MA383: Introduction to Modern Algebra

Dylan C. Beck

Acknowledgements

Primarily, the contents of this document were created in the Fall 2022 semester at Baker University. I would like to express my gratitude toward my students in MA383 — especially those who assisted in the enhancement of these notes with comments and suggestions. I am also grateful to Vance Gaffar for his helpful comments and interesting solutions to some of the exercises.

Contents

Chapter 1

Basic Properties of Sets and Logic

Before we delve into the theory of modern algebra, we must first understand and appreciate that mathematics is a language of its own; thus, it is imperative for us to develop the necessary diction, grammar, and syntax in order for us to effectively communicate. We accomplish this formally via the tools of set theory and the calculus of logic. Even now, these branches of mathematics enjoy an ongoing ubiquity and significance that makes them an active area of research, but we will not trouble ourselves with these subtle complexities. (Explicitly, if it matters to the reader, we will adopt the standard axioms of the Zermelo-Fraenkel set theory with the Axiom of Choice.)

1.1 Sets and Set Operations

We define a **set** X as a collection of like objects, e.g., functions or real numbers. We refer to an arbitrary object x of X as an **element** (or **member**) of X. If x is an element of X, then we write $x \in X$ to denote that "x is an element (or member) of the set X." We may also say in this case that x "belongs to" or "lies in" X, or we may wish to emphasize that X "contains" x. Conversely, if X does not contain y, then we write $y \notin X$ to signify that "y is not an element of X."

If there are "few enough" distinct elements of X, then we can explicitly write down X using pointy braces. For instance, $X = \{1, 2, 3, 4, 5, 6\}$ is a finite set consisting of the first six positive integers. Unfortunately, as the number of members of X increases, such an explicit expression of X becomes cumbersome to write down; instead, we may use **set builder notation** to express a set whose members possess a closed-form. Explicitly, set builder notation exhibits an arbitrary element x of the attendant set X followed by a bar $|$ and a list of qualitative information about x, e.g.,

$$X = \{1, 2, 3, 4, 5, 6\} = \{x \mid x \text{ is an integer and } 1 \leq x \leq 6\}.$$

Even more, set builder notation can be used to write down infinite sets. We will henceforth fix the following notation for the natural numbers $\mathbb{Z}_{\geq 0} = \{n \mid n \text{ is a non-negative integer}\}$, the integers $\mathbb{Z} = \{n \mid n \text{ is an integer}\}$, and the rational numbers $\mathbb{Q} = \left\{\frac{a}{b} \mid a \text{ and } b \text{ are integers such that } b \neq 0\right\}$. Using the rational numbers, one can construct the real numbers $\mathbb{R} = \{x \mid x \text{ is a real number}\}$.

Like with the arithmetic of real numbers, there are mathematical operations on sets that allow us, e.g., to compare them; take their differences; and combine them. For instance, every element of $Y = \{1, 2, 3, 4, 5\}$ is also an element of $X = \{1, 2, 3, 4, 5, 6\}$, but the element 6 of X is not contained

in Y. We express this by saying that Y is a **proper subset** of X: the additional modifier "proper" is used to indicate that X and Y are not the same set (because they do not have the same members). Put into symbols, we write that $Y \subsetneq X$ whenever it is true that (i.) every element of Y is also an element of X and (ii.) there exists an element of X that is not contained in Y; this can be read as "Y is contained in X, but Y does not equal X." We may also say that Y is "included in" X. One other way to indicate that Y is a (proper) subset of X is by saying that X is a (proper) **superset** of Y, in which case we write that $X \supseteq Y$ (or $X \supsetneq Y$). If we could step through the paper and look at the superset containment $X \supseteq Y$ from the other side, it would be nothing more than $Y \subseteq X$.

We introduce the **relative complement** of Y with respect to X to formalize our previous observation that 6 belongs to X but does not belong to Y. By definition, the relative complement of Y with respect to X is the set consisting of the elements of X that are not elements of Y. We use the symbolic notation $X \setminus Y = \{w \in X \mid w \notin Y\}$ to denote the relative complement of Y with respect to X, e.g., we have that $X \setminus Y = \{6\}$ in our running example. We may view the relative complement of Y with respect to X as the "set difference" of X and Y. Conversely, the two sets X and Y "overlap" in $\{1, 2, 3, 4, 5\}$ because they both contain the elements 1, 2, 3, 4, and 5. We define the **intersection** $X \cap Y = \{w \mid w \in X \text{ and } w \in Y\}$ of the sets X and Y as the set consisting of those elements that belong to both X and Y; in this case, we have that $X \cap Y = \{1, 2, 3, 4, 5\}$.

Consider next the finite sets $V = \{1, 2, 3\}$ and $W = \{4, 5, 6\}$. Because none of the elements of V belong to W and none of the element of W belong to V, the intersection of V and W does not possess any elements; it is empty! Conventionally, this is called the **empty set**, and it is denoted by $\emptyset$. Put another way, our observations thus far in this paragraph can be stated as $V \cap W = \emptyset$. We will soon see that the empty set is a proper subset of every nonempty set. Going back to our discussion of V and W, we remark that the keen reader might have already noticed that $W = X \setminus V$ and $V = X \setminus W$, i.e., every element of X lies in either V or W (but not both because there are no elements that lie in both V and W). We say in this case that the set X is the **union** of the two sets V and W, and we write $X = V \cup W$. Generally, the union of two sets X and Y is the set consisting of all objects that are either an element of X or an element of Y — that is, $X \cup Y = \{w \mid w \in X \text{ or } w \in Y\}$.

If X and Y are any sets, then one can form the **Cartesian product** of X and Y; this is the set that consists of ordered pairs (x, y) for each element $x \in X$ and $y \in Y$, i.e., the Cartesian product of X and Y is the set $X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y$. Observe that the Cartesian product $\mathbb{Z} \times \mathbb{Z}$ of the integers $\mathbb{Z}$ with itself is the collection of integer points in the Cartesian plane $\mathbb{R} \times \mathbb{R}$. We refer to a subset R of the Cartesian product $X \times X$ as a **relation** on X. Every set X admits a relation called the **diagonal** Δ_X of X that consists precisely of the elements of $X \times X$ of the form (x, x). Put another way, the diagonal of X is the relation $\Delta_X = \{(x, x) \mid x \in X\} \subseteq X \times X$.

One important consideration in the arithmetic of sets is the number of elements in a finite set X. For instance, in our previous examples, it is clear that $X = \{1, 2, 3, 4, 5, 6\}$ consists of six elements, but $Y = \{1, 2, 3, 4, 5\}$ possesses five elements. Observe that this immediately distinguishes the sets X and Y. We refer to the number of elements in a finite set X as the **cardinality** of X, denoted by $\#X$ or $|X|$. Like we previously mentioned, we have that $|X| = 6$ and $|Y| = 5$. If X and Y are finite sets with cardinalities $|X|$ and $|Y|$, then the Cartesian product $X \times Y$ has cardinality $|X| \cdot |Y|$ because an element of $X \times Y$ is uniquely determined by the ordered pair (x, y). Cardinality can be defined even for infinite sets, but additional care must be taken in this case, so we will not bother.

Like with real numbers, functions can be defined between arbitrary sets. Explicitly, a **function**

$f : X \to Y$ from a set X to a set Y is merely an assignment of each element $x \in X$ to a unique (not necessarily distinct) element $f(x) \in Y$; the **domain** of $f : X \to Y$ is X, and the **codomain** of f is Y. Out of desire for notational convenience, we may sometimes omit the letter $f : X \to Y$ when defining a function f from a set X to a set Y and simply use an arrow $X \to Y$ to indicate the sets involved and an arrow $x \mapsto f(x)$ to declare the element $f(x) \in Y$ onto which the element $x \in X$ is sent; often, this will become clearer in practice. Every set X possesses a function $\mathrm{id}_X : X \to X$ that is called the **identity function** and defined by $\mathrm{id}_X(x) = x$. If X is a subset of Y, then the **inclusion** $X \subseteq Y$ can be viewed as the function $X \to Y$ that sends $x \mapsto x$, where the symbol x that appears to the left of the arrow $\mapsto$ is viewed as an element of X, and the symbol x that appears to the right of the arrow $\mapsto$ is then viewed as an element of Y. Or in the usual notation, the inclusion may be thought of as the function $f : X \to Y$ defined by $f(x) = x$. Even more, every set X induces a function $\delta_X : X \to X \times X$ that is called the **diagonal function** (of X) and defined by $\delta_X(x) = (x, x)$. By Exercise 1.10.4, the diagonal Δ_X of X is exactly the image of the diagonal function δ_X of X, hence there should be no confusion in terminologies. Conversely, we say that a function $* : X \times X \to X$ that sends $(x_1, x_2) \mapsto x_1 * x_2$ is a **binary operation**; implicit in the definition of a binary operation $*$ is the requirement that $x_1 * x_2$ is an element of X for every pair of elements $x_1, x_2 \in X$. For instance, addition is a binary operation on the real number $\mathbb{R}$.

Each time we define a function $f : X \to Y$, in addition, we implicitly distinguish the collection of elements $y \in Y$ such that $y = f(x)$ for some element $x \in X$; this is called the **image** of X (in Y) with respect to f, and it is denoted by $f(X) = \{y \in Y \mid y = f(x) \text{ for some element } x \in X\}$. Conversely, if W is a subset of Y, then the collection of elements $x \in X$ such that $f(x) \in W$ is the **pre-image** of W (in X) with respect to f. Explicitly, we have that $f^{-1}(W) = \{x \in X \mid f(x) \in W\}$. We note that for any subsets $V \subseteq X$ and $W \subseteq Y$, it is always the case that $V \subseteq f^{-1}(f(V))$ and $f(f^{-1}(W)) \subseteq W$; however, the superset containments $V \supseteq f^{-1}(f(V))$ and $f(f^{-1}(W)) \supseteq W$ do not always hold (cf. Exercise 1.10.7). We introduce two properties of functions that are sufficient to guarantee that these superset inclusions. If $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ for any pair of elements $x_1, x_2 \in X$, then we say that $f : X \to Y$ is **injective**. Essentially, a function $f : X \to Y$ is injective if and only if distinct elements $x_1, x_2 \in X$ induce distinct elements $f(x_1), f(x_2) \in Y$. We will soon verify this formally. Even more, we say that $f : X \to Y$ is **surjective** if for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$. One way to think about the surjective property is that every element of Y is "mapped onto" or "covered" by an element of X. If $f : X \to Y$ is both injective and surjective, then we say that f is **bijective**. We may think about a bijection $f : X \to Y$ as a relabelling of the elements of Y using the names of elements of X; in this way, two sets X and Y are "essentially the same" if there exists a bijection $f : X \to Y$.

Proposition 1.1.1. *Let $f : X \to Y$ be any function between any two sets X and Y.*

1.) *If f is injective, then $f^{-1}(f(V)) = V$ for any set $V \subseteq X$.*

2.) *If f is surjective, then $f(f^{-1}(W)) = W$ for any set $W \subseteq Y$.*

Proof. 1.) By Exercise 1.10.7, it suffices to prove that $f^{-1}(f(V)) \subseteq V$. Let x be an arbitrary element of $f^{-1}(f(V))$. By definition of the pre-image $f^{-1}(f(V))$ of $f(V)$, this means that $f(x) \in f(V)$. By definition of the image $f(V)$, we have that $f(x) = f(v)$ for some element $v \in V$. Last, by assumption that f is injective and $V \subseteq X$, we conclude that $x = v$, hence x is an element of V.

(2.) By Exercise 1.10.7, it suffices to prove that $W \subseteq f(f^{-1}(W))$. Let w be any element of W. By assumption that f is surjective and $W \subseteq Y$, there exists an element $x \in X$ such that $w = f(x)$. By definition of the pre-image $f^{-1}(W)$, it follows that $x \in f^{-1}(W)$. By definition of the image $f(f^{-1}(W))$, we conclude that $w = f(x)$ for some element $x \in f^{-1}(W)$ so that $w \in f(f^{-1}(W))$. $\square$

Conversely, if $f^{-1}(f(V)) = V$ holds for any set $V \subseteq X$, then $f : X \to Y$ must be injective; likewise, if $f(f^{-1}(W)) = W$ for any set $W \subseteq Y$, then f must be surjective (cf. Exercise 1.10.8).

1.2 Logic and Truth Tables

We have thus far garnered a working knowledge of set theory, and we have seen some mathematical proofs. We turn our attention next to fleshing out some details regarding the calculus of logic that will soon assist us with writing proofs. We will assume throughout this section that P and Q are **statements**, i.e., P and Q are complete sentences that assert some property or quality that can be unambiguously measured as true or false. For instance, "Every positive whole number is an integer" is an example of a (true) statement; however, "The weather in Kansas City is lovely this time of year" is not a statement because some individuals might think so while others might not.

We will be interested primarily in logical constructions of the form $P \implies Q$, where the double-arrow $\implies$ stands for "implies." Under this convention, the entire expression $P \implies Q$ can be read either as "P implies Q" or "If P, then Q." Unsurprisingly, statements of this form are called **implications**. We refer to P in this construction as the **antecedent** and to Q as the **consequent**. We may deduce the validity of a statement $P \implies Q$ by constructing the following **truth table**.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 1.1: the truth table for the implication $P \implies Q$

Perhaps the best way to understand the above truth table is by example. For instance, if P is the statement that "3 is an odd number" and Q is the statement that "Madrid is the capital of Spain," then $P \implies Q$ must be true because both P and Q are true statements. On the other hand, if P is false, then the implication $P \implies Q$ is true regardless of the **truth-value** (or verity) of Q; in this case, $P \implies Q$ is called a **vacuous truth**, or it is said to be vacuously true. Essentially, the idea is that P cannot be satisfied because it is false, so the implication must be true: if P is the statement that "17 is larger than 38," then $P \implies Q$ is true regardless of the statement Q. On the other hand, if the statement P is true but the statement Q is false, then the statement $P \implies Q$ must be false because the consequent is false. By example, we can verify this intuition in the case that P is the statement that "3 is an odd number" and Q is the statement that "17 is larger than 38": certainly, the statement $P \implies Q$ is false (read it aloud to convince yourself), hence the verity of the antecedent P has no bearing on $P \implies Q$ because the consequent Q is false.

Unfortunately, in some situations, it is difficult to establish the verity of a statement Q from a statement P that is known to be true. Under these circumstances, it is not possible to determine

if the statement $P \implies Q$ is true or false because this depends entirely on whether Q is true or false; however, it is possible in some cases to extract a statement $S(P, Q)$ (depending upon P and Q) that is **logically equivalent** to the implication $P \implies Q$. We say that two statements S and S' are logically equivalent if and only if their values in a truth table are equal. Consequently, if we could demonstrate that the statement $S(P, Q)$ were true, then $P \implies Q$ must be true, as well.

We examine next some different ways to construct new statements from two given statements P and Q. One way to do so is by considering the case that either P or Q is true. Put into symbols, the **disjunction** $P \vee Q$ is the statement "either P or Q," for which the upside-down wedge $\vee$ denotes the connective "or." Crucially, if either P or Q is true, then $P \vee Q$ must also be true. On the other hand, we may also think about when both P and Q are true, which gives rise to the statement "both P and Q" or the **conjunction** $P \wedge Q$; this is true if and only if both P and Q are true, hence if one of P or Q is false, then $P \wedge Q$ is also false. Be careful not to confuse the upside-down wedge $\vee$ (meaning "or") with the right-side up $\wedge$ (meaning "and"). Last, the **negation** $\neg P$ of the statement P is the statement "not P." Observe that the truth-value for $\neg P$ is the opposite of the truth-value of P. Ultimately, we may construct the following truth tables for the above scenarios.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	$\neg P$	$P \vee \neg P$	$P \wedge \neg P$
T	F	T	F
T	F	T	F
F	T	T	F
F	T	T	F

Table 1.2: the truth tables for the disjunction $P \vee Q$, conjunction $P \wedge Q$, $P \vee \neg P$, and $P \wedge \neg P$

We note that the statement $P \vee \neg P$ ("P or not P") is always true; it is a **tautology**. On the other hand, the statement $P \wedge \neg P$ is always false; it is a **self-contradiction**; this proves the following.

Theorem 1.2.1 (Law of the Excluded Middle)**.** *If P is any statement, then either P or $\neg P$ is true.*

Theorem 1.2.2 (Law of Non-Contradiction)**.** *If P is any statement, then "P and not P" is false.*

We concern ourselves next with the interplay between the disjunction, conjunction, negation, and implication. Often, it is useful in mathematics to determine when a statement $P \implies Q$ is false. Put another way, we wish to determine if P does not imply Q, i.e., if P is not sufficient information from which to deduce the verity of Q. One way to accomplish this is to prove that the consequent Q is false when the antecedent P is true; this is a valid law of inference because the statements $\neg(P \implies Q)$ and $P \wedge \neg Q$ are logically equivalent, as the following truth table bears.

P	Q	$\neg Q$	$P \implies Q$	$\neg(P \implies Q)$	$P \wedge \neg Q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

Table 1.3: the truth table for the negated implication $\neg(P \implies Q)$ and $P \wedge \neg Q$

Both of column $\neg(P \implies Q)$ and $P \wedge \neg Q$ take the same truth-values, hence these statements are logically equivalent. We will also consider the negation of the disjunction $P \vee Q$ ("P or Q") and the negation of the conjunction $P \wedge Q$ ("P and Q"). By Table 1.2, if "P or Q" is not true (i.e., its negation is true), then neither P nor Q can be true. Likewise, by the same table, if "P and Q" is not true (i.e., its negation is true), then either P must not be true or Q must not be true. Collectively, these observations constitute the so-called **De Morgan's Laws** that we prove below.

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
T	T	F	F	T	F	F	T	F	F
T	F	F	T	T	F	F	F	T	T
F	T	T	F	T	F	F	F	T	T
F	F	T	T	F	T	T	F	T	T

Table 1.4: the truth table for $\neg(P \vee Q)$ and $\neg(P \wedge Q)$

Theorem 1.2.3 (De Morgan's Laws)**.** *Let P and Q be any statements.*

1.) $\neg(P \vee Q)$ *is logically equivalent to* $\neg P \wedge \neg Q$.

2.) $\neg(P \wedge Q)$ *is logically equivalent to* $\neg P \vee \neg Q$.

Proof by contraposition is yet another indispensable law of inference we will employ. We say that the **contrapositive** of the implication $P \implies Q$ is the implication $\neg Q \implies \neg P$ formed by taking the implication of the negation of Q and the negation of P. For instance, suppose that P is the statement that "The sun is shining in Kansas City" and Q is the statement that "Bob rides his bike to work." Consider the implication $P \implies Q$ given by the statement, "If the sun is shining in Kansas city, then Bob rides his bike to work"; its contrapositive is the statement, "If Bob does not ride his bike to work, then the sun is not shining in Kansas City." Proof by contraposition exploits that the implications $P \implies Q$ and $\neg Q \implies \neg P$ are logically equivalent, as we can verify below.

P	Q	$P \implies Q$	$\neg Q$	$\neg P$	$\neg Q \implies \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Table 1.5: the truth table for $P \implies Q$ and its contrapositive $\neg Q \implies \neg P$

Last, the **proof by contradiction** (or *reductio ad absurdum*) rounds out the tools that we will most often use in mathematical proofs. Essentially, the proof by contradiction constitutes a valid law of inference by a combination of the Law of the Excluded Middle (which asserts that either a statement or its negation must be true), the Law of Non-Contradiction (which asserts that a statement and its negation cannot both be true), and Table 1.3 (which asserts that $\neg(P \implies Q)$ and $P \wedge \neg Q$ are logically equivalent): one of the statements $P \implies Q$ or $\neg(P \implies Q)$ must be true, hence if we can establish that $P \wedge \neg Q$ is not true, then it must be the case that $\neg(P \implies Q)$ is not true (because these two statements are logically equivalent) so that $P \implies Q$ is true. For instance,

if we define an even number to be a whole number that is divisible by two, then we may appeal to a proof by contradiction to establish that twice any whole number is also even. Explicitly, suppose that P is the statement that "x is a whole number" and Q is the statement that "$2x$ is an even number." If we wish to establish the verity of the implication $P \implies Q$ given by the statement, "If x is a whole number, then $2x$ is an even number," then we may assume to the contrary that P is true (i.e., x is a whole number) and $\neg Q$ is also true (i.e., $2x$ is not an even number); all together, we are assuming $P \wedge \neg Q$, i.e., "x is a whole number and $2x$ is not an even number." By definition, $2x$ is an even number because it is twice a whole number, so we have arrived at a contradiction — namely, that $2x$ is an even number (by definition) and $2x$ is not an even number (by assumption). Ultimately, the statement $P \wedge \neg Q$ cannot be true, hence $P \implies Q$ must be true. Generally, a successful proof by contradiction begins by assuming (to the contrary) that P is true and that Q is not true; then, a contradiction of the form (a.) $P \wedge \neg P$ or (b.) $Q \wedge \neg Q$ is derived. Observe that if $\neg P$ can be deduced from $\neg Q$ (i.e., (a.) holds) then a proof by contraposition may be simpler than a proof by contradiction; on the other hand, if Q can be deduced from P (i.e., (b.) holds), then a **direct proof** may be simpler than a proof by contradiction. Bear this in mind always.

Given any two statements P and Q, we have already considered the implication $P \implies Q$ and its contrapositive $\neg Q \implies \neg P$; however, we could also consider the implication $Q \implies P$ and its contrapositive $\neg P \implies \neg Q$. We refer to the statement $Q \implies P$ as the **converse** of the implication $P \implies Q$; the statement $\neg P \implies \neg Q$ is the **inverse** of the implication $P \implies Q$. Generally, the implication is not logically equivalent to its converse, as the next truth table shows.

P	Q	$P \implies Q$	$Q \implies P$	$\neg P$	$\neg Q$	$\neg P \implies \neg Q$
T	T	T	T	F	F	T
T	F	F	T	F	T	T
F	T	T	F	T	F	F
F	F	T	T	T	T	T

Table 1.6: the truth table for $P \implies Q$, its converse $Q \implies P$, and its inverse $\neg P \implies \neg Q$

Unsurprisingly, we find that the converse $Q \implies P$ and the inverse $\neg P \implies \neg Q$ are logically equivalent because they are contrapositives of one another; however, the implication and its converse are not logically equivalent, hence the implication and its inverse are not logically equivalent.

If P implies Q, then we say that P is **sufficient** for Q or that Q is **necessary** for P. One can rephrase this by saying that P is sufficient for Q when it is true that Q holds if P holds; equivalently, we may say that Q is necessary for P when it is true that P holds only if P holds, i.e., if Q does not hold, then P does not hold. We note that if P is sufficient for Q (or Q is necessary for P), then it might not be true that P is necessary for Q (or that Q is sufficient for P) because the converse is not logically equivalent to the implication; however, if P is both necessary and sufficient for Q, then we have that $P \implies Q$ and $Q \implies P$ so that $P \iff Q$, i.e., "P if and only if Q." If this holds, then we say that P and Q are **(materially) equivalent** statements. Observe that the material equivalence $P \iff Q$ is logically equivalent to the conjunction $(P \implies Q) \wedge (Q \implies P)$.

Even more, **logical quantifiers** allow us to symbolically express the concepts of "for all" (or "for every") and "there exists" (or "for at least one" or "for some"). Explicitly, we adopt the **universal quantifier** $\forall$ as the symbolic representation of the phrase "for all" and the **existential quantifier** $\exists$ as the symbolic representation of the phrase "there exists." Using these quantifiers,

we may convert statements involving quantities into purely symbolic expressions. For instance, that the sum of any whole number and one is a whole number can be written symbolically as $(\forall n \in \mathbb{Z})(n+1 \in \mathbb{Z})$. On the other hand, there exists a non-negative whole number whose difference with one is negative, i.e., $(\exists n \in \mathbb{Z}_{\geq 0})(n-1 \notin \mathbb{Z}_{\geq 0})$. (Explicitly, the non-negative integer $n = 0$ satisfies this property.) Observe that every real number x admits a **unique** real number y such that $x + y = 0$; using logical quantifiers yields $(\forall x \in \mathbb{R})(\exists! y \in \mathbb{R})(x + y = 0)$ with the **uniqueness quantifier** $\exists!$ signifying both the existence ($\exists$) and uniqueness (!). Put another way, the logical quantifier $\exists!$ denotes that "there exists one and only one" element with the prescribed property.

1.3 Sets and Set Operations, Revisited

Using the calculus of logic, we may deduce further properties of sets and set operations. Before proceeding to any new material, we provide first a reinterpretation of Section 1.1 in the language of Section 1.2. We will assume to this end that X and Y are arbitrary (possibly empty) sets.

- We may view the set membership $x \in X$ as the statement "x is an element of X"; its negation is the statement that "x is not an element of X" (or $x \notin X$ in symbols).
- We have that $X \subseteq Y$ ("X is a subset of Y") if and only if for every element $x \in X$, it is true that $x \in Y$, i.e., if and only if it is true that $(\forall x \in X)(x \in Y)$. Consequently, the empty set $\emptyset$ is a subset of every set: there are no elements in $\emptyset$, hence $(\forall e \in \emptyset)(e \in X)$ is vacuously true!
- If it holds that $X \subseteq Y$ and $(\exists y \in Y)(y \notin X)$ ("there exists an element $y \in Y$ such that $y \notin X$"), then we say that X is a proper subset of Y, and we write $X \subsetneq Y$; otherwise, it must be the case that $Y \subseteq X$, hence X and Y are equal, i.e., we must have that $X = Y$.
- Elements of either X or Y comprise the union $X \cup Y$ of X and Y. Put another way, we have that $X \cup Y$ is the superset of both X and Y for which $(w \in X) \vee (w \in Y)$ is true.
- Elements of both X and Y comprise the intersection $X \cap Y$ of X and Y. Put another way, we have that $X \cap Y$ is the subset of both X and Y for which $(w \in X) \wedge (w \in Y)$ is true.
- Elements in Y but not in X comprise the relative complement $Y \setminus X$ of X with respect to Y. Put another way, we have that $Y \setminus X$ is the subset of Y for which $(y \in Y) \wedge (y \notin X)$ is true.
- We may view the Cartesian product $X \times Y$ of X and Y as the collection of all ordered pairs (x, y) for which the statement $(x \in X) \wedge (y \in Y)$ is true.

We will suppose now that W is an arbitrary set for which the inclusions $X \subseteq W$ and $Y \subseteq W$ hold. We say in this case that W is our **universe**, and we may view all elements of X and Y as elements of W via the aforementioned inclusions. We obtain the following membership laws.

Theorem 1.3.1 (Law of the Excluded Middle for Sets)**.** *For any element $w \in W$, we must have that either $w \in X$ or $w \notin X$, and the analogous statement holds for Y in place of X.*

Theorem 1.3.2 (Law of Non-Contradiction for Sets)**.** *For any element $w \in W$, we cannot have that both $w \in X$ and $w \notin X$, and the analogous statement holds for Y in place of X.*

We omit the proofs of the following facts because they follow immediately from the Law of the Excluded Middle and the Law of Non-Contradiction for the statement P that "$w \in X$." Even more, there are analogous De Morgan's Laws for the relative complements of $X \cup Y$ and $X \cap Y$ in W.

Theorem 1.3.3 (De Morgan's Laws for Sets)**.** *Let $X \subseteq W$ and $Y \subseteq W$ be arbitrary sets.*

1.) *We have that $W \setminus (X \cup Y) = (W \setminus X) \cap (W \setminus Y)$.*

2.) *We have that $W \setminus (X \cap Y) = (W \setminus X) \cup (W \setminus Y)$.*

We leave the proofs of De Morgan's Laws for Sets as Exercise 1.10.14.

Often, we will deal with more sets than simply a pair; in this case, it is easiest to adopt the following notation. Let $X_1, X_2, \ldots, X_n$ be arbitrary sets such that $X_i \subseteq W$ for each integer $1 \leq i \leq n$. Each set X_i is **indexed** by a subscript i for distinction. We may consider the union

$$\bigcup_{i=1}^{n} X_i = X_1 \cup X_2 \cup \cdots \cup X_n = \{w \mid w \in X_i \text{ for some integer } 1 \leq i \leq n\}.$$

Once again, we note that the subscript i indicates the set X_i under consideration; the identification $i = 1$ beneath the union symbol indicates that we will begin with $i = 1$; and the superscript n above the union symbol indicates that we will end with $i = n$. Put another way, the elements of $\cup_{i=1}^{n} X_i$ are precisely those elements $w \in W$ such that $w \in X_i$ for some integer $1 \leq i \leq n$, i.e., it holds that $w \in \cup_{i=1}^{n} X_i$ if and only if $(\exists i \in \{1, 2, \ldots, n\})(w \in X_i)$. We may also consider the intersection

$$\bigcap_{i=1}^{n} X_i = X_1 \cap X_2 \cap \cdots \cap X_n = \{w \mid w \in X_i \text{ for all integers } 1 \leq i \leq n\}.$$

Observe that $w \in \cap_{i=1}^{n} X_i$ if and only if $(\forall i \in \{1, 2, \ldots, n\})(w \in X_i)$. Generally, the following extension of De Morgan's Laws for Sets holds; its proof is left as Exercise 1.10.15.

Proposition 1.3.4. *Let $X_1, X_2, \ldots, X_n \subseteq W$ be arbitrary sets.*

1.) *We have that $W \setminus (X_1 \cup X_2 \cup \cdots \cup X_n) = (W \setminus X_1) \cap (W \setminus X_2) \cap \cdots \cap (W \setminus X_n)$.*

2.) *We have that $W \setminus (X_1 \cap X_2 \cap \cdots \cap X_n) = (W \setminus X_1) \cup (W \setminus X_2) \cup \cdots \cup (W \setminus X_n)$.*

If $X_i \cap X_j = \emptyset$, then we say that X_i and X_j are **disjoint**. Even more, if the sets $X_1, X_2, \ldots, X_n$ satisfy the condition that X_i and X_j are disjoint (i.e., $X_i \cap X_j = \emptyset$) for every pair of integers $1 \leq i < j \leq n$, then we say that $X_1, X_2, \ldots, X_n$ are **pairwise disjoint** (or **mutually exclusive**). Observe that if $X_i = \emptyset$ for any integer $1 \leq i \leq n$, then $X_i \cap X_j = \emptyset$ for all integers $1 \leq j \leq n$. Consequently, we may restrict our attention to collections of nonempty pairwise disjoint sets. We say that the collection $\mathcal{P} = \{X_1, X_2, \ldots, X_n\}$ forms a **partition** of the set W if and only if

(i.) X_i is nonempty for each integer $1 \leq i \leq n$;

(ii.) $W = X_1 \cup X_2 \cup \cdots \cup X_n$; and

(iii.) $X_1, X_2, \ldots, X_n$ are pairwise disjoint (i.e., $X_i \cap X_j = \emptyset$ for every pair of integers $1 \leq i < j \leq n$).

We note that every set W admits a trivial partition $\mathcal{W} = \{\{w\} \mid w \in W\}$ via the **singleton** sets $\{w\}$ for each element $w \in W$; however, many sets we will consider throughout this course allow for more interesting partitions. Explicitly, every integer is either odd or even; the quality of being odd or even is called the **parity** of an integer. Consequently, the integers $\mathbb{Z}$ can be partitioned via $\mathcal{P} = \{\mathbb{O}, \mathbb{E}\}$, where $\mathbb{O} = \{n \mid n \text{ is an odd integer}\}$ and $\mathbb{E} = \{n \mid n \text{ is an even integer}\}$.

Generally, a partition of an arbitrary set W need not be finite. Every property of the previous paragraph can be reformulated in the case that the **index set** I is arbitrary. Particularly, we say that an arbitrary collection $\mathcal{P} = \{X_i \mid i \in I\}$ form a partition of W if and only if

(i.) X_i is nonempty for each index $i \in I$;

(ii.) $W = \cup_{i \in I} X_i$; and

(iii.) the sets X_i are pairwise disjoint (i.e., $X_i \cap X_j = \emptyset$ for every pair of distinct indices $i, j \in I$).

1.4 Equivalence Relations and Partial Orders

We will continue to assume that X is an arbitrary set. Recall that a relation on X is by definition a subset R of the Cartesian product $X \times X$. We say that R is **reflexive** if and only if $(x, x) \in R$ for all elements $x \in X$ if and only if R contains the diagonal Δ_X of X (i.e., $R \supseteq \Delta_X$) Even more, if it holds that $(x_2, x_1) \in R$ whenever $(x_1, x_2) \in R$, then R is **symmetric**. Last, if $(x_1, x_2) \in R$ and $(x_2, x_3) \in R$ together imply that $(x_1, x_3) \in R$, then we refer to the relation R as **transitive**. Relations that are reflexive, symmetric, and transitive distinguished as **equivalence relations**. Every set admits at least one equivalence relation, as our next proposition illustrates.

Proposition 1.4.1. *If X is an any set, the diagonal Δ_X of X is an equivalence relation on X.*

Essentially, as an equivalence relation on X, the diagonal of X captures equality of the elements of X: if $(x_1, x_2) \in \Delta_X$, then we must have that $x_1 = x_2$, and if $x_1 = x_2$, then $(x_1, x_2) \in \Delta_X$.

We shall soon discover that there are many objects on which it is fruitful to consider certain equivalence relations. Classically, the rational numbers $\mathbb{Q}$ are constructed by defining an equivalence relation on the integers $\mathbb{Z}$. Before we prove this, let us try an example of a different flavor.

Example 1.4.2. Consider the collection $\mathcal{C}^1(\mathbb{R})$ of functions $f : \mathbb{R} \to \mathbb{R}$ whose first derivatives $f'(x)$ are continuous for all real numbers x. Let E denote the relation on $\mathcal{C}^1(\mathbb{R})$ defined by $(f, g) \in E$ if and only if $f'(x) = g'(x)$ for all real numbers x. Because E is defined by equality and equality is reflexive, symmetric, and transitive, it follows that E is an equivalence relation on $\mathcal{C}^1(\mathbb{R})$.

Let E denote an equivalence relation on an arbitrary set X. Often, it is convenient to adopt the notation that $x_1 \sim_E x_2$ if and only if $(x_1, x_2) \in E$, in which case we may also say that x_1 and x_2 are **equivalent modulo** E. (We note that this convention is due to Carl Friedrich Gauss; it can be understood as asserting that x_1 and x_2 are "the same except for differences accounted for by E.") We define the **equivalence class** of an element $x_0 \in X$ as the collection of elements $x \in X$ that are equivalent to x_0 modulo E, i.e., $[x_0] = \{x \in X \mid x \sim_E x_0\} = \{x \in X \mid (x, x_0) \in E\}$.

Example 1.4.3. Consider the equivalence relation E defined on the set $\mathcal{C}^1(\mathbb{R})$ of Example 1.4.2. By the Fundamental Theorem of Calculus, if $f'(x) = g'(x)$, then there exists a real number C such

that $f(x) = g(x) + C$. Conversely, if $f(x) = g(x) + C$ for some real number C, then $f'(x) = g'(x)$. We conclude that the equivalence classes of $\mathcal{C}^1(\mathbb{R})$ modulo E are given precisely by the sets

$$[g] = \{f \in \mathcal{C}^1(\mathbb{R}) \mid f(x) = g(x) + C \text{ for some real number } C\}.$$

Our next proposition illustrates that a pair of equivalence classes of X modulo E are either equal or disjoint; as a corollary, we obtain a relationship between equivalence relations and partitions.

Proposition 1.4.4. *Let E denote an equivalence relation on an arbitrary set X. Every pair of equivalence classes of X modulo E are either equal or disjoint.*

Proof. Consider any pair $[x_1]$ and $[x_2]$ of equivalence classes of X modulo E. By Exercise 1.10.10, it suffices to prove that $[x_1] = [x_2]$ if they are not disjoint. Consequently, we may assume that there exists an element $x \in [x_1] \cap [x_2]$. By definition, this means that $(x, x_1) \in E$ and $(x, x_2) \in E$. By assumption that E is an equivalence relation, it follows that $(x_1, x) \in E$ by symmetry, hence the transitivity of E implies that $(x_1, x_2) \in E$. Given any element $x_0 \in [x_1]$, we have that $(x_0, x_1) \in E$ implies that $(x_0, x_2) \in E$ by transitivity, hence we conclude that $[x_1] \subseteq [x_2]$. Likewise, the symmetry of E implies that $(x_2, x_1) \in E$, hence the same argument as the previous sentences shows that $[x_2] \subseteq [x_1]$. Combined, the containments $[x_1] \subseteq [x_2]$ and $[x_2] \subseteq [x_1]$ yields that $[x_1] = [x_2]$. □

Corollary 1.4.5. *Let X be an arbitrary set. Every equivalence relation on X induces a partition of X. Conversely, every partition of X induces an equivalence relation on X.*

Proof. By Proposition 1.4.4, if E is an equivalence relation on X, then the collection $\mathcal{P}$ of distinct equivalence classes of X modulo E is pairwise disjoint. Even more, every equivalence class of X modulo E is nonempty because E is reflexive. Last, every element of X belongs to some equivalence class of X modulo E, hence we have that X is the union of its distinct equivalence classes.

Conversely, suppose that $\mathcal{P} = \{X_i \mid i \in I\}$ is a partition of X indexed by I. Consider the relation $E_{\mathcal{P}} = \{(x_1, x_2) \mid x_1, x_2 \in X_i \text{ for some index } i \in I\} \subseteq X \times X$. By definition of a partition, every element $x \in X$ lies in X_i for some index $i \in I$, hence $(x, x) \in E_{\mathcal{P}}$ for every element $x \in X$, i.e., $E_{\mathcal{P}}$ is reflexive. By definition of $E_{\mathcal{P}}$, if $(x_1, x_2) \in E_{\mathcal{P}}$, then $(x_2, x_1) \in E_{\mathcal{P}}$, hence $E_{\mathcal{P}}$ is symmetric. Last, if $(x_1, x_2), (x_2, x_3) \in E_{\mathcal{P}}$, then $x_1, x_2 \in X_i$ and $x_2, x_3 \in X_j$ for some indices $i, j \in I$. By definition of a partition, we have that $X_i \cap X_j = \emptyset$ if and only if i and j are distinct, hence we must have that $i = j$ by assumption that $x_2 \in X_i \cap X_j$. We conclude that $(x_1, x_3) \in X_i$ so that $(x_1, x_3) \in E_{\mathcal{P}}$, i.e., $E_{\mathcal{P}}$ is transitive. Ultimately, this shows that $E_{\mathcal{P}}$ is an equivalence relation on X. □

We say that a relation R on an arbitrary set X is **antisymmetric** if for every pair of elements $x_1, x_2 \in X$, the inclusions $(x_1, x_2) \in R$ and $(x_2, x_1) \in R$ together imply that $x_1 = x_2$. Equivalence relations are defined as reflexive, symmetric, and transitive relations on a set; however, if we replace the requirement of symmetry with the condition of antisymmetry, then we obtain a **partial order**. Explicitly, a partial order P on X is a subset $P \subseteq X \times X$ that is reflexive, antisymmetric, and transitive. Every set admits at least one partial order. Once again, it is simply the diagonal.

Proposition 1.4.6. *If X is any set, the diagonal Δ_X of X is a partial order on X.*

Like with equivalence relations, there are interesting examples of partial orders.

Example 1.4.7. The real numbers $\mathbb{R}$ are partially ordered via the usual less-than-or-equal-to $\leq$.

Example 1.4.8. Divisibility constitutes a partial order on the non-negative integers $\mathbb{Z}_{\geq 0}$. Explicitly, consider the relation $D = \{(a, b) \mid a \text{ divides } b\} \subseteq \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$. Observe that a divides a, hence D is reflexive. Even more, if a divides b and b divides a, then there exist integers m and n such that $b = am$ and $a = bn$; together, these identities yield that $a = bn = amn$. Certainly, if $a = 0$, then $b = 0$, hence we may assume that a is nonzero. Cancelling a factor of a from both sides gives that $mn = 1$, which in turn implies that $m = n = 1$ because a and b are non-negative. Ultimately, this proves that $a = b$, hence D is antisymmetric. Last, if a divides b and b divides c, then a divides c.

Every set admits a partial order, hence every set is a **partially ordered set**; however, there can be many ways to view a set as a partially ordered set. We say that a pair of elements p and q of a partial order P on a set X are **comparable** if it holds that either $(p, q) \in P$ or $(q, p) \in P$; otherwise, the elements p and q are said to be **incomparable**. Every pair of prime integers are incomparable with respect to the partial order of divisibility on the non-negative integers. Conversely, if every pair of elements $p, q \in P$ are comparable, then P is a **total order** on X. Observe that if $Y \subseteq X$, then we may define a partial order $P|_Y = \{(y_1, y_2) \in Y \times Y \mid (y_1, y_2) \in P\}$ on Y by viewing the elements of Y as elements of X. If $P|_Y$ is a total order on $Y \subseteq X$, then we say that Y is a **chain** (with respect to P) in X. We say that an element $x_0 \in X$ is an **upper bound** of Y (with respect to P) if it holds that $(y, x) \in P$ for every element $y \in Y$. We will also say that an element $x_0 \in X$ is **maximal** (with respect to P) if it does not hold that $(x_0, x) \in P$ for any element $x \in X \setminus \{x_0\}$. Our next theorem combines each of these ingredients to comprise one of the most ubiquitous results in mathematics; it will hold vital importance in our study of (two-sided) ideals of unital rings.

Theorem 1.4.9 (Zorn's Lemma)**.** *Let X be an arbitrary set. Let P be a partial order on X. If every chain Y in X has an upper bound in Y, then Y admits a maximal element $y_0 \in Y$.*

1.5 The Principle of Mathematical Induction

One of the most useful proof techniques is the **Principle of Mathematical Induction**. We say that a subset S of real numbers is **hereditary** if it holds that $x + 1 \in S$ whenever we have that $x \in S$. Basically, the Principle of Mathematical Induction is a property of the non-negative integers that asserts that if S is any hereditary subset of non-negative integers such that the smallest element n_0 of S satisfies a statement $P(n_0)$ involving n_0, then every element n of S satisfies the statement $P(n)$. Before we proceed to the definition of the Principle of Mathematical Induction, let us see some examples of properties of integers for which a proof by induction is appropriate.

Example 1.5.1. Consider the positive integer $o(n) = \sum_{i=0}^{n-1}(2i + 1) = 1 + 3 + 5 + \cdots + (2n - 1)$, i.e., the sum of the first n consecutive odd positive integers. We may compute $o(n)$ for small values of n. Explicitly, we have that $o(1) = 1$ and $o(2) = 1 + 3 = 4$ and $o(3) = 1 + 3 + 5 = 9$ and so on.

n	1	2	3	4	5
$o(n)$	1	4	9	16	25

Table 1.7: the sum of first n consecutive odd positive integers

Observe that $o(n) = n^2$ for each integer $1 \leq n \leq 5$. Continuing with the table, we would find that $o(n) = n^2$ for all integers $1 \leq n \leq k$ for any positive integer k. Consequently, we have the following.

Conjecture 1.5.2. If $o(n)$ is defined as in Example 1.5.1, then $o(n) = n^2$ for all integers $n \geq 1$.

