

# Abstract Algebra

C. Caruvana

Fall 2025

## Contents

<b>1</b>	<b>Brief History and a Motivating Example</b>	<b>2</b>
<b>2</b>	<b>Brief Commentary on Mathematical Proofs</b>	<b>3</b>
2.1	Direct Proof . . . . .	3
2.2	Proof by Contrapositive . . . . .	4
2.3	Proof by Contradiction . . . . .	4
<b>3</b>	<b>Sets, Relations, and Functions</b>	<b>4</b>
3.1	Sets . . . . .	5
3.2	Operations with Sets . . . . .	5
3.3	Cartesian Products, Relations, and Functions . . . . .	7
3.4	Equivalence Relations . . . . .	10
<b>4</b>	<b>Introducing Groups</b>	<b>12</b>
4.1	Getting to Know Groups . . . . .	12
4.2	Subgroups . . . . .	19
4.3	An Introduction to Homomorphisms . . . . .	20
4.4	Cyclic Groups and Subgroups . . . . .	23
<b>5</b>	<b>Permutation Groups</b>	<b>28</b>
5.1	Permutations and Symmetric Groups . . . . .	28
5.2	Dihedral Groups . . . . .	37
5.3	Cayley's Theorem . . . . .	38
<b>6</b>	<b>Cosets and Lagrange's Theorem</b>	<b>38</b>
6.1	Cosets . . . . .	38
6.2	Lagrange's Theorem . . . . .	41
<b>7</b>	<b>Creating New Groups From Old</b>	<b>43</b>
7.1	Direct Products . . . . .	43
7.2	Normal Subgroups and Quotient Groups . . . . .	48
7.2.1	Normal Subgroups . . . . .	48
7.2.2	Quotient Groups . . . . .	49

7.2.3 Isomorphism Theorems . . . . .	51
<b>8 Classifying Finite Abelian Groups</b>	<b>57</b>

## Comment on Assumed Knowledge

Throughout these notes, we will assume the reader is familiar with the division algorithm and fundamental properties of the determinant for square matrices. For reference, we list the particular facts that will be used throughout.

**The Division Algorithm.** For any integer  $n$  and any positive integer  $d$ , there are unique integers  $q$  and  $r$  with  $0 \leq r < d$  such that  $n = dq + r$ .

**Fact.** For square matrices  $A$  and  $B$ ,  $\det(AB) = \det(A) \cdot \det(B)$ .

## 1 Brief History and a Motivating Example

The following historical commentary has been gathered from the Wikipedia articles on [History of Algebra](#) and [Abstract Algebra](#).

The word *algebra* is derived from the Arabic *al-jabr* which appeared in the title of a treatise written in 830 by Al-Khwarizmi, a Persian mathematician. The treatise itself was about linear and quadratic equations. Note, however, that societies all around the world had independently developed their own studies of solving algebraic equations well before Al-Khwarizmi's treatise.

For the ancient Babylonians and the Greeks, algebraic concepts were largely geometric. In fact, Greek and Vedic Indian mathematicians used geometry to solve certain algebraic equations. Much later, Descartes (1596-1650) introduced modern notation and showed that problems of geometry can be expressed and solved in terms of algebra.

Diophantus and Brahmagupta, independently, moved away from the geometric perspective toward one focused on finding numbers that satisfied given equations.

Sharaf al-Din al-Tusi began the transition from static equation solving to a more functional approach, where functions are seen as dynamic entities representing motion.

It is not until the 19th and 20th centuries that *abstract algebra* is developed.

Abstract algebra, which we understand as the study of “algebraic structure,” emerged through the identification of common themes in problems of number theory, geometry, analysis, and algebraic equation solving. In this semester, we will be focusing on a branch of abstract algebra known as *group theory*. Loosely speaking, a group is a collection of objects with a particular kind of operation. We will define them carefully after considering some motivating examples and setting up our mathematical formalism.

**Example 1.1.** Consider, for example, the possible symmetric positions of a line segment:



There are two possible actions on this structure: “do nothing” or reversing the poles. Note that reversing the poles twice has the same effect as “doing nothing.”

Another way to model this example is to use “words.” Let  $P$  represent the “positive” side and  $N$  represent the “negative” side. As presented, the word  $PN$  represents the initial orientation. Reversing the poles yields the word  $NP$ . Thus, the possible states are thus  $PN$  and  $NP$ .

We can also abstract away the “actions” here of *doing nothing* and *reversing the poles*. Let  $0$  represent the action of “doing nothing” and  $1$  represent the action of “reversing the poles.” In the following table, consider the rows as indicating which of the two actions to be applied first, and then the columns indicate which operation is done afterwards.

	0	1
0	0	1
1	1	0

As noted above and displayed in the second row, second column of the table, reversing the poles twice results in the same action as the “doing nothing” action.

## 2 Brief Commentary on Mathematical Proofs

One of the primary activities in this course is proof-writing. Mathematical proofs are formal arguments that establish the logical necessity of a given statement. Generally speaking, a *statement* is any expression which has a truth value. For example, “2 is even” is a statement (and is true) and “ $12 + 5 = 60$ ” is a statement (which is false). An expression like  $x + 5$  is not a statement because there is not a coherent way to assign a truth value to it.

The general structure of discourse here consists of two things: there are the objects of discourse and there are statements referring to the objects.

Of primary importance are conditional statements of the form “if  $p$ , then  $q$ ,” where  $p$  and  $q$  are statements themselves. We will also deal with quantified statements:

- $\forall x P(x)$  is the statement “for every  $x$ ,  $x$  satisfies  $P$ ,” and
- $\exists x P(x)$  is the statement “there exists an  $x$  such that  $x$  satisfies  $P$ ,”

### 2.1 Direct Proof

A standard mathematical proof proving that the implication “if  $p$ , then  $q$ ” is true starts by assuming  $p$  and deducing the logical necessity of the truth of  $q$ . We begin with a very basic example, introducing the conventional proof-writing format in the process.

**Claim.** Suppose  $x$  represents a real number. If  $3x + 2 = 17$ , then  $x = 5$ .

*Proof.* Suppose  $3x + 2 = 17$ . By subtracting 2 from both sides of the equation, we obtain that  $3x = 15$ . Then, dividing by 3 on both sides of the equation yields that  $x = 5$ .  $\square$

Formal proofs are written in a narrative fashion using the expected natural language, sometimes assisted by some mathematical symbols. Like anything else, proof-writing is a skill that improves with practice.

## 2.2 Proof by Contrapositive

Another valid proof technique for proving “if  $p$ , then  $q$ ,” is to prove what is known as the corresponding *contrapositive* statement: “if it’s not true that  $q$ , then it’s not true that  $p$ .”

Let’s see a basic example.

**Claim.** Suppose  $x$  represents a real number. If  $x^3 - 1 < 0$ , then  $x < 1$ .

*Proof.* We proceed by way of the contrapositive. So, suppose  $x \geq 1$ . It follows that  $x^3 \geq 1$  and, then, that  $x^3 - 1 \geq 0$ .  $\square$

**Sanity Check 2.1.** If  $x$  is a real number and  $x \geq 1$ , why is it that  $x^3 \geq 1$ ?

**Exercise 2.2.** An integer  $n$  is said to be *even* if there is an integer  $k$  such that  $n = 2k$ . In other words,  $n$  is even if 2 divides  $n$  with no remainder. Prove that, given an integer  $n$ , if  $n^2$  is even, then  $n$  is even.

## 2.3 Proof by Contradiction

Proof by contradiction, also known as *reductio ad absurdum*, is an ancient argument style used often in Platonic dialogues. The basic format is this: First you pose the objection, “suppose what you claim to be true is false.” You then attempt to deduct a logical impossibility. The standard introductory proof by contradiction (known certainly to the ancient Greeks) is that of the irrationality of  $\sqrt{2}$ .

**Claim.** The number  $\sqrt{2}$  is not rational.

*Proof.* By way of contradiction, suppose that  $\sqrt{2}$  is rational. By taking out any common factors, we can thus write  $\sqrt{2} = \frac{p}{q}$  where  $p$  and  $q$  are integers with no common factors.

Squaring both sides, we obtain that  $2 = \frac{p^2}{q^2}$  and, thus, that  $2q^2 = p^2$ . It follows that  $p^2$  is even and, thus, by Exercise 2.2,  $p$  is even. That is,  $p = 2k$  for some integer  $k$ . It follows that

$$\begin{aligned} 2q^2 &= (2k)^2 \\ &= 4k^2. \end{aligned}$$

Dividing by 2 yields  $q^2 = 2k^2$ . Hence,  $q^2$  is even which, again, by Exercise 2.2, asserts that  $q$  is even. We now see that  $p$  and  $q$  are both even, contradicting the assumption that  $p$  and  $q$  had no common factors. Therefore,  $\sqrt{2}$  is irrational.  $\square$

**Sanity Check 2.3.** Why can we write ratios of integers in so-called reduced terms? (*Hint.* See the *Fundamental Theorem of Arithmetic*.)

## 3 Sets, Relations, and Functions

The theory of sets provides us with a twofold benefit: they offer us a foundation on which to formalize our mathematics and they off us a relatively simple structure with which to continue practicing the basics of proof-writing.

## 3.1 Sets

A *set* is a well-defined collection of primitive objects. In the case of pure set theory, the *only* primitive objects are sets, themselves. In the language of set theory, we use the symbol  $\in$  as a relation between an object (it can be a set)  $x$  and a set  $A$  in the following way:  $x \in A$  is the statement that  $x$  is an element of the set  $A$ . For example, if we say that  $X$  is the set of all positive real numbers, then  $1 \in X$  and  $-5 \notin X$ .

Guided by convention, we use  $\mathbb{R}$  to refer to the set of all real numbers,  $\mathbb{Z}$  to refer to the set of all integers,  $\mathbb{Q}$  to refer to the set of all rational numbers, and  $\mathbb{N}$  to refer to the set of all natural numbers. Not all mathematicians agree whether  $\mathbb{N}$  contains 0 or not. To align with our chosen textbook, we will observe the convention that  $\mathbb{N}$  consists of only the positive integers.

One can define (finite) or refer to sets using *set-roster* notation; e.g.  $X = \{a, b, c\}$ . Here,  $X$  is asserted to be the set containing as its elements  $a$ ,  $b$ , and  $c$ .

The most common method to define or refer to sets is the *set-builder* notation;

$$X = \{x \in \mathbb{R} : x > 0\}.$$

Here,  $X$  is asserted to be the set of positive real numbers. The expression  $\{x \in \mathbb{R} : x > 0\}$  can be read as:

► “The set of real numbers  $x$  such that  $x$  is positive.”

Another set that will be important to us is the set  $\mathbb{C}$  consisting of all complex numbers; that is,  $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$  where  $i$  is chosen to be a solution to the equation  $x^2 + 1 = 0$ .

Note that our expression for  $\mathbb{C}$  above is not of the form  $\{x \in X : P(x)\}$  where  $X$  is a set and  $P$  is a *predicate* of  $x$ . We won’t concern ourselves here with the details of this notation and will simply accept it as a valid incarnation of set-builder notation.

**Definition 3.1.** Two sets  $A$  and  $B$  are said to be *equal*, denoted  $A = B$ , if they consist of exactly the same elements.

**Definition 3.2.** For two sets  $A$  and  $B$ , we say that  $B$  is a *subset* of  $A$ , denoted by  $B \subseteq A$ , if every element of  $B$  is an element of  $A$ . If  $B \subseteq A$  and  $B \neq A$ , then we say that  $B$  is a *proper subset* of  $A$ , which we may denote by  $B \subsetneq A$ .<sup>1</sup>

**Pro Tip.** Two sets  $A$  and  $B$  are equal if and only if  $A \subseteq B$  and  $B \subseteq A$ . Hence, a common strategy for proving that two sets are equal is to prove that they are both subsets of the other.

**Definition 3.3.** The *empty set*, denoted by either  $\emptyset$  or  $\{\}$ , is the unique set containing no elements.

## 3.2 Operations with Sets

We can form new sets from old with some basic operations.

---

<sup>1</sup>Our chosen textbook uses the notation  $\subset$  in place of  $\subseteq$ . As such, we must avoid using the visual relationships between  $\leq$  and  $\subseteq$ , and  $<$  and  $\subset$  here.

**Definition 3.4.** Given two sets  $A$  and  $B$ , the *union* of  $A$  and  $B$ , denoted by  $A \cup B$ , is the set consisting of all  $x$  such that either  $x \in A$  or  $x \in B$ .

**Comment.** In mathematics, the “or” is always the *inclusive* or. So, a phrase of the form “ $p$  or  $q$ ” is only to be interpreted as meaning “ $p$ , or  $q$ , or both.” We will address one way to deal with the exclusive or below.

**Definition 3.5.** Given two sets  $A$  and  $B$ , the *intersection* of  $A$  and  $B$ , denoted by  $A \cap B$ , is the set consisting of all  $x$  such that  $x \in A$  and  $x \in B$ .

**Exercise 3.1.** Prove that, for sets  $A$  and  $B$ ,

- $A \cup B = B \cup A$  and
- $A \cap B = B \cap A$ .<sup>2</sup>

**Exercise 3.2.** Prove that, for sets  $A$ ,  $B$ , and  $C$ ,

- $A \cup (B \cup C) = (A \cup B) \cup C$  and
- $A \cap (B \cap C) = (A \cap B) \cap C$ .<sup>3</sup>

**Definition 3.6.** Given two sets  $A$  and  $B$ , we define the *set difference*  $A \setminus B$  to be

$$\{x \in A : x \notin B\}.$$

When a given context  $U$  (referred to as the *universal set*) is understood, we define the *complement* of a set  $A \subseteq U$  to be  $A' = U \setminus A$ .

The *symmetric difference* between two sets exemplifies the concept of the exclusive or. The standard convention for the symmetric difference is as follows:

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

We will return to this later.

**Definition 3.7.** Two sets  $A$  and  $B$  are said to be *disjoint* if  $A \cap B = \emptyset$ .

The operations of union and intersection extend well beyond contexts where only two sets are involved.

**Definition 3.8.** Suppose  $\mathcal{A}$  is a set of sets (that is, each  $A \in \mathcal{A}$  is a set). We define

$$\bigcup \mathcal{A} = \bigcup_{A \in \mathcal{A}} A = \{x : \exists A \in \mathcal{A} (x \in A)\}.$$

Similarly, we define

$$\bigcap \mathcal{A} = \bigcap_{A \in \mathcal{A}} A = \{x : \forall A \in \mathcal{A} (x \in A)\}.$$

---

<sup>2</sup>That is, the union and intersection operations are *commutative*.

<sup>3</sup>That is, the union and intersection operations are *associative*.

These will often show up over *countable* sets; e.g. if  $A_n$  is a set for each  $n \in \mathbb{N}$ , then

$$\bigcup_{n=1}^{\infty} A_n = \bigcup_{n \in \mathbb{N}} A_n = \{x : \exists n \in \mathbb{N} (x \in A_n)\}.$$

**Proposition 3.9.** For any set  $A$ ,

- $A \cup A = A \cap A = A \cup \emptyset = A$  and
- $A \setminus A = A \cap \emptyset = \emptyset$ .

**Proposition 3.10** (Distributive Properties). For sets  $A$ ,  $B$ , and  $C$ ,

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$  and
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .

**Theorem 3.11** (DeMorgan's Laws). For any two subsets  $A$  and  $B$  of a given universal set  $U$ ,

- $(A \cap B)' = A' \cup B'$  and
- $(A \cup B)' = A' \cap B'$ .

**Exercise 3.3.** Prove Theorem 3.11.

### 3.3 Cartesian Products, Relations, and Functions

Cartesian products inherit their name from Descartes.

**Definition 3.12.** Given sets  $X$  and  $Y$ , the *Cartesian product* of  $X$  with  $Y$  is

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

For example, the usual coordinate plane is  $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ .

**Definition 3.13.** For sets  $X$  and  $Y$ , a *relation* between  $X$  and  $Y$  is a subset of  $X \times Y$ . When  $R \subseteq X \times Y$ , we sometimes use the notation  $xRy$  to mean  $(x, y) \in R$ .

**Definition 3.14.** Given two sets  $X$  and  $Y$ , a *function*  $f$  with *domain*  $X$  and *codomain*  $Y$  is a relation between  $X$  and  $Y$  with the following properties:

- For every  $x \in X$ , there is some  $y \in Y$  such that  $(x, y) \in f$ .<sup>4</sup>
- For every  $x \in X$  and  $y, z \in Y$ , if  $(x, y) \in f$  and  $(x, z) \in f$ , then  $y = z$ .<sup>5</sup>

---

<sup>4</sup>In some contexts, *partial* functions are used and only have to satisfy the second property listed here (that is, they need not have full domain).

<sup>5</sup>This is formally stating that there is a unique element  $y \in Y$  which satisfies  $(x, y) \in f$ . In less formal language, this is a version of the Vertical Line Test.

We use the notation  $f : X \rightarrow Y$  to denote that  $f$  is a function from  $X$  to  $Y$ . We will also use the notation  $f(x)$  to denote the unique member of  $Y$  such that  $(x, f(x)) \in f$ . The *image* or *range* of a function  $f : X \rightarrow Y$  is defined to be  $f[X] = \{f(x) : x \in X\}$ .<sup>6</sup>

**Comment.** We will say that two functions  $f$  and  $g$  are *equal*, denoted  $f = g$ , if they are equal *as sets*.

**Example 3.15.** The relation

$$R = \{(x, y) \in \mathbb{R}^2 : x^2 = y^4\}$$

is not a function. Consider the fact that both  $(1, 1) \in R$  and  $(1, -1) \in R$ .

You may recall exercises from previous courses with the flavor of “rewrite *blah* as a function of *blech*” which involved algebraic manipulation of expressions. For example, in the equation  $x = y^2$ ,  $x$  can be seen as a function of  $y$ , but  $y$  *cannot* be seen as a function of  $x$ . In these kinds examples, the issue of the domain tends to be ignored due to course focus, and they are typically intervals of real numbers, anyway.

We would like to point out here, though, that there are situations in which an equation can express  $y$  as a function of  $x$ , but cannot be rewritten using familiar algebraic tools in the form  $y = f(x)$ .

**Exercise 3.4.** Show that the relation

$$R = \{(x, y) \in \mathbb{R}^2 : x = y + y^5\}$$

is a function. (*Hint.* You can use techniques from Calculus to show that  $y = x + x^5$  is a bijection. Then, by the discussion below, it must have an inverse function, and that inverse function is exactly  $R$ .)

Before we get to function inverses, we will need the notion of *composition*.

**Definition 3.16.** Suppose  $R \subseteq X \times Y$  and  $S \subseteq Y \times Z$ . The *composition* relation  $S \circ R \subseteq X \times Z$  is defined to be

$$S \circ R = \{(x, z) \in X \times Z : \exists y \in Y ((x, y) \in R, (y, z) \in S)\}.$$

**Exercise 3.5.** Suppose  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ . Show that the composition  $g \circ f$  is a function  $X \rightarrow Z$ .

Since relations serve as a broader context than functions, we start by defining the *inverse* of a relation, which always exists and is, itself, a relation.

**Definition 3.17.** Given  $R \subseteq X \times Y$ , we define the *inverse relation* of  $R$  to be

$$R^{-1} = \{(y, x) \in Y \times X : (x, y) \in R\}.$$

---

<sup>6</sup>Note the divergence in the notation here from the chosen textbook’s. Either is acceptable, though it is sometimes useful to distinguish between a function being applied to particular elements of its domain and sets consisting of such applications.

Under what conditions is  $R^{-1}$  guaranteed to be a function from  $Y$  to  $X$ ? Examining Definition 3.14 in this context should naturally draw one to the following notions.

**Definition 3.18.** Suppose  $f : X \rightarrow Y$  is a function. Then

- $f$  is *injective* or *one-to-one* provided that, for  $x_1, x_2 \in X$ , if  $f(x_1) = f(x_2)$ , then  $x_1 = x_2$ .<sup>7</sup>
- $f$  is *surjective* or *onto* if, for every  $y \in Y$ , there is some  $x \in X$  such that  $f(x) = y$ .
- $f$  is *bijective* if it is both injective and surjective.

**Definition 3.19.** For any space  $X$ , we define the *identity* map  $\text{id}_X : X \rightarrow X$  by the rule  $\text{id}_X(x) = x$ . Note that  $\text{id}_X$  is a bijection.

Though the following does not align yet with Definition 3.17, we present it in this incarnation for the sake of familiarity.

**Definition 3.20.** Suppose  $f : X \rightarrow Y$  and  $g : Y \rightarrow X$ . The function  $g$  is said to be the *inverse* function of  $f$ , denoted by  $f^{-1}$ , if  $g \circ f = \text{id}_X$  and  $f \circ g = \text{id}_Y$ . In the case that a function  $f : X \rightarrow Y$  has an inverse function,  $f$  is said to be *invertible*.

**Theorem 3.21.** A function is invertible if and only if it is bijective.

In other words, a function is invertible if and only if its inverse relation is, itself, a function.

**Example 3.22.** Consider  $S : \mathbb{R} \rightarrow [0, \infty)$  defined by  $S(x) = x^2$ . Note that  $S$  is surjective but not injective. Hence,  $S$  is not invertible.

Note, however, that the standard square root function  $\text{sqrt} : [0, \infty) \rightarrow [0, \infty)$ , which chooses, for each  $y \geq 0$ , the *non-negative* solution to  $x^2 = y$ , is a function with the property that  $S \circ \text{sqrt} = \text{id}_{[0, \infty)}$ . On the other hand, for any  $x \in \mathbb{R}$ ,  $\text{sqrt} \circ S(x) = |x|$ , the absolute value of  $x$ .

**Exercise 3.6.** Define  $f : \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Q}$  by the rule  $f(k, n) = \frac{k}{n}$ . Show that  $f$  is surjective but not injective.

Even when we restrict our attention to invertible functions, the composition operation fails to be commutative.

**Example 3.23.** Consider  $f : \mathbb{R} \rightarrow \mathbb{R}$  defined by  $f(x) = x + 2$  and  $g : \mathbb{R} \rightarrow \mathbb{R}$  defined by  $g(x) = x^3$ . Note that

$$g \circ f(x) = (x + 2)^3$$

and that

$$f \circ g(x) = x^3 + 2.$$

Since  $g \circ f(0) = 8$  and  $f \circ g(0) = 2$ , we see that  $g \circ f \neq f \circ g$ .

---

<sup>7</sup>This is a version of the Horizontal Line Test.

**Exercise 3.7.** Find a pair of functions  $f, g : \mathbb{R} \rightarrow \mathbb{R}$  that aren't inverses of each other such that neither is the identity function  $\text{id}_{\mathbb{R}}$  and the equation  $g \circ f = f \circ g$  is satisfied.

**Exercise 3.8.** Suppose  $f : W \rightarrow X$ ,  $g : X \rightarrow Y$ , and  $h : Y \rightarrow Z$ . Prove that composition is associative; that is, show that  $(h \circ g) \circ f = h \circ (g \circ f)$ .

**Exercise 3.9.** Suppose  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ . Prove each of the following.

- (a) If  $f$  and  $g$  are both injective, then so is  $g \circ f$ .
- (b) If  $f$  and  $g$  are both surjective, then so is  $g \circ f$ .
- (c) If  $f$  and  $g$  are both bijections, then so is  $g \circ f$ .

**Exercise 3.10.** Consider the set  $X = \{0, 1\}$  consisting of two elements. List all of the bijections of  $X$ . Can you see any similarity here with Example 1.1?

Another important concept related to functions is that of pre-images or fibers, though the standard notation overloads the notation for function inverses.

**Definition 3.24.** For a function  $f : X \rightarrow Y$ , the *pre-image* or *fiber* of a point  $y \in Y$  is defined to be

$$f^{-1}(y) = \{x \in X : f(x) = y\}.$$

So a function is invertible if and only if every fiber consists of exactly one element of the domain.

**Sanity Check 3.11.** When  $f$  is invertible, what is the discrepancy between  $f^{-1}(y)$  used as the *inverse function value at  $y$*  and  $f^{-1}(y)$  used as the *fiber of  $f$  at  $y$* ?

