Abstract Algebra

C. Caruvana

Fall 2025

Contents

1 Brief History and A Motivating Example **2**

2 Brief Commentary on Mathematical Proofs **3**
- 2.1 Direct Proof . . . 3
- 2.2 Proof by Contrapositive . . . 4
- 2.3 Proof by Contradiction . . . 4

3 Sets, Relations, and Functions **4**
- 3.1 Sets . . . 5
- 3.2 Operations with Sets . . . 5
- 3.3 Cartesian Products, Relations, and Functions . . . 7
- 3.4 Equivalence Relations . . . 10

4 Introducing Groups **12**
- 4.1 Getting to Know Groups . . . 12
- 4.2 Subgroups . . . 19
- 4.3 An Introduction to Homomorphisms . . . 20
- 4.4 Cyclic Groups and Subgroups . . . 22

5 Permutation Groups **27**
- 5.1 Dihedral Groups . . . 36
- 5.2 Cayley's Theorem . . . 37

6 Cosets and Lagrange's Theorem **37**
- 6.1 Cosets . . . 37

7 Creating New Groups From Old **40**
- 7.1 Direct Products . . . 40
- 7.2 Normal Subgroups and Quotient Groups . . . 43

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.

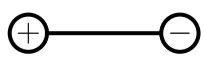
Diophantus and Brahmagupta, independently, moved away from the geometric perspective toward one focused on finding numbers that satisfied given equations.

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 $x = 5$. □

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 $x^3 - 1 \geq 0$. □

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 $\sqrt{2} = \dfrac{p}{q}$ where p and q are integers with no common factors. Squaring both sides, we obtain that $2 = \dfrac{p^2}{q^2}$ 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. □

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 $B \subsetneq A$.[1]

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.

[1] 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
- $A \cap B = B \cap A$.[2]

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

- $A \cup (B \cup C) = (A \cup B) \cup C$ and
- $A \cap (B \cap C) = (A \cap B) \cap C$.[3]

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:

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

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

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

[2] That is, the union and intersection operations are *commutative*.
[3] 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 $(x, y) \in f$.[4]
- For every $x \in X$ and $y, z \in Y$, if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.[5]

[4] 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).

[5] 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 $f : X \to Y$ 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 $f : X \to Y$ is defined to be $f[X] = \{f(x) : x \in X\}$.[6]

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 $f : X \to Y$ and $g : Y \to Z$. Show that the composition $g \circ f$ is a function $X \to Z$.

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

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

[6] 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 $f : X \to Y$ 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 $x_1 = x_2$.[7]
- 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 $\mathrm{id}_X : X \to X$ by the rule $\mathrm{id}_X(x) = x$. Note that 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 $f : X \to Y$ and $g : Y \to X$. The function g is said to be the *inverse* function of f, denoted by f^{-1}, if $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. In the case that a function $f : X \to Y$ 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 $S : \mathbb{R} \to [0, \infty)$ 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 $\mathrm{sqrt} : [0, \infty) \to [0, \infty)$, which chooses, for each $y \geq 0$, the *non-negative* solution to $x^2 = y$, is a function with the property that $S \circ \mathrm{sqrt} = \mathrm{id}_{[0,\infty)}$. On the other hand, for any $x \in \mathbb{R}$, $\mathrm{sqrt} \circ S(x) = |x|$, the absolute value of x.

Exercise 3.6. Define $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ by the rule $f(k, n) = \dfrac{k}{n}$. 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 $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x + 2$ and $g : \mathbb{R} \to \mathbb{R}$ 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 $g \circ f \neq f \circ g$.

[7] This is a version of the Horizontal Line Test.

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

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

Exercise 3.9. Suppose $f : X \to Y$ and $g : Y \to Z$. 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 $f : X \to Y$, 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 $f : X \to Y$ 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.[8]

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

[8] 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 $\mathbb{Z} \to \mathbb{Z}$.[9] For each $k \in \mathbb{Z}$, consider the function $g_k : \mathbb{Z} \to \mathbb{Z}$ defined by $g_k(n) = n + k$. Note that each g_k is a bijection and that $g_0 = \mathrm{id}_{\mathbb{Z}}$. 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 $\varphi : \mathbb{Z} \to \mathbb{Z}$ by $\varphi(k) = g_k$.[10] 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 $\diamond : G \times G \to G$ 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[11] *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

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

[9] There is a connection here with Cartesian products, but we won't get into those details now.
[10] Formally speaking, g is already a function from $\mathbb{Z}$ to $\mathbb{Z}^{\mathbb{Z}}$.
[11] As will be shown in Sanity Check 4.1, there is only one element that satisfies the identity criterion.

