CHAPTER 2

Groups

The integers have two basic operations: addition and multiplication. It turns out that many mathematical objects also come equipped with generalizations of addition or multiplication. For instance, $\mathbb{Z}_n$ has both an addition and multiplication structure while U_n only has a multiplication operation. Further examples abound in mathematics and this chapter begins their study.

Roughly speaking, gadgets with one operation are called *groups* and gadgets with two operations are called *rings*. We start by studying groups since there is less to worry about with only one operation running amuck.

1. Definitions and Examples

1.1. Binary Operations. First off, we need a definition capable of handling various generalizations of addition or multiplication. If we think about the meaning of, say, addition on $\mathbb{Z}$, what we really have is a map taking a pair of numbers and sputtering out their sum. In fancy language, addition is nothing more than a very special function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

Given an arbitrary set S, the natural way to generalize this is to take a function $B : S \times S \to S$ (B for binary) and to use it to define a souped-up version of addition or multiplication on S. For instance, if we want to use B to define a type of addition on S, we can define $s_1 + s_2 = B(s_1, s_2)$ for $s_1, s_2 \in S$. If we want to think of B as defining a type of multiplication, we can instead write $s_1 \cdot s_2 = B(s_1, s_2)$ or even $s_1 s_2 = B(s_1, s_2)$ if we are lazy. If we prefer to show no bias towards addition or multiplication, we use the generic symbol $*$ and write $s_1 * s_2 = B(s_1, s_2)$.

Definition 2.1. Given a set S, a *binary operation* $*$ on S is a function $B_* : S \times S \to S$. For $s_1, s_2 \in S$, define $s_1 * s_2$ by

$$s_1 * s_2 = B_*(s_1, s_2).$$

For example, in $\mathbb{Z}_n$, consider the map $B_+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ given by $B_+([a], [b]) = [a + b]$. This is the binary operation we used to define addition in $\mathbb{Z}_n$ since, by definition, $[a] + [b] = B_+([a], [b])$. Similarly, the map $B_\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ given by $B_\cdot([a], [b]) = [ab]$ is the binary operation we used to define multiplication on $\mathbb{Z}_n$.

As a less useful example, consider the binary operation $B_* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $B_*(a, b) = a^2 b$ for $a, b \in \mathbb{Z}$. Using this operation, we calculate that $5 * 3 = B_*(5, 3) = 5^2 3 = 75$.

About the only way to mess up a binary operation is to forget that the codomain of a binary operation on S is S. In other words, the result of our generalized addition or multiplication must still be in the original set S. This property of binary operations is sometimes referred to as *closure*.

For instance, the map $B_{*_1} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $B_{*_1}(a, b) = 2ab$ is a binary operation since $2ab \in \mathbb{Z}$. However, the "map" $B_{*_2} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $B_{*_2}(a, b) =$

$\frac{ab}{2}$ is not a binary operation since $\frac{ab}{2}$ is not always in $\mathbb{Z}$. On the other hand, $B_{*_3} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ given by $B_{*_3}(a, b) = \frac{ab}{2}$ is a perfectly fine binary operation since $\frac{ab}{2} \in \mathbb{Q}$.

1.2. Definition of a Group. A group is simply an object with a sufficiently nice generalized version of addition or multiplication.

DEFINITION 2.2. A *group* is a set G with a binary operation $*$ on G satisfying the properties:

(1) (*Associativity*) For $g_1, g_2, g_3 \in G$,

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$$

(2) (*Identity*) There exists an element $e \in G$ so that

$$e * g = g * e = g$$

for all $g \in G$. The element e is called the *identity element*.

(3) (*Inverses*) For every element $g \in G$, there exists an $h \in G$ so that

$$g * h = h * g = e.$$

The element h is called the *inverse* of g.

Some notes are in order before moving on to examples. The first is that when people think of the binary operation $*$ as an additive sort of operation, the symbol $+$ is usually used instead of $*$. In this case, the associative property looks like

$$g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3,$$

the identity property looks like

$$e + g = g + e = g,$$

and the inverse property looks like

$$g + h = h + g = e.$$

Because this setting looks so familiar to normal addition on $\mathbb{Z}$, people sometimes write 0_G, or even just 0, instead of e for the identity element. In that case, the identity property looks like

$$0 + g = g + 0 = g$$

and the inverse property looks like

$$g + h = h + g = 0.$$

For the same reason, people in this setting usually write $-g$ for the inverse of g. Thus the inverse property says that for each $g \in G$, there is an element $-g \in G$ so that

$$g + (-g) = (-g) + g = 0.$$

Of course people also abbreviate statements such as $g_1 + (-g_2)$ with the notation $g_1 - g_2$. When people adopt parts of this sort of notation for a group, they say they are writing a group *additively*.

