# First-Semester Abstract Algebra: A Structural Approach

Jessica K. Sklar
Pacific Lutheran University
sklarjk@plu.edu

Last updated: July 23, 2017

# Acknowledgments

Thank you to Jennifer Nordstrom of Linfield College for introducing me to the American Institute of Mathematics (AIM) Open Textbook Initiative (`https://aimath.org/textbooks/`); to Rob Beezer at the University of Puget Sound for encouraging my engagement with this initiative and for helping me make connections within the community; and to David Farmer at AIM for typesetting this book in MathBook XML (`http://mathbook.pugetsound.edu`).

# Contents

# Introduction

At its most basic level, abstract algebra is the study of structures. Just as an architect may examine buildings or an anthropologist societal hierarchies, an algebraist explores the nature of sets equipped with binary operations that satisfy certain properties. While these structures may not seem at first to be very important, they are at the heart of most, if not all, mathematical endeavors. On an elemental level, they allow us to solve systems of equations; on a more global-level, they are behind some of our most important cryptographic systems. We even use them implicitly when telling time!

Our focus in this course will be exploring some of the most fundamental algebraic structures: namely, groups, rings, and fields. Along the way, we will explore rigorous mathematical notions of similarity and difference: When can we consider two objects to be more or less "the same"? When are they fundamentally different? For instance, consider two houses that have exactly the same construction, but are painted different colors. Are they the same house? No. But viewed structurally (as opposed to aesthetically) they are the same. This means that if we know certain information about one of the houses (say, how far the bathroom is from the kitchen) we know the same information about the other house. However, knowing that the first house is painted yellow does not tell us anything about the second house's color. We explore an analogous idea in mathematics, namely, the concept of *isomorphism*.

Along the way, we will gain experience writing mathematical proofs and will see plenty of specific examples demonstrating more general ideas.

# Chapter 1

# Preliminaries

## 1.1 Notation

To start, we begin learning and/or reviewing some notation. Here is a table of frequently used symbols and abbreviations we will use, along with their meanings.

| **Notation** | **Meaning** |
|---|---|
| $\forall$ | for all/for every |
| $\exists$ | there exists |
| s.t. | such that* |
| $\therefore$ | therefore |
| WLOG or wolog | without loss of generality† |
| WTS | want to show |
| ! | unique (also used to denote factorials) |
| $\Rightarrow$ | implies; also the "if" direction in proofs |
| $\Leftarrow$ | only if; also the "only if" direction in proofs |
| $\Leftrightarrow$ or iff | if and only if |
| w/ | with |
| o.w. | otherwise |

* You can also use $\ni$ to denote "such that," but we will avoid this convention as it can be confused with the notation $\in$, meaning "is an element of."

† We will discuss what this means in greater detail as it arises in our work.

Finally, the notation $:=$ means we are assigning a definition. E.g., writing "Let $S := \{1, 2, 3\}$" means we are defining $S$ to be the set $\{1, 2, 3\}$. We often omit the colon and simply write $=$ in these cases, but we may include it to emphasize the fact that we are defining something.

## 1.2 Sets

Now we provide a "definition" of a basic mathematical object to which we will soon add bells and whistles.

**"Sort of" definition.** A *set* is an (unordered) collection of objects.

We say this is a "sort of" definition because it is not a rigorous definition of a set. For instance, what do we mean by a "collection" of objects? This "definition" will be sufficient for our course, but be warned that defining a set in this vague way can lead to some serious mathematical issues, such as Russell's paradox[1]; a mathematician whose expertise is in set theory may scowl disagreeably if you try to define a set as we have above.

**Definitions and notation.** The members of a set are called its *elements*. If $S$ is a set, we write $x \in S$ to indicate "$x$ is an element of $S$," and $x \notin S$ to indicate "$x$ is not an element of $S$." There is a unique set containing no elements; it is called the *empty set*, and denoted by $\emptyset$.

Sets must be *well defined*: that is, it must be clear exactly which objects are in a set, and which objects aren't. For instance, the set of all integers is well defined, but the set of all big integers is not well defined, since it is unclear what "big" means in this context.

We refer to some sets so frequently in mathematics that we have special notation for them. Common examples are:

| **Notation** | **Meaning** |
|---|---|
| $\mathbb{Z}$ | the set of all integers |
| $\mathbb{Q}$ | the set of all rational numbers |
| $\mathbb{R}$ | the set of all real numbers |
| $\mathbb{C}$ | the set of all complex numbers |
| $\mathbb{N}$ | the set of all natural numbers (that is, the set $\{0, 1, 2, \ldots\}$)* |
| $\mathbb{Z}^+/\mathbb{Q}^+/\mathbb{R}^+$ | the set of all positive integers/rational numbers/real numbers |
| $\mathbb{Z}^-/\mathbb{Q}^-/\mathbb{R}^-$ | the set of all negative integers/rational numbers/real numbers |
| $\mathbb{Z}^-/\mathbb{Q}^-/\mathbb{R}^-/\mathbb{C}^*$ | the set of all nonzero integers/rational numbers/real numbers/ complex numbers |

* Be aware that many books/mathematicians do not include 0 in the set of natural numbers.

We also provide notation for commonly considered sets of matrices:

**Notation.** Given $m, n \in \mathbb{Z}^+$ and a set $S$, we define $\mathbb{M}_{m\times n}(S)$ to be the set of all $m \times n$ matrices over $S$ (that is, of all $m \times n$ matrices with entries in $S$). We use the shorthand notation $\mathbb{M}_n(S)$ for the set $\mathbb{M}_{n\times n}(S)$.

One common way of describing a set is to list its elements in curly braces, separated by commas; you can use ellipses to indicate a repeated pattern of elements. A few examples are $\{1, 4, \pi\}$, $\{3, 4, 5, \ldots\}$, and $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$; the last of these can be written more concisely as $\{0, \pm 2, \pm 4, \ldots\}$. Note that since elements of a set are unordered, the sets $\{1, 4, \pi\}$ and $\{4, \pi, 1\}$, for instance, are identical.

Another method is using *set-builder notation*. This consists of an element name (or names), followed by a colon (meaning "such that"), followed by a Boolean expression involving the

[1] Let $S$ be the set of all sets that aren't members of themselves. Is $S$ a member of itself? If you think carefully about this, you'll see that $S$ can be neither a member of itself, nor not a member of itself. Uh oh! This contradiction is known as Russell's paradox (named for the British philosopher, mathematician, and all-round academic Bertrand Russell). Mathematicians deal with this by declaring that some object collections, called *classes*, are not in fact sets.

element name(s), all surrounded by curly braces.[2] For example,

$$\{x \in \mathbb{Z} : x > 4\}$$

is the set $\{5, 6, 7, \ldots\}$, while

$$\{z \in \mathbb{C} : |z| = 1\}$$

is the set of all complex numbers at distance 1 from the origin in the complex plane.

**Note.** If one simply writes $\{x : x > 4\}$, it is unclear what this set is; it could be the set of all integers greater than 4, or the set of all real numbers greater than 4, or something else. When one can, it is better to identify the named element(s) as a member (members) of a known set, such as $\mathbb{R}$ or $\mathbb{Z}$, whenever possible.

**Definitions and notation.** Set $A$ is a *subset* of $B$ (and set $B$ is a *superset* of $A$) if every element in $A$ is also in $B$. We denote "$A$ is a subset of $B$" by $A \subseteq B$. Sets $A$ and $B$ are said to be *equal*, and we write $A = B$, if they contain exactly the same elements; equivalently, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Set $A$ is a *proper* subset of set $B$ if $A \subseteq B$ but $A \neq B$; we write this $A \subsetneq B$ or $A \subset B$ [3].

**Remark.** One often proves that two sets $A$ and $B$ are equal by proving that $A \subseteq B$ and $B \subseteq A$.

**Example 1.1.** We have the following: $\mathbb{Z}^+ \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

**Definition.** The *power set* of $A$, denoted $P(A)$, is the set of all subsets of $A$. (Note that the power set of any set contains the empty set as an element.)

> **WARNING**
>
> Be careful to use your curly braces correctly when writing power sets! Remember, the power set of a set is a *set of sets*.

The following provides a good example of using braces correctly.

**Example 1.2.** If $A = \{a, b\}$, then $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Note that the element $\{a, b\}$ of $P(A)$ could also be written simply as $A$.

**Definitions and notation.**

1. If $A$ and $B$ are sets, then the *union* of $A$ and $B$, denoted $A \cup B$, is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$; the *intersection* of $A$ and $B$, denoted $A \cap B$, is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$; and the *difference* of $A$ and $B$, denoted $A - B$ (or $A \setminus B$), is the set $A - B = \{x : x \in A \text{ and } x \notin B\}$.

2. More generally, given any collection of sets $A_i$ ($i$ in some index set $I$), the *union* of the $A_i$ is

$$\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ for some } i \in I\},$$

[2] **WARNING:** The use of a colon to denote "such that" is *only* valid in the above set-builder notation context. Outside of this context, you should never use a colon to denote "such that"; instead, write out the actual words or use the abbreviation s.t. (or the symbol $\ni$, though I do not recommended). Conversely, never use one of those ways of indicating "such that" within set-builder notation; always use a colon there. Why? Convention.

[3] **WARNING:** Sometimes the notation $A \subset B$ is merely used to indicate that $A$ is a subset of $B$ (but may equal $B$). Be careful to check what your book or peer means by this notation.

and the *intersection* of the $A_i$ is

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for every } i \in I\}.$$

3. Sets $A$ and $B$ are *disjoint* if $A \cap B = \emptyset$. More generally, sets $A_i$ ($i$ in some index set $I$) are *disjoint* if
$$\bigcap_{i \in I} A_i = \emptyset$$
and are *mutually disjoint* if
$$A_i \cap A_j = \emptyset \text{ for all } i \neq j \in I.$$

Notice that for any sets $A$ and $B$, $A \cap B \subseteq A \subseteq A \cup B$ and $A \cap B \subseteq B \subseteq A \cup B$. Also note that if sets $A_i$ ($i \in I$) are mutually disjoint then they are also disjoint, but they may be disjoint without being mutually disjoint. For example, the sets $\{i, i+1\}$ for $i \in \mathbb{Z}$ are disjoint but not mutually disjoint. (Do you see why?)

We define one more way of "combining" sets.

**Definitions.** Let $A$ and $B$ be sets. Then the *(direct) product* $A \times B$ of $A$ and $B$ is the set

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

An element $(a, b)$ of $A \times B$ is called an *ordered pair*. More generally, if $A_1, A_2, \ldots, A_n$ are sets for some $n \in \mathbb{Z}^+$, then the *product* of the $A_i$ is

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i \text{ for each } i\};$$

the elements $(a_1, a_2, \ldots, a_n)$ of this product are called $n$-tuples (or triples, if $n = 3$).[4] Finally, if each set $A_i$ is the same set $A$, we can use the notation $A^n$ to denote the product

$$A \times A \times \cdots \times A$$

of $n$ copies of $A$.

**Example 1.3.** For example, the Cartesian plane is the set $\mathbb{R}^2$, and the set $\mathbb{Z} \times \mathbb{R}$ consists of exactly the points in the plane with integer $x$-coordinates (that is, the points that lie on vertical lines intersecting the $x$-axis at integer values).

## 1.3 Functions

You have probably encountered functions before. In introductory calculus, for instance, you typically deal with functions from $\mathbb{R}$ to $\mathbb{R}$ (e.g., the function $f(x) = x^2$). More generally, functions "send" elements of one set to elements of another set; these sets may or may not be sets of real numbers. We provide below a "good enough for government work" definition of a function.

**Definitions and notation.** A *function* $f$ from a set $S$ to a set $T$ is a "rule" that assigns to each element $s$ in $S$ a unique element $f(s)$ in $T$; the element $f(s)$ is called the *image of $s$ under*

[4] You can also have products of infinitely many sets, but we will not discuss that in this course.

$f$. If $f$ is a function from $S$ to $T$, we write $f : S \to T$, and call $S$ the *domain* of $f$ and $T$ the *codomain* of $f$. The *range* of $f$ is

$$f(S) = \{f(s) \in T : s \in S\} \subseteq T.$$

More generally, if $U \subseteq S$, the *image of $U$ in $T$ under $f$* is

$$f(U) = \{f(u) \in T : u \in U\}.$$

If $V \subseteq T$, the *preimage of $V$ in $S$ under $f$* is the set

$$f^{\leftarrow}(V) = \{s \in S : f(s) \in V\}.$$

**Example 1.4.** Consider the function $f : \mathbb{Z} \to \mathbb{R}$ defined by $f(x) = x^2$. The domain of $f$ is $\mathbb{Z}$ and the codomain of $f$ is $\mathbb{R}$; the range of $f$ is $\{x^2 : x \in \mathbb{Z}\} = \{0, 1, 4, 9, \ldots\}$. The image of $\{-2, -1, 1, 2\}$ under $f$ is the two-element set $\{1, 4\} \subseteq \mathbb{R}$, and the preimage of $\{4, 25, \pi\}$ under $f$ is the set $\{\pm 2, \pm 5\}$. (Do you see why $\pm\sqrt{\pi}$ are not in this preimage?) What is the preimage of just $\{\pi\}$ under $f$?

The following definitions will be very important in our future work.

**Definitions.** Let $S$ and $T$ be sets, and $f : S \to T$.

1. Function $f$ is *one-to-one* (1-1) if whenever $s_1, s_2 \in S$ with $f(s_1) = f(s_2)$, we have $s_1 = s_2$. Equivalently, $f$ is one-to-one if whenever $s_1 \neq s_2 \in S$, then $f(s_1) \neq f(s_2) \in T$.
2. Function $f$ is *onto* if for every $t \in T$, there exists an element $s \in S$ such that $f(s) = t$. Equivalently, $f$ is onto if $f(S) = T$.
3. Function $f$ is a *bijection* if it is both one-to-one and onto.

We will often have to show functions are one-to-one or onto. Given a function $f : S \to T$, the following methods are recommended.

| | |
|---|---|
| **To prove that $f$ is one-to-one** | Let $s_1, s_2 \in S$ with $f(s_1) = f(s_2)$ and prove that then $s_1 = s_2$. **WARNING:** It is <u>not</u> sufficient to prove that if $s_1 = s_2$ in $S$ then $f(s_1) = f(s_2)$; that is true for any function from $S$ to $T$! Be careful to *assume* and *prove* the correct facts. |
| **To prove that $f$ is *not* one-to-one** | Identify two elements $s_1 \neq s_2$ of $S$ such that $f(s_1) = f(s_2)$. |
| **To prove that $f$ is onto** | Let $t \in T$ and prove that there exists an element $s \in S$ with $f(s) = t$. **WARNING:** It is <u>not</u> sufficient to prove that if $s \in S$ then $f(s)$ is in $T$; that is true for any function from $S$ to $T$! Again, be careful to *assume* and *prove* the correct facts. |
| **To prove that $f$ is *not* onto** | Identify an element $t \in T$ for which there is no $s \in S$ with $f(s) = t$. |

**Example 1.5.** Consider the function $f : \mathbb{R}^* \to \mathbb{R}^+$ defined by $f(x) = x^2$. Function $f$ is *not* one-to-one: indeed, $-1$ and $1$ are in $\mathbb{R}^*$ with $f(-1) = 1 = f(1)$ in $\mathbb{R}^+$. However, $f$ *is* onto: indeed, let $t \in \mathbb{R}^+$. Then $\sqrt{t} \in \mathbb{R}^*$ with $t = f(\sqrt{t})$, so we're done.

**Example 1.6.** Consider the function $f : \mathbb{Z}^+ \to \mathbb{R}$ defined by $f(x) = x/2$. Function $f$ *is* one-to-one: indeed, let $s_1, s_2 \in \mathbb{Z}^+$ with $f(s_1) = f(s_2)$. Then $s_1/2 = f(s_1) = f(s_2) = s_2/2$; multiplying both sides of the equation $s_1/2 = s_2/2$ by 2, we obtain $s_1 = s_2$. However, $f$ is *not* onto: for example, $\pi \in \mathbb{R}$ but there is no positive integer $s$ for which $f(s) = s/2 = \pi$.

Recall that we can combine certain functions using *composition*: if $f : S \to T$ and $g : T \to U$, then $g$ *composed with* $f$ is the function $g \circ f : S \to U$ defined by

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

for all $s \in S$.[5] Also recall that given any set $S$, the *identity function on* $S$ is the function $1_S : S \to S$ defined by $1_S(s) = s$ for every $s \in S$.

**Definitions.** Let $f$ be a function from $S$ to $T$. A function $g$ from $T$ to $S$ is an *inverse* of $f$ if $g \circ f$ and $f \circ g$ are the identity functions on $S$ and $T$, respectively; that is, if for all $s \in S$ and $t \in T$, $g(f(s)) = s$ and $f(g(t)) = t$. If $f$ has an inverse, we say that $f$ is *invertible*.

We present three theorems, omitting the proofs of the first two.

**Theorem 1.7.** *If $f$ has an inverse, then that inverse is unique.*

**Notation.** If $f$ is invertible, we denote its unique inverse by $f^{-1}$.

**Theorem 1.8.** *Function $f : S \to T$ has an inverse if and only if $f$ is a bijection. Also, if $f$ has inverse $f^{-1}$, then $f^{-1}$ is also a bijection.*

**Theorem 1.9.** *Let $f : S \to T$ and $g : T \to U$ be functions. If $f$ and $g$ are both 1-1 [onto], then so is $g \circ f : S \to U$.*

*Proof.* Assume $f$ and $g$ are 1-1. Let $s_1, s_2 \in S$ with $(g \circ f)(s_1) = (g \circ f)(s_2)$. Then $g(f(s_1)) = g(f(s_2))$; since $g$ is one-to-one (since it's a bijection), this shows that $f(s_1) = f(s_2)$. Then since $f$ is one-to-one (since $f$ is also a bijection), we must have $s_1 = s_2$. Thus, $g \circ f$ is one-to-one. □

The proof that $g \circ f$ is onto if $f$ and $g$ are onto is left as an exercise for the reader.

## 1.4 Cardinality

One of the set traits that will be useful to us in distinguishing between algebraic structures is *cardinality*.

**Definitions.** A set is *finite* if it contains a finite number of elements (including the case in which it contains no elements); otherwise, it's *infinite*.

**Definition.** The *cardinality of a finite set* is the number of elements in that set.

But what is the cardinality of an infinite set? This is more subtle. Essentially, it is the "size" of the set, but what does that mean?

[5] More generally, you can compose functions $f : S \to T$ and $g : R \to U$ to form $g \circ f : S \to U$, as long as $f(S) \subseteq R$.

**Definitions and notation.** The symbol $\aleph_0$ denotes the cardinality of the set $\mathbb{Z}$. An arbitrary set $S$ has cardinality $\aleph_0$ if there exists a bijection from $S$ to $\mathbb{Z}$ (equivalently, if there exists a bijection from $\mathbb{Z}$ to $S$).

Note that if there is a bijection from $S$ to $\mathbb{Z}$, then $S$ must be infinite. If the cardinality of $S$ is $\aleph_0$, we say $S$ is *countably infinite*. If $S$ is finite or countably infinite, we say it's *countable*. Finally, an infinite set is *uncountably infinite*, or *uncountable*, if it is not countably infinite. In this class, we don't discuss the cardinality of uncountably infinite sets, but simply note that an uncountable set cannot have the same cardinality as a countable one.

**Notation.** We denote the cardinality of a set $S$ by $|S|$.[6]

So, e.g., $|\{a, b\}| = 2$.

**Example 1.10.** Clearly, $\mathbb{Z}$ itself is countably infinite.

Perhaps surprisingly, a proper subset of a set can have the same cardinality as its superset, as the following example shows.

**Example 1.11.** We claim that $\mathbb{Z}^+$ is countably infinite. Indeed, consider the function $f : \mathbb{Z}^+ \to \mathbb{Z}$ defined by $f(n) = (-1)^n \lfloor n/2 \rfloor$, where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to $x$, for each $x \in \mathbb{R}$. The fact that $f$ is a bijection is demonstrated (though not proven) by the following visual representation, where each number maps via $f$ to the value directly below it:

$$\begin{array}{cccccccccc} & \mathbb{Z}^+ & 1 & 2 & 3 & 4 & 5 & \dots \\ f & \downarrow & & & & & & \\ & \mathbb{Z} & 0 & 1 & -1 & 2 & -2 & \dots \end{array}$$

Note that this means that $\mathbb{Z}$ and its proper subset $\mathbb{Z}^+$ have the same cardinality, that is, the same "size"!

We summarize here examples of countably and uncountably infinite sets. (On pp. 5–6 of [1], Fraleigh sketches proofs of the facts that $\mathbb{Q}$ is countable and that the interval $(0, 1)$ in $\mathbb{R}$ is uncountable. The proof then that $\mathbb{R}$ is uncountable follows from Theorem 1.12, which follows.)

| | |
|---|---|
| Countably infinite sets: | $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Z}^-$, $\mathbb{Z}^*$, $\mathbb{Q}$, $\mathbb{Q}^+$, $\mathbb{Q}^-$, $\mathbb{Q}^*$, $\mathbb{N}$ |
| Uncountably infinite sets: | $\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{R}^-$, $\mathbb{R}^*$, $\mathbb{C}$, $\mathbb{C}^*$, the interval $(0, 1)$ in $\mathbb{R}$ |

The key idea here for us is that if two sets are essentially "the same," then they must have the same "size." Thus, we see that there is some fundamental difference between the sets $\mathbb{Z}$ and $\mathbb{R}$ (in fact, there are many such differences). On the other hand, cardinality alone won't allow us to distinguish structurally between the sets $\mathbb{Z}$ and $\mathbb{Z}^+$.

We end our preliminary chapter with the following theorem and a corollary of it (which can be proved using induction on $n$).

**Theorem 1.12.** *Let $A$ and $B$ be sets.*

1. *If $A \subseteq B$ and $A$ is infinite [uncountable] then so is $B$.*
2. *If $A \subseteq B$ and $B$ is finite [countable] then so is $A$.*

[6] Of course, vertical bars are used to denote other mathematical concepts; for instance, if $x$ is a real number, $|x|$ usually denotes the absolute value of $x$. You must determine from context, and from the nature of the expression within the bars, what vertical bars mean in a particular situation.

3. *If* $|A| = n < \infty$ *and* $|B| = m < \infty$, *then* $|A \times B| = mn$.

4. *Any finite product of countable sets is countable.*[7]

*Proof.* We omit proofs of the statements in Parts 1 and 2. The proof of the statement in Part 3 is left as an exercise for the reader. □

For Part 4: Let $A$ and $B$ be countable sets. Assume that $A$ and $B$ are both countably infinite. Since $\mathbb{Z}^+$ is countably infinite, we can index the elements of $A$ and of $B$ by $\mathbb{Z}^+$, writing

$$A = \{a_1, a_2, \ldots\} \quad \text{and} \quad B = \{b_1, b_2, \ldots\}.$$

Notice that the table

$$\begin{array}{cccc} (a_1, b_1) & (a_1, b_2) & (a_2, b_3) & \cdots \\ (a_2, b_1) & (a_2, b_2) & (a_2, b_3) & \cdots \\ (a_3, b_1) & (a_3, b_2) & (a_3, b_3) & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

contains every element of $A \times B$. We can then list the elements of $A \times B$ by listing the elements in progressive upper-right to lower-left diagonals, starting with $(a_1, b_1)$ and moving to the right along the top row: that is, we can write

$$A \times B = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_2), (a_3, b_1), \ldots\}$$

This implicitly yields a bijection from $\mathbb{Z}^+$ to $A \times B$; thus, $A \times B$ is countably infinite, and hence countable.

The proof in the case that one or both of sets $A$ and $B$ are finite is similar; the corresponding table in that case will simply have either only finitely many rows or finitely many columns, or both.

**Corollary 1.13.** *Let* $n > 1$ *be an integer and let* $A_1, A_2, \ldots, A_n$ *be countable sets. Then* $A_1 \times A_2 \times \cdots \times A_n$ *is countable.*

[7] **Note.** It is **not** true that any countable product of countable (or even finite) sets is countable. Indeed, even the set $\{0, 1\} \times \{0, 1\} \times \cdots$ is uncountable. (If you want to get into the gory details of this, the key is that there is a bijection from this set to the power set of the natural numbers, which Cantor's Theorem tells us is uncountable. You are welcome to jump down this rabbit hole by googling "Cantor's Theorem," if you desire, but know that you will not be responsible for that material in class.)

## 1.5 Exercises

### Exercise 1.1

Yes/No. For each of the following, write Y if the object described is a well-defined set; otherwise, write N. You do NOT need to provide explanations or show work for this problem.

(a) $\{z \in \mathbb{C} : |z| = 1\}$

(b) $\{\varepsilon \in \mathbb{R}^+ : \varepsilon \text{ is sufficiently small}\}$

(c) $\{q \in \mathbb{Q} : q \text{ can be written with denominator } 4\}$

(d) $\{n \in \mathbb{Z} : n^2 < 0\}$

### Exercise 1.2

List the elements in the following sets, writing your answers as sets.

**Example:** $\{z \in \mathbb{C} : z^4 = 1\}$ **Solution:** $\{\pm 1, \pm i\}$

(a) $\{z \in \mathbb{R} : z^2 = 5\}$

(b) $\{m \in \mathbb{Z} : mn = 50 \text{ for some } n \in \mathbb{Z}\}$

(c) $\{a, b, c\} \times \{1, d\}$

(d) $P(\{a, b, c\})$

### Exercise 1.3

Let $S$ be a set with cardinality $n \in \mathbb{N}$. Use the cardinalities of $P(\{a, b\})$ and $P(\{a, b, c\})$ to make a conjecture about the cardinality of $P(S)$. You do not need to prove that your conjecture is correct (but you should try to ensure it is correct).

### Exercise 1.4

Let $f : \mathbb{Z}^2 \to \mathbb{R}$ be defined by $f(a, b) = ab$. (Note: technically, we should write $f((a, b))$, not $f(a, b)$, since $f$ is being applied to an ordered pair, but this is one of those cases in which mathematicians abuse notation in the interest of concision.)

(a) What are $f$'s domain, codomain, and range?

(b) Prove or disprove each of the following statements. (Your proofs do not need to be long to be correct!)

  (i) $f$ is onto;

  (ii) $f$ is 1-1;

  (iii) $f$ is a bijection. (You may refer to parts (i) and (ii) for this part.)

(c) Find the images of the element $(6, -2)$ and of the set $\mathbb{Z}^- \times \mathbb{Z}^-$ under $f$. (Remember that the image of an element is an element, and the image of a set is a set.)

(d) Find the preimage of $\{2, 3\}$ under $f$. (Remember that the preimage of a set is a set.)

### Exercise 1.5

Let $S$, $T$, and $U$ be sets, and let $f : S \to T$ and $g : T \to U$ be onto. Prove that $g \circ f$ is onto.

### Exercise 1.6

Let $|A| = n < \infty$ and $|B| = m < \infty$. Prove that $|A \times B| = mn$.

# Chapter 2

# Groups

## 2.1 Binary operations and structures

So far we have been discussing sets. These are extremely simple objects, essentially mathematical "bags of stuff." Without any added structure, their usefulness is very limited. Imagine, for instance, living with friends in a two-story house without rooms, stairs, closets, or hallways. You have no privacy, cannot access the second floor, etc. A set with no added structure will not help us, say, solve a linear equation. What *will* help us with such things are objects such as groups, rings, fields, and vector spaces. These are sets equipped with *binary operations* which allow us to combine set elements in various ways. We first rigorously define a binary operation.