Observe that $o(1) = 1 = 1^2$ and $o(n+1) = \sum_{i=0}^{n}(2i+1) = \sum_{i=0}^{n-1}(2i+1)+(2n+1) = o(n)+(2n+1)$, hence if we knew that $o(n) = n^2$, then we could conclude that $o(n+1) = n^2 + 2n + 1 = (n+1)^2$. We will soon return to validate this idea: it is precisely the Principle of Mathematical Induction!

Example 1.5.3. Consider the positive integer $c(n) = \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$, i.e., the sum of the first n consecutive positive integers. We may compute $c(n)$ for small values of n. Explicitly, we have that $c(1) = 1$ and $c(2) = 1 + 2 = 3$ and $c(3) = 1 + 2 + 3 = 6$ and so on.

n	1	2	3	4	5
$c(n)$	1	3	6	10	15

Table 1.8: the sum of the first n consecutive positive integers

Even though it is not nearly as obvious as the pattern from Example 1.5.1, one can verify that $c(n) = \frac{n(n+1)}{2}$ for each integer $1 \leq n \leq 5$. Continuing with the table, we would find that $c(n) = \frac{n(n+1)}{2}$ for all integers $1 \leq n \leq k$ for any positive integer k. Consequently, we have the following.

Conjecture 1.5.4. If $c(n)$ is defined as in Example 1.5.3, then $c(n) = \frac{n(n+1)}{2}$ for all integers $n \geq 1$.

Like before, we have that $c(1) = 1 = \frac{1 \cdot 2}{2}$ and $c(n+1) = \sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = c(n) + (n+1)$, hence if we knew that $c(n) = \frac{n(n+1)}{2}$, then we could conclude that

$$c(n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Definition 1.5.5 (Principle of Ordinary Induction)**.** Let $P(n)$ be any statement involving a non-negative integer n. If the following hold, then $P(n)$ holds for all non-negative integers n.

(i.) $P(0)$ is a true statement.

(ii.) $P(k+1)$ is a true statement whenever $P(k)$ is a true statement for some integer $k \geq 1$.

Remark 1.5.6. Be aware that we have taken the Principle of Ordinary Induction as an axiom in our set theory; however, some authors prefer to prove it as a corollary by first *defining* the non-negative integers $\mathbb{Z}_{\geq 0}$ as the intersection of all hereditary subsets of $\mathbb{R}$ that contain 0 (cf. [DW00, Definition 3.5]). Put another way, we may define $\mathbb{Z}_{\geq 0}$ as the intersection of all sets $S \subseteq \mathbb{R}$ such that

(a.) $0 \in S$ and

(b.) if $s \in S$, then $s + 1 \in S$.

Using this axiom, the Principle of Ordinary Induction can be established by proving that the set $S = \{n \in \mathbb{Z}_{\geq 0} \mid P(n) \text{ is a true statement}\}$ is simply $\mathbb{Z}_{\geq 0}$. But this is clear: by definition of S, if $P(0)$ is a true statement, then $0 \in S$; likewise, if $n \in S$, then $P(n)$ is a true statement, hence $P(n+1)$ is a true statement, i.e., $n + 1 \in S$. Combined, these observations illustrate that S is a hereditary subset of $\mathbb{R}$ that contains 0, i.e., $S \supseteq \mathbb{Z}_{\geq 0}$. By definition of S, we have also that $S \subseteq \mathbb{Z}_{\geq 0}$.

By the Principle of Ordinary Induction, we can return to prove Conjectures 1.5.2 and 1.5.4; we leave these as the respective Exercises 1.10.21 and 1.10.22 for the reader. Occasionally, it is desirable to strengthen the hypotheses of the Principle of Ordinary Induction in order to simplify proofs involving induction. Currently, we may view induction as a property of falling dominoes: (a.) if the 0th domino falls and (b.) the nth domino falling causes the $(n+1)$th domino to fall, then all dominoes indexed by the non-negative integers will fall. But suppose that we could knock down all dominoes from the first to the nth domino: this would provide even more power with which to knock down the $(n+1)$th domino! We introduce this as the following.

Definition 1.5.7 (Principle of Complete Induction)**.** Let $P(n)$ be any statement involving a non-negative integer n. If the following hold, then $P(n)$ holds for all non-negative integers n.

(i.) $P(0)$ is a true statement.

(ii.) $P(k+1)$ is a true statement whenever $P(j)$ is a true statement for all integers $1 \leq j \leq k$.

Even though the hypotheses of the Principle of Complete Induction appear to be stronger than the Principle of Ordinary Induction, the two are in fact equivalent to one another (cf. Exercise 1.10.25); together, they are the Principle of Mathematical Induction. Using complete induction, we may obtain another ubiquitous mathematical tool that will prove crucial in our future endeavors.

Theorem 1.5.8 (Well-Ordering Principle)**.** *Every nonempty set of non-negative integers admits a smallest element with respect to the total order $\leq$. Put another way, if $S \subseteq \mathbb{Z}_{\geq 0}$ is a nonempty set, then there exists an element $s_0 \in S$ such that $s_0 \leq s$ for all elements $s \in S$.*

Proof. We will establish the contrapositive, i.e., we will prove that if $S \subseteq \mathbb{Z}_{\geq 0}$ has the property that for every element $s \in S$, there exists an element $s_0 \in S$ such that $s_0 < s$, then S must be empty. Let $P(n)$ be the statement that $n \notin S$. We claim that $P(n)$ holds for all integers $n \geq 0$. We proceed by the Principle of Complete Induction. Observe that if $0 \in S$, then there exists an element $s_0 \in S$ such that $s_0 < 0$. But this is not possible because S consists of non-negative integers. Consequently, we must have that $0 \notin S$, hence $P(0)$ is true. We will assume according to the Principle of Complete Induction that $P(k)$ holds for each integer $1 \leq k \leq n$. By definition, this means that $k \notin S$ for any integer $1 \leq k \leq n$. Observe that if $n+1 \in S$, then there exists an integer $s_0 \in S$ such that $1 \leq s_0 \leq n$. But this is not possible by the hypothesis of our induction. Consequently, we must have that $n+1 \notin S$, i.e., $P(n+1)$ is a true statement whenever $P(k)$ is a true statement for each integer $1 \leq k \leq n$. By the Principle of Complete Mathematical Induction, our proof is complete. □

Conversely, the Well-Ordering Principle implies the Principle of Ordinary Induction, hence it is equivalent to both ordinary induction and complete induction (cf. Exercise 1.10.26).

1.6 The Division Algorithm

Even as early as grade school, we learn the process of dividing one integer by another. Each time we divide an integer a by a nonzero integer b, we obtain an integer q and a non-negative integer r that is strictly smaller than $|b|$ such that $a = qb + r$. Explicitly, we say that a is the **dividend**; b is the **divisor**; q is the **quotient**; and r is the **remainder** of the division. Our aim throughout this

section is to establish that this process is well-founded, i.e., the process of division of an integer a by a nonzero integer b always results in *unique* integers q and r such that $a = qb+r$ and $0 \leq r < |b|$. We will also establish an algorithm that will allow us to efficiently find the integers q and r.

Example 1.6.1. Consider the case that $a = 11$ and $b = 2$. One can easily see that $11 = 5 \cdot 2 + 1$, hence the integers $q = 5$ and $r = 1$ satisfy the requirements that $a = qb + r$ and $0 \leq r < |b|$.

Example 1.6.2. Consider the case that $a = -17$ and $b = 6$. One can easily see that $-17 = -3 \cdot 6 + 1$, hence the integers $q = -3$ and $r = 1$ satisfy the requirements that $a = qb + r$ and $0 \leq r < |b|$.

Example 1.6.3. Consider the case that $a = -8$ and $b = -9$. One can easily see that $-8 = 1(-9) + 1$, hence the integers $q = 1$ and $r = 1$ satisfy the requirements that $a = qb + r$ and $0 \leq r < |b|$.

Each of the previous examples can be completed by noticing that the integer multiples of b are completely determined by b. Consequently, we may consider all integer multiples of b that do not exceed a, i.e., we may consider the collection $D(a, b) = \{a - qb \mid q \text{ is an integer and } a \geq qb\}$. Our idea is to find the largest (in absolute value) integer q such that $a \geq qb$; then, the difference $a - qb$ must be non-negative (by assumption) and strictly smaller than b (otherwise, we could increase q). Using this intuition as our guide, let us return to find $D(a, b)$ in our previous examples.

Example 1.6.4. By definition, we have that $D(11, 2) = \{11 - 2q \mid q \text{ is an integer and } 11 \geq 2q\}$. Observe that $11 \geq 2q$ if and only if $q \leq 11/2$, hence the only valid values of q in $D(11, 2)$ are $q \leq 5$. Consequently, we have that $-2q \geq -10$ so that $11 - 2q \geq 1$. By consecutively decreasing the value of $q \leq 5$, we find that $D(11, 2) = \{1, 3, 5, 7, \dots\}$ consists of all odd positive integers.

Example 1.6.5. We have that $D(-17, 6) = \{-17 - 6q \mid q \text{ is an integer and } -17 \geq 6q\}$. Observe that $-17 \geq 6q$ if and only if $q \leq -17/6$, hence the only valid values of q in $D(-17, 6)$ are $q \leq -3$. Consequently, we conclude that $D(-17, 6) = \{-17 - 6q \mid q \leq -3 \text{ is an integer}\} = \{1, 7, 13, 19, \dots\}$.

Example 1.6.6. We have that $D(-8, -9) = \{-8 + 9q \mid q \text{ is an integer and } -8 \geq -9q\}$. Observe that $-8 \geq -9q$ if and only if $q \geq 8/9$, hence the only valid values of q in $D(-8, -9)$ are $q \geq 1$. Consequently, we conclude that $D(-8, -9) = \{-8 + 9q \mid q \geq 1 \text{ is an integer}\} = \{1, 10, 19, 28, \dots\}$.

Generalizing the collection $D(a, b)$ and using the Well-Ordering Principle yields the following.

Theorem 1.6.7 (Division Algorithm)**.** *Let a be any integer, and let b be any nonzero integer. There exist* unique *integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.*

Proof. Consider the collection $D(a, b) = \{a - qb \mid q \text{ is an integer and } a \geq qb\}$. By definition, $D(a, b)$ consists of non-negative integers. Observe that if $a \geq 0$, then $D(a, b)$ is nonempty because we may take $q = 0$ to conclude that $D(a, b)$ contains a. On the other hand, if $a < 0$, then if $b \geq 1$, we conclude that $D(a, b)$ is nonempty because we may take $q = a - 1$ to find that $D(a, b)$ contains $a - qb$ because $a \geq a - 1 \geq (a - 1)b = qb$. Last, if $a < 0$ and $b \leq -1$, then $D(a, b)$ must once again be nonempty because we may take $q = -(a - 1)$ to find that $D(a, b)$ contains $a - qb$ because $a \geq a - 1 \geq -(a - 1)b = qb$. Ultimately, this shows that $D(a, b)$ is a nonempty subset of non-negative integers, hence the Well-Ordering Principle implies that there exists a smallest element $r(a, b) = a - qb$ with respect to the total order $\leq$. Rearranging this identity and rewriting $r(a, b)$ as r yields that $a = qb + r$. Clearly, it follows that $r \geq 0$, hence it suffices to see that $r < |b|$. On the contrary, suppose that $a - bq = r \geq |b|$. Observe that if $b \geq 1$, then $|b| = b$ yields that $a - qb \geq b$ and $a - (q + 1)b \geq 0$. Considering that $a - (q + 1)b$ is smaller than the smallest element $r(a, b) = a - qb$

of $D(a,b)$, we obtain a contradiction. Likewise, if $b \leq -1$, then $|b| = -b$ implies that $a - qb \geq b$ and $a - (q-1)b \geq 0$. Considering that $b \leq -1$, we find that $a - (q-1)b = a - qb + b < a - qb = r(a,b)$. Once again, this contradicts the fact that $r(a,b)$ is the smallest element of $D(a,b)$. Ultimately, we conclude that there exist integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.

We must prove next that these integers are *unique*. We accomplish this by assuming that there exist integers q' and r' such that $a = q'b + r'$ and $0 \leq r' < |b|$. Considering that $a = qb + r$ by the previous paragraph, we conclude that $qb + r = q'b + r'$ so that $b(q - q') = r' - r$. Observe that if $q' = q$, then it is clear that $r' = r$, hence our proof is complete. Consequently, we may assume on the contrary that $q - q'$ is nonzero, hence we must have that $|b| \leq |r' - r|$. Observe that if $r' > r$, then $|r' - r| = r' - r$ implies that $r' \geq |b| + r \geq |b|$ — a contradiction. Likewise, if $r' < r$, then $|r' - r| = r - r'$ implies that $r \geq |b| + r' \geq |b|$ — a contradiction. Either way, we conclude that $r' = r$ so that $b(q - q') = 0$. By hypothesis that b is nonzero, we conclude that $q - q' = 0$ or $q' = q$. □

We have therefore rigorously verified the method of division we have taken for granted since elementary school! Even though the Division Algorithm does not explicitly provide the steps to compute the unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$, we note that the proof is constructive in the sense that the unique integers q and $0 \leq r < |b|$ can be deduced from the collection $D(a,b) = \{a - qb \mid q \text{ is an integer and } a \geq qb\}$, as we have done in previous examples.

If the Division Algorithm produces a remainder of zero, then we will say that b **divides** a, and we will write that $b \mid a$. Put another way, we have that $b \mid a$ if and only if $a = qb$ for some integer q. If c is any nonzero integer such that $c \mid a$ and $c \mid b$, then we say that c is a **common divisor** of a and b; the **greatest common divisor** of a and b is the unique integer $d = \gcd(a,b)$ such that

(a.) $d \mid a$ and $d \mid b$, i.e., d is a common divisor of a and b and

(b.) if d' is any common divisor of a and b, then $d' \mid d$.

Example 1.6.8. Consider the integers $a = 24$ and $b = 16$. By writing down the prime factorizations of a and b, their greatest common divisor can easily be read off. Observe that $24 = 4 \cdot 6 = 2^3 \cdot 3$ and $16 = 4^2 = 2^4$. Consequently, the greatest common divisor of 24 and 16 is 2^3, i.e., $\gcd(24, 16) = 8$.

Generally, for any nonzero integers a and b, we may determine $\gcd(a,b)$ from the prime factorizations of a and b in the same manner as Example 1.6.8 (cf. Exercise 1.10.32).

Certainly, it is possible that $\gcd(a,b) = 1$, e.g., if both a and b are prime numbers. Generalizing this notion, we say that a and b are **relatively prime** if and only if $\gcd(a,b) = 1$. Our next lemma states that $\gcd(a,b)$ can always be realized as an integer-linear combination of a and b.

Lemma 1.6.9 (Bézout's Identity)**.** *If a and b be are nonzero integers, then there exist integers x and y such that $\gcd(a,b) = ax + by$. Even more, $\gcd(a,b)$ divides $av + bw$ for all integers v and w.*

Proof. Consider the collection $L(a,b) = \{ax + by \mid x, y \text{ are integers and } ax + by \geq 1\}$. Considering the sign of a and b, one of the elements $a + b$, $a - b$, $-a + b$, or $-a - b$ must lie in $L(a,b)$, hence it is nonempty. By the Well-Ordering Principle, there exists a smallest element $d(a,b) = ax + by$ with respect to the total order $\leq$. We will establish that $\gcd(a,b) = d(a,b)$.

By the Division Algorithm, there exist unique integers q_a and r_a such that $a = q_a d(a,b) + r_a$ and $0 \leq r_a < d(a,b)$. By rearranging this identity and using that $d(a,b) = ax + by$, we find that

$$r_a = a - q_a d(a,b) = a - q_a(ax + by) = (1 - q_a x)a - (q_a y)b.$$

Observe that if r_a were nonzero, then it would lie in $L(a,b)$ and satisfy $1 \leq r_a < d(a,b)$, but this is impossible because $d(a,b)$ is the smallest element of $L(a,b)$. Consequently, it must be the case that $r_a = 0$. Likewise, the Division Algorithm with b in place of a yields that $d(a,b)$ divides b. Ultimately, this proves that $d(a,b) \mid a$ and $d(a,b) \mid b$, hence $d(a,b)$ is a common divisor of both a and b.

Consider another common divisor d' of a and b. We must prove that $d' \mid d(a,b)$. By assumption, there exist integers q_a and q_b such that $a = q_a d'$ and $b = q_b d'$, from which it follows that

$$d(a,b) = ax + by = (q_a d')x + (q_b d')y = (q_a x + q_b y)d'.$$

By definition, this implies that d' divides $d(a,b)$ so that $\gcd(a,b) = d(a,b) = ax + by$, as desired.

Last, let v and w be any integers. By the previous two paragraphs, there exist integers q_a and q_b such that $a = q_a \gcd(a,b)$ and $b = q_b \gcd(a,b)$, hence $\gcd(a,b)$ divides $av + bw$. □

Corollary 1.6.10. *If a and b are relatively prime, then $ax + by = 1$ for some integers x and y.*

Corollary 1.6.11. *If a and b are nonzero integers, then $\gcd(a,b)$ is unique.*

Proof. By the proof of Bézout's Identity, we conclude that $\gcd(a,b)$ is unique because it is by construction the smallest (with respect to $\leq$) nonzero integer satisfying some property. □

Even though Bézout's Identity guarantees the existence of integers x and y such that we may write $\gcd(a,b) = ax + by$, it does not provide any tools for explicitly finding these integers x and y.

Example 1.6.12. Consider the case that $a = 24$ and $b = 16$. We know already that $\gcd(a,b) = 8$, and it is not difficult to see that $8 = 24 \cdot 1 + 16(-1)$; however, this can also be seen as follows. By the Division Algorithm, we have that $24 = 1 \cdot 16 + 8$, hence we have that $8 = 24 \cdot 1 + 16(-1)$.

Example 1.6.13. Consider the case that $a = 110$ and $b = 24$. Observe that the unique prime factorizations of 110 and 15 are $110 = 10 \cdot 11 = 2 \cdot 5 \cdot 11$ and $24 = 2^3 \cdot 3$, respectively. By Exercise 1.10.32, it follows that $\gcd(110, 15) = 2$. By successively implementing the Division Algorithm, we may find the integers x and y such that $110x + 24y = 2$, as guaranteed to us by Bézout's Identity. Explicitly, we begin by running the Division Algorithm with $a = 110$ and $b = 24$ to find the unique integers q_1 and $0 \leq r_1 < 24$ such that $110 = 24q_1 + r_1$; then, we run the Division Algorithm with 24 and r_1 to produce the unique integers q_2 and $0 \leq r_2 < r_1$ such that $24 = q_2 r_1 + r_2$. Continuing in this manner produces a strictly decreasing sequence $r_1 > r_2 > \cdots > r_n$ of non-negative integers at the nth step; by the Well-Ordering Principle, this sequence must have a least element, hence the process must eventually terminate. Putting this process to the test, we find that

$$\begin{aligned} 110 &= 4 \cdot 24 + 14, \\ 24 &= 1 \cdot 14 + 10, \\ 14 &= 1 \cdot 10 + 4, \text{ and} \\ 10 &= 2 \cdot 4 + 2. \end{aligned}$$

We find the integers x and y such that $110x + 24y = 2$ by unravelling this process in reverse. Explicitly, our last identity yields that $10 - 2 \cdot 4 = 2$; the identity before that yields that $4 = 14 - 1 \cdot 10$, hence we have that $-2 \cdot 14 + 3 \cdot 10 = 10 - 2 \cdot (14 - 1 \cdot 10) = 2$; the identity before $14 = 1 \cdot 10 + 4$

yields that $10 = 24 - 1 \cdot 14$, hence we have that $3 \cdot 24 - 5 \cdot 14 = -2 \cdot 14 + 3 \cdot (24 - 1 \cdot 14) = 2$; and at last, the identity before $24 = 1 \cdot 14 + 10$ yields that $14 = 110 - 4 \cdot 24$, hence we have that

$$110(-5) + 24(23) = 3 \cdot 24 - 5 \cdot (110 - 4 \cdot 24) = 2.$$

Algorithm 1.6.14 (Euclidean Algorithm)**.** Let a and b be any nonzero integers such that $a \geq b$.

1.) Use the Division Algorithm to find integers q_1 and r_1 such that $a = q_1 b + r_1$ and $0 \leq r_1 < |b|$.

2.) Use the Division Algorithm to find integers q_2 and r_2 such that $b = q_2 r_1 + r_2$ and $0 \leq r_2 < r_1$.

3.) Use the Division Algorithm to find integers q_3 and r_3 such that $r_1 = q_3 r_2 + r_3$ and $0 \leq r_3 < r_2$.

4.) Continue in this manner until r_{n+1} divides r_n. By the Well-Ordering Principle, this must eventually occur, and moreover, it must occur in a finite number of steps.

5.) Use the fact that $r_{n-1} = q_{n+1} r_n + r_{n+1}$ to express that $r_{n+1} = r_{n-1} - q_{n+1} r_n$.

6.) Use the fact that $r_{n-2} = q_n r_{n-1} + r_n$ to express that $r_n = r_{n-2} - q_n r_{n-1}$; then, use the fact that $r_{n+1} = r_{n-1} - q_{n+1} r_n$ to express that $r_{n+1} = r_{n-1} - q_{n+1}(r_{n-2} - q_n r_{n-1})$ so that

$$r_{n+1} = (q_n q_{n+1} + 1) r_{n-1} - q_{n+1} r_{n-2}.$$

7.) Continue in this manner to produce integers x and y such that $r_{n+1} = ax + by$.

By Bézout's Identity, we must have that $\gcd(a, b) \leq r_{n+1}$. Conversely, because r_{n+1} divides r_n by step four, it must divide r_k for all integers $1 \leq k \leq n$ by the fifth through seventh steps above. Consequently, by the second step above, we conclude that r_{n+1} must divide b, and by the first step above, we conclude that r_{n+1} must divide a. Ultimately, this shows that r_{n+1} is a common divisor of a and b, hence we must have that r_{n+1} divides $\gcd(a, b)$; in particular, we have that $r_{n+1} = \gcd(a, b)$.

1.7 The Integers Modulo n

We will assume throughout this section that n is a fixed nonzero integer. By the Division Algorithm, for every integer a, there exist unique integers q_a and r_a such that $a = q_a n + r_a$ and $0 \leq r_a < |n|$. Considering that the remainder r_a of the division of a by n is always a non-negative integer, we may assume without loss of generality that n is a positive integer. We will refer to the unique integer r_a as the remainder of a **modulo** n. Our naming convention is justified by the next proposition.

Proposition 1.7.1. *If $\mathbb{Z}$ is the set of integers, then $R_n = \{(a, r) \mid a = qn + r \text{ for some integer } q\}$ is an equivalence relation on $\mathbb{Z}$ with distinct equivalence classes $\{qn + r \mid q \in \mathbb{Z}\}$ for each integer $0 \leq r \leq n - 1$. Explicitly, the equivalence class of a modulo n is given by $[a] = \{qn + r_a \mid q \in \mathbb{Z}\}$.*

Proof. By definition, we must justify that R_n is (i.) reflexive, (ii.) symmetric, and (iii.) transitive.

(i.) Clearly, the pair (a, a) lies in R_n because we may always write $a = 0 \cdot n + a$ for any integer a.

(ii.) We must next show that if $(a, r) \in R_n$, then $(r, a) \in R_n$. By definition of R_n, if we assume that $(a, r) \in R_n$, then there exists an integer q such that $a = qn + r$. Consequently, the integer $-q$ satisfies that $r = -qn + a = (-q)n + a$, and we conclude that $(r, a) \in R_n$.

(iii.) Last, we will assume that $(a, r) \in R_n$ and $(r, s) \in R_n$. By definition of R_n, there exist integers q and q' such that $a = qn + r$ and $r = q'n + s$. Consequently, we have that $(a, s) \in R_n$ because

$$a = qn + r = qn + (q'n + s) = (q + q')n + s,$$

and the sum $q + q'$ of the two integers q and q' is itself an integer.

We have therefore established that R_n is an equivalence relation on $\mathbb{Z}$; the equivalence class of an arbitrary integer a modulo R_n is defined by $[a] = \{r \in \mathbb{Z} \mid a = qn + r \text{ for some integer } q\}$. By the Division Algorithm, for every integer a, there exist unique integers q_a and r_a such that $a = q_a n + r_a$ and $0 \leq r_a \leq n - 1$. Consequently, we have that $r_a \in [a]$. By Proposition 1.4.4, we conclude that $[a] = [r_a] = \{r \in \mathbb{Z} \mid r = -qn + r_a \text{ for some integer } q \in \mathbb{Z}\} = \{qn + r_a \mid q \in \mathbb{Z}\}$, as desired. □

Example 1.7.2. Observe that R_2 is an equivalence relation on $\mathbb{Z}$ whose distinct equivalence classes consist of the even integers $\mathbb{E} = \{2q \mid q \in \mathbb{Z}\}$ and the odd integers $\mathbb{O} = \{2q + 1 \mid q \in \mathbb{Z}\}$.

We will henceforth refer to the collection $\mathbb{Z}_n$ of equivalence classes of $\mathbb{Z}$ modulo R_n as the equivalence classes of $\mathbb{Z}$ **modulo** n. By Proposition 1.7.1, $\mathbb{Z}_n$ consists of exactly n distinct elements. Even more, for any two integers a and b, we have that $[a] = [b]$ if and only if the remainder of a modulo n is equal to the remainder of b modulo n if and only if there exist unique integers q_a, q_b, and r such that $a = q_a n + r$ and $b = q_b + r$ and $0 \leq r \leq n - 1$ if and only if $b - a = (q_b - q_a)n$. Put another way, two integers lie in the same equivalence class modulo n if and only if their difference is divisible by n. Generally, an equivalence relation is merely a set whose elements possess no arithmetic; however, the above observation allows us to deduce that $\mathbb{Z}_n$ (i.e., the set of equivalence classes of $\mathbb{Z}$ modulo n) admits a notion of addition and multiplication, as we demonstrate next.

Proposition 1.7.3. *Let $\mathbb{Z}_n$ denote the set of equivalence classes of the integers modulo n.*

(1.) *If a and b are arbitrary integers, then $[a]+[b] = [a+b]$ is a well-defined operation. Even more, this addition is associative, commutative, and satisfies that $[a] + [0] = [a] = [0] + [a]$.*

(2.) *Every equivalence class $[a]$ of the integers modulo n admits an additive inverse $[-a]$.*

(3.) *If a and b are arbitrary integers, then $[a][b] = [ab]$ is a well-defined operation. Even more, this multiplication is associative, commutative, distributive, and satisfies that $[a][1] = [a] = [1][a]$.*

(4.) *If a is an arbitrary integer, then $[a]$ admits a multiplicative inverse if and only if $\gcd(a, n) = 1$.*

Proof. (1.) We must demonstrate that if $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $[a_1 + b_1] = [a_2 + b_2]$. By the previous paragraph, if we assume that $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then there exist integers q_a and q_b such that $a_1 - a_2 = q_a n$ and $b_1 - b_2 = q_b n$. Consequently, we have that

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = q_a n + q_b n = (q_a + q_b)n,$$

from which we conclude that $[a_1 + b_1] = [a_2 + b_2]$. Considering that integer addition is associative and commutative, our addition defined here is associative and commutative.

(3.) We must demonstrate that if $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $[a_1b_1] = [a_2b_2]$. By the paragraph preceding the proposition statement, if we assume that $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then there exist integers q_a and q_b such that $a_1 - a_2 = q_a n$ and $b_1 - b_2 = q_b n$. Consequently, we have that

$$a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2) = q_b a_1 n + q_a b_2 n = (q_b a_1 + q_a b_2)n,$$

from which we conclude that $[a_1b_1] = [a_2b_2]$. Considering that integer multiplication is associative and commutative, our multiplication defined here is associative and commutative. Even more, this multiplication is distributive because the first and third parts of the proposition that we have proved thus far establish that $[a]([b] + [c]) = [a][b + c] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$.

(4.) By definition of our multiplication, the equivalence class $[a]$ admits a multiplicative inverse $[b]$ if and only if $[a][b] = [1]$ if and only if $[ab] = [1]$ if and only if $ab - 1 = qn$ for some integer q if and only if $ab - qn = 1$ for some integer q if and only if $\gcd(a, n) = 1$ by Bézout's Identity. Consequently, $[a]$ admits a multiplicative inverse if and only if $\gcd(a, n) = 1$, as desired. □

Combined, the operations of addition and multiplication on $\mathbb{Z}_n$ form the **modular arithmetic**.

Remark 1.7.4. Going forward, we will adopt the standard notation $b \equiv a \pmod{n}$ ("b is equivalent to a modulo n") in place of our current notation that $[b] = [a]$. Explicitly, we will set $b \equiv a \pmod{n}$ if and only if $n \mid (b - a)$ if and only if $b - a = qn$ for some integer q. Under this identification, observe that $[a] = \{r \in \mathbb{Z} \mid a \equiv r \pmod{n}\}$. One immediate advantage of this notation is that we can perform addition and multiplication modulo n in a natural way: indeed, if $b \equiv a \pmod{n}$, then we have that $b + c \equiv a + c \pmod{n}$ and $bc \equiv ac \pmod{n}$ for all integers c because it holds that $(b+c)-(a+c) = b-a = qn$ and $bc-ac = (b-a)c = (qc)n$ in this case. Even more, Proposition 1.7.3 implies that if $b \equiv a \pmod{n}$ and $d \equiv c \pmod{n}$, then $b+d \equiv a+c \pmod{n}$ and $bd \equiv ac \pmod{n}$.

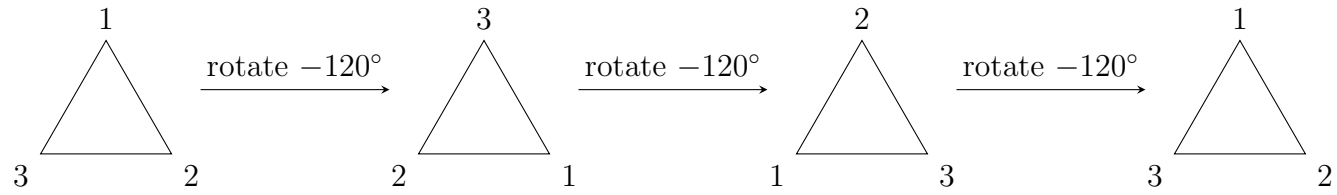
1.8 Rigid Motions

Recall that a **polygon** is a two-dimensional object consisting of straight line segments that intersect to form a closed and bounded region in the plane. Common examples of polygons include triangles, rectangles, and stars. Each of intersection point of a pair of straight line segments is called a **vertex** of the polygon. Particularly, triangles have three vertices; rectangles have four vertices; and stars typically have six vertices. We say that a polygon is **regular** if and only if each of its sides possesses equal length and each (interior) angle formed by the intersection of any two sides has equal measure (in either degrees or radians). Consequently, triangles and rectangles are not necessarily regular polygons; however, equilateral triangles and squares are both examples of regular polygons. We will henceforth refer to a (regular) polygon with n vertices as a (regular) n-**gon**. Under this naming convention, an (equilateral) triangle is a (regular) 3-gon; a (square) rectangle is a (regular) 4-gon; a (regular) pentagon is a (regular) 5-gon; and a (regular) hendecagon is a (regular) 11-gon.

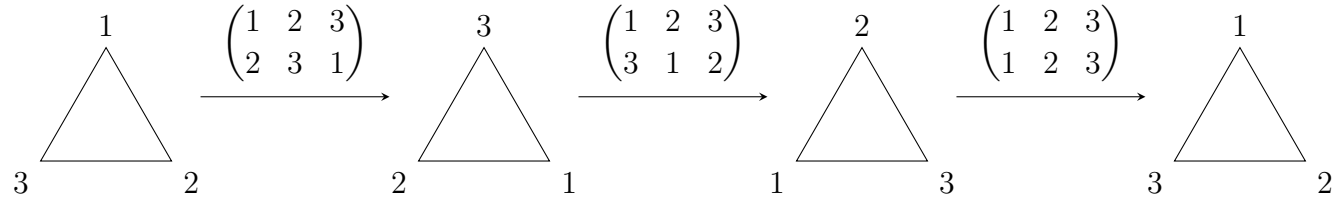
Rigid motions of polygons are those operations that we can perform on polygons without altering the distance between any two vertices of the polygon. For instance, if we have a square in the plane, then we may shift each of the vertices of the square any distance north, south, east, or

west without disturbing the distances between any of the vertices of the square; however, we cannot move just one vertex any nonzero distance north, south, east, or west without altering its distance from another vertex. Put another way, **translation** of a polygon is a rigid motion.

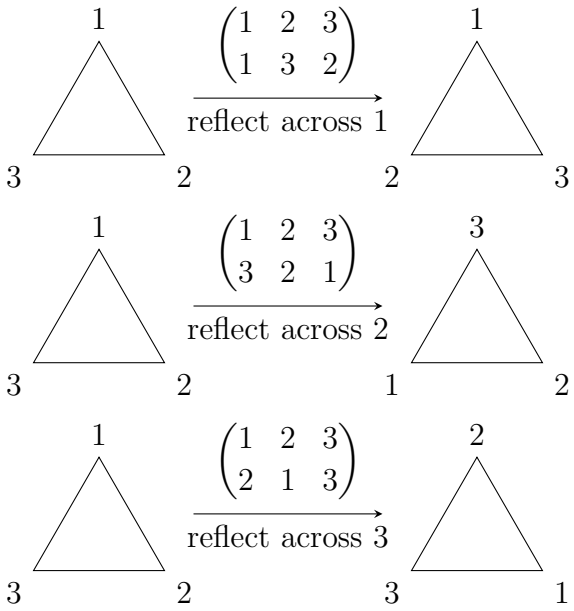
We will fix our attention throughout this section on two specific rigid motions of any regular n-gon. Each of the n vertices of a regular n-gon lies on the circumference of a circle. Consequently, for any integer $1 \leq k \leq n$, a **rotation** of a regular n-gon through an angle of $-360k/n$ degrees produces a copy of the regular n-gon with the ith vertex in place of the $(i+k)$th vertex (modulo n). Pictorially, we may visualize this with the rotations of a regular 3-gon (i.e., an equilateral triangle).



Each rotation is counterclockwise through an angle equal to the common measure of each exterior angle of the n-gon. Consequently, if we perform n rotations, then we wind up with the original arrangement of the vertices of the n-gon. Put another way, the rotations of a regular n-gon through an angle of $-360k/n$ degrees correspond to the **permutations** of the regular n-gon that move vertex i to vertex $i+k$ (modulo n). Explicitly, if we return to our example, we have the following.



On the other hand, a **reflection** of a regular n-gon through a vertex k is a permutation of the vertices of the regular n-gon that fixes the vertex k and swaps some other vertices (depending upon the parity of n). Going back to our example once more, there are three possible reflections.



Combined, these three rotations and three reflections completely exhaust all possible rotations and reflections of the regular 3-gon because there are only $3! = 6$ permutations of the integers $\{1, 2, 3\}$. Even more, if we execute a rotation followed by a reflection (or vice-versa), then we obtain a permutation of the integers $\{1, 2, 3\}$, hence every sequence of rotations and reflections yields a rotation or a reflection. We will return to this concept soon in our discussion of groups.

1.9 Chapter 1 Overview

A **set** X is a collection of distinct objects called **elements** or **members** of X that possess common properties. Elements of X are written abstractly as the lowercase symbol x. We assume the existence of a set $\emptyset$ that does not possess any elements; it is the **empty set**. Every collection of sets comes equipped with certain operations that allow us to combine; compare; and take differences of sets.

- The **union** of the sets X and Y is the set $X \cup Y = \{w \mid w \in X \text{ or } w \in Y\}$.
- The **intersection** of the sets X and Y is the set $X \cap Y = \{w \mid w \in X \text{ and } w \in Y\}$.
- The **relative complement** of X with respect to Y is the set $Y \setminus X = \{w \in Y \mid w \notin X\}$.

We say that Y is a **subset** of X if every element of Y is an element of X, in which case we write $Y \subseteq X$; if Y is a subset of X and there exists an element of X that is not an element of Y, then Y is a **proper subset** of X, in which case we write $Y \subsetneq X$. Observe that Y is a (proper) subset of X if and only if $X \cap Y = Y$ (and $X \cup Y = X$). By the Law of the Excluded Middle, it is always true that $X = Y \cup (X \setminus Y)$ for any set $Y \subseteq X$. If $Y \subseteq X$ and $X \subseteq Y$, then $X = Y$; otherwise, the sets X and Y are distinct. One other way to distinguish a (finite) set X is by the number of elements X possesses — its **cardinality**, denoted by $\#X$ or $|X|$ when this notation is unambiguous.

We define the **Cartesian product** of two sets X and Y to be the set consisting of all ordered pairs (x, y) such that $x \in X$ and $y \in Y$, i.e., $X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}$; a subset R of the Cartesian product $X \times X$ is called a **relation** (on X). Every set X admits a relation called the **diagonal** (of X) and defined by $\Delta_X = \{(x, x) \mid x \in X\}$. Cardinality of sets is multiplicative in the sense that if X and Y are finite sets, then it holds that $|X \times Y| = |X| \cdot |Y|$.

We define a **function** $f : X \to Y$ with **domain** X and **codomain** Y by declaring for each element $x \in X$ a unique (but not necessarily distinct) element $f(x) \in Y$. Every function $f : X \to Y$ induces a subset $f(X) = \{y \in Y \mid y = f(x) \text{ for some element } x \in X\}$ of Y called the **image** of X (in Y) with respect to f. Given any set $W \subseteq Y$, we may also consider the **pre-image** of W (in X) with respect to f, i.e., $f^{-1}(W) = \{x \in X \mid f(x) \in W\}$. We say that $f : X \to Y$ is **injective** if it holds that $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ for any pair of elements $x_1, x_2 \in X$. On the other hand, if for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$, then $f : X \to Y$ is **surjective**. If a function $f : X \to Y$ is both injective and surjective, then it is **bijective**.

We say that a complete sentence P is a **statement** if it asserts something that can be unambiguously measured as true or false. Examples of statements include "3 is an odd number" and "17 is larger than 38"; the first statement is true, but the second statement is false. Using logical connectives, we can form new statements from given statements P and Q. Explicitly, the **implication** $P \implies Q$ is the statement that "P implies Q" (or equivalently, "If P, then Q"); the implication

is false if and only if P is true and Q is false. If P is false, then $P \implies Q$ is called a **vacuous truth**. We define the **disjunction** $P \vee Q$ ("P or Q"), the **conjunction** $P \wedge Q$ ("P and Q"), and the **negation** $\neg P$ ("not P"). Observe that the disjunction $P \vee Q$ is true if and only if P is true or Q is true; the conjunction $P \vee Q$ is true if and only if P is true and Q is true; and the negation $\neg P$ takes the opposite truth-value of P. The Law of the Excluded Middle asserts that either P or $\neg P$ must be true, and the Law of Non-Contradiction asserts that P and $\neg P$ cannot both be true.

We use **truth tables** to deduce the verity of a statement $S(P, Q)$ depending upon two statements P and Q. One can construct a truth table for $S(P, Q)$ by writing all possible **truth-values** of P in one column; all possible truth-values of Q in a subsequent column; and the resultant truth-values of the statement $S(P, Q)$ is a third column. Considering that the statements P and Q could themselves depend upon other statements $P_1, \ldots, P_n$, truth tables may become quite large when the attendant statements are complicated. Generally, we need 2^n rows and $n + 1$ columns to construct the truth table of a statement $S(P_1, \ldots, P_n)$ depending upon n distinct statements $P_1, \ldots, P_n$. If two statements S and S' induce the same truth table, then they are **logically equivalent**; in particular, the truth-values of S are exactly the truth-values of S', hence the verity of the statement S can be deduced from the verity of the statement S' (and vice-versa). If the truth-values for S are all true, then S is a **tautology**; if the truth-values for S are all false, then S is a **self-contradiction**.

De Morgan's Laws are two rules of inference that relate disjunction, conjunction, and negation; explicitly, they assert that (1.) $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ are logically equivalent and (2.) $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent. We define the **contrapositive** of the implication $P \implies Q$ as the statement $\neg Q \implies \neg P$ ("If not Q, then not P") obtained by taking the implication of the negations of Q and P. **Proof by contraposition** is a law of inference that exploits the fact that the contrapositive is logically equivalent to the implication, i.e., the statements $P \implies Q$ and $\neg Q \implies \neg P$ induce the same truth table (cf. Table 1.5). **Proof by contradiction** is a law of inference that can be deduced from the Law of the Excluded Middle, the Law of Non-Contradiction, and the logical equivalence of the statements $\neg(P \implies Q)$ and $P \wedge \neg Q$ (cf. Table 1.3). We carry out a proof by contradiction by first assuming that P is true and that Q is not true; then, we arrive at a contradiction of the form (a.) $P \wedge \neg P$ or (b.) $Q \wedge \neg Q$. We note that if the former holds (i.e., if $\neg P$ can be deduced from $\neg Q$), then a proof by contraposition may be simpler than a proof by contradiction; on the other hand, if the latter holds (i.e., if Q can be deduced from P), then a **direct proof** may be simpler than a proof by contradiction. But any of the three is valid.

Logical quantifiers allow us to symbolically handle statements involving quantities. We use the **universal quantifier** $\forall$ to express that a statement holds "for all" specified objects, and we use the **existential quantifier** $\exists$ to express "there exists" an object satisfying a given statement. We say that an object satisfying a given statement is **unique** if it is the only object that satisfies the given statement. If there exists one and only one object satisfying a specified condition, then we use the **uniqueness quantifier** $\exists!$ to express its existence ($\exists$) and uniqueness (!).

Using logical quantifiers allows us to conveniently state many properties of sets, e.g., the Law of the Excluded Middle for Sets, Law of Non-Contradiction for Sets, and De Morgan's Laws for Sets. Even more, logical quantifiers enable us to extend De Morgan's Laws for Sets to arbitrary unions and arbitrary intersections of sets. Explicitly, we may consider an arbitrary set I as an **index set** for an arbitrary family of sets $\{X_i \mid i \in I\}$ such that each set X_i is a subset of some set W called our **universe**. By definition, the arbitrary union of these sets is simply $\cup_{i \in I} X_i$; membership of an

element $w \in W$ in this arbitrary union is characterized by $w \in \cup_{i \in I} X_i$ if and only if $w \in X_i$ for some index $i \in I$. Likewise, the arbitrary intersection of these sets is $\cap_{i \in I} X_i$ with membership of an element $w \in W$ characterized by $w \in \cap_{i \in I} X_i$ if and only if $w \in X_i$ for all indices $i \in I$. We say that two sets X_i and X_j are **disjoint** if $X_i \cap X_j = \emptyset$; moreover, if $X_i \cap X_j = \emptyset$ for all distinct indices $i, j \in I$, then we say that the sets in $\{X_i \mid i \in I\}$ are **pairwise disjoint** or **mutually exclusive**. We say that the collection $\mathcal{P} = \{X_i \mid i \in I\}$ forms a **partition** of the set W if and only if

(i.) X_i is nonempty for each index $i \in I$;

(ii.) $W = \cup_{i \in I} X_i$; and

(iii.) the sets X_i are pairwise disjoint (i.e., $X_i \cap X_j = \emptyset$ for every pair of distinct indices $i, j \in I$).