Similarly, when people think of $*$ as a multiplicative sort of operation, they often use $\cdot$ instead of $*$. In this situation, the associative property looks like

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

the identity property looks like

$$e \cdot g = g \cdot e = g,$$

and the inverse property looks like

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

Even more commonly, just as we do with ordinary multiplication, the $\cdot$ is omitted altogether. In that case, it is simply understood that two adjacent elements are "multiplied" with the binary operation. In that setting, the associative property looks like

$$g_1(g_2g_3) = (g_1g_2)g_3,$$

the identity property looks like

$$eg = ge = g,$$

and the inverse property looks like

$$gh = hg = e.$$

Because this setting looks so familiar to normal multiplication, people sometimes write 1_G, or even just 1, instead of e for the identity element. In that case, the identity property looks like

$$1 \cdot g = g \cdot 1 = g$$

and the inverse property looks like

$$gh = hg = 1.$$

For the same reason, people in this setting usually write g^{-1} for the inverse of g. Thus the inverse property says that for each $g \in G$, there is an element $g^{-1} \in G$ so that

$$gg^{-1} = g^{-1}g = 1.$$

When people adopt parts of this sort of notation for a group, they say they are writing a group *multiplicatively*. Multiplicative notation is the default notation for most generic groups.

Our final remark addresses the uniqueness of an inverse in a group. We will shortly see (Theorem 2.5) that inverses turn out to be unique and so it is fair to say "the inverse" instead of "an inverse". A similar remark holds for the identity element.

1.3. Examples.

1.3.1. *Additive Arithmetic:* $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{C}, +)$, *and* $(\mathbb{Z}_n, +)$. To be honest, these are rather boring examples even if they are extremely important. Start with $\mathbb{Z}$. Groups have one operation while $\mathbb{Z}$ comes equipped with two. Therefore, if you want to get a group here, it is important to specify which binary operation is going to be used. In order to emphasize that the additive operation is being used, people often write $(\mathbb{Z}, +)$. The reader has probably known since first grade that the set $\mathbb{Z}$ along with the binary operation $+$ satisfies the three properties of a group. Using additive notation (of course), the associative law follows from Axiom 1. The (additive) identity element is $e = 0$ since $n + 0 = 0 + n = 0$ for all $n \in \mathbb{Z}$. Finally, (additive) inverses exist since $n - n = -n + n = 0$. Thus $(\mathbb{Z}, +)$ is a group.

Along with $(\mathbb{Z}, +)$, there are a number of analogous examples of groups: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{C}, +)$, and $(\mathbb{Z}_n, +)$. Here $\mathbb{C}$ is the set of complex numbers and

$\mathbb{R}^n$ is the set of vectors in n-space equipped with vector addition. The verification that each of these objects is a group is almost identical to the argument for $(\mathbb{Z}, +)$ The hardest is $(\mathbb{Z}_n, +)$, but Theorem 1.22 takes care of it all.

Notice, however, that objects such as $(\mathbb{Z}_{\geq 0}, +)$ are not groups. While $\mathbb{Z}_{\geq 0}$ is associative and has an identity, $e = 0$, it fails to have enough inverses. For example, there is no inverse to 2 in $\mathbb{Z}_{\geq 0}$ since $-2 \notin \mathbb{Z}_{\geq 0}$.

1.3.2. *Multiplicative Arithmetic:* $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{R}^+, \cdot)$, $(\mathbb{C}^\times, \cdot)$, *and* $(U_n, \cdot)$. A reasonable question is to ask whether $(\mathbb{Z}, \cdot)$ also forms a group (obvious notation here). The answer is no. With respect to the binary operation of multiplication, $\mathbb{Z}$ is clearly associative (Axiom 1) and there exists a (multiplicative) identity, $e = 1$. However, $(\mathbb{Z}, \cdot)$ fails to satisfy the inverse property. For instance, 2 has no (multiplicative) inverse in $\mathbb{Z}$. Of course if we worked with $\mathbb{Q}$ the whole time instead of $\mathbb{Z}$, then 2 would have an inverse, namely $\frac{1}{2}$. However, even scrapping $(\mathbb{Z}, \cdot)$ and passing to $(\mathbb{Q}, \cdot)$ still does not quite fix the problem since 0 has no (multiplicative) inverse.

Since the only thing preventing $(\mathbb{Q}, \cdot)$ from being a group is the number 0, let us get rid of it. Write $\mathbb{Q}^\times$ for the set of invertible elements in $\mathbb{Q}$; i.e., $\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}$. Then $\mathbb{Q}^\times$ is closed under the binary operation of multiplication. Moreover, $\mathbb{Q}^\times$ contains all its inverses. Thus $(\mathbb{Q}^\times, \cdot)$ is a group. Similar examples (with the obvious notation) include $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, and $(U_n, \cdot)$. Again, the verification that each of these objects is a group is almost identical to the argument for $(\mathbb{Q}^\times, \cdot)$. The only one that requires work is $(U_n, \cdot)$. However, Theorem 1.25 shows closure of the binary operation, Theorem 1.22 gives associativity and the identity, and the existence of inverses follows from the definition.

Finally, notice that the inverse of a positive number is still positive. Thus if $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$ and similarly for $\mathbb{R}^+$, it easily follows that $(\mathbb{Q}^+, \cdot)$ and $(\mathbb{R}^+, \cdot)$ are groups as well. The negative numbers, though, do not form a group. For instance, multiplication on $\mathbb{Q}^-$ is not a binary operation since the product of two numbers lies in $\mathbb{Q}^+$ instead of $\mathbb{Q}^-$. Another problem with $\mathbb{Q}^-$ is that it has no identity element since $1 \notin \mathbb{Q}^-$.

