Contents

1 Section 1: Propositional Logic 3
  1.1 Propositions and Statements ................................. 3
  1.2 Connectives .................................................... 4
  1.3 Valid Arguments ............................................... 7
  1.4 Logical Identities ............................................. 11

2 Section 2: Set Theory 14
  2.1 Quantifiers ...................................................... 14
  2.2 Elementary Set Theory ....................................... 15
  2.3 Common Sets ................................................... 17
  2.4 Operations on Sets ........................................... 18

3 Section 3: Equivalence Relations and Functions 23
  3.1 Orderings ....................................................... 23
  3.2 Equivalence Relations ....................................... 24
  3.3 Functions ....................................................... 27

4 Section 4: Integers 32
  4.1 Induction Principle .......................................... 32
  4.2 Factorization ................................................... 36

5 Section 5: The Euclidean Algorithm 39
  5.1 Division Algorithm ........................................... 39
  5.2 Greatest Common Divisor ................................... 39

6 Section 6: Modular Arithmetic 44
  6.1 Congruence Classes .......................................... 44
  6.2 Units in \( \mathbb{Z}_n \) ........................................... 46
Course Objectives

This course is meant to introduce you to various aspects of mathematics.

- You will be introduced to concepts in logic, set theory, number theory and abstract algebra.

- You will learn to read and produce formal proofs.

This course will conclude with a unit which applies what we have learned (in particular group theory) to coding theory. Although we won’t touch on them, the number theory we learn has pertinent applications to cryptography (e.g., see Section 1.6 on public key cryptography in the textbook).
Section 1: Propositional Logic

Mathematics is founded on logic. The first, most basic form of logic is propositional logic (or symbolic logic) due to George Boole—the logic of and and or without quantifiers or mathematical objects. The next layer of logic is first (and higher-order) logic which involves quantifiers, sets and functions. We start with propositional logic.

1.1 Propositions and Statements

Propositional logic is needed to make very basic mathematical arguments. Mathematical propositions, like “7 is prime”, have definite truth values and are the building blocks of propositional logic. Connectives like “and”, “or” and “not” join mathematical propositions into complex statements whose truth depends only on its constituent propositions. You can think of these statements as polynomials in propositions which act like variables. We want to know when two statements are logically equivalent, or when one implies the other. That is, we want to learn how to reason with mathematical statements.

Consider the following statement:

If the budget is not cut, then a necessary and sufficient condition for prices to remain stable is that taxes will be raised. Taxes will be raised only if the budget is not cut. If prices remain stable, then taxes will not be raised. Hence, taxes will not be raised.

Is this argument logically sound? That is, is the conclusion “taxes will not be raised” true if the premises of the statement are true? To answer this question, we need logic: “propositional calculus.”

Definition 1.1. A proposition is a sentence or assertion that is true (T) or false (F), but not both.

Example 1.2. Some (non-mathematical) propositions:

- \( p \) = “prices will remain stable”
- \( b \) = “the budget will be cut”
- \( r \) = “taxes will be raised”
Definition 1.3. A statement is one of two things:

- a proposition, or
- (two) statements joined by a connective.

The above is a “recursive definition” in that it defines a statement in terms of other statements.

Example 1.4. If \( p \) and \( q \) are propositions then \( p \) and \( q \) are also statements. If \( \land \) and \( \lor \) are connectives then \( p \land q, p \land p, p \lor q, (p \land q) \lor p \), and so on are all statements. You should think of these as “logical polynomials in \( p \) and \( q \)”.

1.2 Connectives

Connectives (a.k.a. truth-functionals, or boolean operators) are functions\(^1\) that take one or more (say up to \( n \)) truth values and output a truth value: i.e., functions of the form

\[
f : \{T,F\}^n \to \{T,F\}.
\]

We now give a list of common connectives.

Definition 1.5 (Negation). Let \( p \) be a proposition (or statement). The negation of \( p \), denoted by \( \neg p \), is the denial of \( p \):

- If \( p \) is \( T \), then \( \neg p \) is \( F \).
- If \( p \) is \( F \), then \( \neg p \) is \( T \).

The definition of negation is summarized by the following truth table.

<table>
<thead>
<tr>
<th>( p )</th>
<th>( \neg p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T )</td>
<td>( F )</td>
</tr>
<tr>
<td>( F )</td>
<td>( T )</td>
</tr>
</tbody>
</table>

The negation or “not” gate is depicted by

\(^1\)We will later examine sets and functions more formally.
Definition 1.6 (Conjunction). Let \( p \) and \( q \) be two propositions. The **conjunction** of \( p \) and \( q \), denoted by \( p \land q \), is another proposition whose truth values are defined by the following table:

\[
\begin{array}{ccc}
 p & q & p \land q \\
 T & T & T \\
 T & F & F \\
 F & T & F \\
 F & F & F \\
\end{array}
\]

Conjunction is also known as “and” and its gate is depicted by

\[ \begin{array}{c}
\end{array} \]

Example 1.7. \( r \land p = \) “taxes will be raised and prices will remain stable”

Definition 1.8 (Disjunction). Let \( p \) and \( q \) be two propositions. The **disjunction** of \( p \) and \( q \), denoted by \( p \lor q \), is another proposition whose truth values are defined by the following table:

\[
\begin{array}{ccc}
 p & q & p \lor q \\
 T & T & T \\
 T & F & T \\
 F & T & T \\
 F & F & F \\
\end{array}
\]

Disjunction is also called “or” and its gate is depicted by

\[ \begin{array}{c}
\end{array} \]

Definition 1.9 (Conditional). Let \( p \) and \( q \) be two propositions. The **conditional** of \( p \) and \( q \), denoted by \( p \rightarrow q \), is another proposition whose truth values are defined by the following table:

\[
\begin{array}{ccc}
 p & q & p \rightarrow q \\
 T & T & T \\
 T & F & F \\
 F & T & T \\
 F & F & T \\
\end{array}
\]
In $p \rightarrow q$, $p$ is called the **antecedent** and $q$ is called the **consequent** of the conditional. The conditional operation can be thought of as “implies.” So $p \rightarrow q$ stands for “$p$ implies $q$,” “$p$ is a sufficient condition for $q$,” “if $p$, then $q$,” “$q$ is a necessary condition for $p$,” “$q$ if $p$” and “$p$ only if $q$.”

One may question why this is the correct truth-table for our intuitive notion of “implies” (particularly the cases where $p = F$). Here are some explanations:

- The way we use implication is through modus ponens: If we know $p \rightarrow q$ is true and we also know that $p$ is true, then we should be able to deduce that $q$ is true. This justifies the first line of the truth table.

- Next, consider what it means for $p \rightarrow q$ to be false. The only time that $p \rightarrow q$ should be false is if we have an instance where $p$ is true, but $q$ is false. We thus have the second line of the truth table.

- Instances where $p$ is false do not provide evidence that $p$ does not imply $q$. To further justify the third and fourth lines of the truth table, observe that one would expect the proposition $r \land s \rightarrow s$ to be always true; in this light, examining the truth table of $r \land s \rightarrow s$, we obtain that when the antecedent $r \land s$ is false no matter what the truth value of the consequent $s$ is (either true or false), we have a true value for $r \land s \rightarrow s$ (in this argument, $r \land s$ stands for $p$ and $s$ stands for $q$).

It is hoped you will find that the above explanations provide a convincing justification of the table. With experience working with implications, it may become more natural. For now, you can also treat this as simply a definition.

**Definition 1.10** (Biconditional). Let $p$ and $q$ be two propositions. The **biconditional of $p$ and $q$**, denoted by $p \leftrightarrow q$, is another proposition whose truth values are defined by the following table:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \leftrightarrow q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The biconditional operation can be thought of as “if and only if.”
The symbols ¬, ∧, ∨, →, ↔ are called connectives, truth functionals, boolean operators, among other things.

The converse of \( p \to q \) is \( q \to p \).

The inverse of \( p \to q \) is \( \neg p \to \neg q \).

The contrapositive of \( p \to q \) is \( \neg q \to \neg p \). An implication is “logically equivalent” to its contrapositive (see Definition 1.15 for the definition of “logical equivalence”).

### 1.3 Valid Arguments

**Example 1.11.**

*If the budget is not cut, then a necessary and sufficient condition for prices to remain stable is that taxes will be raised. Taxes will be raised only if the budget is not cut. If prices remain stable, then taxes will not be raised. Hence, taxes will not be raised.*

Let \( p, b \) and \( r \) be the following propositions:

- \( p = \) “prices will remain stable”
- \( b = \) “the budget will be cut”
- \( r = \) “taxes will be raised”

We have the following premises:

- If the budget is not cut, then a necessary and sufficient condition for prices to remain stable is that taxes will be raised: \( \neg b \to (p \leftrightarrow r) \)
- Taxes will be raised only if the budget is not cut: \( r \to \neg b \)
- If prices remain stable, then taxes will not be raised: \( p \to \neg r \)

The conclusion is:

- Hence, taxes will not be raised: \( \neg r \).

Is this argument valid?

A statement is called a tautology (or logical identity) if it is always true (i.e., it is true for all possible truth-value assignments of its propositions).
Example 1.12. $s = p \lor \neg p$ is a tautology.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\neg p$</th>
<th>$p \lor \neg p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

A statement is called a **contradiction** (or fallacy) if it is always false.

Example 1.13. $s = p \land \neg p$ is a contradiction.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\neg p$</th>
<th>$p \land \neg p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

**Definition 1.14** (Logical Implication). Let $s$ and $q$ be two statement forms involving the same set of propositions. We say that $s$ **logically implies** $q$ and write $s \Rightarrow q$ if whenever $s$ is true, $q$ is also true (i.e., if every assignment of truth values making $s$ true also makes $q$ true).

**Definition 1.15** (Logical Equivalence). Let $s$ and $q$ be two statement forms involving the same set of propositions. We say that $s$ **logically equivalent** $q$ and write $s \Leftrightarrow q$ if both $s$ and $q$ have identical truth tables (i.e., for all truth assignments of their propositions).

Note that $\Rightarrow$ and $\Leftrightarrow$ are logical relationships between statements, while $\rightarrow$ and $\leftrightarrow$ are connective operators used to make statements.

Example 1.16.

- $s = p \rightarrow p$ is a tautology.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$p \rightarrow p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

- If we suppose $s = (p \rightarrow q) \rightarrow p$ and $r = p \lor q$, then $s \Rightarrow r$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \rightarrow q$</th>
<th>$s = (p \rightarrow q) \rightarrow p$</th>
<th>$r = p \lor q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Notice that whenever is $s$ is true, $r$ is also true. Thus, $s$ logically implies $r$. 
Example 1.17. Consider the two statements \( s = p \lor q \) and \( r = \neg(p \leftrightarrow q) \). First note that \( r \) has the same truth-table as a boolean operator called “exclusive or” (xor). The importance of xor is that it corresponds to binary addition.

Now, look at the truth tables below. For every truth-assignment that makes \( r \) true, we also have that \( s \) is true. Thus \( r \) logically implies \( s \); \( r \Rightarrow s \).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( r = \neg(p \leftrightarrow q) )</th>
<th>( s = p \lor q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Exercise 1.18.

- Show that \( (p \rightarrow q) \Leftrightarrow \neg p \lor q \).
- Show that \( (p \leftrightarrow q) \Leftrightarrow (\neg p \lor q) \land (\neg q \lor p) \).

Theorem 1.19. Let \( s \) and \( r \) be two statements in the same propositions.

