.

[4] The letter $\mathbb{H}$ to denote the ring of quaternions is in honor of William Hamilton, who first described them in 1843.

$$-\boldsymbol{j}\cdot\boldsymbol{i} = \boldsymbol{j}\cdot(-1)\cdot\boldsymbol{i} = \boldsymbol{j}\cdot\boldsymbol{k}^2\cdot\boldsymbol{i} = (\boldsymbol{j}\cdot\boldsymbol{k})\cdot(\boldsymbol{k}\cdot\boldsymbol{i}) = \boldsymbol{i}\cdot\boldsymbol{j}.$$

Thus $\boldsymbol{j}\cdot\boldsymbol{i} = -\boldsymbol{i}\cdot\boldsymbol{j}$, and one can similarly check that $\boldsymbol{k}\cdot\boldsymbol{i} = -\boldsymbol{i}\cdot\boldsymbol{k}$ and $\boldsymbol{k}\cdot\boldsymbol{j} = -\boldsymbol{j}\cdot\boldsymbol{k}$.

The ring of quaternions $\mathbb{H}$ played an important role in the development of modern mathematics and physics because it satisfies the so-called *cancellation law*. Thus you know that if α and β are real numbers satisfying $\alpha\cdot\beta = 0$, then either $\alpha = 0$ or $\beta = 0$, and similarly when α and β are complex numbers. It turns out that the same is true if α and β are quaternions! See Exercise 6.15.

Exercises

6.1. Let R be a ring, and let $a, b, \in R$. Prove that

$$(-a)\cdot(-b) = a\cdot b.$$

Be sure to justify each step of your proof by using either a definition or a ring axiom, as we did in our proof of Proposition 6.1(a). This is Proposition 6.1(b).

6.2. Let $\phi : R \to R'$ be a ring homomorphism. Prove that

$$\phi \text{ is injective if and only if } \ker(\phi) = \{0\}.$$

(*Hint*. See Proposition 3.10 for a similar result for groups.)

6.3. Let R be a ring.

(a) Suppose that the map

$$f : R \longrightarrow R, \quad f(a) = a^2,$$

is a ring homomorphism. Prove that $1_R + 1_R = 0_R$. In less fancy notation, prove that $2 = 0$ in the ring R.

(b) Let p be a prime. Suppose that R is a commutative ring in which $p = 0$. Prove that the map

$$f : R \longrightarrow R, \quad f(a) = a^p,$$

is a ring homomorphism. (*Hint*. Use the binomial theorem.)

6.4. Let $m \ge 1$ be an integer, and define a map

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad \phi(a) = a \bmod m.$$

In other words, the map ϕ sends an integer to its congruence class modulo m. Prove that ϕ is a ring homomorphism.

6.5. (a) Let 7 and 11 be elements of the ring $\mathbb{Z}/17\mathbb{Z}$. Compute $\alpha+\beta$ and $\alpha\cdot\beta$.

(b) Let $2 + 4x$ and $1 + 4x + 3x^2$ be elements of the polynomial ring $(\mathbb{Z}/7\mathbb{Z})[x]$. Compute $\alpha+\beta$ and $\alpha\cdot\beta$.

(c) Let $\alpha = 3 + 2i$ and $\beta = 2 - 3i$ be elements of the ring of Gaussian integers $\mathbb{Z}[i]$. Compute $\alpha+\beta$ and $\alpha\cdot\beta$.

(d) Let $\alpha = 3 + 2x - x^2$ and $\beta = 2 - 3x + x^2$ be elements of the polyomial ring $\mathbb{Z}[x]$. Compute $\alpha+\beta$ and $\alpha\cdot\beta$.

(e) Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers, and let $\alpha = (1+i) + (2-i)x - x^2$ and $\beta = (2+i) + (1+3i)x$ be elements of the polynomial ring $R[x]$. Compute $\alpha + \beta$ and $\alpha \cdot \beta$.

(f) Let $\alpha = 1 + 2\boldsymbol{i} - \boldsymbol{j} + \boldsymbol{k}$ and $\beta = 2 - \boldsymbol{i} + 3\boldsymbol{j} - \boldsymbol{k}$ be elements of the ring $\mathbb{H}$ of quaternions. Compute $\alpha + \beta$ and $\alpha \cdot \beta$.

6.6. We have already seen the ring of Gaussian integers $\mathbb{Z}[i]$. More generally, for any integer D that is not the square of an integer,[5] we can form a ring

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}.$$

If $D > 0$, then $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{R}$, while if $D < 0$, then in any case it is a subring of $\mathbb{C}$.

(a) Let $\alpha = 2 + 3\sqrt{5}$ and $\beta = 1 - 2\sqrt{5}$ be elements of $\mathbb{Z}[\sqrt{5}]$. Compute the quantities

$$\alpha + \beta, \quad \alpha \cdot \beta, \quad \alpha^2.$$

(b) Prove that the map

$$\phi : \mathbb{Z}[\sqrt{D}] \longrightarrow \mathbb{Z}[\sqrt{D}], \quad \phi(a + b\sqrt{D}) = a - b\sqrt{D}$$

is a ring homomorphism. (For notational convenience, for $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, people often write $\overline{\alpha} = a - b\sqrt{D}$, similar to the notation for complex conjugation.)

(c) With notation as in (b), prove that

$$\alpha \cdot \overline{\alpha} \in \mathbb{Z} \quad \text{for every } \alpha \in \mathbb{Z}[\sqrt{D}].$$

6.7. Let ρ be the complex number $\rho = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$, and let

$$\mathbb{Z}[\rho] = \{a + b\rho : a, b, \in \mathbb{Z}\}.$$

(a) Prove that $\mathbb{Z}[\rho]$ is a subring of $\mathbb{C}$. (The key here is to prove that if you add or multiply two elements of $\mathbb{Z}[\rho]$, you get back an element of $\mathbb{Z}[\rho]$.)

(b) Prove that $\rho^3 = 1$. Thus ρ is a cube root of unity.

(c) Prove that the polynomial $X^3 - 1$ factors as

$$X^3 - 1 = (X - 1)(X - \rho)(X - \rho^2).$$

6.8. Let R be a commutative ring, let $c \in R$, and let $E_c : R[x] \to R$ be the evaluation map $E_c(f) = f(c)$.

(a) Prove that E_c is a ring homomorphism.

(b) Prove that $E_c(f) = 0$ if and only if there is a polynomial $g(x) \in R[x]$ satisfying $f(x) = (x - c)g(x)$, i.e., prove that $\ker(E_c)$ is the set of multiples of $x - c$.

6.9. Prove that the map

$$\mathbb{C} \hookrightarrow M_2(\mathbb{R}), \quad x + yi \longmapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix},$$

is an injective ring homomorphism.

[5] We rule out the case the D is a square, because if $D = d^2$, then $\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[d] = \mathbb{Z}$, so we don't get an interesting new ring.

6.10. For any ring R, let

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$$

be the set of 2-by-2 matrices with entries in R. Define addition by adding the corresponding entries, and define multiplication as described by (2.1) in Example 2.6.

(a) Prove that $M_2(R)$ is a ring.

(b) Prove that $M_2(R)$ is non-commutative.

(c) Find non-zero elements $A, B \in M_2(R)$ such that $AB = 0$. (In the terminology of Section 7.1, the elements A and B are zero divisors, and $M_2(R)$ is not an integral domain.)

(d) Prove that a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has a multiplicative inverse if and only if $ad - bc$ has a multiplicative inverse in R.

(e) For those who have taken a class in linear algebra, generalize (a), (b), and (c) to $M_n(R)$, the set of n-by-n matrices with entries in R.

6.11. Let R be a commutative ring. We consider the ring of polynomials in two variables[6] with coefficients in R,

$$R[x, y] = \{a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \cdots : a_{ij} \in R\}.$$

In other words, an element of $R[x, y]$ is a sum of the form

$$f(x, y) = \sum_{k=0}^{n} \sum_{i=0}^{k} a_{i,k-i} x^i y^{k-i}.$$

(a) Let $f(x, y) = 3 + 2x - y + x^2 + xy$ and $g(x, y) = 1 - x + 3y - xy + 2y^2$ be elements of the ring $\mathbb{Z}[x, y]$. Compute $f + g$ and $f \cdot g$.

(b) Same question as in (a), except suppose that f and g are in the ring $(\mathbb{Z}/4\mathbb{Z})[x, y]$.

(c) For $b, c \in R$, define an evaluation map

$$E_{b,c} : R[x, y] \longrightarrow R, \quad E_{b,c}\big(f(x, y)\big) = f(b, c).$$

Prove that $E_{b,c}$ is a ring homomorphism.

6.12. Let R be a commutative ring, and let $f(x) =\in R[x]$ be a polynomial with coefficients in R. We define the *formal derivative* $f'(x)$ *of* $f(x)$ by writing $f(x)$ as

$$f(x) = \sum_{k=0}^{n} a_k x^k \quad \text{and setting} \quad f'(x) = \sum_{k=0}^{n} k a_k x^{k-1}.$$

Note that there is no limit being taken, so the formal derivatie makes sense even if, for example, R is a ring such as $\mathbb{Z}/m\mathbb{Z}$. It also means that when doing this exericse, you'll need to directly use the definition of $f'(x)$, since you can't rely on the proofs from calculus.

(a) Let $f(x), g(x) \in R[x]$. Prove that $(f + g)'(x) = f'(x) + g'(x)$.