1.3.3. *The Circle:* $\left(S^1, \cdot\right)$. Write S^1 for the circle in the plane (this notation comes from calculus where S^n is the n-dimensional sphere in $\mathbb{R}^{n+1}$). It turns out there are many ways to look at S^1 (Exercise 2.8). One of the easiest ways is to identify $\mathbb{R}^2$ with $\mathbb{C}$ by the correspondence $(x, y) \leftrightarrow x + iy$. In that setting, define

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

where $|z| = \sqrt{a^2 + b^2}$ is the *length* (also called the *modulus* or *norm*) of $z = a + ib$ with $a, b \in \mathbb{R}$. Recall that complex multiplication satisfies $|z_1 z_2| = |z_1|\,|z_2|$ for $z_1, z_2 \in \mathbb{C}$. Thus, if $z_1, z_2 \in S^1$,

$$|z_1 z_2| = |z_1|\,|z_2| = 1 \cdot 1 = 1$$

so that the product of two elements on S^1 still lies in S^1. Therefore complex multiplication is a binary operation on S^1. To check that $\left(S^1, \cdot\right)$ is a group, first notice that multiplication is associative since it is already associative on all of $\mathbb{C}$. As far as the identity goes, it is clear that $e = 1$ works. Finally, to find inverses, write $\overline{z} = a - ib$ for the *complex conjugate* of z and recall that $|\overline{z}| = |z|$ and $z\overline{z} = |z|^2$.

In particular, if $z \in S^1$, then $\overline{z} \in S^1$ since $|\overline{z}| = |z| = 1$. Moreover, $z^{-1} = \overline{z}$ since

$$\overline{z}z = z\overline{z} = |z|^2 = 1^2 = 1.$$

1.3.4. *Linear Algebra: $GL(n,\mathbb{F})$, $SL(n,\mathbb{F})$, $SO(n,\mathbb{F})$, and $O(n,\mathbb{F})$.* Write $M_{n,m}(\mathbb{F})$ for the set of $n \times m$ matrices with entries in $\mathbb{F}$ where $\mathbb{F}$ (for now) is $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ for $p \in \mathbb{N}$ prime. The reader is surely familiar with the basic properties of matrix algebra when $\mathbb{F} = \mathbb{R}$. Most likely, the reader also saw that most results still hold when $\mathbb{F} = \mathbb{C}$. In fact, almost all basic properties work even when $\mathbb{F} = \mathbb{Q}$ or $\mathbb{F} = \mathbb{Z}_p$. In any case, operations such as matrix addition, multiplication, inverses, and determinants all go through as expected for any choice of $\mathbb{F}$. For instance, under matrix addition, $M_{n,m}(\mathbb{F})$ forms a group that is of course written additively.

However, the more interesting operation is matrix multiplication. Since groups need inverses, define the *General Linear Group* as

$$GL(n,\mathbb{F}) = \{g \in M_{n,n}(\mathbb{F}) \mid g \text{ is invertible}\}.$$

Recall from linear algebra that there are a number of equivalent criteria for determining if $g \in M_{n,n}(\mathbb{F})$ is invertible. The first definition is that g is *invertible* if there is a matrix $h \in M_{n,n}(\mathbb{F})$ so that $gh = hg = I_n$ where I_n is the *identity matrix*

$$I_n = \operatorname{diag}(1,\dots,1) = \begin{pmatrix} 1 & 0 & & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$$

(here 1 means [1] and 0 means [0] in the case of $\mathbb{F} = \mathbb{Z}_p$).

However, as the reader will no doubt remember, one of the theoretically (if not always practically) most useful ways to test for invertibility is to check that $\det g \neq 0$. Hence if $g_1, g_2 \in GL(n,\mathbb{F})$, then $\det(g_1 g_2) = \det g_1 \det g_2 \neq 0$ so that $g_1 g_2 \in GL(n,\mathbb{F})$. In particular, matrix multiplication is a binary operation on $GL(n,\mathbb{F})$. Associativity is known from linear algebra. The identity element is clearly the identity matrix. Finally, inverses exist by definition. Thus, $GL(n,\mathbb{F})$ is a group under matrix multiplication.

There are quite a few variants on this theme. To name only a few, consider the *Special Linear Group* defined by

$$SL(n,\mathbb{F}) = \{g \in GL(n,\mathbb{F}) \mid \det g = 1\},$$

the *Orthogonal Group* defined by

$$O(n,\mathbb{F}) = \{g \in GL(n,\mathbb{F}) \mid gg^T = I_n\}$$

where g^T refers to the transpose of a matrix, and the *Special Orthogonal Group* defined by

$$SO(n,\mathbb{F}) = \{g \in O(n,\mathbb{F}) \mid \det g = 1\}.$$

Using properties of the determinant, it is easy to check that each one of these objects really is a group (see Exercise 2.18). As a final remark, it is worth noting that matrix groups are some of the very most important groups around.