If X is an arbitrary set, then a relation on X is a subset R of the Cartesian product $X \times X$. We say that a relation R on X is **reflexive** if and only if $(x, x) \in R$ for all elements $x \in X$; **symmetric** if and only if $(x_1, x_2) \in R$ implies that $(x_2, x_1) \in R$ for all pairs of elements $x_1, x_2 \in X$; **antisymmetric** if and only if $(x_1, x_2) \in R$ and $(x_2, x_1) \in R$ implies that $x_1 = x_2$ for all pairs of elements $x_1, x_2 \in X$; and **transitive** if and only if $(x_1, x_2) \in R$ and $(x_2, x_3) \in R$ together imply that $(x_1, x_3) \in R$ for all triples of elements $x_1, x_2, x_3 \in X$. **Equivalence relations** are precisely the reflexive, symmetric, and transitive relations; **partial orders** are precisely the reflexive, antisymmetric, and transitive relations. Every equivalence relation E on X induces a partition of E via the **equivalence classes** of elements of X. Explicitly, we say that two elements $x_1, x_2 \in X$ are **equivalent modulo** E if and only if $(x_1, x_2) \in E$, in which case we write that $x_1 \sim_E x_2$; the equivalence class of an element $x_0 \in X$ is the collection of elements $x \in X$ that are equivalent to x_0 modulo E, i.e., the equivalence class of x_0 is $[x_0] = \{x \in X \mid x \sim_E x_0\} = \{x \in X \mid (x, x_0) \in E\}$. Every element of X belongs to one and only one equivalence class of X modulo E, hence X is partitioned by the collection of distinct equivalence classes modulo E (cf. Proposition 1.4.4 and Corollary 1.4.5). Every set admits a partial order, hence every set is a **partially ordered set**; however, there can be many ways to view a set as a partially ordered set because there can be many different partial orders on a set. If P is a partial order on a set X, then we say that a pair of elements $p, q \in P$ are **comparable** if either $(p, q) \in P$ or $(q, p) \in P$; otherwise, we say that p and q are **incomparable**. We say that a partial order P on X is a **total order** on X if every pair of elements $p, q \in P$ are comparable. Every partial order P of X induces a partial order on the subsets $Y \subset X$ via $P|_Y = \{(y_1, y_2) \in Y \times Y \mid (y_1, y_2) \in P\}$; if $P|_Y$ is a total order on $Y \subseteq X$, then we say that Y is a **chain** (with respect to P) in X. We say that an element $x_0 \in X$ is an **upper bound** on Y (with respect to P) if $(y, x) \in P$ for every element $y \in Y$. We will also say that an element $x_0 \in X$ is **maximal** (with respect to P) if it does not hold that $(x_0, x) \in P$ for any element $x \in X \setminus \{x_0\}$. Zorn's Lemma asserts that if P is a partial order on an arbitrary set X such that every chain Y in X has an upper bound in Y, then Y admits a maximal element $y_0 \in Y$ (with respect to P). We will make use of this throughout the course.

One of the most useful tools in mathematics is the **Principle of Mathematical Induction**. Collectively, the Principle of Mathematical Induction contains the (equivalent) Principle of Ordinary Induction and the Principle of Complete Induction. Explicitly, the Principle of Ordinary Induction asserts that if $P(n)$ is any statement about a non-negative integer n such that

(1.) $P(0)$ is a true statement and

(2.) $P(k+1)$ is a true statement whenever $P(k)$ is a true statement,

then $P(n)$ is a true statement for all non-negative integers n; the Principle of Complete Induction asserts that if $P(n)$ is any statement about a non-negative integer n such that

(1.) $P(0)$ is a true statement and

(2.) $P(k+1)$ is a true statement whenever $P(1), P(2), \ldots, P(k)$ are all true statements,

then $P(n)$ is a true statement for all non-negative integers n. One of the benefits of using complete induction is that its stronger hypotheses allow us more information with which to conveniently write proofs that might otherwise be awkward with ordinary induction (cf. Exercise 1.10.24). Even more, the Principle of Mathematical Induction appears also in the guise of the Well-Ordering Principle for the non-negative integers; this powerful tool guarantees that every nonempty set of non-negative integers admits a smallest element with respect to the total order $\leq$. Put another way, if $S \subseteq \mathbb{Z}_{\geq 0}$ is a nonempty set, then there exists an element $s_0 \in S$ such that $s_0 \leq s$ for all elements $s \in S$.

Using the Well-Ordering Principle, we may rigorously establish that for any integer a and nonzero integer b, there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$; this fact is known as the Division Algorithm. We refer to the integer a as the **dividend**; b is the **divisor**; q is the **quotient**; and r is the **remainder**. Conventionally, if we obtain a remainder of zero when we divide an integer a by a nonzero integer b, then we say that b **divides** a; in this case, there exists a unique integer q such that $a = qb$, and we use the notation $b \mid a$. If a and b are any integers, then a nonzero integer c is called a **common divisor** of a and b if it holds that $c \mid a$ and $c \mid b$; the **greatest common divisor** of a and b is the unique integer $d = \gcd(a, b)$ such that

(a.) $d \mid a$ and $d \mid b$, i.e., d is a common divisor of a and b and

(b.) if d' is any common divisor of a and b, then $d' \mid d$.

We say that a and b are **relatively prime** if and only if $\gcd(a, b) = 1$. Bézout's Identity asserts that there exist integers x and y such that $\gcd(a, b) = ax + by$; the Euclidean Algorithm is one method from which the integers x and y guaranteed by Bézout's Identity can be obtained.

By the Division Algorithm, for any positive integer n, we may partition the integers $\mathbb{Z}$ into distinct equivalence classes determined by the unique remainder of an integer **modulo** n. Explicitly, we say that two integers a and b are **equivalent modulo** n if and only if $b - a$ is divisible by n; if this is the case, then we write $b \equiv a \pmod{n}$. One can verify that equivalence modulo n induces an equivalence relation R_n on the integers defined by $(a, b) \in R_n$ if and only if $b \equiv a \pmod{n}$; the distinct equivalence classes of $\mathbb{Z}$ modulo R_n are given by $\{qn + r \mid q \in \mathbb{Z}\}$ for each integer $0 \leq r \leq n - 1$; and the collection $\mathbb{Z}_n$ of equivalence classes of $\mathbb{Z}$ modulo n admits operations of addition and multiplication that together comprise the so-called **modular arithmetic**. Explicitly, if $b \equiv a \pmod{n}$ and $d \equiv c \pmod{n}$, then we have that $b + d \equiv a + c \pmod{n}$ and $bd \equiv ac \pmod{n}$.

Polygons are two-dimensional, closed, and bounded objects determined by the intersection of finitely many straight line segments in the plane; the intersection points are called **vertices**. Examples of polygons include triangles, rectangles, and stars. **Regular** polygons have the additional property that their sides possess equal length and each angle at a vertex has equal measure. Equilateral triangles and squares are regular, but most triangles and rectangles are not regular. Generally,

an n-**gon** is any polygon with n vertices. **Rigid motions** of a polygon are those operations that can be performed on the polygon without altering the distance between any two of its vertices. Regular n-gons have the property that **rotation** by an angle of $-360k/n$ degrees is a rigid motion for each integer $1 \leq k \leq n$. Likewise, **reflection** of a regular n-gon across any one of its n vertices also constitutes a rigid motion of the regular n-gon. Combined, rotations and reflections of a regular n-gon can be performed in any order to produce another rotation or reflection.

1.10 Chapter 1 Exercises

1.10.1 Sets and Set Operations

Exercise 1.10.1. Consider the sets

- $W = \{1, 2, 3, \ldots, 10\}$ of positive integers from 1 to 10;
- $X = \{1, 3, 5, 7, 9\}$ of odd positive integers from 1 to 10;
- $Y = \{2, 4, 6, 8, 10\}$ of even positive integers from 1 to 10;
- $\mathbb{O} = \{n \mid n \text{ is an odd integer}\}$;
- $\mathbb{E} = \{n \mid n \text{ is an even integer}\}$; and
- $\mathbb{Z} = \{n \mid n \text{ is an integer}\}$.

Use the set operations $\subseteq$, $\cup$, $\cap$, and $\setminus$ to describe as many relations among these sets as possible.

Exercise 1.10.2. Let $W, X, Y, \mathbb{O}, \mathbb{E}$, and $\mathbb{Z}_{>0}$ be the sets defined in Exercise 1.10.1.

(a.) Compute the number of elements of $X \times Y$; then, list at least three of them.

(b.) List all elements of the diagonal Δ_X of X.

(c.) Every odd integer can be written as $2k + 1$ for some integer k, and every even integer can be written as 2ℓ for some integer ℓ. Express the sets $\mathbb{O}$ and $\mathbb{E}$ in set-builder notation accordingly.

(d.) Convince yourself that $\mathbb{O}$ and $\mathbb{E}$ have "essentially the same" number of elements; then, find a function $f : \mathbb{O} \to \mathbb{E}$ such that f is injective and f is surjective. Observe that this gives a rigorous justification of the fact that $\mathbb{O}$ and $\mathbb{E}$ have "essentially the same" number of elements.

(e.) Convince yourself that $\mathbb{O}$ and $\mathbb{Z}$ have "essentially the same" number of elements; then, find a function $f : \mathbb{O} \to \mathbb{Z}$ such that f is injective and f is surjective. Conclude from this exercise and the previous one that there are "as many" odd (or even) integers as there are integers.

Exercise 1.10.3. Let W be an arbitrary set. Let $X \subseteq W$ and $Y \subseteq W$ be arbitrary subsets of W.

(a.) Prove that for any subset $Z \subseteq W$ such that $Z \supseteq X$ and $Z \supseteq Y$, it follows that $Z \supseteq X \cup Y$. Conclude that $U = X \cup Y$ is the "smallest" subset of W containing both X and Y.

(b.) Prove that for any subset $Z \subseteq W$ such that $Z \subseteq X$ and $Z \subseteq Y$, it follows that $Z \subseteq X \cap Y$. Conclude that $I = X \cap Y$ is the "largest" subset of W contained in both X and Y.

Consider the relative complement $X' = W \setminus X$ of X in W. We may sometimes refer to X' simply as the **complement** of X if we are dealing only with subsets of W, i.e., if W is our universe.

(c.) Prove that $Y \setminus X = Y \cap X'$. Use part (b.) above to conclude that $C = Y \cap X'$ is the "largest" subset of W that is contained in Y and disjoint from X.

Exercise 1.10.4. Let X be an arbitrary set. Prove that $\Delta_X = \delta_X(X)$, where $\delta_X : X \to X \times X$ is the diagonal function defined by $\delta_X(x) = (x, x)$ and $\Delta_X = \{(x, x) \mid x \in X\}$ is the diagonal of X.

Exercise 1.10.5. Let X and Y be arbitrary finite sets.

(a.) Prove that if $|X| \leq |Y|$, then there exists an injective function $f : X \to Y$.

(b.) Prove that if $|X| \geq |Y|$, then there exists a surjective function $f : X \to Y$.

(c.) Conclude that if $|X| = |Y|$, then there exists a bijective function $f : X \to Y$.
(**Caution:** this is not necessarily true if X and Y are infinite sets.)

(d.) Let $|X| = |Y|$. Prove that a function $f : X \to Y$ is injective if and only if it is surjective.
(**Caution:** this is not necessarily true if X and Y are infinite sets.)

Exercise 1.10.6. Let X and Y be arbitrary sets.

(a.) Prove the converse to part (c.) of Exercise 1.10.5, i.e., establish that if there exists a bijective function $f : X \to Y$, then we must have that $|X| = |Y|$.

(b.) Prove that if there exists a function $f^{-1} : Y \to X$ such that $f^{-1} \circ f = \mathrm{id}_X$, then f is injective.

(c.) Prove that if there exists a function $f^{-1} : Y \to X$ such that $f \circ f^{-1} = \mathrm{id}_Y$, then f is surjective.

Exercise 1.10.7. Let $f : X \to Y$ be any function between any two sets X and Y.

(a.) Prove that $V \subseteq f^{-1}(f(V))$ for any set $V \subseteq X$.

(b.) Exhibit sets $V \subseteq X$ and Y and a function $f : X \to Y$ such that $f^{-1}(f(V)) \not\subseteq V$.
(**Hint:** By Proposition 1.1.1, $f : X \to Y$ cannot be injective.)

(c.) Prove that $f(f^{-1}(W)) \subseteq W$ for any set $W \subseteq Y$.

(d.) Exhibit sets X and $W \subseteq Y$ and a function $f : X \to Y$ such that $W \not\subseteq f(f^{-1}(W))$.
(**Hint:** By Proposition 1.1.1, $f : X \to Y$ cannot be surjective.)

Exercise 1.10.8. Let $f : X \to Y$ be any function between any two sets X and Y.

(a.) Prove that if $f^{-1}(f(V)) = V$ for any set $V \subseteq X$, then f is injective.
(**Hint:** If $f(x_1) = f(x_2)$, then consider the set $V = \{x_1\}$.)

(b.) Prove that if $f(f^{-1}(W)) = W$ for any set $W \subseteq Y$, then f is surjective.
(**Hint:** Consider the set $W = Y$; then, use the definition of $f(f^{-1}(W))$.)

1.10.2 Logic and Truth Tables

Exercise 1.10.9. Let P be the statement that "The sun is shining in Kansas City." Let Q be the statement that "Bob rides his bike to work." Use the letters P and Q and logical connectives such as $\implies$, $\iff$, $\vee$, $\wedge$, and $\neg$ to convert each of the following statements into symbols; then, identify all of the logically equivalent statements, tautologies, and self-contradictions.

(a.) "If the sun is shining in Kansas City, then Bob rides his bike to work."

(b.) "Bob rides his bike to work only if the sun is shining in Kansas City."

(c.) "Either the sun is not shining in Kansas City or Bob rides his bike to work."

(d.) "The sun is shining in Kansas City, and Bob does not ride his bike to work."

(e.) "If the sun is not shining in Kansas City, then Bob does not ride his bike to work."

(f.) "If Bob does not ride his bike to work, then the sun is not shining in Kansas City."

(g.) "Neither the sun is shining in Kansas City nor Bob rides his bike to work."

(h.) "Either the sun is not shining in Kansas City or Bob does not ride his bike to work."

(i.) "The sun is not shining in Kansas City, and Bob does not ride his bike to work."

(j.) "Either Bob rides his bike to work or Bob does not ride his bike to work."

(k.) "The sun is shining in Kansas City, and the sun is not shining in Kansas City."

(l.) "Bob rides his bike to work if and only if the sun is shining in Kansas City."

(m.) "The sun is not shining in Kansas City if and only if Bob does not ride his bike to work."

Exercise 1.10.10. Let P, Q, and R be any statements. Construct a truth table to prove that the statements "If P, then Q or R" and "If P and not Q, then R" are logically equivalent.

Exercise 1.10.11. Let P and Q be any statements. Construct a truth table to prove that the statement "If P or Q but not Q, then P" is a tautology.

Exercise 1.10.12. Use Exercise 1.10.11 to prove that if Bob placed in the top two in a cycling race on Saturday, but he did not place second, then Bob must have placed first.

Exercise 1.10.13. Use a proof by contradiction to prove that if Bob placed in the top two in a cycling race on Saturday, but he did not place second, then Bob must have placed first. Cite any theorems or laws of inference (by name) that you use in your proof.

1.10.3 Sets and Set Operations, Revisited

Exercise 1.10.14. (De Morgan's Laws for Sets) Let $X \subseteq W$ and $Y \subseteq W$ be arbitrary sets.

(a.) Prove that $W \setminus (X \cup Y) = (W \setminus X) \cap (W \setminus Y)$.

(b.) Prove that $W \setminus (X \cap Y) = (W \setminus X) \cup (W \setminus Y)$.

(**Hint:** Define statements P and Q for which $P \vee Q$ is the statement that "$w \in X \cup Y$" and $P \wedge Q$ is the statement that "$w \in X \cap Y$"; then, use De Morgan's Laws to conclude the results.)

Exercise 1.10.15. Let $X_1, X_2, \ldots, X_n \subseteq W$ be arbitrary sets.

(a.) Prove that $W \setminus (X_1 \cup X_2 \cup \cdots \cup X_n) = (W \setminus X_1) \cap (W \setminus X_2) \cap \cdots \cap (W \setminus X_n)$.

(b.) Prove that $W \setminus (X_1 \cap X_2 \cap \cdots \cap X_n) = (W \setminus X_1) \cup (W \setminus X_2) \cup \cdots \cup (W \setminus X_n)$.

(**Hint:** De Morgan's Laws for Sets guarantee that if $w \in W$ and $w \notin X_1 \cup X_2 \cup \cdots \cup X_n$, then it must be that $w \notin X_1$ and $w \notin X_2 \cup X_3 \cup \cdots \cup X_n$. Repeat this process finitely many times.)

Exercise 1.10.16. Let $\mathbb{Z}$ denote the set of integers.

(a.) Provide a partition of $\mathbb{Z}$ into three sets.

(**Hint:** By the Division Algorithm, if we divide any integer by 3, what are the only possible remainders? Use this observation to construct a partition of $\mathbb{Z}$ into three sets.)

(b.) Provide a partition of $\mathbb{Z}$ into four sets.

(c.) Provide a partition of $\mathbb{Z}$ into n sets for any positive integer n.

1.10.4 Equivalence Relations and Partial Orders

Exercise 1.10.17. Consider the set W consisting of all words in the English language.

(a.) Prove that $R = \{(v, w) \in W \times W \mid v \text{ and } w \text{ begin with the same letter}\}$ is an equivalence relation on W; then, determine the number of distinct equivalence classes of W modulo R.

(b.) Prove that $R = \{(v, w) \in W \times W \mid v \text{ and } w \text{ have the same number of letters}\}$ is an equivalence relation on W; then, describe the equivalence class of the word "awesome."

Exercise 1.10.18. Let $\mathbb{Z}$ be the set of integers. Prove that $(a, b) \sim (c, d)$ if and only if $ad = bc$ on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is an equivalence relation. Describe the collection of distinct equivalence classes.

(**Hint:** For the second part of the problem, try replacing the notation (a, b) with a/b, instead.)

Exercise 1.10.19. Let X be an arbitrary set. Consider the collection $S = \{Y \mid Y \subseteq X\}$. Prove that the inclusion $\subseteq$ defines a partial order P on S such that $(Y_1, Y_2) \in P$ if and only if $Y_1 \subseteq Y_2$; then, either prove that P is a total order on S, or provide a counterexample to show that it is not.

Exercise 1.10.20. List the maximal elements of the subset $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of the set $\mathbb{Z}_{\geq 0}$ of non-negative integers with respect to the partial order D of divisibility.

(**Hint:** List as many pairs of comparable elements of S as necessary to compute the chains in S with three or four elements; then, use this information deduce the maximal elements of S.)

1.10.5 The Principle of Mathematical Induction

Exercise 1.10.21. Prove Conjecture 1.5.2 using the Principle of Ordinary Induction.

Exercise 1.10.22. Prove Conjecture 1.5.4 using the Principle of Ordinary Induction.

If X is an arbitrary set, then the **power set** of X is the set $P(X) = \{Y \mid Y \subseteq X\}$, i.e., it is the collection of all subsets of X. Explicitly, if $X = \{x, y\}$, then $P(X) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

Exercise 1.10.23. Let X be an arbitrary finite set with power set $P(X)$.

(a.) Use ordinary induction on $n = |X|$ to prove that $|P(X)| = 2^{|X|}$.

(b.) Let 2^X denote the collection of all functions $f : X \to X$. Exhibit an explicit bijection between $P(X)$ and 2^X; then, conclude from part (a.) above that $|2^X| = 2^{|X|}$.

One of the most curious objects in mathematics is the sequence $(F_n)_{n\geq 0}$ of **Fibonacci numbers** that are defined recursively by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$. We refer to F_n as the nth Fibonacci number. Quite astoundingly, the Fibonacci numbers appear abundantly in nature.

Exercise 1.10.24. Let F_n denote the nth Fibonacci number.

(a.) Prove that $F_n < 2^n$ for each integer $n \geq 0$.

(b.) Prove that $F_{n+1}F_{n-1} = F_n^2 + (-1)^n$ for each integer $n \geq 2$.

(c.) Prove that $\gcd(F_n, F_{n+1}) = 1$ for all integers $n \geq 0$.

Exercise 1.10.25. Prove that the Principle of Ordinary Induction and the Principle of Complete Induction are equivalent to one another by completing the following two steps.

(1.) Given any statement $P(n)$ involving a non-negative integer n, let $Q(n)$ be the statement that $P(k)$ holds for all integers $1 \leq k \leq n$. Use the Principle of Ordinary Induction to prove that the statement $Q(n)$ is true for all integers $n \geq 0$, hence $P(n)$ is true for all integers $n \geq 0$. Unravelling this shows that ordinary induction implies complete induction.

(**Hint:** Observe that $Q(0)$ is vacuously true, hence we may assume that $Q(n)$ is true. By definition, this means that $P(k)$ is true for all integers $1 \leq k \leq n$. What about $P(n+1)$?)

(2.) Given any statement $P(n)$ involving a non-negative integer n, let $Q(n)$ be the statement that $P(k)$ holds for some integer $1 \leq k \leq n$. Use the Principle of Complete Induction to prove that the statement $Q(n)$ is true for all integers $n \geq 0$, hence $P(n)$ is true for all integers $n \geq 0$. Unravelling this shows that complete induction implies strong induction.

(**Hint:** Observe that $Q(0)$ is vacuously true, hence we may assume that $Q(k)$ is true for all integers $1 \leq k \leq n$; in particular, $P(1)$ is true. What does this say about $Q(n+1)$?)

Exercise 1.10.26. Prove that the Well-Ordering Principle and the Principle of Ordinary Induction are equivalent to one another by completing the following three steps.

(1.) Prove that 0 is the smallest non-negative integer with respect to $\leq$.

(2.) Prove that if $S \subseteq \mathbb{Z}_{\geq 0}$ satisfies $0 \in S$ and $n + 1 \in S$ whenever $n \in S$, then $\mathbb{Z}_{\geq 0} \subseteq S$.

(3.) Conclude that the Well-Ordering Principle implies the Principle of Ordinary Induction; then, use Exercise 1.10.25 and the proof of the Well-Ordering Principle to conclude that the Principle of Ordinary Induction implies the Well-Ordering Principle.

1.10.6 The Division Algorithm

Exercise 1.10.27. Recall that a positive integer p is **prime** if and only if the only integers that divide p are $\pm p$ and 1. Prove that if a and b are any integers such that $p \mid ab$, then $p \mid a$ or $p \mid b$.

(**Hint:** We may assume that $p \nmid a$ and show that $p \mid b$; now, use Bézout's Identity.)

Exercise 1.10.28. Let a, b, and c be any integers. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Exercise 1.10.29 (Fundamental Theorem of Arithmetic)**.** Let a be a positive integer. Prove that

(a.) there exist (not necessarily distinct) prime numbers $p_1, \ldots, p_k$ such that $a = p_1 \cdots p_k$ and

(b.) the primes $p_1, \ldots, p_k$ are unique in the sense that if $a = q_1 \ldots q_\ell$, then we must have that $\ell = k$ and $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_k\}$ (i.e., $q_1, \ldots, q_k$ are just a rearrangement of $p_1, \ldots, p_k$).

(**Hint:** Consider the collection N of positive integers that do *not* possess such a prime factorization. Use the Well-Ordering Principle to show that if N is nonempty, then there exists a smallest element n with respect to $\leq$. What can be said about the factors of n? Conclude that N must be empty, hence the existence is established. On the matter of uniqueness, proceed by induction on k.)

Exercise 1.10.30. Let a be any positive integer. Prove that there exist distinct prime numbers $p_1, \ldots, p_n$ and unique non-negative integers $e_1, \ldots, e_n$ such that $a = p_1^{e_1} \ldots p_n^{e_n}$.

Given any integers a and b, the **least common multiple** $\operatorname{lcm}(a, b)$ of a and b can be defined in a manner analogous to the greatest common divisor of a and b. Explicitly, we say that an integer m is a **multiple** of a if and only if $a \mid m$. Consequently, m is a **common multiple** of a and b if and only if $a \mid m$ and $b \mid m$; a least common multiple of a and b is an integer $\ell = \operatorname{lcm}(a, b)$ such that

(a.) $a \mid \ell$ and $b \mid \ell$, i.e., ℓ is a common multiple of a and b and

(b.) if ℓ' is any common multiple of a and b, then $\ell \mid \ell'$.

Exercise 1.10.31. Prove that the $\operatorname{lcm}(a, b)$ is unique.

By the Fundamental Theorem of Arithmetic, for any positive integers a and b, there exist prime numbers $p_1, \ldots, p_k$ and unique non-negative integers $e_1, \ldots, e_k, f_1, \ldots, f_k$ such that $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$. Consider these prime factorizations of a and b for the next three exercises.

Exercise 1.10.32. Prove that $\gcd(a, b) = p_1^{\min\{e_1, f_1\}} \cdots p_k^{\min\{e_k, f_k\}}$.

Exercise 1.10.33. Prove that $\operatorname{lcm}(a, b) = p_1^{\max\{e_1, f_1\}} \cdots p_k^{\max\{e_k, f_k\}}$.

Exercise 1.10.34. Conclude from Exercises 1.10.32 and 1.10.33 that $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.

1.10.7 The Integers Modulo n

Exercise 1.10.35. Complete the following using modular arithmetic.

(a.) If $a \equiv 1 \pmod 6$, find the least positive x for which $5a + 4 \equiv x \pmod 6$.

(b.) If $a \equiv 4 \pmod 7$ and $b \equiv 5 \pmod 7$, find the least positive x for which $6a - 3b \equiv x \pmod 7$.

(c.) (Modular Exponentiation) Use the fact that $2^{2022} \equiv 4 \pmod{10}$ to find $2022^{2022} \pmod{10}$.

Exercise 1.10.36. Consider the collection $\mathbb{Z}_n$ of equivalence classes of the integers modulo n. If $ab \equiv 0 \pmod{n}$, must it be true that $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$? Explain.

Exercise 1.10.37. Let p be any prime number. Consider the collection $\mathbb{Z}_p$ of equivalence classes of the integers modulo p. Prove that if $ab \equiv 0 \pmod{p}$, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Exercise 1.10.38. Let p be any prime number. Consider the collection $\mathbb{Z}_p$ of equivalence classes of the integers modulo p. Prove that $[a]$ admits a multiplicative inverse if and only if $p \nmid a$.

1.10.8 Rigid Motions

Exercise 1.10.39. Prove that for a regular n-gon, there are at most $n! = n(n-1)(n-2)\cdots 2 \cdot 1$ symmetries corresponding to rotation through an angle or reflection across a vertex.

Exercise 1.10.40. List all permutations of the integers $\{1, 2, 3, 4\}$ corresponding to the rotations and reflections of a regular 4-gon. Conclude that the upper bound of Exercise 1.10.39 can be strict.

(**Caution:** Because there are an even number of vertices of the square, only two of the symmetry-preserving reflections of the square will pass through a pair of vertices; however, there are other symmetry-preserving reflections of the square that do not correspond to reflection about a vertex.)

Exercise 1.10.41. Conjecture a formula for the number of symmetry-preserving rotations and reflections of a regular n-gon; then, prove that your formula holds.

(**Hint:** Use the example of Section 8, your work from Exercise 1.10.40, and possibly an additional example to spot the pattern and deduce a formula; then, use the Fundamental Counting Principle.)

Exercise 1.10.42. Consider the regular 3-gon of Section 1.8 with vertices labelled 1, 2, and 3 in clockwise order. Let ρ_k denote rotation of the regular 3-gon through an angle of $-120k$ degrees. Explicitly, there are three distinct rotations ρ_1, ρ_2, and ρ_3. Let ϕ_k denote reflection of the regular 3-gon across the vertex k. Explicitly, there are three distinct reflections ϕ_1, ϕ_2, and ϕ_3. Given any elements $x, y \in \{\rho_1, \rho_2, \rho_3, \phi_1, \phi_2, \phi_3\}$, let yx denote the symmetry obtained by first performing x and subsequently performing y. Explicitly, $\phi_\ell \rho_k$ is the operation of first rotating through an angle of $-120k$ degrees and then reflecting about the vertex ℓ of the original arrangement of the labels 1, 2, and 3. Complete the table below by computing yx according to the rows x and columns y.

$y \backslash x$	ρ_1	ρ_2	ρ_3	ϕ_1	ϕ_2	ϕ_3
ρ_1	ρ_2	ρ_3		ϕ_3		
ρ_2						
ρ_3						
ϕ_1	ϕ_2			ρ_3		
ϕ_2						
ϕ_3						

Chapter 2

Group Theory I

Group theory is the study of algebraic structures equipped with associative binary operations that admit distinguished elements called the multiplicative identity and multiplicative inverses. Even though groups are often relatively tame to describe and possess simple arithmetic, their structure can be surprisingly complex. One of the most significant results in group theory is the development of the so-called solvable groups by the French mathematician Évariste Galois. Using the theory of solvable groups, it is possible to demonstrate that there is no analog to the quadratic formula for polynomials of degree greater than or equal to five. Group theory also appears in the study of coding theory, counting, and symmetries and in applications to biology, chemistry, and physics.

2.1 Groups (Definitions and Examples)

We will assume throughout this chapter that G is a nonempty set. Back in Section 1.1, we defined a **binary operation** on G as a function $* : G \times G \to G$ that sends $(g_1, g_2) \mapsto g_1 * g_2$. We say that G is a **group** with respect to $*$ whenever the following properties hold for the pair $(G, *)$.

(1.) We have that $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ for all elements $g_1, g_2, g_3 \in G$, i.e., $*$ is associative.

(2.) G admits an element $e_G \in G$ such that $e_G * g = g = g * e_G$ for all elements $g \in G$.

(3.) Given any element $g \in G$, there exists an element $g^{-1} \in G$ such that $g * g^{-1} = e_G = g^{-1} * g$.

Example 2.1.1. Let $\mathbb{Z}$ be the set of integers. Observe that (1.) addition of integers is associative; (2.) the integer 0 satisfies that $0 + n = n = n + 0$ for all integers n; and (3.) for any integer n, there exists an integer $-n$ such that $n + (-n) = 0 = -n + n$. Consequently, $(\mathbb{Z}, +)$ is a group. Crucially, we use the usual notation of additive inverses in place of the multiplicative notation above.

Example 2.1.2. Consider the collection $\mathbb{Z}_n$ of equivalence classes of integers modulo n. By Proposition 1.7.1, the distinct elements of $\mathbb{Z}_n$ are given by $r \pmod n$ for each integer $0 \leq r \leq n - 1$, hence it is nonempty. Using modular arithmetic, we may define an associative binary operation $+_n$ on $\mathbb{Z}_n$. Explicitly, we accomplish this by setting $r_1 \pmod n +_n r_2 \pmod n = (r_1 + r_2) \pmod n$. Of course, we may reduce $r_1 + r_2$ modulo n by computing the least non-negative integer x for which $r_1 + r_2 \equiv x \pmod n$; then, we may view $(r_1 + r_2) \pmod n$ as $x \pmod n$, hence $+_n$ is a binary operation on $\mathbb{Z}_n$. Considering that addition of integers is associative, $+_n$ is associative; the identity

element of $\mathbb{Z}_n$ is simply 0 (mod n); and if $1 \leq r \leq n-1$, then the inverse of r (mod n) is simply $(n-r)$ (mod n). Ultimately, this goes to show that $(\mathbb{Z}_n, +_n)$ is a group. Once again, observe that we have used additive notation in place of the multiplicative notation of arbitrary groups.

Example 2.1.3. Consider any regular 3-gon. Let ρ_k denote rotation of the regular 3-gon through an angle of $-120k$ degrees for each integer $1 \leq k \leq 3$. Let ϕ_k denote reflection of the regular 3-gon across the vertex k for each integer $1 \leq k \leq 3$. Consider the set $D_3 = \{\rho_1, \rho_2, \rho_3, \phi_1, \phi_2, \phi_3\}$ of symmetry-preserving rotations and reflections of a regular 3-gon. By Exercise 1.10.42, for any pair of elements $x, y \in D_3$, concatenation yx is an associative binary operation on D_3. Even more, we have that ρ_3 satisfies that $x\rho_3 = x = \rho_3 x$ for all elements $x \in D_3$, hence ρ_3 is the multiplicative identity of D_3; the rotations ρ_1 and ρ_2 are multiplicative inverses of one another; and the reflection ϕ_k is its own multiplicative inverse for each integer $1 \leq k \leq 3$. Consequently, we conclude that D_3 is a group under concatenation: it is typically called the **dihedral group** of order $6 = 2 \cdot 3$.

We say that a group $(G, *)$ is **abelian** if it holds that $g_1 * g_2 = g_2 * g_1$ for all elements $g_1, g_2 \in G$.

Example 2.1.4. Observe that the group $(\mathbb{Z}, +)$ is abelian because addition of integers is commutative. Likewise, for any elements r_1 (mod n) and r_2 (mod n) of $\mathbb{Z}_n$, we have that

$$r_1 \text{ (mod } n) +_n r_2 \text{ (mod } n) = (r_1 + r_2) \text{ (mod } n) = (r_2 + r_1) \text{ (mod } n) = r_2 \text{ (mod } n) +_n r_1 \text{ (mod } n).$$

Consequently, the group $(\mathbb{Z}_n, +_n)$ is abelian, as well. By Exercise 1.10.42, on the other hand, the group D_3 of Example 2.1.3 is not abelian because we have that $\rho_1\phi_1 = \phi_3 \neq \phi_2 = \phi_1\rho_1$.

Example 2.1.5. Let $\mathbb{R}$ be the set of real numbers. Given any positive integer n, let $\mathbb{R}^{n\times n}$ denote the collection of all $n \times n$ real matrices. Under matrix addition, $\mathbb{R}^{n\times n}$ forms a group: the identity element of $\mathbb{R}^{n\times n}$ is the $n \times n$ zero matrix $O_{n\times n}$, and the inverse of an $n \times n$ real matrix A is the real matrix $-A$ whose (i,j)th entry is simply the (i,j)th entry of A with the opposite sign. Considering that addition of real numbers is commutative, it follows that $(\mathbb{R}^{n\times n}, +)$ is abelian.

Even more, let $\mathrm{GL}(n, \mathbb{R})$ denote the subset of $\mathbb{R}^{n\times n}$ consisting of invertible $n \times n$ matrices. Under matrix multiplication, $\mathrm{GL}(n, \mathbb{R})$ forms a group: the multiplicative identity of $\mathrm{GL}(n, \mathbb{R})$ is the $n \times n$ identity matrix $I_{n\times n}$, and the multiplicative inverse of an invertible $n \times n$ matrix A is A^{-1}. Considering that matrix multiplication is not commutative, $(\mathrm{GL}(n, \mathbb{R}), \cdot)$ is not abelian. We refer to this multiplicative group as the **general linear group** of size n over the field $\mathbb{R}$.

We refer to the cardinality of the underlying set defining a group as the **order** of the group. Observe that the additive group $(\mathbb{Z}_n, +_n)$ of the integers modulo n has order $|\mathbb{Z}_n| = n$, and the dihedral group $(D_3, \circ)$ of order six has order $|D_3| = 6$. On the other hand, the additive groups $(\mathbb{Z}, +)$ of integers and $(\mathbb{R}^{n\times n}, +)$ of real $n \times n$ matrices and the multiplicative group $(\mathrm{GL}(n, \mathbb{R}), \cdot)$ of real invertible $n \times n$ matrices have infinitely many elements, hence they each possess infinite order.

Remark 2.1.6. Unfortunately, even if a nonempty set G admits some associative binary operation $*$, it is not always true that $(G, *)$ is a group. Explicitly, multiplication of integers is an associative binary operation on the integers, and the integer 1 satisfies that $n \cdot 1 = n = 1 \cdot n$ for all integers n; however, the integer 0 admits no multiplicative inverse because it always holds that $n \cdot 0 = 0$, and it does not hold that $0 = 1$. Even if we consider the set $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ with respect to integer multiplication, we do not obtain a group because an integer n admits a multiplicative inverse n^{-1} in $\mathbb{Z}^*$ if and only if $n \cdot n^{-1} = 1$ if and only if $n^{-1} = \frac{1}{n}$ is an integer if and only if $n = \pm 1$.

2.2 Groups (Basic Properties and Subgroups)

We will continue to assume throughout this section that $(G, *)$ is a group, i.e., G is a nonempty set and $* : G \times G \to G$ is an associative binary operation with respect to which

(1.) G admits an element $e_G \in G$ such that $e_G * g = g = g * e_G$ for all elements $g \in G$ and

(2.) for each element $g \in G$, there exists an element $g^{-1} \in G$ such that $g * g^{-1} = e_G = g^{-1} * g$.

Our primary objective here is to explore some immediate properties and to illuminate the basic structure of groups. We begin by establishing the uniqueness of the identity and inverses.

Proposition 2.2.1. *If $(G, *)$ is a group, then the element e_G of property (1.) above is unique. Even more, for each element $g \in G$, the element $g^{-1} \in G$ of property (2.) above is unique.*

Proof. We must show that if e is any element of G with the property that $e * g = g = g * e$ for all elements $g \in G$, then $e = e_G$. Crucially, if this holds, then $e * e_G = e_G = e_G * e$ by assumption and $e_G * e = e$ by definition of e_G. But this implies that $e = e_G * e = e * e_G = e_G$, as desired.

Likewise, we must show that if h is any element of G with the property that $g * h = e_G = h * g$, then $h = g^{-1}$. Considering that $*$ is associative and $g^{-1} * g = e_G$, it follows that

$$h = e_G * h = (g^{-1} * g) * h = g^{-1} * (g * h) = g^{-1} * e_G = g^{-1}. \qquad \square$$

Consequently, we refer to the element e_G of property (1.) above as the (multiplicative) **identity element** of G and to the element g^{-1} of property (2.) above as the (multiplicative) **inverse** of g. Our next result greatly simplifies the task of finding multiplicative inverses.

Corollary 2.2.2. *If g is an element of a group $(G, *)$ and $g * h = e_G$, then $h * g = e_G$ and $h = g^{-1}$.*

Proof. By Proposition 2.2.1, it suffices to prove that $h * g = e_G$. By hypothesis that $g * h = e_G$, it follows that $(h * g) * (h * g) = h * (g * h) * g = h * e_G * g = h * g$. Consequently, multiplying both sides of the above identity $(h * g) * (h * g) = h * g$ by $(h * g)^{-1}$ yields the result. $\square$

Usually, we will omit the operation $*$ of G and simply use concatenation, e.g., we will write $g_1 * g_2$ as $g_1 g_2$. By definition of a binary operation, for every pair of elements $g_1, g_2 \in G$, the product $g_1 g_2$ lies in G. Consequently, by property (2.) above, $g_1 g_2$ must have a multiplicative inverse.

Proposition 2.2.3. *If G is a group, then $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$ and $(g_1^{-1})^{-1} = g_1$ for all $g_1, g_2 \in G$.*

Proof. By Corollary 2.2.2, it suffices to verify that $(g_1 g_2)(g_2^{-1} g_1^{-1}) = e_G$ and $g_1^{-1} g_1 = e_G$. $\square$

Existence of multiplicative inverses implies that every group possesses the **cancellation property**, i.e., if $g_1 g_2 = g_1 g_3$ for any elements $g_1, g_2, g_3 \in G$, then it must be the case that $g_2 = g_3$. Likewise, an identity $g_1 g_3 = g_2 g_3$ implies that $g_1 = g_2$. Often, we will invoke this property by using the expression "cancel on both sides" instead of saying "multiply both sides by the inverse."

Given any element $g \in (G, *)$ and any positive integer n, we may define the n-fold powers

$$g^n = \underbrace{g * g * \cdots * g}_{n \text{ times}} \text{ and } g^{-n} = \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{n \text{ times}}$$

of g, and we adopt the convention that $g^0 = e_G$. Under these identifications, we have the following.

Proposition 2.2.4 (Group Exponent Laws)**.** *Let G be a group. Let m and n be any integers.*

(1.) *We have that $g^m g^n = g^{m+n}$ for any element $g \in G$.*

(2.) *We have that $(g^m)^n = g^{mn}$ for any element $g \in G$.*

(3.) *If G is abelian, then $(g_1 g_2)^n = g_1^n g_2^n$ for all elements $g_1, g_2 \in G$.*

We leave the proofs of the Group Exponent Laws as Exercise 2.8.17. Often, we reserve the additive notation for abelian groups, hence in this case, the result is clear because

$$ng = \underbrace{g + g + \cdots + g}_{n \text{ times}} \text{ and } -ng = \underbrace{(-g) + (-g) + \cdots + (-g)}_{n \text{ times}}.$$

Given any nonempty set $H \subseteq G$, we say that H is a **subgroup** of G whenever $(H, *)$ is itself a group. Even more, if H is a nonempty proper subset of G, then $(H, *)$ is called a **proper subgroup** of G in this case. Every group admits a subgroup consisting solely of its identity element $\{e_G\}$; we refer to this as the **trivial subgroup** of G. Generally, though, there are other proper subgroups.

Example 2.2.5. Let $(\mathbb{Z}, +)$ be the abelian group of integers under addition. Given any integer n, consider the collection $n\mathbb{Z} = \{nk \mid k \text{ is an integer}\}$ of integer multiples of n. We can readily verify that $(n\mathbb{Z}, +)$ is a subgroup of $\mathbb{Z}$. Explicitly, the additive identity $0 = n \cdot 0$ lies in $n\mathbb{Z}$, and for any pair of integers k and ℓ, we have that $nk + n\ell = n(k + \ell)$ lies in $n\mathbb{Z}$, hence addition constitutes an associative binary operation on $n\mathbb{Z}$. Observe that the additive inverse of nk is $-nk = n(-k)$.

Example 2.2.6. Consider the dihedral group $D_3 = \{\rho_1, \rho_2, \rho_3, \phi_1, \phi_2, \phi_3\}$ consisting of the symmetry-preserving rotations and reflections of a regular 3-gon. Observe that $(\rho_1) = \{\rho_1, \rho_2, \rho_3\}$ is a subgroup of D_3 with respect to concatenation. Explicitly, we have that $\rho_j \rho_i = \rho_{i+j \pmod 3}$, hence every element of (ρ_1) has a multiplicative inverse in (ρ_1), and concatenation is an associative binary operation on (ρ_1). Even more, ρ_3 is the multiplicative identity of D_3, so it is the multiplicative identity of (ρ_1).

Example 2.2.7. Consider the general linear group $\mathrm{GL}(n, \mathbb{R})$ of size n over the field $\mathbb{R}$. Considering that $\det(AB) = \det(A)\det(B)$ for all $n \times n$ matrices, it follows that the subset

$$\mathrm{SL}(n, \mathbb{R}) = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det(A) = 1\}$$

of $\mathrm{GL}(n, \mathbb{R})$ inherits the associative binary operation of matrix multiplication. By definition, every element of $\mathrm{SL}(n, \mathbb{R})$ has a multiplicative inverse, and the $n \times n$ identity matrix is the multiplicative identity of $\mathrm{SL}(n, \mathbb{R})$, hence it is a subgroup of $\mathrm{GL}(n, \mathbb{R})$ called the **special linear group**.