(i) \( s \leftrightarrow r \) if and only if \( s \leftrightarrow r \) is a tautology.

(ii) \( s \Rightarrow r \) if and only if \( s \rightarrow r \) is a tautology.

(iii) \( s \leftrightarrow r \) if and only if \( s \Rightarrow r \) and \( r \Rightarrow s \).

Proof.

(i) If \( s \leftrightarrow r \) then \( s \) and \( r \) take the same values for every truth-assignment to their propositions. Thus, for a given truth-assignment, we either have \( s = r = T \) in which case \( s \leftrightarrow r \) is true, or \( s = r = F \) in which case \( s \leftrightarrow r \) is true. Since \( s \leftrightarrow r \) is true for all truth assignments, it is a tautology. A similar argument works for the converse.

(ii) If \( s \Rightarrow r \) then whenever a truth-assignment yields \( s = T \), then the same truth assignment gives \( r = T \). Thus, for a given truth assignment, \( s \) is either false and hence \( s \rightarrow r \) is true, or \( s \) is true and consequently \( r \) and \( s \rightarrow r \) are true. A similar analysis of the cases tells us that if \( s \rightarrow r \) is a tautology then \( s \Rightarrow r \).
(iii) We know \( s \leftrightarrow r \) means that \( s \) and \( r \) always take the same truth-value on any assignment to their proposition. So, it’s clear that \( s \leftrightarrow r \) implies \( s \Rightarrow r \) and \( r \Rightarrow s \).

Now assume that both \( s \Rightarrow r \) and \( r \Rightarrow s \). Since \( s \Rightarrow r \), whenever \( s \) is true, \( r \) is also true. Whenever a truth assignment gives \( s = F \), then since \( r \Rightarrow s \), \( r \) must also be false. Thus \( s \) and \( r \) must have the same value for all truth-assignments. That is \( s \leftrightarrow r \).

\[\Box\]

**Definition 1.20.** An argument with premises \( p_1, \ldots, p_n \) and conclusion \( q \) is **valid** if \( p_1 \land \cdots \land p_n \Rightarrow q \).

**Example 1.21.** The argument in our motivating example was

\[
(\neg b \rightarrow (p \leftrightarrow r)) \land (r \rightarrow \neg b) \land (p \rightarrow \neg r) \Rightarrow \neg r.
\]

In order to show that it is a valid argument, it suffices to show that

\[
s = [(\neg b \rightarrow (p \leftrightarrow r)) \land (r \rightarrow \neg b) \land (p \rightarrow \neg r)] \rightarrow \neg r
\]

is a tautology. We can do this by examining all \( 2^3 = 8 \) possible values for \( b, p \) and \( r \), and verify that, on each truth-assignment, \( s \) is true.

Here’s a second approach: We will prove that \( s \) is a tautology by contradiction. In a proof by contradiction, you make an unfounded assumption and look at the logical implications of that assumption. If, using that assumption, we can show something absurd (i.e., false), then we will know that the assumption is false.

In our case, we’ll assume that \( s \) is **not** a tautology. If we can prove a false statement, then we’ll know that our assumption was wrong: we’ll have proven that \( s \) is a tautology.

Assume that \( s \) is not a tautology. Let

\[
q_1 = \neg b \rightarrow (p \leftrightarrow r) \\
q_2 = r \rightarrow \neg b \\
q_3 = p \rightarrow \neg r
\]

so that \( s = (q_1 \land q_2 \land q_3) \rightarrow \neg r \). Since \( s \) is not a tautology, there must be a truth-assignment making \( \neg r = F \) and \( q_1 = q_2 = q_3 = T \). Since \( \neg r = F \),
we know \( r = T \) in our truth-assignment. Further, since \( q_3 = T \), we have \( T = p \rightarrow \neg r = p \rightarrow F \) and therefore, we must have \( p = F \). As \( T = q_2 = r \rightarrow \neg b \) and \( r = T \), we conclude that \( \neg b = T \) and hence \( b = F \).

So, we’ve determined the truth assignment that makes \((q_1 \land q_2 \land q_3) \rightarrow \neg r = F\); it’s \( b = F, p = F \) and \( r = T \). However, with this truth assignment, \( q_1 = T \rightarrow (F \leftrightarrow T) = T \rightarrow F = F \) which shows that \( s = T \). This contradicts our choice of truth-assignment as one that makes \( s = F \). Thus our assumption must have been wrong; \( s \) is a tautology. Consequently, the original argument is valid.

### 1.4 Logical Identities

The logical identities listed in the theorem below allow you to manipulate a statement into another form that is logically equivalent to the original.

**Theorem 1.22.** The following logical identities hold for all statements \( p, q, r \).

\[
\begin{align*}
p \land p & \Leftrightarrow p & \text{Idempotence} \\
p \lor p & \Leftrightarrow p \\
p \land \neg p & \Leftrightarrow F & \text{Contradiction} \\
p \lor \neg p & \Leftrightarrow T & \text{Tautology} \\
p \land F & \Leftrightarrow F \\
p \land T & \Leftrightarrow p \\
p \lor T & \Leftrightarrow T \\
p \lor F & \Leftrightarrow p \\
p \land q & \Leftrightarrow q \land p & \text{Commutativity} \\
p \lor q & \Leftrightarrow q \lor p \\
p \land (q \land r) & \Leftrightarrow (p \land q) \land r & \text{Associativity} \\
p \lor (q \lor r) & \Leftrightarrow (p \lor q) \lor r \\
\neg(p \land q) & \Leftrightarrow (\neg p) \lor (\neg q) & \text{DeMorgan’s Laws} \\
\neg(p \lor q) & \Leftrightarrow (\neg p) \land (\neg q) \\
\neg \neg p & \Leftrightarrow p & \text{Double Negation} \\
p \land (q \lor r) & \Leftrightarrow (p \land q) \lor (p \land r) & \text{Distributivity} \\
p \lor (q \land r) & \Leftrightarrow (p \lor q) \land (p \lor r)
\end{align*}
\]
Proof. Write out the truth tables replacing $\iff$ with $\leftrightarrow$ and check that you get a tautology in each case.

Example 1.23. The logic circuit for the statement $(a \land c) \lor [(\neg a) \lor b]$ has three inputs $(a, b, c)$ and one output (the value of the statement) and four gates ($\land$, $\lor$, $\neg$, $\lor$).

We can find a logically equivalent statement with fewer gates:

$$
(a \land c) \lor [(\neg a) \lor b] \iff [(a \land c) \lor (\neg a)] \lor b \quad \text{using associativity}
$$

$$
\iff [((\neg a) \lor (a \land c)] \lor b \quad \text{using commutativity}
$$

$$
\iff [((\neg a) \lor a) \land (\neg a \lor c)] \lor b \quad \text{using distributivity}
$$

$$
\iff (T \land (\neg a \lor c)) \lor b \quad \text{using tautology}
$$

$$
\iff [((\neg a) \lor c) \lor b \quad \text{using the sixth identity}
$$

This abruptly ends our discussion of propositional logic. We’ve learned about propositions, statements, and connectives. We have one theorem which relates the conditional and biconditional connectives to logical implication and logical equivalence. This theorem lets us prove statements of the form $s \Rightarrow r$ by showing that $s \rightarrow r$ is a tautology – something that can be checked in the truth-table. We’ve also given an example of how one can prove a statement is tautological without using the truth-table (see Example 1.21). Finally, we have a list of rules for manipulating statements into other logically equivalent statements. Using the distributive property, we see that we can expand statements easily, but that logically equivalent statements, even when expanded, can take different forms.

In our last example, Example 1.23, we suggest that we might be able to factor statements to get them into some minimal form. This is, in fact, a difficult task. You might want to read wikipedia’s articles on circuit minimization and Karnaugh maps.

The breakthrough connection between electrical switching circuits and symbolic logic was made by Claude Elwood Shannon in 1938, playing a catalyst role in the digital revolution. Shannon went on in the late 1940s to found the field of information theory, making him regarded as the father of the information age.
As a final note, I suggest you read Section 3.3 of the textbook. It contains a lot of practical advice on how to prove statements in mathematics. This is a skill that we’ll try to hone throughout the rest of this course.
Section 2: Set Theory

Throughout, the symbols “|” and “:” will both stand for “such that” and will be used interchangeably.

2.1 Quantifiers

There is one intermediary topic that we need to address as we pass from propositional logic to set theory – the topic of quantifiers. There are two quantifiers used in mathematics:

- \( \exists \), there exists.
- \( \forall \), for all.

Much like how propositional logic takes a narrow view of the mathematical world, logicians often choose to work in restricted regions of mathematics. For instance, someone studying arithmetic may assume that all variables represent positive integers. Thus a statement like

\[
\exists x, \forall y, y \text{ divides } x \Rightarrow (y = 1 \lor y = x)
\]

which is interpreted as, “there exists an integer \( x \) such that every integer dividing \( x \) is either 1 or \( x \)”. In other words, this statement asserts the existence of a prime number. You’ll note that the order of \( \exists \) and \( \forall \) is important: the statement

\[
\forall y, \exists x, y \text{ divides } x \Rightarrow (y = 1 \lor y = x)
\]

says that “for every integer \( y \), there is some integer \( x \) which, if divisible by \( y \), means \( y \) was 1 or equal to \( x \)”. While not very useful, this statement is true. Given an integer \( y \), we could simply pick \( x = y \) and the implication will be satisfied. For each \( y \), we could also pick \( x \) such that \( y \) does not divide \( x \), and this will also satisfy the implication.

In your real analysis course, you’ll learn the difference between continuity and uniform continuity. In these definitions, a subtle change in the order of the quantifiers makes a significant difference.

Unlike the examples above, we won’t restrict our variables to integers. Our variables will be allowed to be of any mathematical type, so we often need to specify extra conditions on a given variable. Let \( \mathbb{N} = \{0, 1, 2, \ldots\} \) be the set
of natural numbers. Here’s how the existence of a prime number reads if we’re working in all of mathematics:

\[ \exists x, x \in \mathbb{N} \Rightarrow \forall y, y \in \mathbb{N} \Rightarrow [y \text{ divides } x \Rightarrow (y = 1 \lor y = x)]. \]

Here \( x \) is allowed to range over all polynomials, sets, integers, and so on. If it happens to be a natural number then the remaining part of the statement is required to be true as well. For brevity, we often drop the \( \Rightarrow \)’s in favour of some notation before the comma:

\[ \exists x \in \mathbb{N}, \forall y \in \mathbb{N}, y \text{ divides } x \Rightarrow (y = 1 \lor y = x). \]

Finally, there is a De Morgan’s law for quantifiers:

\[ \neg (\exists x, P(x)) \iff \forall x, \neg P(x) \]
\[ \neg (\forall x, P(x)) \iff \exists x, \neg P(x). \]

### 2.2 Elementary Set Theory

Set theory is another crucial pillar in the foundation of mathematics. It would be very easy to say that a set is a collection of mathematical objects and leave it at that. But then you’d never be able to address Russell’s paradox:

Let \( X \) be the set of all sets which do not contain themselves:
\[ X = \{ Y \mid Y \notin Y \}. \] Is \( X \) a member of itself? If it is, then it shouldn’t be. If it’s not, then it should.

To resolve this paradox, there are very strict conditions on which sets we can form. The rules for building sets are given in a list of axioms referred to as ZFC (Zermelo-Fraenkel-Choice). Before we get into the list of axioms, some notation:

(i) \( x \in X \) means \( x \) is in the set \( X \). We also say \( x \) is an element of \( X \) or a member of \( X \).