1.3.5. *Symmetric Group, S_n.* Roughly speaking, the *symmetric group* or *permutation group* on n-letters is the set of all permutations or rearrangements of n objects. It is written as S_n and is also one of the most important groups. To avoid trivialities, we always tacitly assume $n \geq 2$. By relabeling, we may take the n objects to be the numbers $1, 2, \ldots, n$. For example, one element of S_3 rearranges the ordered set $\{1, 2, 3\}$ to $\{2, 3, 1\}$.

In order to make these notions precise, we think of each permutation as a map $\varphi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ that tells how to reorder things. For instance, the permutation $\{1, 2, 3\} \to \{2, 3, 1\}$ is realized by the map (of unordered sets) $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ defined by $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$. Notice that since permutations only rearrange the order, the map σ must be one-to-one and onto—in other words, a bijection.

This leads to our official definition:

$$S_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \sigma \text{ is bijective}\}.$$

If we desire to define an element $\sigma \in S_n$, we have n possible choices for the value of $\sigma(1)$. Since σ is bijective, that leaves $(n-1)$ remaining choices for $\sigma(2)$, then $(n-2)$ choices for $\sigma(3)$, and so on. In particular,

$$|S_n| = n\,(n-1)\,(n-2)\cdots 1 = n!.$$

There is a visual way of writing elements of S_n that is commonly used. Associate to $\sigma \in S_n$ the array

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

For instance, the permutation $\{1, 2, 3\} \to \{2, 3, 1\}$ is represented by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Conversely, the array $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ represents the permutation $\{1, 2, 3\} \to \{1, 3, 2\}$.

In order to make S_n into a group, a bilinear operation is still needed. This is provided by composition of functions. In particular for $\sigma_1, \sigma_2 \in S_n$, define

$$\sigma_1\sigma_2 = \sigma_1 \circ \sigma_2.$$

Since the composition of bijective functions is still bijective, this is a closed operation on S_n. As an example, suppose $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Then

$$\begin{aligned} (\sigma_1\sigma_2)\,(1) &= (\sigma_1 \circ \sigma_2)\,(1) = \sigma_1(\sigma_2(1)) = \sigma_1(1) = 2, \\ (\sigma_1\sigma_2)\,(2) &= (\sigma_1 \circ \sigma_2)\,(2) = \sigma_1(\sigma_2(2)) = \sigma_1(3) = 1, \\ (\sigma_1\sigma_2)\,(3) &= (\sigma_1 \circ \sigma_2)\,(3) = \sigma_1(\sigma_2(3)) = \sigma_1(2) = 3 \end{aligned}$$

so that

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

To see that the axioms of a group are satisfied, first recall that composition of functions is always associative. Next observe that the identity function $\mathrm{Id} \in S_n$

defined by $\mathrm{Id}(k) = k$, $1 \leq k \leq n$, clearly serves as the identity element e. In other words,

$$\mathrm{Id} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

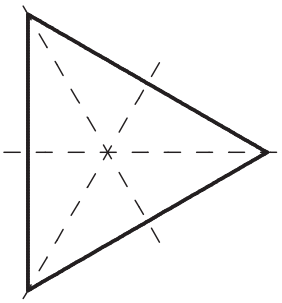
Finally, note that any $\sigma \in S_n$ has an inverse function, σ^{-1}, since it is bijective. By definition, this means $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}$. In particular, σ^{-1} is the required group inverse. For example, the inverse to the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ sends $\{2, 3, 1\} \to \{1, 2, 3\}$. Reordering, we see

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

1.3.6. *Dihedral Groups, D_n.* A *rigid motion* or *isometry* of the plane is a map $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves the distance between any two points; i.e., if $x, y \in \mathbb{R}^2$, then the distance from x to y is the same as the distance from $\varphi(x)$ to $\varphi(y)$. Using composition of functions as the bilinear operation, it is easy to see the set of rigid motions of the plane forms a group (cf. Exercise 2.29). Perhaps surprisingly, it turns out there are only four kinds of rigid motions: parallel translations, rotations about a point, reflections across a line, and glide reflections (a reflection about a line l followed by a translation parallel to l).

Given $S \subseteq \mathbb{R}^2$, the *symmetry group of* S is the set of rigid motions of the plane mapping S to S. It is straightforward to see that composition of functions makes the symmetry group of S into a group (Exercise 2.22). An important example occurs by taking S to be a regular n-gon, $n \geq 3$. In that case, the symmetry group is written D_n and is called the *dihedral group*.

For instance, D_3 is the set of rigid motions that preserve the triangle (the dotted lines are added to help visualize certain reflections):



There are six such motions: the identity map, rotations by 60° and 120°, and the three reflections across the dotted lines. While this is a wonderfully explicit geometric description, the notation can become a bit cumbersome when we turn to D_n for larger values of n.

To motivate notation suitable for D_n, observe that the six linear maps comprising D_3 are completely determined by their action on the three vertices of the triangle. In other words, instead of specifying an element of D_3 by giving an explicit rigid motion of the entire plane, it suffices to simply say where each of the three vertices are mapped. In order to make use of this observation, label the vertices with elements of $\mathbb{Z}_3$. Specifically, refer to the right-most vertex as [1], the top-most vertex as [2], and the bottom-most vertex as [3].