(b) Let $f(x), g(x) \in R[x]$. Prove that $(f \cdot g)'(x) = f(x)g'(x) + g(x)f'(x)$.

(c) Let $f(x), g(x) \in R[x]$. Prove that the formal derivative of $f\big(g(x)\big)$ is $f'\big(g(x)\big)g'(x)$.

[6] We leave it to you to generalize to polynomials in more variables, if you want.

6.13. Let R be a commutative ring. The *group of units of* R is the subset R^* of R defined by

$$R^* = \{a \in R : \text{there is some } b \in R \text{ satisfying } ab = 1\}.$$

Prove that R^* is a group, where we use multiplication for the group law.

6.14. For a commutative ring R, we let R^* denote the group of units of R as defined in Exercise 6.13.

(a) Prove that $\mathbb{Z}^* = \{-1, 1\}$.
(b) Prove that $\mathbb{Q}^* = \{a \in \mathbb{Q} : a \neq 0\}$.
(c) Prove that $\mathbb{Z}[i]^* = \{-1, 1, i, -i\}$.
(d) Consider the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Prove that $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$. Prove that the powers of $1 + \sqrt{2}$, that is, the numbers $(1 + \sqrt{2})^n$ for $n = 1, 2, 3, \ldots$, are all different, and use that fact to deduce that $\mathbb{Z}[\sqrt{2}]^*$ has infinitely many elements.
(e) Prove that $\mathbb{R}[x]^* = \mathbb{R}^*$, i.e., the only polynomials in $\mathbb{R}[x]$ that have multiplicative inverses are the non-zero constants.
(f) Prove that $1 + 2x$ is a unit in the ring $(\mathbb{Z}/4\mathbb{Z})[x]$ of polynomials with coefficients in the ring $\mathbb{Z}/4\mathbb{Z}$. (*Challenge*: Describe the complete unit group $(\mathbb{Z}/4\mathbb{Z})[x]^*$.)

6.15. For a quaternion $\alpha = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \in \mathbb{H}$, we let $\overline{\alpha} = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$.

(a) Prove that $\alpha\overline{\alpha} \in \mathbb{R}$.
(b) Prove that $\alpha\overline{\alpha} = 0$ if and only if $\alpha = 0$.
(c) Suppose that $\alpha, \beta \in \mathbb{H}$ and that $\alpha\beta = 0$. Prove that either $\alpha = 0$ or $\beta = 0$.

Chapter 7

Abstract Algebra — Lecture #7

7.1 Zero Divisors, Integral Domains, and Fields

Rings come in many different shapes and sizes. Some rings have certain properties that make them especially nice. In this section we are going to discuss two such properties.

The first comes from looking at the rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. These rings have the special property that every non-zero element has a multiplicative inverse. This type of ring is so important that it has its own special name.

Definition. A *field* is a commutative ring R with the property that every non-zero element of R has a multiplicative inverse. In other words, a commutative ring R is a field if and only if for every $a \in R$ with $a \neq 0$ there is a $b \in R$ satisfying $ab = 1$.

Example 7.1. In addition to the fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ that we already mentioned, we note that for every prime p, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field. It is an example of a *finite field*, and is frequently denoted $\mathbb{F}_p$ to emphasize its "fieldiness." The fact that $\mathbb{F}_p$ is a field follows from the Linear Congruence Theorem that we proved in the Number Theory Unit. To see why, take any non-zero element $a \in \mathbb{Z}/p\mathbb{Z}$. Then $\gcd(a, p) = 1$, so the Linear Congruence Theorem says that the congruence

$$ax \equiv 1 \pmod{p}$$

has exactly one solution in $\mathbb{Z}/p\mathbb{Z}$. That solution is precisely a multiplicative inverse of a.

There are, of course, lots and lots of rings that are not fields. For example, the rings $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{R}[x]$ are not fields. But these rings do have the following nice property, which is very useful for solving equations.

Cancellation Property: Let R be a commutative ring. We say that R has the *cancellation property* if for every choice of $a, b, c \in R$, the following implication is true:

$$ab = ac \text{ and } a \neq 0 \quad \Longleftrightarrow \quad b = c.$$

Definition. Let R be a ring. An element $a \in R$ is called a *zero divisor* if $a \neq 0$ and there is some non-zero $b \in R$ such that $ab = 0$. A commutative ring R that has no zero divisors is called an *integral domain*. Equivalently, a commutative ring R is an integral domain if the only way to get $ab = 0$ is to have either $a = 0$ or $b = 0$.

It is easy to check that every field is an integral domain, and that a ring R is an integral domain if and only if it has the cancellation property; see Exercises 7.1 and 7.3. There are also lots of rings that are not integral domains, for example

$$\mathbb{Z}/6\mathbb{Z} \text{ is not an integral domain, since } 2 \cdot 3 = 0.$$

7.2 Fun and Games with Polynomial Rings

We start with a fundamental question:

How many roots may a polynomial have?

If R is a ring and $a_1, a_2, \ldots, a_d \in R$ are distinct elements of R, then the polynomial

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_d)$$

has degree d, and it clearly has (at least) d distinct roots in R, since

$$f(a_1) = f(a_2) = \cdots = f(a_d) = 0.$$

Can a degree d polynomial have more than d distinct roots? Seems unlikely. But when we start to look at examples, everything goes to hell!

For example,

$$R = \mathbb{Z}/8\mathbb{Z}, \quad f(x) = x^2 - 1 \in R[x], \quad f(1) = f(3) = f(5) = f(7) = 0.$$

So here we have a polynomial of degree 2 that has 4 distinct roots. Maybe the problem is that this ring R has a nilpotent element, since $2^3 = 0$?

Nope, that's not the problem, since

$$R = \mathbb{Z}/6\mathbb{Z}, \quad f(x) = x^2 + x \in R[x], \quad f(0) = f(2) = f(3) = f(5) = 0.$$

Again we have a polynomial of degree 2 with 4 distinct roots, and this ring R doesn't have nilpotent elements. But it does have zero divisors, since $2 \cdot 3 = 0$. Is that the issue?

Let's see. The ring of quaternions $\mathbb{H}$ in Example 6.8 has no zero divisors (see Exercise 6.15), but

$$R = \mathbb{H}, \quad f(x) = x^2 + 1 \in R[x], \quad f(\boldsymbol{i}) = f(\boldsymbol{j}) = f(\boldsymbol{k}) = 0.$$

So $f(x)$ has degree 2 and at least 3 roots in R. And with more work, one can find even more roots, for example you can check that

$$\left(\frac{1 + 2\boldsymbol{j} + 2\boldsymbol{k}}{3}\right)^2 + 1 = 0.$$

Could the problem be that the ring R is non-commutative?

These examples tell us some of the types of rings that we should avoid. They also illustrate why the following important theorem is not nearly as obvious as it looks.

Theorem 7.2. *Let R be a commutative ring with no zero divisors, and let $f(x) \in R[x]$ be a non-zero polynomial. Then*

$$\#\big\{a \in R : f(a) = 0\big\} \le \deg f.$$

A key tool used in the proof of Theoerm 7.2 is the next lemma, which says that if $f(c) = 0$, then $f(x)$ has a factor of $x - c$. It is interesting to observe that Lemma 7.3 is true for all commutative rings R, although as we've seen, Theorem 7.2 need not be true if R has zero divisors.

Lemma 7.3. *Let R be a commutative ring, let $f(x) \in R[x]$ be a polynomial, and suppose that $c \in R$ is a root of $f(x)$, i.e., suppose that $f(c) = 0$. Then there is a polynomial $g(x) \in R[x]$ so that $f(x)$ factors as*

$$f(x) = (x - c)g(x).$$

Proof. We write $f(x)$ as

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d = \sum_{i=0}^{d} a_ix^i \quad \text{with } a_0, a_1, \ldots, a_d \in R.$$

We are assuming that $f(c) = 0$, so we can subtract $f(c)$ without changing the value,

$$f(x) = f(x) - f(c) = \sum_{i=0}^{d} a_ix^i - \sum_{i=0}^{d} a_ic^i = \sum_{i=0}^{d} a_i(x^i - c^i). \tag{7.1}$$

We observe that each of the $x^i - c^i$ terms can be factored, for example

$$\begin{aligned}
x - c &= (x - c) \cdot 1, \\
x^2 - c^2 &= (x - c) \cdot (x + c), \\
x^3 - c^3 &= (x - c) \cdot (x^2 + xc + c^2), \\
x^4 - c^4 &= (x - c) \cdot (x^3 + x^2c + cx^2 + c^3).
\end{aligned}$$

Do you see the pattern? We can prove the desired formula as follows:

$$\begin{aligned}
&(x-c)\cdot(x^{i-1}+x^{i-2}c+x^{i-3}c^2+\cdots+x^2c^{i-3}+xc^{i-2}+c^{i-1})\\
&\qquad=x\cdot(x^{i-1}+x^{i-2}c+x^{i-3}c^2+\cdots+x^2c^{i-3}+xc^{i-2}+c^{i-1})\\
&\qquad\qquad-c\cdot(x^{i-1}+x^{i-2}c+x^{i-3}c^2+\cdots+x^2c^{i-3}+xc^{i-2}+c^{i-1})\\
&\qquad=(x^i+x^{i-1}c+x^{i-2}c^2+\cdots+x^3c^{i-3}+x^2c^{i-2}+xc^{i-1})\\
&\qquad\qquad-(x^{i-1}c+x^{i-2}c^2+x^{i-3}c^3+\cdots+x^2c^{i-2}+xc^{i-1}+c^i)\\
&\qquad=x^i-c^i,\quad\text{because all of the other terms cancel!}
\end{aligned}$$

We have shown that for every integer $i \ge 0$, there is a polynomial $h_i(x) \in R[x]$ satisfying

$$x^i - c^i = (x-c)h_i(x). \tag{7.2}$$

Using (7.2) in (7.1) gives

$$f(x) = f(x)-f(c) = \sum_{i=0}^{d} a_i(x^i-c^i) = \sum_{i=0}^{d} \underbrace{a_i(x-c)h_i(x)}_{\text{Using (7.2).}} = (x-c)\underbrace{\sum_{i=0}^{d} a_i h_i(x)}_{\text{This is our } g(x).}.$$

This completes the proof that we can factor $f(x)$ as $(x-c)$ times some polynomial in $R[x]$. □

We're now ready to prove that a polynomial of degree d has at most d roots in a commutative ring with no zero divisors. As we do the proof, keep a sharp lookout for where we use the "no zero divisors" condition, since if we don't use it somewhere, then the proof could not be correct.