(ii) \( \emptyset \) is the empty set; this set is assumed to exist. It has the property that \( \forall x, \neg (x \in \emptyset) \). By De Morgan’s law for quantifiers, we can restate this as \( \neg (\exists x, x \in X) \).
(iii) \( X \subseteq Y \) is an abbreviation for \( \forall x, x \in X \Rightarrow x \in Y \). The notation \( X \subset Y \) means \( X \subseteq Y \land X \neq Y \) and we say \( X \) is a proper (or strict) subset of \( Y \). Mathematicians often sloppily use \( \subset \) when they mean \( \subseteq \) (the audacity!), so be cautious.

**Example 2.1.** Let \( X = \{1, 2, \{3\}\} \).

\[
\begin{array}{ccc}
1 \in X & & \{1\} \subseteq X \\
2 \in X & & \{1, 2\} \subseteq X \\
3 \notin X & & \{1, 2, 3\} \not\subseteq X \\
\{3\} \in X & & \{\{3\}\} \subseteq X
\end{array}
\]

In the following, the most readable and important axioms are starred.

(1\*) Extensionality.

\[ \forall X, \forall Y, (\forall Z, Z \in X \leftrightarrow Z \in Y) \Rightarrow X = Y. \]

Two sets are equal if they contain the same elements. In order to prove two sets are equal, we often break the argument into two steps – we show \( X \subseteq Y \) and \( Y \subseteq X \). An argument proving \( X \subseteq Y \) would go

“Let \( x \in X \). Yada, yada, yada. Therefore \( x \in Y \).”

(2) Regularity.

\[ \forall X, (\exists a, a \in X) \Rightarrow (\exists Y, Y \in X \land \neg(\exists Z, Z \in Y \land Z \in X)). \]

Every non-empty set is disjoint (i.e., has no common elements) from one of its members. In other words, if \( X \) is a non-empty set, then for some \( Y \in X \), \( Y \) has no elements in common with \( X \).

(3\*) Subsets. For all statements \( \phi \),

\[ \forall X, \exists Y, \forall x, x \in Y \leftrightarrow (x \in X \land \phi(x)). \]

Given any set, you can restrict that set to a subset. Notationally, we express \( Y \) as

\[ Y = \{x \in X \mid \phi(x)\}. \]

This axiom is needed to avoid paradoxes such as the one by Russell.
(4) Pairing.
\[ \forall x, \forall y, \exists Z, x \in Z \land y \in Z. \]
Given any sets \( x \) and \( y \), there is a set \( Z = \{x, y\} \) which contains both.

(5*) Union.
\[ \forall F, \exists Z, \forall Y, \exists x, (x \in Y \land Y \in F) \Rightarrow x \in Z. \]
Given any collection of sets \( F \), there is a set that contains their union. When \( F \) contains two sets \( X \) and \( Y \), we write their union as
\[ Z = X \cup Y = \{x \mid x \in X \lor x \in Y\}. \]

(6) Replacement. For all statements \( f \),
\[ \forall X, \exists Y, \forall x, x \in X \Rightarrow (\exists y, y \in Y \land y = f(x)). \]
The set \( Y \) is denoted by \( \{y : \exists x \in X, y = f(x)\} \) and is called the “image of \( X \) under \( f \)” (the axiom states that “the image of a set under a function is a set”).

(7*) Axiom of Infinity.
\[ \exists X, \emptyset \in X \land (\forall y, y \in X \Rightarrow y \cup \{y\} \in X) \]
There is a set \( X \) such that \( \emptyset \in X \) and whenever \( y \in X \), then \( y \cup \{y\} \in X \) (such a set is called a “successor set”). In other words, this axiom states that there exists a set whose elements have the recursive structure of the natural numbers. Recall \( \mathbb{N} = \{0\} \cup \{x + 1 \mid x \in \mathbb{N}\} \).

(8*) Power set.
\[ \forall X, \exists Y, \forall Z, Z \subseteq X \Rightarrow Z \in Y. \]
Given a set \( X \), there is a set denoted \( Y = \mathcal{P}(X) \) which contains all subsets of \( X \).

(9) The Axiom of Choice. If \( X \) is a set of non-empty pairwise disjoint sets, then there is a set \( Y \) which has exactly one element in common with each element of \( X \).

2.3 Common Sets
The convention of most mathematicians is to use “blackboard bold” characters for the most commonly used sets of numbers.
Definition 2.2.

- \( \mathbb{N} = \{0, 1, 2, \ldots\} \), natural numbers.
- \( \mathbb{Z} = \{\ldots, -2, 1, 0, 1, 2, \ldots\} \), integers.
- \( \mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\} \), rational numbers.
- \( \mathbb{R} \), real numbers.
- \( \mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\} \), complex numbers.

The following hold:

\[ \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \]

2.4 Operations on Sets

You’ve probably been told that sets are unordered and don’t respect repetitions. For example \( \{1, 2, 3\} = \{3, 2, 1\} = \{2, 3, 3, 1, 3\} \). The reason that sets are unordered, is that there is essentially only one question you can ask of a set \( X \):

“Is \( x \in X \)?”

You can’t ask how many times \( x \) is in \( X \), nor whether it precedes or follows another element. Since the “three” sets above all give the same answer to the questions \( 1 \in X \), \( 2 \in X \), \( 3 \in X \) (all true) and \( x \in X \) false for any other \( x \), we see that they are all the same sets. We can’t distinguish between them using membership (\( \in \)).

We now define operations on sets. The only tools at our disposal are logical operators, membership (\( \in \)), and anything provided in the ZFC axioms (restriction to subsets, power set, union).

Definition 2.3. Let \( X \) and \( Y \) be sets.

- \( X \cup Y = \{x \mid x \in X \lor x \in Y\} \), union.
- \( X \cap Y = \{x \mid x \in X \land x \in Y\} = \{x \in X \mid x \in Y\} \), intersection.
- \( X \setminus Y = \{x \in X \mid x \notin Y\} \), set difference.
• If \( Y \subseteq X \), then we sometimes write \( Y^c = X \setminus Y \) for the complement of \( Y \) in \( X \). Our textbook calls \( X \) the “universal set”. Often this notation is used without explicitly introducing \( X \). You should ask what set the complement is taken in if its not clear from context.

• \( X \triangle Y = (X \cup Y) \setminus (X \cap Y) \), symmetric difference.

• \( \mathcal{P}(X) = \{ Y \mid Y \subseteq X \} \), the power set of \( X \).

• \( X \times Y = \{ (x, y) \mid x \in X \land y \in Y \} \), Cartesian product.

• \( X^n = \underbrace{X \times \cdots \times X}_{n\text{-times}} = \{ (x_1, \ldots, x_n) \mid \forall i, 1 \leq i \leq n \Rightarrow x_i \in X \} \).

• \( Y^X = \{ f : X \to Y \} \).

**Example 2.4.** Let \( X = \{1, 2, 3, 4, 5\} \), \( Y = \{3, 4, 5\} \) and \( Z = \{2, 3, 6\} \) be subsets of \( \mathbb{N} \).

\[
Y \cup Z = \{2, 3, 4, 5, 6\}
\]
\[
X \cup Y = X
\]
\[
X \cap Z = \{2, 3\}
\]
\[
X \cap Y = Y
\]
\[
X \setminus Z = \{1, 4, 5\}
\]
\[
Y \setminus X = \emptyset
\]
\[
Y^c = \{ n \in \mathbb{N} \mid n \leq 2 \} \cup \{ n \in \mathbb{N} \mid n \geq 6 \}
\]
\[
X \triangle Z = \{1, 4, 5, 6\}
\]
\[
\mathcal{P}(Y) = \{ \emptyset, \{3\}, \{4\}, \{5\}, \{3, 4\}, \{3, 5\}, \{4, 5\}, \{3, 4, 5\} \}
\]
\[
Y \times Z = \{ (3, 2), (3, 3), (3, 6), (4, 2), (4, 3), (4, 6), (5, 2), (5, 3), (5, 6) \}
\]
\[
Y^3 = \{ (3, 3, 3), (3, 3, 4), (3, 3, 5), (3, 4, 3), (3, 4, 4), (3, 4, 5), (3, 5, 3), \ldots, (5, 5, 5) \}
\]
\[
Z^X = Z^5 \quad \text{or, perhaps, these are only “in correspondence.”}
\]

In the example above, \( X \), \( Y \) and \( Z \) are **finite** sets. That is to say, the number of distinct elements in these sets is given by a natural number (rather than some “infinite cardinal”). When a set \( X \) is finite, we use \( |X| \) to denote its size. For the sets above \( |X| = 5 \) and \( |Y| = |Z| = 3 \). We will define finite and infinite more carefully when we talk about bijective functions.

Two sets \( X \) and \( Y \) are called disjoint if \( X \cap Y = \emptyset \). A collection of sets \( X_1, \ldots, X_n \) is pairwise disjoint if for each pair of indices \( i \) and \( j \) with \( i \neq j \),
we have \( X_i \cap X_j = \emptyset \). Equivalently, using the contrapositive, \( X_1, \ldots, X_n \) are pairwise disjoint if \( X_i \cap X_j \neq \emptyset \) implies \( i = j \). If \( X_1, \ldots, X_n \) are pairwise disjoint then

\[
|X_1 \cup \cdots \cup X_n| = |X_1| + \cdots + |X_n|.
\]

If your sets are not disjoint, you can use the following theorem relating the size of a union of sets to the sizes of their intersections.

**Theorem 2.5** (Inclusion-exclusion). Let \( X, Y \) and \( Z \) be sets.

\[
|X \cup Y| = |X| + |Y| - |X \cap Y|
\]

\[
|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|
\]

The following theorem lists the basic identities that these set operations satisfy.

**Theorem 2.6.** For any sets \( X, Y \) and \( Z \) (all contained in some “universal set” \( U \)) we have

\[
X \cap X = X
\]

\[
X \cup X = X \quad \text{idempotence}
\]

\[
X \cap X^c = \emptyset
\]

\[
X \cup X^c = U \quad \text{complementation}
\]

\[
X \cap Y = Y \cap X \quad \text{commutativity}
\]

\[
X \cup Y = Y \cup X
\]

\[
X \cap (Y \cap Z) = (X \cap Y) \cap Z \quad \text{associativity}
\]

\[
X \cup (Y \cup Z) = (X \cup Y) \cup Z
\]

\[
(X \cap Y)^c = X^c \cup Y^c
\]

\[
(X \cup Y)^c = X^c \cap Y^c \quad \text{De Morgan laws}
\]

\[
X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)
\]

\[
X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \quad \text{distributivity}
\]

\[
(X^c)^c = X
\]

\[
X \cap \emptyset = \emptyset \quad \text{double complement}
\]

\[
X \cup \emptyset = X \quad \text{properties of the empty set}
\]
\[ X \cap U = X \]
\[ X \cup U = U \quad \text{properties of the universal set} \]
\[ X \cap (X \cup Y) = X \]
\[ X \cup (X \cap Y) = X \quad \text{absorption laws} \]

**Proof.** We will only prove one of the above. Specifically, we prove that \( X \cap U = X \) assuming \( X \subseteq U \).

In order to show that the two sets \( X \cap U \) and \( X \) are equal, we proceed by double inclusion. That is, we first show \( X \cap U \subseteq X \) and later show \( X \subseteq X \cap U \). This suffices to prove \( X \cap U = X \).

For our first containment, \( X \cap U \subseteq X \), take an arbitrary element \( x \in X \cap U \). From the definition of intersection, we know \( x \in X \) and \( x \in U \). Since we have \( x \in X \) and \( x \) was an arbitrary element of \( X \cap U \), we then have that \( X \cap U \subseteq X \).