Remark 2.2.8. We cannot understate the importance of context when discussing the structure of groups and subgroups. Like we mentioned in Remark 2.1.6, a nonempty set with an associative binary operation need not be a group — even if it possesses a multiplicative identity. Likewise, a nonempty subset of a group is not necessarily a subgroup. Crucially, a subgroup must inherit the same binary operation as the group in which it is contained. Observe that the group $(\mathbb{R}^{n \times n}, +)$ of $n \times n$ real matrices contains $\mathrm{GL}(n, \mathbb{R})$ as a subset; however, $\mathrm{GL}(n, \mathbb{R})$ is not a subgroup of $\mathbb{R}^{n \times n}$ because the sum of two invertible matrices is not necessarily invertible. Even more, $\mathbb{R}^{n \times n}$ is not a group with respect to matrix multiplication because not all $n \times n$ matrices are invertible.

Often, it is convenient to use the following proposition and its two corollary to determine when a (nonempty) subset of a group itself constitutes a group with respect to the operation of the group.

Proposition 2.2.9 (Subgroup Test)**.** *Let $(G, *)$ be a group, and let H be any subset of G. We have that $(H, *)$ is a subgroup of G if and only if the following three conditions hold.*

(1.) *H contains the identity element e_G of G.*

(2.) *We have that $h_1 * h_2 \in H$ for all elements $h_1, h_2 \in H$.*

(3.) *We have that $h^{-1} \in H$ for all elements $h \in H$.*

Proof. Certainly, if the above three conditions hold for H, then in order to establish that $(H, *)$ is a group, we need only verify that $*$ is associative. But this holds by viewing H as a subset of G.

Conversely, suppose that $(H, *)$ is a subgroup of G. Condition (2.) holds because H is itself a group, hence it suffices to check that conditions (1.) and (3.) are satisfied. By assumption that H is a group, it admits an identity element e_H. Observe that as elements of G, we have that $e_H e_H = e_H = e_H e_G$. Cancellation on the left yields that $e_H = e_G$, as desired. Last, for all elements $h \in H$, there exists a unique element $h' \in H$ such that $hh' = e_H = h'h$. Considering that $e_H = e_G$, it follows that $hh' = e_G$, hence Proposition 2.2.2 yields that $h' = h^{-1}$ lies in H. □

Corollary 2.2.10 (Two-Step Subgroup Test)**.** *Given a group $(G, *)$ and a nonempty set $H \subseteq G$, we have that $(H, *)$ is a subgroup of G if and only if*

(1.) *we have that $h_1 * h_2 \in H$ for all elements $h_1, h_2 \in H$ and*

(2.) *we have that $h^{-1} \in H$ for all elements $h \in H$.*

Proof. Clearly, if $(H, *)$ is a subgroup of G, then the stated properties of H must hold. Conversely, if we assume that the second and third conditions of the Subgroup Test hold, then the first condition holds because we have that $e_G = h * h^{-1}$ lies in H for all elements $h \in H$ and H is nonempty. □

Corollary 2.2.11 (One-Step Subgroup Test)**.** *Given a group $(G, *)$ and a nonempty set $H \subseteq G$, we have that $(H, *)$ is a subgroup of G if and only if $h_1 * h_2^{-1} \in H$ for all elements $h_1, h_2 \in H$.*

Proof. Once again, if $(H, *)$ is a subgroup of G, then the stated property of H must hold. Conversely, by the Subgroup Test, it suffices to demonstrate that the following conditions holds.

(1.) H contains the identity element e_G of G.

(2.) We have that $h_1 * h_2 \in H$ for all elements $h_1, h_2 \in H$.

(3.) We have that $h^{-1} \in H$ for all elements $h \in H$.

We verify condition (1.) by noting that $e_G = h_1 h_1^{-1}$ is in H for any element $h_1 \in H$. Consequently, condition (3.) follows because $h^{-1} = e_G h^{-1}$ for all elements $h \in H$ and $e_G \in H$. Last, condition (2.) holds by using Proposition 2.2.3 and condition (3.) to see that $h_1 * h_2 = h_1 * (h_2^{-1})^{-1} \in H$. □

Each of the above corollaries achieves one more step of reduction from the most tedious Subgroup Test; the most common form that we will use is the One-Step Subgroup Test.

Before we conclude this section, we provide an example to motivate the study of subgroups.

Example 2.2.12. We will soon come to see that like the order of a group, the subgroups admitted by a group provide a concrete way to distinguish that group from other groups of the same order. Consider the groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ with respect to modular addition. Both of these have order four, but we will demonstrate that they are distinct by showing that $\mathbb{Z}_4$ admits only one non-trivial proper subgroup while $\mathbb{Z}_2 \times \mathbb{Z}_2$ admits three non-trivial proper subgroups. If we drop the modulo n notation for this example, the elements of $\mathbb{Z}_4$ are $\{0, 1, 2, 3\}$, and its **Cayley table** is as follows.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

By looking for the additive identity 0 in this table, we find that the only non-trivial subgroup of $(\mathbb{Z}_4, +_4)$ is given by $\{0, 2\}$. On the other hand, the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ admits the following Cayley table.

$(+_2, +_2)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Once again, by looking for the additive identity $(0,0)$ in this table, we find three non-trivial subgroups: they are $\{(0,0),(1,0)\}$, $\{(0,0),(0,1)\}$ and $\{(0,0),(1,1)\}$. Consequently, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are distinct groups of order four; the latter is famously called the **Klein four-group**.

2.3 Cyclic Groups

We begin our stratification of groups based on their structure by studying those groups that are "simplest" in the following sense. Given any group G and any element $g \in G$, we have that g^n lies in G for any integer n. Even more, these elements naturally give rise to a subgroup of G.

Proposition 2.3.1. *Given any group G and any element $g \in G$, the collection $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ of integer powers of g forms a subgroup of G called the* **cyclic subgroup** *generated by g.*

Proof. Certainly, the set $\langle g \rangle$ is nonempty because it contains $g^0 = e_G$. Even more, for any elements $g^m, g^n \in \langle g \rangle$, we have that $g^m(g^n)^{-1} = g^m g^{-n} = g^{m-n}$ by the Group Exponent Laws so that $g^m(g^n)^{-1}$ lies in $\langle g \rangle$. We conclude by the One-Step Subgroup Test that $\langle g \rangle$ is a subgroup of G. □

Example 2.3.2. Consider the dihedral group $D_3 = \{\rho_1, \rho_2, \rho_3, \phi_1, \phi_2, \phi_3\}$ of order six. Observe that the distinct powers of ρ_1 are given by ρ_1, ρ_1^2, and ρ_1^3. Consequently, we have that $\langle \rho_1 \rangle = \{\rho_1, \rho_1^2, \rho_1^3\}$. Considering that $\rho_1^2 = \rho_2$ and $\rho_1^3 = \rho_3$, this is the subgroup of D_3 consisting of all rotations of the regular 3-gon. On the other hand, for any reflection ϕ_k, we have that ϕ_k^2 does not affect any change, hence it is the identity ρ_3. Put another way, we have that $\langle \phi_k \rangle = \{\phi_k, \rho_3\}$ for each integer $1 \leq k \leq 3$.

Using additive notation, the cyclic subgroup generated by an element g of an abelian group $(G, +)$ is simply $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$. We have unwittingly already encountered such groups.

Example 2.3.3. Observe that for any integer n, the cyclic subgroup of $(\mathbb{Z}, +)$ generated by n is given by $n\mathbb{Z} = \{qn \mid q \in \mathbb{Z}\} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$, i.e., the collection of multiples of n.

Remark 2.3.4. If H is a subgroup of G that contains some element $g \in G$, then H contains the cyclic subgroup $\langle g \rangle$ because it contains all powers of g by the second property of the Subgroup Test. Consequently, the cyclic subgroup $\langle g \rangle$ is in this sense the "smallest" subgroup of G that contains g.

We will say that G is a **cyclic group** if it admits an element $g \in G$ such that $G = \langle g \rangle$. Like we have mentioned before, we will say in this case that g is a **generator** of G. By definition, the order of the cyclic subgroup $\langle g \rangle$ is the (possibly infinite) number of distinct elements of $\langle g \rangle$. If it happens that $\langle g \rangle$ is finite, then the **order** of g is the smallest positive integer $r = \text{ord}(g)$ such that $g^r = e_G$. Consequently, the distinct elements of $\langle g \rangle$ are $g^0, g^1, \dots, g^{r-1}$ so that $\text{ord}(g) = \#\langle g \rangle$.

Example 2.3.5. Every nonzero element of the additive group of integers $(\mathbb{Z}, +)$ has infinite order. Even more, every integer n can be written as $n \cdot 1$ or $(-n)(-1)$, hence we have that $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. On the other hand, the subgroups $n\mathbb{Z}$ are proper for all integers n such that $|n| \geq 2$.

Example 2.3.6. Consider the abelian group $(\mathbb{Z}_{10}, +_{10})$ of equivalence classes of $\mathbb{Z}$ modulo 10 with respect to addition modulo 10. Observe that $\langle 5 \rangle = \{0, 5\}$, hence we have that $\text{ord}(5) = 2$. On the other hand, we have that $\langle 1 \rangle = \{0, 1, 2, \dots, 9\} = \langle 9 \rangle$, hence both 1 and 9 generate $(\mathbb{Z}_{10}, +_{10})$.

Example 2.3.7. Consider the dihedral group $D_3 = \{\rho_1, \rho_2, \rho_3, \phi_1, \phi_2, \phi_3\}$ of order six. By Example 2.3.2 and Exercise 1.10.42, every subgroup of D_3 is cyclic, but D_3 is not itself a cyclic group.

Even more, our next propositions illustrate several important properties of cyclic groups.

Proposition 2.3.8. *Every cyclic group is abelian.*

Proof. If G is cyclic, then G admits an element $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$. Consequently, for any elements $g_1, g_2 \in G$, there exist integers n_1 and n_2 such that $g_1 = g^{n_1}$ and $g_2 = g^{n_2}$. By the Group Exponent Laws, we conclude that $g_1 g_2 = g^{n_1} g^{n_2} = g^{n_1 + n_2} = g^{n_2 + n_1} = g^{n_2} g^{n_1} = g_2 g_1$. □

Corollary 2.3.9. *Groups that are not abelian are not cyclic.*

Proposition 2.3.10. *Every subgroup of a cyclic group is cyclic.*

Proof. We will assume that G is a cyclic group that is generated by some element $g \in G$. Explicitly, we will write that $G = \{g^n \mid n \in \mathbb{Z}\}$. Consider any subgroup $H \subseteq G$. Certainly, if $H = \{e_G\}$, then H is trivially cyclic. Consequently, we may assume that H admits a non-identity element $h \in H$. By hypothesis that G is cyclic, there exists an integer n such that $h = g^n$. By the Two-Step Subgroup Test and the Group Exponent Laws, we must have that $h^{-1} = (g^n)^{-1} = g^{-n}$ lies in H. Considering that h is not the identity element of G, we must have that $n > 0$ or $-n > 0$, so we may assume without loss of generality that $n > 0$. Ultimately, this analysis reveals that the collection $S = \{i \in \mathbb{Z}_{>0} \mid g^i \in H\}$ is nonempty, hence the Well-Ordering Principle ensures that S admits a smallest element s with respect to $\leq$. We will prove in the next paragraph that $H = \langle g^s \rangle$.

Consider any element $k \in H$. By assumption that G is cyclic, there exists an integer m such that $k = g^m$. By the Division Algorithm, there exist unique integers q and r such that $m = qs + r$ and $0 \leq r < s$. Consequently, we have that $k = g^m = g^{qs+r} = g^{qs} g^r$. By multiplying both sides of this identity (on the left) by g^{-qs}, we find that $g^r = g^{-qs} k$ lies in H. But this is impossible unless $r = 0$ because $0 \leq r < s$ and s is the smallest positive integer such that g^s lies in H. We conclude that $m = qs$, and every element of H can be written as $g^{qs} = (g^s)^q$ for some unique integer q. □

Corollary 2.3.11. *Every subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$ for some non-negative integer n.*

By paragraph preceding Example 2.3.5, the order of an element g of a group G is the smallest positive integer $r = \text{ord}(g)$ such that $g^r = e_G$. Our next two results demonstrate that the order of a generator of a cyclic group determines the order of all other elements of the group.

Lemma 2.3.12. *Let G be a cyclic group. If g is generates G, then $g^n = e_G$ if and only if $\text{ord}(g) \mid n$.*

Proof. Certainly, if $\text{ord}(g) \mid n$, then $g^n = e_G$ because there exists an integer q such that $n = \text{ord}(g)q$, and the Group Exponent Laws imply that $g^n = g^{\text{ord}(g)q} = (g^{\text{ord}(g)})^q = e_G^q = e_G$. Conversely, by the Division Algorithm, there exist unique integers q and r such $n = \text{ord}(g)q + r$ and $0 \leq r < \text{ord}(g)$. Observe that if r were nonzero, then it would be a smaller positive integer than $\text{ord}(g)$ with the property that $g^r = e_G^q g^r = (g^{\text{ord}(g)})^q = g^{\text{ord}(g)q} g^r = g^{\text{ord}(g)q+r} = g^n = e_G$ — a contradiction. □

Corollary 2.3.13. *If $g \in G$ has finite order and $g^n = e_G$, then $\text{ord}(g) \mid n$.*

Proof. Every element of G generates a cyclic group $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ of order $\text{ord}(g)$. □

Proposition 2.3.14. *Let G be a cyclic group. If g generates G, then for any integer n, the order of g^n is $\text{ord}(g)/\gcd(n, \text{ord}(g))$.*

Proof. We denote $\text{ord}(g) = d$. By definition, the order of g^n is the smallest positive integer r such that $(g^n)^r = g^{nr} = e_G$ by the Group Exponent Laws. By Corollary 2.3.13, if $g^{nr} = e_G$, then $d \mid nr$, hence r is the smallest positive integer such that $d \mid nr$. Considering that $\gcd(n, d)$ divides both n and d, we seek the smallest positive integer r such that $d/\gcd(n, d)$ divides $nr/\gcd(n, d)$. By Bézout's Identity, the integers $d/\gcd(n, d)$ and $n/\gcd(n, d)$ are relatively prime, hence Exercise 1.10.28 yields that $d/\gcd(n, d)$ divides r so that $r \geq d/\gcd(n, d) > 0$ and $r = d/\gcd(n, d)$. □

We conclude this section with a corollary that determines all generators of a cyclic group.

Corollary 2.3.15. *If G is a cyclic group that is generated by some element $g \in G$, then g^n is a generator of G for all integers n such that $\gcd(n, \text{ord}(g)) = 1$.*

Proof. By Proposition 2.3.14, if n is any integer such that $\gcd(n, \text{ord}(g)) = 1$, then the order of g^n is $\text{ord}(g)$, and this is precisely the order of the entire group G; thus, g^n generates G. □

2.4 Complex Numbers as a Group Under Multiplication

Complex numbers arise naturally out of consideration of the solutions to certain polynomials with real coefficients. Explicitly, if x is a variable, then the quadratic polynomial $x^2 + 1$ does not possess a real root because the square of any real number is non-negative. We may therefore construct a solution i of the polynomial equation $x^2 + 1 = 0$; in this case, it holds that $i^2 = -1$ so that $i = \sqrt{-1}$.

Complex numbers are defined as the collection $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$. Consequently, we may view i itself as a complex number. We refer to the real number a of the complex number $a + bi$ as the **real part** of $a + bi$, and the real number b is the **imaginary part** of $a + bi$. Complex numbers admit a notion of addition that allow us to view $\mathbb{C}$ as the two-dimensional real vector space $\mathbb{C} = \mathbb{R}\langle 1, i \rangle$. Explicitly, we define $(a + bi) + (c + di) = (a + b) + (c + d)i$ according to

usual addition of vectors with respect to a basis. Consequently, the additive identity element of $\mathbb{C}$ is $0+0i$. We may also define multiplication of complex numbers by "foiling" the expression

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i.$$

We note that multiplication of complex numbers is associative, distributive, and commutative because multiplication of real numbers is associative, distributive, and commutative. Even more, one can readily verify that the multiplicative identity of $\mathbb{C}$ is $1+0i$. Last, observe that if a and b are nonzero, then $a+bi$ and $a-bi$ are nonzero, and we have that $(a+bi)(a-bi) = a^2+b^2$. Consequently, it follows that every nonzero complex numbers $a+bi$ admits a multiplicative inverse

$$(a+bi)^{-1} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

We summarize the contents of this section thus far in the following.

Proposition 2.4.1. *Let $\mathbb{C}$ denote the complex numbers. Let $\mathbb{C}^\times = \mathbb{C} \setminus \{0+0i\}$.*

(1.) *We have that $(\mathbb{C}, +)$ is an abelian group under complex addition; the identity is $0+0i$.*

(2.) *We have that $(\mathbb{C}^\times, \cdot)$ is an abelian group under complex multiplication; the identity is $1+0i$.*

We refer to the complex number $a-bi$ as the **complex conjugate** of $a+bi$, and the real number $\sqrt{a^2+b^2} = (a+bi)(a-bi)$ is the **modulus** of $a+bi$. Often, authors throughout the literature will denote $z = a+bi$; its complex conjugate $\bar{z} = a-bi$; and its modulus $|z| = \sqrt{a^2+b^2}$.

Proposition 2.4.2. *Let $z = a+bi$ for some nonzero real numbers a and b.*

(1.) *We have that $|\bar{z}| = |z|$ and $|z|^2 = z\bar{z}$.*

(2.) *We have that $\left|\frac{z}{c}\right| = \frac{|z|}{|c|}$ for all nonzero real numbers c.*

(3.) *We have that $z^{-1} = \frac{\bar{z}}{|z|^2}$ and $|z^{-1}| = \frac{1}{|z|}$.*

Graphically, complex numbers can be realized via their structure as the two-dimensional real vector space $\mathbb{C} = \mathbb{R}\langle 1, i\rangle \cong \mathbb{R} \times \mathbb{R}$. Consequently, the complex number $a+bi$ may be identified with the point (a,b) in the Cartesian plane whose x-axis corresponds to the real part of a complex number and whose y-axis corresponds to the imaginary part of the complex number. Using the polar coordinates interpretation of the Cartesian plane $\mathbb{R} \times \mathbb{R}$, we obtain the polar form for the complex numbers. Explicitly, any ordered pair of real numbers (a,b) can be written as $a = r\cos\theta$ and $b = r\sin\theta$ for some real numbers $r = \sqrt{a^2+b^2}$ and $0 \leq \theta < 2\pi$, hence the complex number $a+bi$ can be written as $r(\cos\theta + i\sin\theta)$ such that r is the modulus of $a+bi$ and $0 \leq \theta < 2\pi$. Often, the most convenient way to express the complex number $r(\cos\theta + i\sin\theta)$ is as $r\,\mathrm{cis}\,\theta$.

Example 2.4.3. Consider the complex number $\sqrt{2}-i\sqrt{2}$. Observe that the modulus of $\sqrt{2}-i\sqrt{2}$ is $r = \sqrt{2+2} = 2$, hence it suffices to find $0 \leq \theta < 2\pi$. By viewing $\sqrt{2}-i\sqrt{2}$ as the point $(\sqrt{2}, -\sqrt{2})$ in the fourth quadrant of the Cartesian plane, we know that $3\pi/2 < \theta < 2\pi$. Even more, there exists an angle $0 < \phi < \pi/2$ such that $\theta = 2\pi - \phi$ and $\tan\phi = 1$. We conclude that $\phi = \arctan(1) = \pi/4$ so that $\theta = 7\pi/4$. Ultimately, we obtain the polar form $\sqrt{2}-i\sqrt{2} = 2\,\mathrm{cis}(7\pi/4)$.

Conversely, if we begin with the polar form of a complex number $\sqrt{3}\,\mathrm{cis}(2\pi/3)$, then unravelling this notation gives that $\sqrt{3}\,\mathrm{cis}(2\pi/3) = \sqrt{3}(\cos(2\pi/3) + i\sin(2\pi/3)) = -\sqrt{3}/2 + 3i/2$.

Even more, the polar representation can be the most efficient way to multiply complex numbers. We leave the proof of the following proposition as Exercise 2.8.42 for the reader.

Proposition 2.4.4. *We have that* $(r_1 \operatorname{cis} \theta_1)(r_2 \operatorname{cis} \theta_2) = r_1 r_2 \operatorname{cis}(\theta_1 + \theta_2)$.

Corollary 2.4.5 (DeMoivre's Theorem)**.** *We have that* $(r \operatorname{cis} \theta)^n = r^n \operatorname{cis}(n\theta)$ *for all integers* $n \geq 0$.

Proof. By the Principle of Ordinary Induction on $n \geq 0$, this follows from Proposition 2.4.4. □

Corollary 2.4.6. *We have that* $|z_1 z_2| = |z_1| \cdot |z_2|$ *for all complex numbers* z_1 *and* z_2.

Corollary 2.4.7. *We have that* $|z^n| = |z|^n$ *for all complex numbers* z *and all integers* n.

Example 2.4.8. One of the benefits of DeMoivre's Theorem is that it makes quick work of exponentiation of complex numbers that would normally require the Binomial Theorem. Explicitly, if we wish to compute $(\sqrt{2} - i\sqrt{2})^7$, then we simply recognize that $\sqrt{2} - i\sqrt{2} = 2 \operatorname{cis}(7\pi/4)$ by Example 2.4.3, and DeMoivre's Formula gives $(\sqrt{2} - i\sqrt{2})^7 = 2^7 \operatorname{cis}(49\pi/4) = 128 \operatorname{cis}(\pi/4) = 64(\sqrt{2} + i\sqrt{2})$.

Consider the set $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. By definition, we have that a complex number z lies in $\mathbb{T}$ if and only if $|z| = 1$ if and only if the Cartesian coordinate representation of z lies in the unit circle. By Corollary 2.4.6, if $|z_1| = 1$ and $|z_2| = 1$, then $|z_1 z_2| = 1$, hence we have that $z_1 z_2$ lies in $\mathbb{T}$ for all elements $z_1, z_2 \in \mathbb{T}$. Even more, if $|z| = 1$, then $|z^{-1}| = 1$ by Proposition 2.4.2, hence z^{-1} lies in $\mathbb{T}$ for all elements $z \in \mathbb{T}$. By the Two-Step Subgroup Test, we conclude the following.

Proposition 2.4.9. *Let* $(\mathbb{C}^\times, \cdot)$ *denote the multiplicative group of complex numbers. We have that* $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ *is a subgroup of* $(\mathbb{C}^\times, \cdot)$ *called the* **circle group**.

Recall that a **root** of a polynomial $a_n x^n + \cdots + a_1 x + a_0$ with complex coefficients $a_0, a_1, \ldots, a_n$ is a complex number z such that $a_n z^n + \cdots + a_1 z + a_0 = 0$. Even though it is a classical theorem of algebra, the following is typically proved using complex analysis. Consequently, we will not attempt in this course to supply any justification ourselves; we will take it for granted.

Theorem 2.4.10 (Fundamental Theorem of Algebra)**.** *Let* n *be a positive integer. Every univariate polynomial of degree* n *with complex coefficients has exactly* n *(not necessarily distinct) roots.*

Consequently, the polynomial equation $z^3 = 1$ has exactly three solutions over the complex numbers. Certainly, one solution is simply $z = 1$; however, the other two solutions have nonzero imaginary part. Explicitly, we may factor $x^3 - 1 = (x - 1)(x^2 + x + 1)$ such that $x^2 + x + 1$ has no real roots because the discriminant $b^2 - 4ac$ of the Quadratic Formula is negative. Generally, for any positive integer n, we refer to the roots of the polynomial $x^n - 1$ as the nth **roots of unity**.

Proposition 2.4.11. *If* n *is a positive integer, then the* n*th roots of unity are* $\operatorname{cis}(2k\pi/n)$ *for each integer* $0 \leq k \leq n - 1$*; they form a cyclic subgroup of the circle group* $\mathbb{T}$.

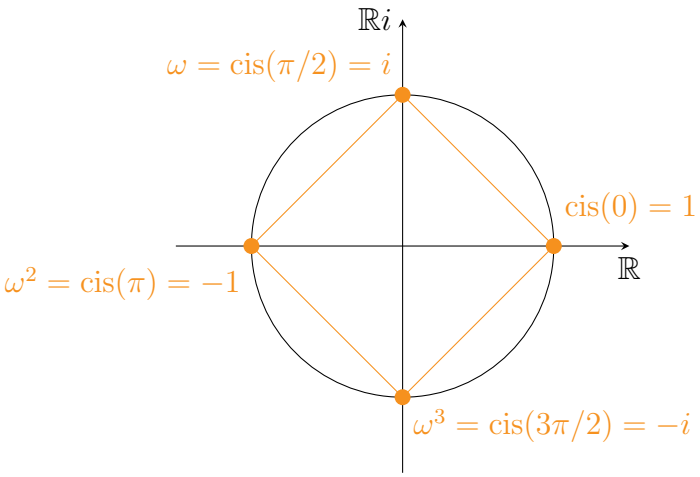
Proof. By the Fundamental Theorem of Algebra, it suffices to prove that $\operatorname{cis}(2k\pi/n)^n = 1$ for each integer $0 \leq k \leq n - 1$ because for any pair of integers $0 \leq i < j \leq n - 1$, we have that $\operatorname{cis}(2i\pi/n)$ and $\operatorname{cis}(2j\pi/n)$ are distinct. Observe that $\operatorname{cis}(2k\pi/n)^n = \operatorname{cis}(2kn\pi/n) = \operatorname{cis}(2k\pi) = 1$ holds by DeMoivre's Theorem. Last, the nth roots of unity form a cyclic subgroup of the circle group $\mathbb{T}$ once again by DeMoivre's Theorem because $\operatorname{cis}(2k\pi/n) = \operatorname{cis}(2\pi/n)^k$ for each integer $0 \leq k \leq n - 1$. □

We refer to a generator of the cyclic subgroup of $\mathbb{T}$ consisting of the nth roots of unity as a **primitive** nth root of unity. By Propositions 2.4.11 and 2.3.15, we obtain the following.

Corollary 2.4.12. *If n is a positive integer, then $\operatorname{cis}(2k\pi/n)$ is a generator for the cyclic subgroup of $\mathbb{T}$ consisting of the nth roots of unity if and only if $\gcd(k,n)=1$. Put another way, if we denote $\omega=\operatorname{cis}(2\pi/n)$, then $\omega^k=\operatorname{cis}(2k\pi/n)$ generates the nth roots of unity if and only if $\gcd(k,n)=1$.*

Pictorially, the nth roots of unity consist of n equally-spaced points on the circumference of the unit circle; the distance between any two consecutive nth roots of unity is given by the angle measure of $2\pi/n$ radians; and a primitive nth root of unity is one for which successive rotation by the angle $2k\pi/n$ generates all of the nth roots of unity on the unit circle after $n-1$ steps.

Example 2.4.13. Below are the fourth roots of unity on the unit circle.



2.5 The Symmetric Group on n Letters

Given a nonempty set X, we may consider the set of bijections from the set X to itself. Conventionally, we use the Fraktur "S" with subscript X to denote this set. Explicitly, we have that $\mathfrak{S}_X=\{f:X\to X\mid f \text{ is injective and surjective}\}$. Certainly, the identity map $\operatorname{id}_X:X\to X$ defined by $\operatorname{id}_X(x)=x$ for every element $x\in X$ is a bijection, hence $\mathfrak{S}_X$ is nonempty. Given any two bijections $f,g:X\to X$, it follows that $f\circ g$ is a bijection from X to itself so that $\mathfrak{S}_X$ is closed with respect to function composition. Composition of functions is associative, so function composition is an associative binary operation on $\mathfrak{S}_X$. Last, for any bijection $f:X\to X$, there exists a unique function $f^{-1}:X\to X$ such that $f\circ f^{-1}=\operatorname{id}_X=f^{-1}\circ f$: indeed, for every element $x\in X$, there exists an element $y\in X$ such that $x=f(y)$ because f is surjective; this element $y\in X$ is unique because f is injective, so we may define $f^{-1}(x)=y$. We conclude therefore that $(\mathfrak{S}_X,\circ)$ is a group. We refer to $\mathfrak{S}_X$ as the **symmetric group on the set** X. Considering that a bijection is by definition a **permutation**, we say that $\mathfrak{S}_X$ the group of permutations of the set X.

Observe that if X is a finite set, then there exists a bijection between X and the set $\{1,2,\ldots,|X|\}$ that maps an element from X uniquely to some element of $\{1,2,\ldots,|X|\}$. Consequently, in order to study the group of permutations of a finite set, we may focus our attention on the permutation groups of the finite sets $[n]=\{1,2,\ldots,n\}$ for all positive integers n. We refer to the group $\mathfrak{S}_{[n]}$ as

the **symmetric group on** n **letters**, and we adopt the shorthand $\mathfrak{S}_n$. Conventionally, the elements of $\mathfrak{S}_n$ are denoted by Greek letters such as sigma σ and tau τ; in particular, the identity function on $\mathfrak{S}_n$ is the Greek letter iota ι. Composition $\sigma \circ \tau$ is typically abbreviated by concatenation $\sigma\tau$, and the product $\sigma\tau$ is read from right to left (and not from left to right), as we are dealing with functions. Our first result concerning the symmetric group on n letters is the following.

Proposition 2.5.1. *We have that* $|\mathfrak{S}_n| = n! = n(n-1)(n-2)\cdots 2 \cdot 1$.

Proof. By definition, the elements of $[n]$ are bijections from $[n]$ to itself. Each bijection $\sigma : [n] \to [n]$ is uniquely determined by the values of $\sigma(1), \sigma(2), \ldots, \sigma(n)$. Consequently, we may construct a bijection from $[n]$ to itself by specifying the value $\sigma(i)$ for each of the integers $1 \leq i \leq n$ in turn. Certainly, there are n distinct choices for the value of $\sigma(1)$. Once this value has been specified, there are $n-1$ distinct choices for the value of $\sigma(2)$ that differ from $\sigma(1)$. Once both $\sigma(1)$ and $\sigma(2)$ have been specified, there are $n-2$ distinct choices for the value of $\sigma(3)$ that differ from both $\sigma(1)$ and $\sigma(2)$. Continuing in this manner, there are $n-i+1$ distinct choices for the value of $\sigma(i)$ that differ from $\sigma(1), \sigma(2), \ldots, \sigma(i-1)$ for each integer $1 \leq i \leq n$. By the Fundamental Counting Principle, there are $\prod_{i=1}^{n}(n-i+1) = n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ distinct bijections from $[n]$ to itself. □

By Exercise 1.10.7, every element σ of $\mathfrak{S}_n$ is uniquely determined by $\sigma(1), \sigma(2), \ldots, \sigma(n)$, hence we may visualize σ as the following $2 \times n$ array by listing $\sigma(i)$ beneath each integer $1 \leq i \leq n$.

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

Using the notation σ^n to denote the composition $\sigma \circ \cdots \circ \sigma$ of σ with itself n times, we have that $\sigma^2(i) = \sigma \circ \sigma(i) = \sigma(\sigma(i))$ for each integer $1 \leq i \leq n$, so we may build upon this array to list the image $\sigma^2(i)$ of $\sigma(i)$ under σ beneath $\sigma(i)$ for each integer $1 \leq i \leq n$ as follows.

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

Continuing in this manner, each of the integers $1 \leq i \leq n$ must eventually appear in the ith column twice because the integers $i, \sigma(i), \sigma^2(i), \ldots, \sigma^n(i)$ cannot all be distinct. Let r_i denote the first row of the ith column for which it holds that $\sigma^{r_i}(i) = i$, i.e., r_i is the smallest positive integer not exceeding n for which the integers $i, \sigma(i), \ldots, \sigma^{r_i-1}(i)$ are all distinct. Observe that the columns of the resulting array allow us to easily read off the consecutive integers $i, \sigma(i), \sigma^2(i), \ldots, \sigma^{r_i-1}(i)$. Considering that $\sigma(\sigma^{r_i-1}(i)) = \sigma^{r_i}(i) = i$, it follows that $i, \sigma(i), \sigma^2(i), \ldots, \sigma^{r_i-1}(i)$ constitute a **cycle**; we will refer to the positive integer r_i as the **length** of the cycle $(i, \sigma(i), \sigma^2(i), \ldots, \sigma^{r_i-1}(i))$, and we will say that the cycle itself is an r_i-cycle. Cycles of length two are commonly called **transpositions**. By definition, the order of a cycle as an element of the permutation group $\mathfrak{S}_n$ is its length, i.e., if σ is an r_i-cycle, then $\mathrm{ord}(\sigma) = r_i$. Conventionally, cycles are written without commas, but we will use them when convenient. We will also say that two cycles $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ are **disjoint** if the entries a_i and b_j are pairwise distinct for all pairs of integers $1 \leq i \leq k$ and $1 \leq j \leq \ell$.

Example 2.5.2. We have already encountered the symmetric group $\mathfrak{S}_3$ on three letters in a different guise. Consider the dihedral group $D_3 = \{\rho_1, \rho_2, \rho_3, \phi_1, \phi_2, \phi_3\}$ of order six whose elements ρ_k are the rotations about an angle of $-120k$ degrees and whose elements ϕ_k are the reflections about the vertex k of a regular 3-gon. Going back to the main example of Section 1.8, we have the following.

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \phi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Considering that $\rho_3(i) = i$ for each integer $1 \leq i \leq 3$, it follows that ρ_3 is the identity element of $\mathfrak{S}_3$. Carrying out the process of the previous paragraph, we obtain the cycles of $\mathfrak{S}_3$. Generally, the identity permutation ι is a cycle of length one; this can be verified here by looking at ρ_3 above. Each of the other above permutations is not a cycle because the entries of some column are distinct. Consequently, we must apply the permutations until each column has a repeated integer.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Consequently, the permutation ρ_1 is the 3-cycle (132); the permutation ρ_2 is the 3-cycle (123); the permutation ϕ_1 is the 2-cycle (23); the permutation ϕ_2 is the 2-cycle (13); and the permutation ϕ_3 is the 2-cycle (12). We will explore this phenomenon when we discuss general dihedral groups. By Exercise 1.10.42, we have that $\phi_1\rho_1 \neq \rho_1\phi_1$, hence the symmetric group is not necessarily abelian.

Example 2.5.3. Consider the following permutation σ in **two-line notation**.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 4 & 1 & 7 & 6 & 3 \end{pmatrix}$$

Computing the disjoint cycles of σ amounts to building upon the above array row-by-row until each of the integers $1 \leq i \leq 8$ appears in the ith column twice. Explicitly, we have the following array.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 4 & 1 & 7 & 6 & 3 \\ 5 & 1 & 3 & 4 & 2 & 6 & 7 & 8 \\ 1 & 2 & 8 & 4 & 5 & 7 & 6 & 3 \end{pmatrix}$$

Consequently, the disjoint cycles of σ are (125), (38), (4), and (67). Even though we have used two-line notation to express most permutations up to this point, it is occasionally most convenient to adopt the **one-line notation** of a permutation σ by specifying all of its disjoint cycles. Explicitly, in one-line notation, we may write $\sigma = (125)(38)(4)(67)$. Cycles are by definition expressed in one-line notation. Even more, our next two propositions demonstrate that it is possible to find the one-line notation of any permutation and that the representation of a permutation as a product of disjoint cycles is unique up to a rearrangement of the non-trivial cycles appearing in the product.

Proposition 2.5.4. *Every permutation can be written as a product of disjoint cycles.*

Proof. Given any permutation σ of $[n]$, observe that the integers $1, \sigma(1), \ldots, \sigma^n(1)$ cannot all be distinct. Consequently, there exists an integer $1 \leq r_1 \leq n-1$ such that $\sigma^{r_1}(1) = 1$; the integers $1, \sigma(1), \ldots, \sigma^{r_1-1}(1)$ are distinct; and $\sigma_1 = (1, \sigma(1), \ldots, \sigma^{r_1-1}(1))$ is a cycle of length r_1. Consider the smallest integer i_2 that does not appear as an entry of σ_1. Once again, the integers $i_2, \sigma(i_2), \ldots, \sigma^n(i_2)$ cannot all be distinct, so there must be an integer $1 \leq r_2 \leq n-1$ such that $\sigma^{r_2}(i_2) = i_2$. Like before, we obtain a cycle $\sigma_2 = (i_2, \sigma(i_2), \ldots, \sigma^{r_2-1}(i_2))$ of length r_2. Crucially, we note that σ_1 and σ_2 are disjoint. Explicitly, if it were the case that $\sigma^i(1) = \sigma^j(i_2)$ for some integers $0 \leq i \leq r_1 - 1$ and $0 \leq j \leq r_2 - 1$, then it would follow that $\sigma^{r_2-j+i}(1) = \sigma^{r_2}(i_2) = i_2$ so that i_2 appears as an entry of σ_1 — a contradiction. Continuing in this manner, we may construct disjoint cycles $\sigma_1, \sigma_2, \ldots, \sigma_k$ such that every element of $[n]$ lies in one and only one cycle and $\sigma = \sigma_1 \cdots \sigma_k$. □

Proposition 2.5.5. *Every pair of disjoint cycles σ and τ commute, i.e., we have that $\sigma\tau = \tau\sigma$.*

Proof. Consider an integer $1 \leq i \leq n$. Crucially, we note that if i is does not appear in the one-line notation of σ, then $\sigma(i) = i$. Considering that σ and τ are disjoint, it follows that $\tau(i)$ cannot be an entry of σ in one-line notation, hence we have that $\sigma\tau(i) = \tau(i) = \tau\sigma(i)$. Consequently, it suffices to consider the case that i appears in the one-line notation of σ. Consider the entry j of σ corresponding to $\sigma(i) = j$ in one-line notation. By assumption that σ and τ are disjoint, neither of the integers i and j can appear as an entry of τ, hence we have that $\tau(i) = i$ and $\tau(j) = j$. We conclude therefore that $\sigma\tau(i) = \sigma(i) = j = \tau(j) = \tau\sigma(i)$. By the Law of the Excluded Middle, every integer $1 \leq i \leq n$ either appears in the one-line notation of σ or not, so our proof is complete. □

Corollary 2.5.6. *Every permutation can be written as a product of disjoint cycles in a manner that is unique up to the arrangement of the disjoint cycles appearing in the product.*

Consequently, we refer to the representation of a permutation σ as a product $\sigma_k \cdots \sigma_2\sigma_1$ of disjoint cycles as the **cycle decomposition** of σ. Because the order of the disjoint cycles does not matter, we will henceforth simplify the notation to $\sigma = \sigma_1 \cdots \sigma_k$. Later, it will be important to note that if the cycles σ_i have length r_i for each integer $1 \leq i \leq k$, then $r_1 + \cdots + r_k = n$ because each of the integers $1, 2, \ldots, n$ appears in one and only one cycle σ_i. We are now able to prove the following.

Proposition 2.5.7. *Let σ be any permutation with cycle decomposition $\sigma_1 \cdots \sigma_k$. Let r_i denote the length of the cycle σ_i. We have that* $\mathrm{ord}(\sigma) = \mathrm{lcm}(r_1, \ldots, r_k)$.

Proof. By Proposition 2.5.5, the disjoint cycles $\sigma_1, \ldots, \sigma_k$ commute, hence we have that

$$\mathrm{ord}(\sigma) = \mathrm{ord}(\sigma_1 \cdots \sigma_k) = \min\{r \geq 1 \,|\, (\sigma_1 \cdots \sigma_k)^r = \iota\} = \min\{r \geq 1 \,|\, \sigma_k^r \cdots \sigma_1^r = \iota\}.$$

We claim that $\sigma_k^r \cdots \sigma_1^r = \iota$ if and only if $\sigma_i^r = \iota$ for each integer $1 \leq i \leq k$. Certainly, if $\sigma_i^r = \iota$ for each integer $1 \leq i \leq k$, then $\sigma_k^r \cdots \sigma_1^r = \iota$. Conversely, if $\sigma_i^r \neq \iota$ for some integer $1 \leq i \leq k$, then $\sigma_k^r \cdots \sigma_1^r \neq \iota$ because the cycles $\sigma_1, \ldots, \sigma_k$ are disjoint. Consequently, we conclude that

$$\begin{aligned}\mathrm{ord}(\sigma) &= \min\{r \geq 1 \,|\, \sigma_i^r = \iota \text{ for each integer } 1 \leq i \leq k\} \\ &= \min\{r \geq 1 \,|\, \mathrm{ord}(\sigma_i) = r_i \text{ divides } r \text{ for each integer } 1 \leq i \leq k\} = \mathrm{lcm}(r_1, \ldots, r_k).\end{aligned}$$

Explicitly, the second equality follows from Corollary 2.3.13, and the third equality follows from the definition of the least common multiple that precedes Exercise 1.10.31. □

Permutations of order two are called **involutions**. By Propositions 2.5.6 and 2.5.7, a permutation is an involution if and only if its cycle decomposition is the product of disjoint transpositions.

Example 2.5.8. Consider the permutation σ of Example 2.5.3 with disjoint cycles (125), (38), (4), and (67). By Proposition 2.5.6, its cycle decomposition is given by $\sigma = (125)(38)(4)(67)$, hence we have that $\text{ord}(\sigma) = \text{lcm}(3, 2, 1, 2) = \text{lcm}(6, 1, 2) = \text{lcm}(6, 2) = 6$ by Proposition 2.5.7.

Corollary 2.5.6 guarantees that every permutation can be written as a product of disjoint cycles uniquely up to the arrangement of the factors. Consequently, if we are handed the cycle decomposition of a permutation, it is natural to ask how to reconstruct its two-line notation representation.

Algorithm 2.5.9. We can reconstruct the two-line notation for any permutation σ from its cycle decomposition $\sigma_1 \cdots \sigma_k$ as follows.

1.) Find the largest positive integer n lying in some cycle σ_i.

2.) Build a $2 \times n$ array with the integers $1, 2, \ldots, n$ listed in ascending order in the first row.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ & & & \end{pmatrix}$$

3.) Begin to fill the space below the integer 1 by first locating the integer 1 in some cycle σ_{i_1}.

4.) If 1 is immediately followed by a right parenthesis, then $\sigma(1)$ is the integer that begins the cycle σ_{i_1}; otherwise, $\sigma(1)$ is the integer that immediately follows 1 in the cycle σ_{i_1}.

5.) Repeat the above two steps until the integers $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are all found.

Example 2.5.10. Consider the permutation $\sigma = (135)(48)(276)$. Observe that the largest positive integer n lying in some cycle is $n = 8$. Consequently, we will build the two-line notation of σ from the the 2×8 array with the integers $1, 2, \ldots, 8$ listed in ascending order in the first row.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & & & & & & & \end{pmatrix}$$

Observe that 1 lies in the cycle (135); it is immediately followed by 3, hence we have that $\sigma(1) = 3$.
Observe that 2 lies in the cycle (276); it is immediately followed by 7, hence we have that $\sigma(2) = 7$.
Observe that 3 lies in the cycle (135); it is immediately followed by 5, hence we have that $\sigma(3) = 5$.
Observe that 4 lies in the cycle (48); it is immediately followed by 8, hence we have that $\sigma(4) = 8$.
Observe that 5 lies in the cycle (135); it is immediately followed by a right parenthesis, hence we have that $\sigma(5) = 1$. Continuing in this manner, we obtain the two-line notation for σ.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 8 & 1 & 2 & 6 & 4 \end{pmatrix}$$

Unfortunately, there is no guarantee that we will be handed the cycle decomposition of a permutation; rather, if we are given a product of (not necessary disjoint) cycles, the following algorithm generalizes the method of Algorithm 2.5.9 to find the two-line notation for the resulting permutation.