Proof of Theorem 7.2. We are going to use induction on n to prove the following statement:

> **Statement(n)**: Let $f(x) \in R[x]$ be a non-zero polynomial, and let $\alpha_1,\ldots,\alpha_n \in F$ be distinct roots of $f(x)$. Then there is a polynomial $g(x) \in R[x]$ such that $f(x)$ factors as
>
> $$f(x) = (x-\alpha_1)\cdots(x-\alpha_n)g(x). \tag{7.3}$$

We start our induction proof of **Statement(n)** with the case $n = 1$. So we let α_1 be a root of $f(x)$. Then Lemma 7.3 says that we can find a polynomial $g_1(x) \in R[x]$ so that

$$f(x) = (x-a_1)g_1(x).$$

This completes the proof in the case that $n = 1$.

Suppose next that we know that **Statement(n)** is true for $\alpha_1,\ldots,\alpha_n$. Let $\beta \in R$ be a new root of $f(x)$ that is distinct from $\alpha_1,\ldots,\alpha_n$. Then

$$0 = f(\beta) = (\beta - \alpha_1)\cdots(\beta - \alpha_n)g(\beta).$$

All of the $\beta - \alpha_i$ are non-zero, and we are working in a ring R that has no zero-divisors, so we deduce that $g(\beta) = 0$. Applying Lemma 7.3 to $g(x)$, we find that

$$g(x) = (x - \beta)h(x) \quad \text{for some } h(x) \in R[x].$$

Hence

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_n)g(x) = (x - \alpha_1)\cdots(x - \alpha_n)(x - \beta)h(x),$$

which proves that **Statement$(n+1)$** is true.

We now know that **Statement(n)** is true for all $n \ge 1$. We let $d = \deg(f)$ and $e = \deg(g)$, which lets us write

$$f(x) = ax^d + (\text{terms of lower degree}) \quad \text{and} \quad g(x) = bx^e + (\text{terms of lower degree})$$

for some non-zero a and b. Substituting these into (7.3) and expanding the product gives

$$\begin{aligned} f(x) &= ax^d + (\text{terms of lower degree}) \\ &= (x - \alpha_1)\cdots(x - \alpha_n)\cdot g(x) \quad \text{from (7.3)}, \\ &= (x - \alpha_1)\cdots(x - \alpha_n)\cdot \big(bx^e + (\text{terms of lower degree})\big) \\ &= bx^{n+e} + (\text{terms of lower degree}). \end{aligned}$$

This proves that

$$\deg(f) = d = n + e \ge n,$$

which completes the proof of Theorem 7.2. □

Exercises

7.1. Let m be a positive integer.
(a) Prove that $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.
(b) Prove that $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

7.2. Let R be a field. Prove that R is an integral domain, i.e., prove that R does not have any zero divisors.

7.3. Let R be a ring. Prove that R is an integral domain if and only if it has the cancellation property.

7.4. Let R be a finite integral domain, i.e., R is an integral domain and it has finitely many elements. Prove that R is a field. (*Hint*. Let $a \in R$ with $a \ne 0$. Prove that the map

$$R \longrightarrow R, \quad b \longmapsto ab,$$

is injective, then that it is also surjective, and hence its image contains the element 1.)

7.5. Let R be a commutative ring.

(a) Prove that there is exactly one integral domain R such that the map

$$f : R \longrightarrow R, \quad f(a) = a^6,$$

is a ring homomorphism. (You'll need to use the fact that $1_R \neq 0_R$.)

(b) Find all integral domains R such that the map

$$f : R \longrightarrow R, \quad f(a) = a^{15},$$

is a ring homomorphism.

(c) For each of parts (a) and (b), find at least one ring that is not an integral domain for which the indicated map is a ring homomorphism.

(d) Let p and q be distinct primes. Characterize all integral domains R for which the map $f(a) = a^{pq}$ is a ring homomorphism. (*Author's Note*: I haven't worked out the solution to this problem.)

7.6. Suppose that R is a commutative ring that does have zero divisors. Prove that there is a polynomial $f(x) \in R[x]$ of that has more distinct roots in R than its degree.

Chapter 8

Abstract Algebra — Lecture #8

8.1 Unit Groups

The theme of this section is that lurking inside every ring is an interesting group.

Definition. Let R be a commutative ring.[1] The *group of units of* R is the subset R^* of R defined by

$$R^* = \{a \in R : \text{there is some } b \in R \text{ satisfying } ab = 1\},$$

where the group law is ring multiplication. The elements of R^* are called *units*.

Proposition 8.1. *The set of units R^* is a group with group law being ring multiplication.*

Proof. We first check that if $a_1, a_2 \in R^*$, then their product a_1a_2 is in R^*. From the definition of R^*, we can find $b_1, b_2 \in R^*$ satisfying $a_1b_1 = 1$ and $a_2b_2 = 1$. Then

$$(a_1a_2)(b_1b_2) = (a_1b_1)(a_2b_2) = 1 \cdot 1 = 1,$$

so $a_1a_2 \in R^*$. It remains to check the group axioms, but that's easy, since $1 \in R$ is the identity element, the existence of inverses is exactly what defines the elements of R^*, and the associative law for multiplication is one of the ring axioms. □

Example 8.2. The ring of integers $\mathbb{Z}$ and the ring of Gaussian integers $\mathbb{Z}[i]$ have finite unit groups,

$$\mathbb{Z}^* = \{\pm 1\} \quad \text{and} \quad \mathbb{Z}[i]^* = \{\pm 1 \pm i\}.$$

The ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ has infinite unit group, since $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$, and all of the power $(1 + \sqrt{2})^n$ are different. The unit group of the polynomial ring $\mathbb{R}[x]$ consists of the non-zero constant polynomials, i.e., $\mathbb{R}[x]^* = \mathbb{R}^*$. We leave the proofs of these assertions to you; see Exercise 8.1.

[1] For a non-commutative ring R, an element a is a *unit* if there are elements $b, c \in R$ such that $ab = ca = 1$, i.e., the element a needs a left-inverse and a right-inverse. See Exercise 8.4.

Example 8.3. A ring R is a field if and only if

$$R^* = \{a \in R : a \neq 0\}, \tag{8.1}$$

since (8.1) says exactly that every non-zero element of R has a multiplicative inverse.

The next example is sufficiently important to merit a formal statement and proof.

Proposition 8.4. *Let $m \geq 1$ be an integer. Then*

$$(\mathbb{Z}/m\mathbb{Z})^* = \big\{a \bmod m : \gcd(a,m) = 1\big\}.$$

In particular, if p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field, often denoted $\mathbb{F}_p$.

Proof. Suppose that $\gcd(a,m) = 1$. We know from the Number Theory Unit that we can find $u, v \in \mathbb{Z}$ satisfying $au + mv = 1$. Hence

$$au = 1 - mv \equiv 1 \pmod{m}.$$

Thus u is a multiplicative inverse for a in the ring $\mathbb{Z}/m\mathbb{Z}$, so $a \bmod m$ is in $(\mathbb{Z}/m\mathbb{Z})^*$.

For the other direction, suppose that $a \bmod m$ is in $(\mathbb{Z}/m\mathbb{Z})^*$. This means that we can find some $b \bmod m$ in $(\mathbb{Z}/m\mathbb{Z})^*$ so that

$$(a \bmod m) \cdot (b \bmod m) = 1 \bmod m \quad \text{in } (\mathbb{Z}/m\mathbb{Z})^*.$$

In other words, $ab \equiv 1 \pmod{m}$, so $ab - 1 = cm$ for some c. This equation shows that $\gcd(a,m) = 1$, since any number dividing both a and m also divides 1. □

Example 8.5. The first few cases of Proposition 8.4 are

$$(\mathbb{Z}/3\mathbb{Z})^* = \{1,2\},\ (\mathbb{Z}/4\mathbb{Z})^* = \{1,3\},\ (\mathbb{Z}/5\mathbb{Z})^* = \{1,2,3,4\},\ (\mathbb{Z}/6\mathbb{Z})^* = \{1,5\}.$$

The group $(\mathbb{Z}/5\mathbb{Z})^*$ has four elements, but we can say even more. Computing

$$2^2 \equiv 4 \pmod{5}, \quad 2^3 \equiv 3 \pmod{5}, \quad 2^4 \equiv 1 \pmod{5},$$

we see that $(\mathbb{Z}/5\mathbb{Z})^*$ is a cyclic group of order four.