For our second containment, \( X \subseteq X \cap U \), take an arbitrary element \( x \in X \). We need to show that \( x \in X \cap U \). Since \( X \subseteq U \), we know that any element of \( X \) is an element of \( U \). In particular, \( x \in X \) so \( x \in U \). Thus, \( x \in X \) and \( x \in U \). Therefore \( x \in X \cap U \). We conclude that \( X \subseteq X \cap U \).

Since we have shown both \( X \cap U \subseteq X \) and \( X \subseteq X \cap U \), we must have \( X \cap U = X \).

Using double inclusion is the most common way to show that two sets are equal. When you write such a proof, you’ll want to clearly mention both inclusions and why each holds. It is very common for one direction to be significantly harder than the other. The previous proof was meant to introduce you to this technique, and so, was excessively verbose. Here’s how one can write the proof more concisely:

**Theorem 2.7.** If \( X \subseteq U \) then \( X \cap U = X \).

**Proof.** Show that \( X \cap U = X \) by double inclusion. Take \( x \in X \cap U \), arbitrarily. Since \( x \in X \cap U \), \( x \in X \). Therefore \( X \cap U \subseteq X \). For the opposite inclusion, take \( x \in X \). Since \( X \subseteq U \), we have \( x \in U \) as well. Therefore \( x \in X \cap U \) and consequently \( X \subseteq X \cap U \). Since we have proven both containments, we know \( X \cap U = X \).

We’ve already introduced Cartesian products of sets \( X^n \) whose elements are \( n \)-tuples (pairs, triples, quadruples, quintuples, etc., depending on \( n \)). An \( n \)-tuple \((x_1, x_2, \ldots, x_n) \in X^n \) is an ordered sequence of elements \( x_i \in X \). You can
also think of it as a function \( \{1, \ldots, n\} \to X \) which assigns \( i \mapsto x_i \). (There’s really no other information in the function other than a choice of output \( x_i \) for each input \( i \)).

We generalize this idea: a **family** of elements of \( X \) is an indexed collection \((x_i)_{i \in A}\) where \( A \) is our index set and each \( x_i \in X \). If \( A = \{1, \ldots, n\} \) then our family is simple an \( n \)-tuple \((x_1, \ldots, x_n)\). If \( A = \mathbb{N} \) then our family \((x_i)_{i \in \mathbb{N}}\) is a sequence \( x_0, x_1, x_2, \ldots \) and so on. Our index set may be more exotic as well.
Section 3: Equivalence Relations and Functions

Definition 3.1. If $X$ and $Y$ are sets, then a **binary relation** from $X$ to $Y$ is a subset $R \subseteq X \times Y$. Whenever $(x, y) \in R$, we write $xRy$ and say that “$x$ is related to $y$ under $R$.”

Quite often $X$ and $Y$ will be the same set. In this case, we simply say that $R$ is a relation on $X$. Relations are used to mathematically represent orderings by size, divisibility, or containment. They are also used to group objects together and form equivalences between objects. Finally, functions are a specific type of relation.

Example 3.2.

(i) Let $X = \{1, 2, 3, 4\}$. The “strictly less than” relation $L$ on $X$ is the subset $L \subseteq X \times X$ given by $L = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$.

(ii) Let $X = \{2, 3, 4, 5, 6\}$. The divisibility relation $D$ on $X$ is the subset $D \subseteq X \times X$ given by $D = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6)\}$.

(iii) Let $X = \{1, 2, 3, 4\}$. The equality relation $E$ on $X$ is the subset $E \subseteq X \times X$ given by $D = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$.

(iv) Let $f : \{3, 4, 5\} \to \{0, 1\}$ be the function with $f(3) = f(5) = 0$ and $f(4) = 1$. This function is given by the relation $f \subseteq \{3, 4, 5\} \times \{0, 1\}$ defined as $f = \{(3, 0), (4, 1), (5, 0)\}$. This set is often called the **graph of $f$**, rather than $f$ itself (we will thoroughly examine functions in Section 3.3).

3.1 Orderings

A set $X$ can be ordered with either a partial order or a total order.

Definition 3.3. A partial order on $X$ is a binary relation $\leq$ on $X$ that is **reflexive**, **antisymmetric** and **transitive**.

- reflexive: $x \leq x$ for all $x \in X$.
- anti-symmetric: $x \leq y$ and $y \leq x$ implies $x = y$ for all $x, y \in X$.
- transitive: $x \leq y$ and $y \leq z$ implies $x \leq z$ for all $x, y, z \in X$. 
A total order is a partial order where every pair \( x, y \in X \) satisfies either \( x \leq y \) or \( y \leq x \).

**Example 3.4.**

(i) The sets \( \mathbb{Z}, \mathbb{Q}, \text{ and } \mathbb{R} \) are totally ordered by \( \leq \), using the usual definition.

(ii) The set \( \mathbb{N} \) is partially ordered by divisibility. For \( a, b \in \mathbb{N} \), we write \( a \mid b \) if there exists \( c \in \mathbb{N} \) with \( ca = b \) and say that \( a \) divides \( b \). This is a partial order on \( \mathbb{N} \), but not a total order since \( 5 \nmid 7 \) and \( 7 \nmid 5 \).

(iii) The set \( \mathbb{Z} \) is not partially ordered by divisibility since \( -3 \mid 3 \) and \( 3 \mid -3 \) but \( 3 \neq -3 \) (this breaks antisymmetry).

(iv) The powerset \( \mathcal{P}(X) \) of a set \( X \) (i.e., the set of all subsets of \( X \)), is ordered by containment; \( Y \subseteq Z \).

### 3.2 Equivalence Relations

**Definition 3.5.** A relation \( E \) on a set \( X \) is an equivalence relation if it is reflexive, symmetric and transitive.

- **reflexive**: \( xEx \) for all \( x \in X \).
- **symmetric**: \( xEy \) implies \( yEx \) for all \( x, y \in X \).
- **transitive**: \( xEy \) and \( yEz \) implies \( xEz \) for all \( x, y, z \in X \).

Whenever two elements \( x, y \in X \) satisfy \( xEy \) we say they are **equivalent**.

**Example 3.6.**

(i) Equality is an equivalence relation on \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \), and any other set you can think of.

(ii) The relation \( \leq \) is not an equivalence relation since it is not symmetric; \( 2 \leq 3 \), but \( 3 \nleq 2 \).

(iii) Let \( A = \{ \text{all students in Mthe217} \} \). Let \( a \sim b \) if \( a \) and \( b \) have the same age. Then \( \sim \) is an equivalence relation on \( A \).

(iv) Congruence modulo \( n \): Fix \( n \in \mathbb{Z} \). We say \( a, b \in \mathbb{Z} \) are **congruent modulo** \( n \) and write

\[
a \equiv b \mod n
\]
if \( n \) divides \( a - b \) (i.e., \( a - b = qn \) for some \( q \in \mathbb{Z} \)). We show in Proposition 3.7 that congruence modulo \( n \) is an equivalence relation on \( \mathbb{Z} \); this equivalence relation will be later studied more closely.

**Proposition 3.7.** Congruence is an equivalence relation on \( \mathbb{Z} \).

**Proof.** We first show that congruence is reflexive. If we take \( a \in \mathbb{Z} \), then \( a - a = 0 = 0 \cdot n \). Therefore \( a \equiv a \mod n \).

Now we show that congruence is symmetric. If we have any \( a, b \in \mathbb{Z} \) with \( a \equiv b \mod n \) then \( a - b = qn \) for some \( q \in \mathbb{Z} \). Thus, \( b - a = (-q)n \) and hence \( b \equiv a \mod n \). This shows the symmetry of congruence.

Finally, for transitivity, take \( a, b, c \in \mathbb{Z} \) with \( a \equiv b \mod n \) and \( b \equiv c \mod n \). We want to show that \( a \equiv c \mod n \). First, \( a - b = qn \) and \( b - c = rn \) for some \( q, r \in \mathbb{Z} \). Adding these two expressions gives \( a - c = qn + rn = (q+r)n \). Thus, \( a \equiv c \mod n \).

**Definition 3.8.** Given an equivalence relation \( \sim \) on \( X \), the **equivalence class** of \( a \in X \) is the set \([a] = \{ b \in X \mid b \sim a \} \).

If our equivalence relation is congruence modulo \( n \) on \( \mathbb{Z} \), then equivalence classes of integers are called **congruence classes**.

**Proposition 3.9.** Suppose \( \sim \) is an equivalence relation on \( X \). For \( a, b \in X \), 
\( a \sim b \) if and only if \([a] = [b] \).

**Proof.** In order to show the forward direction, we assume that \( a \sim b \); we aim to show \([a] = [b] \) by double inclusion. Take an arbitrary element \( c \in [b] \). Since \( c \in [b] \) we have \( b \sim c \). As \( a \sim b \), we know \( a \sim c \) by transitivity. Therefore \( c \in [a] \). We have shown \([b] \subseteq [a] \). The reverse containment \([a] \subseteq [b] \) holds by symmetry. Thus, \([a] = [b] \).

For the opposite direction, assume that \([a] = [b] \). Since \( b \sim b \), we have \( b \in [b] = [a] \) and hence \( a \sim b \). Therefore \([a] = [b] \) implies \( a \sim b \).

**Example 3.10.** There are 5 different congruence classes of integers modulo 5.

\[
[0] = \{ \ldots, -15, -10, -5, 0, 5, 10, 15, \ldots \} \\
[1] = \{ \ldots, -14, -9, -4, 1, 6, 11, 16, \ldots \} \\
[2] = \{ \ldots, -13, -8, -3, 2, 7, 12, 17, \ldots \} \\
[3] = \{ \ldots, -12, -7, -2, 3, 8, 13, 18, \ldots \} \\
[4] = \{ \ldots, -11, -6, -1, 4, 9, 14, 19, \ldots \}
\]
Note that \([5] = [0]\) since \(5 \equiv 0 \mod 5\), \([6] = [1]\) since \(6 \equiv 1 \mod 5\) and so on. Note also that the above congruence classes are pairwise disjoint and their union yields the entire set \(\mathbb{Z}\).

**Definition 3.11.** Suppose \(\sim\) is an equivalence relation on \(X\). The set of all equivalence classes of elements in \(X\) is called the **quotient set** and is denoted by
\[
S/\sim = \{ [a] \mid a \in S \}.
\]

If \(X = \mathbb{Z}\) and our equivalence relation \(\sim\) is congruence modulo \(n\), then we write \(\mathbb{Z}_n = \mathbb{Z}/\sim\).

From the previous example \(|\mathbb{Z}_5| = 5\) and, more generally, \(|\mathbb{Z}_n| = n\).

**Proposition 3.12.** Let \(\sim\) be an equivalence relation on \(X\). The sets in \(X/\sim\) are pairwise disjoint and their union is \(X\).

*Proof.* In order to show that distinct equivalence classes are disjoint (i.e., \([a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset\), we prove the contrapositive (which is logically equivalent). In other words, we need to show that if \([a], [b] \in X/\sim\) have \([a] \cap [b] \neq \emptyset\) then \([a] = [b]\).

If we assume \([a] \cap [b] \neq \emptyset\), then there exists \(c \in [a] \cap [b]\). As \(c \in [a]\) and \(c \in [b]\), we have \(a \sim c\) and \(b \sim c\). By transitivity \(a \sim b\) and therefore \([a] = [b]\) by our previous proposition. This shows that the equivalence classes in \(X/\sim\) are pairwise disjoint.