**Definitions and notation.** A *binary operation* on a set $S$ is a function from $S \times S$ to $S$. Given a binary operation $*$ on $S$, for each $(a, b) \in S \times S$ we denote $*((a, b))$ in $S$ more simply by $a * b$. (Intuitively, a binary operation $*$ on $S$ assigns to each pair of elements $a, b \in S$ a unique element $a * b$ of $S$.)

A set $S$ equipped with a binary operation $*$ is called a *binary (algebraic) structure*, and is denoted by $\langle S, * \rangle$, or just by $S$, if $*$ is understood from context.

**Remarks.**

1. For $*$ to be a binary operation on $S$, $a*b$ must be **well defined** and **in S** for each $a, b \in S$. For instance, we cannot define a binary operation on $\mathbb{R}$ by

$$a * b = \text{ the greatest number less than } a + b$$

since there *is* no such "greatest number." Nor can we define a binary operation on $\mathbb{Z}$ by $a * b = ab/2$, since for, say, $a = b = 1 \in \mathbb{Z}$, $ab/2 = 1/2 \notin \mathbb{Z}$.

2. Not every binary operation is denoted by $*$. In fact, many already have common notations: for instance, $+$ on $\mathbb{Z}$ or $\circ$ on the set of functions from $\mathbb{R}$ to $\mathbb{R}$. We will assume these common notations represent the "usual" binary operations we know them to mean, unless otherwise noted.

3. Do not mix up the $*$ that indicates a binary operation and the superscript $^*$ that indicates that we are only considering the nonzero elements of a given set (e.g., $\mathbb{R}^*$). You should be able to tell which type of $*$ we are using from context and placement. Also, make sure you correctly place these symbols!

**Definition.** A binary operation $*$ on a set $S$ is *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

**Remark.** When a binary operation is associative, we can omit parentheses when operating on set elements. For example, $+$ is associative on $\mathbb{Z}$, so we can unambiguously write the (equal) expressions $1 + (2 + 3)$ and $(1 + 2) + 3$ as $1 + 2 + 3$.

**Definitions.** A binary operation $*$ on set $S$ is *commutative* if

$$a * b = b * a$$

for all $a, b \in S$. We say that specific elements $a$ and $b$ of $S$ *commute* if $a * b = b * a$.

**Definition.** Let $\langle S, * \rangle$ be a binary structure. An element $e$ in $S$ is an *identity element of* $\langle S, * \rangle$ if $x * e = e * x = x$ for all $x \in S$.

**Note.** Sometimes an identity element of $\langle S, * \rangle$ is referred to as an *identity element of $S$ under* $*$, or, when $*$ is clear from context, simply as an *identity element of* $S$.

**WARNING**

Not every binary structure contains an identity element! (Ex: $\langle \mathbb{Z}, - \rangle$)

A natural question to ask is if a binary structure can have more than one identity element? The answer is no!

**Theorem 2.1.** *A binary structure $\langle S, * \rangle$ has **at most one** identity element. That is, identity elements in binary structures, when they exist, are unique.*

*Proof.* Assume that $e$ and $f$ are identity elements of $S$. Then since $e$ is an identity element, $e * f = f$ and since $f$ is an identity element, $e * f = e$. Thus, $e = f$. □

**Definition.** Let $\langle S, * \rangle$ be a binary structure with identity element $e$. Then for $a \in S$, $b$ is an *(two-sided) inverse of $a$ in $\langle S, * \rangle$* if $a * b = b * a = e$.

**Note.** We can also refer to such an element $b$ as an *inverse for $a$ in $S$ under* $*$, or, when $*$ is clear from context, simply as an *inverse of* $a$.

**WARNING**

1. Not every element in a binary structure with an identity element has an inverse!
2. If a binary structure **does not have** an identity element, it **doesn't even make sense** to say an element in the structure does or does not have an inverse!

**Theorem 2.2.** *Let $\langle S, * \rangle$ be a binary structure with an identity element, where $*$ is associative. Let $a \in S$. If $a$ has an inverse, then its inverse is unique.*

*Proof.* Let $e$ be the identity element of $S$. Suppose $a$ has inverses $b$ and $c$. Then $a * b = e$ so, multiplying both sides of the equation by $c$ on the left, we have $c * (a * b) = c * e = c$. But since $*$ is associative, we have $c * (a * b) = (c * a) * b = e * b = b$. But $b = c$. Thus, $a$'s inverse is unique. □

## 2.2 Exercises, Part I

### Exercise 2.1

For each of the following, write Y if the given "operation" is a well-defined binary operation on the given set; otherwise, write N. In each case in which it isn't a well-defined binary operation on the set, provide a *brief* explanations. You do not need to prove or explain anything in the cases in which it is a binary operation.

(a) $+$ on $\mathbb{C}^*$

(b) $*$ on $\mathbb{R}^+$ defined by $x * y = \log_x y$

(c) $*$ on $\mathbb{M}_2(\mathbb{R})$ defined by $A * B = AB^{-1}$

(d) $*$ on $\mathbb{Q}^*$ defined by $z * w = z/w$

### Exercise 2.2

Define $*$ on $\mathbb{Q}$ by $p * q = pq + 1$. Prove or disprove that $*$ is (a) commutative; (b) associative.

### Exercise 2.3

Prove that matrix multiplication is not commutative on $\mathbb{M}_2(\mathbb{R})$.

### Exercise 2.4

Prove or disprove each of the following statements.

(a) The set $2\mathbb{Z} = \{2x : x \in \mathbb{Z}\}$ is closed under addition in $\mathbb{Z}$.

(b) The set $S = \{1, 2, 3\}$ is closed under multiplication in $\mathbb{R}$.

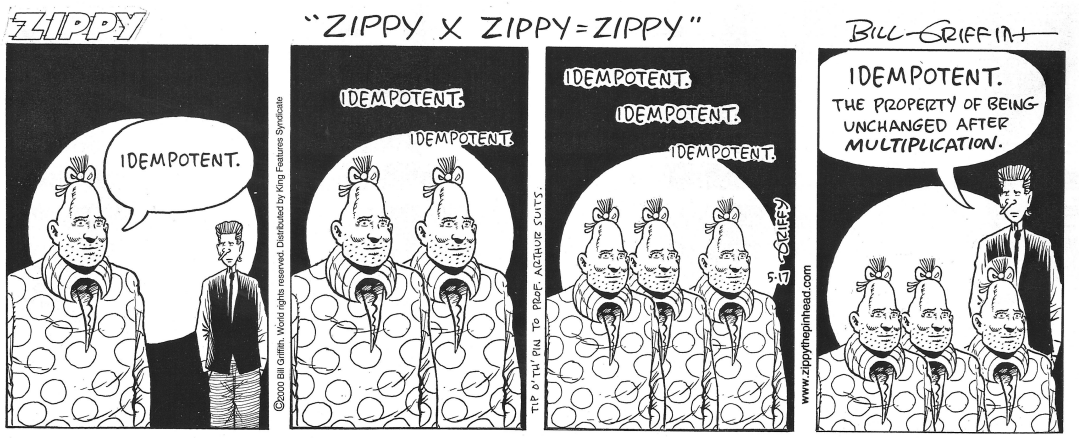
(c) The set

$$U = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$

is closed under multiplication in $\mathbb{M}_2(\mathbb{R})$. (Recall that $U$ is the set of *upper-triangular matrices* in $\mathbb{M}_2(\mathbb{R})$.)

### Exercise 2.5

Let $*$ be an associative and commutative binary operation on a set $S$. An element $u \in S$ is said to be an *idempotent* in $S$ if $u * u = u$. Let $H$ be the set of all idempotents in $S$. Prove that $H$ is closed under $*$.




©Bill Griffith. Reprinted with permission.

## 2.3 The definition of a group

At this point you may be asking yourself, why do we care? We've covered a lot of definitions and proved some theorems, but what is the goal of all this? Well, there are actually many goals that we can achieve using such material. Consider the following as an example. Suppose we want to solve the equation $5 + x = 2$. We can probably solve this quite easily almost just by looking at it ($x = -3$), but what facts are we actually using there? If we break down the reasoning leading to this answer, we may obtain something like the following set of steps.

$$\begin{array}{rrcr} & 5+x & = & 2 \\ \Rightarrow & -5+(5+x) & = & -5+2 \\ \Rightarrow & (-5+5)+x & = & -3 \\ \Rightarrow & 0+x & = & -3 \\ \Rightarrow & x & = & -3 \end{array} .$$

In line 2, we add the inverse of 5 in $\langle \mathbb{Z}, + \rangle$ to each side of the equation. In line 3, we use associativity of $+$ in $\mathbb{Z}$ (along with computation), while in line 4 we use the fact that $-5$ is the additive inverse of 5 (that is, the inverse of 5 in $\mathbb{Z}$ under $+$). Finally, in line 5 we use the fact that 0 is an additive identity element in $\mathbb{Z}$ (that is, the identity element in $\mathbb{Z}$ under $+$).

In summary, we used **associativity, identity elements, and inverses** in $\mathbb{Z}$ to solve the given equation. This perhaps suggests that these would be useful traits for a binary structure and/or its operation to have. They are in fact so useful that a binary structure displaying these characteristics is given a special name. We note that these axioms are rather strong; "most" binary structures aren't groups.

**Definition and notation.** A *group* is a set $G$, equipped with a binary operation $*$, that satisfies the following three *group axioms*:

$\mathscr{G}_1$: $*$ is associative on $G$;

$\mathscr{G}_2$: There exists an identity element for $*$ in $G$;

$\mathscr{G}_3$: Every element $a \in G$ has an inverse in $G$.

We denote group $G$ under $*$ by the binary structure notation $\langle G, * \rangle$, or simply by $G$ if the operation $*$ is known from context (or need not be known in the current situation).

**IMPORTANT NOTE**

When proving/disproving that a set $G$ is/is not a group under an (apparent) operation $*$:

- The first thing you should do is check to make sure that $\langle G, * \rangle$ is a binary structure by making sure $G$ is closed under $*$—if not, it doesn't make sense to check to see if axioms $\mathscr{G}_1$–$\mathscr{G}_3$ hold). (For instance: $\mathbb{Z}^*$ has no chance of being a group under $\div$, since, e.g., $3, 4 \in \mathbb{Z}^*$ but $3 \div 4 \notin \mathbb{Z}^*$.)
- You should never check $\mathscr{G}_3$ before confirming $\mathscr{G}_2$ holds, because it makes no sense to look for inverses if you haven't confirmed that $G$ contains an identity element under $*$.

## 2.4 Examples of groups/nongroups, Part I

Let's look at some examples of groups/nongroups.

**Example 2.3.** We claim that $\mathbb{Z}$ is a group under addition. Indeed, we already know that $\mathbb{Z}$ is closed under addition and that addition is associative on the integers. The integer 0 acts as an identity element of $\mathbb{Z}$ under addition (since $a + 0 = 0 + a = a$ for each $a \in \mathbb{Z}$), and each element $a$ in $G$ has inverse $-a$ since $a + (-a) = -a + a = 0$.

**Example 2.4.**

1. For each following binary structure $\langle G, * \rangle$, determine whether or not $G$ is a group.
2. For those that are *not* groups, determine the first group axiom that fails, and provide a proof that it fails.

| | | | |
|---|---|---|---|
| $\langle \mathbb{Q}, + \rangle$ | $\langle \mathbb{Z}, - \rangle$ | $\langle \mathbb{R}, \cdot \rangle$ | $\langle \mathbb{C}^*, \cdot \rangle$ |
| $\langle \mathbb{R}, + \rangle$ | $\langle \mathbb{Z}^+, + \rangle$ | $\langle \mathbb{Z}^*, \cdot \rangle$ | $\langle \mathbb{M}_n(\mathbb{R}), + \rangle$ |
| $\langle \mathbb{C}, + \rangle$ | $\langle \mathbb{Z}, \cdot \rangle$ | $\langle \mathbb{R}^*, \cdot \rangle$ | $\langle \mathbb{M}_n(\mathbb{R}), \cdot \rangle$ |

If you have taken linear algebra, you have also probably seen a collection of matrices that is a group under matrix multiplication.

**Definitions.** For $n \in \mathbb{Z}^+$, we define $GL(n, \mathbb{R})$ by

$$GL(n, \mathbb{R}) := \{M \in \mathbb{M}_n(\mathbb{R}) : \det M \neq 0\}.$$

In other words, $G$ is the set of all invertible $n \times n$ matrices over $\mathbb{R}$. We also define subset $SL(n, \mathbb{R})$ of $GL(n, \mathbb{R})$, by

$$SL(n, \mathbb{R}) := \{M \in \mathbb{M}_n(\mathbb{R}) : \det M = 1\}.$$

**Notation.** We may use the notation $\mathbf{0}$ to denote a zero matrix and $I_n$ to denote an $n \times n$ identity matrix.

**Remark.** Throughout this course, if we are discussing a set $GL(n, \mathbb{R})$ or $SL(n, \mathbb{R})$, you should assume $n \in \mathbb{Z}^+$, unless otherwise noted.

**Theorem 2.5.** *$GL(n,\mathbb{R})$ and $SL(n,\mathbb{R})$ are closed under matrix multiplication (so $\langle GL(n,\mathbb{R}),\cdot\rangle$ and $\langle SL(n,\mathbb{R}),\cdot\rangle$ are binary structures).*

*Proof.* Let $A, B \in GL(n,\mathbb{R})$. Then $\det(AB) = (\det A)(\det B) \neq 0$ (since $\det A, \det B \neq 0$), so $AB \in GL(n,\mathbb{R})$. Similarly, if $A, B \in SL(n,\mathbb{R})$, then $\det(AB) = (\det A)(\det B) = 1(1) = 1$, so $AB \in SL(n,\mathbb{R})$. □

**Example 2.6.** The binary structures $GL(n,\mathbb{R})$ and $SL(n,\mathbb{R})$ are groups under matrix multiplication.

*Proof.* Let $G := GL(n,\mathbb{R})$. We show that $G$, under matrix multiplication, satisfies the three group axioms.

$\mathscr{G}_1$: Matrix multiplication is always associative.

$\mathscr{G}_2$: The $n \times n$ identity matrix

$$I_n := \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \in G$$

acts as an identity element for $\langle G,\cdot\rangle$ since

$$AI_n = I_n A = A$$

for all $A \in G$.

$\mathscr{G}_3$: Let $A \in G$. Since $\det A \neq 0$, $A$ has (matrix multiplicative) inverse $A^{-1}$ in $\mathbb{M}_2(\mathbb{R})$. But we need to verify that $A^{-1}$ is in $G$. This is in fact the case, however, since $A^{-1}$ is invertible (it has inverse $A$), hence $\det A^{-1} \neq 0$. Thus, $A^{-1}$ is also in $G$.

So $G$ is a group under multiplication.
The proof that $SL(n,\mathbb{R})$ is a group under multiplication is left as an exercise for the reader. □

These groups are very important in many areas of mathematics, including linear algebra and geometry. Because of this, we have special names for them (which give rise to the "GL" and "SL" in their names).

**Definitions.** For $n \in \mathbb{Z}^+$, $GL(n,\mathbb{R})$ is called the *general linear group of degree $n$ over $\mathbb{R}$* and $SL(n,\mathbb{R})$ is called the *special linear group of degree $n$ over $\mathbb{R}$*.

**Example 2.7.** Define $*$ on $\mathbb{Q}^*$ by $a * b = (ab)/2$ for all $a, b \in \mathbb{Q}^*$. Prove that $\langle \mathbb{Q}^*, *\rangle$ is a group.

*Proof.* First, $\mathbb{Q}^*$ is closed under $*$, since $(ab)/2$ is rational and nonzero whenever $a, b$ are rational and nonzero.

Next, we check that $\mathbb{Q}^*$ under $*$ satisfies the group axioms. Since multiplication is commutative on $\mathbb{Q}$, $*$ is clearly commutative on $\mathbb{Q}^*$, and so our work to show $\mathscr{G}_2$ and $\mathscr{G}_3$ is marginally reduced.

$\mathscr{G}_1$: Associativity of $*$ on $\mathbb{Q}^*$ is inherited from associativity of multiplication on $\mathbb{Q}^*$.

$\mathscr{G}_2$: Notice that the perhaps "obvious" choice, 1, is not an identity element for $\mathbb{Q}^*$ under $*$: for instance, $1 * 3 = 3/2 \neq 3$. Rather, $e$ is such an identity element if and only if for all $a \in \mathbb{Q}$ we have $a = e * a = (ea)/2$. We clearly have $a = (2a)/2$ for all $a \in \mathbb{Q}^*$; so 2 acts as an identity element for $\mathbb{Q}^*$ under $*$.

$\mathscr{G}_3$: Let $a \in \mathbb{Q}^*$. Since $a \neq 0$, it makes sense to divide by $a$; then $4/a \in \mathbb{Q}^*$, with $a * (4/a) = (a(4/a))/2 = 2$.

Thus, $\langle \mathbb{Q}^*, * \rangle$ is a group. □

## 2.5 Group conventions and properties

Before we discuss more examples, we present a theorem and look at some conventions we follow and notation we use when discussing groups in general; we also discuss some properties of groups.

### 2.5.1 Some group conventions

**Theorem 2.8.** *The identity element of a group is unique (by Theorem 2.1), and given any element $a$ of a group $G$, the inverse of $a$ in $G$ is unique (by Theorem 2.2).*

- We usually **don't** use the notation $*$ when describing group operations. Instead, we use the multiplication symbol $\cdot$ for the operation in an arbitrary group, and call applying the operation "multiplying"—even though the operation may not be "multiplication" in the non-abstract, traditional sense! It may actually be addition of real numbers, composition of functions, etc.

  Moreover, when actually operating in a group $\langle G, \cdot \rangle$, we typically omit the $\cdot$. That is, for $a, b \in G$, we write the product $a \cdot b$ as $ab$. We call this the "product" of $a$ and $b$. We will generally use $e$ or $e_G$ as our default notation for an identity element of group,[1] and $a^{-1}$ to denote the inverse of element $a$ in $G$.

  **WARNING**

  Although it is what we call *multiplicative notation* for an inverse, do not assume $a^{-1}$ is what we usually think of as a multiplicative inverse for $a$; remember, we don't even know if elements of a group are numbers! The type of inverse that $a^{-1}$ is (a multiplicative inverse for a real number? an additive inverse for a real number? a multiplicative inverse for a matrix? an inverse function for a function from $\mathbb{R}$ to $\mathbb{R}$?) depends on both $G$'s elements and its operation.

- For every element $a$ in a group $\langle G, \cdot \rangle$ and $n \in \mathbb{Z}^+$, we use the expression $a^n$ to denote the product

$$\underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ times}}$$

  and $a^{-n}$ to denote $(a^{-1})^n$ (that is, the product of $n$ copies of $a^{-1}$). Finally, we define $a^0$ to be $e$. Note that our "usual" rules for exponents then hold in an arbitrary group: that is, if $a$ is in group $\langle G, \cdot \rangle$ and $m, n \in \mathbb{Z}$, then $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn} = (a^n)^m$.

[1] Many mathematicians denote a group's identity element by 1, rather than $e$.

There are exceptions to these conventions:

- When working with an operation that is known to be commutative, we typically continue to use additive notation ($+$ for the group operation, $-a$ for the inverse of element $a$ in the group) and call the operation "addition," though using $\cdot$ is also valid in these cases. When we use additive notation, we do not omit the $+$ when operating in a group $\langle G, + \rangle$, and we call $a + b$ a *sum* rather than a product.[2] For $n \in \mathbb{Z}^+$, we write $na$ instead of $a^n$; we also write $0a$ instead of $a^0$. Finally, note that $(-n)a = n(-a) = -(na)$ (where $-a$ and $-(na)$ indicate the additive inverses of $a$ and $na$, respectively); we can therefore unambiguously use the notation $-na$ for this element. Using this notation, note that for $m \in \mathbb{Z}$, $na + ma = (n + m)a$ and $n(ma) = (nm)a$.

> **WARNING**
>
> Be careful to always know where an element you are working with lives! For instance, if, as above, $n \in \mathbb{Z}^+$ and $a$ is a group element, $-n$ and $-a$ look similar but may mean very different things. While $-n$ is a negative integer, $-a$ may be the additive inverse of a matrix in $\mathbb{M}_2(\mathbb{R})$, the additive inverse 2 of the number 4 in $\mathbb{Z}_6$, or even something completely unrelated to numbers.

We summarize multiplicative versus addition notation in the following table, where $a, b$ are elements of a group $G$.

| | **Multiplicative notation*** | **Additive notation†** |
|---|---|---|
| Operation notation | $\cdot$ | $+$ |
| $a$ operated with $b$ | product $ab$ | sum $a + b$ |
| Identity element | 1 (or $e$ or $e_G$) | 0 (or $e$ or $e_G$) |
| Inverse of $a$ | $a^{-1}$ | $-a$ |

* Used in an arbitrary group.
† Used only in abelian groups.

- We **do** use the notation $*$ when using multiplicative or additive notation would lead to confusion. For instance, if we want to define an operation on $\mathbb{Q}^*$ that assigns to pair $(a, b)$ the quantity $ab/2$, it would be unwise to use multiplicative or additive notation for this operation since we already have conventional meanings of $ab$ and $a+b$. Similarly, we would not denote the identity element of $\mathbb{Q}^*$ under this operation by 0 or 1, since the identity element in this group is the rational number 2, and writing $0 = 2$ or $1 = 2$ would look weird.

- If there is a default notation for a particular operation (say, $\circ$ for composition of functions) or identity element (say, $I_n$ in $GL(n, \mathbb{R})$) we usually use that notation instead.

[2] Also, when working with an operation that is known to be commutative, the identity element may be denoted by 0 rather than by $e$, $e_G$, or 1.

### 2.5.2 Some group properties

While we don't need to worry about "order" when multiplying a group element $a$ by itself, we **do** need to worry about it in general.

> **WARNING**
>
> Group operations need *not* be commutative!

**Definitions.** A group $\langle G, \cdot \rangle$ is said to be *abelian*[3] if $ab = ba$ for all $a, b \in G$. Otherwise, $G$ is *nonabelian*.

**Remark.** If we know that a binary operation $\cdot$ on a set $G$ is commutative, then in checking to see if axioms $\mathscr{G}_2$ and $\mathscr{G}_3$ hold we need only verify that there exists $e \in G$ such that $ae = a$ (we don't need to check that $ea = a$) for all $a \in G$ and that for each $a \in G$ there exists $b \in G$ such that $ab = e$ (we don't need to check that $ba = e$).

**Remark.** If $G$ is not known to be abelian, we must be careful when multiplying elements of $G$ by one another: multiplying on the left is, in general, not the same as multiplying on the right!

**Definitions.** If $G$ is a group, then the cardinality $|G|$ of $G$ is called the *order of* $G$. If $|G|$ is finite, then $G$ is said to be a *finite group*; otherwise, it's an *infinite group*.

**Example 2.9.** Of the groups we've discussed, which are abelian? Which are infinite/finite?

We have already seen that identity elements of groups are unique, and that each element $a$ of a group $G$ has a unique inverse $a^{-1} \in G$. Here are some other basic properties of groups.

**Theorem 2.10.** *If $\langle G, \cdot \rangle$ is a group, then* **left and right cancellation laws** *hold in $G$. That is, if $a, b, c \in G$, then*

1. *If $ab = ac$, we have $b = c$ (the left cancellation law); and*
2. *If $ba = ca$, we have $b = c$ (the right cancellation law).*

*Proof.* Let $a, b, c \in G$ and assume that $ab = ac$. Multiplying both equation sides on the left by $a^{-1}$, we obtain

$$\begin{aligned} & a^{-1}(ab) = a^{-1}(ac) \\ \Rightarrow \quad & (a^{-1}a)b = (a^{-1}a)c \\ \Rightarrow \quad & eb = ec \\ \Rightarrow \quad & b = c \end{aligned}$$

This proves that the left cancellation law holds. A similar proof shows that the right cancellation law holds. □

**Theorem 2.11.** *Let $\langle G, \cdot \rangle$ be a group and let $a, b \in G$. Then there exist* **unique** *elements $x, y \in G$ such that $ax = b$ and $ya = b$.*

[3] The word "abelian" is derived from the surname of mathematician Niels Henrik Abel.

*Proof.* If $x = a^{-1}b$ and $y = ba^{-1}$, then $ax = a(a^{-1}b) = (aa^{-1})b = eb = b$ and $ya = (ba^{-1})a = b(a^{-1}a) = be = b$. So such elements $x$ and $y$ exist. The fact that they are unique follows from the cancellation laws: if $ax = b$ and $ax' = b$ then $x = x'$ by left cancellation, and if $ya = b$ and $y'a = b$ then $y = y'$ by right cancellation. □

**WARNING**

We only of necessity have $(ab)^{-1} = a^{-1}b^{-1}$ if $G$ is known to be abelian!

However, we do have the following:

**Theorem 2.12.** *If $a$ and $b$ are elements of a group $\langle G, \cdot \rangle$, then*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

*Proof.* We have that

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

Similarly, $(b^{-1}a^{-1})(ab) = e$. □

## 2.6 Examples of groups/nongroups, Part II

**Example 2.13.** Let $n \in \mathbb{Z}^+$. We define $n\mathbb{Z}$ by

$$n\mathbb{Z} = \{nx : x \in \mathbb{Z}\} :$$

that is, $n\mathbb{Z}$ is the set of all (integer) multiples of $n$.

**Theorem 2.14.** *$n\mathbb{Z}$ is a group under $+$ (the usual addition of integers).*

*Proof.* Let $x, y \in n\mathbb{Z}$. Then there exist $a, b \in \mathbb{Z}$ such that $x = na$ and $y = nb$. Then $x + y = na + nb = n(a + b) \in n\mathbb{Z}$. So $\langle n\mathbb{Z}, + \rangle$ is a binary structure. The remainder of the proof is left as an exercise for the reader. □

**Remark.** When we are discussing a group $n\mathbb{Z}$, assume that $n \in \mathbb{Z}^+$, unless otherwise noted.

We use an example from our next class of groups all the time; in fact, most six-year-olds do as well, since it is used when telling time! Before we get to the example, we need some more definitions and some notation. Throughout the following discussion, assume $n$ is a fixed positive integer.

**Definitions and notation.** We say integers $a$ and $b$ are *congruent modulo [or mod] $n$* if $n$ divides $a - b$. If $a$ and $b$ are congruent mod $n$, we write $a \equiv b \pmod{n}$.

**Example 2.15.** $1, 7, 13$, and $-5$ are all congruent mod 6.

The following is a profoundly useful theorem; it's so important, it has a special name. We omit the proof of this theorem, but direct interested readers to for, instance, p. 5 in [3].

**The Division Algorithm.** Let $n \in \mathbb{Z}^+$ and let $a$ be any integer. Then there exist unique integers $q$ and $r$, with $0 \leq r < n$, such that $a = qn + r$.[4]

It follows that for each positive integer $n$ and integer $a$, there exists a unique element $R_n(a)$ (the $r$ in the above theorem) of the set $\{0, 1, 2, \ldots, n-1\}$ such that $a$ is congruent to $R_n(a)$ modulo $n$. For example, $R_3(4) = 1$, $R_3(0) = 0$, $R_3(17) = 2$, and $R_3(-5) = 1$.

**Definition.** $R_n(a)$ is the *remainder* when we divide $a$ by $n$. (Note: You were probably already familiar with the remainder when you divide a **positive** integer by $n$.)

**Definition.** We define *addition modulo* $n$, $+_n$, on $\mathbb{Z}$ by, for all $a, b \in \mathbb{Z}$,

$$a +_n b = R_n(a + b),$$

that is, the unique element of $\{0, 1, \ldots, n-1\}$ that's congruent to the integer $a + b$ modulo $n$.