Algorithm 2.5.11. We reconstruct the two-line notation for any permutation $\sigma = \sigma_1 \cdots \sigma_k$ that is a product of (not necessarily disjoint) cycles $\sigma_1, \ldots, \sigma_k$ as follows.

1.) Find the largest positive integer n lying in some cycle σ_i.

2.) Build a $2 \times n$ array with the integers $1, 2, \ldots, n$ listed in ascending order in the first row.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ & & & \end{pmatrix}$$

3.) Begin to fill the space below the integer 1 by first locating the integer 1 in the cycle σ_{i_1} that is farthest to the right among the cycles in the product $\sigma_1 \cdots \sigma_k$.

4.) If 1 is immediately followed by a right parenthesis, then 1 maps to the integer b_{i_1} that begins σ_{i_1}; otherwise, 1 maps to the integer n_{i_1} that immediately follows 1 in σ_{i_1}.

5.) Locate the integer b_{i_1} or n_{i_1} in the cycle that is farthest to the right among the cycles in the product $\sigma_1 \cdots \sigma_{i_1 - 1}$; then, repeat the third step. If $i_1 = 1$, then $\sigma(1) = b_{i_1}$ or $\sigma(1) = n_{i_1}$.

6.) Repeat the third and fourth steps until it is not possible; the last integer found is $\sigma(1)$.

7.) Repeat the above four steps until the integers $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are found.

One useful way to think about and to understand the mechanics of this algorithm is that function composition is read from right to left. Considering that each cycle is itself a permutation, in order to find the image of i under the composite function $\sigma_1 \cdots \sigma_k$, we follow the image of i under the successive composite functions σ_k, $\sigma_{k-1}\sigma_k$, etc., up to $\sigma_1 \cdots \sigma_k$. Further, if the integer $\sigma_i(i)$ does not appear in σ_{i+1}, then $\sigma_{i+1}\sigma_i(i) = \sigma_i(i)$, hence we must only consider the cycle farthest to the right that contains the integer under consideration: all cycles that do not contain $\sigma_i(i)$ will fix $\sigma_i(i)$.

Example 2.5.12. We will write the permutation $\sigma = (134)(45)(14)(23)$ of $\mathfrak{S}_5$ in two-line notation. Using the algorithm above, we find that 1 maps to 4; then, 4 maps to 5; and finally, 5 does not appear in any cycle to the left of (45), so it follows that $\sigma(1) = 5$. We find next that 2 maps to 3; then, 3 maps to 4; and there are no permutations to the left of (134), so it follows that $\sigma(2) = 4$. We find next that 3 maps to 2 in the last cycle, and 2 does not appear in any cycle to the left of (23), so it follows that $\sigma(3) = 2$. We find next that 4 maps to 1; then, 1 maps to 3; and there are no permutations to the left of (134), so it follows that $\sigma(4) = 3$. Last, we find that 5 maps to 4; then, 4 maps to 1; and there are no permutations to the left of (134), so it follows that $\sigma(5) = 1$. We conclude therefore that σ can be written in two-line notation as follows.

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

Often, it is advantageous to omit the cycles of length one when describing a permutation via its cycle decomposition. For instance, the permutation $\sigma = (123)$ can be viewed as the 3-cycle

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

in $\mathfrak{S}_3$ or as the permutation τ in $\mathfrak{S}_n$ for any integer $n \geq 3$ that acts as σ on the subset $\{1, 2, 3\}$ and acts as the identity on the subset $\{4, \ldots, n\}$. Consequently, a permutation is uniquely determined by its cycle decomposition (excluding 1-cycles) regardless of the symmetric group to which it belongs.

Proposition 2.5.13. *For every integer $n \geq 3$, the symmetric group $\mathfrak{S}_n$ is not abelian.*

Proof. Consider the cycles $\sigma = (12)$ and $\tau = (13)$ in $\mathfrak{S}_3$. By the paragraph above, we may view σ and τ as elements of $\mathfrak{S}_n$ for every integer $n \geq 3$. Considering that $\sigma\tau = (12)(13) = (132)$ is not equal to $\tau\sigma = (13)(12) = (123)$, we conclude that $\mathfrak{S}_n$ is not abelian for any integer $n \geq 3$. □

Computing the inverse of a permutation can be quite tedious; however, if we have a permutation σ written as its cycle decomposition $\sigma = \sigma_1 \cdots \sigma_k$, then the inverse of σ can be obtained as follows. Observe that if σ_i has length r_i, then $\sigma_i \sigma_i^{r_i - 1} = \sigma_i^{r_i} = \iota = \sigma_i^{r_i - 1}\sigma_i$. Consequently, we have that $\sigma_i^{-1} = \sigma_i^{r_i - 1}$. Considering that disjoint cycles commute, we have the following.

Proposition 2.5.14. *Let σ be any permutation with cycle decomposition $\sigma_1 \cdots \sigma_k$ and cycle type $(r_1, \ldots, r_k)$. We have that $\sigma^{-1} = \sigma_1^{r_1 - 1} \cdots \sigma_k^{r_k - 1}$.*

Ultimately, Proposition 2.5.14 makes small work of the matter of finding inverses of permutations written in cycle decomposition: observe that $(a_1, \ldots, a_k)^{-1} = (a_1, a_k, a_{k-1}, \ldots, a_3, a_2)$.

2.6 Dihedral Groups

Previously, in Section 1.8, we considered the rigid motions of a regular n-gon. Explicitly, we noticed that rotation of a regular n-gon through an angle of $-360k/n$ degrees produces a copy of the regular n-gon with the ith vertex in place of the $(i+k)$th vertex (modulo n). Likewise, the reflection of any regular n-gon across a vertex k swaps the labels of the vertices other than k according to the parity of n. Our immediate aim is to establish that the collection D_n of these rotations and reflections of a regular n-gon constitutes a subgroup of order $2n$ of the symmetric group $\mathfrak{S}_n$ on n letters.

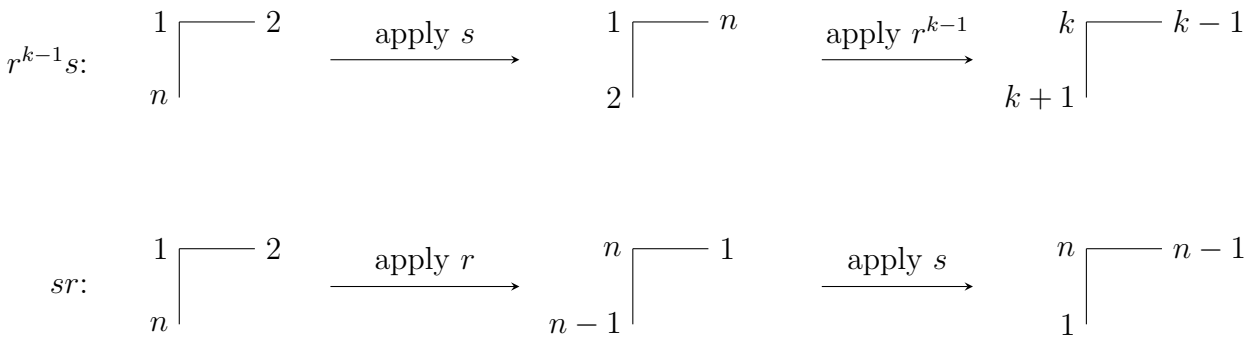
Proposition 2.6.1. *Let $n \geq 3$ be an integer. Let D_n denote the set of symmetry-preserving rotations and reflections of a regular n-gon. Every element of D_n can be written as a product of some distinguished elements $r, s \in D_n$ such that r has order n; s has order two; and $sr = r^{n-1}s$.*

Proof. Consider the rotation r of the regular n-gon through the angle $-360/n$ degrees and the reflection s of the regular n-gon about the vertex 1. Conventionally, we denote by sr the composite function $s \circ r$. Observe that r has order n: indeed, it follows that r^k is the rotation of the regular n-gon through an angle of $-360k/n$ degrees, and the rational numbers $-360k/n$ are distinct for each integer $1 \leq k \leq n$. On the other hand, r^{n+1} is the rotation through the angle $-360 - 360/n$ degrees; this has the same effect as rotating about the angle $-360/n$ degrees, hence we conclude that $r^{n+1} = r$, and the order of r is n. Certainly, the order of s is two because reflection about the vertex 1 twice does not swap any of the vertices, i.e., we have that s^2 is the identity permutation.

We will demonstrate next that every reflection of the regular n-gon can be achieved by performing r and s sequentially in some order. We claim that $r^{k-1}s$ is a distinct reflection of the regular n-gon for each integer $1 \leq k \leq n$. Observe that s has the effect of labelling the vertices $1, 2, \ldots, n$ of the regular n-gon counterclockwise (as opposed to the usual clockwise order); then, r^{k-1} replaces vertex

1 with the label k, vertex n with the label $k-1$, and vertex 2 with the label $k+1$ (modulo n). Consequently, we conclude that $r^{k-1}s$ is a distinct reflection for each integer $1 \leq k \leq n$. Considering that there are n reflections of any regular n-gon, they must be precisely $s, rs, r^2s, \ldots, r^{n-1}s$.

Last, we attend to sr. Observe that r has the effect of labelling vertex 1 with label n, vertex 2 with label 1, and vertex n with label $n-1$; then, under s, vertex 1 retains the label n, vertex 2 obtains the label $n-1$, and vertex n obtains the label 1. Put another way, we have that $sr = r^{n-1}s$. □



Proposition 2.6.2. *Let $n \geq 3$ be an integer. Let D_n denote the set of symmetry-preserving rotations and reflections of a regular n-gon. We have that D_n is a subgroup of $\mathfrak{S}_n$ of order $2n$.*

Proof. Every symmetry-preserving rotation or reflection of the regular n-gon can be viewed as a permutation of the integers $1, \ldots, n$, hence D_n is a subset of $\mathfrak{S}_n$. By Proposition 2.6.1, the distinct elements of D_n are $r, r^2, \ldots, r^n, s, rs, r^2s, \ldots, r^{n-1}s$, hence D_n has order $2n$. Even more, every rotation r^k has a multiplicative inverse r^{n-k}, and every reflection r^ks is its own multiplicative inverse. Consequently, by the Two-Step Subgroup Test, it suffices to prove that $xy \in D_n$ for any elements $x, y \in D_n$. Certainly, the product of two rotations is a rotation, hence we may assume that x and y are not both rotations. By Proposition 2.6.1, we may assume first that $x = r^k$ and $y = r^\ell s$ for some integers $1 \leq k, \ell \leq n$. Observe that $xy = r^{k+\ell}s$; by taking the exponent $k+\ell$ modulo n, we conclude that xy lies in D_n. Conversely, if $x = r^ks$ and $y = r^\ell$ for some integers $1 \leq k, \ell \leq n$, we conclude that $xy = r^ksr^\ell = r^kr^{\ell(n-1)}s = r^{\ell(n-1)+k}s$ lies in D_n. Last, if $x = r^ks$ and $y = r^\ell s$ for some integers $1 \leq k, \ell \leq s$, then $xy = r^ksr^\ell s = r^kr^{\ell(n-1)}s^2 = r^{\ell(n-1)+k}$ is in D_n. □

We will henceforth refer to D_n as the **dihedral group** of order $2n$ in light of Proposition 2.6.2. We adopt the convention that the identity of this group is 1; it is obtained from the original arrangement of the n vertices of the regular n-gon in clockwise order by doing nothing.

Example 2.6.3. Consider the dihedral group D_4 of order 8, i.e., the group of symmetry-preserving rotations and reflections of a square. By Proposition 2.6.1, the elements of D_4 are the identity element 1; the rotation r by $-90°$; the rotation r^2 by $-180°$; the rotation r^3 by $-270°$; the reflection s across vertices 1 and 3; the reflection rs across the line perpendicular to side 12; the reflection r^2s across the vertices 2 and 4; and the reflection r^3s across the line perpendicular to side 14.

Considering that every symmetry-preserving rotation and reflection of a square is a bijection from the set $\{1, 2, 3, 4\}$ to itself, we can realize each of the eight elements of D_4 as a permutation of the integers 1, 2, 3, and 4. Explicitly, the following hold in two-line and one-line notation.

$$1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1) \qquad s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24)$$

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234) \qquad rs = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

$$r^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24) \qquad r^2s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (13)$$

$$r^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432) \qquad r^3s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

We leave the above details for the reader to check pictorially in Exercise 2.8.48.

Example 2.6.4. Consider the dihedral group D_5 of order 10, i.e., the group of symmetry-preserving rotations and reflections of a regular pentagon. By Proposition 2.6.1, the elements of D_5 are the identity element 1; the rotation r by $-72°$; the rotation r^2 by $-144°$; the rotation r^3 by $-216°$; the rotation r^4 by $-288°$; the reflection s across vertex 1; the reflection rs across vertex 4; the reflection r^2s across vertex 2; the reflection r^3s across vertex 5; and the reflection r^4s across vertex 3.

$$\begin{aligned} 1 &= (1) & s &= (24)(35) \\ r &= (12345) & rs &= (12)(35) \\ r^2 &= (13524) & r^2s &= (13)(45) \\ r^3 &= (14253) & r^3s &= (14)(23) \\ r^4 &= (15432) & r^4s &= (15)(24) \end{aligned}$$

We leave the above details for the reader to check pictorially in Exercise 2.8.49.

2.7 Chapter 2 Overview

This section is currently under construction.

2.8 Chapter 2 Exercises

2.8.1 Groups (Definitions and Examples)

Exercise 2.8.1. Explain why $\mathbb{R}$ does not form a group with respect to multiplication.

Exercise 2.8.2. Use the definition of a group to prove that $\{-1, 1\}$ forms an abelian group with respect to multiplication; you may assume that integer multiplication is associative.

Exercise 2.8.3. Let i denote the complex number satisfying that $i^2 = -1$. Use the definition of a group to prove that $\{-1, 1, -i, i\}$ forms an abelian group with respect to multiplication; you may assume that complex multiplication is associative and commutative.

Exercise 2.8.4. Use the definition of a group to prove that $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ forms an abelian group with respect to multiplication; you may use that real multiplication is associative and commutative.

Exercise 2.8.5. Let G be a group. We say that an element $g \in G$ is **idempotent** if it holds that $g^2 = g$. Prove that the only idempotent element of a group is the identity element e_G.

Exercise 2.8.6. Given a positive integer n, let $\mathbb{Z}_n$ denote the collection of equivalence classes of the integers modulo n. Explain why $\mathbb{Z}_n$ does not form a group with respect to multiplication modulo n.

(**Hint:** Exercise 1.10.36 could be a useful reference here.)

Exercise 2.8.7. Given a prime integer p, let $\mathbb{Z}_p$ denote the collection of equivalence classes of the integers modulo p. Prove that $\mathbb{Z}_p$ forms an abelian group with respect to multiplication modulo p.

(**Hint:** Exercise 1.10.38 could be a useful reference here.)

Exercise 2.8.8. Given a positive integer n, let $\mathbb{Z}_n$ denote the collection of equivalence classes of integers modulo n. Prove that the set $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$ forms a group with respect to multiplication modulo n; this group is called the **multiplicative group of integers modulo** n.

Exercise 2.8.9. Consider the nonempty set $G = \mathbb{R} \setminus \{-1\}$.

(a.) Prove that $* : G \times G \to G$ defined by $x * y = x + y + xy$ is a binary operation on G.

(b.) Use the definition of a group to prove that $(G, *)$ is an abelian group.

Exercise 2.8.10. Prove that a group G is abelian if $(gh)^2 = g^2h^2$ for all elements $g, h \in G$.

(**Hint:** Compute $(gh)^2$ in two ways; then, compare your results.)

Exercise 2.8.11. Prove that a group G is abelian if $g^2 = e_G$ for every element $g \in G$.

(**Hint:** Use the fact that G is abelian if and only if $ghg^{-1}h^{-1} = e_G$ for all elements $g, h \in G$.)

Exercise 2.8.12. Prove that a group G is abelian if $gh = g^{-1}h^{-1}$ for all elements $g, h \in G$.

(**Hint:** Essentially, this follows as a corollary of Exercise 2.8.11.)

Exercise 2.8.13. Prove that a group G is abelian if $g^3 = e_G$ and $g^4h = hg$ for all elements $g, h \in G$.

Exercise 2.8.14. Prove that any group of order four must be abelian.

2.8.2 Groups (Basic Properties and Subgroups)

Exercise 2.8.15. Use Exercise 2.8.4 and the One-Step Subgroup Test to prove that $\{-1, 1\}$ forms an abelian group with respect to multiplication.

Exercise 2.8.16. Let i denote the complex number satisfying that $i^2 = -1$. Use the One-Step Subgroup Test to prove that $\{-1, 1, -i, i\}$ forms an abelian group with respect to multiplication.

Exercise 2.8.17. Prove that the Group Exponent Laws hold for any group G.

Exercise 2.8.18. Let G be a group. Prove that $Z(G) = \{x \in G \mid gx = xg \text{ for all elements } g \in G\}$ is a subgroup of G called the **center** of G (the notation is derived from the German "das Zentrum").

Exercise 2.8.19. Let G be a group. Prove that the **centralizer** $C_G(x) = \{g \in G \mid gx = xg\}$ of any element $x \in G$ is a subgroup of G.

Exercise 2.8.20. Let G be a group with a subgroup H. Prove that for any element $g \in G$, the set $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subseteq G$ is a subgroup of G; this is called the **conjugate** of H by g.

Exercise 2.8.21. Let G be a group. Prove that the **normalizer** $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ of any subgroup $H \subseteq G$ is itself a subgroup of G.

(**Hint:** Observe that if $gHg^{-1} = H$, then for every element $h \in H$, there exists an element $k \in H$ such that $h = gkg^{-1}$. Conclude that $g^{-1}hg$ lies in H for every element $g \in N_G(H)$.)

Exercise 2.8.22. Let G be a group. Prove that for any subgroups H and K of G, the intersection $H \cap K = \{g \in G \mid g \in H \text{ and } g \in K\}$ is a subgroup of G.

Exercise 2.8.23. Let G be a group. Prove that for any subgroups H and K of G, the collection of products $HK = \{hk \mid h \in H \text{ and } k \in K\}$ is a subgroup of G if and only if $HK = KH$.

2.8.3 Cyclic Groups

Exercise 2.8.24. Explain if the rational numbers $\mathbb{Q}$ form a cyclic group with respect to addition.

Exercise 2.8.25. Let $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\}$ denote the multiplicative group of integers modulo a prime number p. Verify that $\mathbb{Z}_p^*$ is a cyclic group of order $p - 1$ for $p = 2, 3, 5, 7$, and 11.

Exercise 2.8.26. Let $\mathbb{Z}_n^*$ denote the multiplicative group of integers modulo n. Prove that there exists a non-identity element $a \in \mathbb{Z}_n^*$ of order two, i.e., such that $a^2 \equiv 1 \pmod{n}$.

(**Hint:** Observe that for any positive integer n, we have that $n^2 - 2n + 1 \equiv 1 \pmod{n}$.)

Exercise 2.8.27. Let $(\mathbb{Z}_p, +)$ denote the additive group of integers modulo a prime number p. Prove that $(\mathbb{Z}_p, +)$ admits no subgroups other than itself and the trivial subgroup.

Euler's totient function is the unique piecewise function $\varphi : \mathbb{Z} \to \mathbb{Z}_{>0}$ defined by $\varphi(1) = 1$ and $\phi(n) = \#\{k \in \mathbb{Z} \mid k \geq 1 \text{ and } \gcd(n, k) = 1\}$ for all integers $n \geq 2$. Explicitly, we note that $\phi(n)$ is precisely the number of positive integers that are relatively prime to n.

Exercise 2.8.28 (Euler's Theorem)**.** Prove that $|\mathbb{Z}_n^*| = \phi(n)$ for every positive integer n. Use this to deduce **Euler's Theorem** that $a^{\phi(n)} \equiv 1 \pmod{n}$ for all integers a such that $\gcd(n, a) = 1$.

Exercise 2.8.29 (Fermat's Little Theorem)**.** Prove that $|\mathbb{Z}_p^*| = p - 1$ for every prime integer p. Use this to deduce **Fermat's Little Theorem** that $a^{p-1} \equiv 1 \pmod{n}$ for all integers a such that $p \nmid a$.

Exercise 2.8.30. Let G be a group. Prove that the following statements holds.

(a.) Given any element $g \in G$, we have that $\text{ord}(g^{-1}) = \text{ord}(g)$.

(b.) Given any element $x \in G$, we have that $\text{ord}(gxg^{-1}) = \text{ord}(x)$ for all elements $g \in G$.

(**Hint:** Observe that $(gxg^{-1})^r = (gxg^{-1})(gxg^{-1}) \cdots (gxg^{-1})$ with r factors of gxg^{-1}; then, simplify the blue terms, and collect the orange terms using the Group Exponent Laws.)

(c.) Given any elements $g, h \in G$, we have that $\text{ord}(gh) = \text{ord}(hg)$.

(**Hint:** Observe that $hg = hghh^{-1} = h(gh)h^{-1}$; then, use part (b.) to conclude the result.)

Exercise 2.8.31. Let G be an abelian group. Consider any elements $g, h \in G$ such that $\text{ord}(g) = r$, $\text{ord}(h) = s$, and $\text{ord}(gh) = t$ are all finite.

(a.) Prove that $t \mid rs$.

(b.) Prove that $r \mid st$ and that $s \mid rt$. Conclude that $\dfrac{r}{\gcd(r,s)} \left| \dfrac{s}{\gcd(r,s)}t \right.$ and $\dfrac{s}{\gcd(r,s)} \left| \dfrac{r}{\gcd(r,s)}t \right.$.

(c.) Prove that $\dfrac{r}{\gcd(r,s)} \left| t \right.$ and $\dfrac{s}{\gcd(r,s)} \left| t \right.$. Conclude that $\dfrac{rs}{\gcd(r,s)^2} \left| t \right.$.

Ultimately, conclude that if $\text{ord}(g)$ and $\text{ord}(h)$ are relatively prime, then $\text{ord}(gh) = \text{ord}(g)\,\text{ord}(h)$.

(**Hint:** Corollary 2.3.13 yields (a.). On the first part of (b.), to quote the great Lucian Grand, you will need to make the inspired substitution $h^{st} = e_G$ to find that $g^{st} = g^{st}h^{st}$; simplify and use the corollary. Use Exercise 1.10.28 for the first part of (c.) and Exercise 1.10.34 for the second part.)

Exercise 2.8.32. Let G be an abelian group. Let p be a prime number. Prove that for any elements $g, h \in G$ with $\text{ord}(g) = p^m$ and $\text{ord}(h) = p^n$, we have that $\text{ord}(gh) = \max\{m, n\}$.

Exercise 2.8.33. Let G be a cyclic group of order n. Prove that $\text{ord}(x) \mid n$ for all elements $x \in G$.

Exercise 2.8.34. Let G be a cyclic group of order n. Prove that for all positive integers $d \mid n$, there exists a (cyclic) subgroup of G of order d.

Exercise 2.8.35. Let G be an abelian group. Prove that the set $G_T = \{g \in G \mid \text{ord}(g) \text{ is finite}\}$ of elements of G of finite order is a subgroup of G called the **torsion subgroup**.

Exercise 2.8.36. Prove that if a group G is not cyclic, then it admits (at least) one proper non-trivial subgroup. Conclude that if G has no proper non-trivial subgroups, then G is cyclic.

2.8.4 Complex Numbers as a Group Under Multiplication

Exercise 2.8.37. Prove that if $z \in \mathbb{C}^\times$ has finite order, then we must have that $|z| = 1$. Conclude that every nonzero complex number such that $|z| \neq 1$ has infinite order.

Exercise 2.8.38. Find all elements of finite order in the multiplicative group of complex numbers.

Exercise 2.8.39. Graph the fifth roots of unity. List each of them as a complex number of the form $\text{cis}(\theta)$ for some angle $0 \leq \theta < 2\pi$ and in the form $a + bi$ for some nonzero real numbers a and b; then, indicate which of the fifth roots of unity are primitive fifth roots of unity.

Exercise 2.8.40. Graph the sixth roots of unity. List each of them as a complex number of the form $\text{cis}(\theta)$ for some angle $0 \leq \theta < 2\pi$ and in the form $a + bi$ for some nonzero real numbers a and b; then, indicate which of the sixth roots of unity are primitive sixth roots of unity. Compare the results of this exercise with your results from Exercise 2.8.39, and explain the differences.

Exercise 2.8.41. Generally, what shape do the nth roots of unity form in the complex plane? Use this information to deduce when the polynomial $x^n - 1$ has two real roots or only one real root.

Exercise 2.8.42. Prove that $(r_1 \,\text{cis}\,\theta_1)(r_2 \,\text{cis}\,\theta_2) = r_1 r_2 \,\text{cis}(\theta_1 + \theta_2)$.

(**Hint:** Use $\cos(\theta_1 + \theta_2) = \cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2$ and $\sin(\theta_1 + \theta_2) = \sin\theta_1 \cos\theta_2 + \sin\theta_2 \cos\theta_1$.)

2.8.5 The Symmetric Group on n Letters

Exercise 2.8.43. Let n be a positive integer. Let $[n] = \{1, 2, \ldots, n\}$. Complete the following steps to obtain an alternate proof of Proposition 2.5.5. Use the first step provided as a guide the rest.

(i.) Use words and symbols to define when a bijection $\sigma : [n] \to [n]$ is a **cycle**.

We have that σ is a cycle if and only if there exists a nonempty set $S \subseteq [n]$ for which the restriction $\sigma|_S : S \to S$ of σ to S is a bijection and $\sigma(i) = i$ for all integers $i \in [n] \setminus S$.

(ii.) Use words and symbols to define the entries of the **one-line notation** of σ.

(iii.) Use words and symbols to define when two cycles σ and τ are **disjoint**.

(iv.) Prove that if i does not appear in either the one-line notation of σ or τ, then $\sigma\tau(i) = \tau\sigma(i)$.

(v.) Prove that if i appears in the one-line notation of σ, then it does not appear in the one-line notation of τ. Conclude in this case that $\sigma\tau(i) = \tau\sigma(i)$.

Exercise 2.8.44. Prove that every k-cycle can be written as a product of transpositions. Conclude by Proposition 2.5.4 that every permutation can be written as a product of transpositions.

(**Hint:** Consider the k-cycle $(a_1, \ldots, a_k)$. Use the fact that permutations are multiplied right to left, hence if a_i does not appear in the one-line notation of σ, then $\sigma \circ (a_1, a_i)$ sends a_1 to a_i.)

Like integers, permutations possess **parity**. Explicitly, we say that a permutation σ is **even** (or **odd**, respectively) if it can be expressed as a product of an even (or odd, respectively) number of transpositions. We will assume that the identity permutation ι is even (cf. [JB21, Lemma 5.14]).

Exercise 2.8.45. Prove that a permutation σ is either even or odd but not both.

(**Hint:** Observe that if $\sigma = \tau_1 \cdots \tau_m$ for some transpositions $\tau_1, \ldots, \tau_m$ and $\sigma = \theta_1 \cdots \theta_n$ for some transpositions $\theta_1, \ldots, \theta_n$, then $\iota = \sigma\sigma^{-1} = \tau_1 \cdots \tau_m \theta_n^{-1} \cdots \theta_1^{-1}$.)

Exercise 2.8.46. Prove that a cycle of odd length is even and a cycle of even length is odd.

Exercise 2.8.47. Consider the collection $\mathfrak{A}_n$ of even permutations on n letters.

(a.) Prove that $\mathfrak{A}_n$ is a subgroup of $\mathfrak{S}_n$ called the **alternating group on n letters**.

(b.) Compute the order of the alternating group $\mathfrak{A}_4$ on four letters.

(**Hint:** Every cycle of odd length is even; all else in $\mathfrak{A}_4$ is a product of disjoint transpositions.)

(c.) Use part (b.) above and Lagrange's Theorem to compute the index $[\mathfrak{S}_4 : \mathfrak{A}_4]$ of $\mathfrak{A}_4$ in $\mathfrak{S}_4$.

2.8.6 Dihedral Groups

Exercise 2.8.48. Verify the explanation of Example 2.6.3 by using pictures to illustrate how each of the eight elements $1, r, r^2, r^3, s, rs, r^2s, r^3s$ of D_4 acts on the square.

Exercise 2.8.49. Verify the explanation of Example 2.6.4 by using pictures to illustrate how each of the ten elements $1, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s$ of D_5 acts on the regular pentagon.

Exercise 2.8.50. Prove that the dihedral group D_n of order $2n$ is not abelian for $n \geq 3$.

(**Hint:** On the contrary, if $rs = sr$, then what can be said about r by Proposition 2.6.1?)

Exercise 2.8.51. Prove that the dihedral group D_n of order $2n$ admits elements x and y of order two such that their product xy has order n. Conclude that the order of a product of two elements of order two can be any positive integer exceeding two.

Exercise 2.8.52. Consider the center $Z(D_n) = \{x \in D_n \mid yx = xy \text{ for all } y \in D_n\}$ of the dihedral group D_n of order $2n$. Complete the following steps to prove that

$$Z(D_n) = \begin{cases} \{1\} & \text{if } n \text{ is odd and} \\ \{1, r^{\frac{n}{2}}\} & \text{if } n \text{ is even.} \end{cases}$$

(i.) Every element of D_n is of the form $r^i s^j$ for some integers $0 \leq i \leq n-1$ and $0 \leq j \leq 1$. By definition, for any element $x \in Z(D_n)$, we must have that $xr = rx$. Conclude that if $x = r^k s$ for some integer $0 \leq k \leq n-1$, then $xr \neq rx$, i.e., x is not in $Z(D_n)$.

(ii.) Use the step (i.) to prove that if $x \in Z(D_n)$, then $x = r^k$ for some integer $0 \leq k \leq n-1$.

(iii.) On the other hand, for any element $x \in Z(D_n)$, we must have that $xs = sx$. By the previous part, we may assume that $x = r^k$ for some integer $0 \leq k \leq n-1$, hence we must have that $r^k s = sr^k$. Use the identity $sr = r^{n-1}s$ to find that if $x \in Z(D_n)$, then $r^k = r^{nk-k}$.

(iv.) Cancelling a factor from both sides of the last identity of part (iii.), we find that $r^{nk-2k} = 1$. By Corollary 2.3.13, conclude that $n \mid (nk-2k)$.

(v.) Observe that if $n \mid (nk-2k)$, then there exists an integer q such that $nk-2k = nq$. Conclude that $n \mid 2k$, hence we must have that $n = 0$ or $n = 2k$. Ultimately, conclude the desired result.

Exercise 2.8.53. Prove that if $n \geq 4$, then there exists an element $\sigma \in \mathfrak{S}_n$ such that $\sigma \notin D_n$. Conclude that the dihedral group of order $2n$ is a proper subgroup of $\mathfrak{S}_n$ for all integers $n \geq 4$.

(**Hint:** Every element of D_n must do what to the consecutive clockwise vertices n, 1, and 2?)

Chapter 3

Group Theory II

One of the primary objectives of group theory is to solve the classification problem for groups. Explicitly, it is natural to ask the ways in which two groups differ from one another. We define this distinction formally by asking whether two groups are isomorphic. Groups that are isomorphic are "essentially the same" in the sense that the elements of one group can be "renamed" to obtain the elements of the other group, and the binary operations on each group are "compatible" with one another. Ultimately, we will find that isomorphic groups possess the same properties. We devote this chapter to developing the necessary tools and solving the classification problem in some cases.

3.1 Cosets and Lagrange's Theorem

Central to the study of groups is the question of finding all proper non-trivial subgroups of any group. We have already seen in Example 2.2.12 that the abelian groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ both have order four, but they are distinct from one another as groups because $(\mathbb{Z}_4, +)$ admits only one non-trivial proper subgroup compared to the three non-trivial proper subgroups of $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Our aim throughout this section is to prove Lagrange's Theorem; it is a powerful tool in group theory that drastically narrows down the possible subgroups of any group of finite order.

We will assume throughout this section that $(G, *)$ is a group. If $(H, *)$ is a subgroup of G, then the **left coset** of H in G **represented** by an element $g \in G$ is the collection $g * H = \{g * h \mid h \in H\}$ of all products of all elements of H with g on the left. We define right cosets analogously.

Example 3.1.1. Consider the dihedral group $D_3 = \{1, r, r^2, s, rs, r^2s\}$ and its subgroup $H = \{1, s\}$. We obtain the left cosets $1H = H = sH$, $rH = \{r, rs\} = rsH$, and $r^2H = \{r^2, r^2s\} = r^2sH$. We obtain the right cosets $H1 = H = Hs$, $Hr = \{r, r^2s\} = Hr^2s$, and $Hr^2 = \{r^2, rs\} = Hrs$ by using the identity $sr = r^2s$ of Proposition 2.6.1. Observe that $rH \neq Hr$ and $r^2H \neq Hr^2$, hence it is not necessarily true that the left and right cosets with respect to the same representative are equal.

Conversely, it holds that the left and right cosets of the subgroup $K = \{1, r, r^2\}$ in D_3 coincide for each representative. Explicitly, the left cosets $1K = K = rK = r^2K$ coincide with the right cosets $K1 = K = Kr = Kr^2$ and $sK = \{s, rs, r^2s\} = rsK = r^2sK$ and $Ks = \{s, rs, r^2s\} = Krs = Kr^2s$. We will return to this example and discuss this phenomenon in greater detail in Section 3.2.

We note that if G is abelian, then it holds that $g * h = h * g$ for all elements $g \in G$ and $h \in H$, hence the left and right cosets of H in G are equal, and we may refer to them simply as cosets.

Example 3.1.2. Consider the group $(\mathbb{Z}, +)$ and its subgroup $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$. Observe that $0 + 2\mathbb{Z} = \{0 + 2n \mid n \in \mathbb{Z}\} = \{2n + 0 \mid n \in \mathbb{Z}\} = 2\mathbb{Z} + 0$ consists of all even integers and $1 + 2\mathbb{Z} = \{1 + 2n \mid n \in \mathbb{Z}\} = \{2n + 1 \mid n \in \mathbb{Z}\} = 2\mathbb{Z} + 1$ consists of all odd integers. Consequently, there are only two left cosets of $2\mathbb{Z}$ in $\mathbb{Z}$, and the left and right cosets of $2\mathbb{Z}$ in $\mathbb{Z}$ coincide.

We provide the following propositions to summarize and generalize our current observations.

Proposition 3.1.3. *Let G be a group with a subgroup H. Given any element $g \in G$, the cosets gH and Hg of H in G represented by g satisfies that $gH = ghH$ and $Hg = Hhg$ for all elements $h \in H$. Put another way, the left and right coset representatives of H in G are not unique.*

Proof. Observe that for every element $h \in H$, we have that $gh = ghe_G$ lies in ghH because H is a subgroup of G, hence we conclude that $gH \subseteq ghH$. Conversely, for any element $h' \in H$, we have that hh' is an element of H so that ghh' lies in gH for all elements $h' \in H$, i.e., $ghH \subseteq gH$. □

Proposition 3.1.4. *Let G be a group. Consider any pair of elements $g_1, g_2 \in G$. If H is a subgroup of G, then the following properties of the left cosets of H in G are equivalent.*

(i.) *We have that $g_1H = g_2H$.*

(ii.) *We have that $g_1H \supseteq g_2H$.*

(iii.) *We have that $g_2 \in g_1H$.*

(iv.) *We have that $g_1^{-1}g_2 \in H$.*

(v.) *We have that $Hg_1^{-1} = Hg_2^{-1}$.*

Even more, the above properties hold for the right cosets of H in G, as well.

Proof. We leave it to the reader as Exercise 3.10.1 to prove directly the the first three implications hold. We will assume that $g_1^{-1}g_2 \in H$. Consequently, for every element $h \in H$, we have that $hg_1^{-1}g_2$ lies in H by assumption that H is a subgroup of G. Put another way, we have that $Hg_1^{-1}g_2 \subseteq H$, from which it follows that $Hg_1^{-1} \subseteq Hg_2^{-1}$. Conversely, we have that $g_2^{-1}g_1 = (g_1^{-1}g_2)^{-1}$, and we conclude as before that $Hg_2^{-1} \subseteq Hg_1^{-1}$, hence the fifth property above holds. Last, if $Hg_1^{-1} = Hg_2^{-1}$ holds, then we claim that $g_1H = g_2H$. By hypothesis, for every element $h_1 \in H$, there exists an element $h_2 \in H$ such that $h_1g_1^{-1} = h_2g_2^{-1}$. By taking the inverses of both sides, we find that $g_1h_1^{-1} = g_2h_2^{-1}$. Consequently, it follows that $g_1h_1 = g_2h_2^{-1}h_1^2$ lies in g_2H by assumption that H is a subgroup. We conclude that $g_1H \subseteq g_2H$; the other inclusion is proved analogously, hence equality holds. □

Given a group G with a subgroup H, we refer to the number $[G : H]$ of distinct left cosets of H in G as the **index** of H in G. We note that it is possible that $[G : H]$ is infinite. Explicitly, the rational numbers $\mathbb{Q}$ form a subgroup of the additive group $(\mathbb{R}, +)$ of real numbers such that $[\mathbb{R} : \mathbb{Q}]$ is infinite (cf. Exercise 3.10.2). Often, we will restrict our attention to the case that there are finitely many left cosets of H in G, hence $[G : H]$ will typically be a positive integer.

Example 3.1.5. Consider the dihedral group $D_3 = \{1, r, r^2, s, rs, r^2s\}$ and its subgroups $H = \{1, s\}$ and $K = \{1, r, r^2\}$ of Example 3.1.1. We established previously that $[G : H] = 3$ and $[G : K] = 2$.

Example 3.1.6. We established in Example 3.1.2 that $[\mathbb{Z} : 2\mathbb{Z}] = 2$ as groups under addition.

Our next proposition illustrates that we do not need to define an analogous term to measure the number of right cosets of H in G; in fact, this is exactly equal to the index of H in G.

Proposition 3.1.7. *Let G be a group. Given any subgroup H of G, the number of right cosets of H in G is equal to the left cosets of H in G, i.e., the index $[G : H]$ of H in G.*

Proof. Once again, by Exercise 1.10.5(d.), it suffices to provide a bijection $f_g : gH \to Hg$ for each element $g \in G$. We claim that such a function is given by the rule $f_g(gH) = Hg^{-1}$. We must first establish that this definition results in a **well-defined** function, i.e., we must demonstrate that if $g_1H = g_2H$, then $Hg_1^{-1} = Hg_2^{-1}$. (Essentially, this is the converse of the definition of injective.) But this holds by Proposition 3.1.4. Even more, the same proposition illustrates that if $Hg_1^{-1} = Hg_2^{-1}$, then $g_1H = g_2H$, i.e., it holds that f_g is injective. Last, f_g is surjective by construction. □

Before we prove Lagrange's Theorem, we provide two more crucial observations about left cosets.

Lemma 3.1.8. *Let G be a group with a subgroup H. Every left coset of H in G has the cardinality as H. Put another way, for every element $g \in G$, we have that $|gH| = |H|$.*

Proof. By Exercise 1.10.5(d.), it suffices to provide a bijection $f_g : H \to gH$ for each element $g \in G$. We may define one by declaring that $f_g(h) = gh$ for every element $h \in H$. By definition, every element of gH can be written as gh for some element $h \in H$, hence f_g is surjective. Cancellation holds in G, hence $gh_1 = f_g(h_1) = f_g(h_2) = gh_2$ implies that $h_1 = h_2$, i.e., f_g is injective. □

Lemma 3.1.9. *Let G be a group with a subgroup H. We have that $g_1H \sim g_2H$ if and only if $g_1g_2^{-1} \in H$ is an equivalence relation on the left cosets of H in G. Consequently, the left cosets of H in G partition G, i.e., G is the disjoint union of the distinct left cosets of H in G.*

Proof. We must demonstrate that the relation on the left cosets of H in G defined by $g_1H \sim g_2H$ if and only if $g_1g_2^{-1} \in H$ is reflexive, symmetric, and transitive.

1.) By assumption that H is a subgroup of G, we have that $e_G = g_1g_1^{-1}$ lies in H for all left cosets g_1H of H in G, hence we have that $g_1H \sim g_1H$, and the relation is reflexive.

2.) If $g_1H \sim g_2H$, then $g_1g_2^{-1}$ lies in H. Once again, by hypothesis that H is a subgroup of G, it follows that $g_2g_1^{-1} = (g_1g_2^{-1})^{-1} \in H$ so that $g_2H \sim g_1H$, i.e., the relation is symmetric.

3.) If $g_1H \sim g_2H$ and $g_2H \sim g_3H$, then both $g_1g_2^{-1}$ and $g_2g_3^{-1}$ lie in H. Consequently, their product $g_1g_3^{-1} = (g_1g_2^{-1})(g_2g_3^{-1})$ lies in H so that $g_1H \sim g_3H$, and the relation is transitive.

By Proposition 3.1.4, the inclusion $g_1g_2^{-1} \in H$ is equivalent to equality of the left cosets $g_1H = g_2H$, hence left coset equality is an equivalence relation on the left cosets of H in G. By Corollary 1.4.5, we conclude that the left cosets of H in G partition G: the members of the partition are the disjoint equivalence classes of G modulo this relation, i.e., they are the disjoint left cosets of H in G. □

Theorem 3.1.10 (Lagrange's Theorem)**.** *Given a group G and any subgroup H of G, we have that $|G| = [G : H]|H|$. Put another way, the order of any subgroup H of G must divide the order of G.*

Proof. By Lemma 3.1.9, there exists a bijection between G and the union of $[G : H]$ many disjoint left cosets of H in G. Each of these left cosets of H in G has $|H|$ elements by Lemma 3.1.8. □

Remark 3.1.11. We note that if $[G : H] = n$ is finite, then we can be more explicit about the details of the proof of Lagrange's Theorem. By Lemma 3.1.9, there exist elements $g_1, \ldots, g_n \in G$ such that $g_1H, \ldots, g_nH$ are pairwise disjoint and $G = g_1H \cup \cdots \cup g_nH$. Consequently, we have that $|G| = \sum_{i=1}^{n} |g_iH|$. Lemma 3.1.8 yields that $|g_iH| = |H|$, and there are $[G : H]$ summands.

Corollary 3.1.12. *If G is a finite group with subgroups $H \supseteq K$, then $[G : K] = [G : H][H : K]$.*

Proof. By assumption that K is a subgroup of G and $H \supseteq K$, it follows by the Subgroup Test that K is a subgroup of H. Consequently, if $|G|$ is a positive integer, then $|H|$ and $|K|$ are positive integers, and Lagrange's Theorem yields that $[G : K] = |G|/|K| = (|G|/|H|)(|H|/|K|) = [G : H][H : K]$. □

Like we mentioned at the beginning of this section, Lagrange's Theorem provides a tool with which we may determine the possible subgroups of a group based on the order of the group.