As every \([a] \in X/\sim\) is a subset of \(X\), the union of all these sets is still a subset of \(X\); \(\bigcup_{[a] \in X/\sim} [a] \subseteq X\). If we take \(b \in X\) arbitrarily, then \(b \in [b] \in X/\sim\). Therefore \(b \in \bigcup_{[a] \in X/\sim} [a]\). This shows that \(X \subseteq \bigcup_{[a] \in X/\sim} [a]\). Therefore these sets are equal. \(\Box\)

**Definition 3.13.** Let \(X\) be a set. A set \(Y \subseteq \mathcal{P}(X)\) of subsets of \(X\) is a **partition** of \(X\) if the sets in \(Y\) are pairwise disjoint and their union is \(X\).

From the previous proposition, \(X/\sim\) is a partition of \(X\) for any equivalence relation \(\sim\). The reverse also holds:

**Proposition 3.14.** Let \(Y\) be a partition of \(X\). Define a relation on \(X\) by \(a \sim b\) if there exists \(Z \in Y\) with \(a \in Z\) and \(b \in Z\). The relation \(\sim\) is an equivalence relation.
3.3 Functions

Definition 3.15. A function \( f : X \to Y \) is a relation \( \text{Gr}(f) \subseteq X \times Y \) which satisfies the following condition: for all \( x \in X \) there exists a unique (exactly one) \( y \in Y \) with \((x, y) \in \text{Gr}(f)\).

For \( x \in X \), the unique element \( y \in Y \) such that \((x, y) \in \text{Gr}(f)\) is denoted \( y = f(x) \) and called the image of \( x \) under \( f \). For function \( f : X \to Y \), the set \( X \) is called the domain of \( f \) while \( Y \) is called the range or codomain of \( f \). \( \text{Gr}(f) \) is also called the graph of \( f \).

Remark 3.16. A less formal definition of a function \( f : X \to Y \) is that it is a “rule” that assigns to every element \( x \in X \) exactly one element \( y \in Y \) called the image of \( x \) under \( f \) and denoted by \( y = f(x) \).

Definition 3.17. Let \( f : X \to Y \) be a function and let \( A \subseteq X \) and \( B \subseteq Y \) be sets. The image of \( A \) under \( f \) is the set \[ f(A) = \{ f(a) \mid a \in A \} \]

\[ = \{ y \in Y \mid \exists a \in A, f(a) = y \}. \]

The image of the whole domain is simply called the image of \( f \): \( \text{Im} f = f(X) \). The pre-image of \( B \) is the set \( f^{-1}(B) = \{ x \in X \mid f(x) \in B \} \). The pre-image of an element \( y \in Y \) is the set \( f^{-1}(y) = \{ x \in X \mid f(x) = y \} \).

Observe that \( f(A) \subseteq Y \) while \( f^{-1}(B) \subseteq X \).

Example 3.18. Let \( f : \mathbb{R} \to \mathbb{R} \) be given by \( f(x) = x^2 \). Using interval notation,

- \( f([2, 3]) = [4, 9] \),
- \( f((-3, 2)) = [0, 9] \),
- \( f^{-1}([4, 9]) = [-3, -2] \cup [2, 3] \), and
- \( f^{-1}(2) = \{ \sqrt{2}, -\sqrt{2} \} \).

Exercise 3.19. Let \( f : X \to Y \). Show that the relation on \( X \) defined by \( a \sim b \) if \( f(a) = f(b) \) is an equivalence relation. Such equivalence relation is called the kernel equivalence of the function \( f \).

Definition 3.20. Let \( \sim \) be an equivalence relation on set \( X \), and let \( f : X \to Y \) be a function. The function \( \overline{f} : X/\sim \to Y \) given by \( \overline{f}([x]) = f(x) \) is well-defined on the quotient set \( X/\sim \) if \( f \) is constant on the equivalence classes of \( X \) (i.e., for all \( a, b \in X \) with \( a \sim b \) we have \( f(a) = f(b) \)).
Note that if $f : X/\sim \to Y$ is not well-defined on $X/\sim$, then $f$ is not a function.

**Example 3.21.** Let $f : \mathbb{Z} \to \{0, 1\}$ be given by

$$f(a) = \begin{cases} 
0 & \text{a is even,} \\
1 & \text{a is odd.}
\end{cases}$$

The function $f : \mathbb{Z}_5 \to \{0, 1\}$ given by $f([a]) = f(a)$ is not well-defined. For example, $2 \equiv 7 \mod 5$ and 2 is even while 7 is odd. Therefore $f(a)$ is not constant on $a \in [2] = \{\ldots, -8, -3, 2, 7, \ldots, \}$ since it outputs both 0 and 1. In other words, since $[2] = [7]$, we can’t define a function with $0 = f([2]) = f([7]) = 1$.

If instead we define $f : \mathbb{Z}_4 \to \{0, 1\}$ by $f([a]) = f(a)$, then $f$ is well-defined: if $a \equiv b \mod 4$ then $a - b = 4q$ for some $q \in \mathbb{Z}$, so either $a$ and $b$ are both odd, or both even since they differ by a multiple of 4.

Common practice is to skip the definition of $f$. For example, $g : \mathbb{Z}_4 \to \{0, 1\}$ given by

$$g([a]) = \begin{cases} 
0 & \text{a is even,} \\
1 & \text{a is odd}
\end{cases}$$

is a well-defined function and equal to $f$ above.

**Definition 3.22.** A function $f : X \to Y$ is **injective** (one-to-one) if for every $a, b \in X$ with $a \neq b$ we have $f(b) \neq f(a)$. A function $f : X \to Y$ is **surjective** (onto) if for every $c \in Y$, there exists some $a \in X$ with $f(a) = c$. A function which is both injective and surjective is called **bijective**.

Note that we could have used the contrapositive to define injectivity: $f$ is injective if for all $a, b \in X$, $f(a) = f(b)$ implies $a = b$. We also could have said that $f : X \to Y$ is surjective if $\text{Im}(f) = Y$.

If there is a bijection $f : X \to Y$, some authors will say that $f$ gives a one-to-one correspondence between the elements of $X$ and the elements of $Y$. (We do not say there is a correspondence if $f$ is only injective.)

**Example 3.23.**

(i) Let $f : \mathbb{N} \to \mathbb{N}$ where $f(n) = 2n + 1$. This function is injective since $f(m) = f(n) \Rightarrow 2m + 1 = 2n + 1 \Rightarrow 2m = 2n \Rightarrow m = n$. This function is not surjective since $4 \notin \text{Im} f$. 
(ii) Let \( g : \mathbb{R} \to \mathbb{R} \) where \( g(x) = 2x + 1 \). This function is both injective (same proof as above) and surjective. (Proof: Given \( y \in \mathbb{R} \), \( g\left(\frac{y-1}{2}\right) = 2\frac{y-1}{2} + 1 = y \).) Thus, \( g \) is a bijection.

(iii) The function \( h : \mathbb{R} \to \mathbb{R} \) given by \( h(x) = x^2 \) is neither injective nor surjective. However, the function \( k : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} \) with \( k(x) = x^2 \) is bijective, where \( \mathbb{R}_{\geq 0} \) denotes the set of the non-negative reals.

(iv) The identity function \( \text{id}_X : X \to X \) defined by \( \text{id}_X(x) = x \) is a bijection.

Definition 3.24. The composition \( g \circ f : X \to Z \) of two functions \( f : X \to Y \) and \( g : Y \to Z \) is the function defined by \( (g \circ f)(x) = g(f(x)) \).

An endomorphism is a function \( f : X \to X \). Endomorphisms can be composed with themselves repeatedly: \( f^n = f \circ \cdots \circ f \), \( n \) times.

Example 3.25. Let \( f, g : \mathbb{R} \to \mathbb{R} \) be given by \( f(x) = x + 1 \) and \( g(x) = x^2 \). Then \( f \circ g(x) = f(x^2) = x^2 + 1 \) and \( g \circ f(x) = g(x + 1) = (x + 1)^2 \). So, \( f \circ g \neq g \circ f \).

Lemma 3.26. Let \( f : A \to B \), \( g : B \to C \) and \( h : C \to D \) be functions. Then:

(i) \( f \circ \text{id}_A = f = \text{id}_B \circ f \).

(ii) \( h \circ (g \circ f) = (h \circ g) \circ f \) (composition is associative).

(iii) If \( f \) and \( g \) are injective then \( g \circ f \) is injective.

(iv) If \( f \) and \( g \) are surjective then \( g \circ f \) is surjective.

(v) If \( f \) and \( g \) are bijective then \( g \circ f \) is bijective.

Proof of iii. Suppose \( f \) and \( g \) are injective and \( x, y \in A \) are distinct elements (i.e., \( x \neq y \)). As \( f \) is injective, \( f(x) \neq f(y) \). Since \( g \) is injective, \( g(f(x)) \neq g(f(y)) \). Therefore, \( (g \circ f)(x) \neq (g \circ f)(y) \), proving that \( g \circ f \) is injective.

Definition 3.27. Suppose \( f : X \to Y \) and \( g : Y \to X \) are functions. The function \( g \) is called a compositional inverse (or inverse) of \( f \) if both \( f \circ g = \text{id}_Y \) and \( g \circ f = \text{id}_X \).

Clearly, if \( g \) is an inverse of \( f \) then \( f \) is an inverse of \( g \).
Lemma 3.28. If there is a compositional inverse of $f : X \to Y$ then that compositional inverse is unique.

Proof. Assume that both $g : Y \to X$ and $h : Y \to X$ are compositional inverses of $f$. We have

$$g = g \circ \text{id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \text{id}_X \circ h = h,$$

proving $g = h$. Since any two compositional inverses of $f$ must be equal, if $f$ has a compositional inverse, then it is unique. \qed

The above proof shows something more specific: if $f$ has a left inverse $g$ and a right inverse $h$ (i.e., $g \circ f = \text{id}_X$ and $f \circ h = \text{id}_Y$) then these single-sided inverses are equal and $f$ has a compositional inverse.

Definition 3.29. A function $f : X \to Y$ is invertible if it has a compositional inverse. The unique compositional inverse of $f$ is denoted $f^{-1} : Y \to X$.

Example 3.30.

(i) The function $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3\}$ and its compositional inverse are given below.

$$
\begin{align*}
  f(1) &= 3 & f^{-1}(1) &= 2 \\
  f(2) &= 1 & f^{-1}(2) &= 3 \\
  f(3) &= 2 & f^{-1}(3) &= 1 \\
  f(4) &= 5 & f^{-1}(4) &= 5 \\
  f(5) &= 4 & f^{-1}(5) &= 4
\end{align*}
$$

(ii) $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ has compositional inverse $\ln : \mathbb{R}_{>0} \to \mathbb{R}$.

(iii) $\sin : [-\pi/2, \pi/2] \to [-1, 1]$ has compositional inverse $\arcsin : [-1, 1] \to [-\pi/2, \pi/2]$.

(iv) $\text{id}_X : X \to X$ is its own compositional inverse.
Theorem 3.31. A function is invertible if and only if it is a bijection.

Proof. Assume \( f : X \to Y \) is invertible. Take \( a, b \in X \) with \( a \neq b \). As \( f^{-1}(f(a)) = a \neq b = f^{-1}(f(b)) \) we see that \( f(a) \neq f(b) \). Thus, \( f \) is injective. If we pick \( c \in Y \) then \( f(f^{-1}(c)) = c \) and therefore \( c \in \text{Im} \, f \). Thus \( f \) is surjective and hence bijective.