8.2 Examples of Unit Groups

We will discuss the unit groups of some of the following rings in class, and you'll investigate others as homework:

1. (a) $\mathbb{Z}^*$. (b) $\mathbb{Q}^*$. (c) $\mathbb{Z}[i]^*$.
2. Describe the unit group of the ring

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

For example, show that $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$, and by taking powers, show that $\mathbb{Z}[\sqrt{2}]^*$ is an infinite group.

3. $\mathbb{R}[x]^*$, and more generally, $F[x]^*$ for any commutative field F.
4. $(\mathbb{Z}/4\mathbb{Z})[x]^*$. For example, show that $1 + 2x \in (\mathbb{Z}/4\mathbb{Z})[x]^*$. What are some other units in this ring? Try to describe all of the units.
5. $M_2(\mathbb{R})^*$, and more generally, $M_2(R)^*$ for any commutative ring R.

Challenge Problems

6. Let $D \in \mathbb{Z}$ be an integer that is not a perfect square. Describe the unit group of the ring
$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}.$$
(*Hint*. The cases $D > 0$ and $D < 0$ look very different.)
7. Let R be an arbitrary commutative ring. What does $R[x]^*$ look like?

Exercises

8.1. (a) Compute the unit group $\mathbb{Z}^*$.

(b) Compute the unit group $\mathbb{Q}^*$.

(c) Compute the unit group $\mathbb{Z}[i]^*$.

(d) Consider the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Prove that $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$. Prove that the powers of $1 + \sqrt{2}$, that is, the numbers $(1 + \sqrt{2})^n$ for $n = 1, 2, 3, \ldots$, are all different, and use that fact to deduce that $\mathbb{Z}[\sqrt{2}]^*$ has infinitely many elements. (*Challenge*: Prove that every element of $\mathbb{Z}[\sqrt{2}]^*$ has the form $\pm(1 + \sqrt{2})^n$ for some $n \in \mathbb{Z}$. You probably won't be able to solve this challenge problem, but it's well worth thinking about!)

(e) Prove that $\mathbb{R}[x]^* = \mathbb{R}^*$, i.e., the only polynomials in $\mathbb{R}[x]$ that have multiplicative inverses are the non-zero constants. Generalize to $F[x]^*$ for any field F.

(f) Prove that $1 + 2x$ is a unit in the ring $(\mathbb{Z}/4\mathbb{Z})[x]$ of polynomials with coefficients in the ring $\mathbb{Z}/4\mathbb{Z}$. (*Challenge*: Describe the complete unit group $(\mathbb{Z}/4\mathbb{Z})[x]^*$.)

(g) *Challenge Problem* Desecribe $R[x]^*$ for an arbitrary commutative ring R.

(h) Describe $M_2(\mathbb{R})^*$, and more generally, $M_2(R)^*$ for any commutative ring R.

8.2. (a) Let R be a commutative ring, and suppose that its unit group R^* is finite, say $n = \#R^*$. Prove that every element $a \in R$ satisfies
$$a^n = 1.$$
(*Hint*. Use Lagrange's theorem, more specifically Corollary 4.5.)

(b) Let p be a prime, and let $a \in \mathbb{Z}$ be an integer with $p \nmid a$. Use (a) to prove:

Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$.

(*Hint*. Consider the unit group of $\mathbb{Z}/p\mathbb{Z}$.)

8.3. The unit group $(\mathbb{Z}/p\mathbb{Z})^*$ of a finite field is always cyclic, although this is not so easy to prove! But there are lots of other rings with interesting unit groups.

(a) Are the following groups cyclic? If so, find a generator.

$$(\mathbb{Z}/4\mathbb{Z})^*, \quad (\mathbb{Z}/6\mathbb{Z})^*, \quad (\mathbb{Z}/8\mathbb{Z})^*, \quad (\mathbb{Z}/9\mathbb{Z})^*, \quad (\mathbb{Z}/15\mathbb{Z})^*.$$

From your small amount of data, can you make a conjecture about when $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic? In particular, if p is prime, when do you think that $(\mathbb{Z}/p^2\mathbb{Z})^*$ is cyclic?

(b) Let's turn the problem on its head. We know that $\mathbb{F}_p^*$ is cyclic for all primes p. Sometimes 2 is a generator of $\mathbb{F}_p^*$, sometimes it's not:
2 is a generator of $\mathbb{F}_p^*$ for $p = 3, 5, 11, 13, 19, 29, 37, 53, 59$.
2 is a not generator of $\mathbb{F}_p^*$ for $p = 7, 17, 23, 31, 41, 43, 47$.
Do you think that 2 is a generator of $\mathbb{F}_p^*$ for infinitely many primes p? How about 3? How about 4? Etc.

8.4. Let R be a non-commutative ring. The *group of* (*two-sides*) *units of* R is the following subset of R:

$$R^* = \{a \in R : \text{there are } b, c \in R \text{ satisfying } ab = ca = 1\}.$$

(a) If $ab = ca = 1$, prove that $b = c$.

(b) Prove that R^* is a group, where we use multiplication for the group law.

Chapter 9

Abstract Algebra — Lecture #9

9.1 Product Rings

The theme of this section is that we can build bigger, more complicated rings from smaller, simpler rings. Why, you may ask, would we want to make our life more more complicated? It's hard enough understanding things that aren't complicated! The answer is that eventually people use the process in reverse, i.e., they take a complicated ring and break it up into smaller, easier pieces.

The building procedure that we use is probably already familiar to you, since it's more-or-less the same as the way that the vector space $\mathbb{R}^n$ is built using n-tuples of elements of $\mathbb{R}$.

Definition. Let $R_1, \ldots, R_n$ be rings. The *product of* $R_1, \ldots, R_n$ is the ring

$$R_1 \times \cdots \times R_n = \big\{(a_1, \ldots, a_n) : a_1 \in R_1, \ldots, a_n \in R_n\big\}.$$

In other words, the product $R_1 \times \cdots \times R_n$ is the set of n-tuples, where the first entry is chosen from R_1, the second entry from R_2, etc. We make $R_1 \times \cdots \times R_n$ into a ring using coordinate-wise addition and multiplication,

$$\begin{aligned}(a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 + b_1, \ldots, a_n + b_n),\\ (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) &= (a_1 \cdot b_1, \ldots, a_n \cdot b_n).\end{aligned}$$

We leave it as an exercise to prove that $R_1 \times \cdots \times R_n$ is a ring; see Exercise 9.5.

Example 9.1. The product ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has 6 elements,

$$(0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2).$$

Some examples of addition and multiplication in the ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ are

$$(1,1) + (1,2) = (0,0) \quad \text{and} \quad (0,2) \cdot (1,2) = (0,1).$$

It turns out that the product ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}/6\mathbb{Z}$. This is a very special case of Theorem 9.3, which we prove later in this section.

Example 9.2. The product ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has 8 elements,

$$(0,0),\ (0,1),\ (0,2),\ (0,3),\ (1,0),\ (1,1),\ (1,2),\ (1,3).$$

It is not isomorphic to the ring $\mathbb{Z}/8\mathbb{Z}$. To see why, note that if $\phi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is a homomorphism, then $\phi(1) = (1,1)$ by definition, so

$$\begin{aligned}\phi(4) = \phi(1+1+1+1) &= \phi(1) + \phi(1) + \phi(1) + \phi(1) \\ &= (1,1) + (1,1) + (1,1) + (1,1) = (0,0).\end{aligned}$$

Thus $\phi(4) = \phi(0)$, so ϕ cannot be injective.

Theorem 9.3 (Chinese Remainder Theorem)**.** *Let m and n be positive integers satisfying $\gcd(m,n) = 1$. Then the homomorphism*

$$F : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad F(a \bmod mn) = \big(a \bmod m, a \bmod n\big),$$

is an isomorphism.

Proof. We first ask for the kernel of F. We have

$$\begin{aligned}F(a \bmod mn) = (0,0) \quad &\Longleftrightarrow \quad a \equiv 0 \pmod m \quad \text{and} \quad n \equiv 0 \pmod n \\ &\Longleftrightarrow \quad m \mid a \quad \text{and} \quad n \mid a \\ &\Longleftrightarrow \quad mn \mid a \quad \text{since } \gcd(m,n) = 1, \\ &\Longleftrightarrow \quad a = 0 \text{ in } \mathbb{Z}/mn\mathbb{Z}.\end{aligned}$$

This proves that $\ker(F) = \{0\}$, so Exercise 6.2, which is just an adaptation of Proposition 3.10, tells us that F is injective. On the other hand, we have

$$\#(\mathbb{Z}/mn\mathbb{Z}) = mn \quad \text{and} \quad \#(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = mn,$$

so F is an injective map between sets of the same finite cardinality. Therefore F is also surjective, so it is an isomorphism. □

Example 9.4 (The Chinese Remainder Theorem Reinterpreted)*.* The surjectivity of the map in Theorem 9.3 can be interpreted as follows: Assume that $\gcd(m,n) = 1$. Then for all $b, c \in \mathbb{Z}$, the simultaneous congruences

$$x \equiv b \pmod m \quad \text{and} \quad x \equiv c \pmod n \tag{9.1}$$

has a solution $x \in \mathbb{Z}$. This is the usual statement of the Chinese Remainder Theorem in elementary number theory textbooks. There are many generalizations, some of which you will investigate in the exercises.