### 3.4 Equivalence Relations

**Definition 3.25.** For a set  $X$ , a relation  $\simeq \subseteq X \times X$  is said to be an *equivalence relation* if the following three properties hold:

- (Reflexivity) For every  $x \in X$ ,  $x \simeq x$ .
- (Symmetry) For every  $x, y \in X$ , if  $x \simeq y$ , then  $y \simeq x$ .
- (Transitivity) For every  $x, y, z \in X$ , if both  $x \simeq y$  and  $y \simeq z$ , then  $x \simeq z$ .

In this case, we will often use the phrasing “ $\simeq$  is an equivalence relation *on  $X$* .”

The equality relation itself is an equivalence relation.

**Exercise 3.12.** Show that, if  $R \subseteq X \times X$  is an equivalence relation, then

- $R^{-1} = R$  and
- $R \circ R = R$ .

**Exercise 3.13.** Suppose  $f : X \rightarrow Y$  and define  $\simeq$  on  $X$  by the following rule:  $x \simeq y$  provided that  $f(x) = f(y)$ . Show that  $\simeq$  is an equivalence relation.

**Exercise 3.14.** Let  $X = \mathbb{Z} \times \mathbb{N}$  and define  $(k, m) \simeq (\ell, n)$  by

$$kn = \ell m.$$

Show that  $\simeq$  is an equivalence relation.<sup>8</sup>

**Definition 3.26.** Suppose  $\simeq$  is an equivalence relation on a set  $X$ . For  $x \in X$ , we define the  $\simeq$ -equivalence class (or simply called the *equivalence class* when there is no possibility for confusion) to be

$$[x]_{\simeq} = \{y \in X : x \simeq y\}.$$

When the equivalence relation  $\simeq$  is understood, we may suppress the subscript and refer to the equivalence class of  $x$  as  $[x]$ .

**Comment.** Using the notion of equivalence classes, we can formally define the rational numbers to be the set of equivalence classes of the  $\simeq$  relation defined in Exercise 3.14.

**Exercise 3.15.** Suppose  $\simeq$  if an equivalence relation on a set  $X$ . Show that, for any  $x, y \in X$ , either  $[x] = [y]$  or  $[x] \cap [y] = \emptyset$ .

**Example 3.27.** Let  $n \geq 2$ ,  $n \in \mathbb{Z}$ , and define, for  $p, q \in \mathbb{Z}$ ,  $p \equiv q \pmod{n}$  if there exists  $k \in \mathbb{Z}$  with  $p - q = nk$ . Then  $\cdot \equiv \cdot \pmod{n}$  is an equivalence relation.

*Proof.* For  $p \in \mathbb{Z}$ , note that  $p - p = 0 = n \cdot 0$ . Since  $0 \in \mathbb{Z}$ ,  $p \equiv p \pmod{n}$ .

For symmetry, suppose  $p \equiv q \pmod{n}$ . By definition, that means there is some  $k \in \mathbb{Z}$  for which  $p - q = nk$ . Note that  $q - p = -nk = n \cdot (-k)$ . Since  $-k \in \mathbb{Z}$ , we see that  $q \equiv p \pmod{n}$ .

Finally, for transitivity, suppose  $p \equiv q \pmod{n}$  and  $q \equiv r \pmod{n}$ . Then let  $k, \ell \in \mathbb{Z}$  be such that  $p - q = nk$  and  $q - r = n\ell$ . Observe that

$$\begin{aligned} p - r &= p - q + q - r \\ &= nk + n\ell \\ &= n(k + \ell). \end{aligned}$$

Since  $k + \ell \in \mathbb{Z}$ , we see that  $p \equiv r \pmod{n}$ , finishing the proof.  $\square$

For each  $n \geq 2$ ,  $n \in \mathbb{Z}$ , we define  $\mathbb{Z}_n$  to be the set of equivalence classes for the equivalence relation  $\cdot \equiv \cdot \pmod{n}$ . We will also use the notation  $k \% n$  to be the unique integer in the interval  $[0, n)$  such that  $k \equiv (k \% n) \pmod{n}$ .

**Exercise 3.16.** Consider  $\mathbb{Z}_2$ .

(a) Show that,

- for any even  $n \in \mathbb{Z}$ ,  $[n] = [0]$  and

---

<sup>8</sup>In fact, it is the standard notion of equivalence for rational numbers.

- for any odd  $n \in \mathbb{Z}$ ,  $[n] = [1]$ .

Conclude that  $\mathbb{Z}_2$  consists of exactly two elements.

- (b) Consider addition in  $\mathbb{Z}_2$  to be defined as  $[x] + [y] = [x + y]$ . Can you see any similarity here with Example 1.1?

Let  $\mathbb{Z}^{\mathbb{Z}}$  denote the set of all functions  $\mathbb{Z} \rightarrow \mathbb{Z}$ .<sup>9</sup> For each  $k \in \mathbb{Z}$ , consider the function  $g_k : \mathbb{Z} \rightarrow \mathbb{Z}$  defined by  $g_k(n) = n + k$ . Note that each  $g_k$  is a bijection and that  $g_0 = \text{id}_{\mathbb{Z}}$ . We can also see each  $g_k$  as a shifting of  $\mathbb{Z}$ . For example, if we envision  $\mathbb{Z}$  on a horizontal line ordered in increasing order,  $g_3$  has the effect of shifting all points over by three units to the right,  $g_0$  has the effect of doing nothing, and  $g_{-5}$  has the effect of shifting all points over by four units to the left.

Given the symbols above, we can define  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$  by  $\varphi(k) = g_k$ .<sup>10</sup> We will return to this idea later.

## 4 Introducing Groups

### 4.1 Getting to Know Groups

**Definition 4.1.** Let  $G$  be a set and  $\diamond : G \times G \rightarrow G$  be a function, also referred to as a *binary operation*. The set  $G$  with the binary operation  $\diamond$ ,  $(G, \diamond)$ , is said to be a *group* if the following properties hold:

- (Associativity) For any  $a, b, c \in G$ ,  $a \diamond (b \diamond c) = (a \diamond b) \diamond c$ .
- (Identity) There exists  $e \in G$  such that, for every  $g \in G$ ,  $g \diamond e = e \diamond g = g$ . Any such  $e \in G$  is referred to as the<sup>11</sup> *identity*.
- (Inverses) For any  $g \in G$ , there is some  $h \in G$  such that  $g \diamond h = h \diamond g = e$ , where  $e$  is the identity. As will be shown in Proposition 4.2, inverse elements are unique so we will use  $g^{-1}$  to denote the *inverse* of  $g$ .

**Sanity Check 4.1.** Suppose  $(G, \diamond)$  is a group. Why is the identity  $e \in G$  unique? (*Hint.* Suppose  $e_1, e_2 \in G$  satisfy the identity condition for the group. Show that  $e_1 = e_2$ .)

**Proposition 4.2.** In any group, the inverse of a given element of the group is unique.

*Proof.* Let  $(G, \diamond)$  be a group with identity  $e$ . Suppose  $g \in G$  and  $h_1, h_2 \in G$  are such that  $g \diamond h_1 = h_1 \diamond g = e$  and  $g \diamond h_2 = h_2 \diamond g = e$ . Observe that

$$\begin{aligned} h_1 &= h_1 \diamond e \\ &= h_1 \diamond (g \diamond h_2) \\ &= (h_1 \diamond g) \diamond h_2 \\ &= e \diamond h_2 \\ &= h_2. \end{aligned}$$

---

<sup>9</sup>There is a connection here with Cartesian products, but we won't get into those details now.

<sup>10</sup>Formally speaking,  $g$  is already a function from  $\mathbb{Z}$  to  $\mathbb{Z}^{\mathbb{Z}}$ .

<sup>11</sup>As will be shown in Sanity Check 4.1, there is only one element that satisfies the identity criterion.

Therefore,  $h_1 = h_2$ . □

A common practice in algebra is to use juxtaposition for the “multiplicative” operation of the group. In particular, we may say that  $(G, \cdot)$  is a group and let  $gh = g \cdot h$  for  $g, h \in G$ .

This convention also inspires “exponent” notation. For a group  $(G, \cdot)$ , we will consider  $g^0 = e$ , the identity, and  $g^1 = g$ . Then, for  $n \in \mathbb{N}$ , assuming  $g^n$  has been defined, we set  $g^{n+1} = g^n g$ . We also define  $g^{-n} = (g^n)^{-1}$ .

**Exercise 4.2.** Let  $(G, \cdot)$  be a group. Show that, for  $g \in G$ ,  $(g^{-1})^{-1} = g$ .

**Exercise 4.3.** Let  $(G, \cdot)$  be a group and define  $\varphi : G \rightarrow G$  by  $\varphi(g) = g^{-1}$ . Show that  $\varphi$  is a bijection.

**Exercise 4.4.** Let  $(G, \cdot)$  be a group and  $g, h \in G$ . Show that  $(gh)^{-1} = h^{-1}g^{-1}$ .

**Exercise 4.5 (Left- and Right-cancellation Laws).** Let  $(G, \cdot)$  be a group and  $a, g, h \in G$ . Show that

- $ag = ah \implies g = h$  and
- $ga = ha \implies g = h$ .

**Exercise 4.6.** Let  $(G, \cdot)$  be a group and  $g, h \in G$ . For  $n, m \in \mathbb{Z}$ , show that

- $g^n g^m = g^{n+m}$  and
- $(g^n)^m = g^{nm}$ .

**Exercise 4.7.** Let  $(G, \diamond)$  be a group and let  $p \in G$ . Define  $\varphi : G \rightarrow G$  by  $\varphi(g) = g \diamond p$ . Show that  $\varphi$  is a bijection and determine the inverse function of  $\varphi$ .

**Example 4.3.** The integers  $\mathbb{Z}$  with their usual binary operation of addition  $+$  forms a group.

**Definition 4.4.** If a group  $(G, \diamond)$  satisfies the property that  $g \diamond h = h \diamond g$  for all  $g, h \in G$ , then  $G$  is said to be *Abelian* or *commutative*.

Note that the integer group  $(\mathbb{Z}, +)$  is Abelian.

**Exercise 4.8.** Suppose  $(G, \cdot)$  is an Abelian group. Show that, for any  $g, h \in G$  and  $n \in \mathbb{Z}$ ,  $(gh)^n = g^n h^n$ .

**Example 4.5.** Let  $\text{Sym}(\mathbb{R})$  consist of all bijections  $\mathbb{R} \rightarrow \mathbb{R}$ . With the operation of function composition  $\circ$ ,  $(\text{Sym}(\mathbb{R}), \circ)$  is a group with identity  $\text{id}_{\mathbb{R}}$ . By Example 3.23, this group is not commutative.

**Example 4.6.** Let  $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ . Then  $(\mathbb{R}^+, \cdot)$ , where  $\cdot$  is the standard multiplication operation, is an Abelian group with identity 1.

Note that Examples 4.5 and 4.6 can justify the overloading of the  $\cdot^{-1}$  operator seen in, for example, Calculus courses. In some cases, it is used to refer to the functional inverse, and in other cases, it is used to refer to the multiplicative inverse.

**Exercise 4.9.** Show that  $(\mathbb{R}, \cdot)$ , where  $\cdot$  is multiplication, is not a group.

**Exercise 4.10.** Is  $(\mathbb{N}, \cdot)$  a group? Why or why not?

**Example 4.7.** Expanding on Exercise 3.16, let  $n \geq 2$ ,  $n \in \mathbb{Z}$ , and define  $\oplus : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  by the rule

$$[x] \oplus [y] = [x + y].$$

Then  $(\mathbb{Z}_n, \oplus)$  is an Abelian group with identity  $[0]$ . As is common, we can identify each  $[x]$  with the unique  $0 \leq y < n$  for which  $x \equiv y \pmod{n}$ . In Figure 1, we provide the particular *Cayley table* for each of the groups  $\mathbb{Z}_2$ ,  $\mathbb{Z}_3$ , and  $\mathbb{Z}_5$ , with the identifications specified above.

$\oplus$	0	1	$\oplus$	0	1	2	$\oplus$	0	1	2	3	4
0	0	1	0	0	1	2	0	0	1	2	3	4
1	1	0	1	1	2	0	1	1	2	3	4	0
			2	2	0	1	2	2	3	4	0	1
							3	3	4	0	1	2
							4	4	0	1	2	3

Figure 1: Cayley tables for  $(\mathbb{Z}_2, \oplus)$ ,  $(\mathbb{Z}_3, \oplus)$ , and  $(\mathbb{Z}_5, \oplus)$ , respectively.

**Example 4.8.** For  $n \geq 2$ ,  $n \in \mathbb{Z}$ , define  $* : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  by the rule

$$[x] * [y] = [x \cdot y].$$

In Figure 2, we consider two Cayley tables for this operation in the contexts  $n = 5, 6$ .

$*$	0	1	2	3	4	$*$	0	1	2	3	4	5
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	1	0	1	2	3	4	5
2	0	2	4	1	3	2	0	2	4	0	2	4
3	0	3	1	4	2	3	0	3	0	3	0	3
4	0	4	3	2	1	4	0	4	2	0	4	2
						5	0	5	4	3	2	1

Figure 2: Cayley tables for  $(\mathbb{Z}_5, *)$  and  $(\mathbb{Z}_6, *)$ , respectively.

Ignoring the zero rows and columns, we obtain the tables in Figure 3, highlighting zero entries in red. Note that  $(\mathbb{Z}_5 \setminus \{0\}, *)$  forms a group but  $(\mathbb{Z}_6 \setminus \{0\}, *)$  does not.

*	1	2	3	4		*	1	2	3	4	5
1	1	2	3	4		1	1	2	3	4	5
2	2	4	1	3		2	2	4	0	2	4
3	3	1	4	2		3	3	0	3	0	3
4	4	3	2	1		4	4	2	0	4	2
5	5	4	3	2		5	5	4	3	2	1

Figure 3: Cayley tables for  $(\mathbb{Z}_5 \setminus \{0\}, *)$  and  $(\mathbb{Z}_6 \setminus \{0\}, *)$ , respectively.

In fact, if we let  $\mathbb{Z}_n^+ = \mathbb{Z}_n \setminus \{0\}$ , then  $(\mathbb{Z}_n^+, *)$  is a group if and only if  $n$  is prime. Recall that an integer  $n \geq 2$  is said to be *composite* if there are integers  $2 \leq a, b < n$  such that  $ab = n$ . If the integer  $n \geq 2$  is not composite, it is *prime*.

Recall the standard notation of divisibility: if  $n \in \mathbb{Z}$  and  $d \in \mathbb{N}$ , we write  $d | n$  if there is an integer  $k$  such that  $n = dk$ .

A fact that we will use here without proof is

**Theorem 4.9** (The Fundamental Theorem of Arithmetic). Every integer greater than 1 has a unique prime factorization.

Using The Fundamental Theorem of Arithmentic, one can prove

**Lemma 4.10** (“Euclid’s Lemma”). If a prime  $p$  divides a product  $ab$ , then either  $p | a$  or  $p | b$ .

Note that, by mathematical induction, Euclid’s Lemma can be extended to the following assertion:

If a prime  $p$  divides a product  $a_1a_2 \cdots a_n$ , then  $p | a_j$  for some  $j \in \{1, 2, \dots, n\}$ .

The following lemma can be seen as a rephrasing of Euclid’s Lemma.

**Lemma 4.11.** If  $p$  is a prime number, then, for integers  $0 \leq a, b < p$ , if  $ab \equiv 0 \pmod{p}$ , then either  $a = 0$  or  $b = 0$ .

**Theorem 4.12.** Let  $p \geq 2$ ,  $p \in \mathbb{Z}$ , and consider  $\mathbb{Z}_p^+$  with the operation  $*$  defined in Example 4.8. Then  $(\mathbb{Z}_p^+, *)$  is a group if and only if  $p$  is prime.

*Proof.* First note that, if  $p$  is composite, then we can write  $p = ab$  for some  $2 \leq a, b < p$ . Note then that  $ab \equiv 0 \pmod{p}$  and so  $\mathbb{Z}_p^+$  is not closed under the operation  $*$ . Consequently,  $(\mathbb{Z}_p^+, *)$  is not a group.

Now suppose  $p$  is prime. By Lemma 4.11,  $\mathbb{Z}_p^+$  is closed under  $*$ . We also know that 1 satisfies the identity criterion and that multiplication is associative. So the only thing to show is that every element of  $\mathbb{Z}_p^+$  has an inverse. So consider  $2 \leq n < p$  and the set  $\{n^k : k \in \mathbb{N}\}$ . Note that  $\{n^k : k \in \mathbb{N}\}$  is an infinite subset of natural numbers. However,

since  $\mathbb{Z}_p^+$  is finite,  $\{n^k \pmod p : k \in \mathbb{N}\}$  is also finite. Consequently, there must be some  $j, k \in \mathbb{N}$ ,  $j < k$ , such that  $n^j \equiv n^k \pmod p$ . It follows that

$$p \mid n^j - n^k = n^j(1 - n^{k-j}).$$

Since  $p \nmid n$ , it must be the case that  $p \mid 1 - n^{k-j}$ , which is equivalent to  $n^{k-j} \equiv 1 \pmod p$ . Since  $2 \leq n < p$ , we must have that  $k-j > 1$ . Hence,  $n \cdot n^{k-j-1} \equiv 1 \pmod p$ . Therefore,  $n$  has a multiplicative inverse.  $\square$

We are now equipped to prove

**Theorem 4.13** (Wilson's Theorem). An integer  $p > 1$  is prime if and only if

$$(p-1)! \equiv -1 \pmod p$$

where  $x!$  is the factorial of  $x$ . Equivalently, the integer  $p > 1$  is prime if and only if

$$\frac{(p-1)! + 1}{p}$$

is an integer.

*Proof.* <sup>12</sup> First, suppose  $p$  is composite. We proceed here by cases.

First, suppose  $p > 4$ . Then we write  $p = ab$  where  $2 \leq a, b < p$ . Since  $p > 4$ , we can assume without loss of generality that  $a \geq 3$ . Note now that  $2 \leq a-1$  and  $1 \leq b-1$ , and, thus,

$$2 \leq (a-1)(b-1) = ab - a - b + 1 \implies a + b \leq ab - 1 = p - 1.$$

It follows that

$$(p-1)! = 1 \cdot 2 \cdots a(a+1) \cdots (a+b) \cdots (ab-1).$$

In particular, there is an integer  $m$  for which

$$(p-1)! = a(a+1) \cdots (a+b)m.$$

Note that

$$b \mid (a+1)(a+2) \cdots (a+b)$$

since the right-hand expression is the product of  $b$  consecutive integers. Hence, there is an integer  $k$  for which

$$(a+1)(a+2) \cdots (a+b) = bk.$$

We can thus rewrite our equation above as

$$(p-1)! = abkm = pkm.$$

It follows that  $(p-1)! \equiv 0 \pmod p$ .

In the case that  $p = 4$ , note that  $3! = 6 \equiv 2 \pmod 4$ . Since  $2 \not\equiv -1 \pmod 4$ , we have finished this direction of the proof.

---

<sup>12</sup>This proof is adapted from comments appearing in [math.se/307](#) and [math.se/164852](#).

Finally, suppose  $p$  is prime. In this portion of the proof, we wish to show that the product  $(p - 1)!$  consists of two types of elemental products, one of which produces a factor of  $-1$  and the other producing a factor of  $1$ . So consider

$$P = \{(n, m) \in \mathbb{Z}_p^+ \times \mathbb{Z}_p^+ : n \leq m \wedge nm \equiv 1 \pmod{p}\}.$$

Since, by Theorem 4.12,  $(\mathbb{Z}_p^+, *)$  is a group, we have that, for every  $x \in \mathbb{Z}_p^+$  there is some  $y \in \mathbb{Z}_p^+$  such that either  $(x, y) \in P$  or  $(y, x) \in P$ .

We now consider

$$H = \{n \in \mathbb{Z}_p^+ : \exists m \in \mathbb{Z}_p^+ (n, m) \in P\}.$$

By the uniqueness of inverses, we know that  $n \mapsto n^{-1}$ ,  $H \rightarrow \mathbb{Z}_p^+$ , is an injective function. Also, by the property mentioned above, note that, for any  $x \in \mathbb{Z}_p^+ \setminus H$ , there is some  $y \in H$  such that  $x = y^{-1}$ .

We now split  $H$  into two disjoint subsets:

$$H_{id} = \{n \in H : n = n^{-1}\} \text{ and } H_\star = \{n \in H : n \neq n^{-1}\}.$$

We start by showing that  $H_{id} = \{[1], [-1]\}$ . So let  $n \in H_{id}$  and note that  $n = n^{-1}$  is equivalent to  $n^2 \equiv 1 \pmod{p}$ . It follows that

$$p \mid n^2 - 1 = (n + 1)(n - 1) \implies p \mid n + 1 \vee p \mid n - 1.$$

Hence, if  $n^2 \equiv 1 \pmod{p}$ , then either  $n \equiv 1 \pmod{p}$  or  $n \equiv -1 \pmod{p}$ . This establishes that  $H_{id} \subseteq \{[1], [-1]\}$ . For equality, simply note that  $p - 1 \equiv -1 \pmod{p}$  and that  $(-1)^2 = 1$ .

Finally, enumerate  $H_\star = \{a_1, \dots, a_k\}$  and note that

$$(p - 1)! = (p - 1)a_1a_1^{-1}a_2a_2^{-1} \cdots a_k a_k^{-1} \equiv -1 \pmod{p}.$$

This finishes the proof. □

**Example 4.14.** Let  $\mathbb{F}$  be either  $\mathbb{R}$  or  $\mathbb{C}$ . Then define

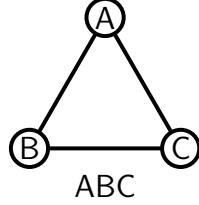
$$\mathrm{GL}(2, \mathbb{F}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0 \right\}$$

and

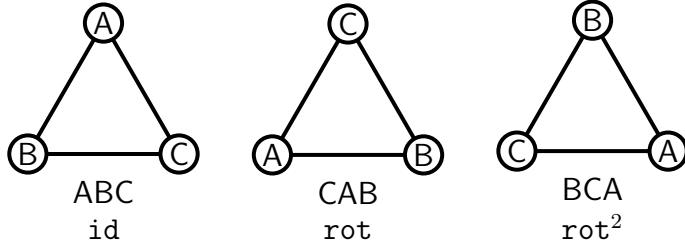
$$\mathrm{SL}(2, \mathbb{F}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1 \right\}.$$

With the operation of matrix multiplication, both  $\mathrm{GL}(2, \mathbb{F})$  and  $\mathrm{SL}(2, \mathbb{F})$  are non-Abelian groups.  $\mathrm{GL}(2, \mathbb{F})$  is referred to as the *general linear group* and  $\mathrm{SL}(2, \mathbb{F})$  is referred to as the *special linear group*.

**Example 4.15.** Consider the symmetries of an equilateral triangle with labeled vertices and code each state of the triangle with a word where the first letter corresponds to the top vertex, the second letter corresponds to the bottom left vertex, and the third letter corresponds to the bottom right vertex:

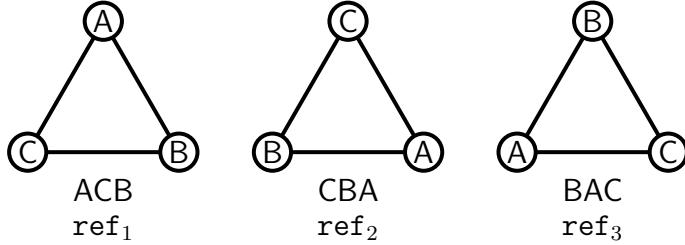


Let  $\text{id}$  represent the null action and let  $\text{rot}$  denote a counterclockwise rotation. We use juxtaposition to indicate actions done in succession, so the orbit of  $\text{rot}$  looks like this:



Note here<sup>13</sup> that  $\text{rot}^{-1} = \text{rot}^2$  and that  $\text{rot}^3 = \text{id}$ .

We also identify three possible reflections:



It is clear that  $\text{ref}_j^2 = \text{id}$  for  $j = 1, 2, 3$ .