For instance, rotation by 60° maps vertex [1] to [2], [2] to [3], and [3] to [1] = [4]. In particular, rotation by 60° is realized by the map $[k] \to [k+1]$ on $\mathbb{Z}_3$. Similarly, rotation by 120° is realized by the map $[k] \to [k+2]$. The identity map is of course realized by the map $[k] \to [k]$. The reflections also have simple formulas. For instance, reflection across the horizontal dotted line maps [1] → [1], [2] → [3], and [3] → [2]. As the reader can readily check, this is realized by the map $[k] \to [2-k]$. Similarly, the other two reflections are given by the maps $[k] \to [1-k]$ and $[k] \to [3-k]$.

Therefore, let $R_j : \mathbb{Z}_3 \to \mathbb{Z}_3$ be defined by $R_j([k]) = [k+j]$ and let $W_j : \mathbb{Z}_3 \to \mathbb{Z}_3$ be defined by $R_j([k]) = [j-k]$. Given our above identifications, we see that

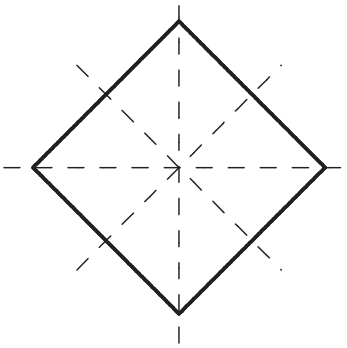
$$D_3 = \{R_0, R_1, R_2, W_0, W_1, W_2\}$$

with the binary operation given by composition of functions. For instance since

$$(R_1 \circ W_1)([k]) = R_1([1-k]) = [2-k] = W_2([k]),$$

it follows that $R_1W_1 = W_2$. Similarly since $R_1(R_1([k])) = [2+k] = R_2([k])$, it follows that $R_1R_1 = R_2$.

In a similar spirit, D_4 is the set of rigid motions that preserve the square (again, the dotted lines are included to help visualize certain reflections):



There are eight such motions: rotations by 0°, 90°, 180°, and 270° degrees and the four reflections across the dotted lines. Restricting our attention again to the vertices and labeling them by elements of $\mathbb{Z}_4$, it is easy to see that the rotations are realized by the maps $[k] \to [k+j]$ and that the reflections are realized by the maps $[k] \to [j-k]$ on $\mathbb{Z}_4$ for $j \in \{0,1,2,3\}$. Thus defining $R_j : \mathbb{Z}_4 \to \mathbb{Z}_4$ by $R_j([k]) = [k+j]$ and $W_j : \mathbb{Z}_4 \to \mathbb{Z}_4$ by $W_j([k]) = [j-k]$, it follows that

$$D_4 = \{R_0, R_1, R_2, R_3, W_0, W_1, W_2, W_3\}.$$

The binary operation is composition of functions. For instance, here $(R_1 \circ W_1)([k]) = R_1([1-k]) = [2-k] = W_2([k])$ so that $R_1W_1 = W_2$.

The general case can be handled by similar geometric considerations. Instead of belaboring the point, we jump to the punch line and give a more computationally friendly realization of the dihedral groups.

DEFINITION 2.3. Fix $n \in \mathbb{Z}$, $n \geq 3$.

(1) For $j \in \mathbb{Z}$, let $R_j : \mathbb{Z}_n \to \mathbb{Z}_n$ be defined by $R_j([k]) = [j+k]$ and let $W_j : \mathbb{Z}_n \to \mathbb{Z}_n$ be defined by $W_j([k]) = [j-k]$.

(2) The *dihedral group* is

$$D_n = \{R_j, W_j \mid j \in \mathbb{Z}\}.$$

The binary operation is composition of functions.

THEOREM 2.4. *Fix $n \in \mathbb{Z}$, $n \geq 3$. The dihedral group, D_n, is a group with*

$$|D_n| = 2n$$

satisfying the following relations:

$$\begin{aligned} R_i R_j &= R_{i+j} \text{ and } R_j^n = \mathrm{Id}, \\ W_i W_j &= R_{i-j} \text{ and } W_j^2 = \mathrm{Id}, \\ R_i W_j &= W_{i+j} \text{ and } W_i R_j = W_{i-j}. \end{aligned}$$

In particular, the identity element is R_0 and we can also write

$$D_n = \{R_1^j, R_1^j W_0 \mid 0 \leq j \leq n-1\}.$$

PROOF. To see that D_n is a group, it suffices to prove the above relations since (i) associativity always holds for composition of functions, (ii) R_0 clearly serves as an identity, and (iii) $R_j^{-1} = R_{-j}$ and $W_j^{-1} = W_j$. The verification of the identities is straightforward. For instance, to show $R_i W_j = W_{i+j}$, simply calculate that

$$R_i(W_j([k])) = R_i([j-k]) = [i+j-k] = W_{i+j}([k]).$$

The rest of the relations are handled similarly and are left to the reader (Exercise 2.26). □

1.4. Exercises 2.1–2.29.

1.4.1. *Arithmetic.*

EXERCISE 2.1. **(a)** With respect to addition, show that the set of even integers, $2\mathbb{Z}$, is a group but that the set of odd integers, $2\mathbb{Z}+1$, is not a group.

(b) With respect to complex multiplication, show $\pm\{1, i\}$ is a group.