Example 9.5. It is not hard to solve the system of congruences (9.1) in practice. We do an an example that illustrates the general technique. Supose that we want to solve

$$x \equiv 8 \pmod{11} \quad \text{and} \quad x \equiv 3 \pmod{17}. \tag{9.2}$$

It is easy to solve the first congruence, for example $x = 8$ is a solution. But there are many other solutions, such as $x = 19$ and $x = -3$. Indeed, we know that every solution to the first congruence looks like $x = 8 + 11y$ for some y. We exploit this flexibility by substituting $x = 8 + 11y$ into the second congruence, which yields

$$\begin{aligned} 8 + 11y &\equiv 3 \pmod{17}, \\ 11y &\equiv -5 \equiv 12 \pmod{17}. \end{aligned}$$

We know how to solve this sort of congruence, we just need to multiply both sides by the inverse of 11 modulo 17. Using the Euclidean algorithm, or just trial-and-error since the numbers are so small, we find that $14 \cdot 11 \equiv 1 \pmod{17}$, so

$$y \equiv 14 \cdot 11y \equiv 14 \cdot 12 \equiv 168 \equiv 15 \pmod{17}.$$

This gives $y = 15$ as a value for y, and substituing into $x = 8 + 11y$, we find that $x = 8 + 11 \cdot 15 = 173$ solves the simultaneous congruences (9.2).

The next result combines two themes: product rings and unit groups.

Proposition 9.6. *Let $R_1, \ldots, R_n$ be rings. Then the unit group of the product is isomorphic to the product of the unit groups, i.e.,*

$$(R_1 \times \cdots \times R_n)^* \cong R_1^* \times \cdots \times R_n^*.$$

Proof. If $(a_1, \ldots, a_n) \in (R_1 \times \cdots \times R_n)^*$, then by definition there is a $(b_1, \ldots, b_n) \in R_1 \times \cdots \times R_n$ satisfying

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (1, 1, \ldots, 1).$$

This means that $a_i b_i = 1$, so $a_i \in R_i^*$, and hence $(a_1, \ldots, a_n) \in R_1^* \times \cdots \times R_n^*$.

For the other direction, suppose that $(a_1, \ldots, a_n) \in R_1^* \times \cdots \times R_n^*$. This means that $a_i \in R_i^*$, so for each i we can find a $b_i \in R_i$ satisfying $a_i b_i = 1$. It follows that

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) \qquad = (1, 1, \ldots, 1).$$

Hence $(a_1, \ldots, a_n) \in (R_1 \times \cdots \times R_n)^*$. □

We can use the Chinese remainder theorem and properties of unit groups to give a quick proof of a beautiful multiplication formula.

Definition. The *Euler phi function* is the function on positive integers defined by

$$\phi(m) = \bigl\{0 \le a < m : \gcd(a, m) = 1\bigr\}.$$

Equivalently, from Proposition 8.4,

$$\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^*.$$

Example 9.7. The first few values of Euler's phi function are

$$\phi(1) = 1,\ \phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2,\ \phi(7) = 6.$$

Corollary 9.8. *Let $m, n \ge 1$ be positive integers satisfying $\gcd(m,n) = 1$. Then*

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. Theorem 9.3 tells us that there is a ring isomorphism

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Then Proposition 9.6 tells us that there is an isomorphism of unit groups

$$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*.$$

Counting the number of elements on each side yields

$$\begin{array}{ccccc} \#(\mathbb{Z}/mn\mathbb{Z})^* & = & \#(\mathbb{Z}/m\mathbb{Z})^* & \cdot & \#(\mathbb{Z}/n\mathbb{Z})^* \\ \uparrow & & \uparrow & & \uparrow \\ \text{this is } \phi(mn) & & \text{this is } \phi(m) & & \text{this is } \phi(n) \end{array}$$

Hence $\phi(mn) = \phi(m)\phi(n)$. □

See Exercise 9.4 for many additional properties of Euler's phi function.

Exercises

9.1. The first recorded instance of the Chinese Remainder Theorem appears in a Chinese mathematical work that is more than 1500 years old. Somewhat surprisingly, it deals with the harder problem of three simultaneous congruences.

> "We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"
> *Sun Tzu Suan Ching* (Master Sun's Mathematical Manual)
> Circa AD 300, volume 3, problem 26.

Solve Master Sun's problem.

9.2. Solve the following simultaneous congrunces.
(a) $x \equiv 3 \pmod 7$ and $x \equiv 5 \pmod{11}$.
(b) $x \equiv 37 \pmod{117}$ and $x \equiv 41 \pmod{119}$.
(c) $x \equiv 3 \pmod 7$ and $x \equiv 5 \pmod{11}$ and $x \equiv 7 \pmod{13}$.
(d) $x \equiv 3 \pmod 7$ and $x \equiv 5 \pmod{11}$ and $x \equiv 7 \pmod{13}$ and $x \equiv 11 \pmod{17}$.
(e) $2x \equiv 1 \pmod 3$ and $3x \equiv 2 \pmod 5$ and $5x \equiv 3 \pmod 7$.

9.3. Let $m_1, \ldots, m_r \in \mathbb{Z}$ be positive integers with the property that

$$\gcd(m_i, m_j) = 1 \quad \text{for all distinct indices } i \ne j.$$

Let $m = m_1 m_2 \cdots m_r$. Prove that the map

$$\begin{aligned}\phi : \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z},\\ a \bmod m &\longmapsto (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_r),\end{aligned}$$

is a ring isomorphism.

Restate the surjectivity in terms of simultaneous congruences, as we did in Example 9.4.

9.4. For this exericse, the function $\phi(n)$ is Euler's phi function.

(a) Let p be a prime. Prove that $\phi(p) = p - 1$.

(b) More generally, let p^e be a power of a prime and prove that $\phi(p^e) = p^e - p^{e-1}$. Is it true that $\phi(p^e) \stackrel{?}{=} \phi(p)^e$?

(c) Generalize Corollary 9.8 as follows. Suppose that $m_1, m_2, \ldots, m_r$ are positive integers satisfying $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Prove that

$$\phi(m_1 m_2 \cdots m_r) = \phi(m_1)\phi(m_2)\cdots\phi(m_r).$$

(d) Let $m \geq 1$. Prove that

$$\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right),$$

where the product is over the distinct primes that divide m.

9.5. Let $R_1, \ldots, R_n$ be rings. Prove that the product $R_1 \times \cdots \times R_n$, with addition and multiplication as given in Definition 9.1, is a ring.

Chapter 10

Abstract Algebra—Lecture #10+

Lecture 10???!!! What's that about? Math 760's Unit 5 only has 9 lectures. So the material in this chapter is for those who want to learn a bit more about rings on their own. If we had another week, these are topics that we would probably have discussed.

10.1 Ideals and Quotient Rings

Do you recall how we constructed the ring $\mathbb{Z}/m\mathbb{Z}$ of integer modulo m starting from the ring $\mathbb{Z}$? We simply pretended that that two integers a and b are "the same" if their difference $a - b$ is a multiple of m. In fancier language, we defined an equivalence relation on $\mathbb{Z}$ by the rule

$$a \text{ is equivalent to } b \text{ if } a - b \text{ is a multiple of } m,$$

and we then defined $\mathbb{Z}/m\mathbb{Z}$ to be the set of equivalence classes. Of course, it takes some work to check that addition and multiplication of equivalence classes makes sense.

Our goal in this section is to generalize this important construction to arbitrary (commutative) rings. The first step is the generalize the concept of being a "multiple of m."

Definition. Let R be a commutative ring. An *ideal* of R is a non-empty subset $I \subseteq R$ with the following two properties:

- If $a \in I$ and $b \in I$, then $a + b \in I$.
- If $a \in I$ and $r \in R$, then $ra \in I$.

One way to create an ideal is to start with some element of R and take all of its multiples.

Definition. Let R be a commutative ring and let $c \in R$. The *principal ideal generated by* c, denoted cR or (c), is the set of all multiples of c,

$$cR = \{rc : r \in R\}.$$

We let you verify that cR is an ideal; see Exercise 10.1.

In some rings, such as $\mathbb{Z}$ and $\mathbb{Z}[i]$ and $\mathbb{R}[x]$, every ideal is a principal ideal, although it requires real work to prove that these assertions are valid. On the other hand, there are rings such as $\mathbb{Z}[x]$ that have non-principal ideals; see Exercise 10.7.

We now create a quotient ring R/I by identifying pairs of elements of R if their difference is in I, just as we did when we defined $\mathbb{Z}/m\mathbb{Z}$. We note that for a given $a \in R$, the set of $b \in R$ that are equivalent to a consists of the set of b such that $b-a \in I$, or equivalently, such that b is in the set that is naturally denoted by $a + I$. This prompts the following definitions.

Definition. Let R be a commutative ring, and let I be an ideal of R. Then for each element $a \in R$, the *coset of* a is the set

$$a + I = \{a + c : c \in I\}.$$

We note that a is an element of its coset, since $0 \in I$. If $a, b \in R$ satisfy $b - a \in I$, then people sometimes write

$$b \equiv a \pmod{I}$$

and say that "b is congruent to a modulo I." Given two cosets $a + I$ and $b + I$, we define their sum and product by the formulas

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = (a \cdot b) + I,$$

and we denote the collection of distinct cosets by R/I.