Therefore, $h_1 = h_2$. $\square$

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 inspired "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 $\varphi : G \to G$ by $\varphi(g) = g^{-1}$. Show that φ 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 $\varphi : G \to G$ by $\varphi(g) = g \diamond p$. Show that φ is a bijection and determine the inverse function of φ.

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 $\mathrm{Sym}(\mathbb{R})$ consist of all bijections $\mathbb{R} \to \mathbb{R}$. With the operation of function composition $\circ$, $(\mathrm{Sym}(\mathbb{R}), \circ)$ is a group with identity $\mathrm{id}_{\mathbb{R}}$. 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 $\oplus : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ 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
0	0	1
1	1	0

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
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 $* : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ 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	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

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

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	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 $d \mid n$ 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 $p \mid a$ or $p \mid b$.

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

If a prime p divides a product $a_1 a_2 \cdots a_n$, then $p \mid a_j$ for some $j \in \{1, 2, \ldots, n\}$.

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 $\mathbb{Z}_n^+$ 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. □

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. [12] 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.

[12] 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 $n \mapsto n^{-1}$, $H \to \mathbb{Z}_p^+$, 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 $H_\star = \{a_1, \ldots, a_k\}$ and note that

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

This finishes the proof. □

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

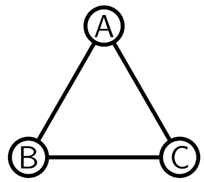
$$\mathrm{GL}(2,\mathbb{F}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0 \right\}$$

and

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

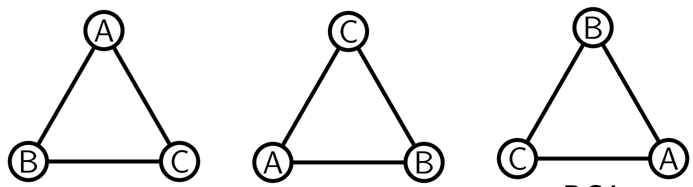
With the operation of matrix multiplication, both $\mathrm{GL}(2,\mathbb{F})$ and $\mathrm{SL}(2,\mathbb{F})$ are non-Abelian groups. $\mathrm{GL}(2,\mathbb{F})$ is referred to as the *general linear group* and $\mathrm{SL}(2,\mathbb{F})$ is referred to as the *special linear group*.

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:



ABC

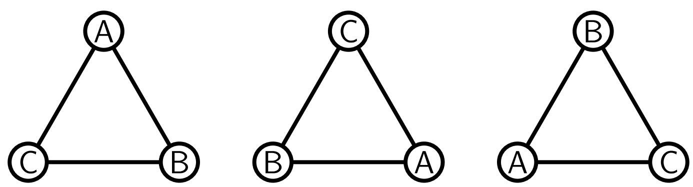
Let $\texttt{id}$ represent the null action and let $\texttt{rot}$ denote a counterclockwise rotation. We use juxtaposition to indicate actions done in succession, so the for orbit of $\texttt{rot}$ looks like this:



ABC $\texttt{id}$ | CAB $\texttt{rot}$ | BCA $\texttt{rot}^2$

Note here[13] that $\texttt{rot}^{-1} = \texttt{rot}^2$ and that $\texttt{rot}^3 = \texttt{id}$.