**Remark.** Addition mod 24 is what we use to tell time!

The set $\{0, 1, 2, \ldots, n-1\}$ of remainders when dividing by $n$ is so important we give it a special notation.

**Notation.** We denote by $\mathbb{Z}_n$ the set $\{0, 1, 2, \ldots, n-1\}$.

Throughout this course, if we are discussing a set $\mathbb{Z}_n$, you should assume $n \in \mathbb{Z}^+, n \geq 2$, unless otherwise noted. (Though it will rarely come up for us, we may occasionally make reference to $\mathbb{Z}_1 = \{0\}$.)

**WARNING**

Note that by our definition of $\mathbb{Z}_n$, the integer $n$ itself is <u>not</u> in $\mathbb{Z}_n$!

We are now ready to consider our next type of group.

**Example 2.16.** For each $n \in \mathbb{Z}^+$, $\langle \mathbb{Z}_n, +_n \rangle$ is a group, called the *cyclic group of order* $n$ (we will see later why we use the word "cyclic" here). This group is abelian and of order $n$.

*Proof.* We first check that $\mathbb{Z}_n$ is closed under $+_n$. Note that by the definition of $+_n$, $a +_n b \in \mathbb{Z}_n$ for each $a, b \in \mathbb{Z}$. Thus, $a +_n b \in \mathbb{Z}_n$ for each $a, b \in \mathbb{Z}_n$.

We next check that $\mathbb{Z}_n$ under $+_n$ satisfies the three group axioms. Note that since addition is commutative on $\mathbb{Z}$,

$$a +_n b = R_n(a + b) = R_n(b + a) = b +_n a$$

for all $a, b \in \mathbb{Z}_n$. Again, a simpler way of stating this is that commutativity of $+_n$ on $\mathbb{Z}_n$ is inherited from the commutativity of addition on $\mathbb{Z}$. One nice result of this is that since $+_n$ is commutative on $\mathbb{Z}_n$, we have less to check when verifying group axioms $\mathscr{G}_2$ and $\mathscr{G}_3$.

[4] This is actually a special case of a more general theorem, which states that given any integers $n$ and $a$, there exist unique integers $q$ and $r$, with $0 \leq r < |n|$, such that $a = qn + r$.

$\mathscr{G}_1$: Let $a, b, c \in \mathbb{Z}_n$. We want to show that $(a +_n b) +_n c = a +_n (b +_n c)$. Now,

$$\begin{aligned}(a +_n b) +_n c &= R_n(a+b) +_n c \\ &\equiv R_n(a+b) + c && \pmod{n} \\ &\equiv (a+b) + c && \pmod{n} \\ &\equiv a + (b+c) && \pmod{n} \\ &\equiv a + R_n(b+c) && \pmod{n} \\ &\equiv a +_n (b +_n c) && \pmod{n}.\end{aligned}$$

So $(a +_n b) +_n c$ and $a +_n (b +_n c)$ are congruent mod $n$. Since both of these values are in $\{0, 1, \ldots, n-1\}$, this implies that they are equal, as desired.

$\mathscr{G}_2$: Clearly, $0 \in \mathbb{Z}_n$ acts as an identity element under $+_n$, since

$$0 +_n a = R_n(0+a) = R_n(a)$$

for each $a \in \mathbb{Z}_n$.

$\mathscr{G}_3$: Let $a \in \mathbb{Z}_n$. If $a = 0$, then clearly $a$ has inverse $0 \in \mathbb{Z}_n$ since $0 +_n 0 = 0$. If $a \neq 0$, then the element $n - a \in \mathbb{Z}_n$ is an inverse for $a$ since

$$a +_n (n-a) = R_n(a + (n-a)) = R_n(n) = 0.$$

Since $+_n$ is commutative on $\mathbb{Z}_n$, $\mathbb{Z}_n$ is an abelian group under $+_n$. Finally, we already know that $|\mathbb{Z}_n| = |\{0, 1, 2, \ldots, n-1\}| = n$. □

**Remark.** In practice, we often omit the subscript $n$ and just write $+$ when discussing addition modulo $n$ on $\mathbb{Z}_n$.

**WARNING**

Do not confuse $n\mathbb{Z}$ and $\mathbb{Z}_n$! They are very different as sets and as groups.

**Example 2.17.** In the group $\langle \mathbb{Z}_8, + \rangle$ (where, as indicated by our above remark, $+$ means addition modulo 8), we have, for instance, $3 + 7 = 2$ and $7 + 7 = 6$. The numbers 2 and 6 are each other's inverse, and $7^{-1} = 1$. The number 0 has inverse 0 (it can't be 8, since $8 \notin \mathbb{Z}_8$!).

**Definition.** For $n \in \mathbb{Z}^+$, we define binary operation $\cdot_n$ (*multiplication modulo* $n$) on $\mathbb{Z}_n$ by $a \cdot_n b = r_n(a)$, the remainder when $ab$ is divided by $n$.

**Remark.** $\mathbb{Z}_n$ is never a group under $\cdot_n$ (do you see why?).

But we can consider the following

**Definition.** For $n \in \mathbb{Z}^+$, let $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$.

**Example 2.18.** $\langle \mathbb{Z}_n^\times, \cdot \rangle$ is a group under multiplication. We omit the proof.

We end by considering a few more examples.

**Example 2.19.** Let $F$ be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, and define *pointwise addition* $+$ on $F$ by

$$(f+g)(x) = f(x) + g(x)$$

for all $f, g \in F$ and $x \in \mathbb{R}$. We claim that $F$ is a group under pointwise addition. (For variety, in this proof we don't explicitly refer to $\mathscr{G}_1$–$\mathscr{G}_3$, though we certainly do verify they hold.) Indeed, if $f, g \in F$ then clearly $f + g$ is also a function from $\mathbb{R}$ to $\mathbb{R}$, so $F$ is closed under $+$.

Next, let $f, g, h \in F$. Then for all $x \in \mathbb{R}$,

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x) + h(x) \\ &= ((f(x)+g(x)) + h(x) \\ &= f(x) + (g(x)+h(x)) && \text{(since addition is associative on } \mathbb{R}) \\ &= f(x) + (g+h)(x) \\ &= (f + (g+h))(x) && .\end{aligned}$$

Note that the key fact used in this argument is that $f(x)$, $g(x)$ and $h(x)$ all lie in $\mathbb{R}$, and addition is associative on $\mathbb{R}$. When you get used to such arguments, it is sufficient to say that associativity of $+$ on $F$ is *inherited* from the associativity of addition on $\mathbb{R}$.

Next, let $z : \mathbb{R} \to \mathbb{R}$ be the function $z(x) = 0$ for all $x$. Then for all $f \in F$ and $x \in \mathbb{R}$,

$$(f+z)(x) = f(x) + z(x) = f(x) + 0 = f(x) = 0 + f(x) = z(x) + f(x) = (z+f)(x).$$

So $z$ is an identity element of $\langle F, + \rangle$.

Finally, let $f \in F$, and define $g \in F$ by $g(x) = -f(x)$ for all $x \in \mathbb{R}$. It is easy then to see that $g$ is an inverse for $f$ in $F$.

Hence, $F$ is a group under pointwise addition. Note that it is uncountably infinite and abelian.

**Example 2.20.** The set $F$ is **not** a group under function composition (do you see why?). But if we define $B$ to be the set of all **bijections** from $\mathbb{R}$ to $\mathbb{R}$, then $B$ is a group under function composition. (Prove it!) $B$ is uncountably infinite and nonabelian.

**Example 2.21.** Let $\langle G_1, *_1 \rangle$, $\langle G_2, *_2 \rangle$ , ..., $\langle G_n, *_n \rangle$ be groups ($n \in \mathbb{Z}^+$). Then the *group product*

$$G = G_1 \times G_2 \times \cdots \times G_n$$

is a group under the *componentwise* operation $*$ defined by

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n)$$

for all $(g_1, g_2, \ldots, g_n), (h_1, h_2, \ldots, h_n) \in G$.

For instance, considering multiplication on $\mathbb{R}^*$, matrix multiplication on $GL(2, \mathbb{R})$, and addition modulo 6 on $\mathbb{Z}_6$, we have that $\langle \mathbb{R}^* \times GL(2, \mathbb{R}) \times \mathbb{Z}_6, * \rangle$ is a group in which, for instance,

$$\left(-1, \begin{bmatrix} 1 & 3 \\ 0 & -1 \end{bmatrix}, 3\right) * \left(\pi, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, 4\right) = \left(-\pi, \begin{bmatrix} 5 & 4 \\ -1 & -1 \end{bmatrix}, 1\right).$$

**Example 2.22.** A common example of a group product is the group $\mathbb{Z}_2^2$, equipped with componentwise addition modulo 2.

**Definition.** The group $\mathbb{Z}_2^2$ is known as the *Klein 4-group.*[5]

[5]Felix Klein was a German mathematician; you may have heard of him in relation to the Klein Bottle. You may see the group $\mathbb{Z}_2^2$ denoted by $V$, for "Vierergruppe," the German word for "four-group".

## 2.7 Summaries of groups we've seen

When you see the following identified as groups, you should assume they are equipped with the following operations, unless otherwise. Throughout, assume $m, n \in \mathbb{Z}^+$.

| **Group(s)** | **Operation** | **Properties** |
|---|---|---|
| $\mathbb{Z}$, $\mathbb{Q}$ | addition of numbers | countably infinite; abelian |
| $n\mathbb{Z}$ | addition of numbers | countably infinite; abelian* |
| $\mathbb{R}$, $\mathbb{C}$ | addition of numbers | uncountable; abelian |
| $\mathbb{Q}^*$, $\mathbb{Q}^+$ | multiplication of numbers | countably infinite; abelian |
| $\mathbb{R}^*$, $\mathbb{R}^+$, $\mathbb{C}^*$ | multiplication of numbers | uncountable; abelian |
| $\mathbb{M}_{m\times n}(\mathbb{R}), \mathbb{M}_n(\mathbb{R})$ | matrix addition | uncountable; abelian |
| $GL(n,\mathbb{R}), SL(n,\mathbb{R})$ | matrix multiplication | uncountable; nonabelian† |
| $\mathbb{Z}_n$ | addition mod $n$ | finite; abelian |
| $\mathbb{Z}_2^2$ | componentwise addition mod 2 | finite; abelian |
| $F$ | pointwise addition | uncountable; abelian |
| $B$ | composition | uncountable; nonabelian |

* Unless $n = 0$.
† Unless $n = 1$.

## 2.8 Exercises, Part II

### Exercise 2.6

True/False. For each of the following, write T if the statement is true; otherwise, write F. You do NOT need to provide explanations or show work for this problem.

(a) For every positive integer $n$, there exists a group of order $n$.

(b) For every integer $n \geq 2$, $\mathbb{Z}_n$ is abelian.

(c) Every abelian group is finite.

(d) For every integer $m$ and integer $n > 2$, there exist infinitely many integers $a$ such that $a$ is congruent to $m$ modulo $n$.

(e) A binary operation $*$ on a set $S$ is commutative if and only if there exist $a, b \in S$ such that $a * b = b * a$.

(f) If $\langle S, * \rangle$ is a binary structure, then the elements of $S$ must be numbers.

(g) If $e \in \langle S, * \rangle$ is an identity element of $S$, then $e$ is an idempotent in $S$ (that is, $e * e = e$).

(h) If $s \in \langle S, * \rangle$ is an idempotent, then $s$ must be an identity element of $S$.

### Exercise 2.7

Let $G$ be the set of all functions from $\mathbb{Z}$ to $\mathbb{R}$. Prove that pointwise multiplication on $G$ is commutative. (**Note.** To prove that two functions, $h$ and $j$, sharing the same domain $D$ are equal, you need to show that $h(x) = j(x)$ for every $x \in D$.)

### Exercise 2.8

Decide which of the following binary structures are groups. For each, if the binary structure *isn't* a group, prove that. (Remember, you should *not* state that inverses do or do not exist for elements until you have made sure that the structure contains an identity element!) If the binary structure *is* a group, prove that.

(a) $\mathbb{Q}$ under multiplication

(b) $\mathbb{M}_2(\mathbb{R})$ under addition

(c) $\mathbb{M}_2(\mathbb{R})$ under multiplication

(d) $\mathbb{R}^+$ under $*$, defined by $a * b = \sqrt{ab}$ for all $a, b \in \mathbb{R}^+$

### Exercise 2.9

Give an example of an abelian group containing 711 elements.

### Exercise 2.10

Let $n \in \mathbb{Z}$. Prove that $n\mathbb{Z}$ is a group under the usual addition of integers. **Note:** You may use the fact that $\langle n\mathbb{Z}, + \rangle$ is a binary structure if you provide a reference for this fact.

### Exercise 2.11

Let $n \in \mathbb{Z}^+$. Prove that $SL(n, \mathbb{R})$ is a group under matrix multiplication. **Note:** You may use the fact that $\langle SL(n\mathbb{R}), \cdot \rangle$ is a binary structure if you provide a reference for this fact.

### Exercise 2.12

(a) List three distinct integers that are congruent to 6 modulo 5.

(b) List the elements of $\mathbb{Z}_5$.

(c) Compute:

(i) $4 + 5$ in $\mathbb{Z}$;

(ii) $4 + 5$ in $\mathbb{Q}$;

(iii) $4 +_6 5$ in $\mathbb{Z}_6$;

(iv) the inverse of 4 in $\mathbb{Z}$;

(v) the inverse of 4 in $\mathbb{Z}_6$.

(d) Why does it not make sense for me to ask you to compute $4 +_3 2$ in $\mathbb{Z}_3$? **Please answer this using a complete, grammatically correct sentence.**

### Exercise 2.13

Let $G$ be a group with identity element $e$. Prove that if every element of $G$ is its own inverse, then $G$ is abelian.

### Exercise 2.14 *(Extra Credit)*

Let $G$ be a group. The subset

$$Z(G) := \{z \in G : zg = gz \text{ for all } g \in Z(G)\}$$

of $G$ is called the *center* of $G$. In other words, $Z(G)$ is the set of all elements of $G$ that commute with every element of $G$. Prove that $Z(G)$ is closed in $G$.

# Chapter 3

# Homorphisms and Isomorphisms

## 3.1 Groups of small order

Let's start exploring groups in order of increasing, well, order. Before we do this, it will be helpful to introduce the notion of a *group table* (also known as a *Cayley table*[1]) for a finite group. Given a finite group $G$, list its elements in some fixed order, say, $a_1, a_2, \ldots, a_n$, and then construct its group table by creating an array with exactly one row and exactly one column corresponding to each group element. We then put in the row $i$ and column $j$ the element $a_i a_j$ of $G$. Note that a single group can have group tables that look different from one another, since reordering a group's elements will change its table.

**Example 3.1.** Consider the group $\mathbb{Z}_4$ under addition modulo 4. Ordering the elements of $\mathbb{Z}_4$ as $1, 2, 3, 4$, we have the following group table for $\langle \mathbb{Z}_4, + \rangle$:

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Now, clearly, there is no group of order 0 (do you see why?). Is there a group of order 1? Well, suppose $\langle G, * \rangle$ is such a group. Since $G$ must contain an identity element $e$, we must have $G = \{e\}$, and since $e$ is $G$'s identity element, we must have $e * e = e$. Clearly, in this case, the three group axioms hold. So $G$ is a valid group, without much going on in it.

**Definition.** If $G$ is a group with $|G| = 1$, then $G$ is called the *trivial group*[2].

Next suppose that group $\langle G, \cdot \rangle$ has order 2. Then $G$ must contain an identity element, $e$, and a non-identity element, $a$. Since $e$ is its own inverse, and inverses are unique, $a$ must be its own inverse as well. So $G$ must have the following table.

[1] Named after the British mathematician Arthur Cayley.

[2] A good question to ask here is why it's called "the" trivial group, rather than "a" trivial group. Indeed, there are infinitely many groups of order 1! (Do you see why?) But it turns out that all of these groups are **structurally** the same. Hence mathematicians end up thinking of them as various instantiations of one group, rather than separate groups. We will discuss this in more depth shortly, when we introduce the idea of *isomorphism*.

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

It is straightforward to show that such a structure does satisfy all the group axioms (the only one we really need to check is associativity).

Now, what if group $\langle G, \cdot \rangle$ has order 3? Note that **you can't have any entry appear more than once in the same row or same column** (excluding of course the labels outside the grid we're filling in), given Theorem 2.11. Is there only one way of filling in the table for a group of order 3? (Hint: consider what element must be the second row, third column entry.)

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | | | |
| $a$ | | | |
| $b$ | | | |

Finally, what if group $\langle G, \cdot \rangle$ has order 4? It turns out in this case there are **two** valid ways of filling in a group table!

What we have been doing here is really getting into the idea of the **structure** of groups, and when we can consider groups to be essentially "the same" or fundamentally "different." We approach this more formally via the concepts of homomorphism and isomorphism.

## 3.2 Introduction to homomorphisms and isomorphisms

**Definitions.** Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary structures. A function $\phi$ from $S$ to $S'$ is a *homomorphism* if

$$\phi(a * b) = \phi(a) *' \phi(b)$$

for all $a, b \in S$. An *isomorphism* is a homomorphism that is also a bijection.

Intuitively, you can think of a homomorphism $\phi$ as a "structure-preserving" map: if you multiply and then apply $\phi$, you get the same result as when you first apply $\phi$ and then multiply. Isomorphisms, then, are both structure-preserving and cardinality-preserving.

**Note.** We may omit the $*$ and $*'$, as per our group conventions, but we include them here to emphasize that the operations in the structures may be distinct from one another. When we omit them and write $\phi(st) = \phi(s)\phi(t)$, then it is the writers' and readers' responsibility to keep in mind that $s$ and $t$ are being operated together using the operation in $S$, while $\phi(s)$ and $\phi(t)$ are being operated together using the operation in $S'$.

**Remark.** There may be more than one homomorphism [isomorphism] from one binary structure to another (see Example 3.2).

**Example 3.2.** For each of the following, decide whether or not the given function $\phi$ from one binary structure to another is a homomorphism, and, if so, if it is an isomorphism. Prove or disprove your answers! For Parts 6 and 7, $C^0$ is the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$; $C^1$ is the set of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ whose derivatives are continuous; and each $+$ indicates pointwise addition on $C^0$ and $C^1$. (Note that $C^1$ and $C^0$ are not groups, since elements of them will not have inverses unless they are bijections.)

1. $\phi : \langle \mathbb{Z}, + \rangle \to \langle \mathbb{Z}, + \rangle$ defined by $\phi(x) = x$;
2. $\phi : \langle \mathbb{Z}, + \rangle \to \langle \mathbb{Z}, + \rangle$ defined by $\phi(x) = -x$;
3. $\phi : \langle \mathbb{Z}, + \rangle \to \langle \mathbb{Z}, + \rangle$ defined by $\phi(x) = 2x$;
4. $\phi : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^+, \cdot \rangle$ defined by $\phi(x) = e^x$;
5. $\phi : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^*, \cdot \rangle$ defined by $\phi(x) = e^x$;
6. $\phi : \langle C^1, + \rangle \to \langle C^0, + \rangle$ defined by $\phi(f) = f'$ (the derivative of $f$);
7. $\phi : \langle C^0, + \rangle \to \langle \mathbb{R}, + \rangle$ defined by $\phi(f) = \displaystyle\int_0^1 f(x)\,dx$.

**Example 3.3.** Let $\langle G, \cdot \rangle$ be a group and let $a \in G$. Then the function $c_a$ from $G$ to $G$ defined by $c_a(x) = axa^{-1}$ (for all $x \in G$) is a homomorphism. Indeed, let $x, y \in G$. Then

$$\begin{aligned} c_a(xy) &= a(xy)a^{-1} \\ &= (ax)e(ya^{-1}) \\ &= (ax)(a^{-1}a)(ya^{-1}) \\ &= (axa^{-1})(aya^{-1}) \\ &= c_a(x)c_a(y). \end{aligned}$$

The homomorphism $c_a$ is called *conjugation by* $a$.[3]

We end with a theorem stating basic facts about homomorphisms from one group to another. (**Note.** This doesn't apply to arbitrary binary structures, which may or may not even have identity elements.)

**Theorem 3.4.** *Let $\langle G, \cdot \rangle$ and $\langle G', \cdot' \rangle$ be groups with identity elements $e$ and $e'$, respectively, and let $\phi$ be a homomorphism from $G$ to $G'$. Then:*

1. *$\phi(e) = e'$; and*
2. *For every $a \in G$, $\phi(a)^{-1} = \phi(a^{-1})$.*

*Proof.* For Part 1, note that

$$\begin{aligned} \phi(e) \cdot' e' &= \phi(e) && \text{(by definition of } e') \\ &= \phi(e \cdot e) && \text{(by definition of } e) \\ &= \phi(e) \cdot' \phi(e) && \text{(since } \phi \text{ is a homomorphism).} \end{aligned}$$

Thus, by left cancellation, $e' = \phi(e)$. The proof of Part 2 is left as an exercise for the reader. □

[3] Homomorphisms from a group $G$ to itself are called *automorphisms*. Thus, conjugation by any element $a$ in $G$ is an automorphism of $G$. (Beware: Some texts refer to the function $x \mapsto a^{-1}xa$ as "conjugation by $a$." Either version of conjugation by $a$ in group $G$ is an automorphism of $G$.)

## 3.3 Isomorphic groups

One of the key ideas we've discussed in determining whether binary structures are essentially "the same" or "different." We approach this rigorously using the concept of *isomorphic* groups.

**Definitions and notation.** We say that two groups $G$ and $G'$ (or binary structures $S$ and $S'$) are *isomorphic*, and write $G \simeq G'$, if there exists an isomorphism from $G$ to $G'$. We say that $G$ is *isomorphic to* $G'$ *via* $\phi$ if $\phi$ is an isomorphism from $G$ to $G'$. If there exists no isomorphism from $G$ and $G'$, then we say that $G$ and $G'$ are *nonisomorphic*, and write $G \not\simeq G'$.

> **WARNING**
>
> Just because a particular map (even an "obvious" one) from group $G$ to group $G'$ is not an isomorphism, we do not know that $G$ and $G'$ are not isomorphic! For instance, the map $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x) = 2x$ for all $x$ is **not** an isomorphism (since it's not onto), but $\mathbb{Z}$ **is** isomorphic to itself, as we will see in Part 1 of Theorem 3.5.

Isomorphic groups have **the same structure** as far as algebraists are concerned. Again, picture two houses that are identical except for the colors they are painted. Though they differ in some ways (one house is red while the other is green), they are structurally identical. Isomorphic groups have identical structures, though the elements of one group may differ greatly from those of the other. Returning to the house analogy: if two houses are structurally identical, we can learn many things about one house by looking at the other (e.g., how many bathrooms it has, whether it has a basement, etc.). Similarly, suppose we know a great deal about group $G$ and are given a new group, $G'$. If we prove that $G'$ is isomorphic to $G$, then we can likely deduce information about $G'$ from the information we know about $G$.

**Theorem 3.5.** *Let $\langle G, \cdot \rangle$, $\langle G', \cdot' \rangle$, and $\langle G'', \cdot'' \rangle$ be groups.*

1. *Group $G$ is isomorphic to itself.*
2. *If $\phi$ is an isomorphism from $G$ to group $G'$, then there exists an isomorphism from $G'$ to $G$. Hence, $G \simeq G'$ if and only if $G' \simeq G$.*
3. *If $G \simeq G'$ and $G' \simeq G''$, then $G \simeq G''$.*

*Proof.* For Part 1: The identity map $1_G : G \to G$ defined by $1_G(a) = a$ for all $a \in G$ is clearly an isomorphism.

For Part 2: Since $\phi$ is an isomorphism, it's a bijection, hence has inverse $\phi^{-1}$. From Theorem 1.8, we know that $\phi^{-1}$ must also be a bijection (in this case, from $G'$ to $G$). So it suffices to show that $\phi^{-1}$ is a homomorphism. Let $a, b \in G'$. We want to show that $\phi^{-1}(a \cdot' b) = \phi^{-1}(a) \cdot \phi^{-1}(b)$. Since $\phi$ is 1-1, it suffices to show that

$$\phi(\phi^{-1}(a \cdot' b)) = \phi(\phi^{-1}(a) \cdot \phi^{-1}(b)).$$

Notice, we have $\phi(\phi^{-1}(a \cdot' b)) = a \cdot' b$; further, we have

$$\phi(\phi^{-1}(a) \cdot \phi^{-1}(b)) = \phi(\phi^{-1}(a)) \cdot' \phi(\phi^{-1}(b)) = a \cdot' b.$$

This shows that $\phi^{-1}(a \cdot' b) = \phi^{-1}(a) \cdot \phi^{-1}(b)$, as desired.

For Part 3: Since $G \simeq G'$ and $G' \simeq G''$, there exist isomorphisms $\phi : G \to G'$ and $\psi : G' \to G''$. Define $\theta : G \to G''$ by $\theta = \psi \circ \phi$. Since $\phi$ and $\psi$ are both bijections, $\theta$ is a bijection (Theorem 1.9). Next, let $a, b \in G$. The

$$\begin{aligned}
\theta(a \cdot b) &= \psi(\phi(a \cdot b)) && \text{(by definition of } \theta) \\
&= \psi(\phi(a) \cdot' \phi(b)) && \text{(since } \phi \text{ is a homomorphism)} \\
&= \psi(\phi(a)) \cdot'' \psi(\phi(b)) && \text{(since } \psi \text{ is a homomorphism)} \\
&= \theta(a) \cdot'' \theta(b) && \text{(by definition of } \theta).
\end{aligned}$$

Thus, $\theta$ is a homomorphism, and hence, since it is also a bijection, an isomorphism. □

To show that given groups $G$ and $G'$ are isomorphic, we must do three things:

1. **Define** a function $\phi$ from $G$ to $G'$ (or from $G'$ to $G$, as we have Theorem 3.5);
2. Prove that $\phi$ is a homomorphism; and
3. Prove that $\phi$ is a bijection.*

* Remember, you can show that $\phi$ is a bijection by proving that it's one-to-one and onto, **or** by showing that it has an inverse.

**WARNING**

Do **NOT** try to prove that a function $\phi$ is an isomorphism WITHOUT DEFINING $\phi$!

We know provide some terminology that will be helpful for our study of the structures of groups.

**Definition.** Given a certain property (or properties), we say there is a *unique group* with that property (or properties) *up to isomorphism* if any two groups sharing that property (or properties) are isomorphic to one another.

This may seem a little abstruse at the moment, but seeing examples will help illuminate the concept.

**Example 3.6.**

1. If $G$ and $G'$are groups with $|G| = |G'| = 1$, then $G \simeq G'$, since the map from $G$ to $G'$ sending $G$'s identity (and sole) element to $G'$'s identity (and sole) element is clearly an isomorphism. This is why we can mildly abuse terminology and call any group of order 1 *the* trivial group instead of *a* trivial group: $G$ and $G'$ may technically be different groups, but structurally they are identical, so we can consider them to be more or less "the same." Thus, there is a unique group of order 1, up to isomorphism.

2. Let $G$ be a group with $|G| = 2$. Then $G$ must consist of an identity element $e$ and a nonidentity element $a$, and have the following group table. Compare the group tables of $G$ and the specific two-element group $\mathbb{Z}_2$.

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Note that the first table looks exactly like the second table if we replace $*$ with $+$, each $e$ with 0, and each $a$ with 1. This shows that groups $G$ and $\mathbb{Z}_2$ have identical structures; more precisely, it shows that the function $\phi$ from $G$ to $\mathbb{Z}_2$ defined by $\phi(e) = 0$ and $\phi(a) = 1$ is an isomorphism. Since any group of order 2 is isomorphic to $\mathbb{Z}_2$, using Theorem 3.5 we see that there is a unique group of order 2, up to isomorphism.