For the other direction, assume that \( f : X \to Y \) is a bijection. Given \( c \in Y \), we know there exists \( a \in X \) with \( f(a) = c \) as \( f \) is surjective. If \( b \in X \) has \( f(b) = c = f(a) \) then \( a = b \) as \( f \) is injective. Thus, there is a unique element \( a \in X \) which maps to \( c \). So, define a map \( g : Y \to X \) by \( g(c) = a \) where \( a \) is the unique element with \( f(a) = c \). Since \( f(g(c)) = f(a) = c \) and \( g(f(a)) = g(c) = a \), we see that \( f \) is invertible with inverse \( g \).

Corollary 3.32. The composition of two invertible functions is invertible.

Proof. This can be proven directly, or one can use the fact that a composition of two bijections is again a bijection. \( \square \)

Definition 3.33. Two sets \( X \) and \( Y \) have the same cardinality if there exists a bijection between \( X \) and \( Y \). If \( X \) and \( Y \) have the same cardinality, we write \( |X| = |Y| \).

Example 3.34.

(i) There is a bijection between \( \mathbb{N} \) and \( \mathbb{Z} \) and there is a bijection between \( \mathbb{Z} \) and \( \mathbb{Q} \). Therefore,

\[
|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|.
\]

Any set that has the same cardinality as \( \mathbb{N} \) is called countable.

(ii) Cantor’s diagonal argument shows that there is no bijection between \( \mathbb{N} \) and \( \mathbb{R} \). Thus, \( \mathbb{R} \) is not countable. Since the inclusion map \( \iota : \mathbb{N} \to \mathbb{R}, \iota(n) = n \), is an injection, we write \( |\mathbb{N}| < |\mathbb{R}| \). There can be no proof that there exists a set \( X \) with \( |\mathbb{N}| < |X| < |\mathbb{R}| \), nor can there be a proof that no such set exists. Therefore, one cannot use mathematics to decide whether there are infinite sets smaller than \( \mathbb{R} \) that are not countable. (See the wikipedia article on the Continuum Hypothesis.)
Section 4: Integers

4.1 Induction Principle

We have seen that the axiomatic of infinity defines the natural numbers recursively:

Axiom 4.1 (Axiom of Infinity). The set $\mathbb{N}$ of natural numbers is the smallest set containing

- the integer 0, and
- the integer $n + 1$, whenever $n \in \mathbb{N}$.

Since $0 \in \mathbb{N}$, we know that $0 + 1 = 1 \in \mathbb{N}$. Since $1 \in \mathbb{N}$, we know that $1 + 1 = 2 \in \mathbb{N}$, and so on.

Theorem 4.2 (Mathematical Induction). Let $(p(n))_{n \in \mathbb{N}} = (p(0), p(1), p(2), \ldots)$ be a sequence of mathematical statements whose truths depend only on $n$. If

- $p(0)$ is true, and
- we can prove that $p(n) \Rightarrow p(n + 1)$ for an arbitrary $n \in \mathbb{N}$,

then $p(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let $X = \{n \in \mathbb{N} \mid p(n) = T\} \subseteq \mathbb{N}$ be the set of natural numbers for which $p(n)$ is true. Clearly $0 \in X$ as we have assumed $p(0)$ is true. Furthermore, if $n \in X$ then $p(n)$ is true and therefore $p(n + 1)$ is also true. (We are assuming we have a general proof that $p(n) \Rightarrow p(n + 1)$ for any $n \in \mathbb{N}$.) Thus, if $n \in X$ then $n + 1 \in X$ as well. By the axiom of infinity, $\mathbb{N} \subseteq X$. Thus $X = \mathbb{N}$ and $p(n)$ is true for all $n \in \mathbb{N}$. \hfill $\square$

In a proof by mathematical induction, the proof that $p(0) = T$ is called the base case. The proof that $p(n) \Rightarrow p(n + 1)$ is called the inductive case. When the assumption that $p(n) = T$ is used, it is referred to as the inductive hypothesis. Mathematical induction can be used to prove statements $p(n)$ that hold for $n \in \mathbb{Z}_{\geq N} = \{n \in \mathbb{Z} \mid n \geq N\}$ where $N$ is a given integer. One simply has to change the base case to prove $p(N) = T$; the inductive case remains the same. Indeed, we have the following.
Theorem 4.3 (Induction with Arbitrary Base). Let \( N \) be an integer and let \((p(n))_{n \in \mathbb{Z}_N} = (p(N), p(N+1), p(N+2), \ldots)\) be a sequence of mathematical statements whose truths depend only on \( n \). If

- \( p(N) \) is true, and
- we can prove that \( p(k) \Rightarrow p(k+1) \) for an arbitrary integer \( k \geq N \),

then \( p(n) \) is true for all integers \( n \geq N \).

Proof. Let \( q(n) = p(n+N) \) for each integer \( n \geq 0 \). Then \( q(0) = p(N) \) is true by the first assumption. Also, \( q(k) \Rightarrow q(k+1) \) for each \( k \geq 0 \) since \( p(k+N) \Rightarrow p(k+N+1) \) by the second assumption.

Thus \( q(n) \) is true for all integers \( n \geq 0 \) by induction (Theorem 4.2); in other words, \( p(n) \) is true for all \( n \geq N \). \( \square \)

The following theorems, though interesting on their own, are examples of mathematical induction in action.

Theorem 4.4 (Gauss’s Punishment). For every integer \( n \geq 1 \),

\[
1 + 2 + \cdots + n = \frac{n(n+1)}{2}.
\]

Proof. If \( n = 1 \) then \( 1 + 2 + \cdots + n = 1 \) and \( n(n+1)/2 = (1)(2)/2 = 1 \). Therefore, the theorem holds in this case.

Assume that the formula holds for some integer \( n \geq 1 \). We now show that the formula holds for \( n+1 \). The sum \( 1 + 2 + \cdots + n + (n+1) = (1 + 2 + \cdots + n) + (n+1) = n(n+1)/2 + (n+1) \) using our assumption that the theorem holds for \( n \). Since \( n(n+1)/2 + (n+1) = (n+1)(n/2 + 1) = (n+1)(n+2)/2 \) we see that \( 1 + 2 + \cdots + n + (n+1) = (n+1)(n+2)/2 \) and hence the theorem holds for \( n+1 \).

We have shown that the theorem holds for \( n = 1 \) and if the theorem holds for some \( n \geq 1 \) then it also holds for \( n+1 \). By mathematical induction, the theorem holds for all \( n \geq 1 \). \( \square \)

Theorem 4.5. For all \( n \geq 1 \), \( x^n - 1 = (x-1)(x^{n-1} + \cdots + 1) \).

Proof. We proceed by induction on \( n \). For the base case, when \( n = 1 \), \( x^1 - 1 = x - 1 \) and \( (x-1)(x^{n-1} + \cdots + 1) = (x-1)(1) = x - 1 \). Therefore, the theorem holds when \( n = 1 \).
For our inductive step, assume that \( x^n - 1 = (x - 1)(x^{n-1} + \cdots + 1) \) with the aim of showing that \( x^{n+1} - 1 = (x - 1)(x^n + \cdots + 1) \). Using our inductive hypothesis,

\[
x^{n+1} - 1 = x^{n+1} - x^n + x^n - 1 = (x - 1)x^n + (x - 1)(x^{n-1} + \cdots + 1) = (x - 1)(x^n + x^{n-1} + \cdots + 1).
\]

Therefore, the theorem holds for \( n + 1 \). By induction, the theorem holds for all \( n \geq 1 \).

We now introduce two other variants of mathematical induction.

**Theorem 4.6 (Strong Induction).** Let \( N \) be an integer and let \( (p(n))_{n \in \mathbb{Z} \geq N} = (p(N), p(N+1), p(N+2), \ldots) \) be a sequence of mathematical statements whose truths depend only on \( n \). If

- \( p(N) \) is true, and
- we can prove that \( [p(N) \land p(N+1) \land \cdots \land p(k)] \Rightarrow p(k+1) \) for an arbitrary \( k \geq N \),

then \( p(n) \) is true for all \( n \geq N \).

**Proof.** For each \( n \geq N \), let \( q(n) \) be the statement that \( [p(N) \land p(N+1) \land \cdots \land p(n)] \) is true.

Then \( q(N) \) is true by the first assumption. Also, if \( q(k) \) is true for \( k \geq N \), then the second assumption directly imply that \( p(k+1) \) is true and hence \( q(k+1) \) is also true. Thus \( q(n) \) is true for all \( n \geq N \) by Theorem 4.3, and therefore \( p(n) \) is true for all \( n \geq N \).

**Remark 4.7.** Strong induction allows us to use a stronger inductive hypothesis than in Theorem 4.3. Instead of assuming that \( p(n) \) is true while trying to show \( p(n+1) \), we get to assume that every \( p(k) \) is true for \( N \leq k \leq n \).

In the next section, we will use strong induction to show that every integer has a factorization into primes.

**Theorem 4.8 (Well-Ordering Principle).** Any non-empty set \( X \subseteq \mathbb{N} \) of natural numbers has a least element (i.e., there exists \( m \in X \) such that \( m \leq x \) for all \( x \in X \)).
Proof. We will prove this result using strong induction (Theorem 4.6 with \( N = 0 \)).

Let \( X \) be a non-empty set of natural numbers (\( X \subseteq \mathbb{N} \)) and assume that \( X \) has no least element. We will show that this assumption results in a contradiction.

Let \( p(n) \) be the statement “\( n \) is not a member of \( X \).” Then \( p(0) \) is true, since if 0 were to be an element of \( X \), then it would be the least element of \( X \) (but \( X \) is assumed to have no least element). Also, if \( p(0), p(1), \ldots, p(k) \) are true for some \( k \geq 0 \), then none of the numbers 0, 1, \ldots, \( k \) are elements of \( X \). But then \( k + 1 \) is not in \( X \) (if it were in \( X \), it would be the least element of \( X \)). Thus \( p(k + 1) \) is true. Thus by strong induction, we have that \( p(n) \) is true for all integers \( n \geq 0 \), that is \( n \notin X \) for all natural numbers \( n \in \mathbb{N} \). This directly yields that the set \( X \) is empty, contradicting our original assumption on \( X \) being non-empty.

\( \square \)

**Theorem 4.9.** Mathematical induction (Theorem 4.2) \( \iff \) induction with arbitrary base (Theorem 4.3) \( \iff \) strong induction (Theorem 4.6) \( \iff \) the well-ordering principle (Theorem 4.8).

**Proof.** We already showed that Theorem 4.2 \( \Rightarrow \) Theorem 4.3 \( \Rightarrow \) Theorem 4.6 \( \Rightarrow \) Theorem 4.8. To complete, the proof we next show that Theorem 4.8 \( \Rightarrow \) Theorem 4.2 (i.e., that the well-ordering principle implies the principle of mathematical induction).

Suppose that the two assumptions of the principle of mathematical induction (Theorem 4.2) hold for statement \( p(n) \). Let \( X \) be a set of natural numbers \( x \) for which \( p(x) \) is false:

\[
X = \{ x \in \mathbb{N} : p(x) = F \}.
\]

We will show by contradiction (using the well-ordering principle) that \( X \) is empty and conclude that \( p(n) \) is true for all integers \( n \geq 0 \), hence proving the principle of mathematical induction.