We also identify three possible reflections:



ACB $\texttt{ref}_1$ | CBA $\texttt{ref}_2$ | BAC $\texttt{ref}_3$

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

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

$$\texttt{rot} \cdot \texttt{ref}_1 = \texttt{ref}_2 \qquad \texttt{rot} \cdot \texttt{ref}_2 = \texttt{ref}_3 \qquad \texttt{rot} \cdot \texttt{ref}_3 = \texttt{ref}_1$$

$$\texttt{rot}^2 \cdot \texttt{ref}_1 = \texttt{ref}_3 \qquad \texttt{rot}^2 \cdot \texttt{ref}_2 = \texttt{ref}_1 \qquad \texttt{rot}^2 \cdot \texttt{ref}_3 = \texttt{ref}_2$$

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

$$\texttt{ref}_1 \cdot \texttt{rot} = \texttt{ref}_3 \qquad \texttt{ref}_2 \cdot \texttt{rot} = \texttt{ref}_1 \qquad \texttt{ref}_3 \cdot \texttt{rot} = \texttt{ref}_2$$

$$\texttt{ref}_1 \cdot \texttt{rot}^2 = \texttt{ref}_2 \qquad \texttt{ref}_2 \cdot \texttt{rot}^2 = \texttt{ref}_3 \qquad \texttt{ref}_3 \cdot \texttt{rot}^2 = \texttt{ref}_1$$

Let[14]

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

[13] One clockwise rotation undoes one counter-clockwise rotation.

[14] More on the choice of notation later.

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

$\cdot$	id	rot	$\texttt{rot}^{-1}$	$\texttt{ref}_1$	$\texttt{ref}_2$	$\texttt{ref}_3$
id	id	rot	$\texttt{rot}^{-1}$	$\texttt{ref}_1$	$\texttt{ref}_2$	$\texttt{ref}_3$
rot	rot	$\texttt{rot}^{-1}$	id	$\texttt{ref}_2$	$\texttt{ref}_3$	$\texttt{ref}_1$
$\texttt{rot}^{-1}$	$\texttt{rot}^{-1}$	id	rot	$\texttt{ref}_3$	$\texttt{ref}_1$	$\texttt{ref}_2$
$\texttt{ref}_1$	$\texttt{ref}_1$	$\texttt{ref}_3$	$\texttt{ref}_2$	id	$\texttt{rot}^{-1}$	rot
$\texttt{ref}_2$	$\texttt{ref}_2$	$\texttt{ref}_1$	$\texttt{ref}_3$	rot	id	$\texttt{rot}^{-1}$
$\texttt{ref}_3$	$\texttt{ref}_3$	$\texttt{ref}_2$	$\texttt{ref}_1$	$\texttt{rot}^{-1}$	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,

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

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

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

Let $\wp(X)$ be the set of all subsets of X. Show that $(\wp(X), \triangle)$ 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 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 $\varphi : G \to H$ 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 $\varphi : \mathbb{R} \to \mathbb{R}^+$ by the rule $\varphi(x) = 2^x$. Then φ 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 $\varphi : G \to H$ 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 $\varphi : G \to H$ is a homomorphism from the group $(G, \diamond)$ to the group $(H, \bullet)$. Show that, for any $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Definition 4.23. Suppose $\varphi : G \to H$ 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 φ to be

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

Exercise 4.17. Suppose $\varphi : G \to H$ 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 $\varphi : G \to H$ is a homomorphism from the group $(G, \diamond)$ to the group $(H, \bullet)$. Suppose E is a subgroup of G. Show that

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

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 4.18. Suppose $\varphi : G \to H$ 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 4.19. Suppose $(G, \diamond)$, $(H, \bullet)$, and $(K, *)$ are groups and that $\varphi : G \to H$ and $\psi : H \to K$ are homomorphisms. Show that $\psi \circ \varphi$ is a homomorphism.

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

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

Exercise 4.20. Suppose $\varphi : G \to H$ is a bijective homomorphism from the group $(G, \diamond)$ to the group $(H, \bullet)$. Show that φ^{-1} is necessarily a homomorphism.

Exercise 4.21. Let $R = \{\mathtt{id}, \mathtt{rot}, \mathtt{rot}^{-1}\}$, 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 $(a, b) + (c, d) = (a \oplus c, b \oplus d)$.[15] 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 4.22. 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 $\varphi : G \to H$ is a surjective homomorphism. If G is Abelian, then H is Abelian.

Proof. Let $h_1, h_2 \in H$ be arbitrary. Since φ 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 $\varphi : G \to \{1\}$ 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.