3. A similar argument shows that there is a unique group of order 3 up to isomorphism: specifically, any group of order 3 is isomorphic to $\mathbb{Z}_3$.

4. We will see later, in Example 3.12, that there is *not* a unique group of order 4 up to isomorphism: that is, there are two nonisomorphic groups of order 4.

**Example 3.7.** The groups $\langle \mathbb{R}, + \rangle$ and $\langle \mathbb{R}^+, \cdot \rangle$ are isomorphic.

*Proof.* Define $\phi : \mathbb{R} \to \mathbb{R}^+$ by $\phi(x) = e^x$. Our map $\phi$ is a homomorphism since for every $x, y \in \mathbb{R}$, we have

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$

Moreover, $\phi$ is a bijection, since it has inverse function $\ln x : \mathbb{R}^+ \to \mathbb{R}$. Hence, $\mathbb{R} \simeq \mathbb{R}^+$ via isomorphism $\phi$. □

**Example 3.8.** Let $n \in \mathbb{Z}^+$. Then the groups $\langle n\mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ are isomorphic. The proof of this is left as an exercise for the reader.

We have now seen examples in which we have proved that two groups are isomorphic. How, though, do we prove that two groups are **not** isomorphic? It is usually wildly impractical, if not impossible, to check that no function from one group to the other is an isomorphism. For instance, it turns out that $\mathbb{R}^*$ is not isomorphic to $GL(2, \mathbb{R})$ (see Example 3.9), but there are infinitely many bijections from $\mathbb{R}^*$ to $GL(2, \mathbb{R})$—it is impossible to check that each one is not an isomorphism. Instead, we use *group invariants*.

**Definition.** A group property $P$ is called a *group invariant* if it is preserved under isomorphism.

Group invariants are **structural** properties. Some examples of group invariants are:

1. Cardinality (since any isomorphism between groups is a bijection);

2. Abelianness (the proof that this is a group invariant is left as an exercise for the reader);

3. Number of elements which are their own inverses (proven by an argument similar to that in Example 3.12).

A nonexample of a group invariant is the property of being a subset of $\mathbb{R}$.

**Example 3.9.** The group $\mathbb{R}$ cannot be isomorphic to the group $GL(2, \mathbb{R})$ since the former group is abelian and the latter nonabelian.

**Example 3.10.** The groups $\mathbb{R}$ and $\mathbb{Q}$ cannot be isomorphic since the former group is uncountable and the latter countable.

Sometimes we must resort to trickier methods in order to decide whether or not two groups are isomorphic.

**Example 3.11.** The groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic. We use contradiction to prove this. Suppose that $\mathbb{Z}$ and $\mathbb{Q}$ are isomorphic via isomorphism $\phi : \mathbb{Q} \to \mathbb{Z}$. Let $a \in \mathbb{Q}$. Then $a/2 \in \mathbb{Q}$ with $a/2 + a/2 = a$. Then

$$\phi(a/2) + \phi(a/2) = \phi(a/2 + a/2) = \phi(a);$$

since $\phi(a/2)$ is in $\mathbb{Z}$, $\phi(a)$ must be evenly divisible by 2. But $a$ was arbitrary in $\mathbb{Q}$ and $\phi$ is onto, so this means every element of $\mathbb{Z}$ must be evenly divisible by 2, which is clearly false. Thus, $\mathbb{Z} \not\cong \mathbb{Q}$.

**Example 3.12.** The groups $\mathbb{Z}_4$ and $V = \mathbb{Z}_2^2$ are not isomorphic. Why? Well, they are both abelian of order 4, so we cannot use cardinality or commutativity to prove they are nonisomorphic. The gist of our argument will be to note that every element in $V$ is its own inverse; so if $V$ and $\mathbb{Z}_4$ are isomorphic (hence structurally identical) we must have that every element of $\mathbb{Z}_4$ is also its own inverse, which doesn't hold (e.g., in $\mathbb{Z}_4$, $3 + 3 = 2$, not 0).

A rigorous proof of the fact that $V$ and $\mathbb{Z}_4$ are not isomorphic is as follows: For now, denote the usual operation on $V$ by $*$. Suppose that $V$ and $\mathbb{Z}_4$ are isomorphic, via isomorphism $\phi$ from $V$ to $\mathbb{Z}_4$. Then since $\phi$ is onto, there exists an element $a \in V$ such that $\phi(a) = 3$. Then

$$\begin{aligned} 3 + 3 &= \phi(a) + \phi(a) && \text{(by definition of } a\text{)} \\ &= \phi(a * a) && \text{(since } \phi \text{ is a homomorphism)} \\ &= \phi((0,0)) && \text{(since every element of } V \text{ is its own inverse)} \\ &= 0, \end{aligned}$$

since $\phi$ is a homomorphism, so sends identity element to identity element. But this is a contradiction, since $3 + 3 = 2 \neq 0$ in $\mathbb{Z}_4$. Thus, $V \not\cong \mathbb{Z}_4$.

## 3.4 Exercises

### Exercise 3.1

True/False. For each of the following, write T if the statement is true; otherwise, write F. You do NOT need to provide explanations or show work for this problem.Throughout, let $G$ and $G'$ be groups.

(a) If there exists a homomorphism $\phi : G \to G'$, then $G$ and $G'$ must be isomorphic groups.

(b) There is an integer $n \geq 2$ such that $\mathbb{Z} \simeq \mathbb{Z}_n$.

(c) If $|G| = |G'| = 3$, then we must have $G \simeq G'$.

(d) If $|G| = |G'| = 4$, then we must have $G \simeq G'$.

### Exercise 3.2

For each of the following functions, prove or disprove that the function is (i) a homomorphism; (ii) an isomorphism. (Remember to work with the default operation on each of these groups!)

(a) The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 2n$.

(b) The function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$.

(c) The function $h : \mathbb{Q}^* \to \mathbb{Q}^*$ defined by $h(x) = x^2$.

### Exercise 3.3

Define $d : GL(n, \mathbb{R}) \to \mathbb{R}^*$ by $d(A) = \det A$. Prove/disprove that $d$ is:

(a) a homomorphism

(b) 1-1

(c) onto

(d) an isomorphism.

### Exercise 3.4

Complete the group tables for $\mathbb{Z}_4$ and $\mathbb{Z}_8^\times$. Use the group tables to decide whether or not $\mathbb{Z}_4$ and $\mathbb{Z}_8^\times$ are isomorphic to one another. (You do not need to provide a proof.)

### Exercise 3.5

Let $n \in \mathbb{Z}^+$. Prove that $\langle n\mathbb{Z}, + \rangle \simeq \langle \mathbb{Z}, + \rangle$.

### Exercise 3.6

(a) Let $G$ and $G'$ be groups, where $G$ is abelian and $G \simeq G'$. Prove that $G'$ is abelian.

(b) Give an example of groups $G$ and $G'$, where $G$ is abelian and there exists a homomorphism from $G$ to $G'$, but $G'$ is NOT abelian.

### Exercise 3.7 *(Extra Credit)*

Let $\langle G, \cdot \rangle$ and $\langle G', \cdot' \rangle$ be groups with identity elements $e$ and $e'$, respectively, and let $\phi$ be a homomorphism from $G$ to $G'$. Let $a \in G$. Prove that $\phi(a)^{-1} = \phi(a^{-1})$.

# Chapter 4

# Subgroups

## 4.1 Introduction to subgroups

Sometimes groups are too complicated to understand directly. One method that can be used to identify a group's structure is to study its *subgroups*.

**Definitions and notation.** A *subgroup* of a group $G$ is a subset of $G$ that is also a group under $G$'s operation. If $H$ is a subgroup of $G$, we write $H \leq G$; if $H \subseteq G$ is not a subgroup of $G$, we write $H \not\leq G$.

> **WARNING**
>
> Do not confuse sub**groups** with sub**sets**! All subgroups of a group $G$ are, by definition, subsets of $G$, but not all subsets of $G$ are subgroups of $G$ (see Example 4.1, Parts 2–5, below). Whether or not a subset of $G$ is a subgroup of $G$ depends on the operation of $G$.

**Example 4.1.**

1. Consider the subset $\mathbb{Z}$ of the group $\mathbb{Q}$, assuming that $\mathbb{Q}$ is equipped with the usual addition of real numbers (as we indicated above that we would assume, by default). Since we already know that $\mathbb{Z}$ is a group under this operation, $\mathbb{Z}$ is not just a subset but in fact a subgroup of $\mathbb{Q}$ (under addition).

2. Instead, consider the subset $\mathbb{Q}^+$ of the group $\mathbb{Q}$. This subset is <u>not</u> a group under $\mathbb{Q}$'s operation $+$, since it does not contain an identity element for $+$. Therefore, $\mathbb{Q}^+$ is a subset but not a subgroup of $\mathbb{Q}$.

3. Let $I$ be the subset
$$I = \mathbb{R} - \mathbb{Q} = \{x \in \mathbb{R} : x \text{ is irrational}\}$$
of the group $\mathbb{R}$. The set $I$ is <u>not</u> a group under $\mathbb{R}$'s operation $+$ since it is not closed under addition: for instance, $\pi, -\pi \in I$, but $\pi + (-\pi) = 0 \notin I$. So $I$ is a subset but not a subgroup of $\mathbb{R}$.

4. Consider the subset $\mathbb{Z}^+$ of the group $\mathbb{R}^+$. The set $\mathbb{Z}^+$ is closed under multiplication, multiplication is associative on $\mathbb{Z}^+$, and $\mathbb{Z}^+$ does contain an identity element (namely, 1). However, most elements of $\mathbb{Z}^+$ do not have inverses in $\mathbb{Z}^+$ under multiplication: for instance, the inverse of 3 would have to be $1/3$, but $1/3 \notin \mathbb{Z}^+$. Therefore, $\mathbb{Z}^+$ is a subset but not a subgroup of $\mathbb{R}^+$.

5. Consider the subset $GL(n, \mathbb{R})$ of $\mathbb{M}_n(\mathbb{R})$. We know that $GL(n, \mathbb{R})$ is a group, so it might be tempting to say that it is a subgroup of $\mathbb{M}_n(\mathbb{R})$; to be a subgroup of $\mathbb{M}_n(\mathbb{R})$, $GL(n, \mathbb{R})$ must be a group under $\mathbb{M}_n(\mathbb{R})$'s operation, which is matrix addition. While $GL(n, \mathbb{R})$ is a group under matrix multiplication, it is not a group under matrix addition: for instance, it is not closed under matrix addition, since $I_n, -I_n \in GL(n, \mathbb{R})$ but $I_n + (-I_n)$ is the matrix consisting of all zeros, which is not in $GL(n, \mathbb{R})$. So $GL(n, \mathbb{R})$ is a subset but not a subgroup of $\mathbb{M}_n(\mathbb{R})$.

6. Consider the subset $H = \{0, 2\}$ of $\mathbb{Z}_4$. The subset $H$ is closed under addition modulo 4 ($0 + 0 = 0$, $0 + 2 = 2 + 0 = 2$, $2 + 2 = 0$), addition modulo 4 is always associative, $H$ contains an identity element (namely, 0) under addition modulo 4, and both 0 and 2 have inverses in $\mathbb{Z}_4$ under this operation (0 and 2 are each their own inverses). Thus, $H$ **is** a subgroup of $\mathbb{Z}_4$.

7. Let $G$ be a group. Then $\{e_G\}$ and $G$ are clearly both subgroups of $G$.

**Definitions.** Let $G$ be a group. The subgroups $\{e_G\}$ and $G$ of $G$ are called the *trivial subgroup* and the *improper subgroup* of $G$, respectively. Not surprisingly, if $H \leq G$ and $H \neq \{e_G\}$, $H$ is called a *nontrivial* subgroup of $G$, and if $H \leq G$ and $H \neq G$, $H$ is called a *proper subgroup* of $G$.[1]

Note that in the cases above, we saw subsets of groups fail to be subgroups because they were not closed under the groups' operations; because they did not contain identity elements; or because they didn't contain an inverse for each of their elements. None, however, failed because the relevant group's operation was not associative on them. This is not a coincidence: rather, since any element of a subset of a group $G$ also lives in $G$, any associative operation on $G$ is of necessity associative on any closed subset of $G$. Therefore, when we are checking to see if $H \subseteq G$ is a subgroup of group $G$, we need only check for closure, an identity element, and inverses.

**Lemma 4.2.** *Let $G$ be a group.*

1. *If $H$ is a subgroup of $G$ then the identity element $e_H$ of $H$ is $e_G$, the identity element of $G$.*

2. *If $H$ is a subgroup of $G$ and $a \in H$ has inverse $a^{-1}$ in $G$, then $a$'s inverse in $H$ is also $a^{-1}$.*

*Proof.* For Part 1: Since $e_H$ is in both $H$ and $G$, by the definition of $e_H$, we have $e_H e_H = e_H$, and by the definition of $e_G$ we have $e_G e_H = e_H$. So $e_H e_H = e_G e_H$, and thus by right cancellation, $e_H = e_G$.

Next, for Part 2, let $b$ be the inverse of $a$ in $H$. Then using Part 1 of this lemma and the definition of an inverse, $ab = e_H = e_G = aa^{-1}$. By left cancellation, then, we have that $b = a^{-1}$. □

**Corollary 4.3.** *Let $H \subseteq G$. If the identity element of $G$ is not in $H$, then $H \not\leq G$.*

## 4.2 Proving that a subset of a group is or isn't a subgroup

Using Lemma 4.2 and the argument preceding it, we have the following.

[1] Sometimes the notation $H < G$ is used to indicated that $H$ is a proper subgroup of $G$, but sometimes it is simply used to mean that $H$ is a subgroup—proper or improper—of $G$.

**Theorem 4.4.** *A subset $H$ of a group $G$ is a subgroup of $G$ if and only if*

1. *$H$ is closed under $G$'s operation;*
2. *The identity element of $G$ is in $H$; and*
3. *For each $a \in H$, $a$'s inverse in $G$ is contained in $H$.*

**Example 4.5.** For each of the following, prove that the given subset $H$ of group $G$ is or is not a subgroup of $G$.

1. $H = 3\mathbb{Z}$, $G = \mathbb{Z}$.
2. $H = \{0, 1, 2, 3\}$, $G = \mathbb{Z}_6$;
3. $H = \mathbb{R}^*$, $G = \mathbb{R}$;
4. $H = \{(0, x, y, z) : x, y, z \in \mathbb{R}\}$, $G = \mathbb{R}^4$.

**Example 4.6.** eneralizing Part 1 of the above theorem, we have $n\mathbb{Z} \leq \mathbb{Z}$ for every $n \in \mathbb{Z}^+$. The proof of this is left as an exercise for the reader.

**Example 4.7.** Consider the group $\langle F, + \rangle$, where $F$ is the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ and $+$ is pointwise addition. Which of the following are subgroups of $F$?

$H = \{f \in F : f(5) = 0\}$;

$K = \{f \in F : f \text{ is continuous}\}$;

$L = \{f \in F : f \text{ is differentiable}\}$.

Are any of $H$, $K$, and $L$ subgroups of one another?

In fact, we can narrow down the number of facts we need to check to prove a subset $H \subseteq G$ is a subgroup of $G$ to only two.

**Theorem 4.8.** ***Two-Step Subgroup Test.*** *Let $G$ be a group and $H \subseteq G$. Then $H$ is a subgroup of $G$ if*

1. *$H \neq \emptyset$; and*
2. *For each $a, b \in H$, $ab^{-1} \in H$.*

*Proof.* Assume that the above two properties hold. Since $H \neq \emptyset$, there exists an $x \in G$ such that $x \in H$. Then $e_G = xx^{-1}$ is in $H$, by the second property. Next, for every $a \in H$ we have $a^{-1} = e_G a^{-1} \in H$ (again by the second property). Finally, if $a, b \in H$ then we've already shown $b^{-1} \in H$; so $ab = a(b^{-1})^{-1} \in H$, yet again by the second property. Thus, $H \leq G$. □

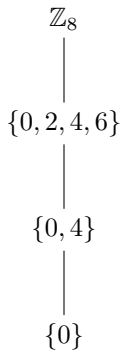
**Example 4.9.**

1. Use the Two-Step Subgroup Test to prove that $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
2. Use the Two-Step Subgroup Test to prove that $SL(n, \mathbb{R})$ is a subgroup of $GL(n, \mathbb{R})$.

**N.** ote that if $H$ is a subgroup of a group $G$ and $K$ is a subset of $H$, then $K$ is a subgroup of $H$ if and only if it's a subgroup of $G$.

It can be useful to look at how subgroups of a group relate to one another. One way of doing this is to consider *subgroup lattices* (also known as *subgroup diagrams*. To draw a subgroup lattice for a group $G$, we list all the subgroups of $G$, writing a subgroup $K$ below a subgroup $H$, and connecting them with a line, if $K$ is a subgroup of $H$.

**Example 4.10.** Consider the group $\mathbb{Z}_8$. We will see later that the subgroups of $\mathbb{Z}_8$ are $\{0\}$, $\{0, 2, 4, 6\}$, $\{0, 4\}$ and $\mathbb{Z}_8$ itself. So $\mathbb{Z}_8$ has the following subgroup lattice.




**Example 4.11.** Referring to Example 4.7, draw the portion of the subgroup lattice for $F$ that shows the relationships between itself and its proper subgroups $H$, $K$, and $L$.

**Example 4.12.** Indicate the subgroup relationships between the following groups: $\mathbb{Z}$, $12\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{R}$, $6\mathbb{Z}$, $\mathbb{R}^+$, $3\mathbb{Z}$, $G = \langle \{\pi^n : n \in \mathbb{Z}\}, \cdot \rangle$ and $J = \langle \{6^n : n \in \mathbb{Z}\}, \cdot \rangle$.

We end with a theorem about homomorphisms and subgroups that leads us to another group invariant.

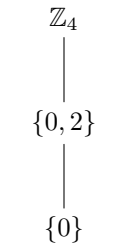
**Theorem 4.13.** *Let $G$ and $G'$ be groups, let $\phi$ a homomorphism from $G$ to $G'$, and let $H$ a subgroup of $G$. Then $\phi(H)$ is a subgroup of $G'$.*

*Proof.* This proof is left as an exercise for the reader. □

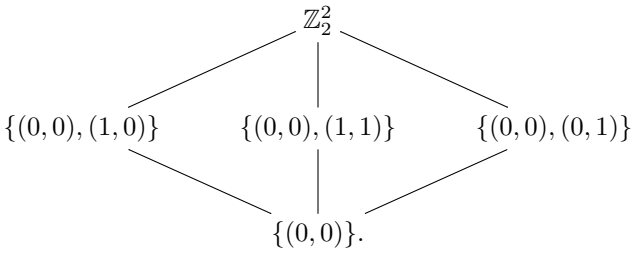
**Corollary 4.14.** *If $G \simeq G'$ and $G$ contains exactly $n$ subgroups ($n \in \mathbb{Z}^+$), then so does $G'$.*

This is another way of, for instance, distinguishing between the groups $\mathbb{Z}_4$ and the Klein 4-group $Z_2^2$.

**Example 4.15.** By inspection, $\mathbb{Z}_4$ has subgroup lattice



and $\mathbb{Z}_2^2$ has subgroup lattice




Since $\mathbb{Z}_4$ contains exactly 3 subgroups and $\mathbb{Z}_2^2$ exactly 5, we have that $\mathbb{Z}_4 \ncong V$.

## 4.3 Exercises

### Exercise 4.1

True/False. For each of the following, write T if the statement is true; otherwise, write F. You do NOT need to provide explanations or show work for this problem.Throughout, let $G$ and $G'$ be groups.

(a) Every group contains at least two distinct subgroups.

(b) If $H$ is a proper subgroup of group $G$ and $G$ is finite, then we must have $|H| < |G|$.

(c) $7\mathbb{Z}$ is a subgroup of $14\mathbb{Z}$.

(d) A group $G$ may have two distinct proper subgroups which are isomorphic (to one another).

### Exercise 4.2

Give specific, precise examples of the following groups $G$ with subgroups $H$:

(a) A group $G$ with a proper subgroup $H$ of $G$ such that $|H| = |G|$.

(b) A group $G$ of order 12 containing a subgroup $H$ with $|H| = 3$.

(c) A nonabelian group $G$ containing a nontrivial abelian subgroup $H$.

(d) A finite subgroup $H$ of an infinite group $G$.

### Exercise 4.3

Let $n \in \mathbb{Z}^+$.

(a) Prove that $n\mathbb{Z} \leq \mathbb{Z}$.

(b) Prove that the set $H = \{A \in \mathbb{M}_n(\mathbb{R}) : \det A = \pm 1\}$ is a subgroup of $GL(n, \mathbb{R})$.

(**Note:** Your proofs do not need to be long to be correct!)

### Exercise 4.4

For each group $G$ and subset $H$, decide whether or not $H$ is a subgroup of $G$. In the cases in which $H$ is <u>not</u> a subgroup of $G$, provide a proof. (**Note.** Your proofs do not need to be long to be correct!)

(a) $G = \mathbb{Z}$, $H = \mathbb{R}$

(b) $G = \mathbb{Z}_{15}$, $H = \{0, 5, 10\}$

(c) $G = \mathbb{Z}_{15}$, $H = \{0, 4, 8, 12\}$

(d) $G = \mathbb{C}$, $H = \mathbb{R}^*$

(e) $G = \mathbb{C}^*$, $H = \{1, i, -1, -i\}$

(f) $G = \mathbb{M}_n(\mathbb{R})$, $H = GL(n, \mathbb{R})$

(g) $G = GL(n, \mathbb{R})$, $H = \{A \in \mathbb{M}_n(\mathbb{R}) : \det A = -1\}$

### Exercise 4.5

Let $G$ and $G'$ be groups, let $\phi$ a homomorphism from $G$ to $G'$, and let $H$ a subgroup of $G$. Then $\phi(H)$ is a subgroup of $G'$.

### Exercise 4.6 *(Extra Credit)*

Recall that an element $u$ of a binary structure is said to be an *idempotent* if $u^2 = u$. Let $G$ be an abelian group, and let $U$ be the set of all idempotents of $G$. Prove that $U$ is a subgroup of $G$.

# Chapter 5

# Cyclic Groups

## 5.1 Introduction to cyclic groups

Certain groups and subgroups of groups have particularly nice structures.

**Definition.** A group is *cyclic* if it is isomorphic to $\mathbb{Z}_n$ for some $n \geq 1$, or if it is isomorphic to $\mathbb{Z}$.

**Example 5.1.** Examples/nonexamples of cyclic groups.

1. $n\mathbb{Z}$ and $\mathbb{Z}_n$ are cyclic for every $n \in \mathbb{Z}^+$.
2. $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{M}_2(\mathbb{R})$, and $GL(2, \mathbb{R})$ are uncountable and hence can't be cyclic.
3. $\mathbb{Z}_2^2$ is not cyclic since it would have to be isomorphic to $\mathbb{Z}_4$ if it were (since it has order 4).
4. $\mathbb{Q}$ isn't cyclic. If it were cyclic it would have to be isomorphic to $\mathbb{Z}$, since $\mathbb{Q}$ is an infinite group (so can't be isomorphic to $\mathbb{Z}_n$ for any $n$). But we showed in Example 3.11 that $\mathbb{Q} \ncong \mathbb{Z}$.

**Remark.** Clearly, cyclicity is a group invariant.

**Theorem 5.2.** *If $G$ is cyclic, then $G$ is abelian; however, $G$ can be abelian but not cyclic.*

*Proof.* Since $\mathbb{Z}$ and each $\mathbb{Z}_n$ are abelian, every cyclic group is abelian. But, for instance, $\mathbb{R}$ is an abelian noncyclic group (it can't be cyclic because it is uncountable). □

**Definition.** Let $a$ be an element of a group $G$. Then

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\}$$

is called the *(cyclic) subgroup of $G$ generated by $a$.* (We will later see why the words "cyclic" and "generated" are used here.)

**Remark.** Note that in the above definition, we were using multiplicative notation. Using additive notation, we have $\langle a \rangle = \{na : n \in \mathbb{Z}\} = \{\ldots, -2a, -a, 0a, 1a, 2a, \ldots\}$.

**Theorem 5.3.** *Let $a$ be an element of a group $G$. Then $\langle a \rangle \leq G$.*

*Proof.* Let $x, y \in \langle a \rangle$. Then $x = a^i$, $y = a^j$ for some $i, j \in \mathbb{Z}$. So $xy = a^i a^j = a^{i+j} \in \langle a \rangle$. Next, $e_G = a^0 \in H$. Finally, $(a^i)^{-1} = a^{-i} \in H$. So $\langle a \rangle$ is a subgroup of $G$. □

**Theorem 5.4.** *Let $G$ be a group with identity element $e$, and let $a \in G$. Then the group $\langle a \rangle$ is cyclic.*

*Proof.* **Case 1.** There is no positive integer $k$ with $a^k = e$. In this case, we claim $\langle a \rangle \simeq \mathbb{Z}$. Indeed: Let $\phi : \mathbb{Z} \to \langle a \rangle$ be defined by $\phi(i) = a^i$. Clearly, $\phi$ is a homomorphism that is onto. So to show that $\phi$ is an isomorphism, it suffices to show that $\phi$ is one-to-one. Let $i, j \in \mathbb{Z}$ with $\phi(i) = \phi(j)$. Then $a^i = a^j$. Without loss of generality, we may assume $i \geq j$. Then, multiplying both sides of the equation by $a^{-j}$ (on the right or on the left) we obtain $a^{i-j} = e$. Since $i - j \in \mathbb{N}$ and there is no positive integer $k$ with $a^k = e$, we must have $i - j = 0$, so $i = j$. Thus, $\phi$ is an isomorphism from $\mathbb{Z}$ to $\langle a \rangle$.

**Case 2.** There is a positive integer $k$ such that $a^k = e$. In this case, let $n$ be the least such positive integer. In this case, we claim $\langle a \rangle \simeq \mathbb{Z}_n$. Indeed: Let $\phi : \mathbb{Z}_n \to \langle a \rangle$ be defined by $\phi(i) = a^i$. We will find it useful to use the following, which holds in this context:

**Lemma 5.5.** ***(Clock Lemma)*** *If $s, t \in \mathbb{Z}$, then $a^s = a^t$ if and only if $s$ is congruent to $t$ modulo $n$.*

*Proof.* By the Division Algorithm, there exist $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_n$ with $s - t = qn + r$. Then $a^{s-t} = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$. Since $0 \leq r < n$, be definition of $n$ we have that $a^{s-t} = e$ if and only if $r = 0$; that is, $a^s = a^t$ if and only if $s$ and $t$ are congruent modulo $n$. □

Let $i, j \in \mathbb{Z}$. We want to show that $\phi(i +_n j) = \phi(i)\phi(j)$, that is, that $a^{i+_n j} = a^i a^j$. Since $i + j$ is congruent to $i +_n j$ modulo $n$, $a^i a^j = a^{i+j} = a^{i+_n j}$, by the Clock Lemma. So $\phi$ is a homomorphism. Next we show that $\phi$ is one-to-one. Let $i, j \in \mathbb{Z}_n$ with $\phi(i) = \phi(j)$, so $a^i = a^j$. Then, by the Clock Lemma, $i$ and $j$ are congruent modulo $n$. Since they're both in $\mathbb{Z}_n$, they must be equal, so $\phi$ is one-to-one. Finally, we show that $\phi$ is onto. let $x \in \langle a \rangle$. Then $x = a^i$ for some $i \in \mathbb{Z}$. Letting $r$ be the remainder when we divide $i$ by $n$, we have $r \in \mathbb{Z}_n$ with $i$ congruent to $r$ modulo $n$; so, again using the Clock Lemma, $x = a^i = a^r$. Since $r \in \mathbb{Z}_n$, $x = \phi(r)$. So $\phi$ is onto. Thus, $\phi$ is an isomorphism. □

**Definition and notation.** Let $G$ be a group and let $a \in G$. We define the *order* of $a$, denoted $o(a)$, to be $|\langle a \rangle|$. (Note: If there exists a positive integer $k$ such that $a^k = e$, then the least such integer is the order of $a$; otherwise, $o(a) = \infty$.)