Now, for any two action  $a$  and  $b$  listed above, let  $a \cdot b$  represent the action obtained by first applying  $a$  and then applying  $b$ . It can then be verified that

$$\text{rot} \cdot \text{ref}_1 = \text{ref}_2 \quad \text{rot} \cdot \text{ref}_2 = \text{ref}_3 \quad \text{rot} \cdot \text{ref}_3 = \text{ref}_1$$

$$\text{rot}^2 \cdot \text{ref}_1 = \text{ref}_3 \quad \text{rot}^2 \cdot \text{ref}_2 = \text{ref}_1 \quad \text{rot}^2 \cdot \text{ref}_3 = \text{ref}_2$$

It can be verified directly as above, or by applying Exercise 4.4 to the equations above, that

$$\text{ref}_1 \cdot \text{rot} = \text{ref}_3 \quad \text{ref}_2 \cdot \text{rot} = \text{ref}_1 \quad \text{ref}_3 \cdot \text{rot} = \text{ref}_2$$

$$\text{ref}_1 \cdot \text{rot}^2 = \text{ref}_2 \quad \text{ref}_2 \cdot \text{rot}^2 = \text{ref}_3 \quad \text{ref}_3 \cdot \text{rot}^2 = \text{ref}_1$$

Let<sup>14</sup>

$$S_3 = \{\text{id}, \text{rot}, \text{rot}^{-1}, \text{ref}_1, \text{ref}_2, \text{ref}_3\}.$$

---

<sup>13</sup>One clockwise rotation undoes one counter-clockwise rotation.

<sup>14</sup>More on the choice of notation later.

Then  $(S_3, \cdot)$  is a non-Abelian group and its corresponding Cayley table is:

.	id	rot	$\text{rot}^{-1}$	$\text{ref}_1$	$\text{ref}_2$	$\text{ref}_3$
id	id	rot	$\text{rot}^{-1}$	$\text{ref}_1$	$\text{ref}_2$	$\text{ref}_3$
rot	rot	$\text{rot}^{-1}$	id	$\text{ref}_2$	$\text{ref}_3$	$\text{ref}_1$
$\text{rot}^{-1}$	$\text{rot}^{-1}$	id	rot	$\text{ref}_3$	$\text{ref}_1$	$\text{ref}_2$
$\text{ref}_1$	$\text{ref}_1$	$\text{ref}_3$	$\text{ref}_2$	id	$\text{rot}^{-1}$	rot
$\text{ref}_2$	$\text{ref}_2$	$\text{ref}_1$	$\text{ref}_3$	rot	id	$\text{rot}^{-1}$
$\text{ref}_3$	$\text{ref}_3$	$\text{ref}_2$	$\text{ref}_1$	$\text{rot}^{-1}$	rot	id

**Comment.** Note that every element of  $S_3$  in Example 4.15 codes a bijection of a given set of three elements. In fact,  $(S_3, \cdot)$  is exactly the group of bijections on the set  $\{A, B, C\}$  under function composition.

Another thing to note here is that a copy of  $(\mathbb{Z}_3, \oplus)$  lives inside of  $S_3$ ; indeed,

$$(\{\text{id}, \text{rot}, \text{rot}^{-1}\}, \cdot)$$

can be verified to be a copy of  $(\mathbb{Z}_3, \oplus)$ .

**Exercise 4.11.** Let  $X$  be a non-empty set and, for  $A, B \subseteq X$ , define the *symmetric difference* between  $A$  and  $B$  to be

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Let  $\wp(X)$  be the set of all subsets of  $X$ . Show that  $(\wp(X), \Delta)$  is an Abelian group.

## 4.2 Subgroups

**Definition 4.16.** For a group  $(G, \cdot)$ , we say that  $H \subseteq G$  is a *subgroup* of  $G$  if  $(H, \cdot)$  is a group. The singleton set consisting of the identity element is a subgroup of any given group, and is referred to as the *trivial subgroup*. If  $H$  is a proper subset of  $G$  and is a subgroup of  $G$ , we say that  $H$  is a *proper subgroup* of  $G$ .

**Example 4.17.** The integer group  $(\mathbb{Z}, +)$  is a (proper) subgroup of  $(\mathbb{R}, +)$ .

Since the associativity of the operation is inherited, to determine whether a subset of a group is a subgroup, it suffices to check that the subset contains the group identity and is *closed* under the group operations.

**Proposition 4.18.** Suppose  $(G, \cdot)$  is a group and  $H \subseteq G$ . Then  $H$  is a subgroup of  $G$  if and only if the following three conditions are satisfied:

- $e \in H$ .
- For  $g, h \in H$ ,  $gh \in H$ .
- For  $h \in H$ ,  $h^{-1} \in H$ .

In fact, there is a single condition to check that verifies whether a subset is a subgroup.

**Proposition 4.19.** Let  $(G, \cdot)$  be a group and  $H \subseteq G$ . Then  $H$  is a subgroup of  $G$  if and only if  $H \neq \emptyset$  and, for  $g, h \in H$ ,  $gh^{-1} \in H$ .

*Proof.* First, note that, if  $H$  is a subgroup,  $e \in H$  so  $H \neq \emptyset$ . Then, for  $g, h \in H$ ,  $h^{-1} \in H$  and so  $gh^{-1} \in H$ .

For the reverse direction, we verify the conditions of Proposition 4.18. Since  $H \neq \emptyset$  there is some  $x \in H$ . By the hypothesis,  $xx^{-1} = e \in H$ .

Now, for any  $y \in H$ , since  $e \in H$ ,  $ey^{-1} = y^{-1} \in H$ .

Finally, consider  $g, h \in H$ . From Exercise 4.2, we know that  $h = (h^{-1})^{-1}$ . From the argument above, we also know that  $h^{-1} \in H$ . Hence, by the hypothesis, we have that

$$gh = g(h^{-1})^{-1} \in H,$$

finishing the proof.  $\square$

**Exercise 4.12.** Let  $\mathbb{F}$  be  $\mathbb{R}$  or  $\mathbb{C}$ . Show that, as defined in Example 4.14,  $\mathrm{SL}(2, \mathbb{F})$  is a subgroup of  $\mathrm{GL}(2, \mathbb{F})$ . (*Hint.* There is an important property about determinants that can be helpful here.)

**Example 4.20.** The subgroups of  $(\mathbb{Z}_4, \oplus)$  are  $\{0\}$ ,  $\{0, 2\}$ , and  $\mathbb{Z}_4$ . It is straightforward to verify that each three of these are subgroups of  $\mathbb{Z}_4$ . To see that they are the only ones, suppose you have a subgroup  $H$ . It will suffice to show that, if  $1 \in H$ , then  $H = \mathbb{Z}_4$ . Indeed, note that  $-1 \equiv 3 \pmod{4}$  so  $3 \in H$ . Moreover,  $1 + 1 = 2 \in H$ .

**Exercise 4.13.** Let  $(G, \cdot)$  be a group and  $\mathcal{H}$  be a set of subgroups of  $G$ . Show that  $\bigcap \mathcal{H}$  is a subgroup of  $G$ .

**Exercise 4.14.** Provide a counterexample to the following statement: Let  $(G, \cdot)$  be a group and suppose that  $H_1$  and  $H_2$  are subgroups of  $G$ . Then  $H_1 \cup H_2$  is a subgroup of  $G$ .

### 4.3 An Introduction to Homomorphisms

**Definition 4.21.** Suppose  $(G, \diamond)$  and  $(H, \bullet)$  are groups. A function  $\varphi : G \rightarrow H$  is said to be a *homomorphism* if, for all  $g, h \in G$ ,

$$\varphi(g \diamond h) = \varphi(g) \bullet \varphi(h).$$

**Example 4.22.** Consider the groups  $(\mathbb{R}, +)$  and  $(\mathbb{R}^+, \cdot)$ , where  $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ . Define  $\varphi : \mathbb{R} \rightarrow \mathbb{R}^+$  by the rule  $\varphi(x) = 2^x$ . Then  $\varphi$  is a homomorphism. Indeed, check that

$$\begin{aligned} \varphi(x + y) &= 2^{x+y} \\ &= 2^x \cdot 2^y \\ &= \varphi(x) \cdot \varphi(y). \end{aligned}$$

**Exercise 4.15.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Let  $e_G$  be the identity element of  $G$  and  $e_H$  be the identity element of  $H$ . Prove that  $\varphi(e_G) = e_H$ . (*Hint.* First establish that  $\varphi(g) \bullet \varphi(e_G) = \varphi(g)$  for any  $g \in G$ .)

**Exercise 4.16.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Show that, for any  $g \in G$ ,  $\varphi(g^{-1}) = \varphi(g)^{-1}$ .

**Exercise 4.17.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism between multiplicative groups  $G$  and  $H$ . Show that, for any positive integer  $n$ ,  $\varphi(g^n) = \varphi(g)^n$ .

**Definition 4.23.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Let  $e_H$  be the identity element of  $H$ . We define the *kernel* of  $\varphi$  to be

$$\ker(\varphi) = \varphi^{-1}(e_H) = \{g \in G : \varphi(g) = e_H\}.$$

**Exercise 4.18.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Prove that  $\ker(\varphi)$  is a subgroup of  $G$ .

**Proposition 4.24.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Suppose  $E$  is a subgroup of  $G$ . Then

$$\varphi[E] = \{\varphi(g) : g \in E\}$$

is a subgroup of  $H$ .

*Proof.* To prove the proposition, we will apply Proposition 4.19.

Since  $E$  is a subgroup of  $G$ ,  $e_G \in E$ . Then, by Exercise 4.15,  $\varphi(e_G) = e_H \in \varphi[E]$ . Hence,  $\varphi[E] \neq \emptyset$ .

To finish the proof, suppose  $h_1, h_2 \in \varphi[E]$ . By definition, there are  $g_1, g_2 \in E$  such that  $\varphi(g_1) = h_1$  and  $\varphi(g_2) = h_2$ . Since  $E$  is a subgroup of  $G$  and  $g_1, g_2 \in E$ , we see that  $g_1 \diamond g_2^{-1} \in E$ . By the corresponding application of Exercise 4.16, we see that

$$\begin{aligned}\varphi(g_1 \diamond g_2^{-1}) &= \varphi(g_1) \bullet \varphi(g_2^{-1}) \\ &= \varphi(g_1) \bullet \varphi(g_2)^{-1} \\ &= h_1 \bullet h_2^{-1}.\end{aligned}$$

Again, as  $g_1 \diamond g_2^{-1} \in E$ , we see that

$$h_1 \bullet h_2^{-1} = \varphi(g_1 \diamond g_2^{-1}) \in \varphi[E].$$

Conclusively, Proposition 4.19 applies, and  $\varphi[E]$  is a subgroup of  $H$ . □

**Exercise 4.19.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Suppose  $E$  is a subgroup of  $H$ . Show that

$$\varphi^{-1}(E) = \{g \in G : \varphi(g) \in E\}$$

is a subgroup of  $G$ .

**Exercise 4.20.** Suppose  $(G, \diamond)$ ,  $(H, \bullet)$ , and  $(K, *)$  are groups and that  $\varphi : G \rightarrow H$  and  $\psi : H \rightarrow K$  are homomorphisms. Show that  $\psi \circ \varphi$  is a homomorphism.

**Definition 4.25.** Suppose  $(G, \diamond)$  and  $(H, \bullet)$  are groups. A bijection  $\varphi : G \rightarrow H$  is said to be an *isomorphism* if  $\varphi$  is a homomorphism and its inverse  $\varphi^{-1}$  is also a homomorphism. In such a case, we say that  $(G, \diamond)$  and  $(H, \bullet)$  are *isomorphic*, which is denoted by  $G \cong H$ .

In fact, the algebraic structure necessitates that any bijective homomorphism be an isomorphism.

**Exercise 4.21.** Suppose  $\varphi : G \rightarrow H$  is a bijective homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Show that  $\varphi^{-1}$  is necessarily a homomorphism.

Whether or not a homomorphism is injective depends completely on its kernel.

**Exercise 4.22.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism from the group  $(G, \diamond)$  to the group  $(H, \bullet)$ . Show that  $\varphi$  is injective if and only if its kernel is the trivial subgroup of  $G$ .

**Exercise 4.23.** Let  $R = \{\text{id}, \text{rot}, \text{rot}^{-1}\}$ , as in the context of Example 4.15.

(a) Show that  $R$  is a subgroup of  $S_3$ .

(b) Show that  $(R, \cdot)$  and  $(\mathbb{Z}_3, \oplus)$  are isomorphic.

**Example 4.26.** Let  $G = \mathbb{Z}_2 \times \mathbb{Z}_2$  and define  $+$  by  $(a, b) + (c, d) = (a \oplus c, b \oplus d)$ .<sup>15</sup> Note that

$$G = \{(0, 0), (0, 1), (1, 0), (1, 1)\},$$

so  $G$  consists of four distinct elements. We argue here that  $G$  and  $\mathbb{Z}_4$  are not isomorphic.

Note that every element of  $G$  is its own inverse. However, in  $\mathbb{Z}_4$ , the inverse of 1 is 3. So  $G$  and  $\mathbb{Z}_4$  are not isomorphic.

**Exercise 4.24.** For the group  $G$  defined in Example 4.26, show that  $G$  has exactly 5 subgroups.

Homomorphisms also preserve algebraic properties, like that of being Abelian.

**Proposition 4.27.** Suppose  $(G, \diamond)$  and  $(H, \bullet)$  are groups and that  $\varphi : G \rightarrow H$  is a surjective homomorphism. If  $G$  is Abelian, then  $H$  is Abelian.

*Proof.* Let  $h_1, h_2 \in H$  be arbitrary. Since  $\varphi$  is surjective, there are  $g_1, g_2 \in G$  for which  $\varphi(g_1) = h_1$  and  $\varphi(g_2) = h_2$ . Note then that

$$h_1 \bullet h_2 = \varphi(g_1) \bullet \varphi(g_2) = \varphi(g_1 \diamond g_2) = \varphi(g_2 \diamond g_1) = \varphi(g_2) \bullet \varphi(g_1) = h_2 \bullet h_1.$$

Therefore,  $H$  is Abelian. □

Since the trivial mapping  $\varphi : G \rightarrow \{1\}$  defined by  $\varphi(x) = 1$  is a homomorphism from any group to the trivial group, the reverse direction to Proposition 4.27 does not necessarily hold.

---

<sup>15</sup>This, as we will elaborate on later, is known as a *direct product*.

## 4.4 Cyclic Groups and Subgroups

The groups  $(\mathbb{Z}, +)$  and  $(\mathbb{Z}_n, \oplus)$ , where  $n \in \mathbb{N}$ , are examples of what we call *cyclic groups* since they can be seen as *generated* by a single non-identity element. In these cases, the element 1 can be seen as the generating element.

**Definition 4.28.** For a group  $(G, \cdot)$  and  $a \in G$ , let  $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ . We will refer to  $\langle a \rangle$  as a *cyclic subgroup* of  $G$ , and we will say that  $a$  is the *generator* of  $\langle a \rangle$ .

If  $G = \langle a \rangle$  for some  $a \in G$ , we say that  $G$  is a *cyclic group*.

**Theorem 4.29.** Let  $(G, \cdot)$  be a group and  $a \in G$ . Then  $\langle a \rangle$  is a subgroup of  $G$  and, furthermore,  $\langle a \rangle$  is the smallest (with respect to subset inclusion) subgroup of  $G$  which contains  $a$ .

Based on Exercise 4.13, letting  $\mathcal{H}_a$  be the set of all subgroups of a group  $(G, \cdot)$  containing  $a \in G$ , we can see that

$$\langle a \rangle = \bigcap \mathcal{H}_a.$$

**Exercise 4.25.** Let  $(G, \cdot)$  be a group with no proper nontrivial subgroups. Show that  $G$  is necessarily cyclic.

We will record the following basic observation here for use later.

**Lemma 4.30.** In a group  $(G, \cdot)$ , given  $a, b \in G$ , if there is some  $k \in \mathbb{Z}$  for which  $b = a^k$ , then  $\langle b \rangle \subseteq \langle a \rangle$ .

*Proof.* Suppose that  $a, b \in G$  and  $k \in \mathbb{Z}$  are as in the hypothesis. We show that  $\langle b \rangle \subseteq \langle a \rangle$ . So let  $x \in \langle b \rangle$ , which means that  $x = b^m$  for some  $m \in \mathbb{Z}$ . Note then that

$$x = b^m = (a^k)^m = a^{km} \in \langle a \rangle.$$

Since  $x \in \langle b \rangle$  was arbitrary, we see that  $\langle b \rangle \subseteq \langle a \rangle$ . □

**Exercise 4.26.** Let  $(G, \cdot)$  be a group and  $a \in G$ . Show that the mapping  $k \mapsto a^k$ ,  $\mathbb{Z} \rightarrow G$ , is a homomorphism from the group  $(\mathbb{Z}, +)$  to  $(G, \cdot)$ .

Conclude that every cyclic subgroup of a given group is a homomorphic image of  $(\mathbb{Z}, +)$ .

It follows immediately that homomorphisms preserve the algebraic property of being cyclic.

**Proposition 4.31.** Suppose  $(G, \diamond)$  and  $(H, \bullet)$  are groups and that  $\varphi : G \rightarrow H$  is a surjective homomorphism. If  $G$  is cyclic, then  $H$  is cyclic.

*Proof.* By Exercise 4.26, there exists a surjective homomorphism  $\psi : \mathbb{Z} \rightarrow G$ . Then, by Exercise 4.20,  $\varphi \circ \psi : \mathbb{Z} \rightarrow H$  is a surjective homomorphism. It follows that  $H$  is cyclic with generator  $\varphi \circ \psi(1)$ . □

Since  $(\mathbb{Z}, +)$  is Abelian, we can use Proposition 4.27 to conclude that:

**Theorem 4.32.** Every cyclic group is Abelian.

As the contrapositive of Theorem 4.32, if a group is non-Abelian, then it is not cyclic. For example,  $\mathrm{GL}(2, \mathbb{R})$  is not cyclic since it is non-Abelian.

**Theorem 4.33.** Every non-trivial subgroup of  $(\mathbb{Z}, +)$  is of the form  $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$  for some  $n \in \mathbb{N}$ .

*Proof.* It is straight-forward to verify that  $n\mathbb{Z}$ ,  $n \in \mathbb{N}$ , is a subgroup of  $(\mathbb{Z}, +)$ . So we need only show these are the only subgroups. Let  $H$  be a non-trivial subgroup of  $(\mathbb{Z}, +)$ . Since  $H$  is non-trivial, it must contain some  $k \neq 0$ . Moreover, as  $H$  is a subgroup,  $-k \in H$ . Since either  $k$  or  $-k$  is positive,  $H$  contains at least one positive element. Let  $m$  be the smallest positive integer in  $H$ . Evidently,  $m\mathbb{Z} \subseteq H$ .

To finish the proof, we show that  $H \subseteq m\mathbb{Z}$ . So suppose  $h \in H$ . Since  $h \in \mathbb{Z}$  and  $m$  is a positive integer, we can write  $h = mq + r$  where  $0 \leq r < m$ . Note that  $mq \in m\mathbb{Z} \subseteq H$ , and so  $h - mq = r \in H$ . Since  $0 \leq r < m$  and  $m$  was set to be the smallest positive element of  $H$ ,  $r = 0$ . That is,  $h = mq \in m\mathbb{Z}$ .  $\square$

**Corollary 4.34.** Every subgroup of a cyclic group is cyclic.

Some cyclic groups, like  $(\mathbb{Z}, +)$  itself, are infinite. Others, like  $(\mathbb{Z}_n, \oplus)$ ,  $n \in \mathbb{N}$ , are finite. In  $\mathbb{Z}_6$ , note that the “powers” of 2 forms the sequence  $(2, 4, 0, 2, 4, 0, \dots)$ . Similarly, note that the “powers” of 5 forms the sequence  $(5, 4, 3, 2, 1, 0, 5, 4, 3, 2, 1, 0, \dots)$ . In both (cycling) sequences, we reach the identity. In the case of 2, we reach the identity as the third iterate. In the case of 5, we reach the identity as the sixth iterate.

**Definition 4.35.** Let  $(G, \cdot)$  be a group. For  $a \in G$ , we define the *order* of  $a$ , denoted by  $\mathrm{ord}(a)$ , to be the least positive integer  $n$  such that  $a^n = e_G$ , if any such integer exists. Otherwise, we say that the order of  $a$  is infinite.

In the example involving  $\mathbb{Z}_6$  above, we see that the element 2 has order 3 and that the element 5 has order 6.

**Lemma 4.36.** Let  $(G, \cdot)$  be a group and suppose  $a \in G$  is such that  $a \neq e_G$ . If  $a^n = e_G$  for a positive integer  $n$ , then the order of  $a$  divides  $n$ .

*Proof.* Let  $d = \mathrm{ord}(a)$  and suppose that  $a^n = e_G$ . By the definition of the order,  $d \leq n$  and, by the division algorithm, we can write  $n = dq + r$  where  $q$  and  $r$  are integers with  $0 \leq r < d$ . Note then that

$$e_G = a^n = a^{dq+r} = (a^d)^q a^r = a^r.$$

Since  $r < d$  and  $a^r = e_G$ , it must be the case that  $r = 0$ . Hence,  $n = dq$ , which establishes that  $d$  divides  $n$ .  $\square$

The word *order* is also overloaded with the following definition, but the dependence on context should avoid potential confusion.

**Definition 4.37.** Let  $(G, \cdot)$  be a group. If  $G$  is finite, we use the *order* of  $G$  to mean the cardinality of  $G$ . When  $G$  is infinite, we say that the *order* of  $G$  is infinite.

**Remark.** Note here that the order of an element  $g \in G$  corresponds to the order of the corresponding cyclic subgroup  $\langle g \rangle$ .

As some quick examples, the trivial group consisting of the identity element has order 1, the group  $(\mathbb{Z}_7, \oplus)$  has order 7, and the group  $(\mathbb{Z}, +)$  has infinite order.

**Exercise 4.27.** Suppose  $(G, \cdot)$  is a cyclic group of order  $n$ . Show that  $G$  is isomorphic to  $(\mathbb{Z}_n, +)$ .

In the context of  $\mathbb{Z}_n$ , we can capture the order of any element in terms of its gcd with  $n$ . To accomplish this, we will use the following fact without proof.

**Theorem 4.38** (Bézout's Identity). Let  $a$  and  $b$  be integers. Then there exist integers  $x$  and  $y$  such that

$$ax + by = \gcd(a, b).$$

More generally, given integers  $a_1, a_2, \dots, a_n$ , there are integers  $x_1, x_2, \dots, x_n$  such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \gcd(a_1, a_2, \dots, a_n).$$

Toward our goal of characterizing the order of elements in  $\mathbb{Z}_n$ , we start with a basic observation regarding divisors of  $n$ .

**Lemma 4.39.** If  $a \in \mathbb{Z}_n$  is such that  $a$  divides  $n$ , then  $\text{ord}(a) = \frac{n}{a}$ .

*Proof.* If  $a$  divides  $n$ , then there is an integer  $k$  for which  $ak = n$ . Since  $0 < a < n$  and  $n > 0$ , we see that  $k$  must be positive. Note that, for any  $\ell$  with  $0 < \ell < k$ ,  $a\ell < ak = n$ . So  $k$  is indeed the least positive integer for which  $ak \equiv 0 \pmod{n}$ . Since  $k = \frac{n}{a}$ , we see that  $\text{ord}(a) = \frac{n}{a}$ .  $\square$

**Lemma 4.40.** For any  $a \in \mathbb{Z}_n$ , where  $n > 1$  and  $a > 0$ ,  $\langle a \rangle = \langle \gcd(a, n) \rangle$ .

*Proof.* First, note that  $a = \gcd(a, n) \cdot k$  for some  $k \in \mathbb{Z}$  since  $\gcd(a, n)$  divides  $a$ . Hence, by Lemma 4.30,  $\langle a \rangle \subseteq \langle \gcd(a, n) \rangle$ .

To finish the proof, we show that  $\langle \gcd(a, n) \rangle \subseteq \langle a \rangle$ . By Bézout's Identity, there are integers  $x$  and  $y$  such that  $ax + ny = \gcd(a, n)$ . In particular,  $ax \equiv \gcd(a, n) \pmod{n}$ . So, again, Lemma 4.30 applies to guarantee that  $\langle \gcd(a, n) \rangle \subseteq \langle a \rangle$ .