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*.

[15] This, as we will elaborate on later, is known as a *direct product*.

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 4.23. 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 4.24. Let $(G, \cdot)$ be a group and $a \in G$. Show that the mapping $k \mapsto a^k$, $\mathbb{Z} \to G$, 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 $\varphi : G \to H$ is a surjective homomorphism. If G is cyclic, then H is cyclic.

Proof. By Exercise 4.24, there exists a surjective homomorphism $\psi : \mathbb{Z} \to G$. Then, by Exercise 4.19, $\varphi \circ \psi : \mathbb{Z} \to H$ 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, $h = mq \in m\mathbb{Z}$. □

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 $\mathbb{Z}_6$, not that the group "powers" of 2 forms the sequence $(2, 4, 0, 2, 4, 0, \ldots)$. Similarly, note that the group "powers" of 5 forms the sequence $(5, 4, 3, 2, 1, 0, 5, 4, 3, 2, 1, 0, \ldots)$. 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 $a^n = e$, 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.

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

Definition 4.36. 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.

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 $(\mathbb{Z}_7, +)$ has order 7, and the group $(\mathbb{Z}, +)$ has infinite order.

Exercise 4.25. 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 4.37 (Bézout's Identity)**.** Let a and b be integers. Then there exist integers x and y such that

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

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

Lemma 4.38. If $a \in \mathbb{Z}_n$ is such that a divides n, then $\mathrm{ord}(a) = \dfrac{n}{a}$.

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 ℓ with $0 < \ell < k$, $a\ell < ak = n$. So k is indeed the least positive integer for which $ak \equiv 0 \pmod{n}$. Since $k = \dfrac{n}{a}$, we see that $\text{ord}(a) = \dfrac{n}{a}$. □

Lemma 4.39. 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, $\langle a \rangle = \langle \gcd(a, n) \rangle$. □

Proposition 4.40. Given $a \in \mathbb{Z}_n$, where $n > 1$ and $a > 0$,

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

Proof. By Lemma 4.39, $\langle a \rangle = \langle \gcd(a, n) \rangle$, In particular, this means that

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

Since $\gcd(a, n)$ divides n, Lemma 4.38 affirms that

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

□

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 4.41. Let $(G, \cdot)$ be a 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. □

Exercise 4.26. 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 4.42. 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

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

By induction, if $g_1, \ldots, g_k \in G$ commute, are each of finite order, and $\langle g_\ell\rangle \cap \langle g_j\rangle = \{e_G\}$ for $\ell \neq j$, then

$$\mathrm{ord}(g_1 g_2 \cdots g_k) = \mathrm{lcm}(\mathrm{ord}(g_1), \mathrm{ord}(g_2), \ldots, \mathrm{ord}(g_k)).$$

Proof. Let $p = \mathrm{ord}(g)$, $q = \mathrm{ord}(h)$, $m = \mathrm{lcm}(p, q)$, and $r = \mathrm{ord}(gh)$. 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, $m \leq r$, finishing the proof. □

The condition that $\langle g\rangle \cap \langle h\rangle = \{e_G\}$ in Proposition 4.42 is a necessary one since

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

regardless of what properties g may have.

The condition that the elements g and h commute in Proposition 4.42 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 4.27. 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 $(\mathrm{GL}(2, \mathbb{R}), \cdot)$, A and B both have finite orders, but that AB has infinite order.

Example 4.43 (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^{th} *roots of unity*. As you will be asked to show in Exercise 4.28, H_n is a cyclic subgroup of $\mathbb{S}^1$ of order n; indeed, $(H_n, \cdot)$ is isomorphic to $(\mathbb{Z}_n, +)$.

Exercise 4.28. 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.

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

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 $\{1, 2, \ldots, n\}$), 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 $90°$ 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

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

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 σ 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 $\mathrm{supp}(\sigma) = \{a_1, a_2, \dots, a_k\}$. In such a case, we use the *cycle notation*

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

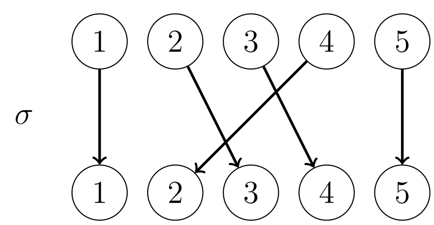
for σ. For convenience, we will use () to denote the identity permutation, which we will call the *trivial* cycle or permutation.