**Remark.** Do not confuse the order of a group with the order of an element of a group. These are related concepts, but they are distinct, and have distinct notations: as we've seen, the order of a group, $G$, is denoted by $|G|$, while the order of an element $a$ of a group is denoted by $o(a)$.

We have the following handy theorem.

**Theorem 5.6.** *Let $a \in G$. Then $o(a) = o(a^{-1})$.*

*Proof.* First, assume $o(a) = n < \infty$. Then

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e,$$

so $o(a^{-1}) \leq n = o(a)$. Using the same argument, we have $n = o(a) \leq o(a^{-1})$. Since $o(a^{-1}) \leq n$ and $n \leq o(a^{-1})$, $o(a^{-1}) = n = o(a)$.

On the other hand, assume $o(a) = \infty$. Then $a^{-1}$ must also have infinite order, since if it had finite order $m$, $a$ would, by the above argument, have order less than or equal to $m$. □

Unfortunately, there's no formula one can simply use to compute the order of an element in an arbitrary group. However, in the special case that the group is cyclic of order $n$, we do have such a formula. We present the following result without proof.

**Theorem 5.7.** *For each $a \in \mathbb{Z}_n$, $o(a) = n/\gcd(n, a)$.*

Here are some examples of cyclic subgroups of groups, and orders of group elements.

**Example 5.8.**

1. In $\mathbb{Z}$, $\langle 2\rangle = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z}$. More generally, given any $n \in \mathbb{Z}$, in $\mathbb{Z}$ we have $\langle n\rangle = n\mathbb{Z}$. For $a \in \mathbb{Z}$, $o(a) = \infty$ if $a \neq 0$; $o(0) = 1$.
2. In $\mathbb{Z}_8$, we have $\langle 0\rangle = \{0\}$, $\langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \mathbb{Z}_8$, $\langle 2\rangle = \langle 6\rangle = \{0, 2, 4, 6\}$, and $\langle 4\rangle = \{0, 4\}$.
3. In $\mathbb{R}$, $\langle \pi\rangle = \pi\mathbb{Z}$, so $o(\pi) = \infty$.
4. In $\mathbb{R}^*$, $\langle \pi\rangle = \{\pi^n : n \in \mathbb{Z}\}$. Again, $o(\pi) = \infty$.
5. In $\mathbb{M}_2(\mathbb{R})$,
$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} c & c \\ 0 & c \end{bmatrix} : c \in \mathbb{Z} \right\} = \left\{ c \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} : c \in \mathbb{Z} \right\}.$$
The order of the the matrix is therefore infinity.
6. In $\mathbb{M}_2(\mathbb{Z}_2)$, if $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, then $\langle A\rangle = \{A, \mathbf{0}\}$, so $A$ has order 2.
7. In $GL(2, \mathbb{Z}_2)$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has order 2. (Why?)
8. In $GL(2, \mathbb{R})$, $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ has order 4. (Why?)
9. In $GL(2, \mathbb{R})$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order. (Why?)
10. In $GL(4, \mathbb{Z}_2)$, $A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ has order 2. (Why?)

**Theorem 5.9.** *Every cyclic group $G$ is of the form $\langle a\rangle$ for some $a \in G$.*

*Proof.* Let $G$ be cyclic. Suppose $|G| = \infty$. Then there is an isomorphism $\phi : \mathbb{Z} \to G$. Note that $\mathbb{Z} = \langle 1\rangle$. So
$$G = \phi(\mathbb{Z}) = \{\phi(a) \,:\, a \in \mathbb{Z}\} = \{\phi(a(1)) \,:\, a \in \mathbb{Z}\} = \{a\phi(1) \,:\, a \in \mathbb{Z}\} = \langle \phi(1)\rangle.$$
A similar argument shows that there exists $a \in G$ such that $G = \langle a\rangle$ when $|G| < \infty$. □

**Definitions.** Let $G$ be a group. An element $a \in G$ is a *generator of $G$* (equivalently, *$a$ generates $G$*) if $\langle a\rangle = G$.

**Remarks.**

1. Note that if $G$ has a generator, then it is necessarily a cyclic group.

2. Note that an element $a$ of a group $G$ generates $G$ if and only if every element of $G$ is of the form $a^n$ for some $n \in \mathbb{Z}$.

3. Generators of groups need not be unique. For instance, we saw in Example 5.8 that each of the elements $1, 3, 5$ and $7$ of $\mathbb{Z}_8$ is a generator for $\mathbb{Z}_8$.

**Example 5.10.**

1. $\mathbb{Z}$ has generator 1 and generator $-1$.

2. Given $n \in \mathbb{Z}$, $nZ$ has generator $n$ and generator $-n$.

3. Given $n \geq 2$ in $\mathbb{Z}$, the generators of $\mathbb{Z}_n$ are exactly the elements $a \in \mathbb{Z}_n$ such that $\gcd(n, a) = 1$. (This follows from Theorem 5.7.)

**Remark.** Order of elements provides another group invariant.

**Theorem 5.11.** *Let $\phi : G \to G'$ be a group isomorphism and let $a \in G$. Then $o(\phi(a)) = o(a)$.*

*Proof.* This follows from the fact that $\phi(\langle a \rangle) = \langle \phi(a) \rangle$. □

**Corollary 5.12.** *If groups $G$ and $G'$ are isomorphic then for any $n \in \mathbb{Z}^+$, the number of elements of $G$ of order $n$ is the same as the number of elements of $G'$ of order $n$.*

**Example 5.13.** Since 1 in $\mathbb{Z}_4$ has order 4 but every element in $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order less than or equal to 2, these groups cannot be isomorphic.

**WARNING**

Note, however, that just because the orders of elements of two groups "match up" the groups need not be isomorphic. For example, every element of $\mathbb{Z}$ has infinite order, except for its identity element, which has order 1; the same is true for the group $\mathbb{Q}$. However, we have previously proven that these groups are not isomorphic.

## 5.2 Exploring the subgroup lattices of cyclic groups

We now explore the subgroups of cyclic groups. A complete proof of the following theorem is provided on p. 61 of [1].

**Theorem 5.14.** *Every subgroup of a cyclic group is cyclic.*

**Sketch of proof:** Let $G = \langle a \rangle$ and $H \leq G$. If $H = \{e\}$, then clearly $H$ is cyclic. Else, there exists an element $a^i$ in $H$ with $i > 0$; let $d$ be the least positive integer such that $a^d \in H$. It turns out that $H = \langle a^d \rangle$.

**Corollary 5.15.** *Every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$. (Note that $n\mathbb{Z} \simeq \mathbb{Z}$ unless $n = 0$.)*

Really, it suffices to study the subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$ to understand the subgroup lattice of every cyclic group.

We provide the following theorem without proof.

**Theorem 5.16.** *The nontrivial subgroups of $\mathbb{Z}_n$ are exactly those of the form $\langle d \rangle$, where $d$ is a positive divisor of $n$. Note that $|\langle d \rangle| = n/d$ for each such $d$.*[1]

In fact:

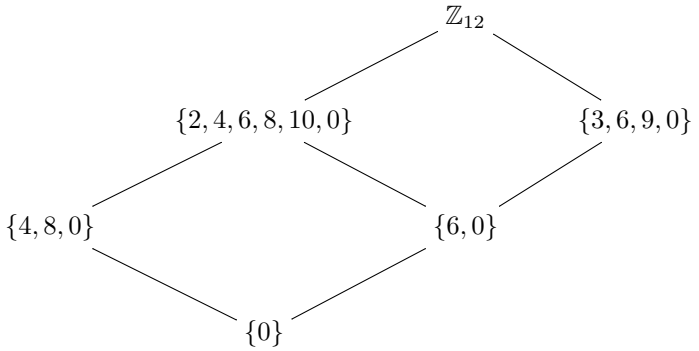
**Theorem 5.17.** *$\mathbb{Z}_n$ has a unique subgroup of order $k$, for each positive divisor $k$ of $n$.*

**Example 5.18.** How many subgroups does $\mathbb{Z}_{18}$ have? What are the generators of $\mathbb{Z}_{15}$?

Well, the positive divisors of 18 are $1, 2, 3, 6, 9$, and 18, so $\mathbb{Z}_{18}$ has exactly six subgroups (namely, $\langle 1 \rangle$, $\langle 2 \rangle$, etc.). The generators of $\mathbb{Z}_{15}$ are the elements of $\mathbb{Z}_{15}$ that are relatively prime to 15, namely $1, 2, 4, 7, 8, 11, 13$, and 14.

**Example 5.19.** Draw a subgroup lattice for $\mathbb{Z}_{12}$.

The positive divisors of 12 are $1, 2, 3, 4, 6$, and 12; so $\mathbb{Z}_{12}$'s subgroups are of the form $\langle 1 \rangle$, $\langle 2 \rangle$, etc. So $\mathbb{Z}_{12}$ has the following subgroup lattice.




[1] **Remark.** It turns out that for each $0 \neq a \in \mathbb{Z}_n$, $\langle a \rangle = \left\langle \frac{n}{\gcd(n, a)} \right\rangle$. Note that it follows that $|\langle a \rangle| = n/\gcd(n, a)$ for every $0 \neq a \in \mathbb{Z}_n$.

## 5.3 Exercises

### Exercise 5.1

True/False. For each of the following, write T if the statement is true; otherwise, write F. You do NOT need to provide explanations or show work for this problem.Throughout, let $G$ be a group with identity element $e$.

(a) If $G$ is infinite and cyclic, then $G$ must have infinitely many generators.

(b) There may be two distinct elements $a$ and $b$ of a group $G$ with $\langle a\rangle = \langle b\rangle$.

(c) If $a, b \in G$ and $a \in \langle b\rangle$ then we must have $b \in \langle a\rangle$.

(d) If $a \in G$ with $a^4 = e$, then $o(a)$ must equal 4.

(e) If $G$ is countable then $G$ must be cyclic.

### Exercise 5.2

Give examples of the following.

(a) An infinite noncyclic group $G$ containing an infinite cyclic subgroup $H$.

(b) An infinite noncyclic group $G$ containing a finite nontrivial cyclic subgroup $H$.

(c) A cyclic group $G$ containing exactly 20 elements.

(d) A nontrivial cyclic group $G$ whose elements are all matrices.

(e) A noncyclic group $G$ such that every proper subgroup of $G$ is cyclic.

### Exercise 5.3

Find the orders of the following elements in the given groups.

(a) $2 \in \mathbb{Z}$

(b) $-i \in \mathbb{C}^*$

(c) $-I_2 \in GL(2, \mathbb{R})$

(d) $-I_2 \in \mathbb{M}_2(\mathbb{R})$

(e) $(6, 8) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10}$

### Exercise 5.4

For each of the following, if the group is cyclic, list *all* of its generators. If the group is *not* cyclic, write NC.

(a) $5\mathbb{Z}$ (b) $\mathbb{Z}_{18}$ (c) $\mathbb{R}$ (d) $\langle\pi\rangle$ in $\mathbb{R}$ (e) $\mathbb{Z}_2^2$ (f) $\langle 8\rangle$ in $\mathbb{Q}^*$

## Exercise 5.5

Explicitly identify the elements of the following subgroups of the given groups. You may use set-builder notation if the subgroup is infinite, or a conventional name for the subgroup if we have one.

(a) $\langle 3 \rangle$ in $\mathbb{Z}$

(b) $\langle i \rangle$ in $C^*$

(c) $\langle A \rangle$, for $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in \mathbb{M}_2(\mathbb{R})$

(d) $\langle (2,3) \rangle$ in $\mathbb{Z}_4 \times \mathbb{Z}_5$

(e) $\langle B \rangle$, for $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$

## Exercise 5.6

Draw subgroup lattices for (a) $\mathbb{Z}_6$, (b) $\mathbb{Z}_{13}$, and (c) $\mathbb{Z}_{18}$.

## Exercise 5.7

Let $G$ be a group with no nontrivial proper subgroups. Prove that $G$ is cyclic.

# Chapter 6

# Permutation Groups and Dihedral Groups

We have already been introduced to two important classes of nonabelian groups: namely, the matrix groups $GL(n, \mathbb{R})$ and $SL(n, \mathbb{R})$ for $n \geq 2$. We now consider a more general class of (mostly) nonabelian groups: permutation groups.

## 6.1 Introduction to permutation groups

**Definitions.** A *permutation* on a set $A$ is a bijection from $A$ to $A$. We say a permutation $\sigma$ on $A$ *fixes* $a \in A$ if $\sigma(a) = a$.

**Example 6.1.** Let $A$ be the set $A = \{\Delta, \star, \$\}$. Then the functions $\sigma : A \to A$ defined by

$$\sigma(\Delta) = \star, \quad \sigma(\star) = \Delta, \quad \text{and } \sigma(\$) = \$$$

and $\tau : A \to A$ defined by

$$\tau(\Delta) = \$, \quad \tau(\star) = \Delta, \quad \text{and } \tau(\$) = \star$$

are both permutations on $A$.

**Definitions and notation.** Composition of permutations on a set $A$ is often called *permutation multiplication*, and if $\sigma$ and $\tau$ are permutations on a set $A$, we usually omit the composition symbol and write $\sigma \circ \tau$ simply as $\sigma\tau$.

> **WARNING**
>
> For us, if $\sigma$ and $\tau$ are permutations on a set $A$, then applying $\sigma\tau$ to $A$ means first applying $\tau$ and then applying $\sigma$. This is due to the conventional right-to-left reading of function compositions.

That is, if $a \in A$, by $\sigma\tau(a)$ we mean $\sigma(\tau(a))$. (Some other books/mathematicians do not use this convention, and read permutation multiplication from left-to-right. Make sure to always know what convention your particular author or colleague is using!)

**Example 6.2.** Let $A$, $\sigma$, and $\tau$ be as in Example 6.1. Then $\sigma\tau$ is the function from $A$ to $A$ defined by

$$\sigma\tau(\Delta) = \$, \quad \sigma\tau(\star) = \star, \quad \text{and } \sigma\tau(\$) = \Delta,$$

while $\tau\sigma$ is the function from $A$ to $A$ defined by

$$\tau\sigma(\Delta) = \Delta, \quad \tau\sigma(\star) = \$, \quad \text{and } \tau\sigma(\$) = \star$$

.

**Definition.** Given a set $A$, we let $S_A$ be the set of all permutations on $A$.

**Theorem 6.3.** *Given a set A:*

- *$S_A$ is a group under permutation multiplication.*
- *If $A$ has finite cardinality $n$, then $|S_A| = n!$ (if $|A| = \infty$ then $|S_A|$ is also $\infty$).*
- *$S_A$ is abelian if $|A| = 1$ or 2, and nonabelian otherwise.*

*Proof.* Let $\sigma, \tau \in S_A$. Since a composition of bijections is a bijection (see Theorem 1.9), $\sigma\tau$ is a bijection from $A$ to $A$, hence is in $S_A$. So $S_A$ is closed under composition.

$\mathscr{G}_1$: Function composition is always associative.

$\mathscr{G}_2$: The identity function $1_A : A \to A$ defined by

$$1_A(a) = a \text{ for all } a \in A$$

clearly acts as an identity element in $S_A$. Henceforth, we will denote $1_A$ by $e$.

$\mathscr{G}_3$: Let $\sigma \in S_A$. Since $\sigma$ is a bijection, $\sigma$ has an inverse function $\sigma^{-1}$ that is also a bijection from $A$ to $A$ (Theorem 1.8). Since $\sigma^{-1} \in S_A$ with $\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1_A$, every element of $S_A$ has an inverse element in $S_A$.

So $S_A$ is a group. □

Clearly $|S_A| = \infty$ when $|A| = \infty$, and a straightforward combinatorial argument yields that when $|A| = n \in \mathbb{Z}^+$, we have $|S_A| = n!$. Finally, if $|A| = 1$ or 2, then $|S_A| = 1! = 1$ or $|S_A| = 2! = 2$ so $S_A$ must be abelian (as it's a group of order 1 or 2). On the other hand, suppose $|A| > 2$. Then $A$ contains at least three distinct elements, say $x$, $y$, and $z$. Let $\sigma$ be the permutation of $A$ swapping $x$ and $y$ and fixing every other element of $A$, and let $\tau$ be the permutation of $A$ swapping $y$ and $z$ and fixing every other element of $A$. Then $\sigma\tau(x) = y$ while $\tau\sigma(x) = z$, so $\sigma\tau \neq \tau\sigma$, and hence $S_A$ is nonabelian. We will in the future use language provided by the following definition:

**Definition.** A group is said to be a *permutation group* if it is a subgroup of $S_A$ for some set $A$.

**Remark.** Notice that if $A$ and $B$ are sets, then $|A| = |B|$ if and only if $S_A \simeq S_B$.

Thus, for any set $B$ with $|B| = n \in \mathbb{Z}^+$, we have $S_B \simeq S_A$, where $A = \{1, 2, \ldots, n\}$. Since we are concerned in this course primarily with group structures which are invariant under isomorphism, we may focus now on groups of permutations on the set $\{1, 2, \ldots, n\}$ $(n \in \mathbb{Z}^+)$.[1]

[1] We can, in fact, define $S_0$, the set of all permutations on the empty set. One can show, using the fact that a function is a relation on a Cartesian product of sets, that $S_0$ is the trivial group. However, this will not be relevant in this text.

## 6.2 Symmetric groups

**Definition and notation.** When $A = \{1, 2, \ldots, n\}$ ($n \in \mathbb{Z}^+$), we call $S_A$ the *symmetric group on $n$ letters* and denote it by $S_n$.

**Remark.** Throughout this course, if we are discussing a group $S_n$, you should assume $n \in \mathbb{Z}^+$.

It is important for us to be able to easily describe specific elements of $S_n$. It would be cumbersome to describe, for instance, an element of $S_3$ by saying it swaps 1 and 2 and fixes 3; imagine how much more cumbersome it could be to describe an element of, say, $S_{100}$! One can somewhat concisely describe a permutation $\sigma$ of $S_n$ by listing out the elements $1, 2, \ldots, n$ and writing the element $\sigma(i)$ below each $i$ for $i = 1, 2, \ldots, n$. For instance, if $\sigma$ sends 1 to 2, we'd write the number 2 below the number 1. The convention is to enclose these two rows of numbers in a single set of parentheses, as in the following example.

**Example 6.4.** We can denote the element $\sigma$ of $S_3$ that swaps 1 and 2 and fixes 3 by

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

and the element $\tau$ of $S_3$ that sends 1 to 3, 2 to 1, and 3 to 2 by

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

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

But even this notation is unnecessarily cumbersome. Instead, we use *cycle notation*.

**Definitions and notation.** A permutation $\sigma$ in $S_n$ is called a *$k$-cycle* or a *cycle of length $k$* (or, less specifically, a *cycle*) if there exist elements $a_1, a_2, \ldots, a_k$ in $\{1, 2, \ldots, n\}$ such that

$\sigma(a_i) = a_{i+1}$ for each $i = 1, 2, \ldots, k-1$;
$\sigma(a_k) = a_1$; and
$\sigma(x) = x$ for every other element of $\{1, 2, \ldots, n\}$.

We use the *cycle notation* $\sigma = (a_1 a_2 \cdots a_k)$ to describe such a cycle. A 2-cycle is often called a *transposition*.

**Example 6.5.** The permutation $\tau$ in $S_3$ that sends 1 to 3, 2 to 1, and 3 to 2 is a cycle. It can be denoted by $\tau = (132)$. Similarly, the cycle $\rho$ in $S_3$ swapping 1 and 3 can be denoted by $\rho = (13)$. On the other hand, the permutation in $S_4$ that swaps 1 with 2 and 3 with 4 is <u>not</u> a cycle.

**Remark.** Given a $k$-cycle $\sigma = (a_1 a_2 \cdots a_k)$, there are $k$ different expressions for $\sigma$. Indeed, we have

$$\sigma = (a_1 a_2 \cdots a_k) = (a_2 a_3 \cdots a_k a_1) = (a_3 a_4 \cdots a_k a_1 a_2) = \cdots = (a_k a_1 \cdots a_{k-1}).$$

**Example 6.6.** The permutation $\tau$ described in Example 6.5 can also be written as (321) and as (213).

However, by convention, we usually "start" a cycle $\sigma$ with the smallest of the numbers that $\sigma$ doesn't fix: e.g., we'd write $\sigma = (213)$ as $(132)$.

**Definitions.** Two cycles $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ are said to be *disjoint* if $a_i \neq b_j$ for all $i$ and $j$. Cycles $\sigma_1$, $\sigma_2$, ..., $\sigma_m$ are *disjoint* if $\sigma_i$ and $\sigma_j$ are disjoint for each $i \neq j$. (Notice: this version of disjointness is what we usually refer to as *mutual* disjointness.)

**Remark.** Note that if cycles $\sigma$ and $\tau$ are disjoint, then $\sigma$ and $\tau$ commute; that is, $\sigma\tau = \tau\sigma$.

**WARNING**

If cycles $\sigma$ and $\tau$ are not disjoint then they may not commute. For instance, see Example 6.4, where $\sigma\tau \neq \tau\sigma$.

Note that any permutation of $S_n$ is a product of disjoint cycles (where by "product" we mean the permutation resulting from permutation multiplication).

**Definition.** Writing a permutation in *(disjoint) cycle notation* means writing it as a product of disjoint cycles, where each cycle is written in cycle notation.

**Remark.** Note that if $\sigma$ in $S_n$ is written in cycle notation and the number $a \in \{1, 2, \ldots, n\}$ appears nowhere in $\sigma$'s representation, this means that $\sigma$ fixes $a$. The only permutation that we cannot really write in cycle notation is the identity element $1_A$ of $S_A$, which we henceforth denote by $e$.

**Example 6.7.** The permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix}$$

is the product of disjoint cycles $(132)$ and $(46)$, so in cycle notation we have

$$\sigma = (132)(46).$$

Note that we could also write $\sigma$ as $(321)(46)$, $(213)(64)$, $(64)(132)$, etc.

While it is true that we also have $\sigma = (13)(23)(46)$, this is not a disjoint cycle representation of $\sigma$ since both $(13)$ and $(23)$ "move" the element 3.

**Example 6.8.** In $S_4$, let $\sigma = (243)$ and $\tau = (13)(24)$. Then $\sigma\tau = (123)$ and $\tau\sigma = (134)$.

**Example 6.9.** In $S_9$, let $\sigma = (134)$, $\tau = (26)(17)$, and $\rho = (358)(12)$. Find the following, writing your answers using disjoint cycle notation.

| | | | |
|---|---|---|---|
| $\sigma^{-1}$ | $\sigma^{-1}\tau\sigma$ | $\sigma^2$ | $\sigma^3$ |
| $\rho^2$ | $\rho^{-2}$ | $\sigma\tau$ | $\sigma\rho$ |

**Example 6.10.** Explicitly express all the elements of $S_4$ in disjoint cycle notation.

**Theorem 6.11.** *Any $k$-cycle has order $k$ in $S_n$. More generally, if permutation $\sigma$ can be written in disjoint cycle notation as $\sigma = \sigma_1\sigma_2\cdots\sigma_m$, then*

$$\begin{aligned} o(\sigma) &= \text{lcm}(o(\sigma_1), o(\sigma_2), \ldots, o(\sigma_m)) \\ &= \text{lcm}(\text{length}(\sigma_1), \text{length}(\sigma_2), \ldots, \text{length}(\sigma_m)), \end{aligned}$$

*where* lcm *denotes the least common multiple.*

**WARNING**

Permutation $\sigma$ must be in disjoint cycle notation for the above formula to hold. For instance, let $\sigma = (12)(23)$ in $S_3$. The transpositions (12) and (23) both have order 2, but $o(\sigma) \neq \text{lcm}(2,2) = 2$. Rather, $o(\sigma) = 3$, since in disjoint cycle notation $\sigma$ can be written as $\sigma = (123)$. You must write a permutation using disjoint cycle notation before attempting to use this method to compute its order!

**Example 6.12.**

1. Find the orders of each of the elements in Example 6.9, including $\sigma$, $\tau$, and $\rho$ themselves.
2. Explicitly list the elements of $\langle\sigma\rangle$, $\langle\tau\rangle$, and $\langle\rho\rangle$.

## 6.3 Alternating groups

Note that every $k$-cycle $(a_1 a_2 \dots a_k) \in S_n$ can be written as a product of (not necessarily disjoint) transpositions:

$$(a_1 a_2 \dots a_k) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2).$$

We therefore have the following theorem.

**Theorem 6.13.** *Every permutation in $S_n$ can be written as a product of transpositions.*

**Definition.** We say that a permutation in $S_n$ is *even* [resp., *odd*] if it can be written as a product of an even [resp., odd] number of transpositions.

**Theorem 6.14.** *Every permutation in $S_n$ is even or odd, but not both.*

*Proof.* We already know that every permutation is $S_n$ is a product of transpositions, so must be even or odd. For proof that no permutation is both even *and* odd, see, for instance, Proof 1 or 2 of Theorem 9.15 on p. 91 in [1]. □

**Lemma 6.15.** *For each $2 \leq k \leq n$, then a $k$-cycle is even if $k$ is odd, and odd if $k$ is even.*

*Proof.* This proof is left as an exercise for the reader. □

**Example 6.16.** In $S_3$, the permutations $e$, $(123) = (13)(12)$, and $(132) = (12)(13)$ are even, while the permutations (12), (13), and (23) are odd.

**Example 6.17.** List all of the even [resp., odd] permutations in $S_4$.

It turns out that the set of all even permutations in $S_n$ is a subgroup of $S_n$. The proof of this is left as an exercise for the reader.

**Definition.** The set of all even permutations in $S_n$ is a subgroup of $S_n$, called the *alternating group on $n$ letters*, and denoted by $A_n$.

We end with this theorem, whose proof can be found on p. 93 of [1].

**Theorem 6.18.** $A_n = (n!)/2$.

## 6.4 Cayley's Theorem

One might wonder how "common" permutation groups are in math. They are, it turns out, ubiquitous in abstract algebra: in fact, **every group** can be thought of as a group of permutations! We will prove this, but we first need the following lemma. (We will not use the maps $\rho_a$ or $c_a$, defined below, in our theorem, but define them here for potential future use.)

**Lemma 6.19.** *Let $G$ be a group and $a \in G$. Then the following functions are permutations on $G$, and hence are elements of $S_G$:*

*(i)* $\lambda_a : G \to G$ *defined by* $\lambda_a(x) = ax$;

*(ii)* $\rho_a : G \to G$ *defined by* $\rho_a(x) = xa$;

*(iii)* $c_a : G \to G$ *defined by* $c_a(x) = axa^{-1}$.