Therefore,  $\langle a \rangle = \langle \gcd(a, n) \rangle$ .  $\square$

**Proposition 4.41.** Given  $a \in \mathbb{Z}_n$ , where  $n > 1$  and  $a > 0$ ,

$$\text{ord}(a) = \frac{n}{\gcd(a, n)}.$$

*Proof.* By Lemma 4.40,  $\langle a \rangle = \langle \gcd(a, n) \rangle$ . In particular, this means that

$$\text{ord}(a) = \text{ord}(\gcd(a, n)).$$

Since  $\gcd(a, n)$  divides  $n$ , Lemma 4.39 affirms that

$$\text{ord}(a) = \text{ord}(\gcd(a, n)) = \frac{n}{\gcd(a, n)}.$$

$\square$

In fact, for any finite cyclic group  $G$  of order  $n$ ,  $G$  has a subgroup of order  $d$  for any divisor  $d$  of  $n$ .

**Proposition 4.42.** Let  $(G, \cdot)$  be a cyclic group of order  $n$  and let  $d > 1$  be a divisor of  $n$ . Then  $G$  has a subgroup of order  $d$ .

*Proof.* Let  $n$  and  $d$  be as in the hypothesis. Then  $n = dk$  for some positive integer  $k$ . Note that  $G$  is isomorphic to  $\mathbb{Z}_n$ , so we restrict our attention to  $\mathbb{Z}_n$ . Note that  $k \in \mathbb{Z}_n$  and that the order of  $k$  is  $d$ . Therefore,  $\langle k \rangle$  is a subgroup of order  $d$ .  $\square$

**Exercise 4.28.** Suppose  $(G, \cdot)$  is a group which has a unique nontrivial proper subgroup. Show that  $G$  is a cyclic group of order  $p^2$ , where  $p$  is a prime number.

For elements in a group that commute and for which their corresponding cyclic subgroups only have the identity element in common, we can compute the order of their product based on their respective orders.

**Proposition 4.43.** Suppose  $(G, \cdot)$  is a group and that  $g, h \in G$  are elements of finite order such that  $gh = hg$  and that  $\langle g \rangle \cap \langle h \rangle = \{e_G\}$ . Then

$$\text{ord}(gh) = \text{lcm}(\text{ord}(g), \text{ord}(h)).$$

More generally, if  $g_1, g_2, \dots, g_k \in G$  commute, are each of finite order, and

$$\langle g_j \rangle \cap H_j = \{e_G\}$$

where

$$H_j = \{g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_k^{\alpha_k} : \alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{Z}, \alpha_j = 0\},$$

for every positive integer  $j \leq k$ ,

$$\text{ord}(g_1 g_2 \cdots g_k) = \text{lcm}(\text{ord}(g_1), \text{ord}(g_2), \dots, \text{ord}(g_k)).$$

*Proof.* Let  $p = \text{ord}(g)$ ,  $q = \text{ord}(h)$ ,  $m = \text{lcm}(p, q)$ , and  $r = \text{ord}(gh)$ . Since  $m$  is a multiple of both  $p$  and  $q$ , then we can write  $m = pa$  and  $m = qb$  for integers  $a$  and  $b$ . Note then that

$$(gh)^m = g^m h^m = (g^p)^a (h^q)^b = e_G.$$

So  $r \leq m$ .

To show that  $m \leq r$ , we first by claiming that  $r \geq \max\{p, q\}$ . To see this, consider the fact that

$$g^r h^r = (gh)^r = e_G \implies g^r = h^{-r}.$$

It follows that  $g^r \in \langle g \rangle \cap \langle h \rangle$ , and so  $g^r = e_G$ . In a similar fashion,  $h^r \in \langle g \rangle \cap \langle h \rangle = \{e_G\}$ . So  $p \leq r$  and  $q \leq r$ . Hence, we can write  $r = ps_1 + t_1$  and  $r = qs_2 + t_2$  where  $s_1, t_1, s_2$ , and  $t_2$  are integers with  $0 \leq t_1 < p$  and  $0 \leq t_2 < q$ . Then note that

$$e_G = (gh)^r = g^r h^r = (g^p)^{s_1} g^{t_1} (h^q)^{s_2} h^{t_2} = g^{t_1} h^{t_2}.$$

Since  $t_1 < r$  and  $t_2 < q$ , it must be the case that  $t_1 = t_2 = 0$ . In particular,  $r$  is a multiple of both  $p$  and  $q$ . Therefore,  $m \leq r$ .

Now, for the more general case, suppose the proposition holds for all  $k \leq n$  for  $n \geq 2$  and suppose  $g_1, g_2, \dots, g_k, g_{k+1} \in G$  satisfy the stated hypotheses. Note that, in particular,  $g_1, g_2, \dots, g_k$  satisfy the stated hypotheses, so we can use the inductive hypothesis to conclude that

$$\text{ord}(g_1 g_2 \cdots g_k) = \text{lcm}(\text{ord}(g_1), \text{ord}(g_2), \dots, \text{ord}(g_k)).$$

Now, since all of the  $g_j$  commute with each other, then  $h := g_1 g_2 \cdots g_k$  and  $g_{k+1}$  commute with each other. Moreover,

$$\langle g_{k+1} \rangle \cap \langle h \rangle \subseteq \langle g_{k+1} \rangle \cap H_{k+1} = \{e_G\}.$$

Hence, the former assertion of the proposition applies to guarantee that

$$\text{ord}(hg_{k+1}) = \text{lcm}(\text{ord}(h), \text{ord}(g_{k+1})) = \text{lcm}(\text{ord}(g_1), \text{ord}(g_2), \dots, \text{ord}(g_{k+1})),$$

finishing the proof.  $\square$

The condition that  $\langle g \rangle \cap \langle h \rangle = \{e_G\}$  in Proposition 4.43 is a necessary one since

$$\text{ord}(gg^{-1}) = 1,$$

regardless of what properties  $g$  may have.

For the more general statement, consider  $\{01, 10, 11\}$ , as the three non-identity elements of the group in Example 4.26 written in string form. Note that these elements all commute with each other and that they generate cyclic subgroups that have pairwise trivial intersection. However,

$$\text{ord}(01 + 10 + 11) = \text{ord}(00) = 1 \neq \text{lcm}(2, 2, 2).$$

The condition that the elements  $g$  and  $h$  commute in Proposition 4.43 is also a necessary one. In fact, for elements that don't commute, it's possible to have two elements of finite order with a product that has infinite order.

**Exercise 4.29.** Let

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

Prove that, as elements of  $(\text{GL}(2, \mathbb{R}), \cdot)$ ,  $A$  and  $B$  both have finite orders, but that  $AB$  has infinite order.

**Example 4.44** (Roots of Unity). Recall that the complex numbers  $\mathbb{C}$  can be expressed in the form  $x + iy$  where  $x, y \in \mathbb{R}$  and  $i$  is chosen to be a solution to the equation  $x^2 + 1 = 0$ . After this choice has been made, there are two roots to the equation  $x^2 + 1 = 0$  over  $\mathbb{C}$ :  $i$  and  $-i$ . Let  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ . Then  $(\mathbb{C}^*, \cdot)$ , where  $\cdot$  is the usual multiplication of complex numbers, forms an Abelian group. We define the *modulus* of a complex number  $x + iy$  to be

$$|x + iy| = \sqrt{x^2 + y^2}.$$

It can then be shown that

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

is a subgroup of  $(\mathbb{C}^*, \cdot)$ .  $\mathbb{S}^1$  is known as the *circle group*.

Let  $n \in \mathbb{N}$  and consider

$$H_n = \{z \in \mathbb{C} : z^n = 1\}.$$

The elements of  $H_n$  are referred to as the  $n^{\text{th}}$  *roots of unity*. As you will be asked to show in Exercise 4.30,  $H_n$  is a cyclic subgroup of  $\mathbb{S}^1$  of order  $n$ ; indeed,  $(H_n, \cdot)$  is isomorphic to  $(\mathbb{Z}_n, \oplus)$ .

**Exercise 4.30.** Show that, for  $n \in \mathbb{N}$ ,  $(H_n, \cdot)$  is cyclic. (*Hint.* Use DeMoivre's Theorem.)

## 5 Permutation Groups

Permutation groups form another important category of groups and arise naturally from the study of geometric symmetries. Permutation groups also have applications to the theory of finding solutions to polynomial equations.

### 5.1 Permutations and Symmetric Groups

**Definition 5.1.** Given a set  $X$ , a *permutation* of  $X$  is a bijection  $p : X \rightarrow X$ .

**Definition 5.2.** For a nonempty set  $X$ , we define the *symmetric group* on  $X$  to be the set  $S_X$  of all permutations of  $X$  endowed with the binary operation of composition  $\circ$ .

If the set  $X$  is finite, with  $n \in \mathbb{N}$  elements (which, without loss of generality, can be taken to be  $\{1, 2, \dots, n\}$ ), then we let  $S_n$  denote  $S_X$ .

**Definition 5.3.** A group is called a *permutation group* if it is a subgroup of  $(S_n, \circ)$  for some  $n \in \mathbb{N}$ .

**Exercise 5.1.** Show that  $(S_n, \circ)$  is of order  $n!$ .

Recall Example 4.15 and observe that  $(S_3, \circ)$  in our updated notation corresponds exactly to the group of symmetries of an equilateral triangle. Note also that  $(S_3, \circ)$  is not Abelian. Hence:

**Comment.** In general, permutation groups are not Abelian.

However, full symmetric groups tend to be strictly larger than groups of geometric symmetries. For example, a square has 8 symmetries (the identity, a counterclockwise rotation by  $90^\circ$  which generates three non-identity rotations, and four reflections), but  $(S_4, \circ)$  is a group of order  $4! = 24$  by Exercise 5.1. By labeling the four corners of the square, we can see that the symmetries of the square naturally forms a subgroup of  $(S_4, \circ)$ , so the symmetries of the square is a non-trivial example of a permutation group.

When working with symmetric groups, it is convenient to employ *cycle notation*.

**Definition 5.4.** For a permutation  $p$  of a set  $X$ , we define the *support* of  $p$  to be

$$\text{supp}(p) = \{x \in X : p(x) \neq x\}.$$

That is, the support of  $p$  is the set of points of  $X$  that are moved to points other than themselves by  $p$ .

**Definition 5.5.** A *cycle* of length  $k \geq 2$  is a permutation  $\sigma$  of  $n \geq k$  symbols such that there exists a collection  $\{a_1, a_2, \dots, a_k\}$  of distinct symbols such that  $\sigma(a_j) = a_{j+1}$ , for  $1 \leq j < k$ ,  $\sigma(a_k) = a_1$ , and  $\text{supp}(\sigma) = \{a_1, a_2, \dots, a_k\}$ . In such a case, we use the *cycle notation*

$$(a_1 \ a_2 \ a_3 \ \cdots \ a_k)$$

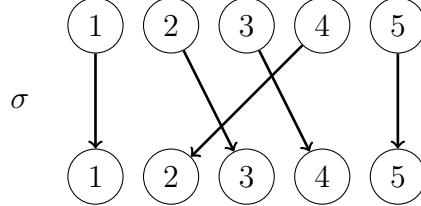
for  $\sigma$ . For convenience, we will use  $()$  to denote the identity permutation, which we will call the *trivial cycle* or permutation.

**Comment.** Since we will generally be phrasing symmetric groups as the group of permutations of  $\{1, 2, \dots, n\}$ , for  $n \in \mathbb{N}$ , given any cycle  $\sigma$  of  $S_n$ , we can choose  $a_1$  to be the minimal element of the support of  $\sigma$ . This uniquely determines a cycle notation for  $\sigma$ .

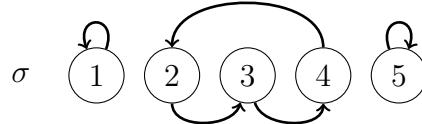
**Example 5.6.** Consider  $X = \{1, 2, 3, 4, 5\}$ . By  $(2 \ 3 \ 4)$ , we mean the permutation  $\sigma$  of  $X$  where

$$\sigma(1) = 1 \quad \sigma(2) = 3 \quad \sigma(3) = 4 \quad \sigma(4) = 2 \quad \sigma(5) = 5$$

Another representation of  $\sigma$ :



We may also describe  $\sigma$  using a directed graph:



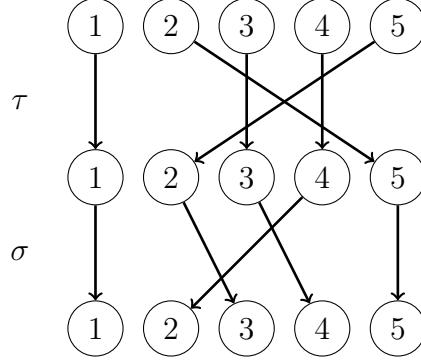
In this case, note that  $\text{supp}(\sigma) = \{2, 3, 4\}$ .

**Remark.** When using cycle notation, we will use juxtaposition to represent the operation of function composition.

**Example 5.7.** Let  $X = \{1, 2, 3, 4, 5\}$ ,  $\sigma = (2 \ 3 \ 4)$ , and  $\tau = (2 \ 5)$ . Then we use the notation  $\sigma\tau = (2 \ 3 \ 4)(2 \ 5)$  to be  $\sigma \circ \tau$ , which is the mapping

$$\sigma\tau(1) = 1 \quad \sigma\tau(2) = 5 \quad \sigma\tau(3) = 4 \quad \sigma\tau(4) = 2 \quad \sigma\tau(5) = 3$$

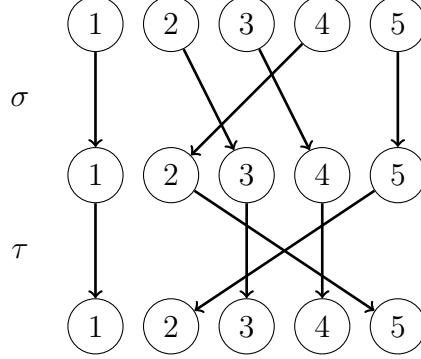
Note that this aligns with the following graphical representation (note that  $\tau$  is applied *before*  $\sigma$  because of how we notate function composition):



We can express  $\sigma\tau$  using cycle notation:

$$\sigma\tau = (2 \ 5 \ 3 \ 4).$$

Note that switching the order generates a different permutation:



That is,

$$\tau\sigma(1) = 1 \quad \tau\sigma(2) = 3 \quad \tau\sigma(3) = 4 \quad \tau\sigma(4) = 5 \quad \tau\sigma(5) = 2$$

We can also express  $\tau\sigma$  using cycle notation:

$$\tau\sigma = (2 \ 3 \ 4 \ 5).$$

In this case, we have that  $\sigma\tau \neq \tau\sigma$ .

So, in general, cycles do not commute with each other. However, there are cases in which cycles *do* commute.

**Definition 5.8.** Two cycles  $\sigma$  and  $\tau$  are said to be *disjoint* if  $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$ .

**Exercise 5.2.** Show that, if  $\sigma$  and  $\tau$  are disjoint cycles, then  $\sigma\tau = \tau\sigma$ .

Despite the scenario in Example 5.7 where  $\sigma\tau$  and  $\tau\sigma$  could be rewritten as single cycles, not all permutations can be expressed as a single cycle. Indeed, for  $X = \{1, 2, 3, 4, 5\}$ , the permutation  $(1 \ 2)(4 \ 5)$  cannot be simplified into a single cycle. We can, however, express permutations as products of disjoint cycles.

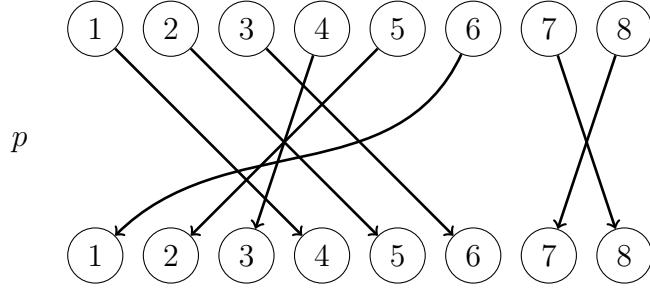
**Theorem 5.9.** Every permutation in  $S_n$  can be written as the product of disjoint cycles.

*Proof.* Let  $X = \{1, 2, \dots, n\}$  and  $\sigma \in S_n$ . Then define  $A_1 = \{\sigma^m(1) : m \in \mathbb{Z}\}$ . Note that  $1 \in A_1$ , so  $A_1 \neq \emptyset$ . Also note that  $A_1$  is the support of a cycle containing 1.

Now, for  $k \in \mathbb{N}$ , suppose we have defined  $\{A_j : j \leq k\}$ . If  $X = \bigcup\{A_j : j \leq k\}$ , then each  $A_j$  corresponds to a cycle, and these cycles are pair-wise disjoint, so we are done. Otherwise, we can let  $x$  be the minimal element of  $X \setminus \bigcup\{A_j : j \leq k\}$ . Then we define  $A_{k+1} = \{\sigma^m(x) : m \in \mathbb{Z}\}$ . Note that  $x \in A_{k+1}$ , so  $A_{k+1} \neq \emptyset$ .

Since  $X$  is finite and each  $A_k$  to be defined by the process above is non-empty and pair-wise disjoint, the process must terminate at some finite stage. It follows that  $\sigma$  can be rewritten as a product of disjoint cycles.  $\square$

To see how the proof above functions in context, let  $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$  and consider the permutation  $p$  described by



Note that the *orbit* of 1 under  $p$  generates the cycle

$$(1 \ 4 \ 3 \ 6).$$

Then  $A_1 = \{1, 3, 4, 6\}$ . Then  $X \setminus A_1 = \{2, 5, 7, 8\}$ . The smallest value of this set is 2 and the orbit of 2 under  $\sigma$  generates the cycle

$$(2 \ 5).$$

Then  $A_2 = \{2, 5\}$  and  $X \setminus (A_1 \cup A_2) = \{7, 8\}$ . The smallest of these values is 7, and 7 generates the final cycle

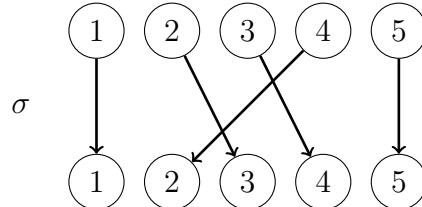
$$(7 \ 8).$$

Therefore,

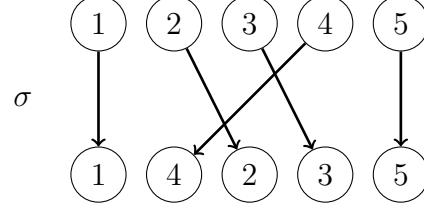
$$p = (1 \ 4 \ 3 \ 6)(2 \ 5)(7 \ 8). \quad (1)$$

Another useful way to represent permutations is as matrices.

**Example 5.10.** Refer back to the  $\sigma$  and  $\tau$  of Example 5.7. To faithfully capture the “action” of the permutation, we want to find a matrix for  $\sigma$  which describes the rearrangement of the symbols, as in the following diagram:



If we keep the same “action,” but shuffle the locations, then we obtain



Rewriting these as column matrices, we are looking for a matrix which accomplishes the following “action”:

$$\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} \xrightarrow{\text{curve}} \begin{bmatrix} 1 \\ 4 \\ 2 \\ 3 \\ 5 \end{bmatrix}$$

Adding subscripts to the right-hand column matrix indicating their position, we can recover the original bijection:

$$1_1 \\ 4_2 \\ 2_3 \\ 3_4 \\ 5_5$$

The value of the entry is mapped to its subscript under the original bijection.

Now, thinking of using row swapping operations, we can capture  $\sigma$  with

$$\hat{\sigma} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and, in a similar way,  $\tau$  can be captured with

$$\hat{\tau} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Another way to read these matrices is to note that, for example, in  $\hat{\sigma}$ , the second column has the 1 in the third row. In the original bijection, 2 is mapped to 3. Similarly, the fourth column has the 1 in the second row, and the original bijection sent 4 to 2.

Now, we can verify that

$$\hat{\sigma} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \\ 2 \\ 3 \\ 5 \end{bmatrix}$$

and that

$$\hat{\tau} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \\ 3 \\ 4 \\ 2 \end{bmatrix}.$$

Note that

$$\hat{\sigma}\hat{\tau} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \\ 5 \\ 3 \\ 2 \end{bmatrix} \quad \text{and} \quad \hat{\tau}\hat{\sigma} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \\ 2 \\ 3 \\ 4 \end{bmatrix}.$$

Note that, interpreting the resulting column matrix, particularly in the case  $\hat{\sigma}\hat{\tau}$ , we have a map which does the following:

$$1 \mapsto 1, \quad 4 \mapsto 2, \quad 5 \mapsto 3, \quad 3 \mapsto 4, \quad 2 \mapsto 5$$

Observe that this corresponds exactly to  $\sigma\tau$  from Example 5.7.

**Fact 5.11.** For each  $p \in S_n$ , define

$$\hat{p} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix}$$

where

$$a_{j,k} = \begin{cases} 1, & j = p(k) \\ 0, & \text{otherwise} \end{cases}$$

Then the mapping  $p \mapsto \hat{p}$ ,  $S_n \rightarrow \text{GL}(n, \mathbb{R})$ , is an injective homomorphism of groups. Moreover,  $\det(\hat{p}) = \pm 1$ , which can be verified by considering cofactor expansions and the fact that each row/column of  $\hat{p}$  has exactly one occurrence of 1. At each recursive step in the cofactor expansion, one will be able to select a row/column with exactly one entry of 1 contributing a 1 or  $-1$  to the determinant. At “the bottom” of the recursion, one is left computing either

$$\det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1$$

or

$$\det \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = -1.$$

Hence, the final determinant is either 1 or  $-1$ .

**Definition 5.12.** Given a permutation  $p \in S_n$ , we define the *sign* of  $p$  to be

$$\text{sgn}(p) = \det(\hat{p}).$$

By Fact 5.11,  $\text{sgn}(p) = \pm 1$ .

**Exercise 5.3.** Consider  $G = \{-1, 1\}$ . Show that the map  $\text{sgn} : S_n \rightarrow G$  is a homomorphism from  $(S_n, \circ) \rightarrow (G, \cdot)$ .

**Definition 5.13.** For  $S_n$ , we define the *alternating group*  $A_n$  to consist of all  $p \in S_n$  with  $\text{sgn}(p) = 1$ . Note that, by Exercise 4.18,  $A_n$  is a subgroup of  $S_n$ .

There is another way to motivate the alternating group, and that's via *transpositions*.

**Definition 5.14.** Any cycle of the form<sup>16</sup>  $(a b)$  is called a *transposition*.

**Comment.** Note that any transposition is its own inverse. Hence, every transposition is of order 2.

In the context of  $(S_3, \circ)$ , using the notation for the group elements in Example 4.15,

$$\begin{array}{lll} \text{id} = () & \text{rot} = (\text{A C B}) & \text{rot}^2 = (\text{A B C}) \\ \text{ref}_1 = (\text{B C}) & \text{ref}_2 = (\text{A C}) & \text{ref}_3 = (\text{A B}) \end{array}$$

Note from the corresponding Cayley table, that

$$(\text{A C B}) = (\text{A C})(\text{B C}) \quad \text{and} \quad (\text{A B C}) = (\text{A B})(\text{B C}).$$

So then the subgroup  $\{(), (\text{A C})(\text{B C}), (\text{A B})(\text{B C})\}$  of  $(S_3, \circ)$  or order 3 consists of elements that can be written as the product of an even number of transpositions. In fact, this subgroup is exactly  $A_3$ .

**Exercise 5.4.** Show that the subgroup  $\{\text{id}, \text{rot}, \text{rot}^{-1}\}$  of  $S_3$  is  $A_3$  by computing the sign of every element of  $S_3$ .