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 σ of S_n, we can choose a_1 to be the minimal element of the support of σ. This uniquely determines a cycle notation for σ.

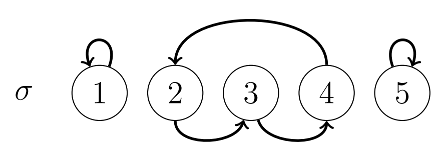
Example 5.6. Consider $X = \{1, 2, 3, 4, 5\}$. By (2 3 4), we mean the permutation σ of X where

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

Another representation of σ:



We may also describe σ using a directed graph:



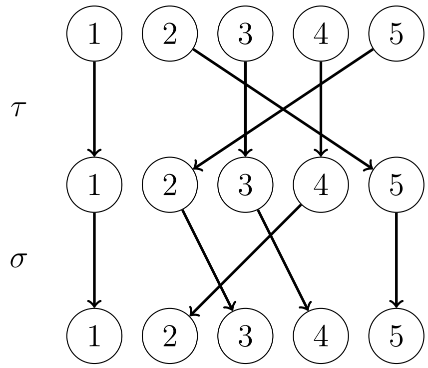
In this case, note that $\mathrm{supp}(\sigma) = \{2, 3, 4\}$.

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

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

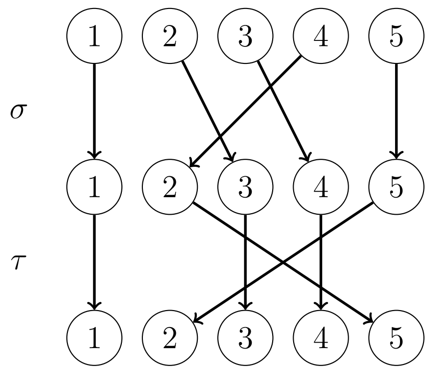
Note that this aligns with the following graphical representation (note that τ is applied *before* σ because of how we notate function composition):



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,

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

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 σ and τ are said to be *disjoint* if $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$.

Exercise 5.2. Show that, if σ and τ 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.

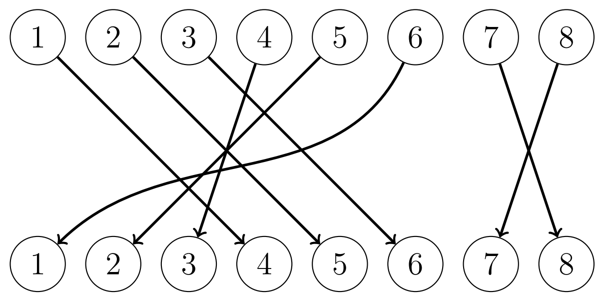
Proof. Let $X = \{1, 2, \ldots, n\}$ and $\sigma \in S_n$. Then define $A_1 = \{\sigma^m(1) : m \in \mathbb{Z}\}$. Note that $1 \in A_1$, so $A_1 \neq \emptyset$. Also note that A_1 is the support of a cycle containing 1.

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 σ can be rewritten as a product of disjoint cycles. □

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

p



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 σ 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

$$(7\ 8).$$

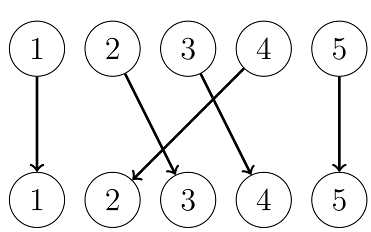
Therefore,

$$p = (1\ 4\ 3\ 6)(2\ 5)(7\ 8). \tag{1}$$

Another useful way to represent permutations is as matrices.