(c) With respect to multiplication, show $\{5^a \mid a \in \mathbb{Q}\}$ is a group.

(d) With respect to addition, show $\{a \in \mathbb{Z} \mid a \equiv 0 \bmod(3)\}$ is a group but that $\{a \in \mathbb{Z} \mid a \equiv 1 \bmod(3)\}$ is not.

(e) With respect to multiplication in $\mathbb{R}$, show $(0, 1]$ is not a group.

(f) Show that $U_9 = \mathbb{Z}_9 \backslash \{[0], [3], [6]\}$ and that $\{[1], [4], [7]\} \subseteq U_9$ is a group with respect to multiplication.

EXERCISE 2.2. Define a binary operation on $\mathbb{R}$ by $x * y = x + y + 1$.

(a) Find $e \in \mathbb{R}$ so that $x * e = e * x = x$ for all $x \in \mathbb{R}$.

(b) Given $x \in \mathbb{R}$, find $y \in \mathbb{R}$ so that $x * y = y * x = e$.

(c) Show $*$ makes $\mathbb{R}$ into a group.

EXERCISE 2.3. Define a binary operation on $\mathbb{R}$ by $x * y = x + xy$. Show $*$ is not associative and that there is no identity element. In particular, $*$ does not make $\mathbb{R}$ into a group.

EXERCISE 2.4. Let $n \in \mathbb{N}$ and let $\zeta(n) = \{z \in \mathbb{C} \mid z^n = 1\}$.

(a) Show $\zeta(n)$ is a group under complex multiplication.

(b) Show $\zeta(n) = \{e^{\frac{2k\pi i}{n}} \mid k = 0, 1, \ldots, (n-1)\}$.

(c) Show there is a bijection $\varphi : \mathbb{Z}_n \to \zeta(n)$ so that $\varphi([a] + [b]) = \varphi([a])\varphi([b])$.

EXERCISE 2.5 ($\mathbb{Z}_n[x]$). Let $\mathbb{Z}_n[x]$, $n \in \mathbb{N}$, be the set of polynomials with coefficients in $\mathbb{Z}_n$; i.e., $\mathbb{Z}_n[x] = \{\sum_{k=0}^{\infty} a_k x^k \mid a_k \in \mathbb{Z}_n$, all but finitely many $a_k = [0]\}$. Define addition and multiplication of polynomials in the usual fashion. Namely, if $f = \sum_k a_k x^k$ and $g = \sum_k a'_k x^k$,

$$f + g = \sum_k (a_k + a'_k)\, x^k \quad \text{and} \quad fg = \sum_k \left(\sum_{j=0}^{k} a_j a'_{k-j} \right) x^k.$$

(a) Show the above definitions of addition and multiplication are well defined binary operations on $\mathbb{Z}_n[x]$.

(b) Show $\mathbb{Z}_n[x]$ is a group under addition.

(c) Show $\mathbb{Z}_n[x]$ is not a group under multiplication.

EXERCISE 2.6 (Baby Division Alogrithm for Polynomials). If $f = \sum_k a_k x^k \in \mathbb{Z}_n[x]$ with $f \neq [0]$, $a_m \neq [0]$, and $a_k = [0]$ for $k > m$, we say the *degree* of f is $\deg(f) = m$ (cf. Exercise 2.5). If $a \in \mathbb{Z}_n$, write $f(a) = \sum_{k=0}^{m} a_k a^k \in \mathbb{Z}_n$.

(a) Fix $a \in \mathbb{Z}_n$ and $f \in \mathbb{Z}_n[x]$ with $\deg(f) = m$. Show there is $h_{m-1} \in \mathbb{Z}_p[x]$ with $\deg(h_{m-1}) \leq (m-1)$ so $f = a_m(x-a)^m + h_{m-1}$.

(b) Show $f = \sum_{k=0}^{m} b_k (x-a)^k$ for some $b_k \in \mathbb{Z}_n$ with $b_m = a_m$ and $b_0 = f(a)$.

(c) Show f can be written as $f = (x-a)g + f(a)$ for some $g \in \mathbb{Z}_n[x]$ with $\deg(g) = m - 1$.

EXERCISE 2.7 (Zeros). If $f \in \mathbb{Z}_n[x]$ with $f \neq [0]$ and $a \in \mathbb{Z}_n$, we say a is a *zero* of f if $f(a) = [0]$ (cf. Exercise 2.6).

(a) If $\deg(f) = m$, show $a \in \mathbb{Z}_p$ is a zero of f if and only if $f = (x-a)g$ for some $g \in \mathbb{Z}_n[x]$ with $\deg(g) = m - 1$.

(b) If p is a prime and $f \in \mathbb{Z}_p[x]$ has $\deg(f) = m$, show f has at most m (distinct) zeros in $\mathbb{Z}_p$.

(c) Show by example that if p is replaced by a nonprime, then part (b) can be false. *Hint:* In $\mathbb{Z}_8$, look at $x^2 - [1]$.

1.4.2. *Circle.*

EXERCISE 2.8. Recall that we defined $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. Let $S' = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$, $S = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$, and $SO(2, \mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$.

(a) Show $S^1 = S'$ and establish a bijection between S^1 and S.