**Proposition 5.15.** Every non-trivial cycle can be written as a product of transpositions.

*Proof.* Consider the cycle  $(a_1 a_2 \cdots a_k)$ , where  $k \geq 2$ , and observe that

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

Indeed, for  $a_j$ , where  $1 \leq j < k$ , the first transposition affecting  $a_j$  will be  $(a_j a_{j+1})$ , taking  $a_j$  to  $a_{j+1}$ . Then  $a_{j+1}$  appears in no further transpositions. In the case we have  $a_k$ ,  $a_k$  first gets moved to  $a_{k-1}$ , which then gets moved to  $a_{k-2}$  in the transposition  $(a_{k-2} a_{k-1})$ . This continues in this way until we reach  $(a_1 a_2)$ , finally taking  $a_2$  to  $a_1$ . So, in the end,  $a_k$  is mapped to  $a_1$ , finishing the proof.  $\square$

---

<sup>16</sup>Note that  $a \neq b$  by convention.

We note however that the decomposition of cycles into a product of transpositions is not unique. Indeed, note that

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

Nevertheless, we have the following result governing the parity of products of transpositions.

**Theorem 5.16.** If a cycle  $\sigma$  can be written as the product of an even number of transpositions, then any decomposition of  $\sigma$  into a product of transpositions must consist of an even number of transpositions. Consequently, if a cycle  $\sigma$  can be written as the product of an odd number of transpositions, then any decomposition of  $\sigma$  into a product of transpositions must consist of an odd number of transpositions.

*Proof.* Note that every transposition  $\tau$  has the property that  $\text{sgn}(\tau) = -1$ . Since the  $\text{sgn}$  function is a homomorphism, any product of an even number of transpositions has a positive sign, and any product of an odd number of transpositions has an odd sign.  $\square$

**Remark.** Using the cycle decomposition into transpositions as in the proof of Proposition 5.15, we see that a  $(k+1)$ -cycle, where  $k \in \mathbb{N}$ , can be written as a product of  $k$ -many transpositions. Hence, any  $(2k+1)$ -cycle is even and any  $(2k)$ -cycle is odd.

In fact, as long as  $n \geq 3$ , the alternating group is generated by the 3-cycles.

**Theorem 5.17.** For  $n \geq 3$ , any even permutation can be written as the product of 3-cycles. In other words, the alternating group  $A_n$  is generated by the 3-cycles.

*Proof.* It suffices to show that a product of transpositions can be written as a product of 3-cycles. So let  $(a \ b)$  and  $(c \ d)$  be transpositions (hence,  $a \neq b$  and  $c \neq d$ ). We proceed by cases.

If  $\{a, b\} = \{c, d\}$ , then  $(a \ b) = (c \ d)$ . It follows that

$$(a \ b)(c \ d) = () = (1 \ 2 \ 3)(1 \ 3 \ 2).$$

Now suppose that  $|\{a, b\} \cap \{c, d\}| = 1$ . Without loss of generality, suppose  $b = d$ . Note then that

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

For the final case, suppose that  $(a \ b)$  and  $(c \ d)$  are disjoint transpositions. Then verify that

$$(a \ b)(c \ d) = (a \ d \ c)(a \ b \ c).$$

Finally, since any even permutation can be written as a product of an even number of transpositions, and each product of a pair of transpositions can be written as a product of 3-cycles, then every even permutation can be written as a product of 3-cycles.  $\square$

**Proposition 5.18.** In any finite permutation group, the number of even permutations is equal to the number of odd permutations. In other words, exactly half of all the permutations in a finite permutation group are even.

*Proof.* Consider the permutation group  $S_n$ , where  $n > 1$ . For convenience, let  $B = S_n \setminus A_n$ , the set of odd permutations. Fix a transposition  $\tau \in S_n$  and define a function  $f : B \rightarrow A_n$  by the rule  $f(p) = \tau p$ . Note that the map  $f$  is defined since  $\tau p$  is an even permutation whenever  $p$  is an odd permutation. To finish the proof, we will show that  $f$  is a bijection.

First, suppose  $p, q \in B$  are such that

$$\tau p = f(p) = f(q) = \tau q.$$

We can then left-multiply by  $\tau^{-1} = \tau$  to yield that  $p = q$ . That is,  $f$  is injective.

To see that  $f$  is a surjection, let  $p \in A_n$  and consider  $\tau p \in B$ . Since  $\tau^{-1} = \tau$ , we see that  $f(\tau p) = \tau \tau p = p$ . Hence,  $f$  is a surjection.  $\square$

We show here that we can compute the order of any permutation using only information about its “cycle type.”

**Lemma 5.19.** The order of any  $n$ -cycle is  $n$ .

*Proof.* Suppose  $\sigma = (a_0 \ a_1 \ a_2 \ \dots \ a_{n-1})$ . Note that, for  $k \geq 1$ ,  $\sigma^k(a_0) = a_{k \% n}$ . So, for any  $k$ ,  $1 \leq k < n$ ,  $\sigma^k \neq ()$ . However,  $\sigma^n = ()$  since, for any  $j$ ,  $0 \leq j < n$ ,  $\sigma^n(a_j) = a_{(j+n) \% n} = a_j$ . Therefore,  $\text{ord}(\sigma) = n$ .  $\square$

Since all permutation can be expressed as a product of disjoint cycles, a common way to refer to permutations is in terms of their *cycle type*. For example,

$$(1 \ 2)(3 \ 4)(5 \ 6 \ 7)$$

is a cycle of type  $(2, 2, 3)$ .

**Proposition 5.20.** The order of a permutation of cycle type  $(n_1, n_2, \dots, n_k)$  is

$$\text{lcm}(n_1, n_2, \dots, n_k).$$

*Proof.* Let  $\sigma_j$  be the  $n_j$ -cycle, for  $1 \leq j \leq k$ , and let

$$H_j = \{\sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \cdots \sigma_k^{\alpha_k} : \alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{Z}, \alpha_j = 0\}.$$

To verify that

$$\langle \sigma_j \rangle \cap H_j = \{()\},$$

note that, for any integer  $a$ ,  $\text{supp}(\sigma_j^a) \subseteq \text{supp}(\sigma_j)$ . Also, note that, for integers  $\alpha_1, \alpha_2, \dots, \alpha_k$  where  $\alpha_j = 0$ ,

$$\begin{aligned} & \text{supp}(\sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \cdots \sigma_k^{\alpha_k}) \\ & \subseteq \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2) \cup \cdots \cup \text{supp}(\sigma_{j-1}) \cup \text{supp}(\sigma_{j+1}) \cup \cdots \cup \text{supp}(\sigma_k), \end{aligned}$$

since the cycles are disjoint. That is,

$$\text{supp}(\sigma_j) \cap \text{supp}(\sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \cdots \sigma_k^{\alpha_k}) = \emptyset.$$

Consequently,

$$\langle \sigma_j \rangle \cap H_j = \{()\}.$$

By Lemma 5.19, we know that each  $\sigma_j$  has order  $n_j$ . By Exercise 5.2, we have that disjoint cycles commute. Therefore, by Proposition 4.43, the proposition obtains.  $\square$

We can also use combinatorial techniques to determine the total number of  $k$ -cycles in a symmetric group.

**Proposition 5.21.** Let  $n > 1$  and  $k$  be an integer  $2 \leq k \leq n$ . Then there are

$$\frac{P(n, k)}{k} = \frac{n!}{k \cdot (n - k)!}$$

distinct  $k$ -cycles in  $S_n$ .

*Proof.* First, note that there are

$$P(n, k) = \frac{n!}{(n - k)!}$$

tuples of  $k$  distinct elements from  $X := \{1, 2, \dots, n\}$ . Given a particular tuple of distinct elements from  $X$ , note that  $k$  of the corresponding cycles are equivalent; indeed, note that

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

Therefore, the total number of distinct  $k$ -cycles is

$$\frac{P(n, k)}{k},$$

finishing the proof. □

## 5.2 Dihedral Groups

The *dihedral groups* are special subgroups of permutation groups corresponding to rigid motions of regular polygons.

**Definition 5.22.** Consider a regular (all angles are equal and all side lengths are equal) polygon with  $n$  vertices. The group of rigid motions of the given polygon, called a *dihedral group*, is denoted by  $D_n$ , and can be viewed as a subgroup of  $S_n$ .<sup>17</sup>

**Theorem 5.23.** The order of  $D_n$ , for  $n \geq 3$ , is  $2n$ .

*Proof.* Any rigid motion of a polygon with  $n$  vertices can be fully described by where it sends a single pair of adjacent vertices. Then, for a given fixed pair of adjacent vertices  $(a, b)$ , the vertex  $a$  can be moved to one of  $n$  vertices, and  $b$  can then be sent to one of the two vertices which are adjacent to the vertex  $a$  was moved to. Hence, there are at most  $2n$  rigid motions.

To see that this upper-bound is attained, note that there are  $n$  distinct rotations. To address the number of reflections, we consider two cases.

When  $n$  is odd, there is a single reflection that fixes a given vertex. Hence, there are  $n$  distinct reflections. Since no rotation fixes any vertices, we see that the total number of rigid motions is at least  $n + n = 2n$ .

---

<sup>17</sup>Note that group theorists typically write  $D_{2n}$  to refer to  $D_n$ , which is partially motivated by Theorem 5.23.

When  $n$  is even, any reflection that fixes one vertex fixes another vertex opposite to the vertex under consideration. So there are  $n/2$  reflections that fix vertices. In this context, there are also  $n/2$  reflections that pass through two opposing sides of the given polygon. Hence, there are  $\frac{n}{2} + \frac{n}{2} = n$  reflections. Like above, the total number of rigid motions is at least  $n + n = 2n$ .

Conclusively, the order of  $D_n$  is  $2n$ . □

When working in the context of a dihedral group  $D_n$ , we can label the vertices of the corresponding polygon with the integers 1 through  $n$  in a counterclockwise fashion. We can then let  $r$  denote the counterclockwise rotation that takes vertex 1 to vertex 2. With this choice,  $r$  has order  $n$  within  $D_n$ ; that is,  $r^n = 1$ .

Now, let  $s$  denote the reflection that fixes vertex 1. We argue here that any other reflection can be obtained as a product  $r^k s$ , for some  $0 \leq k < n$ . Consider an arbitrary reflection  $g$  and note that  $g$  moves vertex 1 to some other vertex  $1 \leq k \leq n$ . Then observe that  $g = r^{k-1}s$ .

**Remark.** Using the notation above, we have just finished arguing that

$$D_n = \{r^k : 0 \leq k < n\} \cup \{r^k s : 0 \leq k < n\}$$

where  $\{r^k : 0 \leq k < n\}$  is the set of all rotations and  $\{r^k s : 0 \leq k < n\}$  is the set of all reflections.

**Exercise 5.5.** In the context of  $D_n$ , show that  $sr^k s = r^{-k}$ , where  $k$  is an integer. (*Hint.* Note that  $r^k s$  is a reflection and that every reflection has order 2.)

### 5.3 Cayley's Theorem

**Exercise 5.6.** Let  $(G, \cdot)$  be a group and, for  $g \in G$ , define  $T_g : G \rightarrow G$  by the rule  $T_g(x) = gx$ . Show that  $T_g$  is a permutation of  $G$ .

**Exercise 5.7.** Suppose  $(G, \cdot)$  is a group and let  $S_G$  denote the symmetric group on  $G$ . Define  $\varphi : G \rightarrow S_G$  by the rule  $\varphi(g) = T_g$ , where  $T_g$  is as defined in Exercise 5.6. Show that  $\varphi$  is an injective homomorphism.

As a direct consequence of Exercise 5.7, we have:

**Theorem 5.24** (Cayley's Theorem). Every group is (isomorphic to) a permutation group. In particular, if  $(G, \cdot)$  is a group of order  $n \in \mathbb{N}$ , it is isomorphic to a subgroup of  $S_n$ .

**Remark.** Since Fact 5.11 affirms that  $S_n$ , where  $n \in \mathbb{N}$ , is isomorphic to a subgroup of  $\mathrm{GL}(2, \mathbb{R})$ , any group of order  $n$  is isomorphic to a subgroup of  $\mathrm{GL}(2, \mathbb{R})$ .

## 6 Cosets and Lagrange's Theorem

### 6.1 Cosets

**Definition 6.1.** Let  $(G, \cdot)$  be a group and  $H$  be a subgroup of  $G$ . We let  $gH = \{gh : h \in H\}$  and refer to  $gH$  as a *left-coset*; likewise, we say that  $Hg = \{hg : h \in H\}$  is a *right-coset*.

**Example 6.2.** Consider the symmetric group  $S_3$  and the subgroup  $H = \{(), (1 2)\}$ . We will list both the left-cosets of  $H$  and the right-cosets of  $H$ . First, note that

$$S_3 = \{(), (1 2), (1 3), (2 3), (1 2 3), (1 3 2)\}.$$

We can list out the elements  $gh$  where  $g \in S_3$  and  $h \in H$  in tabular form:

	( $)$	( $1 2$ )
( $)$	( $)$	( $1 2$ )
( $1 2$ )	( $1 2$ )	( $)$ )
( $1 3$ )	( $1 3$ )	( $1 2 3$ )
( $2 3$ )	( $2 3$ )	( $1 3 2$ )
( $1 2 3$ )	( $1 2 3$ )	( $1 3$ )
( $1 3 2$ )	( $1 3 2$ )	( $2 3$ )

So the distinct left-cosets of  $H$  in this context are

$$\left\{ \begin{array}{l} H = (1 2)H = \{(), (1 2)\} \\ (1 3)H = (1 2 3)H = \{(1 3), (1 2 3)\} \\ (2 3)H = (1 3 2)H = \{(2 3), (1 3 2)\} \end{array} \right.$$

We can also list out the elements  $hg$  where  $g \in S_3$  and  $h \in H$  in tabular form:

	( $)$	( $1 2$ )	( $1 3$ )	( $2 3$ )	( $1 2 3$ )	( $1 3 2$ )
( $)$	( $)$	( $1 2$ )	( $1 3$ )	( $2 3$ )	( $1 2 3$ )	( $1 3 2$ )
( $1 2$ )	( $1 2$ )	( $)$ )	( $1 3 2$ )	( $1 2 3$ )	( $2 3$ )	( $1 3$ )

So the distinct right-cosets of  $H$  in this context are

$$\left\{ \begin{array}{l} H = H(1 2) = \{(), (1 2)\} \\ H(1 3) = H(1 3 2) = \{(1 3), (1 3 2)\} \\ H(2 3) = H(1 2 3) = \{(2 3), (1 2 3)\} \end{array} \right.$$

Note in both cases that there are three distinct cosets.

**Lemma 6.3.** Let  $(G, \cdot)$  be a group and  $H$  be a subgroup of  $G$ . Suppose  $g_1, g_2 \in G$ . Then the following are equivalent:

$$(i) \quad g_1 H = g_2 H$$

$$(ii) \quad H g_1^{-1} = H g_2^{-1}$$

$$(iii) \quad g_2 \in g_1 H$$

$$(iv) \quad g_2^{-1} \in H g_1^{-1}$$

$$(v) \quad g_1^{-1} g_2 \in H$$

(vi)  $g_2^{-1}g_1 \in H$

*Proof.* (i)  $\implies$  (ii): Suppose that  $g_1H = g_2H$ .

We will start by showing that  $Hg_1^{-1} \subseteq Hg_2^{-1}$ . So consider  $hg_1^{-1} \in Hg_1^{-1}$ , for  $h \in H$ , and note that

$$(hg_1^{-1})^{-1} = g_1h^{-1} \in g_1H = g_2H.$$

Then there is some  $k \in H$  for which  $(hg_1^{-1})^{-1} = g_2k$ . Observe that

$$hg_1^{-1} = ((hg_1^{-1})^{-1})^{-1} = (g_2k)^{-1} = k^{-1}g_2^{-1} \in Hg_2^{-1}.$$

Hence,  $Hg_1^{-1} \subseteq Hg_2^{-1}$ .

We now show that  $Hg_2^{-1} \subseteq Hg_1^{-1}$ . So consider  $hg_2^{-1}$ , where  $h \in H$ . Like above,  $(hg_2^{-1})^{-1} = g_2h^{-1} \in g_2H = g_1H$ . Then there is some  $k \in H$  for which  $(hg_2^{-1})^{-1} = g_1k$ . As before, observe that

$$hg_2^{-1} = ((hg_2^{-1})^{-1})^{-1} = (g_1k)^{-1} = k^{-1}g_1^{-1} \in Hg_1^{-1}.$$

So  $Hg_2^{-1} \subseteq Hg_1^{-1}$ .

Thus,  $Hg_1^{-1} = Hg_2^{-1}$ .

(ii)  $\implies$  (iii): Suppose  $Hg_1^{-1} = Hg_2^{-1}$ . Then there are  $h, k \in H$  such that  $hg_1^{-1} = kg_2^{-1}$ . Note that

$$\begin{aligned} hg_1^{-1} = kg_2^{-1} &\implies hg_1^{-1}g_2 = k \\ &\implies g_1^{-1}g_2 = h^{-1}k \\ &\implies g_2 = g_1h^{-1}k \in g_1H. \end{aligned}$$

(iii)  $\implies$  (iv): Suppose  $g_2 \in g_1H$ . Then there is some  $h \in H$  for which  $g_2 = g_1h$ . It follows that

$$g_2^{-1} = (g_1h)^{-1} = h^{-1}g_1^{-1} \in Hg_1^{-1}.$$

(iv)  $\implies$  (v): Suppose that  $g_2^{-1} \in Hg_1^{-1}$ . Then there is some  $h \in H$  for which  $g_2^{-1} = hg_1^{-1}$ . Note then that  $g_2 = g_1h^{-1}$  and, furthermore, that  $g_1^{-1}g_2 = h^{-1} \in H$ .

(v)  $\implies$  (vi): Suppose that  $g_1^{-1}g_2 \in H$ . Then

$$g_2^{-1}g_1 = (g_1^{-1}g_2)^{-1} \in H.$$

(vi)  $\implies$  (i): Suppose  $g_2^{-1}g_1 \in H$ .

We start by showing that  $g_1H \subseteq g_2H$ . So let  $h \in H$  be arbitrary and note that

$$g_1h = g_2g_2^{-1}g_1h = g_2(g_2^{-1}g_1h) \in g_2H$$

since  $g_2^{-1}g_1 \in H$ .

We finish by showing that  $g_2H \subseteq g_1H$ . So consider  $g_2h$  for  $h \in H$ . Note that  $g_1^{-1}g_2 = (g_2^{-1}g_1)^{-1} \in H$  since  $g_2^{-1}g_1 \in H$ . It follows that

$$g_2h = g_1g_1^{-1}g_2h = g_1(g_1^{-1}g_2h) \in g_1H$$

since  $g_1^{-1}g_2h \in H$ .

Therefore,  $g_1H = g_2H$ . □

**Exercise 6.1.** Let  $(G, \cdot)$  be a group and  $H$  be a subgroup of  $G$ . Define a relation  $\simeq$  on  $G$  by the rule  $g \simeq h$  provided that  $g^{-1}h \in H$ . Show that  $\simeq$  is an equivalence relation on  $G$  and that the equivalence classes of  $\simeq$  are precisely the left-cosets of  $H$ .

**Exercise 6.2.** Let  $(G, \cdot)$  be a group and  $H$  be a subgroup of  $G$ . Show that the left-cosets form a partition of  $G$ .

**Exercise 6.3.** Let  $(G, \cdot)$  be a group and  $H$  be a subgroup of  $G$ . Fix  $g \in G$  and define  $t_\ell : H \rightarrow gH$  and  $t_r : H \rightarrow Hg$  by  $t_\ell(x) = gx$  and  $t_r(x) = xg$ . Show that both  $t_\ell$  and  $t_r$  are bijections and conclude that each left-coset of  $H$  and each right-coset of  $H$  has the same cardinality as  $H$ .

**Proposition 6.4.** Let  $(G, \cdot)$  be a group and  $H$  be a subgroup of  $G$ . Then the number of distinct left-cosets of  $H$  is the same as the number of distinct right-cosets of  $H$ .

*Proof.* Let  $L_H$  be the set of left-cosets of  $H$  and  $R_H$  be the set of right-cosets of  $H$ . We define  $\gamma : L_H \rightarrow R_H$  by  $\gamma(gH) = Hg^{-1}$ , where  $g \in G$ . Note that  $\gamma$  is seen to be both well-defined and injective by Lemma 6.3. So, to finish the proof, we need only show that  $\gamma$  is surjective. Note that an arbitrary right-coset of  $H$  must be  $Hg$  for some  $g \in G$ . Then observe that

$$\gamma(g^{-1}H) = H(g^{-1})^{-1} = Hg,$$

finishing the proof.  $\square$

## 6.2 Lagrange's Theorem

Now that we know that all cosets are of the same size and that the number of left-cosets is equal to the number of right-cosets, we define the index of a subgroup within a group.

**Definition 6.5.** For a group  $(G, \cdot)$ , we say that the *index* of a subgroup  $H$  of  $G$ , denoted by  $[G : H]$ , is the number of distinct left-cosets of  $H$ .

**Theorem 6.6** (Lagrange's Theorem). Suppose  $(G, \cdot)$  is a finite group and that  $H$  is a subgroup of  $G$ . Then

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

*Proof.* We show that  $|G| = [G : H] \cdot |H|$ . Suppose  $[G : H] = j \in \mathbb{N}$  and let  $R := \{g_1, g_2, \dots, g_j\}$  be such that  $\{g_1H, g_2H, \dots, g_jH\}$  is the complete set of distinct left-cosets. Define  $p : R \times H \rightarrow G$  by the rule  $p(g, h) = gh$ . We will show that  $p$  is a bijection.

First, suppose  $(g_k, h_1), (g_\ell, h_2) \in R \times H$  are such that

$$p(g_k, h_1) = g_kh_1 = g_\ell h_2 = p(g_\ell, h_2).$$

Note then that

$$g_\ell^{-1}g_k = h_2h_1^{-1} \in H.$$

By Lemma 6.3,  $g_\ell H = g_k H$ . Hence, by our definition of  $R$ ,  $g_\ell = g_k$ . It follows that  $h_1 = h_2$ , so  $p$  is injective.

To see that  $p$  is surjective, let  $g \in G$ . Since the left-cosets of  $H$  partition  $G$ , there exists some  $g_k \in R$  such that  $g \in g_k H$ . Then there is some  $h \in H$  for which  $g = g_k h$ . Note then that  $p(g_k, h) = g$ . So  $p$  is a surjection.

Since  $p$  is a bijection,

$$|G| = |R \times H| = [G : H] \cdot |H|,$$

finishing the proof.  $\square$

**Corollary 6.7.** In a finite group  $G$ , the order of any element divides  $|G|$ . Consequently, if  $n = |G|$  and  $g \in G$ ,  $g^n = e_G$ .

*Proof.* Let  $n = |G|$ ,  $g \in G$ , and  $r = \text{ord}(g)$ . Note that  $r = |\langle g \rangle|$  and that  $\langle g \rangle$  is a subgroup of  $G$ . By Lagrange's Theorem,  $r$  divides  $n$ . Hence, there is some integer  $k$  for which  $rk = n$ . It follows that  $g^n = g^{rk} = (g^r)^k = e_G$ .  $\square$

As a particular application, we obtain Fermat's Little Theorem.

**Corollary 6.8** (Fermat's Little Theorem). If  $p$  is a prime and  $a \in \mathbb{Z}$ , then  $a^p \equiv a \pmod{p}$ .

*Proof.* By Theorem 4.12, we know that  $\mathbb{Z}_p^+$  is a group under multiplication. Note that the order of  $\mathbb{Z}_p^+$  is  $p - 1$ . If  $a \equiv 0 \pmod{p}$ , then it is clear that  $a^p \equiv a \pmod{p}$ . So suppose  $a \not\equiv 0 \pmod{p}$ . Then there is some  $x \in \mathbb{Z}_p^+$  for which  $a \equiv x \pmod{p}$ . By Corollary 6.7,  $x^{p-1} \equiv 1 \pmod{p}$ . Hence,  $x^p \equiv x \pmod{p}$  which yields that  $a^p \equiv a \pmod{p}$ .  $\square$

**Exercise 6.4.** Suppose  $(G, \cdot)$  is a group and  $H$  is a subgroup of  $G$  with the property that  $|H| \geq \frac{|G|}{2}$ . Show that, for every  $g \in G$  and every  $h \in H$ ,  $ghg^{-1} \in H$ .