*Proof.* For (i): If $x_1, x_2 \in G$ with $\lambda_a(x_1) = \lambda_a(x_2)$, then $ax_1 = ax_2$; so, by left cancellation, $x_1 = x_2$. Thus, $\lambda_a$ is one-to-one. Further, each $y \in G$ equals $\lambda_a(a^{-1}y)$ for $a^{-1}y \in G$, so $\lambda_a$ is onto. Thus, $\lambda_a$ is a bijection from $G$ to $G$: that is, it's a permutation on $G$. The proofs for $\rho_a$ and $c_a$ are similar. □

**Terminology.** We say that $\lambda_a$, $\rho_a$, and $c_a$ perform on $G$, respectively, *left multiplication by $a$*, *right multiplication by $a$*, and *conjugation by $a$*. (Nota bene: sometimes when people talk about conjugation by $a$ they instead are referring to the permutation of $G$ that sends each $x$ to $a^{-1}xa$.)

Now we are ready for our theorem:

**Theorem 6.20.** ***(Cayley's Theorem)*** *Let $G$ be a group. Then $G$ is isomorphic to a subgroup of $S_G$. Thus, every group can be thought of as a group of permutations.*

*Proof.* For each $a \in G$, let $\lambda_a$ be defined, as above, by $\lambda_a(x) = ax$ for each $x \in G$; recall that each $\lambda_a$ is in $S_G$. Now define $\phi : G \to S_G$ by $\phi(a) = \lambda_a$, for each $a \in G$.

We claim that $\phi$ is both a homomorphism and one-to-one. Indeed, let $a, b \in G$. Now, $\phi(a)\phi(b)$ and $\phi(ab)$ are both functions with domain $G$, so we need to show $(\phi(a)\phi(b))(x) = (\phi(ab))(x)$ for each $x \in G$. Well, let $x \in G$. Then

$$\begin{aligned}
(\phi(a)\phi(b))(x) &= (\lambda_a\lambda_b)(x) \\
&= \lambda_a(\lambda_b(x)) && \text{(since the operation on } S_G \text{ is composition)} \\
&= \lambda_a(bx) \\
&= a(bx) \\
&= (ab)x \\
&= \lambda_{ab}(x) \\
&= (\phi(ab))(x).
\end{aligned}$$

So $\phi$ is a homomorphism. Further, if $a, b \in G$ with $\phi(a) = \phi(b)$, then $\lambda_a = \lambda_b$. In particular, $\lambda_a(e) = \lambda_b(e)$. But $\lambda_a(e) = ae = a$ and $\lambda_b(e) = be = b$, so $a = b$. Thus, $\phi$ is one-to-one.

Since by definition $\phi(G)$ we have that $\phi$ maps $G$ **onto** $\phi(G)$, we conclude that $\phi$ provides an isomorphism from $G$ to the subgroup $\phi(G)$ of $S_G$. □

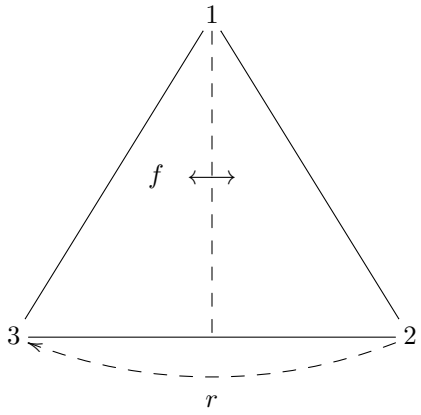
**Nota bene.** In general, $\phi(G) \neq S_G$, so we cannot conclude that $G$ is isomorphic to $S_G$ itself; rather, we may only conclude that it is is isomorphic to some subgroup of $S_G$.

**Remark.** While we chose to use the maps $\lambda_a$ to prove the above theorem, we could just as well have used the maps $\rho_a$ or $c_a$, instead.

## 6.5 Dihedral groups

Dihedral groups are groups of symmetries of regular $n$-gons. We start with an example.

**Example 6.21.** Consider a regular triangle $T$, with vertices labeled 1, 2, and 3. We show $T$ below, also using dotted lines to indicate a vertical line of symmetry of $T$ and a rotation of $T$.




Note that if we reflect $T$ over the vertical dotted line (indicated in the picture by $f$), $T$ maps onto itself, with 1 mapping to 1, and 2 and 3 mapping to each other. Similarly, if we rotate $T$ clockwise by 120° (indicated in the picture by $r$), $T$ again maps onto itself, this time with 1 mapping to 2, 2 mapping to 3, and 3 mapping to 1. Both of these maps are called *symmetries* of $T$; $f$ is a *reflection* or *flip* and $r$ is a *rotation*.

Of course, these are not the only symmetries of $T$. If we compose two symmetries of $T$, we obtain a symmetry of $T$: for instance, if we apply the map $f \circ r$ to $T$ (meaning first do $r$, then do $f$) we obtain reflection over the line connecting 2 to the midpoint of line segment $\overline{13}$. Similarly, if we apply the map $f \circ (r \circ r)$ to $T$ (first do $r$ twice, then do $f$) we obtain reflection over the line connecting 3 to the midpoint of line segment $\overline{12}$. In fact, every symmetry of $T$ can be obtained by composing applications of $f$ and applications of $r$.

For convenience of notation, we omit the composition symbols, writing, for instance, $fr$ for $f \circ r$, $r \circ r$ as $r^2$, etc. It turns out there are exactly six symmetries of $T$, namely:

1. the map $e$ from $T$ to $T$ sending every element to itself;
2. $f$ (that is, reflection over the line connecting 1 and the midpoint of $\overline{23}$);
3. $r$ (that is, clockwise rotation by 120°);
4. $r^2$ (that is, clockwise rotation by 240°);
5. $fr$ (that is, reflection over the line connecting 2 and the midpoint of $\overline{13}$); and
6. $fr^2$ (that is, reflection over the line connecting 3 and the midpoint of $\overline{12}$).

Declaring that $f^0 = r^0 = e$, the set

$$D_3 = \{e, f, r, r^2, fr, fr^2\} = \{f^i r^j : i = 0, 1, j = 0, 1, 2\}$$

is the collection of all symmetries of $T$.

**Remark.** Notice that $rf = fr^2$ and that $f^2 = r^3 = e$.

**Theorem 6.22.** *$D_3$ is a group under composition.*

*Proof.* We first show that $D_3$ is closed under composition. As noted above, $rf = fr^2$. So any map of the form $f^i r^j f^k r^l$ $(i, k = 0, 1,\ j, l = 0, 1, 2)$ can be written in the form $f^s r^t$ for some $s, t \in \mathbb{N}$. Finally, let $R_2(s)$ and $R_3(t)$ be the remainders when you divide $s$ by 2 and $t$ by 3; then $f^s r^t = f^{R_2(s)} r^{R_3(t)} \in D_3$. So $D_3$ is closed under composition.

Next:

$\mathscr{G}_1$: Function composition is always associative.

$\mathscr{G}_2$: The function $e$ clearly acts as identity element in $D_3$.

$\mathscr{G}_3$: Let $x = f^i r^j \in D_3$. Then $y = r^{3-j} f^{2-i}$ is in $D_3$ (since $D_3$ is closed under composition) with $xy = yx = e$.

So $D_3$ is a group. □

Let us look at $D_3$ another way. Note that each map in $D_3$ can be uniquely described by how it permutes the vertices $1, 2, 3$ of $T$: that is, each map in $D_3$ can be uniquely identified with a unique element of $S_3$. For instance, $f$ corresponds to the permutation (23) in $S_3$, while $fr$ corresponds to the permutation (13). In turns out that $D_3 \simeq S_3$, via the following correspondence

$$\begin{array}{ccc} e & \leftrightarrow & e \\ f & \leftrightarrow & (23) \\ r & \leftrightarrow & (123) \\ r^2 & \leftrightarrow & (132) \\ fr & \leftrightarrow & (13) \\ fr^2 & \leftrightarrow & (12) \end{array}$$

The group $D_3$ is an example of class of groups called *dihedral groups*.

**Definition.** Let $n$ be an integer greater than or equal to 3. We let $D_n$ be the collection of symmetries of the regular $n$-gon. It turns out that $D_n$ is a group (see below), called the *dihedral group of order* $2n$ (Note: Some books and mathematicians instead denote the group of symmetries of the regular $n$-gon by $D_{2n}$—so, for instance, our $D_3$, above, would instead be called $D_6$. Make sure you are aware of the convention your book or colleague is using.)

**Theorem 6.23.** *Let $n$ be an integer greater than or equal to 3. Then, again using the convention that $f^0 = r^0 = e$, $D_n$ can be uniquely described as*

$$D_n = \{f^i r^j : i = 0, 1, j = 0, 1, \ldots, n-1\}$$

*with the relations*

$$rf = fr^{n-1} \quad \textit{and} \quad f^2 = r^n = e.$$

*The dihedral group $D_n$ is a nonabelian group of order $2n$.*

*Proof.* The proof that $D_n$ is a group parallels the proof, above, that $D_3$ is a group. It is clear that $D_n$ is nonabelian (e.g., $rf = fr^{n-1} \neq fr$) and has order $2n$. □

**Remark.** Throughout this course, if we are discussing a group $D_n$ you should assume $n \in \mathbb{Z}^+$, $n \geq 3$, unless otherwise noted.

**Definition.** We say that an element of $D_n$ is written in *standard form* if it is written in the form $f^i r^j$ where $i \in \{0, 1\}$ and $j \in \{0, 1, \ldots, n-1\}$.

**Theorem 6.24.** *Each $D_n$ is isomorphic to a subgroup of $S_n$.*

**Sketch of proof.** We described above how $D_3$ is isomorphic to a subgroup (namely, the improper subgroup) of $S_3$. One can show that each $D_n$ is isomorphic to a subgroup of $S_n$ by similarly labeling the vertices of the regular $n$-gon $1, 2, \ldots, n$ and determining how these vertices are permuted by each element of $D_n$.

**WARNING**

While $D_3$ is actually isomorphic to $S_3$ itself, for $n > 3$ we have that $D_n$ is not isomorphic to $S_n$ but is rather isomorphic to a proper subgroup of $S_n$. When $n > 3$ you can see that $D_n$ cannot be isomorphic to $S_n$ since $|D_n| = 2n < n! = |S_n|$ for $n > 3$.

It is important to be able to do computations with specific elements of dihedral groups. We have the following theorem.

**Theorem 6.25.** *The following relations hold in $D_n$, for every $n$:*

1. *For every $i$, $r^i f = fr^{-i}$ (in particular, $rf = fr^{-1} = fr^{n-1}$);*
2. *$o(fr^i) = 2$ for every $i$ (in particular, $f^2 = e$);*
3. *$o(r) = o(r^{-1}) = n$;*
4. *If $n$ is even, then $r^{n/2}$ commutes with every element of $D_n$.*

*Proof.*

1. We use induction on the exponent of $r$. We already know that $r^1 f = fr^{-1}$. Now suppose $r^{i-1} f = fr^{-(i-1)}$ for some $i \geq 2$. Then
$$r^i f = r(r^{i-1} f) = r(fr^{-(i-1)}) = (rf)r^{-i+1} = (fr^{-1})r^{-i+1} = fr^{-i}.$$
2. For every $i$, $fr^i \neq e$, but
$$(fr^i)^2 = (fr^i)(fr^i) = f(r^i f)r^i = f(fr^{-i})r^i = f^2 r^0 = e.$$
3. This follows from Theorem 5.6 and the fact that $o(r) = n$.
4. The proof of this statement is left as an exercise for the reader. □

**Example 6.26.**

1. Write $fr^2 f$ in $D_3$ in standard form. Do the same for $fr^2 f$ in $D_4$.
2. What is the inverse of $fr^3$ in $D_5$? Write it in standard form.
3. Explicitly describe an isomorphism from $D_4$ to a subgroup of $S_4$.

**Example 6.27.** Classify the following groups up to isomorphism. (**Hint:** You may want to look at the number of group elements that have a specific finite order.)

| | | | |
|---|---|---|---|
| $\mathbb{Z}$ | $\mathbb{Z}_6$ | $\mathbb{Z}_2$ | $S_6$ |
| $\mathbb{Z}_4$ | $\mathbb{Q}$ | $3\mathbb{Z}$ | $\mathbb{R}$ |
| $S_2$ | $\mathbb{R}^*$ | $S_3$ | $\mathbb{Q}^*$ |
| $\mathbb{C}^*$ | $\langle \pi \rangle$ in $\mathbb{R}^*$ | $D_6$ | $\langle (134)(25) \rangle$ in $S_5$ |
| $\mathbb{R}^+$ | $D_3$ | $\langle r \rangle$ in $D_4$ | $17\mathbb{Z}$ |

## 6.6 Exercises

Throughout these exercises, write all of your permutations using disjoint cycle notation.

### Exercise 6.1

Let $\sigma = (134)$, $\tau = (23)(145)$, $\rho = (56)(78)$, and $\alpha = (12)(145)$ in $S_8$. Compute the following.

(a) $\sigma\tau$ (b) $\tau\sigma$ (c) $\tau^2$ (d) $\tau^{-1}$ (e) $o(\tau)$ (f) $o(\rho)$ (g) $o(\alpha)$ (h) $\langle\tau\rangle$

### Exercise 6.2

Prove Lemma 6.15.

### Exercise 6.3

Prove that $A_n$ is a subgroup of $S_n$.

### Exercise 6.4

Prove or disprove: The set of all odd permutations in $S_n$ is a subgroup of $S_n$.

### Exercise 6.5

Let $n$ be an integer greater than 2. $m \in \{1, 2, \ldots, n\}$, and let $H = \{\sigma \in S_n : \sigma(m) = m\}$ (in other words, $H$ is the set of all permutations in $S_n$ that fix $m$).

(a) Prove that $H \leq S_n$.

(b) Identify a familiar group to which $H$ is isomorphic. (You do not need to show any work.)

### Exercise 6.6

Write $rfr^2frfr$ in $D_5$ in standard form.

### Exercise 6.7

Prove or disprove: $D_6 \simeq S_6$.

### Exercise 6.8

Which elements of $D_4$ (if any)

(a) have order 2?

(b) have order 3?

Write all your elements in standard form.

### Exercise 6.9

Let $n$ be an even integer that's greater than or equal to 4. Prove that $r^{n/2} \in Z(D_n)$: that is, prove that $r^{n/2}$ commutes with every element of $D_n$. (Do NOT simply refer to the last statement in Theorem 6.25; that is the statement you are proving here.)

# Chapter 7

# The Wonderful World of Cosets

We have already seen one way we can examine a complicated group $G$: namely, study its subgroups, whose group structures are in some cases much more directly understandable than the structure of $G$ itself. But if $H$ is a subgroup of a group $G$, if we only study $H$ we lose all the information about $G$'s structure "outside" of $H$. We might hope that $G - H$ (that is, the set of elements of $G$ that are not in $H$) is also a subgroup of $G$, but we immediately see that cannot be the case since the identity element of $G$ must be in $H$, and $H \cap (G - H) = \emptyset$. Instead, let's ask how we can get at some understanding of $G$'s entire structure using a subgroup $H$? It turns out we use what are called *cosets* of $H$; but before we get to those, we need to cover some preliminary material.

## 7.1 Partitions of and equivalence relations on sets

**Definitions.** Let $S$ be a set. Then a collection of subsets $P = \{S_i\}_{i \in I}$ (where $I$ is some index set) is a *partition* of $S$ if each $S_i \neq \emptyset$ and each element of $S$ is in exactly one $S_i$. In other words, $P = \{S_i\}_{i \in I}$ is a partition of $S$ if and only if:

(i) each $S_i \neq \emptyset$;

(ii) the $S_i$ are mutually disjoint (that is, $S_i \cap S_j = \emptyset$ for $i \neq j \in I$); and

(iii) $S = \bigcup_{i \in I} S_i$.

The $S_i$ are called the *cells* of the partition.

**Example 7.1.**

1. The set $\{1, 2, 3\}$ has 5 partitions: namely,

   $$\{\{1, 2, 3\}\}, \{\{1, 2\}, \{3\}\}, \{\{1, 3\}, \{2\}\}, \{\{2, 3\}, \{1\}\} \text{ and } \{\{1\}, \{2\}, \{3\}\}.$$

   The first partition we've mentioned has one cell, the next three have two cells, and the last one has three cells.

2. The following is a 2-celled partition of $\mathbb{Z}$:

   $$\{\{x \in \mathbb{Z} : x \text{ is even}\}, \{x \in \mathbb{Z} : x \text{ is odd}\}\}.$$

The number of partitions of a finite set of $n$ elements gets large very quickly as $n$ goes to infinity. Indeed, there are 52 partitions of a set containing just 5 elements![1] But our goal here is not to count the number of partitions of a given set, but rather to use particular partitions of a group $G$ to help us study that group's structure. We turn now to our next definition.

**Definitions and notation.** Let $S$ be a set. Then a *relation* on $S$ is a subset $\mathscr{R}$ of $S \times S$.[2] If $\mathscr{R}$ is a relation on $S$ and $x, y \in S$, then we say $x$ is *related to* $y$, and write $x\mathscr{R}y$, if $(x, y) \in \mathscr{R}$; otherwise, we say that $x$ is *not related* to $y$, and write $x\not\mathscr{R}y$.

**Remark.** If there is a conventional notation used to denote a particular relation on a set, we will usually use that notation, rather than $\mathscr{R}$, to denote the relation.

We are already familiar with some relations on $\mathbb{R}$. Common such relations are $=$, $\neq$, $<$, $\leq$, $>$, and $\geq$; they contain exactly the elements we'd expect them to contain.

**Example 7.2.**

1. $<$ is a relation on $\mathbb{R}$ that contains, for instance, $(3, 4)$ but not $(3, 3)$ or $(4, 3)$; $\leq$ is a relation on $\mathbb{R}$ that contains $(3, 4)$ **and** $(3, 3)$ but not $(4, 3)$.
2. Given any $n \in \mathbb{Z}^+$, congruence modulo $n$, denoted $\equiv_n$, is a relation on $\mathbb{Z}$, where $\equiv_n$ is defined to be $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : n \text{ divides } x - y\}$.
3. We can define a relation $\mathscr{D}$ on $C^1$ (the set of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ whose derivatives are continuous) by declaring that $(f, g) \in C^1 \times C^1$ is in $\mathscr{D}$ if and only if $f' = g'$.

**Definitions.** Let $\mathscr{R}$ be a relation on a set $S$. Then $\mathscr{R}$ is said to be:
*reflexive on* $S$ if $x\mathscr{R}x$ for every $x \in S$;
*symmetric on* $S$ if whenever $x, y \in S$ with $x\mathscr{R}y$ we also have $y\mathscr{R}x$; and
*transitive on* $S$ if whenever $x, y, z \in S$ with $x\mathscr{R}y$ and $y\mathscr{R}z$ we also have $x\mathscr{R}z$.
A relation that is reflexive, symmetric, **and** transitive is called an *equivalence relation.*

**Remarks.**

1. You can think of an equivalence relation on a set $S$ as being a "weak version" of equality on $S$. Indeed, $=$ is an equivalence relation on any set $S$, but it also has a very special property that most equivalence relations **don't** have: namely, no element of $S$ is related to **any other element** of $S$ under $=$.
2. If we know, or plan to prove, that a relation is an equivalence relation, by convention we will often denote the relation by $\sim$, rather than by $\mathscr{R}$.

**Example 7.3.**

1. $<$ is **not** an equivalence relation on $\mathbb{R}$ because it is not reflexive: for instance, $3 \not< 3$. $\leq$ is also **not** an equivalence relation on $\mathbb{R}$, since even though it is reflexive, it's not symmetric: indeed, $3 \leq 4$ but $4 \not\leq 3$.

[1] The total number of partitions of an $n$-element set is the *Bell number*, $B_n$. There is no trivial way of computing $B_n$, in general, though the $B_n$ do satisfy the relatively simple recurrence relation

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k,$$

for each $n \geq 1$.

[2] More generally, if $S$ and $T$ are sets, a *relation between $S$ and $T$* is a subset of $S \times T$. We will not, however, in our class consider the cases in which $S$ and $T$ are different sets.

2. Given any $n \in \mathbb{Z}^+$, $\equiv_n$ **is** an equivalence relation on $\mathbb{Z}$. The proof of this is left as an exercise for the reader.

3. The relation $\mathscr{D}$ on $C^1$ discussed above (that $f \mathscr{D} g$ iff $f' = g'$) **is** an equivalence relation on $C^1$.

4. $\simeq$ **is** an equivalence relation on any set of groups. This follows from Theorem 3.5.

5. Define relation $\mathscr{R}$ on $\mathbb{Z}$ by $x \mathscr{R} y$ if and only if $xy \geq 0$. Is $\mathscr{R}$ an equivalence relation on $\mathbb{Z}$? Well, for every $x \in \mathbb{Z}$, $x^2 \geq 0$, so $\mathscr{R}$ is reflexive. Moreover, if $x, y \in \mathbb{Z}$ with $xy \geq 0$, then $yx \geq 0$; so $\mathscr{R}$ is symmetric. But $\mathscr{R}$ is **not** transitive: indeed, $3, 0, -4 \in \mathbb{Z}$ with $3(0) = 0 \geq 0$ and $0(-4) = 0 \geq 0$, so $3 \mathscr{R} 0$ and $0 \mathscr{R} -4$; but $3(-4) = -12 \ngeq 0$. So $\mathscr{R}$ isn't transitive, and hence is **not** an equivalence relation.

**Definition.** Given an equivalence relation $\sim$ on a set $S$, for each $x \in S$ we define the *equivalence class of $x$ under $\sim$* to be

$$[x] = \{y \in S : y \sim x\}.$$

These sets $[x]$ ($x \in S$) are called the *equivalence classes of $S$ under $\sim$*.

**Remark.** Note that, by reflexivity of $\sim$, $x \in [x]$ for every $x \in S$.

We have now the following Very Important Lemma:

**Lemma 7.4.** *Let $\sim$ be an equivalence relation on set $S$. Then for $x, y \in S$, the following are equivalent:*

*(i) $y \in [x]$;*
*(ii) $[x] = [y]$;*
*(iii) $x \in [y]$.*

*Proof.* For (i) $\Leftrightarrow$ (ii): Let $x, y \in S$. If $y \in [x]$, then $y \sim x$, so for every $z \in [y]$ (that is, for every $z$ in $S$ with $z \sim y$), we have, by transitivity, $z \sim x$, so $z \in [x]$. On the other hand, by the symmetry of $\sim$ we have $x \sim y$; so for every $z \in [x]$, we have, again by transitivity, that $z \in [y]$. Thus, $[x] = [y]$. Conversely, if $[x] = [y]$, then since $y \in [y] = [x]$.

The proof of (ii) $\Leftrightarrow$ (iii) is nearly identical. □

**Remark and definition..** In many cases there are many distinct elements $x, y \in S$ with $[x] = [y]$; thus, there are usually many different ways we could denote a particular equivalence class of $S$ under $\sim$. Element $y \in S$ is called a *representative* of class $X$ if $y \in X$.

**Example 7.5.**

1. Consider the equivalence relation $\equiv_2$ on $\mathbb{Z}$. Under this relation, $[0] = \{0, \pm 2, \pm 4, \ldots\}$ and $[1] = \{\ldots, -3, -1, 1, 3, \ldots\}$; in fact, if we let $E$ be the set of all even integers and $O$ the set of all odd integers, then for $x \in \mathbb{Z}$, $[x] = E$ if $x$ is even and $O$ if $x$ is odd. Thus, the set of all equivalence classes of $\mathbb{Z}$ under $\equiv_2$ is the 2-element set $\{E, O\}$: every even integer is a representative of $E$, while every odd integer is a representative of $O$.

2. For $f \in C^1$, the equivalence class of $f$ under $\mathscr{D}$ (defined above) is the set of all functions in $C^1$ of the form $g(x) = f(x) + c$, where $c \in \mathbb{R}$.

3. Let $A = \{a, b, c\}$, and define $\sim$ on the power set $P(A)$ of $A$ by $X \sim Y$ if and only if $|X| = |Y|$. It is straightforward to show that $\sim$ is an equivalence relation on $P(A)$, under which $P(A)$ has exactly 4 distinct equivalence classes:

$$[\emptyset] = \{\emptyset\},$$

$$[\{a\}] = [\{b\}] = [\{c\}] = \{\{a\}, \{b\}, \{c\}\},$$

$$[\{a, b\}] = [\{a, c\}] = [\{b, c\}] = \{\{a, b\}, \{a, c\}, \{b, c\}\}, \text{ and}$$

$$[A] = \{A\}.$$

Notice that the complete set $\{E, O\}$ of distinct equivalence classes of $\mathbb{Z}$ under $\equiv_n$ is a partition of $\mathbb{Z}$, and the complete set $\{[\emptyset], [\{a\}], [\{a, b\}], [A]\}$ of distinct equivalence classes of $P(A)$ under $\sim$ is a partition of $P(A)$. This is not a coincidence! It turns out that equivalence relations and partitions go hand in hand.

**Theorem 7.6.** *Let $S$ be a set. Then:*

*(i) If $\sim$ is an equivalence relation on $S$, then the set of all equivalence classes of $S$ under $\sim$ is a partition of $S$; and*

*(ii) If $P$ is a partition of $S$, then the relation on $S$ defined by*

$$x \sim y \text{ if and only } x \text{ is in the same cell of } P \text{ as } y$$

*is an equivalence relation on $S$.*

*Notice that in each case, the cells of the partition are the equivalence classes of the set under the corresponding equivalence relation.*

*Proof.* For (i): Let $\sim$ be an equivalence relation on $S$. Clearly, the equivalence classes of $S$ under $\sim$ are nonempty sets whose union is $S$. Thus, it suffices to show $X \cap Y = \emptyset$ for each pair of equivalence classes $X \neq Y$ of $S$ under $\sim$. Let $X, Y$ be equivalence classes of $S$ under $\sim$ that are NOT disjoint. Then there exists an element $z \in X \cap Y$. Then by Lemma 7.4, $[z] = X$ and $[z] = Y$; so $X = Y$. Thus, if $X \neq Y$, then $X \cap Y = \emptyset$.

For (ii), it is straightforward (almost silly!) to prove that $\sim$ is reflexive, symmetric, and transitive. □

**Example 7.7.**

1. For $n \in \mathbb{Z}^+$, the set of the equivalence classes of $\mathbb{Z}$ under $\equiv_n$ is the partition $\{[0], [1], \ldots, [n-1]\}$ of $\mathbb{Z}$. (The partition $\{E, O\}$ of $\mathbb{Z}$ discussed above is this partition when $n = 2$.)

## 7.2 Introduction to cosets and normal subgroups

Throughout this section, let $G$ be a group with subgroup $H$ and consider two particular relations on $G$:

$$\sim_L \text{ defined by } a \sim_L b \text{ if and only if } a^{-1}b \in H$$

and

$$\sim_R \text{ defined by } a \sim_R b \text{ if and only if } ab^{-1} \in H.$$

**Theorem 7.8.** *$\sim_L$ and $\sim_R$ are equivalence relations on $G$.*

*Proof.* First, let $a \in G$. Then $a^{-1}a = e \in H$, so $a \sim_L a$. Thus, $\sim_L$ is reflexive.

Next, let $a, b \in G$ with $a \sim_L b$. Then $a^{-1}b \in H$, so, since $H$ is a subgroup of $G$, $(a^{-1}b)^{-1} \in H$. But $(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$; thus, $b \sim_L a$, and so $\sim_L$ is symmetric.

Finally, let $a, b, c \in G$ with $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b$ and $b^{-1}c$ are in $H$. Since $H$ is a subgroup of $G$, we must then have $(a^{-1}b)(b^{-1}c) \in H$; but $(a^{-1}b)(b^{-1}c)$ equals $a^{-1}c$. Thus, $a \sim_L c$, and so $\sim_L$ is transitive.