Corollary 3.1.13. *Every group of prime order is cyclic.*

Proof. By Lagrange's Theorem, the order of any non-identity element of a group G of prime order is prime. Consequently, there exists an element $g \in G$ such that $\text{ord}(g) = |G|$, i.e., $G = \langle g \rangle$. □

Corollary 3.1.14. *Every group of prime order is abelian.*

Proof. By Corollary 3.1.13, such a group is cyclic and hence abelian by Proposition 2.3.8. □

Corollary 3.1.15. *If G is a finite group, then $\text{ord}(g)$ divides $|G|$ for every element $g \in G$. Put another way, the order of any element of G divides the order of G.*

Proof. Observe that the order of an element $g \in G$ is exactly the cardinality of the cyclic subgroup $\langle g \rangle$ generated by G. By Lagrange's Theorem, we conclude that $\text{ord}(g)$ divides $|G|$. □

Caution: Lagrange's Theorem states that the order of every subgroup of a finite group divides the order of the group; however, the converse to Lagrange's Theorem is false. Explicitly, there exists a group G and an integer d dividing $|G|$ such that G does not admit a subgroup of order d.

Proposition 3.1.16 (The Converse of Lagrange's Theorem Is False)**.** *The alternating group $\mathfrak{A}_4$ on four letters is a subgroup of the symmetric group $\mathfrak{S}_4$ on four letters of order $12 = 2^2 \cdot 3$. Even more, there is not a subgroup of $\mathfrak{A}_4$ of order $6 = 2 \cdot 3$, hence the converse of Lagrange's Theorem is false.*

Proof. We simplify the clever proof of [Hen19, Example 2.18]. By Exercise 2.8.47, the first sentence of the proposition statement holds. On the contrary, we will assume that there exists a subgroup H of $\mathfrak{A}_4$ of order six. By Lagrange's Theorem, we have that $12 = |\mathfrak{A}_4| = [\mathfrak{A}_4 : H]|H| = 6[\mathfrak{A}_4 : H]$, from which it follows that $[\mathfrak{A}_4 : H] = 2$. Consequently, the only cosets of H in $\mathfrak{A}_4$ are H itself and $\mathfrak{A}_4 \setminus H$ by Remark 3.1.11. By Proposition 3.1.4, we conclude that for every element $\sigma \in \mathfrak{A}_4$, we have that $\sigma^2 H = H$, i.e., $\sigma^2 \in H$: indeed, we must have that either $\sigma^2 H = H$ or $\sigma H = H$, and the latter implies the former. We claim moreover that if σ is a 3-cycle, then σ belongs to H. Given any 3-cycle σ, observe that $\sigma = \sigma^4 = (\sigma^2)^2$ lies in H because σ^2 lies in H. We note that there are $4!/3 = 8$ 3-cycles in $\mathfrak{A}_4$, hence the order of H is at least eight — a contradiction. □

3.2 Quotient Groups and Normal Subgroups

Let G be a group. Given any subgroup H of G, we denote by G/H the collection of left cosets of H in G, i.e., we have that $G/H = \{gH \mid g \in G\}$ and $gH = \{gh \mid h \in H\}$ for all elements $g \in G$.

Proposition 3.2.1. *If G is a group and H is a subgroup of G, then the following are equivalent.*

(1.) *G/H is a group with respect to the operation $(g_1H)(g_2H) = g_1g_2H$.*

(2.) *We have that $gH = Hg$ for all elements $g \in G$.*

(3.) *We have that $gH \subseteq Hg$ for all elements $g \in G$.*

(4.) *We have that $ghg^{-1} \in H$ for all elements $g \in G$ and $h \in H$.*

Proof. We will assume first that G/H is a group with respect to the operation $(g_1H)(g_2H) = g_1g_2H$. Explicitly, the product of two left cosets g_1H and g_2H results in a left coset of H. By definition, for all elements $g_1, g_2 \in G$ and all elements $h_1, h_2 \in H$, we must have that $g_1h_1g_2h_2$ is an element of H. We claim that $gH = Hg$ for all elements $g \in G$. Given any element $h \in H$, by assumption, there exists an element $k \in H$ such that $ghg^{-1}e_G = k$. Consequently, we find that $gh = kg$ so that $gH \subseteq Hg$. Conversely, for every element $h \in H$, there exists an element $k \in H$ such that $g^{-1}hge_G = k$. We conclude therefore that $Hg \subseteq gH$, hence their equality holds.

Certainly, if $gH = Hg$ for all elements $g \in G$, then $gH \subseteq Hg$ for all elements $g \in G$. Even more, if $gH \subseteq Hg$ for all elements $g \in G$, then for every element $h \in H$, there exists an element $h' \in H$ such that $gh = h'g$, hence we have that $ghg^{-1} = h'$ lies in H for all elements $g \in G$ and $h \in H$.

Last, if ghg^{-1} lies in H for all elements $g \in G$ and $h \in H$, then we will demonstrate that G/H is a group with respect to the operation $(g_1H)(g_2H) = g_1g_2H$. Crucially, this operation is clearly associative; the identity element of G/H is the left coset e_GH; and the inverse of a left coset gH is the left coset $g^{-1}H$; however, we have not demonstrated that this is a binary operation on G/H. Explicitly, we must ensure that for any pair of coset representatives $g_1H = g_3H$ and $g_2H = g_4H$, we have that $g_1g_2H = g_3g_4H$. By Proposition 3.1.4, it suffices to prove that $(g_3g_4)^{-1}g_1g_2 \in H$. Considering that $g_1H = g_3H$, it follows that $g_3^{-1}g_1$ lies in H, hence we have that $(g_3g_4)^{-1}g_1g_2 = g_4^{-1}g_3^{-1}g_1g_2$ is of the form $g_4^{-1}hg_2$ for some element $h \in H$. Likewise, we have that $g_4^{-1}g_2$ lies in H by assumption that $g_2H = g_4H$. Our original hypothesis that ghg^{-1} lies in H for all elements $g \in G$ and $h \in H$ yields that $(g_3g_4)^{-1}g_1g_2 = g_4^{-1}hg_2 = (g_4^{-1}hg_4)(g_4^{-1}g_2)$ lies in H. □

We say that H is a **normal** subgroup of G if any of the above conditions of Proposition 3.2.1 holds for H; we denote this situation by $H \trianglelefteq G$. Often, if H is a subgroup of G, then we it is most convenient to write $H \leq G$ in place of the relatively cumbersome "H is a subgroup of G," hence the notation for normal subgroups is a specialization of this notation for subgroups. Even more, we will say that G/H is the **quotient group**, and we will refer to G/H as "G modulo H."

Corollary 3.2.2. *If G is a group and H is a subgroup of G, then G/H is a group of order $[G : H]$ with respect to the operation $(g_1H)(g_2H) = g_1g_2H$ if and only if H is a normal subgroup of G.*

Example 3.2.3. Consider the dihedral group $D_3 = \{1, r, r^2, s, rs, r^2s\}$ of order six and its cyclic subgroup $K = \{1, r, r^2\}$. By Example 3.1.1, we have that $xK = Kx$ for every element $x \in D_3$.

Consequently, it follows by Proposition 3.2.1 that K is a normal subgroup of D_3, i.e., $K \trianglelefteq D_3$. Even more, there are two distinct cosets of K in D_3 — namely, they are K and sK — hence the quotient group D_3/K has two distinct elements K and sK satisfying that $(sK)(sK) = s^2K = K$.

Proposition 3.2.4. *Every subgroup of an abelian group is normal.*

Proof. Let H be any subgroup of an abelian group G. Observe that for every element $g \in G$ and every element $h \in H$, we have that $gh = hg$, i.e., it holds that ghg^{-1} lies in H. □

Example 3.2.5. Consider the abelian group $(\mathbb{Z}, +)$ of the integers under addition and its normal subgroup $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$. By Proposition 3.2.4, $2\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$, hence we may form the quotient group $\mathbb{Z}/2\mathbb{Z}$. By Example 3.1.2, $(\mathbb{Z}/2\mathbb{Z}, +)$ consists of the two distinct cosets $0+2\mathbb{Z}$ and $1+2\mathbb{Z}$ satisfying that $(0+2\mathbb{Z})+(1+2\mathbb{Z}) = 1+2\mathbb{Z}$ and $(1+2\mathbb{Z})+(1+2\mathbb{Z}) = 2+2\mathbb{Z} = 0+2\mathbb{Z}$.

Generally, for any positive integer n, we may consider the subgroup $n\mathbb{Z} = \{qn \mid q \in \mathbb{Z}\}$ of $\mathbb{Z}$. Considering that $\mathbb{Z}$ is abelian, Proposition 3.2.4 yields that $n\mathbb{Z}$ is normal, hence Corollary 3.2.2 implies that $\mathbb{Z}/n\mathbb{Z}$ is a group with respect to the operation $(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$. Consequently, for any integer $k \in \mathbb{Z}$, we have that $k(1+n\mathbb{Z}) = k+n\mathbb{Z}$, hence $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n: the coset $1+n\mathbb{Z}$ generates $\mathbb{Z}/n\mathbb{Z}$, and the cosets $0+n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$ are distinct. We will soon establish that $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_n$ are "indistinguishable" groups under addition.

We demonstrate next that the quotient groups inherits some properties of the original group.

Proposition 3.2.6. *Let G be a group. Let H be a normal subgroup of G.*

(1.) *If G is cyclic, then G/H is cyclic. Explicitly, if $G = \langle g \rangle$, then $G/H = \langle gH \rangle$.*

(2.) *If G is abelian, then G/H is abelian.*

Proof. (1.) By definition, if G is cyclic, then there exists an element $g \in G$ such that every element of G can be written as g^n for some integer n. Consequently, for any coset xH of G/H, there exists an integer n such that $x = g^n$ and $xH = g^nH = (gH)^n$. We conclude that G/H is cyclic.

(2.) By definition, if G is abelian, then $g_1g_2 = g_2g_1$ for all elements $g_1, g_2 \in G$. Consequently, for all cosets g_1H, g_2H of H in G, it follows that $(g_1H)(g_2H) = g_1g_2H = g_2g_1H = (g_2H)(g_1H)$. □

3.3 Group Homomorphisms

Given a pair of groups $(G, *)$ and $(H, \star)$, we say that a function $\varphi : G \to H$ is a **group homomorphism** if and only if $\varphi(g_1 * g_2) = \varphi(g_1) \star \varphi(g_1)$ for all elements $g_1, g_2 \in G$. Put another way, a group homomorphism is a function between groups for which the binary operations of the two groups are compatible in the sense that the image of a product of two elements in the domain is the product of the images of the elements in the codomain. Let us try a few examples before we discuss further.

Example 3.3.1. Consider the group $(\mathbb{Z}, +)$ of integers under addition. Given any integer n, we may define a function $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ by $\varphi_n(m) = mn$. Observe that for any pair of integers ℓ and m, we have that $\varphi_n(\ell+m) = n(\ell+m) = \ell n + mn = \varphi_n(\ell) + \varphi_n(m)$, hence φ is a group homomorphism. Even more, because the domain and codomain of φ are equal, we say that φ is an **endomorphism**.

Example 3.3.2. Consider the group $(\mathbb{Z}/n\mathbb{Z}, +)$ of integers modulo a positive integer n and the multiplicative group $(G, \cdot)$ of the nth roots of unity. By definition of the integers modulo n, every element of $\mathbb{Z}/n\mathbb{Z}$ is of the form $k + n\mathbb{Z}$ for some integer $1 \leq k \leq n$. By definition of the nth roots of unity, every element of G is of the form $\text{cis}(2\pi k/n) = \cos(2\pi k/n) + i\sin(2\pi k/n)$ for some integer $1 \leq k \leq n$, where i is the complex number satisfying that $i^2 = -1$. Consequently, it is natural to consider the function $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\varphi(k + n\mathbb{Z}) = \text{cis}(2\pi k/n)$. **Caution:** this function is defined on the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$, so we must check that this rule is well-defined, i.e., that it does not depend on our choice of coset representative. We assume to this end that we have two different coset representative for the same coset, i.e., suppose that $k+n\mathbb{Z} = \ell+n\mathbb{Z}$. By subtracting $\ell+n\mathbb{Z}$ from both sides, we have that $(k-\ell)+n\mathbb{Z} = 0+n\mathbb{Z}$. Observe that this implies that $k - \ell = mn$ for some integer m so that $k = mn + \ell$ and $2\pi k/n = 2\pi m + 2\pi\ell/n$. Considering that $\cos(2\pi m + \theta) = \cos(\theta)$ and $\sin(2\pi m + \theta) = \sin(\theta)$, we conclude that $\text{cis}(2\pi k/n) = \text{cis}(2\pi m + 2\pi\ell/n) = \text{cis}(2\pi\ell/n)$, hence φ is well-defined. Even more, φ is a group homomorphism because we have that

$$\varphi((k + n\mathbb{Z}) + (\ell + n\mathbb{Z})) = \varphi(k + \ell + n\mathbb{Z}) = \text{cis}(2\pi(k + \ell)/n) = \text{cis}(2\pi k/n)\,\text{cis}(2\pi\ell/n)$$

for any integers k and ℓ by Proposition 2.4.4. Observe that φ respects the ostensibly different binary operations of each group: it takes the sum of two cosets of $\mathbb{Z}$ to a product of complex numbers.

Example 3.3.3. Given any element g of a group G, we claim that the function $\chi_g : G \to G$ defined by $\chi_g(x) = gxg^{-1}$ is a group homomorphism. Observe that for any pair of elements $x, y \in G$, we have that $\chi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \chi_g(x)\chi_g(y)$. Consequently, we have that χ_g is a group homomorphism; it is an endomorphism that sends $x \in G$ to its **conjugate** gxg^{-1} by g.

Example 3.3.4. Consider an abelian group G. We will demonstrate that the inversion function $\varphi : G \to G$ defined by $\varphi(g) = g^{-1}$ is a group endomorphism. By assumption that G is abelian, for any elements $g, h \in G$, we have that $\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \varphi(g)\varphi(h)$.

We begin our more general discussion with some basic properties of group homomorphisms.

Proposition 3.3.5. *Consider a group homomorphism $\varphi : (G, *) \to (H, \star)$.*

1.) *We have that $\varphi(e_G) = e_H$.*

2.) *We have that $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all elements $g \in G$.*

3.) *Given any element $g \in G$, we have that $\varphi(g^n) = \varphi(g)^n$ for any integer n.*

4.) *Given any element $g \in G$, the order of g divides the order of $\varphi(g)$.*

5.) *Given any subgroup K of G, we have that $\varphi(K)$ is a subgroup of H.*

Proof. (1.) Observe that $e_G = e_G e_G$, hence we have that $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Cancelling a factor of $\varphi(e_G)$ from both sides yields that $\varphi(e_G) = e_H$.

(2.) Observe that $gg^{-1} = e_G$, hence part (1.) yields that $e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. By multiplying on the left of each side, we find that $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(3.) Observe that if n is a non-negative integer, then $\varphi(g^n) = \varphi(g) \star \cdots \star \varphi(g)$ with n factors of $\varphi(g)$. By definition, this implies that $\varphi(g^n) = \varphi(g)^n$. Conversely, if n is a negative integer, then $\varphi(g^n) = \varphi(g^{-1} * \cdots * g^{-1}) = \varphi(g^{-1}) \star \cdots \star \varphi(g^{-1})$ with $-n$ factors of $\varphi(g^{-1})$.

(4.) If $\operatorname{ord}(g) = r$, then $e_H = \varphi(e_G) = \varphi(g^r) = \varphi(g)^r$, and the result holds by Corollary 2.3.13.

(5.) Consider a subgroup K of G. We claim that $\varphi(K) = \{\varphi(k) \mid k \in K\}$ is a subgroup of H. Considering that $e_G \in K$, we have that $\varphi(e_G) = e_H$ lies in $\varphi(K)$, hence it is nonempty. We proceed by the One-Step Subgroup Test. Explicitly, for any elements $\varphi(k_1), \varphi(k_2) \in \varphi(K)$, we have that $k_1 * k_2^{-1}$ lies in the subgroup K so that $\varphi(k_1) \star \varphi(k_2)^{-1} = \varphi(k_1) \star \varphi(k_2^{-1}) = \varphi(k_1 * k_2^{-1}) \in \varphi(K)$. □

Because it encodes a lot of important data about the underlying group G, we will take much care to determine the **kernel** $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$ of a group homomorphism $\varphi : G \to H$. Our first result along these lines is that the kernel of a group homomorphism detects injectivity.

Proposition 3.3.6. *If $\varphi : (G, *) \to (H, \star)$ is a group homomorphism, then φ is injective if and only the kernel of φ is the trivial subgroup of G, i.e., $\ker \varphi = \{e_G\}$.*

Proof. We will assume first that φ is injective. Given any element $g \in \ker \varphi$, by the first part of Proposition 3.3.5, we have that $\varphi(g) = e_H = \varphi(e_G)$ so that $g = e_G$ by the injectivity of φ.

Conversely, we will assume that $\ker \varphi$ is trivial. If $\varphi(g_1) = \varphi(g_2)$ for some elements $g_1, g_2 \in G$, then by the second part of Proposition 3.3.5, we have that $e_H = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1 g_2^{-1})$. By hypothesis that $\ker \varphi$ is trivial, it follows that $g_1 g_2^{-1} = e_G$ so that $g_1 = g_2$. □

Example 3.3.7. Consider the group homomorphism $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi_n(m) = mn$ for some nonzero integer n. Observe if m is an integer and $mn = 0$, then we must have that $m = 0$. We conclude that $\ker \varphi_n = \{m \in \mathbb{Z} \mid mn = 0\} = \{0\}$, hence φ_n is injective. We could have also proven this directly: indeed, if $mn = \varphi_n(m) = \varphi_n(\ell) = \ell n$, then cancelling n from both sides gives $m = \ell$.

Example 3.3.8. Let n be a positive integer. Let G denote the multiplicative group of nth roots of unity. Consider the group homomorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\varphi(k + n\mathbb{Z}) = \operatorname{cis}(2\pi k/n)$. We have that $\operatorname{cis}(2\pi k/n) = 1$ if and only if $k = mn$ for some integer m if and only if $k + n\mathbb{Z} = 0 + n\mathbb{Z}$. Consequently, we conclude by Proposition 3.3.6 that φ is injective.

Example 3.3.9. Conjugation by a group element is an injective group endomorphism. Explicitly, we have that $gxg^{-1} = e_G$ if and only if $x = e_G$ for every pair of elements $g, x \in G$.

Example 3.3.10. Inversion is an injective group endomorphism of any abelian group because for any element $g \in G$, we have that $g^{-1} = e_G$ if and only if $g = e_G$.

Example 3.3.11. Consider the function $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\pi(k) = k + n\mathbb{Z}$, where n is a positive integer. Observe that $\pi(k + \ell) = (k + \ell) + n\mathbb{Z} = (k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) = \pi(k) + \pi(\ell)$, hence π is a group homomorphism called the **projection** of $\mathbb{Z}$ onto $\mathbb{Z}/n\mathbb{Z}$. Observe that an integer m lies in $\ker \pi$ if and only if $m + n\mathbb{Z} = 0 + n\mathbb{Z}$ if and only if $m = nr$ for some integer r if and only if m lies in $n\mathbb{Z}$. Consequently, the kernel of π is $n\mathbb{Z}$, hence π is not injective.

We refer to a bijective (i.e., injective and surjective) group homomorphism as a **group isomorphism**. Group isomorphisms can be thought of as a means of relabelling elements in the target group with elements in the domain. Explicitly, if $\varphi : (G, *) \to (H, \star)$ is a group isomorphism, then for every element $h \in H$, there exists an element $g \in G$ such that $h = \varphi(g)$. Put another way, every element of H can be labelled with an element of G. Even more, this labelling is unique because φ is injective, hence if $\varphi(g_1) = \varphi(g_2)$, then $g_1 = g_2$. Otherwise stated, if two elements of H have the same label by an element of G, then the two elements of H are equal. Every element of H may

therefore be labelled uniquely with an element of G. Even more, this labelling respects the binary operations of G and H because it is a group homomorphism. We say that $(G, *)$ and $(H, \star)$ are **isomorphic** if there exists a group isomorphism between them, and we write $(G, *) \cong (H, \star)$.

Example 3.3.12. Let n be a positive integer. Let G denote the multiplicative group of nth roots of unity. Consider the group homomorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\varphi(k + n\mathbb{Z}) = \text{cis}(2\pi k/n)$. Considering that $\mathbb{Z}/n\mathbb{Z}$ and G are finite sets of the same cardinality and φ is injective by Example 3.3.8, we conclude by Exercise 1.10.5 that φ is surjective, hence it is an isomorphism.

Example 3.3.13. Conjugation by a group element is an injective group endomorphism; it is also surjective because every element $x \in G$ can be written as $x = g(g^{-1}xg)g^{-1}$. Consequently, conjugation is an isomorphism from a group to itself; it is a **group automorphism**.

Example 3.3.14. Inversion is an injective group endomorphism of any abelian group; even if the group is not abelian, it is both injective and surjective because every element $g \in G$ satisfies that $g = (g^{-1})^{-1}$. Consequently, inversion is a group automorphism of any abelian group.

Example 3.3.15. Observe that if n is an integer other than ± 1, then the injective group homomorphism $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi_n(m) = mn$ is not surjective because $mn \neq 1$ for any integer m. Consequently, φ_n is not an isomorphism for any integer other than $n = \pm 1$.

Example 3.3.16. Generally, the projection map $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\pi(k) = k + n\mathbb{Z}$ for a positive integer n is not an isomorphism because it is not injective; it is always surjective.

By the paragraph preceding Example 3.3.12, we intuitively suspect that the function inverse of a group isomorphism is a group isomorphism. We could also reasonably expect that two groups are isomorphic only if they have the same properties, e.g., if two groups are isomorphic and one of the groups is cyclic or abelian, then the other group must also be cyclic or abelian.

Proposition 3.3.17. *Consider a group isomorphism $\varphi : (G, *) \to (H, \star)$.*

1.) *We have that $|G| = |H|$.*

2.) *We have that $\varphi^{-1} : H \to G$ is a group isomorphism.*

3.) *We have that G is abelian if and only if H is abelian.*

4.) *We have that G is cyclic if and only if H is cyclic.*

5.) *Every subgroup of G induces a subgroup of H and vice-versa. Particularly, if G and H are isomorphic, then G and H must have the same number of (proper non-trivial) subgroups.*

Proof. (1.) Exercise 1.10.6(a.) demonstrates that $|G| = |H|$ for any pair of sets G and H for which there exists a bijection $\varphi : G \to H$, hence we may move onto the group-theoretic properties.

(2.) Considering that $\varphi : G \to H$ is a bijection, every element of H can be written uniquely as $\varphi(g)$ for some element $g \in G$, hence the function $\varphi^{-1} : H \to G$ defined by $\varphi^{-1}(\varphi(g)) = g$ is well-defined. Certainly, φ^{-1} is surjective; it is injective because if $\varphi^{-1}(\varphi(g)) = g = h = \varphi^{-1}(\varphi(h))$, then $\varphi(g) = \varphi(h)$ by applying φ to each side of the identity $g = h$. Last, we have that

$$\varphi^{-1}(\varphi(g_1) \star \varphi(g_2)) = \varphi^{-1}(\varphi(g_1 * g_2)) = g_1 * g_2 = \varphi^{-1}(\varphi(g_1)) * \varphi^{-1}(\varphi(g_2)).$$

(3.) Given any elements $h_1, h_2 \in H$, we claim that $h_1 \star h_2 = h_2 \star h_1$. By assumption that φ is surjection, there exist elements $g_1, g_2 \in G$ such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$. We conclude that

$$h_1 \star h_2 = \varphi(g_1) \star \varphi(g_2) = \varphi(g_1 * g_2) = \varphi(g_2 * g_1) = \varphi(g_2) \star \varphi(g_1) = h_2 \star h_1$$

by assumption that G is abelian; the same argument applied to $\varphi^{-1} : H \to G$ yields the converse.

(4.) If G is cyclic, then there exists an element $g \in G$ such that every element of G can be written as g^n for some integer n. Considering that φ is surjective, every element of H can be written as $h = \varphi(g^n) = \varphi(g * \cdots * g) = \varphi(g) \star \cdots \star \varphi(g) = \varphi(g)^n$ for some integer n. Consequently, we find that H is cyclic; it is generated by the image of the generator of G under the isomorphism φ.

(5.) By the fifth part of Proposition 3.3.5, every subgroup K of G induces the subgroup $\varphi(K)$ of H, hence H has at least as many subgroups as G. Conversely, every subgroup L of H induces the subgroup $\varphi^{-1}(L)$ of G, hence G has at least as many subgroups as H. We conclude that G and H possess the same number of subgroups. Last, we have that $\varphi(K) = \{e_H\}$ if and only if $K = e_G$ and $\varphi(K) = H$ if and only if $K = G$ because φ is a bijective group homomorphism. □

Using the language of group isomorphisms, we will formally establish that there is "essentially" only one infinite cyclic group, and there is "essentially" only one finite cyclic group.

Theorem 3.3.18. *Every infinite cyclic group is isomorphic to* $(\mathbb{Z}, +)$.

Proof. Consider any infinite cyclic group G. By definition, there exists an element $g \in G$ such that every element of G can be written as g^n for some integer $n \in \mathbb{Z}$. Observe that if $g^m = g^n$ for some integers m and n, then $e_G = g^m(g^n)^{-1} = g^m g^{-n} = g^{m-n}$ by the Group Exponent Laws, hence the order of g (i.e., the order of G) is finite — a contradiction. Consequently, every element of G can be written uniquely as g^n for some integer $n \in \mathbb{Z}$. We may therefore define a bijective function $\varphi : \mathbb{Z} \to G$ by $\varphi(n) = g^n$. Considering that $\varphi(m + n) = g^{m+n} = g^m g^n = \varphi(m)\varphi(n)$ by the Group Exponent Laws, we conclude that φ is an isomorphism, hence G is isomorphic to $(\mathbb{Z}, +)$. □

Lemma 3.3.19. *If $\varphi : G \to H$ is a group homomorphism of finite groups of the same order, then φ is an isomorphism if and only if φ is injective if and only if φ is surjective.*

Proof. By definition, we have that φ is an isomorphism if and only if φ is bijective if and only if φ is injective and surjective. By assumption that G and H are finite groups of the same order, Exercise 1.10.5(d.) implies that φ is bijective if and only if it is injective if and only if it is surjective. □

Theorem 3.3.20. *Every finite cyclic group of order n is isomorphic to* $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proof. Consider a finite cyclic group G of order n. By definition, there exists an element $g \in G$ such that $G = \{g^k \mid 0 \leq k \leq n-1\}$. Consequently, we may define a function $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ by the assignment $\varphi(k + n\mathbb{Z}) = g^k$. We must demonstrate that φ is well-defined, i.e., $\varphi(k + n\mathbb{Z})$ does not depend upon the coset representative of $k + n\mathbb{Z}$. We will assume to this end that $k + n\mathbb{Z} = \ell + n\mathbb{Z}$. By definition, this means that $k - \ell = mn$ and $k = mn + \ell$ for some integer m so that

$$\varphi(k + n\mathbb{Z}) = g^k = g^{mn+\ell} = g^{mn} g^\ell = (g^n)^m g^\ell = (e_G)^m g^\ell = e_G g^\ell = g^\ell = \varphi(\ell + n\mathbb{Z})$$

by the Group Exponent Laws. We conclude that φ is well-defined; it is surjective by definition of $\mathbb{Z}/n\mathbb{Z}$ and φ, hence we conclude by Lemma 3.3.19 that φ is an isomorphism. □

Example 3.3.21. Consider the multiplicative group of complex numbers $G = \{1, -1, i, -i\}$. Observe that $i^2 = -1$, $i^3 = -i$, and $i^4 = 1$, hence G is a finite cyclic group of order four; it is generated by i. Consequently, by Theorem 3.3.20, we conclude that $(G, \cdot) \cong (\mathbb{Z}/4\mathbb{Z}, +)$. Explicitly, by the proof of the theorem, the isomorphism $\varphi : \mathbb{Z}/4\mathbb{Z} \to G$ is defined by $\varphi(n + 4\mathbb{Z}) = i^n$.

3.4 Cayley's Theorem

Cayley's Theorem is an example of a simple observation with larger implications.

Theorem 3.4.1 (Cayley's Theorem)**.** *Every group is isomorphic to a group of permutations.*

Proof. Given a group G and any element $g \in G$, consider the function $\varphi_g : G \to G$ defined by $\varphi_g(x) = gx$. By hypothesis that G is a group, it follows that g^{-1} is an element of G so that

$$\varphi_g \circ \varphi_{g^{-1}}(x) = \varphi_g(g^{-1}x) = gg^{-1}x = e_G x = x = e_G x = g^{-1}gx = \varphi_{g^{-1}}(gx) = \varphi_{g^{-1}} \circ \varphi_g(x)$$

for every element $x \in G$. Consequently, it follows that $\varphi_{g^{-1}}$ is the function inverse of φ_g so that φ_g is a bijection from G to itself by Exercise 1.10.6(b.). By definition, φ_g is a permutation of G, hence it is an element of the symmetric group $\mathfrak{S}_G$ on the set G. We claim that $\sigma : G \to \mathfrak{S}_G$ defined by $\sigma(g) = \varphi_g$ is a group homomorphism. Observe that for any elements $g_1, g_2, x \in G$, we have that

$$\sigma(g_1 g_2)(x) = \varphi_{g_1 g_2}(x) = g_1 g_2 x = \varphi_{g_1}(g_2 x) = \varphi_{g_1} \circ \varphi_{g_2}(x).$$

Considering that $x \in G$ is arbitrary, it follows that $\sigma(g_1 g_2) = \varphi_{g_1} \circ \varphi_{g_2} = \sigma(g_1) \circ \sigma(g_2)$ so that σ is a group homomorphism. Observe that $g \in \ker \sigma$ if and only if if and only if φ_g is the identity function from G to itself if and only if $gx = \varphi_g(x) = x$ for all elements $x \in G$ if and only if $g = e_G$ by cancellation in G. We conclude that σ is injective; its image $\sigma(G)$ is a subgroup of $\mathfrak{S}_G$ by the fifth part of Proposition 3.3.5. Consequently, we conclude that $G \cong (\sigma(G), \circ)$. □

Corollary 3.4.2. *Every finite group of order n is isomorphic to a subgroup of $\mathfrak{S}_n$.*

Proof. By Cayley's Theorem, every finite group G of order n is isomorphic to a subgroup of $\mathfrak{S}_G$. We claim that $(\mathfrak{S}_G, \circ) \cong (\mathfrak{S}_n, \circ)$. By Exercise 1.10.5(c.), there exists a bijection $f : G \to \{1, 2, \ldots, n\}$ because these are finite sets of the same cardinality by assumption. We can extend f to a group isomorphism $\varphi : \mathfrak{S}_G \to \mathfrak{S}_n$ by declaring that for any permutation σ in $\mathfrak{S}_G$, we have that $\varphi(\sigma)$ is the permutation in $\mathfrak{S}_n$ that maps $f(g)$ to $f(h)$ whenever $\sigma(g) = h$. Explicitly, we may define a function $\varphi : \mathfrak{S}_G \to \mathfrak{S}_n$ by $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$. We claim that φ is a well-defined group isomorphism.

(1.) $\varphi(\sigma)$ is a permutation of $\{1, 2, \ldots, n\}$ because it is a bijection from $\{1, 2, \ldots, n\}$ to itself. Consequently, the function φ is well-defined because its image is a subset of $\mathfrak{S}_n$.

(2.) φ is a group homomorphism because $\varphi(\sigma \circ \tau) = f \circ (\sigma \circ \tau) \circ f^{-1} = (f \circ \sigma \circ f^{-1}) \circ (f \circ \tau \circ f^{-1})$ shows that $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$ by the associativity of function composition.

(3.) φ is a bijection with function inverse $\psi : \mathfrak{S}_n \to \mathfrak{S}_G$ defined by $\psi(\rho) = f^{-1} \circ \rho \circ f$. By Exercise 1.10.6, it suffices to note that $\psi \circ \varphi(\sigma) = \psi(f \circ \sigma \circ f^{-1}) = f^{-1} \circ (f \circ \sigma \circ f^{-1}) \circ f = \sigma$. □

Cayley's Theorem expressly motivates the study of symmetric groups because it demonstrates that every group can be "identified with" a group of permutations. Consequently, we will later return to our discussion of symmetric groups to develop even more tools to understand them.

3.5 The Group Isomorphism Theorems

Earlier in this chapter, we mentioned that one of the principal motivations in group theory (and the focus of this chapter) is the classification of groups. Explicitly, we seek to distinguish two groups based on properties such as their order, whether they are cyclic, whether they are abelian, and what kinds of subgroups they admit. Exercise 3.10.20 demonstrates that the existence of a group isomorphism between two groups is an equivalence relation; we say that two groups lie in the same equivalence class modulo this equivalence relation if and only if they are equal **up to isomorphism**. Consequently, we wish to determine all groups with a specified property $\mathcal{P}$ up to isomorphism.

Example 3.5.1. We have already seen in Example 2.2.12 that $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ are two groups of order four that are not isomorphic to one another. Explicitly, the only non-trivial proper subgroup of $\mathbb{Z}/4\mathbb{Z}$ is $2\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 2 + 4\mathbb{Z}\}$; however, there are three non-trivial proper subgroups of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, hence these two groups cannot be isomorphic by Proposition 3.3.17. Every cyclic group of order four is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ by Proposition 3.3.20; we will soon see that every non-cyclic abelian group of order four is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

We will now state and prove the **Group Isomorphism Theorems**; these four theorems provide us with a road map by which we may begin to tackle the classification problem of groups.

Theorem 3.5.2 (First Isomorphism Theorem)**.** *Given any groups $(G, *)$ and $(H, \star)$ and a group homomorphism $\varphi : G \to H$, there exists a group isomorphism $\psi : G/\ker\varphi \to \varphi(G)$.*

Proof. We note that $\varphi(G)$ is a subgroup of H by the fifth part of Proposition 3.3.5. Exercise 3.10.19 shows that $\ker\varphi$ is a normal subgroup of G, hence we may view $G/\ker\varphi$ as a group with respect to the operation $*$ of G. Even more, in order to prove the claim, it suffices to find a group isomorphism $\psi : G/\ker\varphi \to \varphi(G)$. Consider the function $\psi : G/\ker\varphi \to \varphi(G)$ defined by $\psi(g * \ker\varphi) = \varphi(g)$. Considering that ψ is defined on the equivalence classes of an equivalence relation, we must establish that ψ is well-defined, i.e., we must show that if $g*\ker\varphi = h*\ker\varphi$, then $\psi(g*\ker\varphi) = \psi(h*\ker\varphi)$. By Proposition 3.1.4, we have that $g * \ker\varphi = h * \ker\varphi$ if and only if $h^{-1}g \in \ker\varphi$ if and only if $\varphi(h^{-1}g) = e_H$ if and only if $\varphi(h^{-1}) \star \varphi(g) = e_H$ if and only if $\varphi(h)^{-1} \star \varphi(g) = e_H$ if and only if $\varphi(g) = \varphi(h)$ if and only if $\psi(g * \ker\varphi) = \psi(h * \ker\varphi)$. We conclude that ψ is well-defined. By hypothesis that φ is a group homomorphism, it follows that ψ is a group homomorphism. Even more, ψ is surjective because its image is $\varphi(G)$, hence it suffices to show that ψ is injective. Observe that $g * \ker\varphi \in \ker\psi$ if and only if $\varphi(g) = \psi(g * \ker\varphi) = e_H$ if and only if $g \in \ker\varphi$ if and only if $g * \ker\varphi = e_G * \ker\varphi$, hence we conclude that $\ker\psi$ is trivial so that ψ is injective, as desired. □

Theorem 3.5.3 (Second Isomorphism Theorem)**.** *Given any group G with a subgroup H and a normal subgroup N, we have that HN/N and $H/(H \cap N)$ are isomorphic groups.*

Proof. We must first demonstrate that HN is a subgroup of G such that N is a normal subgroup of HN; this proves that HN/N is a group. By Exercise 3.10.11, we find that HN is a subgroup of G, so we will prove that N is a normal subgroup of HN. Every element $n \in N$ can be written as $e_G n$ so that $N \subseteq HN$; moreover, N is a subgroup of G, so it is a subgroup of HN. Last, by Proposition 3.2.1, we have that $gN = Ng$ for all elements $g \in G$, so this identity also holds for all elements $g \in HN$. Put another way, if N is normal in G, then it is normal in any subgroup containing it.

By Exercise 3.10.12, it follows that $H \cap N$ is a normal subgroup of H and $H/(H \cap N)$ is a group. We may now appeal to the First Isomorphism Theorem, hence it suffices to find a surjective group homomorphism $\varphi : H \to HN/N$ such that $\ker \varphi = H \cap N$. Consider the function $\varphi : H \to HN/N$ defined by $\varphi(h) = hN$. Every element of HN/N is of the form $(hn)N$ for some elements $h \in H$ and $n \in N$. Considering that N is a subgroup of G, it follows that $nN = N$, hence every element of HN/N is of the form hN for some element $h \in H$. We conclude that φ is well-defined and surjective. Even more, we have that $\varphi(h_1h_2) = h_1h_2N = (h_1N)(h_2N)$ because N is a normal subgroup of HN. Consequently, φ is a group homomorphism; its kernel consists of those elements $h \in H$ such that $hN = e_GN$. By Proposition 3.1.4, we have that $hN = e_GN$ if and only if $h \in N$, from which it follows that $\ker \varphi = H \cap N$. Our proof is complete by the First Isomorphism Theorem. □

Theorem 3.5.4 (Third Isomorphism Theorem)**.** *Given any group G with normal subgroups N and H such that $N \subseteq H$, we have that $(G/N)/(H/N)$ and G/N are isomorphic groups.*

Proof. By Proposition 3.2.1, we have that $gN = Ng$ for all elements $g \in G$, hence in particular, this identity also holds for all elements $g \in H$. We conclude that N is a normal subgroup of H because it is a subset of H that is a group with respect to the binary operation on G and N is normal in H. Consequently, it follows that H/N is a group; likewise, it is a subgroup of G/N because it is a subset of G/N that is a group under the binary operation on G/N. Even more, we claim that H/N is a normal subgroup of G/N. Consider an element gN of G/N and an element hN of H/N. By definition of the binary operation of G/N, we have that $(gN)(hN) = ghN$. By assumption that H is a normal subgroup of G, we have that $gH = Hg$ for all elements $g \in G$. Explicitly, there exists an element $k \in H$ such that $gh = kg$, from which it follows that $ghN = kgN = (kN)(gN)$. Considering that this holds for all elements $gN \in G/N$ and $hN \in H/N$, we conclude that $(gN)(H/N) \subseteq (H/N)(gN)$ for all elements $gN \in G/N$ so that H/N is a normal subgroup of G/N by Proposition 3.2.1.

We seek a surjective group homomorphism $\varphi : G/N \to G/H$ such that $\ker \varphi = H/N$. Consider the function $\varphi : G/N \to G/H$ defined by $\varphi(gN) = gH$. We must first establish that φ is well-defined because its domain consists of the left cosets of a group. Observe that if $g_1N = g_2N$, then $g_2^{-1}g_1$ is an element of N by Proposition 3.1.4. By assumption that $N \subseteq H$, it follows that $g_2^{-1}g_1$ is an element of H, hence the same proposition demonstrates that $\varphi(g_1N) = g_1H = g_2H = \varphi(g_2N)$ and φ is well-defined. Every element of G/H can be written as gH for some element $g \in G$. Even more, if g does not lie in H, then it does not lie in N because N is a subset of H, hence every left coset gH is the image of the left coset gN, i.e., φ is surjective. Last, we have that gN lies in $\ker \varphi$ if and only if $gH = \varphi(gN) = e_GH$ if and only if $g \in H$ by Proposition 3.1.4, hence we conclude that $\ker \varphi = H/N$. By the First Isomorphism Theorem, we conclude that $(G/H)/(H/N) \cong G/N$. □

Theorem 3.5.5 (Fourth Isomorphism Theorem)**.** *Given a group G with a normal subgroup N, there exists a one-to-one correspondence between the subgroups of G that contain N and the subgroups of G/N induced by the assignment of a subgroup H of G with $N \subseteq H$ to the subgroup H/N of G/N. Even more, this one-to-one correspondence satisfies the following properties.*

1.) *Given any subgroups H and K of G such that $N \subseteq H$ and $N \subseteq K$, we have that $H \subseteq K$ if and only if $H/N \subseteq K/N$. Put another way, this bijective correspondence is inclusion-preserving.*

2.) *Given any subgroups H and K of G such that $N \subseteq H \subseteq K$, we have that*

$$[K : H] = [K/N : H/N].$$

3.) *Given any subgroups H and K of G such that $N \subseteq H$ and $N \subseteq K$, we have that*

$$(H \cap K)/N = (H/N) \cap (K/N).$$

4.) *Given any subgroup H of G such that $N \subseteq H$, we have that $H \trianglelefteq G$ if and only if $H/N \trianglelefteq G/N$.*

Proof. We must prove first that the assignment of a subgroup H of G with $N \subseteq H$ to the subgroup H/N of G/N is both injective and surjective. Observe that if $H/N = K/N$, then for every element $h \in H$, there exists an element $k \in K$ such that $hN = kN$. Consequently, there exist elements $n_1, n_2 \in N$ such that $hn_1 = kn_2$ so that $h = kn_2n_1^{-1}$. By assumption that $N \subseteq K$, it follows that $h = kn_2n_1^{-1}$ is an element of K. We conclude that $H \subseteq K$. Conversely, an analogous argument demonstrates that $K \subseteq H$, from which it follows that $H = K$, and this assignment is injective. Given a subgroup Q of G/N, in order to prove that this assignment is surjective, we must furnish a subgroup H of G that contains N with the property that $Q = H/N$. Every element of G/N is a left coset of N in G, hence every element of Q is a left coset of N in G. Consider the collection $H = \{g \in G \mid gN \in Q\}$ of elements of G that give rise to elements of Q. By assumption that Q is a subgroup of G/N, the left coset e_GN lies in Q, hence we have that $e_G \in H$. Even more, for any elements $h_1, h_2 \in H$, we have that $h_1h_2N = (h_1N)(h_2N)$ lies in Q implies that $h_1h_2 \in H$ and $h_1^{-1}N = (h_1N)^{-1}$ lies in Q implies that $h_1^{-1} \in H$. We conclude by the Two-Step Subgroup Test that H is a subgroup of G. Given any element $n \in N$, we have that $nN = e_GN$ lies in Q, from which it follows that $N \subseteq H$ and $Q = H/N$. Ultimately, this shows that this assignment is surjective.

We turn our attention to the four asserted properties. We note that the first property holds by the first paragraph. Explicitly, if H and K are subgroups of G that contain N and satisfy that $H/N \subseteq K/N$, then it must be the case that $H \subseteq K$. Conversely, if we assume that $H \subseteq K$, then the inclusion $H/N \subseteq K/N$ holds by definition of left cosets. We note that the second property holds by the Third Isomorphism Theorem: if H and K are subgroups of G such that $N \subseteq H \subseteq K$, then the quotient groups K/H and $(K/N)/(H/N)$ are isomorphic; in particular, there is a bijection between K/H and $(K/N)/(H/N)$, hence the number of left cosets of H in K is equal to the number of left cosets of H/N in K/N. Put another way, we have that $[K : H] = [K/N : H/N]$. Even more, the third property holds by straightforward inspection: every element of $(H \cap K)/N$ is of the form $n(H \cap K)$, hence it is a left coset of N in both H and K. Conversely, every element of $(H/N) \cap (K/N)$ is a left coset of N in both H and K, hence it is a left coset of N in $H \cap K$.