**Exercise 6.5.** Let  $(G, \cdot)$  be a group and  $H$  be a subgroup of  $G$ . Suppose that, for every  $g \in G$  and every  $h \in H$ ,  $ghg^{-1} \in H$ . Show that, for every  $g \in G$ ,  $gH = Hg$ ; that is, that the left- and right-cosets are identical.

Recall Proposition 4.42 which can be seen as a converse of Lagrange's Theorem in the context of cyclic groups. The converse to Lagrange's Theorem in the more general context does not hold, however.

**Example 6.9.** The alternating group  $A_4$  is of order 12 and has no subgroup of order 6.

*Proof.* First note that the order of  $A_4$  is  $\frac{4!}{2} = 12$ . Now suppose  $H \subseteq A_4$  is a subgroup with at least 6 elements. By Exercise 6.4, we know that  $php^{-1} \in H$  for any  $p \in A_4$  and  $h \in H$ . By Proposition 5.21, there are

$$\frac{P(4, 3)}{3} = 8$$

distinct 3-cycles in  $S_3$ . Note that every 3-cycle is an element of  $A_4$ . So  $A_4$  has 4 elements which are not 3-cycles. It follows that  $H$  must contain at least one 3-cycle, say  $(a b c)$ . Let  $d \in \{1, 2, 3, 4\} \setminus \{a, b, c\}$  and note that

$$(a b d)(a b c)(a b d)^{-1} = (a b d)(a b c)(a d b) = (b d c) \in H.$$

Since  $H$  is a subgroup, we also have that

$$(a \ b \ c)(b \ d \ c) = (a \ b \ d) \in H.$$

Accounting for inverses, note that we have so far that

$$\{(), (a \ b \ c), (a \ c \ b), (b \ d \ c), (b \ c \ d), (a \ b \ d), (a \ d \ b)\} \subseteq H.$$

Hence,  $|H| \geq 7$ . Therefore,  $A_4$  has no subgroup of order 6.  $\square$

## 7 Creating New Groups From Old

In this section, we will discuss two common ways to create new mathematical objects from existing examples: via Cartesian products and via “quotients.”

### 7.1 Direct Products

**Definition 7.1.** Suppose  $(G, *)$  and  $(H, \circ)$  are groups. We define the binary operation  $\cdot$  on the Cartesian product  $G \times H$  by the rule

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

When  $G$  and  $H$  refer to groups, the notation  $G \times H$  will be understood going forward as meaning the Cartesian product  $G \times H$  paired with this binary operation, and we will refer to the pair  $(G \times H, \cdot)$  as the *direct product* of  $(G, *)$  and  $(H, \circ)$ .

**Exercise 7.1.** Given groups  $(G, *)$  and  $(H, \circ)$ , show that the binary operation on  $G \times H$  defined in Definition 7.1 satisfies the group axioms.

**Exercise 7.2.** Suppose  $(G, *)$  and  $(H, \circ)$  are nontrivial groups. Let  $\varphi : G \rightarrow G \times H$  and  $\psi : H \rightarrow G \times H$  be defined by  $\varphi(g) = (g, e_H)$  and  $\psi(h) = (e_G, h)$ . Show that both  $\varphi$  and  $\psi$  are injective homomorphisms. Conclude that, in this way,  $G \times H$  contains at least two distinct nontrivial proper subgroups: one isomorphic to  $G$  and the other isomorphic to  $H$ .

**Exercise 7.3.** For two groups  $G$  and  $H$ , define  $\pi_1 : G \times H \rightarrow G$  and  $\pi_2 : G \times H \rightarrow H$  by the rules  $\pi_1(g, h) = g$  and  $\pi_2(g, h) = h$ . Show that both  $\pi_1$  and  $\pi_2$  are surjective homomorphisms.

When creating new objects from old, it is common to ask which properties are preserved by the new construction.

**Proposition 7.2.** Suppose  $(G, *)$  and  $(H, \circ)$  are groups. Then the direct product  $G \times H$  is Abelian if and only if both  $G$  and  $H$  are Abelian.

*Proof.* First, suppose  $G$  and  $H$  are both Abelian. Let  $(g_1, h_1), (g_2, h_2) \in G \times H$  and note that

$$\begin{aligned} (g_1, h_1) \cdot (g_2, h_2) &= (g_1 * g_2, h_1 \circ h_2) \\ &= (g_2 * g_1, h_2 \circ h_1) \\ &= (g_2, h_2) \cdot (g_1, h_1). \end{aligned}$$

Conclusively,  $G \times H$  is Abelian.

The other direction follows from Exercise 7.3 and Proposition 4.27, which states that the homomorphic image of an Abelian group is Abelian.  $\square$

The case for the property of being cyclic does not work out similarly.

**Example 7.3.** The direct product of two cyclic groups may fail to be cyclic. Indeed, consider  $(\mathbb{Z}_2, \oplus)$  and the direct product with itself,  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . A straightforward computation shows that no element of  $\mathbb{Z}_2 \times \mathbb{Z}_2$  generates the entire group; indeed, each non-identity element has order 2.

**Theorem 7.4.** For positive integers  $a$  and  $b$ ,  $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$  if and only if  $\gcd(a, b) = 1$ .

*Proof.* First, assume that  $\gcd(a, b) = 1$ . Note that 1 has order  $a$  in  $\mathbb{Z}_a$  and 1 has order  $b$  in  $\mathbb{Z}_b$ . By Proposition 4.43, the order of  $(1, 1)$  in  $\mathbb{Z}_a \times \mathbb{Z}_b$  is

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)} = ab.$$

Since the cardinality of  $\mathbb{Z}_a \times \mathbb{Z}_b$  is  $ab$ , we see that  $\mathbb{Z}_a \times \mathbb{Z}_b$  is cyclic. Hence,  $\mathbb{Z}_a \times \mathbb{Z}_b$  is isomorphic to  $\mathbb{Z}_{ab}$ .

Now assume that  $\gcd(a, b) > 1$  and consider  $(x, y) \in \mathbb{Z}_a \times \mathbb{Z}_b$ , arbitrary. We first note that  $\text{ord}(x)$  is a divisor of  $a$  and that  $\text{ord}(y)$  is a divisor of  $b$ . In particular, we can let  $k_1$  and  $k_2$  be the integers for which  $\text{ord}(x) \cdot k_1 = a$  and  $\text{ord}(y) \cdot k_2 = b$ . We can also let  $\ell_1$  and  $\ell_2$  be the integers for which

$$\text{lcm}(a, b) = a\ell_1 = \text{ord}(x)k_1\ell_1$$

and

$$\text{lcm}(a, b) = b\ell_2 = \text{ord}(y)k_2\ell_2.$$

It follows that

$$\text{lcm}(\text{ord}(x), \text{ord}(y)) \leq \text{lcm}(a, b),$$

and thus that

$$\begin{aligned} \text{ord}((x, y)) &= \text{ord}((x, e_H) \cdot (e_G, y)) \\ &= \text{lcm}(\text{ord}(x), \text{ord}(y)) \\ &\leq \text{lcm}(a, b) \\ &= \frac{ab}{\gcd(a, b)} \\ &< ab. \end{aligned}$$

Hence, no element of  $\mathbb{Z}_a \times \mathbb{Z}_b$  generates  $\mathbb{Z}_a \times \mathbb{Z}_b$ , so  $\mathbb{Z}_a \times \mathbb{Z}_b$  is not cyclic. It is therefore not isomorphic to  $\mathbb{Z}_{ab}$  since  $\mathbb{Z}_{ab}$  is cyclic.  $\square$

**Corollary 7.5.** Let  $G$  be a cyclic group of order  $n$  and let

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

be the prime factorization of  $n$ , where  $\{p_1, p_2, \dots, p_k\}$  is a set of distinct primes and each  $a_j$  is a positive integer. Then

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}.$$

The following factorization theorem will be of use to us later.

**Theorem 7.6.** Suppose  $H$  and  $K$  are subgroups of a group  $G$  with the properties that  $H \cap K = \{e_G\}$ ,  $G = \{hk : h \in H, k \in K\}$ , and  $hk = kh$  for all  $h \in H$  and  $k \in K$ . Then  $G \cong H \times K$ . Moreover, the natural mapping  $(h, k) \mapsto hk$ ,  $H \times K \rightarrow G$ , is a witnessing isomorphism.

*Proof.* Define  $\varphi : H \times K \rightarrow G$  by  $\varphi(h, k) = hk$ . Note that  $\varphi$  is a surjection by the hypothesis.

To see that  $\varphi$  is a homomorphism, let  $(h_1, k_1), (h_2, k_2) \in H \times K$  be arbitrary. Then note that

$$\varphi((h_1, k_1) \cdot (h_2, k_2)) = \varphi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \varphi(h_1, k_1) \cdot \varphi(h_2, k_2).$$

The last thing to show is that  $\varphi$  is injective. So suppose  $(h_1, k_1), (h_2, k_2) \in H \times K$  are such that  $\varphi(h_1, k_1) = \varphi(h_2, k_2)$ . Note that this asserts that  $h_1 k_1 = h_2 k_2$ , which can be rewritten as  $h_2^{-1} h_1 = k_2 k_1^{-1}$ . Since  $h_2^{-1} h_1 \in H$ ,  $h_2^{-1} h_1 = k_2 k_1^{-1} \in K$ , and  $H \cap K = \{e_G\}$ ,  $h_2^{-1} h_1 = k_2 k_1^{-1} = e_G$ . It follows that  $h_1 = h_2$  and that  $k_2 = k_1$ . Therefore,  $(h_1, k_1) = (h_2, k_2)$ , and the proof is complete.  $\square$

In the context of Abelian groups (though it is also true in a slightly more general context) we can extend this result in a natural way to a finite number of factors. Before stating the extension, let's overload some notation. For a group  $(G, \cdot)$  and  $A \subseteq G$ , let  $\langle A \rangle = \bigcap \mathcal{H}_A$ , where  $\mathcal{H}_A$  is the set of all subgroups of  $G$  that contain  $A$ . In other words,  $\langle A \rangle$  is the smallest subgroup of  $G$  which contains every element of  $A$ .

**Corollary 7.7.** Suppose  $G$  is an Abelian group with subgroups  $H_1, H_2, \dots, H_n$  with the properties that  $H_j \cap H_k = \{e_G\}$  for  $j \neq k$ , where

$$\tilde{H}_k = \left\langle \bigcup \{H_\ell : 1 \leq \ell \leq n, \ell \neq j\} \right\rangle,$$

and

$$G = \{h_1 h_2 \cdots h_n : h_1 \in H_1, h_2 \in H_2, \dots, h_n \in H_n\}.$$

Then

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

Before proving the corollary, we comment that the condition on the  $H_j$  in the hypothesis is, in general, necessary. Indeed, consider  $G = \mathbb{Z}_2 \times \mathbb{Z}_2$  where the elements are written as strings and let  $H_1 = \{00, 01\}$ ,  $H_2 = \{00, 10\}$ , and  $H_3 = \{00, 11\}$ . Note that each  $H_j$  is a subgroup of  $G$  and that  $H_j \cap H_k = \{00\}$  for  $j \neq k$ . However,  $G \not\cong H_1 \times H_2 \times H_3$  since  $H_1 \times H_2 \times H_3$  has order 8. The primary issue in this example is that the elements of  $H_2 \cup H_3$  generate the entire group. Note that  $10 + 11 = 01$  and so

$$\langle H_2 \cup H_3 \rangle = H_2 + H_3 = \{00, 10, 11, 01\} = G.$$

So these  $H_j$  do not satisfy the hypotheses of Corollary 7.7.

*Proof of Corollary 7.7.* We induct on the number of factors  $n$ . Note that, when  $n = 2$ , the result becomes a direct application of Theorem 7.6. So suppose the result holds for every  $n \leq k$  where  $k \geq 2$  and suppose  $H_1, H_2, \dots, H_k, H_{k+1}$  are as in the hypotheses.

Let

$$K = \langle H_1 \cup H_2 \cup \dots \cup H_k \rangle$$

and notice that  $K \cap H_{k+1} = \{e_G\}$  by the hypothesis. Since every element of  $G$  can be written as  $h_1 h_2 \dots h_k h_{k+1}$  where  $h_j \in H_j$  by the hypothesis and  $h_1 h_2 \dots h_k \in K$ ,

$$G = \{yh_{k+1} : y \in K, h_{k+1} \in H_{k+1}\},$$

and so Theorem 7.6 applies to assert that

$$G \cong K \times H_{k+1}.$$

So, to finish the proof, we need only show that

$$K \cong H_1 \times H_2 \times \dots \times H_k.$$

By the hypotheses in the statement of the corollary and the inductive hypothesis, it suffices to show that

$$K = \{h_1 h_2 \dots h_k : h_1 \in H_1, h_2 \in H_2, \dots, h_k \in H_k\}.$$

Indeed, note that, for any  $1 \leq j \leq k$ ,

$$H_j \cap \left\langle \bigcup\{H_\ell : 1 \leq \ell \leq k, \ell \neq j\} \right\rangle \subseteq H_j \cap \left\langle \bigcup\{H_\ell : 1 \leq \ell \leq k+1, \ell \neq j\} \right\rangle = \{e_G\},$$

so the subgroups  $H_1, H_2, \dots, H_k$  satisfy the requisite condition.

Now, let

$$K' = \{h_1 h_2 \dots h_k : h_1 \in H_1, h_2 \in H_2, \dots, h_k \in H_k\}$$

and note that, since  $G$  is Abelian,  $K'$  is a subgroup of  $G$ . Note also that  $K \subseteq K'$  since

$$H_1 \cup H_2 \cup \dots \cup H_k \subseteq K'$$

and  $K'$  is a subgroup of  $G$ . On the other hand, if  $h_1 h_2 \dots h_k \in K'$ , note that  $h_j \in K$  for each  $j = 1, 2, \dots, k$ , and so  $h_1 h_2 \dots h_k \in K$ . That is,  $K' \subseteq K$ .

Finally, as

$$K = \{h_1 h_2 \dots h_k : h_1 \in H_1, h_2 \in H_2, \dots, h_k \in H_k\}$$

and the requisite conditions hold for  $H_1, H_2, \dots, H_k$ , the inductive hypothesis applies to guarantee that

$$K \cong H_1 \times H_2 \times \dots \times H_k.$$

Therefore,

$$G \cong K \times H_{k+1} \cong H_1 \times H_2 \times \dots \times H_k \times H_{k+1},$$

finishing the proof.  $\square$

To elaborate a bit more on the condition on the subgroups in the statement of Corollary 7.7, consider  $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ . Considering the way the group is defined, we can verify that the subgroups defined by  $H_1 = \{000, 001\}$ ,  $H_2 = \{000, 010\}$ , and  $H_3 = \{000, 100\}$  meet the criteria in the corollary. As an example, note that  $\langle H_1 \cup H_2 \rangle = \{000, 001, 010, 011\}$ . Then  $\langle H_1 \cup H_2 \rangle \cap H_3 = \{000\}$ . It may help here to think about  $\langle H_1 \cup H_2 \rangle$  as the *span* of  $\{001, 010\}$ . In this way, 011 is a *linear combination* of 001 and 010.

By way of contrast, suppose we randomly reach in and grab three distinct elements of  $G$  of order 2, say 111, 100, and 011. Let  $K_1 = \{000, 111\}$ ,  $K_2 = \{000, 100\}$ , and  $K_3 = \{000, 011\}$ . Note that these are all subgroups of  $G$  and that  $K_j \cap K_\ell = \{000\}$  for  $j \neq \ell$ . However,  $111 \in K_1 \cap \langle K_2 \cup K_3 \rangle$ , so this choice  $\{111, 100, 011\}$  of elements, unlike  $\{001, 010, 100\}$ , doesn't form a *basis* for  $G$ . In a sense,  $\{001, 010, 100\}$  is *linear independent* whereas  $\{111, 100, 011\}$  is not.

Ultimately, without having some intimate knowledge of a given group  $G$  like we have in the particular example  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ , finding the right subgroups that satisfy the condition given in Corollary 7.7 can be challenging, if not impossible.

We end the present discussion on direct products by noting that the direct product construction is not the only way to assign a group structure to a Cartesian product of groups. We include the following example as just a hint of what is possible with Cartesian products, in general.

**Example 7.8.** Consider  $(\mathbb{R}^*, \cdot)$  and  $(\mathbb{R}, +)$ . Define  $*$  on the Cartesian product  $\mathbb{R}^* \times \mathbb{R}$  by the rule

$$(a, b) * (c, d) = (ac, ad + b).$$

Then  $(\mathbb{R}^* \times \mathbb{R}, *)$  is a non-Abelian group, which we prove below. Note then that the direct product  $\mathbb{R}^* \times \mathbb{R}$  cannot be isomorphic to  $(\mathbb{R}^* \times \mathbb{R}, *)$  since the direct product  $\mathbb{R}^* \times \mathbb{R}$  is Abelian.

*Proof.* We prove that  $(\mathbb{R}^* \times \mathbb{R}, *)$  is a non-Abelian group.

To address associativity, consider  $(u, v), (w, x), (y, z) \in \mathbb{R}^* \times \mathbb{R}$ . Then note that

$$\begin{aligned} ((u, v) * (w, x)) * (y, z) &= (uw, ux + v) * (y, z) \\ &= (uwy, uwz + ux + v) \end{aligned}$$

and that

$$\begin{aligned} (u, v) * ((w, x) * (y, z)) &= (u, v) * (wy, wz + x) \\ &= (uwy, u(wz + x) + v) \\ &= (uwy, uwz + ux + v). \end{aligned}$$

Hence,  $*$  is associative.

Now we check that  $(1, 0)$  serves as the identity for  $*$ . Note that

$$(1, 0) * (x, y) = (x, 1 \cdot y + 0) = (x, y)$$

and that

$$(x, y) * (1, 0) = (x, x \cdot 0 + y) = (x, y).$$

For inverses, consider  $(x, y) \in \mathbb{R}^* \times \mathbb{R}$  and consider  $(\frac{1}{x}, -\frac{y}{x})$ . Note that  $\frac{1}{x} \in \mathbb{R}^*$  since  $x \neq 0$  and so  $(\frac{1}{x}, -\frac{y}{x}) \in \mathbb{R}^* \times \mathbb{R}$ . Then, observe that

$$(x, y) * \left(\frac{1}{x}, -\frac{y}{x}\right) = (1, -y + y) = (1, 0)$$

and that

$$\left(\frac{1}{x}, -\frac{y}{x}\right) * (x, y) = \left(1, \frac{y}{x} - \frac{y}{x}\right) = (1, 0).$$

Conclusively,  $(\mathbb{R}^* \times \mathbb{R}, *)$  is a group. The last thing to show is that it is not Abelian. So consider  $(2, 0)$  and  $(1, 2)$ . Note that

$$(2, 0) * (1, 2) = (2, 4)$$

and that

$$(1, 2) * (2, 0) = (2, 2).$$

Thus,  $(2, 0) * (1, 2) \neq (1, 2) * (2, 0)$ .  $\square$

## 7.2 Normal Subgroups and Quotient Groups

### 7.2.1 Normal Subgroups

**Definition 7.9.** A subgroup  $H$  of a group  $(G, \cdot)$  is said to be *normal* if, for every  $g \in G$  and every  $h \in H$ ,  $ghg^{-1} \in H$ .

**Proposition 7.10.** If  $(G, \cdot)$  is an Abelian group, then every subgroup of  $G$  is normal.

**Exercise 7.4.** Suppose  $(G, *)$  and  $(H, \circ)$  are groups. Show that the isomorphic copy of  $G$  in  $G \times H$  obtained via  $g \mapsto (g, e_H)$ ,  $G \rightarrow G \times H$ , and that the isomorphic copy of  $H$  in  $G \times H$  obtained via  $h \mapsto (e_G, h)$ ,  $H \rightarrow G \times H$ , are both normal subgroups of  $G \times H$ .

**Proposition 7.11.** Let  $(G, *)$  and  $(H, \circ)$  be groups and suppose that  $\varphi : G \rightarrow H$  is a homomorphism. Then  $\ker(\varphi)$  is a normal subgroup of  $G$ .

*Proof.* By Exercise 4.18, we have that  $\ker(\varphi)$  is a subgroup of  $G$ , so we need only show it's a normal subgroup. So let  $g \in G$  be arbitrary and  $h \in \ker(\varphi)$ . Note that

$$\varphi(g * h * g^{-1}) = \varphi(g) \circ \varphi(h) \circ \varphi(g)^{-1} = \varphi(g) \circ e_H \circ \varphi(g)^{-1} = e_H.$$

That is,  $g * h * g^{-1} \in \ker(\varphi)$ , and the proof is complete.  $\square$

**Example 7.12.** By Exercise 5.3 and Proposition 7.11, we see that  $A_n$  is a normal subgroup of  $S_n$  for each  $n \in \mathbb{N}$ .

**Example 7.13.** Consider the symmetric group  $S_3$  and the subgroup  $H = \{(), (1 2)\}$ . Then  $H$  is not a normal subgroup of  $S_3$ . Indeed, note that

$$\begin{aligned} (1 3)(1 2)(1 3)^{-1} &= (1 3)(1 2)(1 3) \\ &= (2 3) \notin H. \end{aligned}$$

Note that, if  $K$  is a subgroup of  $H$ , and  $H$  is a subgroup of  $G$ , then  $K$  is a subgroup of  $G$ . Introducing the modifier of normality breaks this transitivity, in general, however.

**Example 7.14.** There is a group  $G$  in which we have a normal subgroup  $H$  of  $G$  and a normal subgroup  $K$  of  $H$  for which  $K$  is not a normal subgroup of  $G$ . Note here that

- $H$  being a normal subgroup of  $G$  means that  $\forall g \in G \forall h \in H (ghg^{-1} \in H)$  and that
- $K$  being a normal subgroup of  $H$  means that  $\forall h \in H \forall k \in K (hkh^{-1} \in K)$ .

For  $K$  to be normal in  $G$ , we would need that, for every  $g \in G$  and every  $k \in K$ ,  $gkg^{-1} \in K$ .

Consider  $D_4$  and, using the notation of §5.2, we write

$$D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}.$$

Let  $H = \{1, r^2, s, r^2s\}$  and  $K = \{1, s\}$ . To show that  $H$  is a subgroup of  $D_4$ , we refer to its Cayley table, where some computations are aided by the use of Exercise 5.5:

	1	$r^2$	$s$	$r^2s$
1	1	$r^2$	$s$	$r^2s$
$r^2$	$r^2$	1	$r^2s$	$s$
$s$	$s$	$r^2s$	1	$r^2$
$r^2s$	$r^2s$	$s$	$r^2$	1

Since  $[G : H] = \frac{|G|}{|H|} = 2$ , we see that  $H$  is a normal subgroup of  $G$  by Exercise 6.4.

Note also that  $K$  is clearly a subgroup of  $H$  and that  $[H : K] = 2$ . Again, by Exercise 6.4,  $K$  is a normal subgroup of  $H$ .

However,  $K$  is not a normal subgroup of  $D_4$ . Indeed, note that

$$rsr^{-1} = r^2s \notin K.$$

**Exercise 7.5.** For a group  $G$ , let  $g \in G$  and define  $\varphi : G \rightarrow G$  by the rule  $\varphi(x) = gxg^{-1}$ . Show that  $\varphi$  is an isomorphism.

**Exercise 7.6.** Suppose  $G$  is a group and that  $H$  is a unique subgroup of  $G$  with order  $k$ , for some positive integer  $k$ . Show that  $H$  is a normal subgroup of  $G$ .

## 7.2.2 Quotient Groups

When dealing with a normal subgroup, we can turn the set of cosets into a group in its own right.

**Definition 7.15.** Suppose  $N$  is a normal subgroup of a group  $(G, \cdot)$ . Then we can define a binary operation on the cosets of  $N$  in the following way:

$$(aN) \cdot (bN) = abN.$$

As will be shown below, this turns the set of cosets into a group, which we will denote by  $G/N$ , and refer to as a *quotient group* or a *factor group*.

**Proposition 7.16.** The set of cosets of a normal subgroup  $N$  of a group  $(G, \cdot)$  with the binary operation defined in Definition 7.15 forms a group.