Assume (by contradiction) that \( X \neq \emptyset \). Then, be the well ordering principle, \( X \) must have a least element, which we denote by \( m \). Since \( p(0) \) is true, we conclude that \( 0 \notin X \). Thus the least element \( m \) of \( X \) must satisfy \( m \geq 1 \). Hence \( m > m - 1 \geq 0 \) and by definition \( m \) being the smallest element of \( X \), we must have that \( p(m - 1) \) is true. Thus (by the second assumption on \( p(\cdot) \) of Theorem 4.2), we have that \( p(m) \) is true, which contradicts the fact that
Thus, we conclude that \( X \) must be empty; thus \( p(n) \) is true for all natural numbers. \( \square \)

### 4.2 Factorization

**Definition 4.10.** For two integers \( a, b \in \mathbb{Z} \) we say that \( a \) divides \( b \) and write \( a \mid b \) if there exists an integer \( q \) with \( b = qa \). If \( a \mid b \) then we call \( a \) a divisor or factor of \( b \).

The natural numbers are partially ordered by divisibility:

- **Reflexivity:** For \( a \in \mathbb{N} \), \( a = (1)a \). Thus, \( a \mid a \).
- **Anti-Symmetry:** For \( a, b \in \mathbb{N} \), if \( a \mid b \) and \( b \mid a \) then there exists \( q, r \in \mathbb{Z} \) with \( b = ra \) and \( a = qb \). Therefore \( b = rqb \). If \( b = 0 \) then \( a = qb = q0 = 0 \) and hence \( a = b \). Otherwise, \( b \neq 0 \) and canceling \( b \) from \( b = rqb \) we get \( rq = 1 \). Since \( r, q \in \mathbb{Z} \) and \( a, b \in \mathbb{N} \), we see that \( r = q = 1 \) and hence \( a = b \).
- **Transitivity:** If \( a \mid b \) and \( b \mid c \) then there exist \( q, r \) with \( b = qa \) and \( c = rb \). Therefore \( c = rqa \) and hence \( a \mid c \).

Within this partial order, 0 is the **top element** (the unique maximum) since for all \( a \in \mathbb{N} \), \( 0 = 0a \) and hence \( a \mid 0 \). Furthermore, 1 is the **bottom element** (the unique minimum) since for all \( a \in \mathbb{N} \), \( a = a(1) \) and hence \( 1 \mid a \).

**Definition 4.11.** An integer \( p > 1 \) is prime if its only positive divisors are 1 and \( p \). Otherwise \( p \) is called composite.

There are some convenient conventions for empty sums and products. A sum with zero summands evaluates to zero. A product of zero terms evaluates to one. A sum or product of a single number is simply that single number. A statement of the form “for all \( x \in X \), \( p(x) \)” is true if \( X = \emptyset \); we call the statement **vacuously true**.

**Theorem 4.12.** Every integer \( n > 1 \) can be expressed as a product \( n = p_1 \cdots p_k \) of one or more primes \( p_1, \ldots, p_k \).

**Proof.** Let \( n > 1 \) be a positive integer.

We will proceed by strong induction. For the base case, \( n = 2 \) is prime and can be written as a product of a single prime – itself.
Assume that every integer $1 \leq k < n$ can be written as the product of primes. If the integer $n$ is prime, then $n$ is the product of one prime – itself – and we are done. If $n$ is not prime, then $n = ab$ where $1 < a < n$ and $1 < b < n$. Our strong inductive hypothesis applies to both $a$ and $b$. That is, both $a$ and $b$ can be expressed as products of primes. Thus, $n = ab$ is also a product of primes – namely those appearing in the expression for $a$ along with those in the expression for $b$.

\[ \square \]

**Lemma 4.13.** If $a \mid (b + c)$ and $a \mid b$ then $a \mid c$.

**Proof.** As $a \mid (b + c)$ there is an integer $q$ with $b + c = qa$. As $a \mid b$ there is an integer $r$ with $b = ra$. Thus, $c = qa - b = qa - ra = (q - r)a$ with $q - r \in \mathbb{Z}$ and therefore $a \mid c$. \[ \square \]

**Theorem 4.14** (Euclid, circa. 300 BC). There are infinitely many primes.

**Proof.** Assume for a contradiction that there is a finite number of primes. This means we can list all the primes as $p_1, \ldots, p_k$. Let $n = p_1 \cdots p_k + 1$.

By our previous theorem, $n$ can be expressed as a product of one or more primes. Let $p_i$ be a prime dividing $n$. Since $p_i$ divides $p_1 \cdots p_k$, there we must have $p_i \mid 1$ by the previous lemma. However, 1 is the only positive integer dividing 1 and 1 is not prime. This contradicts our choice of $p_i$. Therefore, our assumption that there is a finite number of primes is false; there are infinitely many primes. \[ \square \]

**Theorem 4.15** (*Unique Factorization*). Every positive integer can be expressed as a product of primes in a unique way, up to reordering the factors.

For example, $60 = 2^2 \cdot 3 \cdot 5$. Unique factorization is something that holds in other settings as well. For instance, every polynomial with coefficients in a field\(^2\) ($\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ for prime $p$) can be factored into irreducible polynomials over the same field. These irreducible polynomials are unique up to reordering, and up to (arithmetic) multiplication by invertible elements. E.g., for polynomial with coefficients in $\mathbb{Q}$, 2 is invertible since $1/2 \in \mathbb{Q}$. Despite having $2x^2 - 18 = (2x - 6)(x + 3) = (x - 3)(2x + 6)$, we say polynomials over $\mathbb{Q}$ factor uniquely into irreducibles. Really we treat $2x - 6$ and $x - 3$ as the same factor up to scaling by an invertible element (and similarly for $x + 3$ and $2x + 6$). This is an issue if we want to factor all integers (including negative integers); in $\mathbb{Z}$,

\(^2\)Fields will be examined later on.
the only invertible elements (under arithmetic multiplication) are 1 and $-1$. Therefore, $6 = 2 \cdot 3 = (-2) \cdot (-3)$ does not prevent us from saying integers factor uniquely.
Section 5: The Euclidean Algorithm

5.1 Division Algorithm

The Euclidean division and extended division algorithms form the backbone of most arithmetic computations.

Theorem 5.1 (Division Algorithm). Given integers $n$ and $d$ where $d \geq 1$, there exists a unique pair of integers $q, r$ such that $n = qd + r$ and $0 \leq r < d$.

Proof. Let $R = \{ n - ad \mid a \in \mathbb{Z} \text{ and } n - ad \geq 0 \}$. If $n \geq 0$ then $n \in R$ (by using $a = 0$). If $n \leq 0$ then let $a = n$ so $n - ad = n - nd = n(1 - d) \geq 0$ as $n$ and $1 - d$ are negative or zero. Thus, in all cases $R \neq \emptyset$.

Using the well-ordering principle, $R \subseteq \mathbb{N}$ has a least element $r = n - qd \geq 0$. If $r > d$ then $0 \leq r - d = n - (q + 1)d$ and hence $r - d \in R$. This contradicts our choice of $r$ as the least element in $R$. Therefore, $r < d$. Rearranging we get $n = qd + r$.

If $q'$ and $r'$ are integers with $n = q'd + r'$ and $0 \leq r' < d$ then $q'd + r' = qd + r$ and therefore $r - r' = (q - q')d$ and hence $r - r'$ is divisible by $d$. Since $-d < r - r' < d$, we must have $r - r' = 0$ and hence $r' = r$. Thus, $(q - q')d = 0$ and hence $q - q' = 0$ as $d \geq 1$. This shows that $q$ and $r$ are uniquely determined. \hfill \Box

Example 5.2. You can use long division to find $q$ and $r$. For example, the calculation on the right shows $4321 = 360(12) + 1$.

Note that the remainder $r = 1$ falls in the range $0 \leq r < 12$.

5.2 Greatest Common Divisor

Definition 5.3. The greatest common divisor of $n, m \in \mathbb{Z}$ is the unique integer $\gcd(n, m) \in \mathbb{N}$ with

(i) $\gcd(n, m) \mid m$ and $\gcd(n, m) \mid n$,

(ii) if $k \mid m$ and $k \mid n$, then $k \mid \gcd(n, m)$.

The greatest common divisor of two integers, should it exist, is unique since any two non-negative integers with the above properties must divide each other and are therefore equal (by anti-symmetry of division). We will soon prove that $\gcd(n, m)$ always exists.
Example 5.4.

(i) \( \gcd(24, 9) = 3 \)

(ii) \( \gcd(72, 30) = 6 \)

(iii) \( \gcd(100, 0) = 100 \)

Proposition 5.5. Let \( m, n \in \mathbb{Z} \) be two integers with prime factorizations \( m = \pm(p_1^{a_1} \cdots p_k^{a_k}) \) and \( n = \pm(p_1^{b_1} \cdots p_k^{b_k}) \). Here the \( p_i \) are assumed to be distinct primes. (If prime \( p_i \) occurs in \( m \) but not \( n \) then \( b_i = 0 \) and vice versa). The greatest common denominator of \( m \) and \( n \) is

\[
\gcd(m, n) = p_1^\min(a_1, b_1) \cdots p_k^\min(a_k, b_k).
\]

Corollary 5.6.

(i) For \( a, b, m \in \mathbb{Z} \), \( \gcd(am, bm) = m \gcd(a, b) \).

(ii) If \( a, b, c \in \mathbb{Z} \) have \( \gcd(a, c) = 1 \) and \( c \mid ab \) then \( c \mid b \).

(iii) If \( a, b \in \mathbb{Z} \) and \( p \) is prime then if \( p \mid ab \) then \( p \mid a \) or \( p \mid b \).

Given the previous proposition, one might think that we know all there is to know about the greatest common divisor of two integers, since we have a formula for \( \gcd(n, m) \) based on the factorizations of \( n \) and \( m \). The truth is, factorization is hard. While we know factorizations into primes always exist, they are hard to compute. Furthermore, multiplication and addition interact in very complicated ways. So, understanding \( \gcd(n, m) \) multiplicatively says very little about \( \gcd(n, m) \) additively.

The following is a very useful “additive” theorem for \( \gcd(n, m) \).

Theorem 5.7 (Bézout’s Identity). For \( n, m \in \mathbb{N} \) (not both zero), there exist \( a, b \in \mathbb{Z} \) with \( \gcd(n, m) = an + bm \). Furthermore, \( \gcd(n, m) \) is the smallest positive integer of the form \( an + bm \) for \( a, b \in \mathbb{Z} \).

Proof. Let \( W = \{an + bm \mid a, b \in \mathbb{Z} \text{ and } an + bm > 0\} \) be the set of all integer combinations of \( n \) and \( m \) that are positive. If we choose \( a = n \) and \( b = m \) then \( an + bm = n^2 + m^2 > 0 \) (since \( n \) and \( m \) are not both zero). Therefore \( W \neq \emptyset \).

By the well-ordering principle, there is a smallest element \( d \in W \). As \( d \in W \) we may write \( d = sn + tm \) for some \( s, t \in \mathbb{Z} \). We now show that \( d = \gcd(n, m) \) by verifying it has the properties stated in the definition of \( \gcd(n, m) \).
In order to show \( d \) divides \( n \), apply the division algorithm to \( n \) and \( d \). We obtain
\[
n = qd + r \quad \text{for some} \quad 0 \leq r < d.
\]
Solving for \( r \) gives
\[
r = n - qd = n - q(sn + tm) = (1 - qs)n + qtm.
\]
Thus \( r \) is a linear combination of \( n \) and \( m \) and is smaller than \( d \). Since \( d \) is the smallest positive linear combination, \( r \) must be zero. Thus,
\[
n = qd + 0 = qd \quad \text{and hence} \quad d \mid n.
\]
The same argument shows \( d \mid m \).