We now check that our definitions of addition and multiplication of cosets makes sense, and that they turn the collection of cosets into a ring.

Proposition 10.1. *Let R be a commutative ring, and let I be an ideal of R.*

(a) *Let $a+I$ and $a'+I$ be two cosets. Then $a'+I = a+I$ if and only if $a'-a \in I$.*

(b) *Addition and multiplication of cosets is well-defined, in the sense that it doesn't matter which element of the coset we use in the definition.*

(c) *Addition and multiplication of cosets turns R/I into a commutative ring.*[1]

Proof. We prove that multiplication is well-defined, and leave the rest of the proof to you; see Exercise 10.3. Let $a, a', b, b' \in R$ be elements whose cosets satisfy $a' + I = a + I$ and $b' + I = b + I$. We need to prove that $ab + I$ is equal to $a'b' + I$.

The assumption that $a + I = a' + I$ means that there is some $c \in I$ such that $a' = a + c$, and similarly the assumption that $b + I = b' + I$ means that there is some $d \in I$ such that $b' = b + d$. It follows that

$$a'b' = (a + c)(b + d) = ab + \underbrace{ad + bc + cd}_{\text{This is in } I, \text{ since } c,\, d \in I.}.$$

Hence $a'b' - ab \in I$, so from (a), the cosets $a'b' + I$ and $ab + I$ are equal. □

[1] If we want to be precise, we must also insist that $I \neq R$, since if $I = R$, then R/I has only has one element, and we don't allow rings to have $1 = 0$.

Ideals and homomorphisms are closely related, as shown by our next result.

Proposition 10.2. *Let R be a commutative ring.*
(a) *Let I be an ideal of R. Then the map*

$$R \longrightarrow R/I, \quad a \longmapsto a + R,$$

that sends an element to its coset is a ring homomorphism whose kernel is I.
(b) *Let $\phi : R \to R'$ be a ring homomorphism.*
  (i) *The kernel of ϕ is an ideal of R.*
  (ii) *The homomorphism ϕ is injective if and only if* $\ker(\phi) = (0)$.
  (iii) *Writing $I_\phi = \ker(\phi)$ for convenience, there is a well-defined injective ring homomorphism*

$$\bar{\phi} : R/I_\phi \longrightarrow R' \quad \textit{defined by} \quad \bar{\phi}(a + I_\phi) = \phi(a).$$

Proof. We prove (b), and leave (a) as an exercise; see Exercise 10.4. Our first goal is to prove that $\ker(\phi)$ is an ideal. Let $a, b \in \ker(\phi)$. Then

$$\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0,$$

so $a + b \in \ker(\phi)$. Next let $a \in \ker(\phi)$ and $r \in R$. Then

$$\phi(ra) = \phi(r) \cdot \phi(a) = \phi(r) \cdot 0 = 0,$$

so $ra \in \ker(\phi)$. This completes the proof of (i) that $\ker(\phi)$ is an ideal.

Next suppose that $\ker(\phi) = (0)$, and that $\phi(a) = \phi(b)$ for some $a, b \in R$. Then $\phi(a - b) = 0$, so $a - b \in \ker(\phi)$, and hence $a - b = 0$. This proves the ϕ is injective.

Conversely, suppose that ϕ is injective, and let $a \in \ker(\phi)$. Then $0 = \phi(a) = \phi(0)$, so the injectivity of ϕ implies that $a = 0$. This proves that $\ker(\phi) = (0)$, which completes the proof of (ii).

For (iii), we first want to show that the map $\bar{\phi}$ is well-defined. So suppose that $a' + I_\phi = a + I_\phi$ are two ways of writing the same coset. We need to show that $\phi(a') = \phi(a)$. The assumption that $a' + I_\phi = a + I_\phi$ means that $a' = a + b$ for some $b \in I_\phi$. then

$$\phi(a') = \phi(a + b) = \phi(a) + \phi(b) = \phi(a) + 0 = \phi(a).$$

This shows that $\bar{\phi}$ is well-defined. Next, the fact that $\bar{\phi}$ is a ring homomorphism follows directly from the assumption that ϕ is a ring homomorphism. Finally, to see that $\bar{\phi}$ is injective, we observe that

$$\begin{aligned} \bar{\phi}(a' + I_\phi) = \bar{\phi}(a + I_\phi) \quad &\iff \quad \phi(a') = \phi(a) \quad \iff \quad \phi(a' - a) = 0 \\ &\iff \quad a' - a \in I_\phi \quad \iff \quad a' + I_\phi = a + I_\phi. \end{aligned}$$

This completes the proof of Proposition 10.2(b). □

10.2 Prime Ideals and Maximal Ideals

You have seen the importance of prime numbers in the study of number theory. Recall that an integer p is prime if its only (positive) divisors are 1 and p. An important property of prime numbers, which we proved in the Number Theory Unit, is that if p is prime and p divides a product ab, then either p divides a or p divides b. We can rephrase this divisibility property using ideals: if a product ab is in the ideal $p\mathbb{Z}$, then either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. This version is the right way to generalize the notion of primes to arbitrary rings.[2]

Definition. Let R be a commutative ring. An ideal I of R is a *prime ideal* if $I \neq R$ and if whenever a product of elements $ab \in I$, then either $a \in I$ or $b \in I$.

We observe that if I is a prime ideal, then it also has the following property:

$$a \notin I \text{ and } b \notin I \quad \Longrightarrow \quad ab \notin I.$$

This statement is the contrapositive of, hence logically equivalent to, the stated definition of prime ideal.

Example 10.3. Let $m \neq 0$ be an integer. The ideal $m\mathbb{Z}$ is a prime ideal if and only if $|m|$ is a prime number in the usual sense.

Example 10.4. Let F be a field. For every $a, b \in F$ with $a \neq 0$, the principal ideal $(ax + b)F[x]$ is a prime ideal. For every $a, b, c \in F$ such that $a \neq 0$ and $b^2 - 4ac$ is not equal to the square of an element of F, the principal ideal $(ax^2 + bx + c)F[x]$ is a prime ideal. See Exercise 10.8.

The largest possible ideal in a ring R is the entire ring itself. The ideals that are as large as possible without being all of R play an important role.

Definition. Let R be a commutative ring. An ideal I is called a *maximal ideal* if $I \neq R$ and if there are no ideal properly contained between I and R. In other words, if J is an ideal and $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

Example 10.5. Let $p \in \mathbb{Z}$ be a prime number. Then the ideal $p\mathbb{Z}$ is not only a prime ideal, it is also a maximal ideal. This follows by combining Proposition 8.4, which says that $\mathbb{Z}/p\mathbb{Z}$ is a field, with Proposition 10.7 (see below), which says that in general R/I is a field if and only if I is a maximal ideal.

Example 10.6. In the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients, the principal ideals $2\mathbb{Z}[x]$ and $x\mathbb{Z}[x]$ are prime ideals, but they are not maximal ideals, since they are contained in the following non-principal maximal the ideal:

$$\big\{2a(x) + xb(x) : a(x), b(x) \in \mathbb{Z}[x]\big\}.$$

See Exercise 10.7.

[2]There is also an analogue of the "no non-trivial factors" definition to arbitrary rings. Such elements are called *irreducible*.

Just as prime numbers in $\mathbb{Z}$ form the basic building blocks for all numbers, the prime and maximal ideals of a ring R are, in some sense, the basic building blocks underlying the algebraic (and geometric!) structure of R. On the other hand, integral domains and fields are two particularly nice kinds of rings. These observations may help to explain why the next result is so important.

Theorem 10.7. *Let R be a commutative ring, and let I an ideal with $I \neq R$.*
(a) *I is a prime ideal if and only if the quotient ring R/I is an integral domain.*
(b) *I is a maximal ideal if and only if the quotient ring R/I is a field.*

Proof. This theorem consists of two if-and-only-if statements, so there are really four statements that need to be proven.

(a) $\boxed{I = \text{Prime Ideal} \quad \Longrightarrow \quad R/I = \text{Integral Domain}}$

Let $a + I$ and $b + I$ be elements of R/I whose product is zero, i.e.,

$$(a + I) \cdot (b + I) = 0 + I.$$

This means that $ab + I = 0 + I$, so $ab \in I$. The assumption that I is a prime ideal tells us that either $a \in I$ or $b \in I$, which means that either $a + I = I$ or $b + I = I$. Thus at least one of $a + I$ or $b + I$ is equal to $0 + I$, which completes the proof that R/I is an integral domain.

(a) $\boxed{R/I = \text{Integral Domain} \quad \Longrightarrow \quad I = \text{Prime Ideal}}$

Suppose that $a, b \in R$ satisfy $ab \in I$. Then

$$(a + I) \cdot (b + I) = ab + I = 0 + I,$$

so the product of $a + I$ and $b + I$ is zero in the quotient ring R/I. We are assuming that R/I is an integral domain, so we conclude that either $a + I = I$ or $b + I = I$. These in turn imply that either $a \in I$ or $b \in I$, which completes the proof that I is a prime ideal.