(b) Show there is a bijection $\varphi : S^1 \to SO(2, \mathbb{R})$ so that $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$.

1.4.3. *Linear Algebra.*

EXERCISE 2.9. Let $G = GL(2, \mathbb{Z}_2)$.

(a) Write down all elements in G.

(b) Multiply $\begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix} \begin{pmatrix} [0] & [1] \\ [1] & [1] \end{pmatrix}$.

(c) Find $\begin{pmatrix} [0] & [1] \\ [1] & [1] \end{pmatrix}^{-1}$.

(d) Find all $g \in G$ so that $g^2 = I_2$.

EXERCISE 2.10. Let $G = GL(2, \mathbb{Z}_3)$.

(a) Write down all elements in G.

(b) Multiply $\begin{pmatrix}[1] & [2]\\ [0] & [1]\end{pmatrix}\begin{pmatrix}[0] & [1]\\ [1] & [2]\end{pmatrix}$.

(c) Find $\begin{pmatrix}[0] & [1]\\ [1] & [2]\end{pmatrix}^{-1}$.

(d) Find all $g \in G$ so that $g^2 = I_2$.

EXERCISE 2.11. Show the following subsets of $GL(n,\mathbb{F})$ are groups under matrix multiplication.

(a) $D(n,\mathbb{F}) = \{\text{diag}(c_1,\ldots,c_n) \mid c_i \neq 0,\ 1 \leq i \leq n\}$.

(b) $U(n,\mathbb{F}) = \{$upper triangular matrices with 1's on the main diagonal$\}$. *Hint:* Use the cofactor method of computing the inverse to see that $U(n,\mathbb{F})$ contains its inverses.

(c) $N(n,\mathbb{F}) = \{$upper triangular matrices with nonzero entries on the main diagonal$\}$.

EXERCISE 2.12. Let $G = \{\begin{pmatrix} a & b\\ -b & a\end{pmatrix} \mid a^2+b^2 \neq 0,\ a,b \in \mathbb{R}\}$.

(a) Show each $g \in G$ can be uniquely written as $\lambda\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$ for $\lambda \in \mathbb{R}^+$ and $\theta \in [0, 2\pi)$.

(b) With respect to matrix multiplication, show G is a group.

EXERCISE 2.13 (Quaternion Group, Q). Define the symbols $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ as the following elements of $GL(2,\mathbb{C})$:

$$\mathbf{1} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \mathbf{i} = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},\ \mathbf{j} = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\ \mathbf{k} = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}.$$

Using matrix multiplication, show $Q = \pm\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ is a group satisfying $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$, $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$, and $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$. The group Q is called the *Quaternion Group*.

EXERCISE 2.14 (Heisenberg Group). **(a)** Let $H_3(\mathbb{R}) = \left\{\begin{pmatrix}1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix} \mid x,y,z \in \mathbb{R}\right\}$. Show $H_3(\mathbb{R})$ is a group under matrix multiplication. It is called the 3-dimensional *Heisenberg Group*.

(b) Writing matrices in $1\times n\times 1$ block form, let $H_{2n+1}(\mathbb{R}) = \left\{\begin{pmatrix}1 & x & z\\ 0 & I_n & y^T\\ 0 & 0 & 1\end{pmatrix} \mid x, y \in \mathbb{R}^n \text{ and } z \in \mathbb{R}\right\}$ (here $\cdot^T$ denotes *transpose*). Show $H_{2n+1}(\mathbb{R})$ is a group under matrix multiplication. It is called the $(2n+1)$-dimensional *Heisenberg group*.

(c) Find all $Z \in H_{2n+1}(\mathbb{R})$ so that $gZ = Zg$ for all $g \in H_{2n+1}(\mathbb{R})$.

EXERCISE 2.15. Let $(x,y),(x',y') \in \mathbb{R}^\times \times \mathbb{R}$ and define $(x,y) * (x',y') = (xx', xy' + yx')$. Let $M(2,\mathbb{R}) = \left\{\begin{pmatrix}x & y\\ 0 & x\end{pmatrix} \mid x,y \in \mathbb{R},\ x \neq 0\right\}$.

(a) Show $*$ makes $\mathbb{R}^\times \times \mathbb{R}$ into a group.

(b) Show $M(2,\mathbb{R})$ is a group with respect to matrix multiplication.

(c) Show there is a bijection $\varphi : \mathbb{R}^\times \times \mathbb{R} \to M(2,\mathbb{R})$ so that $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.

EXERCISE 2.16. Let $A = \left\{ \begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{R} \right\}$.

(a) Show that matrix multiplication gives an associative binary operation on A.

(b) Show A has a *left identity* and *right inverse*; i.e., show there exits $e_L \in A$ so that (i) $e_L a = a$ for all $a \in A$ and (ii) for each $a \in A$, there is a $b \in A$ so $ab = e_L$.

(c) Nevertheless, show A is not a group.

EXERCISE 2.17 ($SL(2,\mathbb{Z})$). Let $SL(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1 \text{ and } a, b, c, d \in \mathbb{Z} \right\}$. Show $SL(2,\mathbb{Z})$ is a group.