*Proof.* We first show that the binary operation is well-defined. So suppose we have  $a, b, x, y \in G$  such that  $aN = xN$  and  $bN = yN$ . We will show that  $abN = xyN$ . To accomplish this, we will show that  $xy \in abN$ . First, note that, since  $aN = xN$ ,  $x \in aN$ . So there are  $n \in N$  for which  $x = an$ . Note then that  $a^{-1}x = n \in N$ . By normality,  $y^{-1}a^{-1}xy = y^{-1}ny \in N$ . So let  $m = y^{-1}ny$  and consider the fact that

$$y^{-1}a^{-1}xy = m \implies a^{-1}xy = ym \in yN = bN.$$

Since  $ym = bN$ , there is some  $\ell \in N$  for which  $ym = b\ell$ . So now we have that  $a^{-1}xy = b\ell$ . Finally, this yields that  $xy = abl \in abN$ .

For associativity, note that  $(aN \cdot bN) \cdot cN = abN \cdot cN = abcN$  and that  $aN \cdot (bN \cdot cN) = aN \cdot bcN = abcN$ .

For identity, note that  $N = e_G N$  where  $e_G$  is the identity of  $G$  serves as the identity.

Lastly, check that  $g^{-1}N$  serves as the inverse of  $gN$ , for any  $g \in G$ .  $\square$

For the group  $(\mathbb{Z}, +)$  and a subgroup  $n\mathbb{Z}$ , where  $n > 1$ , since  $\mathbb{Z}$  is Abelian,  $n\mathbb{Z}$  is a normal subgroup. Moreover, a straightforward argument verifies that the quotient group  $\mathbb{Z}/n\mathbb{Z}$  and  $\mathbb{Z}_n$  are isomorphic.

**Example 7.17.** The normality condition in Proposition 7.16 is necessary. Consider the symmetric group  $S_3$  and the subgroup  $H = \{(), (1 2)\}$ . The set of left-cosets and right-cosets are not equal, as demonstrated in Example 6.2. Even if we consider only the set of left-cosets, the operation defined in Definition 7.15 is not valid. Consider for example, the cosets  $H = (1 2)H$  and  $(1 3)H$ . In one representation,  $H \cdot (1 3)H = (1 3)H$ . In another representation,

$$(1 2)H \cdot (1 3)H = (1 2)(1 3)H = (1 3 2)H \neq (1 3)H.$$

**Definition 7.18.** For a group  $(G, \cdot)$  and a normal subgroup  $N$  of  $G$ , we define the *canonical homomorphism*  $\varphi : G \rightarrow G/N$  by  $\varphi(g) = gN$ .

**Sanity Check 7.7.** Verify that  $\varphi$  defined in Definition 7.18 is a homomorphism of groups.

Either by direct arguments or by appealing to the canonical homomorphism, it can be shown that the properties of being Abelian or cyclic are preserved by the formation of a quotient group.

**Remark.** Note that, by Proposition 4.27, if  $(G, \cdot)$  is an Abelian group and  $H$  is a (necessarily normal) subgroup of  $G$ , then  $G/H$  is an Abelian group.

Similarly, if  $(G, \cdot)$  is a cyclic group and  $H$  is a (necessarily normal) subgroup of  $G$ , then  $G/H$  is cyclic by Proposition 4.31.

However, quotient groups may gain properties that neither the parent group nor the generating normal subgroup have.

**Example 7.19.** Consider the symmetric group  $S_4$  and its alternating subgroup  $A_4$ . Note that  $S_4/A_4$  is isomorphic to  $(\mathbb{Z}_2, \oplus)$ , and hence cyclic (and consequently Abelian). However, neither  $S_4$  nor  $A_4$  are Abelian. Indeed, note that  $(1\ 2\ 3), (1\ 2\ 4) \in A_4$ . Then note that

$$(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$$

and that

$$(1\ 2\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3).$$

Hence,

$$(1\ 2\ 3)(1\ 2\ 4) \neq (1\ 2\ 4)(1\ 2\ 3),$$

establishing that neither  $A_4$  nor  $S_4$  are Abelian.

It may be tempting to think of the forming of factor groups as a sort of division and that, for a group  $G$  and a normal subgroup  $N$ ,  $G \cong (G/N) \times N$ . However, this is generally not the case.

**Example 7.20.** Recall again  $D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$  and  $R = \{1, r, r^2, r^3\}$ . We know that, by Exercise 5.5,  $R$  is a normal subgroup of  $D_4$ . We also know that

$$[D_4 : R] = \frac{|D_4|}{|R|} = \frac{8}{4} = 2.$$

It follows that  $D_4/R$  is a group of order 2, and hence  $D_4/R \cong \mathbb{Z}_2$ . Note that  $R$  and  $D_4/R$  are Abelian, so  $(D_4/R) \times R$  is an Abelian group. Hence, since  $D_4$  is not Abelian,  $D_4 \not\cong (D_4/R) \times R$ .

### 7.2.3 Isomorphism Theorems

**Theorem 7.21** (The First Isomorphism Theorem). Suppose  $\varphi : G \rightarrow H$  is a surjective homomorphism and that  $K = \ker(\varphi)$ . Let  $\psi : G \rightarrow G/K$  be the canonical homomorphism. Then there exist a unique isomorphism  $\vartheta : G/K \rightarrow H$  such that  $\varphi = \vartheta \circ \psi$ .

The content of The First Isomorphism Theorem can be summarized in the *commuting diagram* Figure 4.

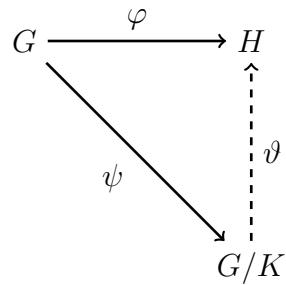


Figure 4: Commuting Diagram for The First Isomorphism Theorem

*Proof.* Let  $\varphi : G \rightarrow H$  and  $\psi : G \rightarrow G/K$  be as in the hypothesis. Define  $\vartheta : G/K \rightarrow H$  by the rule

$$\vartheta(gK) = \varphi(g).$$

We first verify that  $\vartheta$  is well-defined. So consider  $gK, hK \in G/K$  such that  $gK = hK$ . By Lemma 6.3,  $h^{-1}g \in K = \ker(\varphi)$ . That is,

$$e_H = \varphi(h^{-1}g) = \varphi(h)^{-1}\varphi(g).$$

It follows that

$$\vartheta(hK) = \varphi(h) = \varphi(g) = \vartheta(gK).$$

Hence,  $\vartheta$  is well-defined.

To see that  $\vartheta$  is a homomorphism, let  $gK, hK \in G/K$  and note that

$$\begin{aligned} \vartheta(gK)\vartheta(hK) &= \varphi(g)\varphi(h) \\ &= \varphi(gh) \\ &= \vartheta(ghK) \\ &= \vartheta((gK)(hK)). \end{aligned}$$

Hence,  $\vartheta$  is a homomorphism.

We know show that  $\vartheta$  is injective. Suppose  $gK, hK \in G/K$  are such that  $\vartheta(gK) = \vartheta(hK)$ . It follows that

$$\begin{aligned} \varphi(g) = \varphi(h) &\implies e_H = \varphi(g)^{-1}\varphi(h) = \varphi(g^{-1}h) \\ &\implies g^{-1}h \in \ker(\varphi) = K. \end{aligned}$$

By Lemma 6.3,  $gK = hK$ . Hence,  $\vartheta$  is injective.

To see that  $\vartheta$  is surjective, let  $h \in H$ . Since  $\varphi$  was assumed to be surjective, there is some  $g \in G$  for which  $\varphi(g) = h$ . Note then that  $gK \in G/K$  and  $\vartheta(gK) = \varphi(g) = h$ . Thus,  $\vartheta$  is surjective.

Observe that, for any  $g \in G$ ,

$$\vartheta \circ \psi(g) = \vartheta(gK) = \varphi(g).$$

That is,  $\varphi = \vartheta \circ \psi$ .

The final thing to prove is that  $\vartheta$  is the unique isomorphism with the specified properties. So supposed that  $\lambda : G/K \rightarrow H$  is an isomorphism such that  $\varphi = \lambda \circ \psi$ . Let  $gK \in G/K$  be arbitrary and note that

$$\lambda(gK) = \lambda(\psi(g)) = \lambda \circ \psi(g) = \varphi(g) = \vartheta(gK).$$

Since  $\lambda(gK) = \vartheta(gK)$  for every  $gK \in G/K$ , we see that  $\lambda = \vartheta$ , establishing the uniqueness of  $\vartheta$ .  $\square$

We provide some examples here elaborating on how The First Isomorphism Theorem can be used to capture certain quotient groups as familiar groups.

**Example 7.22.** Consider the group  $(\mathbb{R}, +)$  and the subgroup  $\mathbb{Z}$  of  $\mathbb{R}$ . Since  $\mathbb{R}$  is Abelian,  $\mathbb{Z}$  is a normal subgroup of  $\mathbb{R}$ . Now consider the map  $\varphi : \mathbb{R} \rightarrow \mathbb{S}^1$  defined by

$$\varphi(t) = \cos(2\pi t) + i \sin(2\pi t)$$

where  $\mathbb{S}^1$  is the circle group defined in Example 4.44. It can be shown that  $\varphi$  is a surjective homomorphism. Note also that

$$\ker(\varphi) = \mathbb{Z}.$$

Then, by The First Isomorphism Theorem,  $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$ .

**Sanity Check 7.8.** Verify that the  $\varphi$  defined in Example 7.22 is a surjective homomorphism with  $\ker(\varphi) = \mathbb{Z}$ .

In the next example, we will demonstrate one method for finding ideas for homomorphisms yielding a given normal subgroup as the kernel (other than the canonical homomorphism).

**Example 7.23.** Let

$$G = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} : x, y \in \mathbb{C}, x \neq 0 \right\}.$$

Note that the identity matrix is an element of  $G$ , that

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ax & ay + b \\ 0 & 1 \end{bmatrix} \in G,$$

and that

$$\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{bmatrix} \in G.$$

Hence,  $G$  is a subgroup of  $\mathrm{GL}(2, \mathbb{C})$ .

Let

$$H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{C} \right\}.$$

A routine computation shows that  $H$  is a normal subgroup of  $G$ .

To begin to understand the quotient group, we look into the left-coset relation. That is, what properties must two matrices have to guarantee their membership in the same left-coset? Again, recall Lemma 6.3 and note that

$$\begin{aligned} \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}^{-1} &= \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} \frac{a}{x} & \frac{bx-ay}{x} \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Then, observe that, for

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}^{-1} \in H,$$

we would need  $x = a$ . From here, we can conclude that

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} H = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} H.$$

Note that we chose to use the zero in the top-right entry as the canonical representative since it can be verified that

$$D := \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{C}^* \right\}$$

is a group.

Finally, define  $\varphi : G \rightarrow D$  by the rule

$$\varphi \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}.$$

As you will be asked to check,  $\varphi$  is a surjective homomorphism and  $\ker(\varphi) = H$ . Therefore, by The First Isomorphism Theorem,  $G/H \cong D$ .

**Exercise 7.9.** Refer to Example 7.23.

- (a) Show that  $H$  is a normal subgroup of  $G$ .
- (b) Show that  $D$  is a subgroup of  $\mathrm{GL}(2, \mathbb{C})$ .
- (c) Verify that  $\varphi$  is a surjective homomorphism with  $\ker(\varphi) = H$ .

**Remark.** In Example 7.23, note that

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} H = \begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix} H,$$

as well. In such a way,

$$\begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix}$$

can serve as a canonical representative for the coset

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} H,$$

but the set

$$\left\{ \begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{C}^* \right\}$$

of coset representatives is not a subgroup of  $G$ , so we can't naturally generate a homomorphism using these choices.

**Exercise 7.10.** Let  $(G, \cdot)$  and  $(H, \cdot)$  be groups. Let  $\hat{G} = \{(g, e_H) : g \in G\}$  and  $\hat{H} = \{(e_G, h) : h \in H\}$ . Verify that both  $\hat{G}$  and  $\hat{H}$  are normal subgroups of  $G \times H$  and show that  $(G \times H)/\hat{G} \cong H$  and that  $(G \times H)/\hat{H} \cong G$ .

**Definition 7.24.** Let  $(G, *)$  be a group and  $A, B \subseteq G$ . Then we define

$$A * B = \{a * b : a \in A, b \in B\}.$$

**Exercise 7.11.** Suppose that  $H$  and  $K$  are subgroups of a group  $(G, \cdot)$ . Show that

$$H \cup K \subseteq HK.$$

**Theorem 7.25** (The Second Isomorphism Theorem). Suppose that  $H$  is a (not necessarily normal) subgroup of a group  $(G, *)$  and that  $N$  is a normal subgroup of  $G$ . Then  $H * N$  is a subgroup of  $G$ ,  $H \cap N$  is a normal subgroup of  $H$ , and

$$H/(H \cap N) \cong (H * N)/N.$$

*Proof.* For notational convenience, we treat the group  $G$  as a multiplicative group. We start by showing that  $HN$  is a subgroup of  $G$ . First note that  $e_G \in H \cap N$  so  $e_G = e_G \cdot e_G \in HN$ .

Now consider  $h_1n_1, h_2n_2 \in HN$  where  $h_1, h_2 \in H$  and  $n_1, n_2 \in N$ . Note that

$$h_1n_1h_2n_2 = h_1(h_2h_2^{-1})n_1h_2n_2 = h_1h_2(h_2^{-1}n_1h_2)n_2.$$

Since  $N$  is a normal subgroup of  $G$ ,  $h_2^{-1}n_1h_2 \in N$ , and so we have that  $h_1h_2 \in H$  and  $(h_2^{-1}n_1h_2)n_2 \in N$ . That is,  $h_1n_1h_2n_2 \in HN$ .

For the fact that the inverse of every element of  $HN$  is a member of  $HN$ , let  $hn \in HN$  where  $h \in H$  and  $n \in N$ . Note that

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}hn^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

Again, since  $N$  is a normal subgroup of  $G$ ,  $hn^{-1}h^{-1} \in N$  and so  $(hn)^{-1} \in HN$ .

We now show that  $H \cap N$  is a normal subgroup of  $H$ . By Exercise 4.13, we know that  $H \cap N$  is a subgroup of  $G$ , and since  $H \cap N \subseteq H$ , we see that  $H \cap N$  is a subgroup of  $H$ . So we need only show it is a normal subgroup of  $H$ . So let  $h \in H$  and  $n \in H \cap N$  be arbitrary. Since  $N$  is a normal subgroup of  $G$ , we know that  $hnh^{-1} \in N$ . Note also that  $hnh^{-1} \in H$  since  $h, n \in H$ . Hence,  $hnh^{-1} \in H \cap N$ , establishing that  $H \cap N$  is a normal subgroup of  $H$ .

Finally, define  $\varphi : H \rightarrow (HN)/N$  by the rule  $\varphi(h) = hN$ . Note that each coset of  $(HN)/N$  is of the form  $hnN$  where  $h \in H$  and  $n \in N$ . Also, note that  $hnN = hN$ . So we see that  $\varphi$  is a surjection. Note also that  $\varphi$  is a homomorphism since

$$\varphi(h_1)\varphi(h_2) = (h_1N)(h_2N) = h_1h_2N = \varphi(h_1h_2).$$

Hence,  $\varphi$  is a surjective homomorphism.

Note that  $h \in \ker(\varphi)$  if and only if  $\varphi(h) = N$ . Moreover,  $\varphi(h) = hN = N$  holds if and only if  $h \in N$  by Lemma 6.3. So  $\ker(\varphi) = H \cap N$ , and so

$$H/(H \cap N) \cong (HN)/N$$

by The First Isomorphism Theorem. □

The normality of  $N$  in The Second Isomorphism Theorem is necessary to guarantee that  $H * N$  is a subgroup of  $G$ .

**Example 7.26.** Consider

$$D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

and let  $H = \{1, s\}$  and  $K = \{1, rs\}$ . Note that both  $H$  and  $K$  are subgroups of  $G$ , but neither one is a normal subgroup. Note also that

$$HK = \{1, s, rs, r^3\}$$

since  $srs = r^3$ . Then note that  $(r^3)^{-1} = r \notin HK$ . That is,  $HK$  is not a subgroup of  $D_4$ .

Under the assumption that  $N$  is a normal subgroup of a group  $G$  and  $H$  is a subgroup of  $G$ ,  $HN$  is actually the smallest subgroup of  $G$  containing both  $H$  and  $N$ .

**Proposition 7.27.** Suppose  $(G, *)$  is a group,  $N$  is a normal subgroup of  $G$ , and  $H$  is a (not necessarily normal) subgroup of  $G$ . Then  $H * N$  is the smallest subgroup of  $G$  containing  $H \cup N$ .

*Proof.* By Exercise 7.11, we know that  $H \cup N \subseteq H * N$ . By The Second Isomorphism Theorem,  $H * N$  is a subgroup of  $G$ . To see that it is the smallest, suppose  $K$  is a subgroup of  $G$  such that  $H \cup N \subseteq K$ . We show that  $H * N \subseteq K$ . So let  $h * n \in H * N$  be arbitrary, where  $h \in H$  and  $n \in N$ . Note that  $h \in K$  and  $n \in K$ . Since  $K$  is a subgroup of  $G$ ,  $h * n \in K$ . Since  $h * n$  was arbitrary, we see that  $H * N \subseteq K$ .  $\square$

With the established context, given a normal subgroup  $N$  of a group  $G$  and a subgroup  $H$  of  $G$ , we can see  $H \cap N$  as the largest subgroup contained in both  $H$  and  $N$  (kind of like a greatest common divisor), and  $HN$  as the smallest subgroup containing both  $H$  and  $N$  (kind of like a least common multiple). In this way, The Second Isomorphism Theorem can be loosely seen as a very abstract generalization of the familiar identity

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b),$$

for positive integers  $a$  and  $b$ .

**Example 7.28.** Consider the group  $\mathbb{Z}_{60}$  and note that  $\mathbb{Z}_{60}$  is Abelian, so all subgroups of  $\mathbb{Z}_{60}$  are normal. Observe that

$$\langle 10 \rangle = \{0, 10, 20, 30, 40, 50\}$$

and that

$$\langle 6 \rangle = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54\}.$$

Then

$$\langle 10 \rangle \cap \langle 6 \rangle = \{0, 30\} = \langle 30 \rangle.$$

To find  $\langle 10 \rangle + \langle 6 \rangle$ , we use a table:

	0	6	12	18	24	30	36	42	48	54
0	0	6	12	18	24	30	36	42	48	54
10	10	16	22	28	34	40	46	52	58	4
20	20	26	32	38	44	50	56	2	8	14
30	30	36	42	48	54	0	6	12	18	24
40	40	46	52	58	4	10	16	22	28	34
50	50	56	2	8	14	20	26	32	38	44

It follows that  $\langle 10 \rangle + \langle 6 \rangle = \langle 2 \rangle$ .

By The Second Isomorphism Theorem, we see that

$$\langle 10 \rangle / \langle 30 \rangle \cong \langle 2 \rangle / \langle 6 \rangle \text{ and } \langle 6 \rangle / \langle 30 \rangle \cong \langle 2 \rangle / \langle 10 \rangle.$$

If we consider orders,  $|\langle 10 \rangle| = 6$ ,  $|\langle 6 \rangle| = 10$ ,  $|\langle 30 \rangle| = 2 = \gcd(6, 10)$ , and  $|\langle 2 \rangle| = 30 = \text{lcm}(6, 10)$ . Then isolating one of the congruences above and substituting in the corresponding equation involving the orders, we have that

$$\frac{|\langle 10 \rangle|}{|\langle 30 \rangle|} = \frac{|\langle 2 \rangle|}{|\langle 6 \rangle|}$$

$$\frac{6}{\gcd(6, 10)} = \frac{\text{lcm}(6, 10)}{10},$$

which provides the equation

$$6 \cdot 10 = \gcd(6, 10) \cdot \text{lcm}(6, 10) = 2 \cdot 30.$$

We end our discussion of isomorphism theorems with one more application of The Second Isomorphism Theorem.

**Definition 7.29.** A group  $G$  is said to be *metabelian* if there exists an Abelian normal subgroup  $N$  for which  $G/N$  is also Abelian.

**Exercise 7.12.** Refer to Example 7.23 and show that  $G$  is a metabelian group which is not Abelian using  $H$  as the desired Abelian normal subgroup.

**Proposition 7.30.** Every subgroup of a metabelian group is metabelian.

*Proof.* Let  $G$  be a metabelian group and let  $H$  be a subgroup of  $G$ . Since  $G$  is metabelian, we can let  $N$  be an Abelian normal subgroup of  $G$  with the property that  $G/N$  is Abelian. Note then that  $H \cap N$  is an Abelian normal subgroup of  $H$ .

Since  $HN$  is a subgroup of  $G$ ,  $(HN)/N$  is a subgroup of  $G/N$ . Hence,  $(HN)/N$  is Abelian. By The Second Isomorphism Theorem,  $H/(H \cap N) \cong (HN)/N$ , and so  $H/(H \cap N)$  is Abelian.

Therefore,  $H$  is metabelian. □

## 8 Classifying Finite Abelian Groups

Recall that the direct product of Abelian groups is an Abelian group. So any group of the form

$$G = \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}},$$

where each  $p_j$  is a prime number and  $a_j$  is a positive integer, is a finite Abelian group. Also note that the group  $G$  is cyclic if and only if the primes  $p_j$  are all distinct by the proof of Theorem 7.4. In particular, part of the proof of Theorem 7.4 shows that, if  $a$  and  $b$  are positive integers with a common factor, then  $\mathbb{Z}_a \times \mathbb{Z}_b$  is not cyclic. The goal of this section is to prove that every finite Abelian group is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}},$$

where each  $p_j$  is a prime number and  $a_j$  is a positive integer.

**Lemma 8.1.** Suppose  $G$  is a finite Abelian group and that  $p$  is a prime which divides the order of  $G$ . Then  $G$  has an element of order  $p$ .

*Proof.* We proceed by induction on the order of  $G$ .

If  $|G| = 1$ , there is nothing to show since no prime  $p$  divides 1. Hence, the statement of the lemma holds trivially in this case.

Now suppose  $k \geq 1$  and that, for any group  $H$  with  $|H| \leq k$  and any prime  $p$  which divides  $k$ ,  $H$  has an element of order  $p$ . Suppose  $G$  is an Abelian group of order  $k + 1$  and suppose  $p$  is a prime which divides  $k + 1$ . We will proceed by cases.

First, suppose  $G$  has no proper nontrivial subgroups. From here it follows that  $G$  must be a cyclic group of finite order, in which case  $p = k + 1$  and hence any generator of  $G$  has order  $p$ .

Now, suppose  $G$  has a proper nontrivial subgroup  $H$ . Note that  $1 < |H| < |G| = k + 1$ , which means that  $|H| \leq k$ .

If  $p$  divides  $|H|$ , then the inductive hypothesis applies to guarantee the existence of an element  $h \in H$  with order  $p$ . Note that the order of  $h$  in  $G$  is also  $p$ , and so  $G$  has an element of order  $p$ .

Otherwise,  $p$  does not divide  $|H|$ . Since  $G$  is Abelian,  $H$  is a normal subgroup of  $G$ , and so

$$|G| = |H| \cdot [G : H] = |H| \cdot |G/H|$$

by Lagrange's Theorem. Since  $p$  is prime and  $p$  divides  $|G|$  but doesn't divide  $|H|$ ,  $p$  must divide  $|G/H|$ . Since  $|H| > 1$ ,  $|G/H| < |G| = k + 1$ , which establishes that  $|G/H| \leq k$ . Hence, the inductive hypothesis applies to guarantee the existence of some  $gH \in G/H$  with order  $p$ . Since  $p \geq 2$ , by the definition of order, we see that  $gH \neq H$ , and so  $g \notin H$ . On the other hand,  $H = (gH)^p = g^pH$ , which implies that  $g^p \in H$ . Let  $m = |H|$  and note that, since  $p$  is prime and  $p$  does not divide  $m$ ,  $\gcd(m, p) = 1$ . By Bézout's Identity, we can let  $x$  and  $y$  be integers such that  $px + my = 1$ . Since  $g^p \in H$  and  $|H| = m$ , Corollary 6.7 guarantees that  $(g^m)^p = (g^p)^m = e_G$ .