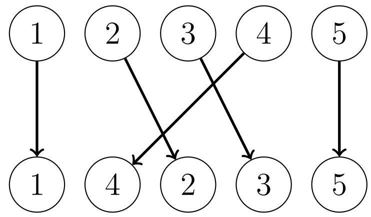
Example 5.10. Refer back to the σ and τ of Example 5.7. To faithfully capture the "action" of the permutation, we want to find a matrix for σ which describes the rearrangement of the symbols, as in the following diagram:

σ



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

σ



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

$$\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{bmatrix} \curvearrowright \begin{bmatrix} 1 \\ 4 \\ 2 \\ 3 \\ 5 \end{bmatrix}$$

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

$$\begin{matrix} 1_1 \\ 4_2 \\ 2_3 \\ 3_4 \\ 5_5 \end{matrix}$$

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

Now, thinking of using row swapping operations, we can capture σ 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, τ 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, particular 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 $p\mapsto\hat{p}$, $S_n\to\mathrm{GL}(n,\mathbb{R})$ is a group isomorphism from $(S_n,\circ)$ to $(\mathrm{GL}(n,\mathbb{R}),\cdot)$. Moreover, $\det(\hat{p})=\pm1$, 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

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

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

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

Definition 5.13. For S_n, we define the *alternating group* A_n to consist of all $p \in S_n$ with $\operatorname{sgn}(p) = 1$. Note that, by Exercise 4.17, 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[16] $(a\ b)$ 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,

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

Note from the corresponding Cayley table, that

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

So then the subgroup $\{(), (\mathsf{A\ C})(\mathsf{B\ C}), (\mathsf{A\ B})(\mathsf{B\ C})\}$ 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 $\{\texttt{id}, \texttt{rot}, \texttt{rot}^{-1}\}$ 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. □

[16] 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 σ can be written as the product of an even number of transpositions, then any decomposition of σ into a product of transpositions must consist of an even number of transpositions. Consequently, if a cycle σ can be written as the product of an odd number of transpositions, then any decomposition of σ into a product of transpositions must consist of an odd number of transpositions.

Proof. Note that every transposition τ has the property that $\operatorname{sgn}(\tau) = -1$. Since the 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 prodct 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 $f : B \to A_n$ by the rule $f(p) = \tau p$. Note that the map f is defined since τp 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. □

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 $\sigma = (a_0\ a_1\ a_2\ \ldots\ a_{n-1})$. 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, $\mathrm{ord}(\sigma) = n$. □

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 $(n_1, n_2, \ldots, n_k)$ is

$$\mathrm{lcm}(n_1, n_2, \ldots, n_k).$$

Proof. Let σ_j be the n_j-cycle, for $1 \leq j \leq k$. To verify that

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

consider that, for integers p and q, σ_j^p and σ_ℓ^q are still disjoint cycles since $\mathrm{supp}(\sigma^r) \subseteq \mathrm{supp}(\sigma)$ for any permutation σ and an integer r.

By Lemma 5.19, we know that each σ_j has order n_j. By Exercise 5.2, we have that disjoint cycles commute. Therefore, by Proposition 4.42, the proposition obtains. □

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 $X := \{1, 2, \ldots, n\}$. 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. □

5.1 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.[17]

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 $n + n = 2n$.

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 $2n$. □

[17] Note that group theorists typically write D_{2n} to refer to D_n, which is partially motivated by Theorem 5.23.

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 $g = r^{k-1}s$.

Exercise 5.5. In the context of D_n, show that $srs = r^{-1}$. (*Hint.* Note that rs is a reflection and that every reflection has order 2.)

5.2 Cayley's Theorem

Exercise 5.6. Let $(G, \cdot)$ be a group and, for $g \in G$, define $T_g : G \to G$ 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 $\varphi : G \to S_G$ by the rule $\varphi(g) = T_g$, where T_g is as defined in Exercise 5.6. Show that φ 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

$$\begin{cases} H = (1\ 2)H = \{(), (1\ 2)\} \\ (1\ 3)H = (1\ 2\ 3)H = \{(1\ 3), (1\ 2\ 3)\} \\ (2\ 3)H = (1\ 3\ 2)H = \{(2\ 3), (1\ 3\ 2)\} \end{cases}$$