Thus, $\sim_L$ is an equivalence relation on $G$. The proof that $\sim_R$ is an equivalence relation is left as an exercise for the reader. □

Now, as equivalence relations, each of $\sim_L$ and $\sim_R$ gives rise to a partition of $G$. What are the cells of those partitions?

**Definition.** Given $a \in G$, we define

$$aH = \{ah : h \in H\}$$

and

$$Ha = \{ha : h \in H\}.$$

We call $aH$ and $Ha$, respectively, the *left* and *right cosets of $H$ containing $a$*.

**Theorem 7.9.** *Let $a \in G$. Then under $\sim_L$, $[a] = aH$ while under $\sim_R$, $[a] = Ha$.*

*Proof.* Let $b \in G$. Then $b \sim_L a \Leftrightarrow a \sim_L b \Leftrightarrow a^{-1}b \in H \Leftrightarrow a^{-1}b = h$ for some $h \in H \Leftrightarrow b = ah$ for some $h \in H \Leftrightarrow b \in aH$. So under $\sim_L$ we have $[a] = aH$. Similarly, under $\sim_R$ we have $[a] = Ha$. □

We next summarize some facts about the left and right cosets of a subgroup $H$ of a group $G$:

**Theorem 7.10.** *Let $G$ be a group with $H \leq G$ and $a, b \in G$.*

1. *The left [right] cosets of $H$ in $G$ partition $G$.*
2. $$b \in aH \Leftrightarrow aH = bH \Leftrightarrow a \in bH$$
   *and*
   $$b \in Ha \Leftrightarrow Ha = Hb \Leftrightarrow a \in Hb.$$
   *In particular, $a \in H \Leftrightarrow aH = H \Leftrightarrow Ha = H$.*
3. *$H$ is the only left or right coset of $H$ that is a subgroup of $G$.*
4. *$|aH| = |H| = |Ha|$.*

*Proof.* Statements 1 and 2 hold because the left and right cosets of $H$ in $G$ are equivalence classes. Statement 3 holds because no left or right coset of $H$ other than $H$ itself can contain $e$, since the left [right] cosets of $H$ are mutually disjoint. For Statement 4: Define $f : H \to aH$ by $f(h) = ah$. It is straightforward to show that $f$ is a bijection, so $|H| = |aH|$. Similarly, $|Ha| = |H|$. □

**Remark.** We can use Statements 2 and 3, above, to save some time when computing left and right cosets of a subgroup of a group.

**Example 7.11.** Find the left and right cosets of $H = \langle(12)\rangle$ in $S_3$.

| $a$ | $aH$ | $Ha$ |
|---|---|---|
| $e$ | $H$ | $H$ |
| $(12)$ | $H$ | $H$ |
| $(13)$ | $\{(13)e, (13)(12)\} = \{(13), (123)\}$ | $\{e(13), (12)(13)\} = \{(13), (132)\}$ |
| $(23)$ | $\{(23)e, (23)(12)\} = \{(23), (132)\}$ | $\{e(23), (12)(23)\} = \{(23), (123)\}$ |
| $(123)$ | $\{(13), (123)\}$ (since $(123) \in (13)H$) | $\{(23), (123)\}$ (since $(123) \in H(23)$) |
| $(132)$ | $\{(23), (132)\}$ (since $(132) \in (23)H$) | $\{(13), (132)\}$ (since $(132) \in H(13)$) |

Thus, $\sim_L$ partitions $S_3$ into $\{H, \{(13), (123)\}, \{(23), (132)\}\}$ and $\sim_R$ partitions $S_3$ into $\{H, \{(13), (132)\}, \{(23), (123)\}\}$.

**Example 7.12.** Find the left and right cosets of $H = \langle f\rangle$ in $D_4$.
This example is left as an exercise for the reader.

We now draw attention to some very important facts:

**WARNING**

For $a, b \in G$:

1. In general, $aH \neq Ha$!
2. $aH = bH$ does not necessarily imply $a = b$ or that there exists an $h \in H$ with $ah = bh$; similarly, $Ha = Hb$ does not necessarily imply $a = b$ or that there exists an $h \in H$ with $ha = hb$.

**Example 7.13.** We saw above that in $S_3$ with $H = \langle(12)\rangle$,

$$(13)H = \{(13), (123)\} \neq \{(13), (132)\} = H(13).$$

Also, $(13)H = (123)H$ but $(13)e \neq (123)e$ and $(13)(12) \neq (123)(12)$.

It turns out that subgroups $H$ for which $aH = Ha$ for all $a \in G$ will be very important to us.

**Definition and notation.** We say that subgroup $H$ of $G$ is *normal* in $G$ if $aH = Ha$ for all $a \in G$. We denote that fact that $H$ is normal in $G$ by writing $H \trianglelefteq G$.

**Remarks.**

1. If $H$ is normal in $G$, we may refer to the left and right cosets of $G$ as simply *cosets*.

2. Of course, if $G$ is abelian, every subgroup of $G$ is normal in $G$. But there can also be normal subgroups of nonabelian groups: for instance, the trivial and improper subgroups of every group are normal in that group.

**Example 7.14.** Find the cosets of $5\mathbb{Z}$ in $\mathbb{Z}$.

Notice that in additive notation, the statement "$a^{-1}b \in H$" becomes $-a + b \in H$. So for $a, b \in \mathbb{Z}$, $a \sim_L b$ if and only if $-a + b \in 5\mathbb{Z}$; that is, if and only if 5 divides $b - a$. In other words, $a \sim_L b$ if and only if $a \equiv_5 b$. So in this case, $\sim_L$ is just congruence modulo 5. Thus, the cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ are

$$\begin{aligned} 5\mathbb{Z} &= \{\ldots, -5, 0, 5, \ldots\} \\ 1 + 5\mathbb{Z} &= \{\ldots, -4, 1, 6, \ldots\}, \\ 2 + 5\mathbb{Z} &= \{\ldots, -3, 2, 7, \ldots\}, \\ 3 + 5\mathbb{Z} &= \{\ldots, -2, 3, 8, \ldots\}, \\ 4 + 5\mathbb{Z} &= \{\ldots, -1, 4, 9, \ldots\}. \end{aligned}$$

Do you see how this example would generalize for $n\mathbb{Z}$ ($n \in \mathbb{Z}^+$) in $\mathbb{Z}$?

**Example 7.15.** Find the cosets of $H = \langle 12 \rangle$ in $4\mathbb{Z}$.

They are

$$\begin{aligned} H &= \{\ldots, -12, 0, 12 \ldots\}, \\ 4 + H &= \{\ldots, -8, 4, 16, \ldots\}, \\ 8 + H &= \{\ldots, -4, 8, 20, \ldots\}. \end{aligned}$$

**Example 7.16.** Find the cosets of $H = \langle 4 \rangle$ in $\mathbb{Z}_{12}$.

They are

$$\begin{aligned} H &= \{0, 4, 8\}, \\ 1 + H &= \{1, 5, 9\}, \\ 2 + H &= \{2, 6, 10\} \\ 3 + H &= \{3, 7, 11\}. \end{aligned}$$

We now consider the set of all left cosets of a subgroup of a group. (Note: There are analogous versions of what follows using right cosets, but we relegate any discussions of that to footnotes.)

**Notation and terminology.** We let $G/H$ denote the set of all left cosets of subgroup $H$ in $G$. We read $G/H$ as "$G$ mod $H$." [3]

## 7.3 The index of a subgroup and Lagrange's Theorem

**Definition.** We define the *index of $H$ in $G$*, denoted $(G : H)$, to be the cardinality of $G/H$. [4]

Note that if $G$ is finite then $(G : H)$ must be finite; however, we see below that if $G$ is infinite then $(G : H)$ could be finite or infinite.

[3] We denote the set of all right cosets of subgroup $H$ in $G$ by $H\backslash G$.

[4] Even though we need not have $aH = Ha$ for all $a \in G$, we do always have $|G/H| = |H\backslash G|$.

**Example 7.17.** If $(\mathbb{R} : \mathbb{Z})$ were finite, then we'd be able to write $\mathbb{R}$ as a finite union of countable sets, implying that $\mathbb{R}$ is countable—which it isn't. Thus, $(\mathbb{R} : \mathbb{Z}) = \infty$.

**Example 7.18.** Since $\langle i \rangle = \{i, -1, -i, 1\}$ is a finite subgroup of $C^*$ and $C^*$ is infinite, we must have that $(C^* : \langle i \rangle)$ is infinite. However, $(C^* : C^*) = 1$.

**Example 7.19.** Referring to our previous examples, we have:

$$\begin{aligned} & (S_3 : \langle (12) \rangle) = 3, \\ & (D_4 : \langle f \rangle) = 4, \\ & (\mathbb{Z} : 5\mathbb{Z}) = 5, \\ & (4\mathbb{Z} : 12\mathbb{Z}) = 3, \\ \text{and} \quad & (\mathbb{Z}_{12} : \langle 4 \rangle) = 4. \end{aligned}$$

Letting $d, n \in \mathbb{Z}^+$ with $d$ dividing $n$, we can generalize the some of the above examples, obtaining:

$$\begin{aligned} & (d\mathbb{Z} : n\mathbb{Z}) = n/d \quad \text{(special case: } (\mathbb{Z} : n\mathbb{Z}) = n) \\ \text{and} \quad & (\mathbb{Z}_n : \langle d \rangle) = d. \end{aligned}$$

Notice that in the cases in which $G$ is finite, $(G : H) = |G|/|H|$. This makes sense, since the left cosets of $H$ in $G$ partition $G$, and each left coset has cardinality $|H|$.

Since the left cosets of a subgroup $H$ of a group $G$ partition $G$ and all have the same cardinality, we have the following two theorems. The first is known as *Lagrange's Theorem*.[5]

**Theorem 7.20.** ***(Lagrange's Theorem)*** *If $G$ is a finite group and $H \leq G$, then $|H|$ divides $|G|$.*

**Theorem 7.21.** *If $G$ is a finite group and $H \leq G$, then $(G : H) = |G|/|H|$.*

**Remark.** The converse of Lagrange's Theorem does not hold. Indeed $A_4$ is a group of order 12 which contains no subgroup of order 6 even though 6 divides $|A_4| = 12$.

We end this chapter with two corollaries to Lagrange's Theorem.

**Corollary 7.22.** *Let $G$ be a finite group and let $a \in G$. Then $a^{|G|} = e_G$.*

*Proof.* Let $d = o(a)$. By Lagrange's Theorem, $d$ divides $|G|$, so there exists $k \in \mathbb{Z}$ with $|G| = dk$. Then $a^{|G|} = a^{dk} = (a^d)^k = (e_G)^k = e_G$. □

**Corollary 7.23.** *Let $G$ be a group of prime order. Then $G$ is cyclic. It follows that for every prime $p$, there exists a unique group of order $p$, up to isomorphism.*

*Proof.* This proof is left as an exercise for the reader. □

[5] Named after the French mathematician Joseph-Louis Lagrange.

## 7.4 Exercises

### Exercise 7.1

How many distinct partitions of the set $S = \{a, b, c, d\}$ are there? You do not need to list them. (Yes, you can find this answer online. But I recommend doing the work yourself for practice working with partitions!)

### Exercise 7.2

(a) Let $n \in \mathbb{Z}^+$. Prove that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

(b) The cells of the induced partition of $\mathbb{Z}$ are called the *residue classes* (or *congruence classes*) *of* $\mathbb{Z}$ *modulo* $n$. Using set notation of the form $\{\ldots, \#, \#, \#, \ldots\}$ for each class, write down the residue classes of $\mathbb{Z}$ modulo 4.

### Exercise 7.3

Let $G$ be a group with subgroup $H$. Prove that $\sim_R$ is an equivalence relation on $G$.

### Exercise 7.4

For each subgroup $H$ of group $G$, (i) find the left and the right cosets of $H$ in $G$, (ii) decide whether or not $H$ is normal in $G$, and (iii) find $(G : H)$.

| Write all permutations using disjoint cycle notation, and write all dihedral group elements in standard form. |
|---|

(a) $H = 6\mathbb{Z}$ in $G = 2\mathbb{Z}$

(b) $H = \langle 4 \rangle$ in $\mathbb{Z}_{20}$

(c) $H = \langle (23) \rangle$ in $G = S_3$

(d) $H = \langle r \rangle$ in $G = D_4$

(e) $H = \langle f \rangle$ in $G = D_4$

### Exercise 7.5

For each of the following, give an example of a group $G$ with a subgroup $H$ that matches the given conditions. If no such example exists, prove that.

(a) A group $G$ with subgroup $H$ such that $|G/H| = 1$.

(b) A finite group $G$ with subgroup $H$ such that $|G/H| = |G|$.

(c) An abelian group $G$ of order 8 containing a non-normal subgroup $H$ of order 2.

(d) A group $G$ of order 8 containing a normal subgroup of order 2.

(e) A nonabelian group $G$ of order 8 containing a normal subgroup of index 2.

(f) A group $G$ of order 8 containing a subgroup of order 3.

(g) An infinite group $G$ containing a subgroup $H$ of finite index.

(h) An infinite group $G$ containing a finite nontrivial subgroup $H$.

## Exercise 7.6

True/False. For each of the following, write T if the statement is true; otherwise, write F. You do NOT need to provide explanations or show work for this problem.Throughout, let $G$ be a group with subgroup $H$ and elements $a, b \in G$.

(a) If $a \in bH$ then $aH$ must equal $bH$.

(b) $aH$ must equal $Ha$.

(c) If $aH = bH$ then $Ha$ must equal $Hb$.

(d) If $a \in H$ then $aH$ must equal $Ha$.

(e) $H$ must be normal in $G$ if there exists $a \in G$ such that $aH = Ha$.

(f) If $aH = bH$ then $ah = bh$ for every $h \in H$.

(g) $|G/H|$ must be less than $|G|$.

(h) $(G : H)$ must be less than or equal to $|G|$.

## Exercise 7.7

Find the indices of:

(a) $H = \langle (15)(24) \rangle$ in $S_5$

(b) $K = \langle (1453)(25) \rangle$ in $S_5$

(c) $L = \langle (2354)(34) \rangle$ in $S_6$

(d) $A_n$ in $S_n$

## Exercise 7.8

Let $G$ be a group of order $pq$, where $p$ and $q$ are prime, and let $H$ be a proper subgroup of $G$. Prove that $H$ is cyclic.

## Exercise 7.9

# Chapter 8

# Factor Groups

## 8.1 Motivation

We mentioned previously that given a subgroup $H$ of $G$, we'd like to use $H$ to get at some understanding of $G$'s entire structure. Recall that we've defined $G/H$ to be the set of all left cosets of $H$ in $G$. What we'd like to do now is equip $G/H$ with some operation under which $G/H$ is a group! The natural way to do this would be to define multiplication on $G/H$ by

$$(aH)(bH) = abH \text{ for all } a, b \in G.$$

Ok, so let's do that! But wait: we're defining this operation by referring to coset representatives, so we'd better make sure our operation is well defined. Only it sadly turns out that in general this operation is <u>not</u> well defined. For example:

**Example 8.1.** Let $H = \langle (12) \rangle$ in $S_3$, and let $a = (13)$ and $b = (132)$. Let $x = aH$ and $y = bH$ in $S_3/H$. Then using the above-defined operation on $G/H$ we'd have

$$xy = (aH)(bH) = abH = (13)(132)H = (23)H.$$

But also $x = (123)H$ and $y = (23)H$, so we'd also have

$$xy = ((123)H)((23)H)) = (123)(23)H = (12)H = H \neq (23)H.$$

So this operation isn't well defined.

The question for us now becomes: what conditions must hold for $H$ in $G$ in order for operation

$$(aH)(bH) = abH$$

on $G/H$ to be well defined? It turns out that this operation is well defined exactly when $H$ is normal in $G$! We state this in the following theorem:

**Theorem 8.2.** *Let $H \leq G$. Then the operation*

$$(aH)(bH) = abH$$

*on $G/H$ is well defined if and only if $H \trianglelefteq G$.*

*Proof.* ($\Leftarrow$) Let $a_1, a_2, b_1, b_2 \in G$ with $a_1H = a_2H$ and $b_1H = b_2H$. We want to show that then $a_1b_1H = a_2b_2H$, that is, that $(a_2b_2)^{-1}a_1b_1 \in H$. Well, since $a_1H = a_2H$ we have $a_2^{-1}a_1 \in H$. So

$$(a_2b_2)^{-1}a_1b_1 = b_2^{-1}(a_2^{-1}a_1)b_1 \in b_2^{-1}Hb_1.$$

Next, since $H \trianglelefteq G$, we have $Hb_1 = b_1H$, so $b_2^{-1}Hb_1 = b_2^{-1}b_1H$; but since $b_1H = b_2H$, we have $b_2^{-1}b_1 \in H$, so $b_2^{-1}b_1H = H$. Thus, $(a_2b_2)^{-1}a_1b_1 \in H$, as desired.

($\Rightarrow$) Let $a \in G$. We want to show that $aH = Ha$. Well, first let $x \in aH$. Then

$$(xH)(a^{-1}H) = xa^{-1}H$$

and, since $xH = aH$,

$$(xH)(a^{-1}H) = (aH)(a^{-1}H) = aa^{-1}H = H.$$

Since our operation on $G/H$ is well defined, this means that $xa^{-1}H = H$, so $xa^{-1} \in H$; thus, $x \in Ha$. We conclude that $aH \subseteq Ha$. The proof that $Ha \subseteq aH$ is similar. □

**Definition.** When $H \trianglelefteq G$, the well defined operation $(aH)(bH) = abH$ on $G/H$ is called *left coset multiplication.*

It is clear that normal subgroups will be very important for us in studying group structures. We therefore spend some time looking at normal subgroups before returning to equipping $G/H$ with a group structure.

## 8.2 Focusing on normal subgroups

We first provide a theorem that will help us in identifying when a subgroup of a group is normal. First, we provide a definition.

**Definition.** Let $H$ be a subgroup of $G$ and $a, b$ in $G$. We define

$$aHb = \{ahb : h \in H\}.$$

**Theorem 8.3.** *Let $H$ be a subgroup of a group $G$. Then the following are equivalent:*

1. *$H$ is normal in $G$;*
2. *$aHa^{-1} = H$ for all $a \in G$;*
3. *$aHa^{-1} \subseteq H$ for all $a \in G$.*

*Proof.* The equivalence of Statements 1 and 2 is clear, as is the fact that Statement 2 implies Statement 3. So it suffices to show that Statement 3 implies Statement 2. Well, assume that $aHa^{-1} \subseteq H$ for all $a \in G$, and let $b \in G$. We want to show that $bHb^{-1} = H$. Since Statement 3 holds, we clearly have $bHb^{-1} \subseteq H$. But, again using Statement 3, we also have $b^{-1}Hb \subseteq H$; multiplying both sides of this equation on the left by $b$ and on the right by $b^{-1}$, we obtain $H \subseteq bHb^{-1}$. Hence, since $bHb^{-1} \subseteq H$ and $H \subseteq bHb^{-1}$, those two sets are equal. Thus, Statement 2 is proven. □

We now consider some examples and nonexamples of normal subgroups of groups.

**Example 8.4.**

1. As previously mentioned, the trivial and improper subgroups of any group $G$ are normal in $G$.

2. As previously mentioned, if group $G$ is abelian then each of its subgroups is normal in $G$.
3. Suppose $H \leq G$ has $(G : H) = 2$. Then $H \trianglelefteq G$. The proof of this is left as an exercise for the reader.
4. Example 7.11 shows that subgroup $H = \langle(12)\rangle$ isn't normal in $S_3$ (for example, $(13)H \neq H(13)$. But $\langle(123)\rangle$ must be normal in $S_3$ since $(S_3 : \langle(123)\rangle) = 6/3 = 2$.
5. $\langle r\rangle$ is normal in $D_n$ since $(D_n : \langle r\rangle) = 2$.
6. $\langle f\rangle$ isn't normal in $D_4$: for instance,
$$r\langle f\rangle r^{-1} = \{e, rfr^3\} = \{e, fr^3r^3\} = \{e, fr^2\} \not\subseteq \langle f\rangle.$$

We consider two other very significant examples.

**Definition, notation, and terminology.** Let $G$ be a group. We let
$$Z(G) = \{z \in G : az = za \text{ for all } a \in G\}.$$
$Z(G)$ is called the *center* of $G$.[1]

**Theorem 8.5.** *Let $G$ be a group. Then $Z(G)$ is a subgroup of $G$.*

*Proof.* Clearly, $e \in Z(G)$. Next, let $z, w \in Z(G)$. Then for all $a \in G$,
$$a(zw) = (az)w = (za)w = z(aw) = z(wa) = (zw)a,$$
so $zw \in Z(G)$. Finally, $az = za$ so, multiplying both sides on the left and right by $z^{-1}$, we have $z^{-1}a = az^{-1}$; thus, $z^{-1} \in Z(G)$. Hence, $Z(G) \leq G$. □

**Theorem 8.6.** *Let $G$ be a group and let $H$ be a subgroup of $G$ with $H \subseteq Z(G)$. Then $H \trianglelefteq G$. In particular, $Z(G)$ is itself a normal subgroup of $G$.*

*Proof.* Let $a \in G$. Then since every element of $Z(G)$ commutes with every element of $G$, every element of $H$ commutes with every element of $G$; so we must have $aH = Ha$. Thus, $H \trianglelefteq G$. □

The next definition is profoundly important for us.

**Definition and notation.** Let $G$ and $G'$ be groups and let $\phi$ be a homomorphism from $G$ to $G'$. Letting $e'$ be the identity element of $G'$, we define the *kernel of* $\phi$, $\operatorname{Ker}\phi$, by
$$\operatorname{Ker}\phi = \{k \in G : \phi(k) = e'\}.$$

**Example 8.7.** Let $G$ and $G'$ be groups and let $\phi$ be a homomorphism from $G$ to $G'$. Then $\operatorname{Ker}\phi$ is a normal subgroup of $G$.

*Proof.* Let $K = \operatorname{Ker}\phi$. We first show that $K$ is a subgroup of $G$. Clearly, the identity element of $G$ is in $K$, so $K \neq \emptyset$. Next, let $k, m \in K$. Then, letting $e'$ denote the identity element of $G'$, we have
$$\phi(km^{-1}) = \phi(k)\phi(m)^{-1} = e'(e')^{-1} = e',$$
so $km^{-1} \in K$. Thus, by the Two-Step Subgroup Test, we have that $K$ is a subgroup of $G$.

Next, let $k \in K$ and let $a \in G$. Then
$$\phi(aka^{-1}) = \phi(a)\phi(k)\phi(a)^{-1} = \phi(a)e'\phi(a)^{-1} = \phi(a)\phi(a)^{-1} = e'.$$
So $aka^{-1} \in K$. Thus, $K \trianglelefteq G$. □

[1] The center of a group was originally introduced in the Exercises of Chapter 2. The Z stands for "zentrum," the German word for "center."

One slick way, therefore, of showing that a particular set is a normal subgroup of a group $G$ is by showing it's the kernel of a homomorphism from $G$ to another group.

**Example 8.8.** Let $n \in \mathbb{Z}^+$. Here is a rather elegant proof of the fact that $SL(n,\mathbb{R})$ is a normal subgroup of $GL(n,\mathbb{R})$: Define $\phi : GL(n,\mathbb{R}) \to \mathbb{R}^*$ by $\phi(A) = \det A$. Clearly, $\phi$ is a homomorphism, and since the identity element of $\mathbb{R}^*$ is 1,

$$\operatorname{Ker}\phi = \{A \in GL(n,\mathbb{R}) \,:\, \det A = 1\} = SL(n,\mathbb{R}).$$

So $SL(n,\mathbb{R}) \trianglelefteq GL(n,\mathbb{R})$.

## 8.3 Factor groups

We now return to the notion of equipping $G/H$, when $H \trianglelefteq G$, with a group structure. We have already proven that left coset multiplication on $G/H$ is well defined when $H \trianglelefteq G$; it turns out that given this, it is very easy to prove that $G/H$ under this operation is a group.

Before we prove this, we introduce a change in our notation: We initiate the convention of frequently using $N$, rather than $H$, to denote a subgroup of a group $G$ when we know that that subgroup is normal in $G$.

**Theorem 8.9.** *Let $G$ be a group with identity element $e$, and let $N \trianglelefteq G$. Then $G/N$ is a group under left coset multiplication (that is, under the operation $(aN)(bN) = abN$ for all $a, b \in G$), and $|G/N| = (G : N)$ (in particular, if $|G| < \infty$, then $|G/N| = |G|/|N|$).*

*Proof.* We already know that since $N \trianglelefteq G$, left coset multiplication on $G/N$ is well defined; further, it is clear that $G/N$ is closed under this operation.

Associativity of this operation on $G/N$ follows from the associativity of $G$'s operation: indeed, if $aN$, $bN$, $cN \in G/N$, then

$$((aN)(bN))(cN) = (abN)(cN) = (ab)cN = a(bc)N = (aN)(bcN) = (aN)((bN)(cN)).$$

Next, $N = eN \in G/N$ acts as an identity element since for all $a \in G$,

$$(aN)(N) = aeN = aN \text{ and } N(aN) = eaN = aN.$$

Finally, let $aN \in G/N$. Then $a^{-1}N \in G/N$ with $(aN)(a^{-1}N) = aa^{-1}N = N$ and $(a^{-1}N)(aN) = a^{-1}aN = N$.

So $G/N$ is a group under left coset multiplication. Since $(G : N)$ is, by definition, the cardinality of $G/N$, we're done. □

**Definition.** When $G$ is a group and $N \trianglelefteq G$, the above group ($G/N$ under left coset multiplication) is called a *factor group* or *quotient group*.

**Example 8.10.** Let $G = \mathbb{Z}$ and $N = 3\mathbb{Z}$. Then $N$ is normal in $G$, since $G$ is abelian, so the set $G/N = \{N, 1+N, 2+N\}$ is a group under left coset multiplication. Noting that $N = 0 + N$, it is straightforward to see that $G/N$ (that is, $\mathbb{Z}/3\mathbb{Z}$) has the following group table:

| $+$ | $0+N$ | $1+N$ | $2+N$ |
|---|---|---|---|
| $0+N$ | $0+N$ | $1+N$ | $2+N$ |
| $1+N$ | $1+N$ | $2+N$ | $0+N$ |
| $2+N$ | $2+N$ | $0+N$ | $1+N$ |

Clearly, if we ignore all the $+N's$ after the 0's, 1's, and $2'$ in the above table, and consider $+$ to be addition mod 3, rather than left coset addition in $\mathbb{Z}/3\mathbb{Z}$, we obtain the group table for $\mathbb{Z}_3$:

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Thus, we see that $\mathbb{Z}/3\mathbb{Z}$ is isomorphic to $\mathbb{Z}_3$. This is not a coincidence! In fact, we have the following:

**Theorem 8.11.** *Let $n, d \in \mathbb{Z}^+$ with $d$ dividing $n$. Then we have:*

1. *$n\mathbb{Z} \trianglelefteq d\mathbb{Z}$ and $\langle d \rangle \trianglelefteq \mathbb{Z}_n$;*
2. *$d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_{n/d}$ (special case: $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$); and*
3. *$Z_n/\langle d \rangle \simeq \mathbb{Z}_d$.*

*Proof.*

1. Since $d$ is a positive divisor of $n$, $n\mathbb{Z}$ and $\langle d \rangle$ are clearly subgroups of, respectively, $d\mathbb{Z}$ and $\mathbb{Z}_n$. Moreover, since $d\mathbb{Z}$ and $\mathbb{Z}_n$ are abelian, all of their subgroups are normal.
2. This follows from the facts that $d\mathbb{Z}/n\mathbb{Z} = \langle d + n\mathbb{Z} \rangle$, hence is cyclic, and that $|d\mathbb{Z}/n\mathbb{Z}| = (d\mathbb{Z} : n\mathbb{Z}) = n/d$ (see Example 7.19). (Unpacking the statement that $d\mathbb{Z}/n\mathbb{Z} = \langle d + n\mathbb{Z} \rangle$: Notice that $d\mathbb{Z} = \langle d \rangle$, so every element of $d\mathbb{Z}$ is of the form $kd$ for some integer $k$. Thus, every element of $d\mathbb{Z}/n\mathbb{Z}$ is of the form $kd + n\mathbb{Z}$ for some integer $k$. But for each $k \in \mathbb{Z}$, using the definition of left coset multiplication we have that $kd + n\mathbb{Z} = k(d + n\mathbb{Z})$. So $d\mathbb{Z}/n\mathbb{Z} = \langle d + n\mathbb{Z} \rangle$.)
3. Similarly, since $\mathbb{Z}_n = \langle 1 \rangle$, $\mathbb{Z}_n/\langle d \rangle = \langle 1 + \langle d \rangle \rangle$, so is cyclic. Since $(\mathbb{Z}_n : \langle d \rangle) = d$ (again, see Example 7.19), $\mathbb{Z}_n/\langle d \rangle$ is isomorphic to $\mathbb{Z}_d$, as desired. □

**Example 8.12.** Let $N = \langle (123) \rangle \leq S_3$. Since $(S_3 : N) = 2$, $N$ must be normal in $S_3$, so $S_3/N$ is a group under left coset multiplication. Since $|S_3/N| = 2$, $S_3/N$ must be isomomorphic to $\mathbb{Z}_2$.