Last, we turn our attention to the fourth property. We will assume to this end that H is a subgroup of G that contains N. We have already demonstrated in the proof of the Third Isomorphism Theorem that if H is a normal subgroup of G, then H/N is a normal subgroup of G/N. Conversely, suppose that H/N is a normal subgroup of G/N. Consequently, the **canonical surjections** $\pi_1 : G \to G/N$ and $\pi_2 : G/N \to (G/N)/(H/N)$ are group homomorphisms by Exercise 3.10.19; the composite function $\pi_2 \circ \pi_1 : G \to (G/N)/(H/N)$ defined by $\pi_2 \circ \pi_1(g) = gH$ is a group homomorphism with kernel H, hence H is a normal subgroup of G by Exercise 3.10.19. □

Example 3.5.6. Consider the general linear group $\mathrm{GL}(2, \mathbb{R}) = \{A \in \mathbb{R}^{2\times 2} \mid \det(A) \neq 0\}$ under matrix multiplication. We will use the First Isomorphism Theorem to prove that the multiplicative group $(\mathbb{R}^\times, \cdot)$ of nonzero real numbers is isomorphic to a subgroup of $\mathrm{GL}(2, \mathbb{R})$. Consider the function $\varphi : \mathbb{R}^\times \to \mathrm{GL}(2, \mathbb{R})$ defined by $\varphi(c) = cI$, where I is the 2×2 identity matrix. Observe that φ is

injective because $cI = dI$ if and only if $c = d$. Even more, it is a group homomorphism because for any real numbers c and d, we have that $\varphi(cd) = (cd)I = (cI)(dI) = \varphi(c)\varphi(d)$. Consequently, $(\mathbb{R}^\times, \cdot)$ is isomorphic to $\varphi(\mathbb{R}^\times) = \{cI \mid c \in \mathbb{R}^\times\}$, i.e., the nonzero real multiples of the identity matrix.

Example 3.5.7. We will prove next that multiplicative group $(\mathbb{R}_{>0}, +)$ of positive real numbers is isomorphic to a proper quotient of the multiplicative group $(\mathbb{R}^\times, \cdot)$ of nonzero real numbers, hence these groups are not isomorphic. Consider the function $\nu : \mathbb{R}^\times \to \mathbb{R}_{>0}$ defined by $\nu(x) = |x|$. Every positive real number can be written as its own absolute value, hence ν is surjective. Even more, ν is a group homomorphism because $\nu(xy) = |xy| = |x| \cdot |y|$. Consequently, we have that $x \in \ker \nu$ if and only if $|x| = 1$ if and only if $x = \pm 1$, hence we have that $\ker \nu = \{-1, 1\}$. By the First Isomorphism Theorem, we conclude that $(\mathbb{R}^\times/\{-1, 1\}, \cdot) \cong (\mathbb{R}_{>0}, \cdot)$ and $(\mathbb{R}_{>0}, \cdot) \ncong (\mathbb{R}^\times, \cdot)$.

Example 3.5.8. Before we conclude this section, we provide an example of the Third Isomorphism Theorem. Consider the additive group $(\mathbb{Z}/n\mathbb{Z}, +)$ of integers modulo a positive integer n. Given any integer m, we may also consider the additive group $(\mathbb{Z}/mn\mathbb{Z}, +)$. Observe that $n\mathbb{Z}/mn\mathbb{Z}$ the cyclic subgroup of $\mathbb{Z}/mn\mathbb{Z}$ generated by the image of n modulo $mn\mathbb{Z}$; in particular, we have that $n\mathbb{Z}/mn\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}/mn\mathbb{Z}$. By the Third Isomorphism Theorem, we have that

$$\frac{\mathbb{Z}/mn\mathbb{Z}}{n\mathbb{Z}/mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Consequently, it grants no additional information to take subsequent quotients of $\mathbb{Z}$.

3.6 The Symmetric Group on n Letters, Revisited

Back in Section 2.5, we introduced the group $(\mathfrak{S}_n, \circ)$ of bijections $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ under function composition, and we referred to this as the **symmetric group on n letters**. Quite a bit can be said about this very interesting group, so we return here to explore and discuss its properties further. By Proposition 2.5.13, we have that $\mathfrak{S}_n$ is not abelian for any integer $n \geq 3$. One way to measure the degree to which a group G fails to be abelian is by examining its **center**

$$Z(G) = \{x \in G \mid gx = xg \text{ for all elements } g \in G\}.$$

Observe that $Z(G)$ is the collection of elements of G that commute with all other elements of G. By Exercise 2.8.18, the center $Z(G)$ is the largest abelian subgroup of G.

Proposition 3.6.1. *For every integer $n \geq 3$, the center $Z(\mathfrak{S}_n)$ of the symmetric group $\mathfrak{S}_n$ is $\{\iota\}$.*

Proof. Certainly, the identity function $\iota : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ defined by $\iota(i) = i$ for all integers $1 \leq i \leq n$ commutes with every bijection $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$; ι is a bijection, so we have that $Z(\mathfrak{S}_n) \supseteq \{\iota\}$. On the contrary, we will assume that there exists a non-trivial permutation σ of $Z(\mathfrak{S}_n)$. Consequently, there exist distinct integers i and j such that $\sigma(i) = j$. By hypothesis that $n \geq 3$, there exists another integer k distinct from i and j. Consider the transposition $\tau = (i, k)$. We have that $\sigma\tau(i) = \sigma(k) \neq j = \tau(j) = \tau\sigma(i)$. For if it were the case that $\sigma(k) = j$, then we would have that $\sigma(k) = \sigma(i)$ so that $k = i$ by hypothesis that σ is a bijection — a contradiction. But then, σ does not commute with τ, contradicting our assumption that σ is in $Z(\mathfrak{S}_n)$. □

Given any permutation $\sigma \in \mathfrak{S}_n$ with cycle decomposition $\sigma_1 \cdots \sigma_k$ such that σ_i has length r_i, we may rearrange (if necessary) σ_i so that $r_1 \leq \cdots \leq r_k$. We refer to the ordered k-tuple $(r_1, \ldots, r_k)$ as the **cycle type** of σ. Considering that an ordered k-tuple $(r_1, \ldots, r_k)$ with $r_1 \leq \cdots \leq r_k$ and $r_1 + \cdots + r_k = n$ is an integer partition of n with k parts by definition, we have the following.

Proposition 3.6.2. *Given any positive integer n, the number of distinct cycle types of permutations in $\mathfrak{S}_n$ is equal to the number of distinct integer partitions of n.*

Given any element x of a group G, we say that an element of the form gxg^{-1} for some element $g \in G$ is **conjugate** to x. We will discuss this notation later in our section on the group actions and the Class Equation. Our next proposition states that cycle type is unique up to conjugation. One direction of this statement is established in the following proposition; the other is proved afterward.

Proposition 3.6.3. *Given any k-cycle $\sigma = (a_1, \ldots, a_k)$, we have that $\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_k))$ for every element τ in $\mathfrak{S}_n$ with $n \geq k$. Put another way, cycle type is preserved under conjugation.*

Proof. Given any integer $1 \leq i \leq n$, we will assume that $\sigma(i) = j$. By hypothesis that τ is a permutation, it follows that τ^{-1} exists and satisfies $\tau^{-1}(\tau(i)) = i$ so that $\sigma\tau^{-1}(\tau(i)) = \sigma(i) = j$. Consequently, we have that $\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$ so that $\tau\sigma\tau^{-1}$ sends $\tau(i)$ to $\tau(j)$.

Given that σ is the k-cycle $\sigma = (a_1, \ldots, a_k)$, it follows that σ fixes all integers in $[n] \setminus \{a_1, \ldots, a_k\}$, hence $\tau\sigma\tau^{-1}$ fixes all integers in $[n] \setminus \{\tau(a_1), \ldots, \tau(a_k)\}$. Likewise, we have that $\sigma(a_i) = a_{i+1}$ for all integers $1 \leq i \leq k-1$ and $\sigma(a_k) = a_1$, hence $\tau\sigma\tau^{-1}$ maps $\tau(a_i)$ to $\tau(a_{i+1})$ for all integers $1 \leq i \leq k-1$ and $\tau\sigma\tau^{-1}$ maps $\tau(a_k)$ to $\tau(a_1)$. Put another way, we have that $\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_k))$. □

Proposition 3.6.4. *For any permutations $\rho, \sigma \in \mathfrak{S}_n$, there exists a permutation $\tau \in \mathfrak{S}_n$ such that $\tau\rho\tau^{-1} = \sigma$ (i.e., ρ and σ are conjugate in $\mathfrak{S}_n$) if and only if ρ and σ have the same cycle type.*

Proof. By definition, if ρ and σ are conjugate in $\mathfrak{S}_n$, then there exists a permutation $\tau \in \mathfrak{S}_n$ such that $\tau\rho\tau^{-1} = \sigma$. We may assume that $\rho = \rho_k \cdots \rho_2\rho_1$ is the cycle decomposition of ρ so that

$$\sigma = \tau\rho\tau^{-1} = (\tau\rho_k\tau^{-1}) \cdots (\tau\rho_2\tau^{-1})(\tau\rho_1\tau^{-1})$$

is the cycle decomposition of σ. By Proposition 3.6.3, it follows that $\tau\rho_i\tau^{-1}$ are cycles of the same length as ρ_i, hence we must have that ρ and σ have the same cycle type.

Conversely, we will assume that ρ and σ have the same cycle type $(r_1, \ldots, r_k)$. Consequently, we have that $\rho = \rho_k \cdots \rho_1$ and $\sigma = \sigma_k \cdots \sigma_1$ for some disjoint cycles ρ_i and some disjoint cycles σ_i with $\text{length}(\rho_i) = r_i = \text{length}(\sigma_i)$. Considering that $[n]$ is a finite set, we may construct a bijection $\tau : [n] \to [n]$ that maps the cycle ρ_i to the cycle σ_i. Even more, we may construct τ in such a way that for any cycle $\rho_i = (a_{i,1}, \ldots, a_{i,r_i})$ and the corresponding cycle $\sigma_i = (b_{i,1}, \ldots, b_{i,r_i})$, we have that $\tau(a_{i,j}) = b_{i,j}$. We claim that $\tau\rho\tau^{-1} = \sigma$. By Proposition 3.6.3, we have that

$$\tau\rho\tau^{-1}(\tau(a_{i,j})) = \tau\rho(a_{i,j}) = \tau(a_{i+1,j}) = b_{i+1,j} = \sigma(b_{i,j}) = \sigma(\tau(a_{i,j})).$$

By construction, we have that τ is a bijection from $[n]$ to itself, hence every element of $[n]$ can be written as $\tau(a_{i,j})$ for some integer $1 \leq a_{i,j} \leq n$. We conclude therefore that $\tau\rho\tau^{-1} = \sigma$. □

Example 3.6.5. Exhibit a permutation that conjugates (123) and (132).

Solution. By the proof of Proposition 3.6.4, we have that $\tau(1) = 1$, $\tau(2) = 3$, and $\tau(3) = 2$, i.e., $\tau = (1)(23)$. Let us verify that $\tau\rho\tau^{-1} = \sigma$. Considering that $\tau\tau = (1)(23)(1)(23) = (1)(2)(3) = \iota$, it follows that $\tau = \tau^{-1}$ so that $\tau\rho\tau^{-1} = (1)(23)(123)(1)(23) = (132) = \sigma$, as desired. ◇

Example 3.6.6. Exhibit a permutation that conjugates $(135)(27)(48)(6)$ and $(1)(258)(34)(67)$.

Solution. Certainly, we could proceed as outlined in the proof of Proposition 3.6.4; however, this answer from Arturo Magidin gives a simpler approach. Begin by writing down the cycle types of the permutations $\rho = (135)(27)(48)(6)$ and $\sigma = (1)(258)(34)(67)$; then, arrange the cycles of ρ and σ in some (not necessarily unique) manner so that the cycles have non-decreasing length; and last, construct a 2×8 array whose first row is ρ and second row is σ. Observe that the cycle type of ρ and σ is $(1, 2, 2, 3)$, hence we may arrange $\rho = (6)(27)(48)(135)$ and $\sigma = (1)(34)(67)(258)$ to obtain

$$\tau = \begin{pmatrix} 6 & 2 & 7 & 4 & 8 & 1 & 3 & 5 \\ 1 & 3 & 4 & 6 & 7 & 2 & 5 & 8 \end{pmatrix}.$$

By reading off the array, we find that $\tau = (12358746)$. Observe that τ conjugates ρ to σ if and only if $\tau\rho\tau^{-1} = \sigma$ if and only if $\tau\rho = \sigma\tau$. We leave it to the reader to verify that $\tau\rho = \sigma\tau$, as desired. ◇

We turn our attention now to the matter of the combinatorics (or mathematics of counting) in the symmetric group. Our first result follows immediately from Propositions 3.6.2 and 3.6.4.

Proposition 3.6.7. *Given any positive integer n, the number of distinct conjugacy classes of the symmetric group $\mathfrak{S}_n$ is equal to the number of distinct integer partitions of n.*

Proof. By Proposition 3.6.4 above, there exists a bijection

$$\{\text{distinct conjugacy classes of } \mathfrak{S}_n\} \leftrightarrow \{\text{distinct cycle types of permutations in } \mathfrak{S}_n\}$$

that sends the conjugacy class of some permutation ρ with cycle type $(r_1, \ldots, r_k)$ to the cycle type $(r_1, \ldots, r_k)$. Explicitly, the permutations ρ and σ are conjugate (and hence in the same conjugacy class) if and only if they have the same cycle type, hence this map is injective. Further, this map is surjective because for any cycle type $(r_1, \ldots, r_k)$, we can construct a permutation ρ with cycle type $(r_1, \ldots, r_k)$. By Proposition 3.6.4, conjugation preserves cycle type. Consequently, we have that

$$\#\{\text{distinct conjugacy classes of } \mathfrak{S}_n\} = \#\{\text{distinct cycle types of permutations in } \mathfrak{S}_n\}.$$

By Proposition 3.6.2 above, the latter is equal to the number of distinct integer partitions of n. □

Often, the best way to count something is to establish a bijection between what we want to count and something for which we already know the cardinality; however, counting can sometimes be successfully accomplished by naïvely underestimating and multiplying by the number of times each element in the set was undercounted. We illustrate this principle in the following proposition.

Proposition 3.6.8. *Given any positive integer n, the number of distinct k-cycles in $\mathfrak{S}_n$ is $\frac{n!}{k(n-k)!}$.*

Proof. Every k-cycle in $\mathfrak{S}_n$ is constructed in the following manner.

1.) Choose k elements from among the n elements of $[n]$. We can do this in $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ ways.

2.) Order the k elements in some way. Bear in mind that there is no "first" term in the ordering because $(a_1, \ldots, a_k)$ is the same as $(a_k, a_1, \ldots, a_{k-1})$, etc. Consequently, the order only matters for $k-1$ of the elements, hence there are $(k-1)!$ ways to order the k elements.

By the Fundamental Counting Principle, there are $\frac{n!}{k!(n-k)!}(k-1)! = \frac{n!}{k(n-k)!}$ k-cycles in $\mathfrak{S}_n$. □

3.7 The Alternating Group on n Letters

We turn our attention to an important subgroup of the symmetric group on n letters. Until now, we have only briefly mentioned the notion of a transposition, i.e., a cycle of length two; however, transpositions are in fact ubiquitous in the study of permutations, as we demonstrate next.

Proposition 3.7.1. *Every permutation can be written as the product of a unique number of transpositions; however, the transpositions need not be disjoint.*

Proof. Considering that every permutation can be written as the product of disjoint cycles, it suffices to show that any cycle $(a_1, \ldots, a_k)$ can be written as a product of (not necessarily disjoint) transpositions. We note that $(a_1, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$ is a product of (not necessarily disjoint) transpositions. By Proposition 3.6.3, we have that cycle type is unique up to conjugation, hence the number of transpositions is uniquely determined by the cycle type of a permutation. □

Considering that every permutation σ in $\mathfrak{S}_n$ can be written as the product of a unique number of (not necessarily disjoint) transpositions, we can define the **parity** of a permutation to be the parity (even or odd) of the number $t(\sigma)$ of transpositions in the transposition decomposition of σ. Further, we refer to the number $\operatorname{sgn}(\sigma) = (-1)^{t(\sigma)}$ as the **sign** of the permutation σ. Observe that σ is even if and only if $\operatorname{sgn}(\sigma) = 1$, and likewise, σ is odd if and only if $\operatorname{sgn}(\sigma) = -1$.

Proposition 3.7.2. *Consider the function* $\operatorname{sgn} : \mathfrak{S}_n \to \{-1, 1\}$ *defined by* $\operatorname{sgn}(\sigma) = (-1)^{t(\sigma)}$. *We have that* $\ker(\operatorname{sgn})$ *is a normal subgroup of* $\mathfrak{S}_n$ *such that* $[\mathfrak{S}_n : \ker(\operatorname{sgn})] = 2$ *and* $|\ker(\operatorname{sgn})| = n!/2$.

Proof. Observe that $\{-1, 1\}$ is a multiplicative group with identity 1. Consequently, the fact that

$$\operatorname{sgn}(\rho\sigma) = (-1)^{t(\rho\sigma)} = (-1)^{t(\rho)+t(\sigma)} = (-1)^{t(\rho)}(-1)^{t(\sigma)} = \operatorname{sgn}(\rho)\operatorname{sgn}(\sigma)$$

illustrates that sgn is a group homomorphism. By Exercise 3.10.19, the kernel of any group homomorphism from G is a normal subgroup of G, hence $\ker(\operatorname{sgn})$ is a normal subgroup of $\mathfrak{S}_n$. By definition of the index, we have that $[\mathfrak{S}_n : \ker(\operatorname{sgn})] = |\mathfrak{S}_n / \ker(\operatorname{sgn})|$. By the First Isomorphism Theorem, we conclude that $\mathfrak{S}_n / \ker(\operatorname{sgn}) \cong \{-1, 1\}$ so that $|\mathfrak{S}_n / \ker(\operatorname{sgn})| = |\{-1, 1\}| = 2$. Last, by Lagrange's Theorem and Proposition 2.5.1, we conclude that $|\ker(\operatorname{sgn})| = |\mathfrak{S}_n|/[\mathfrak{S}_n : \ker(\operatorname{sgn})] = n!/2$. □

We refer to the normal subgroup $\ker(\operatorname{sgn})$ of $\mathfrak{S}_n$ of Proposition 3.7.2 as the **alternating group on n letters**; it is denoted by $\mathfrak{A}_n$ (Fraktur "A") in accordance with the notation $\mathfrak{S}_n$. Observe that a permutation σ lies in $\ker(\operatorname{sgn})$ if and only if $\operatorname{sgn}(\sigma) = 1$ if and only if σ is even, hence the alternating group on n letters is precisely the subgroup of $\mathfrak{S}_n$ consisting of even permutations. Even more, this matches with our intuition: the identity map $\iota : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is the identity element of $\mathfrak{S}_n$; it can be represented as a the product of 1-cycles $\iota = (1)(2)\cdots(n)$ with 0

transpositions, hence we have that $\operatorname{sgn}(\iota) = (-1)^{t(\iota)} = (-1)^0 = 1$ so that ι is even. Given any two even permutations ρ and σ, we have that $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$ because σ^{-1} has the same cycle type as σ and hence the same number of transpositions. By the One-Step Subgroup Test, we conclude that $\operatorname{sgn}(\rho\sigma^{-1}) = (-1)^{t(\rho\sigma^{-1})} = (-1)^{t(\rho)+t(\sigma^{-1})} = (-1)^{t(\rho)+t(\sigma)} = (-1)^{2r+2s} = 1$ so that $\rho\sigma^{-1}$ is even.

Proposition 3.7.3. *Every permutation of odd order is even; however, the converse is not true. Explicitly, there exist even permutations with even order.*

Proof. Given that σ is a permutation of odd order, it follows that $\operatorname{lcm}(r_1, \ldots, r_k)$ is odd, where $(r_1, \ldots, r_k)$ is the cycle type of σ. Consequently, we must have that r_i is odd for each integer $1 \leq i \leq k$. By the proof of Proposition 3.7.1, an r_i-cycle is the product of $r_i - 1$ transpositions, hence σ is the product of $(r_1 - 1) + \cdots + (r_k - 1)$ transpositions. Each of the integers $r_i - 1$ is even, so this sum is even, and σ is a product of an even number of transpositions, i.e., σ is even.

Conversely, if σ is the product of an even number of disjoint transpositions, then σ is even by definition of the parity of a permutation, and the order of σ is two by Proposition 2.5.7. □

3.8 External and Internal Direct Products

Earlier in these notes, we encountered the **Klein four-group** $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. We tacitly assumed that the binary operation on this group was inherited from the binary operation on the underlying factors of the group. Explicitly, the group operation on $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is defined as the componentwise sum of a pair of elements in the group, i.e., we have that $(a, b) + (c, d) = (a + c, b + d)$.

Generally, for any finite collection of groups $G_1, \ldots, G_n$, the **Cartesian product** $G_1 \times \cdots \times G_n$ of these groups can be equipped with a binary operation determined componentwise by the binary operations of the underlying groups. Explicitly, if $(G, *)$ and $(H, \star)$ are groups, then the Cartesian product $G \times H$ has an induced binary operation $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \star h_2)$. Out of desire for notational convenience, when working with the Cartesian product of an arbitrary number of groups, we will simply adopt the following convention to express a product in $G_1 \times \cdots \times G_n$.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

Proposition 3.8.1. *If $G_1, \ldots, G_n$ are any groups, then their Cartesian product $G_1 \times \cdots \times G_n$ is a group with respect to the componentwise binary operation $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$.*

Proof. Essentially, the three group axioms are satisfied because the underlying objects in the Cartesian product are groups, but we bear out the details for the sake of completeness. By definition, the binary operation on $G_1 \times \cdots \times G_n$ is associative because the binary operations of each underlying group are associative; the identity element of $G_1 \times \cdots \times G_n$ must be $(e_{G_1}, \ldots, e_{G_n})$; and the inverse of any element $(g_1, \ldots, g_n)$ of $G_1 \times \cdots \times G_n$ must be the element $(g_1^{-1}, \ldots, g_n^{-1})$ of $G_1 \times \cdots \times G_n$. □

We refer to the group $G_1 \times \cdots \times G_n$ as the **external direct product** of $G_1, \ldots, G_n$. We note that if each group G_i is finite, then the external direct products of $G_1, \ldots, G_n$ must also be finite. Explicitly, we have that $|G_1 \times \cdots \times G_n| = |G_1| \cdots |G_n|$ by the Fundamental Counting Principle.

Example 3.8.2. Considering that the real numbers form an additive group $(\mathbb{R}, +)$, it follows that $(\mathbb{R} \times \mathbb{R}, +)$ is a group under componentwise addition. Often, this group is denoted simply by $\mathbb{R}^2$; its elements are ordered pairs (x, y) of real numbers. Generally, $\mathbb{R}^n$ is defined analogously for $n \geq 3$.

Example 3.8.3. Consider the group $(\mathbb{Z}/2\mathbb{Z})^n$, i.e., the external direct product of $\mathbb{Z}/2\mathbb{Z}$ with itself n times for any positive integer n. Elements of $(\mathbb{Z}/2\mathbb{Z})^n$ are by definition n-tuples consisting of zeros and ones. Explicitly, if $n = 3$, the elements $(0, 1, 0)$ and $(1, 0, 1)$ satisfy that $(0, 1, 0)(1, 0, 1) = (1, 1, 1)$. We note that this operation coincides with addition of integers base two: indeed, there is no significant reason to distinguish between $(0, 1, 0)$ and 010 or $(1, 0, 1)$ and 101.

Example 3.8.4. We may also form the external direct product of $(\mathbb{R}, +)$ and $(\mathbb{R}^\times, \cdot)$ whose elements are ordered pairs (x, y) such that x is a real number and y is a nonzero real number. Unlike the previous example, the operation on each component is different: $(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_1 \cdot y_2)$.

We will demonstrate that many of the properties of the external direct product of finitely many groups are intimately intertwined with the properties of the underlying groups themselves.

Proposition 3.8.5. *Let $G_1, \ldots, G_n$ be groups with external direct product $G_1 \times \cdots \times G_n$. We have that $G_1 \times \cdots \times G_n$ is abelian if and only if $G_1, \ldots, G_n$ are abelian.*

Proposition 3.8.6. *Let $G_1, \ldots, G_n$ be groups with external direct product $G_1 \times \cdots \times G_n$. For any permutation σ of the indices $1, \ldots, n$, we have that $G_1 \times \cdots \times G_n \cong G_{\sigma(1)} \times \cdots \times G_{\sigma(n)}$. Put another way, the arrangement of the factors in the external direct product is unique up to isomorphism.*

We leave the proofs of the previous two propositions as Exercises 3.10.35 and 3.10.37. We demonstrate next that the order of an n-tuple in the external direct product of groups is uniquely determined in an elegant manner by the order of the individual components of the n-tuple.

Proposition 3.8.7. *Let $G_1, \ldots, G_n$ be groups with external direct product $G_1 \times \cdots \times G_n$. We have that* $\operatorname{ord}(g_1, \ldots, g_n) = \operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n))$.

Proof. By definition, the least common multiple ℓ of $\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n)$ is divisible by each of the integers $\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n)$, hence we have that $(g_1, \ldots, g_n)^\ell = (g_1^\ell, \ldots, g_n^\ell) = (e_{G_1}, \ldots, e_{G_n})$. Consequently, we must have that $\operatorname{ord}(g_1, \ldots, g_n)$ divides $\operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n))$ by Corollary 2.3.13. Conversely, if we denote by r the order $\operatorname{ord}(g_1, \ldots, g_n)$ of $(g_1, \ldots, g_n)$, then by definition of the order of an element of a group, we have that $(g_1^r, \ldots, g_n^r) = (g_1, \ldots, g_n)^r = (e_{G_1}, \ldots, e_{G_n})$. Corollary 2.3.13 implies yet again that $\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n)$ divide r, hence r is a common multiple of $\operatorname{ord}(g_1, \ldots, \operatorname{ord}(g_n)$ — namely, we conclude that $\operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n))$ divides r. Each of these integers is positive, and they divide each other, hence they must be equal to one another. □

Proposition 3.8.8. *Let $G_1, \ldots, G_n$ be finite cyclic groups with external direct product $G_1 \times \cdots \times G_n$. We have that $G_1 \times \cdots \times G_n$ is cyclic if and only if* $\gcd(|G_1|, \ldots, |G_n|) = 1$.

Proof. By Exercise 1.10.34, if $\gcd(|G_1|, \ldots, |G_n|) = 1$, then $\operatorname{lcm}(|G_1|, \ldots, |G_n|) = |G_1| \cdots |G_n|$ so that the external direct product $G_1 \times \cdots \times G_n$ is the cyclic group generated by $(g_1, \ldots, g_n)$ such that $G_i = \langle g_i \rangle$ for each integer $1 \leq i \leq n$. Conversely, we will assume that $G_1 \times \cdots \times G_n$ is cyclic with a generator $(g_1, \ldots, g_n)$. We claim that $G_i = \langle g_i \rangle$ for each integer $1 \leq i \leq n$. Every element of $G_1 \times \cdots \times G_n$ can be written as $(g_1, \ldots, g_n)^k = (g_1^k, \ldots, g_n^k)$ for some integer $1 \leq k \leq |G_1| \cdots |G_n|$, hence every element of G_i is equal to g_i^k for some integer k. By Proposition 3.8.7, we conclude that

$$|G_1| \cdots |G_n| = |G_1 \times \cdots \times G_n| = \operatorname{ord}(g_1, \ldots, g_n) = \operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n)) = \operatorname{lcm}(|G_1|, \ldots, |G_n|).$$

Last, by Exercise 1.10.34 again, we have that $|G_1| \cdots |G_n| = \operatorname{lcm}(|G_1|, \ldots, |G_n|) \gcd(|G_1|, \ldots, |G_n|)$, and we conclude the desired result from the above displayed equation. □

One of the most important features of the external direct product $G_1 \times \cdots \times G_n$ of groups is that each of the direct factors G_i can be identified with the normal subgroup of $G_1 \times \cdots \times G_n$ obtained by "forgetting about" the other direct factors. Even more, the external direct product $G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ can be identified with the normal subgroup of $G_1 \times \cdots \times G_n$ obtained by "forgetting about" the direct factor G_i. Conversely, any direct factor and any direct subproduct can be viewed as a quotient of $G_1 \times \cdots \times G_n$. We make these notions rigorous as follows.

Proposition 3.8.9. *Let $G_1, \ldots, G_n$ be groups with external direct product $G_1 \times \cdots \times G_n$.*

1.) *Given any integer $1 \leq i \leq n$, we may view G_i as a subgroup of $G_1 \times \cdots \times G_n$ via the group homomorphism $\gamma_i : G_i \to G_1 \times \cdots \times G_n$ defined by $\gamma_i(g) = (e_{G_1}, \ldots, g, \ldots, e_{G_n})$. Explicitly, the function γ_i sends an element $g \in G_i$ to the n-tuple in $G_1 \times \cdots \times G_n$ whose ith component is g and jth component is the identity element $e_{G_j} \in G_j$ for each integer $1 \leq j \leq n$ except i.*

$$G_i \cong \{(e_{G_1}, \ldots, g, \ldots, e_{G_n}) \mid g \in G_i\} \subseteq G_1 \times \cdots \times G_i \times \cdots \times G_n$$

2.) *Given any integer $1 \leq i \leq n$, we may view $G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ as a subgroup of $G_1 \times \cdots \times G_n$ via the group homomorphism $\varepsilon_i : G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \to G_1 \times \cdots \times G_n$ defined by $\varepsilon_i(g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n) = (g_1, \ldots, g_{i-1}, e_{G_i}, g_{i+1}, \ldots, g_n)$.*

$$G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \cong G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_n$$

3.) *Given any integer $1 \leq i \leq n$, the group G_i is isomorphic to the quotient of $G_1 \times \cdots \times G_n$ by its normal subgroup $G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_n$.*

$$G_i \cong (G_1 \times \cdots \times G_n)/(G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_n)$$

4.) *Given any integer $1 \leq i \leq n$, the external direct product $G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ is isomorphic to the quotient of $G_1 \times \cdots \times G_n$ by its normal subgroup $\gamma_i(G_i)$.*

$$G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \cong (G_1 \times \cdots \times G_i \times \cdots \times G_n)/\gamma_i(G_i)$$

Proof. (1.) Certainly, γ_i is a group homomorphism because the identities $e_{G_j} = e_{G_j} e_{G_j}$ yield that

$$\gamma_i(gh) = (e_{G_1}, \ldots, gh, \ldots, e_{G_n}) = (e_{G_1}, \ldots, g, \ldots, e_{G_n})(e_{G_1}, \ldots, h, \ldots, e_{G_n}) = \gamma_i(g)\gamma_i(h).$$

Even more, we have that $g \in \ker \gamma_i$ if and only if $(e_{G_1}, \ldots, g, \ldots, e_{G_n}) = (e_{G_1}, \ldots, e_{G_i}, \ldots, e_{G_n})$ if and only if $g = e_{G_i}$ so that $\ker \gamma_i = \{e_{G_i}\}$ and γ_i is injective by Proposition 3.3.6. Consequently, by the First Isomorphism Theorem, there exists a group isomorphism $G_i \cong \gamma_i(G_i)$.

(2.) Considering that $e_{G_i} = e_{G_i} e_{G_i}$, once again, we find that ε_i is a group homomorphism because the n-tuple $(g_1 h_1, \ldots, g_{i-1} h_{i-1}, e_{G_i}, g_{i+1} h_{i+1}, \ldots, g_n h_n)$ and the n-tuple

$$(g_1, \ldots, g_{i-1}, e_{G_i}, g_{i+1}, \ldots, g_n)(h_1, \ldots, h_{i-1}, e_{G_i}, h_{i+1}, \ldots, h_n)$$

are equal. By construction, the group homomorphism ε_i is injective: if $(g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$ lies in $\ker \varepsilon_i$, then we must have that $(g_1, \ldots, g_{i-1}, e_{G_i}, g_{i+1}, \ldots, g_n) = (e_{G_1}, \ldots, e_{G_{i-1}}, e_{G_i}, e_{G_{i+1}}, \ldots, e_{G_n})$,

hence the component g_j must be the identity element of G_j for each integer $1 \leq j \leq n$ other than i. We conclude the desired result by the First Isomorphism Theorem.

(3.) Consider the function $\pi_i : G_1 \times \cdots \times G_n \to G_i$ defined by $\pi_i(g_1, \ldots, g_n) = g_i$. We may view π_i as "forgetting about" all other components of an n-tuple of $G_1 \times \cdots \times G_n$ other than the ith component. Exercise 3.10.38(a.) shows that π_i is a group homomorphism with kernel

$$G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_n = \{(g_1, \ldots, g_{i-1}, e_{G_i}, g_{i+1}, \ldots, g_n) \mid g_j \in G_j \text{ for } j \neq i\}.$$

By Exercise 3.10.19, it follows that the above displayed subgroup of $G_1 \times \cdots \times G_n$ is normal. Even more, the First Isomorphism Theorem yields the desired isomorphism.

(4.) Consider the function $\delta_i : G_1 \times \cdots \times G_n \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ defined by $\delta_i(g_1, \ldots, g_n) = (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$. We may view δ_i as "forgetting about" the ith component of an n-tuple in $G_1 \times \cdots \times G_n$. Exercise 3.10.38(b.) shows that δ_i is a group homomorphism with kernel $\gamma_i(G_i) = \{(e_{G_1}, \ldots, g, \ldots, e_{G_n}) \mid g \in G_i\}$, hence $\gamma_i(G_i)$ is a normal subgroup of $G_1 \times \cdots \times G_n$ by Exercise 3.10.19. Last, the desired isomorphism exists by the First Isomorphism Theorem. □

Example 3.8.10. By Proposition 3.8.9, we may view $(\mathbb{Z}, +)$ as a subgroup of $(\mathbb{Z} \times \mathbb{Z}, +)$ by simply "forgetting about" either one of the factors of $\mathbb{Z}$. Explicitly, every integer a can be viewed as the ordered pair $(a, 0)$. Conversely, we may view $(\mathbb{Z}, +)$ as the quotient group $(\mathbb{Z} \times \mathbb{Z}, +)/(\{0\} \times \mathbb{Z}, +)$, in which case an integer a will be identified with the left coset $(a, 0) + \{0\} \times \mathbb{Z}$.

Usually, the external direct product is constructed in order to define a "larger" group from some known "smaller" groups. Conversely, the **internal direct product** can be defined to express a "large" group as a product of two "smaller" groups. Explicitly, we say that a group G can be expressed as an internal direct product of some subgroups H and K of G if and only if

(i.) we have that $H \cap K = \{e_G\}$, i.e., the intersection of H and K is trivial;

(ii.) we have that $G = HK = \{hk \mid h \in H \text{ and } k \in K\}$, i.e., every element of G can be written (not necessarily uniquely) as a product of an element of H and an element of K; and

(iii.) we have that $hk = kh$ for all elements $h \in H$ and $k \in K$, i.e., H and K commute.

Caution: the third requirement that every element of H commutes with every element of K does not imply that every internal direct product is abelian. Explicitly, if H is not abelian, then HK cannot be abelian because H is a subgroup of HK, and subgroups of abelian groups are abelian.

Example 3.8.11. Consider the dihedral group D_6 of order twelve with subgroups $H = \{1, r^3\}$ and $K = \{1, r^2, r^4, s, r^2s, r^4s\}$. We leave it as Exercise 3.10.40 to demonstrate that $D_6 = HK$.

We provide next a sufficient condition to conclude that a group is an internal direct product. Curiously, we make use of the external direct product of a group on our way to our objective.

Proposition 3.8.12. *Let G be a group with normal subgroups N and M. If $N \cap M = \{e_G\}$, then $NM = MN$. Put another way, every pair normal subgroups that intersect trivially commute.*

Proof. Given any elements $n \in N$ and $m \in M$, consider the element $n^{-1}m^{-1}nm$ of G. We must establish that $nm = mn$ or $n^{-1}m^{-1}nm = e_G$. By hypothesis that N is normal in G, it follows that $m^{-1}nm \in N$ so that $n^{-1}m^{-1}nm \in N$. Likewise, by hypothesis that M is normal in G, we have that $n^{-1}m^{-1}n \in M$ so that $n^{-1}m^{-1}nm \in M$. Consequently, we have that $n^{-1}m^{-1}nm = e_G$. □

Proposition 3.8.13. *Let G be a group with normal subgroups $N_1, \ldots, N_k$. If every element of G can be written uniquely as $n_1 \cdots n_k$ for some elements $n_i \in N_i$, then we have that $G \cong N_1 \times \cdots \times N_k$.*

Proof. By assumption that every element of G can be written uniquely as $n_1 \cdots n_k$ for some elements $n_i \in N_i$, it follows that the function $\varphi : N_1 \times \cdots \times N_k \to G$ defined by $\varphi(n_1, \ldots, n_k) = n_1 \cdots n_k$ is a bijection. We must establish that φ is a group homomorphism. Explicitly, we claim that

$$n_1 n_1' \cdots n_k n_k' = \varphi((n_1, \ldots, n_k)(n_1', \ldots, n_k')) = \varphi(n_1, \ldots, n_k)\varphi(n_1', \ldots, n_k') = n_1 \cdots n_k n_1' \cdots n_k'.$$

By Proposition 3.8.12, it suffices to show that $N_i \cap N_j = \{e_G\}$ for all pairs of integers $1 \leq i < j \leq k$. Consider an element $n \in N_i \cap N_j$. Every element of G can be written uniquely as $n_1 \cdots n_k$ for some elements $n_i \in N_i$, hence the unique expression for n according to this is as the product of $i-1$ copies of e_G followed by n followed by $k-i$ copies of e_G because n is an element of N_i. By the same token, we may also express n as the product of $j-1$ copies of e_G followed by n followed by $k-j$ copies of e_G because n is an element of N_j. We conclude therefore that $n = e_G$, as desired. □

Corollary 3.8.14. *Let G be a group with normal subgroups $N_1, \ldots, N_k$ such that $N_i \cap N_j = \{e_G\}$ for each integer $1 \leq i < j \leq k$. If $G = N_1 \cdots N_k$, then $G \cong N_1 \times \cdots \times N_k$. Put another way, the internal direct product of groups is isomorphic to the external direct product of groups.*

Proof. We proceed by the Principle of Ordinary Induction on k. We will assume first that $k = 2$. By Proposition 3.8.13, it suffices to show that every element of G can be written uniquely as $n_1 n_2$ for some elements $n_1 \in N_1$ and $n_2 \in N_2$. Consider the case that $n_1 n_2 = m_1 m_2$ for some elements $m_1 \in N_1$ and $m_2 \in N_2$. We note that $m_1^{-1} n_1 = m_2 n_2^{-1}$ with $m_1^{-1} n_1 \in N_1$ and $m_2 n_2^{-1} \in N_2$. Consequently, the products $m_1^{-1} n_1$ and $m_2 n_2^{-1}$ both lie in $N_1 \cap N_2$, hence they must both be equal to e_G, and we conclude that $m_1 = n_1$ and $m_2 = n_2$. We have successfully established the base case, hence we may assume inductively that the result holds for some integer $k \geq 3$. By Exercise 3.10.11, it follows that $N_1 \cdots N_k$ is a normal subgroup of G with the property that $N_1 \cdots N_k \cap N_{k+1} = \{e_G\}$, hence we conclude from the base case that $G \cong (N_1 \cdots N_k) \times N_{k+1} \cong N_1 \times \cdots \times N_k \times N_{k+1}$. □

3.9 Finite Abelian Groups

Earlier in this chapter, we proved that every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$ and that every finite cyclic group is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$ for some positive integer n. We turn our attention in this section to the less restrictive property of abelianness. Like before, we will provide a characterization of finite abelian groups in terms of isomorphism classes with respect to order.

Consider any positive integer n. By the Fundamental Theorem of Arithmetic, there exist prime numbers $p_1, \ldots, p_k$ and unique non-negative integers $e_1, \ldots, e_k$ such that $n = p_1^{e_1} \cdots p_k^{e_k}$ and

$$\left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| = n = p_1^{e_1} \cdots p_k^{e_k} = \left|\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\right| \cdots \left|\frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}\right| = \left|\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}\right|.$$

Consequently, by Exercise 1.10.5, there exists a bijective function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$. One might naturally ask if (and we would certainly hope that) this bijective function carries the additional structure of a group homomorphism. We answer this in the affirmative as follows.

Proposition 3.9.1. *Given any positive integer $n \geq 2$ with unique prime factorization $n = p_1^{e_1} \cdots p_k^{e^k}$ for some unique prime numbers $p_1, \ldots, p_k$ and unique positive integers $e_1, \ldots, e_k$, we have that*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}.$$

Proof. Observe that each direct factor of the external direct product $(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})$ is a finite cyclic group with $|\mathbb{Z}/p_i^{e_i}\mathbb{Z}| = p_i^{e_i}$ for each integer $1 \leq i \leq k$. Consequently, we have that

$$\gcd\left(\left|\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\right|, \ldots, \left|\frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}\right|\right) = \gcd(p_1^{e_1}, \ldots, p_k^{e_k}) = 1$$

by assumption that $p_1, \ldots, p_k$ are distinct prime numbers. By Proposition 3.8.8, we conclude that $(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})$ is cyclic of order $n = p_1^{e_1} \cdots p_k^{e_k}$; the result holds by Proposition 3.3.20. □

Consequently, every finite cyclic group of order n can be written as the external product of cyclic groups whose orders correspond to the unique prime-power factors of the unique prime factorization of n. Conversely, it is only possible to achieve such a representation as an external direct product of finite cyclic groups by factors of n that are pairwise relatively prime to one another.

Proposition 3.9.2. *Given any positive integers $n_1, \ldots, n_k$, we have that*

$$\frac{\mathbb{Z}}{n_1 \cdots n_k\mathbb{Z}} \cong \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}}$$

if and only if for all indices $1 \leq i < j \leq k$, we have that $\gcd(n_i, n_j) = 1$.

Proof. Each of the quotient groups $\mathbb{Z}/n_i\mathbb{Z}$ is a cyclic group of order n_i for each integer $1 \leq i \leq k$. By Proposition 3.8.8, we have that $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$ is cyclic if and only if $\gcd(n_1, \ldots, n_k) = 1$. Consequently, if we assume that $\gcd(n_i, n_j) = 1$ for all indices $1 \leq i < j \leq k$, then we have that $\gcd(n_1, \ldots, n_k) = 1$ so that $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$ is a cyclic group of order $n_1 \cdots n_k$; the displayed isomorphism is therefore guaranteed by Proposition 3.3.20. Conversely, if we assume to the contrapositive that $\gcd(n_1, n_2) = d \geq 2$ (after possibly relabelling the indices), then the integer $n_1 \cdots n_k/d$ is well-defined because d divides both n_1 and n_2; it is strictly smaller than $n_1 \cdots n_k$. On the contrary, if $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$ were cyclic and generated by $(a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z})$, then the sum of $(a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z})$ with itself $n_1 \cdots n_k/d$ times would be equal to

$$\left(\frac{n_2 \cdots n_k}{d} a_1 n_1 + n_1\mathbb{Z}, \ldots, \frac{n_1 \cdots n_{k-1}}{d} a_k n_k + n_k\mathbb{Z}\right) = (0 + n_1\mathbb{Z}, \ldots, 0 + n_k\mathbb{Z});$$

this is impossible because the order of $(a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z})$ must be $n_1 \cdots n_k$. □

Example 3.9.3. We have that $\mathbb{Z}/12\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ because the prime factorization of 12 is $12 = 2^2 \cdot 3 = 4 \cdot 3$; however, $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ are not isomorphic because $\gcd(2, 6) = 2$.