Our final claim is that  $g^m$  has order  $p$ . By Lemma 4.36, the order of  $g^m$  must divide  $p$  since  $(g^m)^p = e_G$ . Hence, the order of  $g^m$  is either 1 or  $p$ , so we show that the order of  $g^m$  is not 1. Since the only element of order 1 in any group is the identity, we need only show that  $g^m \neq e_G$ . Note that

$$\begin{aligned} g &= g^{px+my} \\ &= g^{px}g^{my} \\ &= (g^p)^x(g^m)^y \end{aligned}$$

which implies that

$$(g^m)^{-y}g = (g^p)^x \in H.$$

Since  $g \notin H$ , it cannot be the case that  $g^m = 1$ . Therefore,  $g^m$  has order  $p$ .  $\square$

**Definition 8.2.** For a prime number  $p$ , we say that a group  $G$  is a  $p$ -group if every element of  $G$  has as its order some power of  $p$ .

For example, both  $\mathbb{Z}_9$  and  $\mathbb{Z}_3 \times \mathbb{Z}_3$  are 3-groups.

**Remark.** Note that any nontrivial  $p$ -group has an element of order  $p$ , in particular. Indeed, suppose  $G$  is a  $p$ -group and let  $g$  be a non-identity element. Then  $\text{ord}(g) = p^m$  for some positive integer  $m$ . Note then that

$$e_G = g^{p^m} = g^{p \cdot p^{m-1}} = \left(g^{p^{m-1}}\right)^p.$$

By the way the order is defined, we see that  $g^{p^{m-1}}$  is an element of order  $p$ .

**Exercise 8.1.** Show that every subgroup of a  $p$ -group is itself a  $p$ -group.

**Lemma 8.3.** The homomorphic image of a  $p$ -group is itself a  $p$ -group.

*Proof.* Let  $G$  be a  $p$ -group and  $\varphi : G \rightarrow H$  be a surjective homomorphism and let  $h \in H$  be arbitrary. Since  $\varphi$  is surjective, let  $g \in G$  be such that  $\varphi(g) = h$ . We now define  $\psi : \langle g \rangle \rightarrow \langle h \rangle$  by  $\psi(g^\alpha) = h^\alpha$ . Note that  $\psi$  is a homomorphism since

$$\psi(g^\alpha g^\beta) = \psi(g^{\alpha+\beta}) = h^{\alpha+\beta} = h^\alpha h^\beta = \psi(g^\alpha)\psi(g^\beta).$$

It is also immediate that  $\psi$  is surjective.

Now,  $\ker(\psi)$  is a subgroup of  $\langle g \rangle$  and  $|\langle g \rangle| = p^m$  for some nonnegative integer  $m$ . By Lagrange's Theorem, it must be the case that  $|\ker(\psi)| = p^k$  for some nonnegative integer  $k \leq m$ . By The First Isomorphism, we can conclude that

$$|\langle h \rangle| = \frac{|\langle g \rangle|}{|\ker \psi|} = \frac{p^m}{p^k} = p^{m-k}.$$

That is, the order of  $h$  is a power of  $p$ , and so  $H$  is a  $p$ -group.  $\square$

**Lemma 8.4.** A finite Abelian group  $G$  is a  $p$ -group if and only if the order of  $G$  is a power of  $p$ .

*Proof.* First, suppose that  $|G| = p^k$  for some positive integer  $k$ . By Lagrange's Theorem, the order of any element of  $G$  must divide  $p^k$ , and hence must be itself a power of  $p$ .

Otherwise, suppose  $|G|$  is not a power of  $p$ . It follows that  $|G|$  must have some other prime divisor,  $q$ . By Lemma 8.1,  $G$  must have an element of order  $q$ , which means that  $G$  is not a  $p$ -group.  $\square$

The main structural fact about  $p$ -groups (Lemma 8.7) is that they can be decomposed into a direct product of cyclic groups, where each factor has some power of  $p$  as its order. Before we move to prove this result, we start with some motivating examples. The main idea is to find an element of maximal order and prove that the cyclic group generated by that element of maximal order can be factored out of the group.

**Example 8.5.** If  $G$  is an Abelian group of order 4, then either  $G \cong \mathbb{Z}_4$  or  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ .

*Proof.* If  $G$  has an element of order 4, then  $G \cong \mathbb{Z}_4$ , and we're done. So suppose  $G$  has no element of order 4. Since the identity element is the only element of order 1 and the order of any element must divide the order of the group, we know that every non-identity element of  $G$  must have order 2. So we can write  $G = \{1, g_1, g_2, g_3\}$  where each  $g_j$  is an element of

order 2. Note that  $\langle g_1 \rangle \cong \mathbb{Z}_2$  and consider  $\langle g_2 \rangle$ . We claim that  $G \cong \langle g_1 \rangle \times \langle g_2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . Note that  $\langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$  and that, by the uniqueness of the identity and the uniqueness of inverses, it must be the case that  $g_1 g_2 = g_3$ . It is thus straightforward to verify that the mapping  $(g_1^p, g_2^q) \mapsto g_1^p g_2^q$ ,  $\langle g_1 \rangle \times \langle g_2 \rangle \rightarrow G$ , is an isomorphism.  $\square$

**Remark.** Note also here that  $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . So, even though  $\mathbb{Z}_4$  has an element of order 2, we cannot factor out a cyclic group of order 2 from  $\mathbb{Z}_4$  in the way we did in Example 8.5. This is why we must look for elements of maximal order.

The relatively simplicity of Example 8.5 doesn't give us a nuanced enough picture of the state of affairs. For example, once we picked out an element of maximal order (of which all non-identity elements were valid candidates), we simply chose some other arbitrary point from the group to decompose it. This may lead one to think that one can simply pick a sequence of distinct elements of relative maximal order to generate the cyclic subgroups in the direct product. This approach, however, does not work, in general.

**Example 8.6.** Let  $G = \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ . There are three elements  $g_1, g_2, g_3 \in G$  of orders 8, 4, and 4, respectively, with the property that  $g_j \notin \langle g_k \rangle$  when  $j \neq k$  and for which the natural mapping

$$(ag_1, bg_2, cg_3) \xrightarrow{\varphi} ag_1 + bg_2 + cg_3, \quad \langle g_1 \rangle \times \langle g_2 \rangle \times \langle g_3 \rangle \rightarrow G,$$

is not an isomorphism. Indeed, consider  $g_1 = (1, 1, 2)$ ,  $g_2 = (2, 0, 0)$ , and  $g_3 = (2, 2, 2)$ . These elements are as claimed, as we'll demonstrate below.

Note that the sequence of iterates of  $g_1$  is

$$(1, 1, 2) \rightarrow (2, 2, 0) \rightarrow (3, 3, 2) \rightarrow (4, 0, 0) \rightarrow (5, 1, 2) \rightarrow (6, 2, 0) \rightarrow (7, 3, 2) \rightarrow (0, 0, 0),$$

the sequence of iterates of  $g_2$  is

$$(2, 0, 0) \rightarrow (4, 0, 0) \rightarrow (6, 0, 0) \rightarrow (0, 0, 0),$$

and the sequence of iterates of  $g_3$  is

$$(2, 2, 2) \rightarrow (4, 0, 0) \rightarrow (6, 2, 2) \rightarrow (0, 0, 0).$$

So  $\text{ord}(g_1) = 8$ ,  $\text{ord}(g_2) = 4$ , and  $\text{ord}(g_3) = 4$ . Moreover,  $g_j \notin \langle g_k \rangle$  when  $j \neq k$ .

Note also that

$$\langle g_1 \rangle \cap \langle g_2 \rangle \cap \langle g_3 \rangle = \{(0, 0, 0), (4, 0, 0)\}.$$

It follows that, after replacing the ordered triple  $(x, y, z)$  with the string  $xyz$ ,

$$\ker(\varphi) = \{(000, 000, 000), (000, 400, 400), (400, 000, 400), (400, 400, 000)\}.$$

Hence,

$$[\langle g_1 \rangle \times \langle g_2 \rangle \times \langle g_3 \rangle : \ker(\varphi)] = \frac{|\langle g_1 \rangle \times \langle g_2 \rangle \times \langle g_3 \rangle|}{|\ker(\varphi)|} = \frac{8 \cdot 4 \cdot 4}{4} = 64 \neq 8 \cdot 4 \cdot 4 = |G|.$$

Therefore,  $\varphi$  is not an isomorphism.

As it will turn out, if we let  $g_1$  be as it is (an element of maximal order in  $G$ ), and we can find some  $h \in G$  of order  $p$  for which  $h \notin \langle g_1 \rangle$ , then we get a workable path to the goal. That will be the general strategy in our proof of Lemma 8.7.

**Lemma 8.7.** If  $G$  is a finite Abelian  $p$ -group, then there is some sequence  $a_1, a_2, \dots, a_m$  of positive integers for which

$$G \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_m}}.$$

*Proof.* By Lemma 8.4, there must be some positive integer  $n$  such that  $|G| = p^n$ . Hence, we will proceed by induction. We will also prove an auxiliary assertion in conjunction with the statement of the lemma: under the assumption that  $g$  is an element of the finite Abelian  $p$ -group  $G$  of maximal order, then  $G \cong \langle g \rangle \times H$  for some subgroup  $H$  of  $G$  where  $(g^\alpha, h) \mapsto g^\alpha h$ ,  $\langle g \rangle \times H \rightarrow G$ , is a witnessing isomorphism. We proceed now by way of induction.

Note that, if  $|G| = p$ , then  $G$  is cyclic and, thus,  $G \cong \mathbb{Z}_p \times \{e_G\} \cong \mathbb{Z}_p$  and both the auxiliary claim and the statement of the lemma are satisfied.

Let  $k \geq 1$  and suppose the asserted auxiliary claim and the statement of the lemma hold for all groups of order  $p^n$  for each  $n \leq k$ . Suppose that  $|G| = p^{k+1}$  and let  $g \in G$  be of maximal order. Note that  $\text{ord}(g) = p^r$  for some positive integer  $r$ , and so  $\langle g \rangle \cong \mathbb{Z}_{p^r}$ . If  $r = k + 1$ , then  $G \cong \mathbb{Z}_{p^{k+1}} \times \{e_G\} \cong \mathbb{Z}_{p^{k+1}}$  and we are done.

So suppose  $r < k + 1$ . It follows that  $\langle g \rangle$  is a proper subgroup of  $G$ .

We argue now that there is some  $h \in G$  with  $h \notin \langle g \rangle$  for which  $\text{ord}(h) = p$ . Since  $\langle g \rangle$  is a proper subgroup of  $G$ ,  $G/\langle g \rangle$  is a nontrivial  $p$ -group by Lemma 8.3. Consequently, there is some element  $x\langle g \rangle \in G/\langle g \rangle$ , where  $x \in G$ , of order  $p$ . In particular,  $x\langle g \rangle \neq \langle g \rangle$  and

$$(x\langle g \rangle)^p = x^p\langle g \rangle = \langle g \rangle.$$

It follows that  $x \notin \langle g \rangle$  and that  $x^p \in \langle g \rangle$ . Hence,  $x^p = g^j$  for some integer  $j$ . Let  $b$  be the positive integer for which  $\text{ord}(x) = p^b$ . Since  $g$  was assumed to be of maximal order,

$$p^b = \text{ord}(x) \leq \text{ord}(g) = p^r.$$

Moreover,

$$e_G = x^{p^b} = x^{p \cdot p^{b-1}} = (x^p)^{p^{b-1}},$$

and we can see that the order of  $x^p$  is  $p^{b-1} < p^b \leq p^r$ . It follows that the order of  $g^j$  is  $p^{b-1} < p^r$ , and so  $\langle g^j \rangle$  is a proper subgroup of  $\langle g \rangle$ . Via the isomorphism  $g^\alpha \mapsto \alpha$ ,  $\langle g \rangle \rightarrow \mathbb{Z}_{p^r}$ , we see that  $\gcd(j, p^r) > 1$  by Lemma 4.40. Hence,  $p$  divides  $j$  and so we can write  $j = pt$  where  $t$  is an integer. So let  $h = xg^{-t}$ . Since  $x \notin \langle g \rangle$ ,  $h \notin \langle g \rangle$ . In particular,  $h \neq e_G$ . Note that

$$h^p = (xg^{-t})^p = x^p g^{-pt} = g^j g^{-j} = e_G.$$

Hence,  $\text{ord}(h) = p$ .

We now consider  $\langle h \rangle$  and argue that  $\langle g \rangle \cap \langle h \rangle = \{e_G\}$ . Indeed, suppose  $h^\alpha \in \langle g \rangle$  where  $0 \leq \alpha < p$  and let  $\beta$  be an integer for which  $h^\alpha = g^\beta$ . Note then that

$$g^\beta = h^\alpha = (xg^{-t})^\alpha = x^\alpha g^{-\alpha t} \implies x^\alpha = g^{\beta+\alpha t} \in \langle g \rangle.$$

Since the order of  $x\langle g \rangle$  is  $p$  and  $0 \leq \alpha < p$ , it must be the case that  $\alpha = 0$ . Hence,  $\langle h \rangle \cap \langle g \rangle = \{e_G\}$ .

Now, since  $\langle g \rangle \cap \langle h \rangle = \{e_G\}$  and the smallest positive integer  $\alpha$  for which  $g^\alpha = e_G \in \langle h \rangle$  is  $p^r$ , we see that  $g^\beta \notin \langle h \rangle$  for every positive integer  $\beta < p^r$ . It follows that

$$\text{ord}(g\langle h \rangle) = p^r = \text{ord}(g).$$

Moreover, since  $\text{ord}(y\langle h \rangle) \leq \text{ord}(y) \leq p^r$  for any  $y \in G$ , we see that  $g\langle h \rangle$  is of maximal order in  $G/\langle h \rangle$ . Combined with the fact that

$$|G/\langle h \rangle| = \frac{|G|}{|\langle h \rangle|} = \frac{p^{k+1}}{p} = p^k,$$

we can apply the inductive hypothesis to conclude that

$$G/\langle h \rangle \cong \langle g\langle h \rangle \rangle \times K$$

where  $K$  is a subgroup of  $G/\langle h \rangle$  and the natural mapping

$$(g^\alpha \langle h \rangle, A) \mapsto g^\alpha \langle h \rangle A, \quad \langle g\langle h \rangle \rangle \times K \rightarrow G/\langle h \rangle,$$

is a witnessing isomorphism. It follows that  $\langle g\langle h \rangle \rangle \cap K = \{\langle h \rangle\}$  since the kernel of the isomorphism is trivial by Exercise 4.22. Let  $H$  be the subgroup of  $G$  guaranteed by Exercise 4.19 for which  $K = \{y\langle h \rangle : y \in H\}$ . Note, in particular, that  $\langle h \rangle \subseteq H$ .

We now claim that  $\langle g \rangle \cap H = \{e_G\}$ . So consider  $y \in \langle g \rangle \cap H$  and note that  $y\langle h \rangle \in \langle g\langle h \rangle \rangle \cap K = \{\langle h \rangle\}$ . Hence,  $y\langle h \rangle = \langle h \rangle$  which implies that  $y \in \langle h \rangle$ . Now we have that  $y \in \langle g \rangle \cap \langle h \rangle = \{e_G\}$ , and so  $y = e_G$ . That is,  $\langle g \rangle \cap H = \{e_G\}$ .

To see that  $G = \langle g \rangle H$ , let  $u \in G$  be arbitrary and note that there is some integer  $\alpha$  and some  $y \in H$  for which

$$u\langle h \rangle = g^\alpha \langle h \rangle \cdot y\langle h \rangle = g^\alpha y\langle h \rangle.$$

It follows that  $u = g^\alpha y h^\beta$  for some integer  $\beta$  and thus, since  $\langle h \rangle \subseteq H$ , we see that  $u \in \langle g \rangle H$ . Hence, by Theorem 7.6,

$$G \cong \langle g \rangle \times H$$

and the natural mapping  $(g^\alpha, \zeta) \mapsto g^\alpha \zeta$ ,  $\langle g \rangle \times H \rightarrow G$ , is a witnessing isomorphism.

Finally, since  $H$  is a proper subgroup of  $G$  and  $H$  is an Abelian  $p$ -group with order  $\leq p^k$ , the inductive hypothesis applies to assert that  $H$  is a direct product of cyclic groups where each factor has as its order some power of  $p$ . Since  $\langle g \rangle$  is a cyclic group with order  $p^r$  and  $G \cong \langle g \rangle \times H$ , the proof is complete.  $\square$

**Exercise 8.2.** Let  $G$  be an Abelian group,  $p$  be a prime number, and

$$H = \{g \in G : \exists k \in \mathbb{Z} (g^{p^k} = e_G)\}.$$

Show that  $H$  is a subgroup of  $G$ .

**Theorem 8.8** (The Fundamental Theorem of Finite Abelian Groups). Let  $G$  be a finite Abelian group. Then there is a sequence  $p_1, p_2, \dots, p_n$  of (not necessarily distinct) primes and a sequence  $a_1, a_2, \dots, a_n$  of positive integers for which

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

In other words, every finite Abelian group is isomorphic to a direct product of cyclic groups.

*Proof.* For every integer  $n > 1$ , consider the prime factorization

$$n = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$$

of  $n$  and let  $\text{pdl}(n) = m$ . The function  $\text{pdl}$  is well-defined by The Fundamental Theorem of Arithmetic. We will use induction on  $\text{pdl}(n)$ .

Suppose  $G$  is a finite Abelian group of order  $n$  with  $\text{pdl}(n) = 1$ . Then  $n = q^b$  for some positive integer  $b$  and some prime  $q$ . It follows that  $G$  is a finite Abelian  $q$ -group and Lemma 8.7 applies to guarantee the theorem statement.

Suppose now that, for  $k \geq 1$ , every finite Abelian group of order  $n$  with  $\text{pdl}(n) \leq k$  satisfies the theorem statement. Then let  $G$  be a finite Abelian group of order  $n$  where  $\text{pdl}(n) = k + 1$  and let

$$n = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k} q_{k+1}^{b_{k+1}}$$

be the prime factorization of  $n$ . Set  $m = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$  and  $r = q_{k+1}^{b_{k+1}}$  for convenience, and let

$$H = \{g \in G : g^m = e_G\}$$

and

$$K = \left\{ g \in G : \exists j \in \mathbb{Z} \quad \left( g^{q_{k+1}^j} = e_G \right) \right\}.$$

Note that  $K$  is a subgroup of  $G$  by Exercise 8.2 and is itself a finite Abelian  $q_{k+1}$ -group. By Lemma 8.7, there is a sequence  $a_1, a_2, \dots, a_\ell$  of positive integers for which

$$K \cong \mathbb{Z}_{q_{k+1}^{a_1}} \times \mathbb{Z}_{q_{k+1}^{a_2}} \times \cdots \times \mathbb{Z}_{q_{k+1}^{a_\ell}}.$$

So, to finish the proof, we will show that  $H$  is a subgroup of  $G$  with order  $m$  and that

$$G \cong H \times K.$$

Indeed, this will suffice since the order of  $H$  is  $m$  and  $\text{pdl}(m) = k$ , which will allow us to apply the inductive hypothesis on  $H$ .

To see that  $H$  is a subgroup of  $G$ , first observe that  $e_G \in H$ . Then suppose  $g, h \in H$  and consider the fact that

$$(gh^{-1})^m = g^m h^{-m} = e_G \cdot h^{-m} = h^m \cdot h^{-m} = e_G.$$

Hence,  $gh^{-1} \in H$ , and Proposition 4.19 applies.

We now aim to show that  $H \cap K = \{e_G\}$ . First, note that any  $g \in K$  has the property that  $g^r = e_G$ . Indeed, if  $g \in K$  then we can let  $\lambda$  be the least positive integer for which

$$g^{q_{k+1}^\lambda} = e_G.$$

It follows that  $\text{ord}(g) = q_{k+1}^\lambda$  and that, since the order of any element of a finite group must divide the order of the group,  $q_{k+1}^\lambda \leq r = q_{k+1}^{b_{k+1}}$ . Then,

$$g^r = g^{q_{k+1}^{b_{k+1}}} = \left(g^{q_{k+1}^\lambda}\right)^{q_{k+1}^{b_{k+1}-\lambda}} = e_G.$$

Now, suppose  $g \in H \cap K$ . Observe that  $\gcd(m, r) = 1$ , so Bézout's Identity informs us that there are integers  $x$  and  $y$  for which  $mx + ry = 1$ . Hence,

$$g = g^{mx+ry} = g^{mx}g^{ry} = (g^m)^x(g^r)^y = e_G.$$

That is,  $H \cap K = \{e_G\}$ .

To see that  $G = HK$ , let  $g \in G$  be arbitrary and note that the order of  $g$  must be of the form

$$q_1^{w_1}q_2^{w_2} \cdots q_k^{w_k}q_{k+1}^{w_{k+1}},$$

where  $w_j$  is an integer with  $0 \leq w_j \leq b_j$  for each positive integer  $j \leq k+1$ . Note that

$$\gcd(q_1^{w_1}q_2^{w_2} \cdots q_k^{w_k}, q_{k+1}^{w_{k+1}}) = 1,$$

so Bézout's Identity guarantees integers  $x$  and  $y$  with the property that

$$xq_1^{w_1}q_2^{w_2} \cdots q_k^{w_k} + yq_{k+1}^{w_{k+1}} = 1.$$

Let  $h_1 = g^{yq_{k+1}^{w_{k+1}}}$  and  $h_2 = g^{xq_1^{w_1}q_2^{w_2} \cdots q_k^{w_k}}$ . Then

$$g = g^{xq_1^{w_1}q_2^{w_2} \cdots q_k^{w_k} + yq_{k+1}^{w_{k+1}}} = g^{xq_1^{w_1}q_2^{w_2} \cdots q_k^{w_k}} \cdot g^{yq_{k+1}^{w_{k+1}}} = h_2h_1 = h_1h_2.$$

To see that  $h_1 \in H$ , note that

$$\begin{aligned} h_1^m &= \left(g^{yq_{k+1}^{w_{k+1}}}\right)^m = g^{ymq_{k+1}^{w_{k+1}}} \\ &= g^{yq_1^{b_1}q_2^{b_2} \cdots q_k^{b_k}q_{k+1}^{w_{k+1}}} \\ &= \left(g^{q_1^{w_1}q_2^{w_2} \cdots q_k^{w_k}q_{k+1}^{w_{k+1}}}\right)^{yq_1^{b_1-w_1}q_2^{b_2-w_2} \cdots q_k^{b_k-w_k}} \\ &= e_G. \end{aligned}$$

To see that  $h_2 \in K$ , note that

$$h_2^{q_{k+1}^{w_{k+1}}} = \left(g^{xq_1^{w_1}q_2^{w_2} \cdots q_k^{w_k}}\right)^{q_{k+1}^{w_{k+1}}} = \left(g^{q_1^{w_1}q_2^{w_2} \cdots q_k^{w_k}q_{k+1}^{w_{k+1}}}\right)^x = e_G.$$

Thus,  $G = HK$ .

We can now apply Theorem 7.6 to establish that

$$G \cong H \times K.$$

The final thing to show is that the order of  $H$  is  $m$ . First, note that the order of any element of  $H$  must divide  $m$  by Lemma 4.36. Since  $\gcd(m, q_{k+1}) = 1$ ,  $H$  can have no elements of

order  $q_{k+1}$ . Hence, by Lemma 8.1,  $q_{k+1} \nmid |H|$ . A similar argument establishes the fact that  $q_j \nmid |K|$  for every positive integer  $j \leq k$ . Now, as

$$q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k} q_{k+1}^{b_{k+1}} = |G| = |H \times K| = |H| \cdot |K|,$$

$|K| = q_{k+1}^{b_{k+1}}$  and  $|H| = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k} = m$ . Finally, as  $\text{pd}(m) = k$ , the inductive hypothesis applies to guarantee that  $H$  is isomorphic to a direct product of finite cyclic groups, finishing the proof.  $\square$