(b) $\boxed{I = \text{Maximal Ideal} \quad \Longrightarrow \quad R/I = \text{Field}}$

Let $a + I$ be a non-zero element of R/I, which means that $a \notin I$. In order to exploit the fact that I is a maximal ideal and to get a into the proof, it is natural to try to construct an ideal J so that

$$I \subseteq \boxed{\text{an ideal } J \text{ that contains } a} \subseteq R.$$

The ideal J has to contain I, and we want it to contain a, and it has to be an ideal, which means that the smallest possiblity is

$$J = \{ar + b : r \in R \text{ and } b \in I\}.$$

We leave it to you to check that this set J is an ideal; see Exercise 10.6. Taking the elements of J with $r = 0$ shows that $I \subset J$, while taking $r = 1$ and $b = 0$ shows that $a \in J$. We know that $a \notin I$, so J is strictly larger than I; in symbols, $I \subsetneq J \subseteq R$.

We are assuming that I is a maximal ideal, so by definition this forces $J = R$. In particular, we have $1 \in J$. Thus there exists some $c \in R$ and some $b \in I$ such that $1 = ac + b$. In terms of elements of R/I, using the fact that $b + I = I$, we find

$$1 + I = (ac + b) + I = ac + I = (a + I) \cdot (c + I).$$

Hence $a + I$ has a multiplicative inverse in R/I, and we've proven that this is true for all non-zero elements of R/I, hence R/I is a field.

(b) $\boxed{R/I = \text{Field} \quad \Longrightarrow \quad I = \text{Maximal Ideal}}$

Let J be an ideal satisfying $I \subseteq J \subseteq R$. If $J = I$, we're done, so we assume that $J \neq I$. This means that we can find some element $a \in J$ with $a \notin I$. Then the coset $a + I \neq 0 + I$, so $a + I$ is a non-zero element of the quotient ring R/I. We are assuming that R/I is a field, so $a + I$ has a multiplicative inverse, say $c + I$. This means that

$$1 + I = (a + I) \cdot (c + I) = ac + I,$$

so there is an element $b \in I$ such that $1 = ac + b$. But $a \in J$, so $ac \in J$, while $b \in I \subset J$, and thus the quantity $ac + b$ is in the ideal J. This proves that $1 \in J$, but then for every $r \in R$ we have $r = r \cdot 1 \in J$. Hence $J = R$, which completes the proof that I is a maximal ideal. □

The strength of Theorem 10.7 is illustrated by the slick proof of the following corollary.

Corollary 10.8. *Every maximal ideal is a prime ideal.*[3]

Proof. It is easy to check that a field is an integral domain; see Exercise 7.2. Then we can apply Theorem 10.7,

$$I \text{ maximal} \quad \Longrightarrow \quad R/I \text{ field} \quad \Longrightarrow \quad R/I \text{ integral domain} \quad \Longrightarrow \quad I \text{ prime}.$$

This completes the proof of the corollary. □

Mini-Remark 7. It would be nice to know that every ring has at least one maximal ideal. It turns out that this assertion is yet another statement that is equivalent to the axiom of choice!

Exercises

10.1. Let R be a commutative ring and let $c \in R$. Prove that $cR = \{rc : r \in R\}$ is an ideal of R. It is called the *principal ideal generated by c*.

10.2. Let R be a commutative ring. Prove that R is a field if and only if its only ideals are the zero ideal (0) and the entire ring R.

10.3. Prove the remaining parts of Proposition 10.1. Let R be a commutative ring, and let I be an ideal of R.

[3]The converse is not true, i.e., there may exist prime ideals that are not maximal; see Example 10.6.

(a) Let $a+I$ and $a'+I$ be two cosets. Prove that $a+I=a'+I$ if and only if $a-a'\in I$.
(b) Prove that addition cosets is well-defined.
(c) Prove that addition and multiplication of cosets turns R/I into a commutative ring.

10.4. Let R be a commutative ring, and let I be an ideal of R. Prove that the map

$$R\longrightarrow R/I,\quad a\longmapsto a+R$$

that sends an element to its coset is a ring homomorphism whose kernel is I. This is Proposition 10.2(a).

10.5. Let I be the principal ideal of $\mathbb{R}[x]$ generated by the polynomial x^2+1. Prove that the map

$$\phi:\mathbb{R}[x]/I\longrightarrow\mathbb{C},\quad \phi\bigl(f(x)+I\bigr)=f(i),$$

is a well-defined isomorphism, where $i=\sqrt{-1}$ as usual. This shows how one can use ring theory to abstractly construct the complex numbers from the real numbers. (*Hint*. One way to do this exercise is to write out all the grubby details, but it is easier to apply Proposition 10.2 to the evaluation homomorphism $E_i:\mathbb{R}[x]\to\mathbb{C}$.)

10.6. Let R be a commutative ring and let I and J be ideals of R.
(a) Prove that the *ideal sum*

$$I+J=\{a+b:a\in I\text{ and }b\in J\}$$

is an ideal of R.
(b) Give an example to show that the set of products $\{ab:a\in I\text{ and }b\in J\}$ need not be an ideal. (*Hint*. If I or J is a principal ideal, then this set will be an ideal, so you'll need to use some non-principal ideals.)
(c) The *ideal product* of two ideals is defined to be

$$IJ=\{a_1b_1+a_2b_2+\cdots+a_nb_n:n\ge1\text{ and }a_1,\ldots,a_n\in I\text{ and }b_1,\ldots,b_n\in J\}.$$

Prove that IJ is an ideal of R.

10.7. Let I be the following subset of the ring $\mathbb{Z}[x]$ of polynomials having integer coefficients:

$$I=\bigl\{2a(x)+xb(x):a(x),b(x)\in\mathbb{Z}[x]\bigr\}.$$

(a) Prove that I is an ideal of $\mathbb{Z}[x]$.
(b) Prove that $I\ne\mathbb{Z}[x]$.
(c) Prove that I is not a principal ideal, i.e., prove that there does not exist a polynomial $c(x)\in\mathbb{Z}[x]$ such that $I=c(x)\mathbb{Z}[x]$.
(d) Prove that I is a maximal ideal of $\mathbb{Z}[x]$.

10.8. (a) Let $m\ne0$ be an integer. Prove that the ideal $m\mathbb{Z}$ is a prime ideal (and hence also a prime ideal) if and only if $|m|$ is a prime number in the usual sense of primes in $\mathbb{Z}$.
(b) Let F be a field, and let $a,b\in F$ with $a\ne0$. Prove that the principal ideal $(ax+b)F[x]$ is a maximal ideal of the polynomial ring $F[x]$.
(c) Again let F be a field, and let $c\in R$ be an element with the property that $4c$ is not the square of an element in F.[4] Prove that the principal ideal $(x^2+c)F[x]$ is a maximal ideal of the polynomial ring $F[x]$.

[4]More prosaically, what this means is that we assume that F does not have characteristic 2 and that c is not the square of an element in F.

10.9. Let R be a ring, let $b, c \in R$, and let $E_{b,c} : R[x,y] \to R$ be the evaluation homomorphism described in Exericse 6.11.

(a) If R is an integral domain, prove that $\ker(E_{b,c})$ is a prime ideal of of $R[x,y]$.

(b) If R is a field, prove that $\ker(E_{b,c})$ is a maximal ideal of of $R[x,y]$.

(*Hint*. Use Proposition 10.2 and Theorem 10.7.)

10.10. Let R be a ring and let I be an ideal of R.

(a) Prove that there is a bijection

$$\{\text{ideals of } R \text{ that contain } I\} \longrightarrow \{\text{ideals of } R/I\}, \quad J \longmapsto J/I,$$

where J/I is the set of cosets

$$J/I = \{a + I : a \in J\}.$$

Let J be an ideal of R that contains I.

(b) Prove that J is a prime ideal of R if and only if J/I is a prime ideal of R/I.

(c) Prove that J is a maximal ideal of R if and only if J/I is a maximal ideal of R/I.

10.11. Let R be a commutative ring. The *nilradical* of R is the set

$$N = \{a \in R : a^n = 0 \text{ for some } n \ge 1\}$$

consisting of all of the nilpotent elements in R.

(a) Prove that N is an ideal of R.

(b) Let P be a prime ideal of R. Prove that $N \subseteq P$.

(c) Prove that

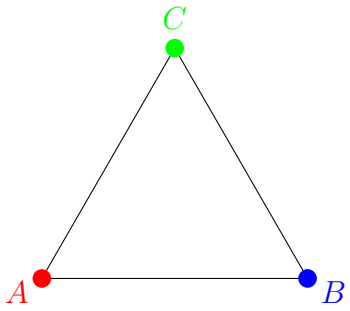
$$N = \bigcap_{\text{prime } P \subseteq R} P,$$

where the intersection is over all prime ideals of R. (*Warning*: You probably won't be able to do this part with the tools that we've developed so far, but it's a very interesting characterization of the nilradical that is worth thinking about.)

Appendix A

Class Exercise: Lecture #1 Symmetries of a Triangle

We investigate the symmetries of a rigid equilateral triange:



• How many ways are there to pick up the triangle, rotate or flip it, and put it back down? Give names to the different motions.

• Make a "multiplication table" that describes what happens when you compose two of the motions.

• For each motion, compute how many times you need to compose it with itself before you get back to the identity motion. What do you notice about these numbers?