In the above examples, we were able to identify $G/N$ up to isomorphism relatively easily because we could determine that $G/N$ was cyclic. In general, however, it can be quite difficult to identify the group structure of a factor group. We explore some powerful tools we can use in this identification in the next section, but first we note a couple properties of $G$ that are "inherited" by any of its factor groups.

**Theorem 8.13.** *Let $G$ be a group and $N \trianglelefteq G$. Then:*

1. *If $G$ is finite, then $G/N$ is finite.*
2. *If $G$ is abelian, then $G/N$ is abelian; and*
3. *If $G$ is cyclic, then $G/N$ is cyclic.*

*Proof.*

1. Clearly this holds, since in this case $|G/N| = |G|/|N|$.
2. The proof of this statement is left as an exercise for the reader.
3. Let $G$ be cyclic. Then there exists $a \in G$ with $G = \langle a \rangle$. We claim $G/N = \langle aN \rangle$. Indeed:
$$\langle aN \rangle = \{(aN)^i : i \in \mathbb{Z}\} = \{a^i N : i \in \mathbb{Z}\}.$$
But every element of $G$ is an integer power of $a$, so this set equals $\{xN : x \in G\}$, that is, it equals $G/N$. □

**WARNING**

However, $G$ can be nonabelian [noncyclic, nonfinite] and yet have a normal subgroup $N$ such that $G/N$ is abelian [cyclic, finite]. (See the examples below.) Intuitively, the idea is that modding out a group by a normal subgroup can introduce abelianness or cyclicity, or finiteness, but not remove one of those characteristics.

**Example 8.14.** $S_3$ is nonabelian (and therefore of course noncyclic), but we saw above that $N = \langle (123) \rangle$ is a normal subgroup of $S_3$ with $S_3/N \simeq \mathbb{Z}_2$, a cyclic (and therefore of course abelian) group.

**Example 8.15.** $\mathbb{Z}$ is an infinite group, but it has finite factor group $\mathbb{Z}/2\mathbb{Z}$.

What do the (normal) subgroups of a factor group $G/N$ look like? Well, they come from the (normal) subgroups of $G$! We have the following theorem, whose proof is tedious but straightforward.

**Theorem 8.16.** ***(Correspondence Theorem)*** *Let $G$ be a group, and let $K \trianglelefteq G$. Then the subgroups of $G/K$ are exactly those of the form $H/K$, where $H \leq G$ with $K \subseteq H$. Moreover, the normal subgroups of $G/K$ are exactly those of the form $N/K$, where $N \trianglelefteq G$ with $K \subseteq N$.*

**Example 8.17.** Let $N = 18\mathbb{Z}$ in $\mathbb{Z}$. Since the subgroups of $\mathbb{Z}$ containing $N$ are the sets $d\mathbb{Z}$ where $d$ is a positive divisor of 18, the subgroups of $\mathbb{Z}/N$ are the sets $d\mathbb{Z}/N$, where, again, $d$ is a positive divisor of 18.

We end this chapter by noting that given any group $G$ and factor group $G/N$ of $G$, there is a homomorphism from $G$ to $G/N$ that is onto. Before we define this homomorphism, we provide some more terminology.

**Definitions.** Let $\phi : G \to G'$ be a homomorphism of groups. Then $\phi$ is can be called an *epimorphism* if $\phi$ is onto, and a *monomorphism* if $\phi$ is one-to-one. (Of course, we already know that an epimorphism that is also a monomorphism is called an "isomorphism.")

We now present the following theorem, whose straightforward proof is left to the reader.

**Theorem 8.18.** *Let $G$ be a group and let $N \trianglelefteq G$. Then the map $\Psi : G \to G/N$ defined by $\Psi(g) = gN$ is an epimorphism.*

**Definition.** We call this map $\Psi$ the *canonical epimorphism from $G$ to $G/N$*.

Notice that given $N \trianglelefteq G$, the kernel of the canonical epimorphism from $G$ to $G/N$ is $N$. Thus, putting this fact together with the fact that every kernel of a homomorphism is a normal subgroup of the homomorphism's domain, we have the following:

**Theorem 8.19.** *Let $G$ be a group and $N$ a subset of $G$. Then $N$ is a normal subgroup of $G$ if and only if $N$ is the kernel of a homomorphism from $G$ to some group $G'$.*

## 8.4 Exercises

### Exercise 8.1

Show that if $H$ is a subgroup of index 2 in a group $G$, then $H$ is normal in $G$.

### Exercise 8.2

Let $H = \{A \in GL(n, \mathbb{R}) : \det A = \pm 1\}$. Prove that $H \trianglelefteq GL(n, \mathbb{R})$.

### Exercise 8.3

Let $G = \mathbb{Z}_6 \times \mathbb{Z}_{14}$ and let $H = \langle 2 \rangle \times \langle 4 \rangle \leq G$. Since $G$ is abelian, $H \trianglelefteq G$. Find the order of the factor group $|G/H|$.

### Exercise 8.4

Consider the subgroup $\langle 18 \rangle$ of $\mathbb{Z}$.

(a) Explain how you know that $\mathbb{Z}/\langle 18 \rangle$ is a group under left coset multiplication.

(b) Find:

(i) $|\mathbb{Z}/\langle 18 \rangle|$.

(ii) $|4 + \langle 18 \rangle|$.

(iii) $o(4 + \langle 18 \rangle)$ in $\mathbb{Z}/\langle 18 \rangle$.

### Exercise 8.5

Let $G = 4\mathbb{Z} \times \mathbb{M}_2(\mathbb{R})$, $H = \langle 2 \rangle \times \langle I_2 \rangle \leq G$, and $K = \langle (23) \rangle \leq S_3$. Explain how you know that the set $G/H$ is a group under left coset multiplication, while the set $S_3/K$ is not.

### Exercise 8.6

Let $H = \langle r^2 \rangle \leq D_4$.

(a) Prove that $H \trianglelefteq D_4$. (Hint: Refer back to Section 6.5.)

(b) It follows that $D_4/H$ is a group under left coset multiplication.

(i) The distinct left cosets of $H$ in $D_4$ are $H$, $rH$, $fH$, and $frH$. Explicitly list the elements of each of these cosets of $H$.

(ii) Complete the group table for $D_4/H$, denoting each coset by $H$, $rH$, $fH$, or $frH$, as appropriate.

(iii) Use the group table for $D_4/H$ to identify a familiar group to which $D_4/H$ is isomorphic.

### Exercise 8.7

Let $G$ be an abelian group and let $N \trianglelefteq G$. Prove that $G/N$ is abelian.

### Exercise 8.8

Let $N$ be a normal subgroup of group $G$, with finite index $m$. Let $a \in G$. Prove that $a^m \in N$.

# Chapter 9

# The Isomorphism Theorems

Recall that our goal here is to use a subgroup of a group $G$ to study not just the structure of the subgroup, but the structure of $G$ outside of that subgroup (the ultimate goal being to get a feeling for the structure of $G$ as a whole). We've further seen that if we choose $N$ to be a normal subgroup of $G$, we can do this by studying both $N$ and the factor group $G/N$. Now, we've noticed that in some cases—in particular, when $G$ is cyclic–it is not too hard to identify the structure of a factor group of $G$. But what about when $G$ and $N$ are more complicated? For instance, we have seen that $SL(5,\mathbb{R})$ is a normal subgroup of $GL(5,\mathbb{R})$. What is the structure of $GL(5,\mathbb{R})/SL(5,\mathbb{R})$? That is not so easy to figure out by looking directly at left coset multiplication in the factor group.

## 9.1 The First Isomorphism Theorem

A very powerful theorem, called the First Isomorphism Theorem, lets us in many cases identify factor groups (up to isomorphism) in a very slick way. Kernels will play an extremely important role in this. We therefore first provide some theorems relating to kernels.

**Theorem 9.1.** *Let $G$ and $G'$ be groups, let $\phi$ be a homomorphism from $G$ to $G'$, and let $K = \operatorname{Ker}\phi$. Then for $a, b \in G$, $aK = bK$ if and only if $\phi(a) = \phi(b)$.*

*Proof.* Let $a, b \in G$. Then

$$\begin{aligned}\phi(a) = \phi(b) &\Leftrightarrow \phi(b)^{-1}\phi(a) = e_{G'}\\ &\Leftrightarrow \phi(b^{-1}a) = e_{G'}\\ &\Leftrightarrow b^{-1}a \in K\\ &\Leftrightarrow a \in bK\\ &\Leftrightarrow aK = bK,\end{aligned}$$

as desired. □

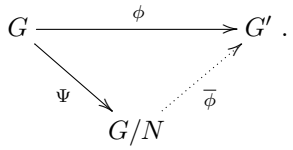
**Corollary 9.2.** *Let $\phi$ be a homomorphism from group $G$ to group $G'$. Then $\phi$ is one-to-one (hence a monomorphism) if and only if $\operatorname{Ker}\phi = \{e_G\}$.*

*Proof.* Clearly, if $\phi$ is one-to-one then $\operatorname{Ker}\phi = \{e_G\}$. Conversely, assume $\operatorname{Ker}\phi = \{e_G\}$. If $a, b \in G$ with $\phi(a) = \phi(b)$, then by the above theorem, $a\operatorname{Ker}\phi = b\operatorname{Ker}\phi$. But $a\operatorname{Ker}\phi = a\{e_G\} = \{a\}$ and $b\operatorname{Ker}\phi = b\{e_G\} = \{b\}$. Thus, $a = b$, and we see that $\phi$ is one-to-one. □

We now prove a theorem that provides the meat and potatoes of the First Isomorphism Theorem.

**Theorem 9.3.** ***(Factorization Theorem)*** *Let $G$ and $G'$ be groups, let $\phi$ be a homomorphism from $G$ to $G'$, let $K = \operatorname{Ker}\phi$, let $N$ be a normal subgroup of $G$ with $N \subseteq K$, and let $\Psi$ be the canonical epimorphism from $G$ to $G/N$. Then the map $\overline{\phi} : G/N \to G'$ defined by $\overline{\phi}(aN) = \phi(a)$ is a well defined homomorphism, with $\overline{\phi} \circ \Psi = \phi$.*

We can summarize this using the following picture:




*Proof.* We define $\overline{\phi} : G/N \to G'$, as indicated above, by $\overline{\phi}(aN) = \phi(a)$ for every $aN \in G/N$. Since $\overline{\phi}$ is defined using coset representatives, we must first show that $\overline{\phi}$ is well defined. So let $aN = bN \in G/N$. Then $\overline{\phi}(aN) = \phi(a)$ and $\overline{\phi}(bN) = \phi(b)$, so we must show that $\phi(a) = \phi(b)$. Since $aN = bN$ and $N \subseteq K$, we have that $aK = bK$ by Statement 6 of Theorem 7.10; thus $\phi(a) = \phi(b)$ (using Lemma 9.1). So $\overline{\phi}$ is well defined.

Next, we show that $\overline{\phi}$ is a homomorphism. Let $aN, bN \in G/N$. Then

$$\overline{\phi}((aN)(bN)) = \overline{\phi}(abN) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aN)\overline{\phi}(bN).$$

Finally, for every $a \in G$,

$$(\overline{\phi} \circ \Psi)(a) = \overline{\phi}(\Psi(a)) = \overline{\phi}(aN) = \phi(a);$$

so $\overline{\phi} \circ \Psi = \phi$, as desired. □

Note that the above theorem does <u>not</u> state that $\overline{\phi}$ is a monomorphism or an epimorphism. This is because in general it may be neither! We do have the following theorem:

**Theorem 9.4.** *Let $G$, $G'$, $\phi$, $N$, and $\overline{\phi}$ be as defined in the Factorization Theorem. Then*

1. *$\overline{\phi}$ is onto (an epimorphism) if and only if $\phi$ is onto (an epimorphism); and*
2. *$\overline{\phi}$ is one-to-one (a monomorphism) if and only if $N = \operatorname{Ker}\phi$.*

*Proof.*

1. This is clear, since $\overline{\phi}(G/N) = \phi(G)$.
2. By Corollary 9.2, $\overline{\phi}$ is one-to-one if and only if $\operatorname{Ker}\overline{\phi} = \{N\}$. But

$$\begin{aligned}\operatorname{Ker}\overline{\phi} &= \{aN \in G/N \,:\, \overline{\phi}(aN) = e_{G'}\} \\ &= \{aN \in G/N \,:\, \phi(a) = e_{G'}\} \\ &= \{aN \in G/N \,:\, a \in \operatorname{Ker}\phi\}.\end{aligned}$$

So $\operatorname{Ker}\overline{\phi} = \{N\}$ if and only if

$$\{aN \in G/N \,:\, a \in \operatorname{Ker}\phi\} = \{N\},$$

in other words if and only if $aN = N$ for all $a \in \operatorname{Ker}\phi$. But

$$\begin{aligned} & aN = N && \text{for all } a \in \operatorname{Ker}\phi \\ \Leftrightarrow\ & a \in N && \text{for all } a \in \operatorname{Ker}\phi \\ \Leftrightarrow\ & \operatorname{Ker}\phi \subseteq N \\ \Leftrightarrow\ & \operatorname{Ker}\phi = N, \end{aligned}$$

since we are given that $N \subseteq \operatorname{Ker}\phi$. Thus, $\overline{\phi}$ is one-to-one if and only if $N = \operatorname{Ker}\phi$, as desired. □

We are now ready to state the all-important First Isomorphism Theorem (which we have essentially already proven).

**Theorem 9.5.** ***(First Isomorphism Theorem)*** *Let $G$ and $G'$ be groups, with homomorphism $\phi : G \to G'$. Let $K = \operatorname{Ker}\phi$. Then $G/K \simeq \phi(G)$. In particular, if $\phi$ is onto, then $G/K \simeq G'$.*

*Proof.* This follows directly from the Factorization Theorem and Theorem 9.4. □

So to prove that a factor group $G/N$ is isomorphic to a group $G'$, it suffices to show there exists an epimorphism from $G$ to $G'$ that has $N$ as its kernel.

**Example 9.6.** Letting $n \in \mathbb{Z}^+$, let's identify a familiar group to which $GL(n,\mathbb{R})/SL(n,\mathbb{R})$ is isomorphic. As in Example 8.8, the map $\phi : GL(n,\mathbb{R}) \to \mathbb{R}^*$ defined by $\phi(A)$ is a homomorphism with kernel $SL(n,\mathbb{R})$. Moreover, *Phi* clearly maps onto $\mathbb{R}^*$: indeed, given $\lambda \in \mathbb{R}^*$, the diagonal matrix having $\lambda$ in the uppermost left position and 1's elsewhere down the diagonal gets sent to $\lambda$ by $\phi$. So by the First Isomorphism Theorem, we have $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \simeq \mathbb{R}^*$.

**Example 9.7.** Let $G = S_3 \times \mathbb{Z}_{52}$ and let $N = S_3 \times \{0\} \subseteq G$. It is straightforward to show that $N$ is normal in $G$. What is the structure of $G/N$? Well, define $\phi : G \to \mathbb{Z}_{52}$ by $\phi((\sigma, a)) = a$. Then $\phi$ is clearly an epimorphism and $\operatorname{Ker}\phi = \{(\sigma, a) \in G : a = 0\} = N$. So $G/N$ is isomorphic to $\mathbb{Z}_{52}$.

Generalizing the above example, we have the following theorem, whose proof we leave to the reader.

**Theorem 9.8.** *Let $G = G_1 \times G_2 \times \cdots \times G_k$ (where $k \in \mathbb{Z}^+$) and let $N_i$ be a normal subgroup of $G_i$ for each $i = 1, 2, \ldots, k$. Then $N = N_1 \times N_2 \times \cdots \times N_k$ is a normal subgroup of $G$, with $G/N \simeq G_1/N_1 \times G_2/N_2 \cdots \times G_k/N_k$.*

We provide one more cool example of using the First Isomorphism Theorem. Clearly, since $\mathbb{R}$ is abelian, $\mathbb{Z}$ is a normal subgroup of $\mathbb{R}$. What is the structure of $\mathbb{R}/\mathbb{Z}$? Well, in modding $\mathbb{R}$ out by $\mathbb{Z}$ we have essentially identified together all real numbers that are an integer distance apart. So we can think of the canonical epimorphism from $\mathbb{R}$ to $\mathbb{R}/\mathbb{Z}$ as wrapping up $\mathbb{R}$ like a garden hose! Thus, one might guess that $\mathbb{R}/\mathbb{Z}$ has some circle-like structure—but if we want to think of it as a group, we have to figure out what the group structure on such a "circle" would be!

We leave, for a moment, our group $\mathbb{R}/\mathbb{Z}$, and look at how we can consider a circle to be a group.

**Notation.** Recall that for every $\theta \in \mathbb{R}$, $e^{i\theta}$ is defined to be $\cos\theta + i\sin\theta$. It is clear then that the set $\{e^{i\theta} : \theta \in \mathbb{R}\}$ is the unit circle in the complex plane; we denote this set by $\mathbb{S}_1$.[1]

[1] We do this because this set is a one-dimensional sphere (i.e., a circle). More generally, an $n$-dimensional sphere, for $n \in \mathbb{N}$, is denoted by $S_n$.

**Remark.** Note that if $\theta_1, \theta_2 \in \mathbb{R}$, then $e^{i\theta_1} = e^{i\theta_2}$ if and only if $\theta_1 - \theta_2 \in 2\pi\mathbb{Z}$.

**Theorem 9.9.** *$\mathbb{S}_1$ is a group under the multiplication $e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$.*

*Proof.* The tricky part is showing that the operation is well defined. Suppose $\theta_1, \theta_2, t_1$, and $t_2$ are in $\mathbb{R}$, with $e^{i\theta_1} = e^{it_1}$ and $e^{i\theta_2} = e^{it_2}$. We want to show that

$$e^{i\theta_1}e^{i\theta_2} = e^{it_1}e^{it_2},$$

i.e., that

$$e^{i(\theta_1+\theta_2)} = e^{i(t_1+t_2)}.$$

Now, $e^{i\theta_1} = e^{it_1}$ and $e^{i\theta_2} = e^{it_2}$ imply that $\theta_1 - t_1 = 2\pi m$ and $\theta_2 - t_2 = 2\pi n$ for some $m$ and $n$ in $\mathbb{Z}$; hence,

$$\theta_1 + \theta_2 - (t_1 + t_2) = 2\pi(m + n) \in 2\pi\mathbb{Z}.$$

Thus, $e^{i(\theta_1+\theta_2)} = e^{i(t_1+t_2)}$, so our operation is well defined.

Next, $\mathbb{S}_1$ is clearly closed under the operation, and associativity follows from associativity of addition in $\mathbb{R}$. Moreover, $e^{i0} = 1$ clearly acts as an identity element in $\mathbb{S}_1$, and if $e^{i\theta} \in \mathbb{S}_1$, then $e^{i\theta}$ has inverse $e^{i(-\theta)} \in \mathbb{S}_1$. So $\mathbb{S}_1$ is a group under the described operation. Beautifully, it turns out that our group $\mathbb{R}/\mathbb{Z}$ is isomorphic to $\mathbb{S}_1$. □

**Theorem 9.10.** $\mathbb{R}/\mathbb{Z} \simeq \mathbb{S}_1$.

*Proof.* We will define an epimorphism $\phi$ from $\mathbb{R}$ to $\mathbb{S}_1$ with $\operatorname{Ker}\phi = \mathbb{Z}$; then we'll have $\mathbb{R}/\mathbb{Z} \simeq \mathbb{S}_1$, by the First Isomorphism Theorem.

Define $\phi : \mathbb{R} \to \mathbb{S}_1$ by $\phi(r) = e^{i2\pi r}$. We have that $\phi$ is a homomorphism, since for every $r, s \in \mathbb{R}$, we have

$$\phi(r + s) = e^{i2\pi(r+s)} = e^{i2\pi r+i2\pi s} = e^{i2\pi r}e^{i2\pi s} = \phi(r)\phi(s).$$

Moreover, $\phi$ is clearly onto, since if $e^{i\theta} \in \mathbb{S}_1$, then

$$e^{i\theta} = e^{i2\pi\left(\frac{\theta}{2\pi}\right)} = \phi\left(\frac{\theta}{2\pi}\right).$$

Finally, $\operatorname{Ker}\phi = \mathbb{Z}$: indeed,

$$\begin{aligned} r \in \operatorname{Ker}\phi &\Leftrightarrow \phi(r) = 1 \\ &\Leftrightarrow e^{i2\pi r} = 1 \\ &\Leftrightarrow \cos 2\pi r + i \sin 2\pi r = 1 \\ &\Leftrightarrow \cos 2\pi r = 1 \text{ and } \sin 2\pi r = 0 \\ &\Leftrightarrow r \in \mathbb{Z}. \end{aligned}$$

Thus, $\operatorname{Ker}\phi = \mathbb{Z}$, and hence $\mathbb{R}/\mathbb{Z} \simeq \mathbb{S}_1$, as desired. □

## 9.2 The Second and Third Isomorphism Theorems

The following theorems can be proven using the First Isomorphism Theorem. They are very useful in special cases.

**Theorem 9.11.** ***(Second Isomorphism Theorem)*** *Let $G$ be a group, let $H \leq G$, and let $N \trianglelefteq G$. Then the set*

$$HN = \{hn : h \in H, n \in N\}$$

*is a subgroup of $G$, $H \cap N \trianglelefteq H$, and*

$$H/(H \cap N) \simeq HN/N.$$

*Proof.* We first prove that $HN$ is a subgroup of $G$. Since $e_G \in HN$, $HN \neq \emptyset$. Next, let $x = h_1n_1, y = h_2n_2 \in HN$ (where $h_1, h_2 \in H$ and $n_1, n_2 \in N$). Then

$$xy^{-1} = h_1n_1(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1}.$$

Since $N \leq G$, $n_1n_2^{-1}$ is in $N$; so $h_1n_1n_2^{-1}h_2^{-1} \in h_1Nh_2^{-1}$, which equals $h_1h_2^{-1}N$, since $N \trianglelefteq G$ implies $Nh_2^{-1} = h_2^{-1}N$. So $xy^{-1} = \in h_1h_2^{-1}N$. But $H \leq G$ implies $h_1h_2^{-1} \in H$; thus, $xy^{-1} \in HN$, and so $HN$ is a subgroup of $G$.

Since $N \trianglelefteq G$ and $N \subseteq HN$, $N$ is normal in $HN$ (do you see why?). So $HN/N$ is a group under left coset multiplication. We define $\phi : H \to HN/N$ by $\phi(h) = hN$ (notice that when $h \in H$, $h \in HN$ since $h = he_G$). Clearly, $\phi$ is a homomorphism. Further, $\phi$ is onto: Indeed, let $y \in HN/N$. Then $y = hnN$ for some $h \in H$ and $n \in N$. But $nN = N$, so $y = hN = \phi(h)$. Finally,

$$\operatorname{Ker}\phi = \{h \in H : \phi(h) = N\} = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N.$$

Thus,

$$H/(H \cap N) \simeq HN/N,$$

by the First Isomorphism Theorem. □

**Theorem 9.12.** ***(Third Isomorphism Theorem)*** *Let $G$ be a group, and let $K$ and $N$ be normal subgroups of $G$, with $K \subseteq N$. Then $N/K \trianglelefteq G/K$, and*

$$(G/K)/(N/K) \simeq G/N.$$

*Proof.* Define $\phi : G/K \to G/N$ by $\phi(aK) = aN$. We have that $\phi$ is well defined: indeed, let $aK = bK \in G/K$. Then by Statement 6 of Theorem 7.10, we have $aN = bN$, that is, $\phi(aK) = \phi(bK)$. So $\phi$ is well defined. $\phi$ is clearly onto, and we have

$$\begin{aligned}\operatorname{Ker}\phi &= \{aK \in G/K : \phi(aK) = N\} \\ &= \{aK \in G/K : aN = N\} \\ &= \{aK \in G/K : a \in N\} \\ &= N/K.\end{aligned}$$

So the desired results hold, by the First Isomorphism Theorem. □

**Example 9.13.** Using the Third Isomorphism Theorem we see that the group

$$(\mathbb{Z}/12\mathbb{Z})/(6\mathbb{Z}/12\mathbb{Z})$$

is isomorphic to the group $\mathbb{Z}/6\mathbb{Z}$, or $\mathbb{Z}_6$.

## 9.3 Exercises

### Exercise 9.1

Let $F$ be the group of all functions from $[0,1]$ to $\mathbb{R}$, under pointwise addition. Let

$$N = \{f \in F : f(1/4) = 0\}.$$

Prove that $F/N$ is a group that's isomorphic to $\mathbb{R}$.

### Exercise 9.2

Let $N = \{1, -1\} \subseteq \mathbb{R}^*$. Prove that $\mathbb{R}^*/N$ is a group that's isomorphic to $\mathbb{R}^+$.

### Exercise 9.3

Let $n \in \mathbb{Z}^+$ and let $H = \{A \in GL(n, \mathbb{R}) : \det A = \pm 1\}$. Identify a group familiar to us that is isomorphic to $GL(n, \mathbb{R})/H$.

### Exercise 9.4

Let $G$ and $G'$ be groups with respective normal subgroups $N$ and $N'$. Prove or disprove: If $G/N \simeq G'/N'$ then $G \simeq G'$.

# GNU Free Documentation License

Version 1.3, 3 November 2008


<http://www.fsf.org/>



### Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed

under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML

using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "**publisher**" means any person or entity that distributes copies of the Document to the public.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

## 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

## 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

# 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

## 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in

an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

# 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

# 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation

of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

# 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `http://www.gnu.org/copyleft/`.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

# 11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

## ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright © YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

# References and Supplemental Resources


[1] John B. Fraleigh, *A First Course in Abstract Algebra (7th ed.)*, Addison Wesley, 2002.

[2] Thomas W. Judson, *Abstract Algebra: Theory and Applications*. Revised edition published under the GNU Free Documentation License, 1997 (revised 2016). `http://abstract.pugetsound.edu/`

[3] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers (5th ed.)*, John Wiley & Sons, 1991.