Example 3.9.4. We have that $\mathbb{Z}/30\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/15\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ because it holds that $30 = 2 \cdot 15 = 2 \cdot 3 \cdot 5$ and $\gcd(2, 15) = 1$ and $\gcd(3, 5) = 1$.

Even if we do not restrict our attention to finite cyclic groups, every finite abelian group can be written as the direct product of finitely generated cyclic groups. Later, we will develop the tools to prove the following theorem; however, we will simply state it in two versions for now.

Theorem 3.9.5 (Fundamental Theorem of Finite Abelian Groups)**.** *Given any finite abelian group G, there exist (not necessarily distinct) prime numbers p_i and non-negative integers e_i such that*

$$G \cong \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}.$$

We refer to the prime powers $p_i^{e_i}$ as the **elementary divisors** *of G; this representation of G as a direct product of finite cyclic groups is called the* **elementary divisor decomposition** *of G.*

Corollary 3.9.6. *Given any finite abelian group G, there exist (not necessarily distinct) positive integers $n_1, \ldots, n_\ell$ such that $n_i \mid n_{i+1}$ for each integer $1 \leq i \leq \ell - 1$ and*

$$G \cong \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_\ell\mathbb{Z}}.$$

We refer to the positive integers n_i as the **invariant factors** *of G; this representation of G as a direct product of finite cyclic groups is called the* **invariant factor decomposition** *of G.*

Out of desire for convenience (and because they are isomorphic groups by Proposition 3.3.20), we will throughout this section freely alternate between the notation of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_n$.

Example 3.9.7. Given any positive integer n, the elementary divisors of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ are obtained via the unique prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$ of n. Explicitly, the elementary divisors are $p_1^{e_1}, \ldots, p_k^{e_k}$ by Proposition 3.9.1. On the other hand, n is the only invariant factor of $\mathbb{Z}/n\mathbb{Z}$.

Example 3.9.8. Observe that for any finite abelian group

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25},$$

the elementary divisors are 2, 2, 2^2, 2^3, 3, 3, 5, and 5^2; however, the invariant factors are unclear.

Algorithm 3.9.9 (Converting Elementary Divisors to Invariant Factors)**.** Let G be a finite abelian group whose elementary divisors are known. Use the following to find the invariant factors of G.

1.) Find the prime number p that appears the most times in the elementary divisor decomposition of G. Given that two or more primes appear an equal number of times, choose one arbitrarily.

2.) Create an array whose first row consists of all powers of p that appear in the elementary divisor decomposition of G, listing these powers in non-increasing order from right to left.

3.) Repeat the second step in the second row with the prime q that appears the second most times (or the same number of times as p) in the elementary divisor decomposition of G.

4.) Continue this process until all primes appearing in the direct product representation of G have been written in a row. One should end with an upper-triangular array.

5.) By multiplying the elements of each consecutive column, we obtain the invariant factors of G.

Example 3.9.10. Consider the finite abelian group G of Example 3.9.8. By following the method outlined in Algorithm 3.9.9 with the group G at hand, we have the following array.

$$\begin{array}{cccc} 2 & 2 & 2^2 & 2^3 \\ & 3 & 3 & 3 \\ & & 5 & 5^2 \end{array}$$

By multiplying the elements of each consecutive column, we obtain the invariant factors of G: they are 2, 6, 60, and 600. By Corollary 3.9.6, we conclude that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{60} \times \mathbb{Z}_{600}$.

Conversely, one can obtain the elementary divisors from the invariant factors.

Algorithm 3.9.11 (Converting Invariant Factors to Elementary Divisors)**.** Let G be a finite abelian group whose invariant factors are known. Use the following to find the elementary divisors of G.

1.) Given the invariant factors n_i of G with $n_1 \mid n_2 \mid n_3 \mid \cdots \mid n_\ell$, express each invariant factor n_i as a product of distinct prime powers by the Fundamental Theorem of Arithmetic.

2.) Construct an upper-triangular array whose ith column consists of the distinct prime powers $p_{i1}^{e_{i1}}, \ldots, p_{ik}^{e_{ik}}$ such that $n_i = p_{i1}^{e_{i1}} \cdots p_{ik}^{e_{ik}}$.

3.) We obtain the elementary divisors of G as the components of the upper-triangular array.

Example 3.9.12. Consider any finite abelian group $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{14} \times \mathbb{Z}_{98} \times \mathbb{Z}_{294}$ with invariant factors 2, 2, $14 = 2 \cdot 7$, $98 = 2 \cdot 7^2$, and $294 = 2 \cdot 3 \cdot 7^2$. By following the procedure outlined in Algorithm 3.9.11 with the group G at hand, we obtain the following array.

$$\begin{array}{ccccc} 2 & 2 & 2 & 2 & 2 \\ & & 7 & 7^2 & 3 \\ & & & & 7^2 \end{array}$$

We find that the elementary divisors of G are 2, 2, 2, 2, 2, 3, 7, 7^2, and 7^2. By the Fundamental Theorem of Finite Abelian Groups, we conclude that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{49} \times \mathbb{Z}_{49}$.

Ultimately, the Fundamental Theorem of Finite Abelian Groups implies that the structure of a finite abelian group G is uniquely determined (up to isomorphism) by its elementary divisors (or equivalently, its invariant factors). Even more, we note that the elementary divisors of G are (not necessarily uniquely) determined by the unique prime factorization of $|G|$. By Exercise 2.8.14, every group of order four is abelian, hence it suffices to note that there are two distinct (up to isomorphism) groups of order four: they are the Klein four-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ and the cyclic group $\mathbb{Z}_4$ of order four. Each of these groups corresponds to a distinct **integer partition** of the integer two. Generally, we define a partition of an integer n as a k-tuple $(n_1, \ldots, n_k)$ such that $n = n_1 + \cdots + n_k$ and $1 \leq n_1 \leq n_2 \leq \cdots \leq n_k$. Considering that $2 = 1 + 1$ and $2 = 2$, there are two distinct integer partitions of 2. Consequently, there are two distinct abelian groups of order $4 = 2^2$. We will denote by $\rho(n)$ the number of distinct integer partitions of the positive integer n.

Proposition 3.9.13. *If n is a positive integer with unique prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, then there are $\rho(e_1) \cdots \rho(e_k)$ distinct finite abelian groups of order n up to isomorphism.*

Proof. By the Fundamental Theorem of Finite Abelian Groups, for any finite abelian group G, there exist (not necessarily distinct) prime numbers q_i and non-negative integers f_i such that

$$G \cong \frac{\mathbb{Z}}{q_1^{f_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{q_\ell^{f_\ell}\mathbb{Z}}.$$

Observe that if the order of G is n, then by the uniqueness of the prime factorization of n, we must have that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_\ell\}$ and $e_1 + \cdots + e_k = f_1 + \cdots + f_\ell$. Considering that there are $\rho(e_1) \cdots \rho(e_k)$ solutions $(f_1, \ldots, f_k)$ to the positive integer identity $e_1 + \cdots + e_k = f_1 + \cdots + f_\ell$, we conclude that there are at most $\rho(e_1) \cdots \rho(e_k)$ distinct finite abelian groups of order n up to isomorphism. Conversely, each of the finite abelian groups obtained as the external direct product corresponding to some integer partition of e_i is distinct by Proposition 3.9.2 because the cyclic groups $\mathbb{Z}_{p_i^{e_i}}$ and $\mathbb{Z}_{p_i^{e_i-1}} \times \mathbb{Z}_{p_i}$ are not isomorphic to one another whenever $e_i \geq 2$. □

Example 3.9.14. Consider a finite abelian group G of order $14553000 = 2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11$. Observe that $3 = 3$, $3 = 1+2$, and $3 = 1+1+1$ are the three distinct integer partitions of three. Even more, there are only two integer partitions $2 = 2$ and $2 = 1 + 1$ of two. Consequently, by Proposition 3.9.13, there are $\rho(3) \cdot \rho(3) \cdot \rho(3) \cdot \rho(2) = \rho(3)^3 \cdot \rho(2) = 3^3 \cdot 2 = 54$ abelian groups of order 14553000.

We have for now stated the Fundamental Theorem of Finite Abelian Groups without proof, but the tools that are developed for the proof are quite useful to understand on their own. Given any abelian group G and any prime number p, consider the set of all elements of G of p-power order

$$G(p) = \{g \in G \mid \operatorname{ord}(g) = p^n \text{ for some integer } n \geq 0\}.$$

Proposition 3.9.15. *If G is an abelian group and p is a prime number, then the set $G(p)$ of all elements $g \in G$ such that $\operatorname{ord}(g) = p^n$ for some integer $n \geq 0$ is subgroup of G.*

Proof. Considering that $\operatorname{ord}(e_G) = 1 = p^0$ for any prime number p, it follows that $G(p)$ is nonempty. By the One-Step Subgroup Test, it suffices to prove that if $\operatorname{ord}(g) = p^m$ and $\operatorname{ord}(h) = p^n$ for some positive integers m and n, then $\operatorname{ord}(gh^{-1}) = p^\ell$ for some integer $\ell \geq 0$; this is Exercise 2.8.32. □

One can view our next proposition as something of a prime factorization property for elements of finite order in an abelian group. Essentially, we prove that every element of finite order in an abelian group can be written as a product of elements of prime-power order.

Proposition 3.9.16. *If G is an abelian group and $g \in G$ has finite order, then for each distinct prime number p_i that divides $\operatorname{ord}(g)$, there exist elements $g_i \in G(p_i)$ such that $g = g_1 \cdots g_k$.*

Proof. We proceed by induction on the number k of distinct prime factors in the unique prime factorization of $\operatorname{ord}(g)$ (cf. Fundamental Theorem of Arithmetic). If $k = 1$, then $\operatorname{ord}(g) = p^n$ for some prime number p and some non-negative integer n, from which it follows that $g \in G(p)$.

We will assume inductively that the proposition holds for all elements of G whose order is divisible by at most $k-1$ distinct primes. If $\operatorname{ord}(g) = p_1^{e_1} \cdots p_k^{e_k}$ for some distinct prime numbers p_i and positive integers e_i, we may factor $\operatorname{ord}(g) = ab$ for $a = p_1^{e_1}$ and $b = p_2^{e_2} \cdots p_k^{e_k}$. By hypothesis that the p_i are distinct, we have that $\gcd(a, b) = 1$, hence by Bézout's Identity, we find that $ax + by = 1$ for some integers x and y. Consequently, we have that $g = g^{ax+by} = g^{ax} g^{by}$. Observe that

$$(g^{by})^a = g^{aby} = g^{y \operatorname{ord}(g)} = (g^{\operatorname{ord}(g)})^y = e_G^y = e_G,$$

from which it follows that $\text{ord}(g^{by}) \mid p_1^{e_1}$ so that g^{by} lies in $G(p_1)$. Likewise, we have that

$$(g^{ax})^b = g^{abx} = g^{x\,\text{ord}(g)} = (g^{\text{ord}(g)})^x = e_G^x = e_G,$$

from which it follows that $\text{ord}(g^{ax}) \mid b$ so that $\text{ord}(g^{ax}) = p_2^{f_2} \cdots p_k^{f_k}$ for some non-negative integers f_i. By induction, we may write $g^{ax} = g_2 \cdots g_k$ for some elements $g_i \in G(p_i)$ for each distinct prime number p_i and $g^{by} = g_1$ for some element $g_1 \in G(p_1)$ so that $g = g^{by+ax} = g^{by} g^{ax} = g_1 g_2 \cdots g_k$. □

Last, we prove that every finite abelian group can be decomposed as an external direct product of its p-**subgroups** $G(p_i)$ for each prime number that divides the order of G.

Theorem 3.9.17. *If G is any finite abelian group, then $G \cong G(p_1) \times \cdots \times G(p_k)$ for some distinct prime numbers $p_1, \ldots, p_k$ that divide the order of G.*

Proof. We claim that if p_i and p_j are distinct prime numbers, then $G(p_i) \cap G(p_j) = \{e_G\}$. By definition, if $g \in G(p_i) \cap G(p_j)$, then there are non-negative integers e_i and e_j with $\text{ord}(g) = p_i^{e_i}$ and $\text{ord}(g) = p_j^{e_j}$. On the contrary, if neither e_i is zero nor e_j is zero, then the identity $p_i^{e_i} = p_j^{e_j}$ yields that p_i divides $p_j^{e_j}$. But by assumption that p_i and p_j are distinct prime numbers, this is impossible. We conclude therefore that either $e_i = 0$ or $e_j = 0$ so that $G(p_i) \cap G(p_j) = \{e_G\}$.

By Proposition 3.8.14, it suffices to show that every element of G can be written uniquely as $g_1 \cdots g_k$ for some elements $g_i \in G(p_i)$, where we define $g_i = e_G$ if the prime number p_i does not divide $\text{ord}(g)$. By Proposition 3.9.16, every element of G can be written as $g_1 \cdots g_k$ for some elements $g_i \in G(p_i)$ for each distinct prime number p_i that divides $\text{ord}(g)$. Consider two representations $g_1 \cdots g_k = h_1 \cdots h_k$ of an element $g \in G$ such that g_i and h_i both lie in $G(p_i)$. By hypothesis that G is abelian, we have that $g_1 h_1^{-1} = h_2 g_2^{-1} \cdots h_k g_k^{-1}$. Considering that $G(p_i)$ is a subgroup of G for each integer $1 \leq i \leq k$ by Proposition 3.9.15, it follows by the One-Step Subgroup Test that $h_i g_i^{-1}$ lies in $G(p_i)$ for each integer $2 \leq i \leq k$. By definition, for each integer $2 \leq i \leq k$, we have that $\text{ord}(h_i g_i^{-1}) = p_i^{e_i}$ for some integer $e_i \geq 0$. Consider the integer $n = p_2^{e_2} \cdots p_k^{e_k}$. We have that

$$(g_1 h_1^{-1})^n = (h_2 g_2^{-1} \cdots h_k g_k^{-1})^n = (h_2 g_2^{-1})^n \cdots (h_k g_k^{-1})^n = e_G$$

by hypothesis that G is abelian and $\text{ord}(h_i g_i^{-1}) = p_i^{e_i}$ divides n. But this implies that $\text{ord}(g_1 h_1^{-1}) \mid n$ by Corollary 2.3.13; on the other hand, $\text{ord}(g_1 h_1^{-1}) = p_1^{e_1}$ for some integer $e_1 \geq 0$ gives that $e_1 = 0$ so that $g_1 h_1^{-1} = e_G$ or $g_1 = h_1$. Repeating this yields that $g_i = h_i$ for all integers $2 \leq i \leq k$. □

Consequently, it is enough to consider $G(p_i)$ for each prime number p_i dividing $|G|$.

Proposition 3.9.18. *If G is an abelian group of order p^n for some prime number p and some integer $n \geq 0$, then G admits a subgroup H such that $G \cong (\mathbb{Z}/p^k\mathbb{Z}) \times H$ and $k = \max\{\text{ord}(g) \mid g \in G\}$.*

Proof. We will prove a slightly different statement by appealing to the Principle of Complete Induction on n. Explicitly, we will prove that for any element $g \in G$ with $\text{ord}(g) = \max\{\text{ord}(x) \mid x \in G\}$, there exists a subgroup H of G such that $G \cong \langle g \rangle \times H$. Once this is established, then we may employ Corollary 3.1.13 and Proposition 3.3.20 to conclude that $G \cong \langle g \rangle \times H \cong (\mathbb{Z}/p^k\mathbb{Z}) \times H$.

If $n = 1$, then G is a finite group of order p, hence we have that $G \cong \mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z}) \times \{e_G\}$. We will assume therefore that the proposition holds for all integers $1 \leq k \leq n-1$. Consider an element $g \in G$ such that $\text{ord}(g) = \max\{\text{ord}(x) \mid x \in G\}$. Observe that if $\text{ord}(g) = p^n$, then G is cyclic, hence

we conclude as before that $G \cong \mathbb{Z}/p^n\mathbb{Z} \cong (\mathbb{Z}/p^n\mathbb{Z}) \times \{e_G\}$. Consequently, it suffices to consider the case that $\text{ord}(g) = p^k$ for some integer $1 \leq k \leq n-1$. We note that $G \setminus \langle g \rangle$ is nonempty because the order of g is strictly smaller than the order of G, hence we may find an element $h \in G \setminus \langle g \rangle$ such that $\text{ord}(h) = \min\{\text{ord}(x) \mid x \in G \text{ and } x \notin \langle g \rangle\}$ by the Well-Ordering Principle.

Observe that $\text{ord}(h) = p^\ell$ for some integer $\ell \geq 1$ by Lagrange's Theorem. By Proposition 2.3.14, we have that $\text{ord}(h^p) = p^\ell / \gcd(p, p^\ell) = p^\ell/p = p^{\ell-1}$, hence we must have that $h^p \in \langle g \rangle$ by assumption that $\text{ord}(h) = \min\{\text{ord}(x) \mid x \notin \langle g \rangle\}$. By definition of $\langle g \rangle$, there exists a positive integer q such that $h^p = g^q$. By raising each of these identical elements to the power of p^{k-1}, we find that $e_G = h^{p^k} = (h^p)^{p^{k-1}} = (g^q)^{p^{k-1}}$ and $\text{ord}(g^q) \leq p^{k-1}$. Corollary 2.3.15 yields that $\gcd(p^{k-1}, q)$ is nonzero, hence p must divide q, i.e., there exists an integer r such that $q = pr$ and $h^p = g^q = g^{pr}$. Consider the product $x = g^{-r}h$. Observe that $x^p = g^{-pr}h^p = g^{-q}h^p = (g^q)^{-1}h^p = (h^p)^{-1}h^p = e_G$, hence $\text{ord}(x)$ must be either one or p; however, if it were the case that $\text{ord}(x) = 1$, then we would have that $e_G = x = g^{-r}h$ so that $h = g^r$ lies in $\langle g \rangle$ — contradicting the definition of h. We conclude therefore that $\text{ord}(x) = p$. Once again, if x were an element of $\langle g \rangle$, then $h = g^r x$ would be an element of $\langle g \rangle$, hence x must be an element of order p that is not contained in $\langle g \rangle$. By construction of h as an element of $G \setminus \langle g \rangle$ of smallest possible order, we conclude that $\text{ord}(h) = p$.

We claim next that $\langle g \rangle \cap \langle h \rangle = \{e_G\}$. Given any element $x \in \langle g \rangle \cap \langle h \rangle$, we have that $\text{ord}(x) \mid p$ by Lagrange's Theorem so that $\text{ord}(x) = 1$ or $\text{ord}(x) = p$. On the contrary, if it were the case that $\text{ord}(x) = p$, then it would follow that $\langle x \rangle = \langle h \rangle$ because they both generate a subgroup of G of order p and $\langle x \rangle \subseteq \langle h \rangle$ by assumption. But at the same time, because x lies in $\langle g \rangle$, this would imply that $h = x^a = (g^b)^a = g^{ab}$ for some positive integers a and b — contradicting the construction of h as an element of $G \setminus \langle g \rangle$. We conclude therefore that $\text{ord}(x) = 1$ so that $\langle g \rangle \cap \langle h \rangle = \{e_G\}$.

By Lagrange's Theorem, the order of the quotient group $G/\langle h \rangle$ is $|G|/\text{ord}(h) = p^n/p = p^{n-1}$. We claim that $\text{ord}(g\langle h \rangle) = \text{ord}(g) = p^k$, from which it will follow by Exercise 3.10.7 that $g\langle h \rangle$ is an element of $G/\langle h \rangle$ of maximum possible order. Observe that for any integer $1 \leq \ell \leq p^k$ such that $e_G\langle h \rangle = (g\langle h \rangle)^\ell = g^\ell \langle h \rangle$, we must have that $g^\ell \in \langle g \rangle \cap \langle h \rangle = \{e_G\}$. Consequently, the only possibility for ℓ is $\text{ord}(g) = p^k$, and we conclude that $\text{ord}(g\langle h \rangle) = p^k$. By our inductive hypothesis applies to $G/\langle h \rangle$ and its subgroup $g\langle h \rangle$ and the Fourth Isomorphism Theorem, there exists a subgroup H of G such that $G/\langle h \rangle \cong \langle g\langle h \rangle \rangle \times H/\langle h \rangle$. We claim at last that $G \cong \langle g \rangle \times H$. Given any element $x \in \langle g \rangle \cap H$, we have that $x\langle h \rangle \in \langle g\langle h \rangle \rangle \cap H/\langle h \rangle = \{e_G\langle h \rangle\}$ by the Fourth Isomorphism Theorem. We conclude therefore that $x \in \langle g \rangle \cap \langle h \rangle = \{e_G\}$, as desired. Considering that $p^{n-1} = p^k|H|/p$, we conclude that $|H| = p^{n-k}$ so that $G = \langle g \rangle H$ and $G \cong \langle g \rangle \times H$ by Corollary 3.8.14. □

3.10 Chapter 3 Exercises

3.10.1 Cosets and Lagrange's Theorem

Exercise 3.10.1. Prove that (i.) $\implies$ (ii.) $\implies$ (iii.) $\implies$ (iv.) of Proposition 3.1.4 hold.

Exercise 3.10.2. Use the One-Step Subgroup Test to establish that the rational numbers $\mathbb{Q}$ form a subgroup of the additive group $(\mathbb{R}, +)$ of real numbers; then, prove that $[\mathbb{R} : \mathbb{Q}]$ is infinite.

Exercise 3.10.3. Let G be a group. Prove that if H is a subgroup of G such that $[G : H] = 2$, then it holds that $gH = Hg$ for all elements $g \in G$.

Exercise 3.10.4. Let G be a group with subgroups H and K. Consider the set

$$HK = \{hk \mid h \in H \text{ and } k \in K\}$$

of Exercise 2.8.23. Prove that if H and K are finite, then $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Exercise 3.10.5. Let G be a cyclic group of order n. By Exercise 2.8.34, for each positive integer $d \mid n$, there exists a cyclic subgroup of G of order d. Complete the following steps to demonstrate that n is the sum of Euler's totient function over its positive divisors, i.e., we have that $n = \sum_{d|n} \phi(d)$ (cf. the paragraph preceding Exercise 2.8.28 for the definition of Euler's totient function).

(a.) Prove that every element of G lies in one and only one cyclic subgroup of order $d \mid n$. Conclude that the cyclic subgroup of G of order $d \mid n$ is unique, i.e., these subgroups partition G.

(b.) Prove that for each positive integer $d \mid n$, there exist $\phi(d)$ generators for the cyclic subgroup of G generated by d. Conclude that the cyclic subgroup of order d contains exactly $\phi(d)$ elements.

Conclude the desired result by combining parts (a.) and (b.) above.

Exercise 3.10.6. Consider Euler's totient function $\phi : \mathbb{Z} \to \mathbb{Z}_{>0}$ defined before Exercise 2.8.28. Complete the following steps to prove that $\phi(n)$ is an even integer for all integers $n \geq 2$.

(a.) Conclude by Exercise 2.8.28 that $\phi(n) = |\mathbb{Z}_n^*|$ for every positive integer n.

(b.) Conclude by Exercise 2.8.26 that there exists an element of order two in $\mathbb{Z}_n^*$.

(c.) Conclude the desired result by Lagrange's Theorem.

3.10.2 Quotient Groups and Normal Subgroups

Exercise 3.10.7. Let G be a group with a normal subgroup H. Prove that $\text{ord}(gH) \mid \text{ord}(g)$ for every element $g \in G$. Conclude that $\max\{\text{ord}(gH) \mid g \in G\} \leq \max\{\text{ord}(g) \mid g \in G\}$.

Exercise 3.10.8. Let G be a group with a subgroup H. Prove that if the index of H in G satisfies that $[G : H] = 2$, then H is a normal subgroup of G.

Exercise 3.10.9. Exhibit a non-cyclic group G and a normal subgroup H of G such that H and G/H are cyclic. Conclude that the converse of the first statement of Proposition 3.2.6 is false.

(**Hint:** By Corollary 3.1.13 and Exercise 3.10.8, it suffices to find a non-abelian group G of order $4 = 2 \cdot 2$ and any subgroup H of G of order two. We have already encountered one.)

Exercise 3.10.10. Exhibit a non-abelian group G and a normal subgroup H of G such that H and G/H are abelian. Conclude that the converse of the second statement of Proposition 3.2.6 is false.

(**Hint:** By Corollary 3.1.14 and Exercise 3.10.8, it suffices to find a non-abelian group G of order $6 = 2 \cdot 3$ and any subgroup H of G of order three. We have already encountered one.)

Exercise 3.10.11. Let G be a group with subgroups H and K. Consider the set

$$HK = \{hk \mid h \in H \text{ and } k \in K\}$$

of Exercises 2.8.23 and 3.10.4. Prove that if H is normal in G or K is normal in G, then HK is a subgroup of G. Even more, prove that if H and K are both normal in G, then HK is normal in G.

Exercise 3.10.12. Let G be a group with a subgroup H and a normal subgroup N. Prove that $H \cap N$ is a normal subgroup of H. Conclude that $H/(H \cap N)$ is a group.

Exercise 3.10.13. Let G be a group. Prove that if H is a subgroup of G such that no other subgroup of G has the same order as H, then H must be a normal subgroup of G.

(**Hint:** Consider the function $\chi_g : H \to gHg^{-1}$ defined by $\chi_g(h) = ghg^{-1}$. Use Exercise 1.10.6(a.).)

Exercise 3.10.14. Let G be a group. Let $Z(G) = \{x \in G \mid gx = xg \text{ for all elements } g \in G\}$ denote the center of G. By Exercise 2.8.18, we note that $Z(G)$ is a subgroup of G.

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

(b.) Prove that if $G/Z(G)$ is cyclic, then G is abelian.

Exercise 3.10.15. Let G be a group. Let $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ denote the normalizer of any subgroup $H \subseteq G$. Let $C_G(H)$ By Exercise 2.8.21, we note that $N_G(H)$ is a subgroup of G.

(a.) Prove that H is a normal subgroup of $N_G(H)$.

(b.) Prove that if K is a subgroup of G and H is a normal subgroup of K, then K is a subgroup of $N_G(H)$. Conclude that $N_G(H)$ is the "largest" subgroup of G with H as a normal subgroup.

Given any element $h \in H$, consider the centralizer $C_G(h) = \{g \in G \mid gh = hg\}$ of h in G. By Exercise 2.8.19, $C_G(x)$ is a subgroup of G. We define the **centralizer** of the subgroup H as the union of the centralizers of all elements $h \in H$ in G, i.e., $C_G(H) = \{g \in G \mid gh = hg \text{ for all elements } h \in H\}$.

(c.) Prove that $C_G(H)$ is a subgroup of G.

(d.) Prove that H is a normal subgroup of $C_G(H)$. Conclude that $C_G(H)$ is a subgroup of $N_G(H)$.

(e.) Prove that $C_G(H)$ is a normal subgroup of $N_G(H)$.

(**Hint:** By Proposition 3.2.1, it suffices to prove that for every triple of elements $h \in H$, $x \in N_G(H)$, and $g \in C_G(H)$, it holds that $(xgx^{-1})h = h(xgx^{-1})$. Use the fact that for every element $x \in N_G(H)$, there exists an element $k \in H$ such that $x^{-1}hx = k$ by definition.)

Exercise 3.10.16. Consider the additive group $(\mathbb{Q}, +)$ of rational numbers. Prove that $\mathbb{Z}$ is a normal subgroup of $\mathbb{Q}$; then, prove that every element of the quotient group $\mathbb{Q}/\mathbb{Z}$ has finite order. Conclude that there exists a group of infinite order such that each of its elements has finite order.

(**Hint:** Determine all possible left coset representatives for $0 + \mathbb{Z}$.)

3.10.3 Group Homomorphisms

Exercise 3.10.17. Prove that if G is a group of even order, then there are an odd number of elements of G of order two. Conclude that a group of even order admits a subgroup of order two.

(**Hint:** Prove that the function $\varphi : G \to G$ defined by $\varphi(g) = g^{-1}$ is a bijection. Conclude that for every non-identity element $g \in G$, there exists a non-identity element $h \in G$ such that $g^{-1} = h$. Count the number of non-identity elements of G to deduce the result of the statement.)

Exercise 3.10.18. Prove that if G is an abelian group of odd order, then for each element $g \in G$, there exists a unique element $h \in G$ such that $h^2 = g$. Conclude that in an abelian group of odd order, every element admits a unique square root.

(**Hint:** Prove that the function $\varphi : G \to G$ defined by $\varphi(g) = g^2$ is a homomorphism. Compute its kernel; then, use Lagrange's Theorem to conclude that φ is in fact an isomorphism.)

Exercise 3.10.19. Let $(G, *)$ and $(H, \star)$ be groups. Consider a group homomorphism $\varphi : G \to H$.

(a.) Prove that $\ker \varphi$ is a normal subgroup of G.

(b.) Conversely, suppose that N is a normal subgroup of G. Prove that there exists a group $(K, \cdot)$ and homomorphism $\pi : G \to K$ such that $N = \ker \pi$. Conclude that the normal subgroups of any group G are precisely the kernels of group homomorphisms from G.

(**Hint:** Consider the **canonical surjection** $\pi : G \to G/N$ defined by $\pi(g) = gN$.)

Exercise 3.10.20. Consider the collection $\mathfrak{G}$ of all groups. Prove that $(G, *) \sim (H, \star)$ if and only if there exists an isomorphism $\varphi : (G, *) \to (H, \star)$ is an equivalence relation on $\mathfrak{G}$.

We note that the equivalence classes of the above equivalence relation are called the **isomorphism classes** of groups. If there are n distinct equivalence classes of groups that satisfy a certain property $\mathcal{P}$, then we say that there are n groups that satisfy property $\mathcal{P}$ **up to isomorphism**.

Exercise 3.10.21. Prove that there is only one infinite cyclic group up to isomorphism.

Exercise 3.10.22. Prove that there is only one cyclic group of order n up to isomorphism.

3.10.4 Cayley's Theorem

Exercise 3.10.23. Let G be a group with a subgroup H such that $[G : H]$ is finite. Prove that there exists a normal subgroup N of G such that $N \subseteq H$ and $[G : N] \mid [G : H]!$.

(**Hint:** We note that by Cayley's Theorem and the First Isomorphism Theorem, it suffices to find a group homomorphism from G to the symmetric group on the left cosets G/H of H in G whose kernel is contained in H. Consider the function $\varphi : G \to \mathfrak{S}_{G/H}$ defined by $\varphi(g)(xH) = gxH$.)

Exercise 3.10.24. Let G be a finite group with a subgroup H such that $[G : H]$ is the smallest prime number p that divides $|G|$. Prove that H is a normal subgroup of G.

(**Hint:** We note that by Exercise 3.10.23, there exists a normal subgroup N of G such that $N \subseteq H$ and $[G : N] \mid p!$. Even more, by Lagrange's Theorem, we have that $[G : H]|H| = |G| = [G : N]|N|$, hence we find that $p!|N| = [G : N]|N|q = pq|H|$. Conclude that $|H| \mid |N|$ so that $H = N$.)

3.10.5 The Group Isomorphism Theorems

Exercise 3.10.25. Prove that $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$ are not isomorphic.

(**Hint:** Exercise 2.8.24 and Proposition 3.3.18 directly imply this.)

Exercise 3.10.26. Let G be a group with a normal subgroup K. Let H be any group such that there exists a group homomorphism $\varphi : G \to H$.

(a.) Prove that if φ is surjective, then $\varphi(K)$ is a normal subgroup of H.

(b.) Prove that if φ is an isomorphism, then we have that $G/K \cong H/\varphi(K)$.

(**Hint:** Consider the function $\psi : G \to H/\varphi(K)$ defined by $\psi(g) = \varphi(g)\varphi(K)$.)

(c.) Conclude that for every group isomorphism $\varphi : G \to G$, we have that $G/K \cong G/\varphi(K)$.

Exercise 3.10.27. Consider the general linear group $\mathrm{GL}(2,\mathbb{R}) = \{A \in \mathbb{R}^{2\times 2} \mid \det(A) \neq 0\}$ and the special linear group $\mathrm{SL}(2,\mathbb{R}) = \{A \in \mathbb{R}^{2\times 2} \mid \det(A) = 1\}$. Let $\mathbb{R}^\times$ denote the set of nonzero real numbers. Complete the following steps to prove that $(\mathrm{GL}(2,\mathbb{R})/\mathrm{SL}(2,\mathbb{R}), \cdot) \cong (\mathbb{R}^\times, \cdot)$.

(a.) Prove that the determinant function is a group homomorphism from $\mathrm{GL}(2,\mathbb{R})$ to $(\mathbb{R}^\times, \cdot)$.

(**Hint:** Prove that $\det(AB) = \det(A)\det(B)$ for any real 2×2 matrices A and B.)

(b.) Prove that φ is surjective with $\ker\varphi = \mathrm{SL}(2,\mathbb{R})$.

(c.) Conclude the desired result by the First Isomorphism Theorem.

Exercise 3.10.28. Consider the circle group $\mathbb{T} = \{\cos\theta + i\sin\theta \mid \theta \in \mathbb{R}\}$ under complex multiplication. Complete the following steps to prove that $(\mathbb{R}/\mathbb{Z}, +) \cong (\mathbb{T}, \cdot)$.

(a.) Prove that the function $\varphi : (\mathbb{R}, +) \to (\mathbb{T}, \cdot)$ defined by $\varphi(\theta) = \cos\theta + i\sin\theta$ is a surjective group homomorphism with $\ker\varphi = \{2\pi n \mid n \in \mathbb{Z}\}$.

(b.) Prove that the function $\mu : (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined by $\mu(x) = 2\pi x$ is a group isomorphism.

(c.) Conclude from parts (b.) and (c.) of Exercise 3.10.26 that $(\mathbb{R}/\mathbb{Z}, +) \cong (\mathbb{T}, \cdot)$.

3.10.6 The Symmetric Group on n Letters, Revisited

Exercise 3.10.29. Compute the number of distinct conjugacy classes in $\mathfrak{S}_5$.

Exercise 3.10.30. Compute the number of distinct 3-cycles in $\mathfrak{S}_5$.

3.10.7 The Alternating Group on n Letters

Exercise 3.10.31. Prove that $\mathfrak{A}_n$ is generated by all three-cycles on n letters.

Exercise 3.10.32. We say that a group G is **simple** if its only normal subgroups are the trivial subgroup $\{e_G\}$ and the group itself. Prove that $\mathfrak{A}_n$ is simple for $n = 3$ and all integers $n \geq 5$. Conclude that $\mathfrak{A}_5$ is the smallest (in terms of order) non-abelian simple group.

Exercise 3.10.33. Prove that $\mathfrak{A}_4$ has a proper nontrivial normal subgroup, hence $\mathfrak{A}_4$ is not simple.

(**Hint:** Consider the injective function $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathfrak{A}_4$ defined by $\varphi(0,0) = (1)$, $\varphi(1,0) = (12)(34)$, $\varphi(0,1) = (13)(24)$, and $\varphi(1,1) = (14)(23)$. Prove that φ is a group homomorphism; then, conclude by the First Isomorphism Theorem that $\varphi(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is a proper nontrivial normal subgroup of $\mathfrak{A}_4$.)

Exercise 3.10.34. We say that a group G is **solvable** if there exist subgroups

$$G_0 = \{e_G\} \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

such that G_i is a normal subgroup of G_{i+1} and the quotient groups G_{i+1}/G_i are abelian for each integer $0 \leq i \leq n-1$. Prove that $\mathfrak{A}_5$ is the smallest (in terms of order) non-solvable group.

We will eventually come to understand that Exercises 3.10.33 and 3.10.34 combined imply that quartic polynomials can be solved by radicals (i.e., there exists a quartic formula) because $\mathfrak{A}_4$ is not simple, but there is no quintic formula because $\mathfrak{A}_5$ is simple. Even more, polynomials of degree exceeding five are not solvable by radicals (hence the name "solvable") because every symmetric group on $n \geq 5$ letters contains an isomorphic copy of $\mathfrak{A}_5$. We note that this rationale was originated by the French mathematician Évariste Galois, who perished in a duel in 1832 at the age of 20.

3.10.8 External and Internal Direct Products

Exercise 3.10.35. Let $G_1, \ldots, G_n$ be groups with external direct product $G_1 \times \cdots \times G_n$. Prove that $G_1 \times \cdots \times G_n$ is abelian if and only if $G_1, \ldots, G_n$ are abelian.

Exercise 3.10.36. Let G, H, and K be groups with external direct product $G \times H \times K$. Prove that the external direct product is associative, i.e., we have that $(G \times H) \times K \cong G \times (H \times K)$.

(**Hint:** Prove that $(G \times H) \times K$ and $G \times (H \times K)$ are both isomorphic to $G \times H \times K$.)

Exercise 3.10.37. Let $G_1, \ldots, G_n$ be groups with external direct product $G_1 \times \cdots \times G_n$. Prove that for any permutation σ of the indices $1, \ldots, n$, we have that $G_1 \times \cdots \times G_n \cong G_{\sigma(1)} \times \cdots \times G_{\sigma(n)}$.

(**Hint:** By Exercise 3.10.36, it suffices to prove that $G \times H \cong H \times G$ for any groups G and H. One can also prove this directly by exhibiting an isomorphism $\varphi : G_1 \times \cdots \times G_n \to G_{\sigma(1)} \times \cdots \times G_{\sigma(n)}$. Or third, it is also possible to proceed by induction on the number n of factors in the product.)

Exercise 3.10.38. Let $G_1, \ldots, G_n$ be groups with external direct product $G_1 \times \cdots \times G_n$.

(a.) Prove that the function $\pi_i : G_1 \times \cdots \times G_n \to G_i$ defined by $\pi_i(g_1, \ldots, g_n) = g_i$ is a group homomorphism with kernel $G_1 \times \cdots \times G_{i-1} \times \{e_{G_i}\} \times G_{i+1} \times \cdots \times G_n$.

(b.) Prove that the function $\delta_i : G_1 \times \cdots \times G_n \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ defined by $\delta_i(g_1, \ldots, g_n) = (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$ is a group homomorphism with kernel

$$\gamma_i(G_i) = \{(e_{G_1}, \ldots, g, \ldots, e_{G_n}) \mid g \in G_i\}.$$

Exercise 3.10.39. Prove that the dihedral group $D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$ cannot be realized as an internal direct product of any pair of proper non-trivial subgroups of D_4.

(**Hint:** On the contrary, if $D_4 = HK$ for some proper non-trivial subgroups H and K of D_4, then we must have that $|H| = 4$ and $|K| = 2$. Prove that H and K must be abelian.)

Exercise 3.10.40. Consider the dihedral group $D_6 = \{1, r, r^2, r^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, r^5s\}$.

(a.) Prove that $K = \{1, r^2, r^4, s, r^2s, r^4s\}$ is a subgroup of D_6.

(**Hint:** Every element of K can be written as $r^{2m}s^n$ for some integers m and n. Use this and the fact that $sr = r^5s$ to conclude that K is closed under the binary operation of D_6.)

(b.) Prove that if $H = \{1, r^3\}$, then D_6 is the internal direct product of H and K.

3.10.9 Finite Abelian Groups

Exercise 3.10.41. Consider any positive integer n with unique prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$ for some distinct primes p_i and non-negative integers e_i. Complete the following steps to prove that

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}.$$

(a.) We proceed by induction on the number k of prime factors of n. By definition, if $k = 2$, then there exist integers p and q such that $\gcd(p, q) = 1$ and $n = pq$. Prove that the order of $(a + p\mathbb{Z}, b + q\mathbb{Z})$ is the smallest positive integer k with $ak \equiv 0 \pmod{p}$ and $bk \equiv 0 \pmod{q}$.

(b.) Conclude that $\text{ord}(1 + p\mathbb{Z}, 1 + q\mathbb{Z})$ is the smallest positive integer k such that $p \mid k$ and $q \mid k$.

(c.) Explain why $\text{lcm}(p, q)$ divides $\text{ord}(1 + p\mathbb{Z}, 1 + q\mathbb{Z})$; then, use Exercise 1.10.34 to verify that $\text{lcm}(p, q) = pq$. Conclude that pq divides the order of $(1 + p\mathbb{Z}, 1 + q\mathbb{Z})$.

(d.) Conversely, explain why the order of $(1 + p\mathbb{Z}, 1 + q\mathbb{Z})$ is at most pq.

(e.) Conclude that $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ is a cyclic group with generator $(1 + p\mathbb{Z}, 1 + q\mathbb{Z})$; then, use Proposition 3.3.20 to establish that $\mathbb{Z}/pq\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z} \times q\mathbb{Z})$.

(f.) By induction, we may assume that the claim holds for k. We must establish the isomorphism in the case that $n = p_1^{e_1} \cdots p_{k+1}^{e_{k+1}}$. Explicitly find positive integers r and s for which $\gcd(r, s) = 1$ and $n = rs$; then, use our induction hypothesis to conclude that $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z})$. Be sure to choose r and s such that $\mathbb{Z}/r\mathbb{Z} \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})$ and $\mathbb{Z}/s\mathbb{Z} \cong \mathbb{Z}/p_{k+1}^{e_{k+1}}$.

References

[Bag19] J. Bagaria. *Zermelo-Fraenkel Set Theory*. 2019. URL: https://plato.stanford.edu/entries/set-theory/ZF.html.

[CKK22] P. Corn, S. Kallasa, and J. Khim. *Axiom of Choice*. 2022. URL: https://brilliant.org/wiki/axiom-of-choice/.

[Con22] K. Conrad. *The Gaussian Integers*. 2022. URL: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf.

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra*. 3rd ed. John Wiley & Sons, Inc., 2004.

[DW00] J.P. D'Angelo and D.B. West. *Mathematical Thinking: Problem Solving and Proofs*. Upper Saddle River, NJ: Prentice-Hall, 2000.

[Gon22] A. Gonzalez. *Fundamental Counting Principle*. 2022. URL: https://brilliant.org/wiki/fundamental-counting-principle/.

[Hen19] Jonah N. Henry. *Groups Satisfying the Converse to Lagrange's Theorem*. 2019. URL: https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=4484&context=theses.

[JB21] T.W. Judson and R.A. Beezer. *Abstract Algebra: Theory and Applications*. 2021.

[Mag11] A. Magidin. *Why are two permutations conjugate iff they have the same cycle structure?* 2011. URL: https://math.stackexchange.com/a/48137/390180.

[Wil15] R.A. Wilson. *An example of a PID which is not a Euclidean domain*. 2015. URL: http://www.maths.qmul.ac.uk/~raw/MTH5100/PIDnotED.pdf.