Appendix B

Class Exercise: Lecture #2
Groups of 2-by-2 matrices

We can form groups of matrices whose entries are in any algebraic system where we can add, subtract, and multply. For example, for any integer $m \ge 2$ we can look at matrices with mod m entries:[1]

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}/m\mathbb{Z},\ ad-bc = 1 \right\}.$$

We are going to investigate the group with $m = 2$, i.e., we look at the group

$$\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}).$$

- How many 2-by-2 matrices are there with entries taken from $\mathbb{Z}/2\mathbb{Z}$?
- How many of them satisfy $ad - bc = 1$?
- Write down the elements of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ and give them names.
- Multiply them and make a multiplication table for the group $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$

- Challenge Problem: If p is a prime, how many elements does $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ have?

[1] See (2.1) in Example 2.6 for the formula for matrix multiplication.

Appendix C

Class Exercise: Lecture #3
Which Groups are Isomorphic?

Consider the following groups:

$\mathcal{C}_n =$ a cyclic group of order n.
$\mathcal{D}_n =$ the n'th dihedral group.
$\mathcal{S}_n =$ the n'th symmetric group.
$\mathcal{Q} =$ the quaternion group.

- For which $n \geq 2$ are $\mathcal{C}_n$ and $\mathcal{S}_n$ isomorphic?

- More generally, for which $n \geq 2$ and $m \geq 2$ are $\mathcal{C}_n$ and $\mathcal{S}_m$ isomorphic?

- For which $n \geq 2$ are $\mathcal{D}_n$ and $\mathcal{S}_n$ isomorphic?

- More generally, for which $n \geq 2$ and $m \geq 2$ are $\mathcal{D}_n$ and $\mathcal{S}_m$ isomorphic?

- Is $\mathcal{Q}$ isomorphic to $\mathcal{D}_4$? Is $\mathcal{Q}$ isomorphic to $\mathcal{C}_8$? Can you find some more groups of order 8 that aren't isomorphic to $\mathcal{Q}$, $\mathcal{D}_4$, or $\mathcal{C}_8$?

Appendix D

Class Exercise: Lecture #4
Bountiful Binary Relations

Let S be a set. Informally, a *binary relation on* S is a rule for checking whether "a is related to b" for elements $a, b \in S$. More formally, a binary relation on S is simply a subset $\mathcal{B} \subset S \times S$, and define

$$\text{"}a \text{ is related to } b\text{"} \quad \text{if and only if} \quad (a, b) \in \mathcal{B}.$$

If this is the case, we'll write $a \mathcal{B} b$.

Interesting properties that a binary relation may possess include:

$\mathcal{B}$ is	*reflexive*	if	$a \mathcal{B} a$	$\forall a \in S$.
$\mathcal{B}$ is	*symmetric*	if	$a \mathcal{B} b \implies b \mathcal{B} a$	$\forall a, b \in S$.
$\mathcal{B}$ is	*transitive*	if	$a \mathcal{B} b$ and $b \mathcal{B} c \implies a \mathcal{B} c$	$\forall a, b, c \in S$.
$\mathcal{B}$ is	*anti-symmetric*	if	$a \mathcal{B} b$ and $b \mathcal{B} a \implies a = b$	$\forall a, b \in S$.

Then we say:

$\mathcal{B}$ is an	*equivalence relation*	if it is reflexive, symmetric, and transitive.
$\mathcal{B}$ is a	*partial order*	if it is reflexive, anti-symmetric, and transitive.

• Which of the following binary relations are reflexive, symmetric, anti-symmetric, and/or transitive? Which are equivalence relations. Which are partial orders?

(a) $S = \mathbb{R}$, and $a \mathcal{B} b$ iff $a \geq b$.
(b) $S = \mathbb{N}$, and $a \mathcal{B} b$ iff $\gcd(a, b) = 1$.
(c) $S = \mathbb{N}$, and $a \mathcal{B} b$ iff $a \mid b$.
(d) S is the set of students are Brown, and $a \mathcal{B} b$ iff a and b have the same birthday.
(e) S is a graph, and $a \mathcal{B} b$ iff $a = b$ or there is an edge connecting a to b.
(f) S is a graph, and $a \mathcal{B} b$ iff $a = b$ or a sequence of edges connects a to b.
(g) $S = \mathbb{R}$, and $f : S \to \mathbb{R}$ is a function, and $a \mathcal{B} b$ iff $f(a) = f(b)$.
(h) $S =$ (the collection of subsets of a set Σ), and $A \mathcal{B} B$ iff $A \subseteq B$.
(i) $S =$ (the collection of subsets of a set Σ), and $A \mathcal{B} B$ iff $A \cap B \neq \emptyset$.
(j) $S =$ (the collection of subsets of a set Σ), and $A \mathcal{B} B$ iff $A \cap B = \emptyset$.

• Come up with some examples of binary relations of your own, and figure out their properties.

Appendix E

Class Exercise: Lecture #5 Conjugate Subgroups in $\mathcal{S}_n$

• Let H be the subgroup of $\mathcal{S}_3$ generated by $\pi = (1, 2, 3)$. Write down the elements of H. Describe the conjugate subgroups $g^{-1}Hg$ of H. How many are there? Is H a normal subgroup?

• Same question for the subgroup of $\mathcal{S}_3$ generated by $\pi = (1, 2)$.

• Same question for the subgroup of $\mathcal{S}_4$ generated by $\pi = (1, 2, 3, 4)$.

• Same question for the subgroup of $\mathcal{S}_4$ generated by $\pi = (1, 2)(3, 4)$.

Appendix F

Class Exercise: Lecture #6
Rings of 2-by-2 matrices

We can form groups of matrices whose entries are in any algebraic system where we can add, subtract, and multply. Thus for any ring R, we can form a ring of 2-by-2 matrices with entries from R:

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$$

We add matrices by adding their corresponding entries, and we multiply matrices using matrix multiplication.[1]

- Find matrices in $M_2(R)$ that don't commute.
- Find non-zero matrices $A, B \in M_2(R)$ with the property that $AB = 0$.
- Consider the following subring of $M_2(R)$:

$$\tilde{M}_2(R) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in R \right\}$$

Show that there is a matrix $J \in \tilde{M}_2(R)$ satisfying $J^2 = -I$.

- Try to find some properties of $\tilde{M}_2(R)$. For example, is it commutative? Can $AB = 0$ if $A \neq 0$ and $B \neq 0$? (The answer may depend on R.) What does $\tilde{M}_2(\mathbb{R})$ look like?

[1] See (2.1) in Example 2.6 for the formula for matrix multiplication.

Appendix G

Class Exercise: Lecture #7
The Degree of a Polynomial

Let R be a commutative ring. Recall that the *degree* of a polynomial $F(x) \in R[x]$ is the exponent on the highest power of x appearing in $F(x)$.

• Let $F(x), G(x) \in R[x]$. How is $\deg(FG)$ related to $\deg(F)$ and $\deg(G)$? Give an inequality, and find some natural condition on R that ensures that the inequality is an equality.

• Let $F(x), G(x) \in R[x]$. How is $\deg(F+G)$ related to $\deg(F)$ and $\deg(G)$? Give an inequality, and find some natural condition on F and G that ensures that the inequality is an equality.

Appendix H

Class Exercise: Lecture #8
The Group of Units in a Ring

We'll work together to describe the following unit groups, to the extent that time allows, and then you can continue the investigation on your own:

1. (a) $\mathbb{Z}^*$. (b) $\mathbb{Q}^*$. (c) $\mathbb{Z}[i]^*$.

2. Describe the unit group of the ring

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

   For example, show that $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$, and by taking powers, show that $\mathbb{Z}[\sqrt{2}]^*$ is an infinite group.

3. $\mathbb{R}[x]^*$, and more generally, $F[x]^*$ for any commutative field F.
4. $(\mathbb{Z}/4\mathbb{Z})[x]^*$. For example, show that $1 + 2x \in (\mathbb{Z}/4\mathbb{Z})[x]^*$. What are some other units in this ring? Try to describe all of the units.

5. $M_2(\mathbb{R})^*$, and more generally, $M_2(R)^*$ for any commutative ring R.

Challenge Problems

6. Let $D \in \mathbb{Z}$ be an integer that is not a perfect square. Describe the unit group of the ring

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}.$$

   (*Hint*. The cases $D > 0$ and $D < 0$ look very different.)

7. Let R be an arbitrary commutative ring. What does $R[x]^*$ look like?

Appendix I

Class Exercise: Lecture #9 Building Bigger (and Better?) Finite Fields

Let p be a prime. We know that there is a field $\mathbb{F}_p$ with p elements. Let's try to construct a field with p^2 elements by mimicking the way that the complex numbers are constructed from the real numbers.

So we let

$$R_p = \{a + bi : a, b \in \mathbb{F}_p\},$$

where i is just a symbol satisfying $i^2 = -1$. Addition and multiplication in R_p work just like addition and multiplication in $\mathbb{C}$,

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i,\\ (a + bi) \cdot (c + di) &= ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i.\end{aligned}$$

It's a tedious, but straightforward, exercise to check that all of the ring axioms hold, so R_p is a ring. And clearly

$$\#R_p = p^2,$$

since every element of R_p looks like $a + bi$, and there are p choices for a and p choices for b.

The Big Question: Is R_p a field?

- **Question 1**. Is R_3 a field?
- **Question 2**. Is R_5 a field?
- **Question 3**. Generalize in any way, shape, or form that you want?
  - Is there always a field with p^2 elements?
  - Can you create a field with p^3 elements?
  - If p and q are distinct primes, can there be a field with pq elements?
  - What does the unit group R_p^* look like?