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

$$\begin{cases} H = H(1\ 2) = \{(), (1\ 2)\} \\ H(1\ 3) = H(1\ 3\ 2) = \{(1\ 3), (1\ 3\ 2)\} \\ H(2\ 3) = H(1\ 2\ 3) = \{(2\ 3), (1\ 2\ 3)\} \end{cases}$$

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) $g_1 H = g_2 H$

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

(iii) $g_2 \in g_1 H$

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

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

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

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 $t_\ell : H \to gH$ and $t_r : H \to Hg$ by $t_\ell(x) = gx$ and $t_r(x) = xg$. Show that both t_ℓ 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 $\gamma : \mathsf{L}_H \to \mathsf{R}_H$ by $\gamma(gH) = Hg^{-1}$, where $g \in G$. Note that γ is seen to be both well-defined and injective by Lemma 6.3. So, to finish the proof, we need only show that γ 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. □

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 $R := \{g_1, g_2, \ldots, g_j\}$ be such that $\{g_1H, g_2H, \ldots, g_jH\}$ is the complete set of distinct left-cosets. Define $p : R \times H \to G$ 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

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

Note then that

$$g_\ell^{-1} g_k = h_2 h_1^{-1} \in H.$$

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. □

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 4.41 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 6.7. 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 $\dfrac{4!}{2} = 12$. Now suppose $H \subsetneq A_4$ 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. □

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 $\varphi : G \to G \times H$ and $\psi : H \to G \times H$ be defined by $\varphi(g) = (g, e_H)$ and $\psi(h) = (e_G, h)$. Show that both φ and ψ 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.

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 two Abelian groups. Then the direct product $G \times H$ is Abelian.

Proof. 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. $\square$

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 $(\mathbb{Z}_2, +)$ 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, $\mathbb{Z}_{ab}$ is isomorphic to $\mathbb{Z}_a \times \mathbb{Z}_b$ 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 4.42, the order of $(1, 1)$ in $\mathbb{Z}_a \times \mathbb{Z}_b$ is

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

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 $\operatorname{ord}(x)$ is a divisor of a and that $\operatorname{ord}(y)$ is a divisor of b. In particular, we can let k_1 and k_2 be the integers for which $\operatorname{ord}(x) \cdot k_1 = a$ and $\operatorname{ord}(y) \cdot k_2 = b$. We can also let ℓ_1 and ℓ_2 be the integers for which

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

and

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

It follows that

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

and thus that

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

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 $\{p_1, p_2, \ldots, p_k\}$ is a set of distinct primes and each a_j is a positive integer. Then G is isomorphic to

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

Note 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 7.6. 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 $\left(\frac{1}{x},-\frac{y}{x}\right)$. Note that $\frac{1}{x}\in\mathbb{R}^*$ since $x\neq 0$ and so $\left(\frac{1}{x},-\frac{y}{x}\right)\in\mathbb{R}^*\times\mathbb{R}$. 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, $(2,0)*(1,2)\neq(1,2)*(2,0)$. □

7.2 Normal Subgroups and Quotient Groups

Definition 7.7. 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 7.8. If $(G,\cdot)$ is an Abelian group, then every subgroup of G is normal.

Exercise 7.3. Suppose $(G,*)$ and $(H,\circ)$ are groups. Show that the isomorphic copy of G in $G\times H$ obtained via $g\mapsto(g,e_H)$, $G\to G\times H$, and that the isomorphic copy of H in $G\times H$ obtained via $h\mapsto(e_G,h)$, $H\to G\times H$, are both normal subgroups of $G\times H$.

Proposition 7.9. Let $(G,*)$ and $(H,\circ)$ be groups and suppose that $\varphi:G\to H$ is a homomorphism. Then $\ker(\varphi)$ is a normal subgroup of G.

Proof. By Exercise 4.17, 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. □

Example 7.10. By Exercise 5.3 and Proposition 7.9, we see that A_n is a normal subgroup of S_n for each $n\in\mathbb{N}$.

Example 7.11. 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

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

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

Definition 7.12. 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 7.13. The set of cosets of a normal subgroup N of a group $(G, \cdot)$ with the binary operation defined in Definition 7.12 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 $xy = ab\ell \in abN$.

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 7.14. The normality condition in Proposition 7.13 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 7.12 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,

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