EXERCISE 2.18. Show $SL(n,\mathbb{F})$, $O(n,\mathbb{F})$, and $SO(n,\mathbb{F})$ are groups.

1.4.4. *Symmetric Group.*

EXERCISE 2.19. Multiply the following elements of S_3 (parts (a)–(c)) or S_5 (parts (d) and (e)):

(a) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

(b) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$,

(c) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$,

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$,

(e) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$.

EXERCISE 2.20. Find the inverse to the following elements of S_3 (parts (a) and (b)) or S_5 (parts (c) and (d)):

(a) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$,

(b) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$,

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$,

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$.

EXERCISE 2.21. Find all $\sigma \in S_3$ so that:

(a) $\sigma^2 = \mathrm{Id}$.

(b) $\sigma^3 = \mathrm{Id}$.

EXERCISE 2.22. Given nonempty $S \subseteq \mathbb{R}^2$, show that the set of rigid motions of the plane mapping S to S forms a group under composition of functions.

1.4.5. *Dihedral groups.*

EXERCISE 2.23. Multiply the following elements of D_3 and write them in the form R_1^j or $R_1^j W_1$ for $0 \le j \le 2$:

(a) $R_1 W_2$,

(b) $W_2 R_1$,

(c) $W_1R_2W_2$,
(d) R_1^{20}.

EXERCISE 2.24. Multiply the following elements of D_4 and write them in the form R_1^j or $R_1^jW_1$ for $0 \leq j \leq 3$:
(a) R_3W_2,
(b) W_3R_2,
(c) $R_2W_2R_1$.

EXERCISE 2.25. Find the inverse of the following elements of D_5 and write them in the form R_1^j or $R_1^jW_1$ for $0 \leq j \leq 4$:
(a) W_1R_4,
(b) $R_2W_3R_1$.

EXERCISE 2.26. Verify the remaining portions of Theorem 2.4.

1.4.6. *Miscellaneous.*

EXERCISE 2.27. For a set S, define a binary operation on the power set $\mathcal{P}(S)$ by $X * Y = (X \cup Y) \backslash (X \cap Y)$. Show that $*$ makes $\mathcal{P}(S)$ into a group.

EXERCISE 2.28. Write $\mathcal{F}(\mathbb{R})$ for the set of all functions $f : \mathbb{R} \to \mathbb{R}$. For $f, g \in \mathcal{F}(\mathbb{R})$, define binary operations $(f+g)$ and $(f \cdot g)$ by $(f+g)(x) = f(x)+g(x)$ and $(f \cdot g)(x) = f(x)g(x)$ for $x \in \mathbb{R}$.
(a) Show $\mathcal{F}(\mathbb{R})$ is a group under addition but not multiplication.
(b) Let $\mathcal{C}^0(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) \mid f \text{ is continuous}\}$. Show $\mathcal{C}^0(\mathbb{R})$ is a group under addition. *Calculus fact:* the sum of continuous functions is continuous.
(c) Let $\mathcal{C}^\infty(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) \mid f \text{ is infinitely differentiable}\}$. Show $\mathcal{C}^\infty(\mathbb{R})$ is a group under addition. *Calculus fact:* the sum of infinitely differentiable functions is infinitely differentiable.
(d) Let $\mathcal{F}^{\text{ev}}(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) \mid f(-x) = f(x),\ x \in \mathbb{R}\}$. Show $\mathcal{F}^{\text{ev}}(\mathbb{R})$ is a group under addition.
(e) Let $\mathcal{F}^+(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) \mid f(x) > 0,\ x \in \mathbb{R}\}$. Show $\mathcal{F}^+(\mathbb{R})$ is a group under multiplication but not addition.
(f) Show $\{f \in \mathcal{F}(\mathbb{R}) \mid f(0) = 0\}$ is a group under addition but that $\{f \in \mathcal{F}(\mathbb{R}) \mid f(0) = 1\}$ is not.

EXERCISE 2.29 (Motions of $\mathbb{R}^n$). A *motion* of $\mathbb{R}^n$ is a bijection of $\mathbb{R}^n$ onto $\mathbb{R}^n$. The set of motions is a group under composition of functions. Arbitrary motions of $\mathbb{R}^n$ are usually not very useful objects; however, certain subsets of motions arise frequently in applications.
(a) A *translation* of $\mathbb{R}^n$ is a motion of the form $T_v : \mathbb{R}^n \to \mathbb{R}^n$ where $T_v(x) = x + v$ for $x, v \in \mathbb{R}^n$. Show the set of translations is a group.
(b) A *linear motion* of $\mathbb{R}^n$ is a motion of the form $T_g : \mathbb{R}^n \to \mathbb{R}^n$ where $T_g(x) = gx$ for $x \in \mathbb{R}^n$ and $g \in GL(n, \mathbb{R})$ where gx is given by matrix multiplication. Show the set of linear motions is a group.
(c) An *affine motion* of $\mathbb{R}^n$ is a motion of the form $T_{g,v} : \mathbb{R}^n \to \mathbb{R}^n$ where $T_{g,v}(x) = gx + v$ for $x, v \in \mathbb{R}^n$ and $g \in GL(n, \mathbb{R})$. Show the set of affine motions is a group.
(d) Show the set of rigid motions of the plane forms a group.