Finally, take an integer \( k \) with \( k \mid n \) and \( k \mid m \). Since \( n = qk \) and \( m = q'k \), we have
\[
d = sn + tm = sqk + tq'k = (sq + tq')k
\]
and hence \( k \) divides \( d \). Therefore
\[
d = \gcd(n,m).
\]

**Lemma 5.8.** If \( n = qm + r \) for any integers then \( \gcd(n,m) = \gcd(m,r) \).

**Proof.** Let \( d = \gcd(n,m) \). We will show that \( d \) is the greatest common divisor of \( m \) and \( r \) using the conditions given in the definition of \( \gcd(m,r) \). Since greatest common divisors are unique, we will be done.

First we check that \( d \) divides both \( m \) and \( r \). As \( d = \gcd(n,m) \) it's clear that \( d \) divides \( m \). Furthermore, \( r = n - qm \). Since \( d \) divides both \( n \) and \( m \), \( d \) divides \( r \).

Next take an integer \( k \) with \( k \mid m \) and \( k \mid r \). As \( n = qm + r \), we have that \( k \) divides \( n \) as well. Therefore, by definition of \( \gcd(n,m) \), the integer \( k \) divides \( d \). Thus \( d = \gcd(m,r) \).

The Euclidean algorithm is an efficient algorithm for computing greatest common divisors.

**Algorithm 5.9 (Euclidean Algorithm).**

```markdown
function GCD(n, m):
    (q, r) = longDivision(n, m)
    if r == 0 then return m
    return GCD(m, r)
```

Let us examine the above algorithm as it applies to two integers \( n, m \).

\[
\begin{align*}
n &= qm + r_1 \\
m &= q_1r_1 + r_2 \\
r_1 &= q_2r_2 + r_3 \\
r_2 &= q_3r_3 + r_4 \\
&\vdots \\
\end{align*}
\]
\[
\begin{align*}
0 &< r_1 < m \\
0 &< r_2 < r_1 \\
0 &< r_3 < r_2 \\
0 &< r_4 < r_3 \\
&\vdots \\
\end{align*}
\]
\[ r_{k-2} = q_{k-1}r_{k-1} + r_k \quad 0 < r_k < r_{k-1} = \gcd(r_{k-2}, r_{k-1}) \]
\[ r_{k-1} = q_k r_k + 0 \quad 0 = r_{k+1} = \gcd(r_{k-1}, r_k) = r_k \]

By the previous lemma, we have

\[ \gcd(n, m) = \gcd(m, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k). \]

At the last stage, where \( r_k \mid r_{k-1} \), the greatest common divisor can be computed explicitly as \( r_k \). Since \( r_{i+1} < r_i \) for all \( i \), the sequence of remainders is strictly decreasing. Since \( r_i \geq 0 \) for all \( i \), the algorithm must terminate in at most \( m + 1 \) steps.

**Example 5.10.** Using the Euclidean algorithm we compute \( \gcd(100, 28) \):

\[
\begin{align*}
100 &= 3(28) + 16 & 0 < 16 < 28 & \gcd(100, 28) \\
28 &= 1(16) + 12 & 0 < 12 < 16 & = \gcd(28, 16) \\
16 &= 1(12) + 4 & 0 < 4 < 12 & = \gcd(16, 12) \\
12 &= 3(4) + 0 & = \gcd(12, 4) = 4
\end{align*}
\]

The running time of the Euclidean algorithm is quadratic in the number of digits of the two inputs, making it extremely fast for most purposes.

Now that we have an algorithm for \( \gcd(n, m) \), we want to find integers \( a, b \) with \( an + bm = \gcd(n, m) \). The extended Euclidean algorithm solves this problem.

**Example 5.11.** In order to find \( a, b \) with \( a(100) + b(28) = \gcd(100, 28) = 4 \), we start at the second last line of the Euclidean algorithm and solve for \( \gcd(100, 28) = 4 \):

\[ 16 = 1(12) + 4 \implies 4 = 16 - 1(12). \]

We now use each of the preceding steps in the Euclidean algorithms to make substitutions until we express \( 4 = \gcd(100, 28) \) in terms of 100 and 28:

\[
\begin{align*}
16 &= 1(12) + 4 \implies 4 &= 16 - 1(12) \\
28 &= 1(16) + 12 \implies 4 &= 16 - 1(28 - 1(16)) \\
&= 2(16) - 1(28) \\
100 &= 3(28) + 16 \implies 4 &= 2(100 - 3(28)) - 1(28) \\
&= 2(100) - 7(28)
\end{align*}
\]

Therefore \( 4 = 2(100) - 7(28) \).
Algorithm 5.12 (Extended Euclidean Algorithm).

// Returns a triple (d, s, t) where \( \gcd(n,m) = d = sn + tm \)
function extendedGCD(n, m):
  (q, r) = longDivision(n, m)
  if \( r = 0 \) then return \((m, 0, 1)\)
  (d, a, b) = extendedGCD(m, r)
  return \((d, b, a - q*b)\)

We can check the recursive step for correctness. When \(\text{extendedGCD}\) is called on \(m\) and \(r\), it returns \((d,a,b)\) with \(am + br = d = \gcd(m,r) = \gcd(n,m)\).

Since \(n = qm + r\), we have

\[
\gcd(n,m) = am + br = am + b(n - qm) = bn + (a - qb)m = sn + tm.
\]

Therefore, the correct output is \((d,b,a - qb)\).
Section 6: Modular Arithmetic

In this section we introduce a new number system: the integers modulo \( n \). This new number system carries with it a definition for addition and multiplication of its elements. Addition and multiplication will act in the familiar way as for real numbers and polynomials, just to give two examples. The arithmetic in this new number system is useful for cryptographic and coding purposes.

6.1 Congruence Classes

We begin by recalling the definition for congruence.

Fix an integer \( n \neq 0 \). Two integers \( a, b \in \mathbb{Z} \) are congruent modulo \( n \) if \( n | (a - b) \). We write \( a \equiv b \pmod{n} \). Congruence is an equivalence relation on the integers. The set of all congruence classes modulo \( n \) (i.e., the quotient set of all equivalence classes) is denoted \( \mathbb{Z}_n \). A general equivalence class \([a] \in \mathbb{Z}_n\) takes the form

\[
[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = \{a + qn \mid q \in \mathbb{Z}\}.
\]

Example 6.1. As \(-3, 1, 5, 9\) all differ by multiples of four, we know that every pair of these numbers is congruent modulo 4. For example, \(-3 \equiv 1 \pmod{4}, -3 \equiv 5 \pmod{4}\), and so on. The congruence class \([1] \in \mathbb{Z}_4\) is

\[
[1] = \{\ldots, -3, 1, 5, 9, \ldots\} = \{4q + 1 \mid q \in \mathbb{Z}\}.
\]

Proposition 6.2. For every congruence class \( X \in \mathbb{Z}_n \), there is a unique integer \( r \) with \( 0 \leq r < n \) and \( X = [r] \). In other words,

\[
\mathbb{Z}_n = \{[0], \ldots, [n-1]\}.
\]

Proof. First, we show that such an \( r \) exists. Every \( X \in \mathbb{Z}_n \) is the congruence class of some \( m \in \mathbb{Z} \). That is \( X = [m] \) for some \( m \). Using the division algorithm, we can divide \( m \) by \( n \) to obtain an expression \( m = qn + r \) where \( q \in \mathbb{Z} \) and \( 0 \leq r < n \). The difference between \( m \) and \( r \) is divisible by \( n \) as \( m - r = qn \). Therefore \( m \equiv r \pmod{n} \) and hence \( X = [m] = [r] \).

For uniqueness, assume that there another integer \( r' \) with \( 0 \leq r' < n \) and \( X = [r'] \). Without loss of generality, assume that \( r' \leq r \). (If this is not the case,
reverse their roles in what is to come.) As \([r] = X = [r']\) we conclude that \(r\) and \(r'\) differ by a multiple of \(n\). If \(r \neq r'\) then \(r - r' > n\) and \(0 \leq r - r' < r < n\), which is contradictory. Therefore \(r = r'\).

Addition and multiplication are binary operators on \(\mathbb{Z}\), meaning they are functions of the form \(\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}\). For example, addition is the map \((a, b) \mapsto a + b\). These functions induce operations on congruence classes.

**Definition 6.3.** Let addition an multiplication on \(\mathbb{Z}_n\) be two binary operators \(\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n\) defined by

\[
[a] + [b] = [a + b] \\
[a] \cdot [b] = [ab].
\]

The rules given above for addition and multiplication seem to depend on the choice of representative given. In fact, they do not.

**Example 6.4.** Take \([3], [5] \in \mathbb{Z}_6\). We can represent these equivalences classes as \([3] = [9]\) and \([5] = [11]\), as well. Addition does not depend on the choice of representative:

\[
[3] + [5] = [3 + 5] = [8] \\
[9] + [11] = [9 + 11] = [20] = [2]\]

Multiplication also does not depend on the choice of representative:

\[
\]

**Proposition 6.5.** The operations of addition and multiplication are well-defined.

**Proof.** Take \(a, b, x, y \in \mathbb{Z}\) with \(a \equiv x \pmod{n}\) and \(b \equiv y \pmod{n}\). That is, \([a] = [x]\) and \([b] = [y]\) in \(\mathbb{Z}_n\). We need to show that \([a] + [b] = [x] + [y]\), or, in other words, addition of congruence classes does not depend on our choices of representatives.

From the definition \([a] + [b] = [a + b]\) and \([x] + [y] = [x + y]\), so it suffices to show that \(a + b \equiv x + y \pmod{n}\). As \(a \equiv x \pmod{n}\), \(n |(a - x)\). Similarly, as \(b \equiv y \pmod{n}\), \(n |(b - y)\). Consequently, \(n\) divides the sum of \(a - x\) and \(b - y\). That is, \(n |((a + b) - (x + y))\) and hence \(a + b \equiv x + y \pmod{n}\). Therefore
\[ [a] + [b] = [a + b] = [x + y] = [x] + [y]. \] So, addition of congruence classes is well defined.

For multiplication, again assume \([a] = [x]\) and \([b] = [y]\). We want to show that \([a] \cdot [b] = [x] \cdot [y]\).

As \([a] = [x]\) and \([b] = [y]\) we know \(n|(a - x)\) and \(n|(b - y)\) and consequently \(a = qn + x\) and \(b = q'n + y\) for some \(q, q' \in \mathbb{Z}\).

We have \(ab = (qn + x)(q'n + y) = qq'n^2 + xq'n + yqn + xy\), we see that \(ab - xy = (qq'n + xq' + yq)n\) and hence \(n|(ab - xy)\). Therefore \(ab \equiv xy \pmod{n}\) and thus \([ab] = [xy]\). Therefore \([a] \cdot [b] = [ab] = [xy] = [x] \cdot [y]\) and so, multiplication of congruence classes is well-defined.

**Example 6.6.** The following are the addition and multiplication tables for \(\mathbb{Z}_6\).

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\cdot</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

### 6.2 Units in \(\mathbb{Z}_n\)

**Definition 6.7.** A ring is a triple \((R, +, \cdot)\) of a set \(R\) along with two binary operations \(+ : R \times R \to R\) and \(\cdot : R \times R \to R\) which satisfy the following properties for all \(a, b, c \in R\):

- (i) \((a + b) + c = a + (b + c)\), (associativity of +).
- (ii) there exists \(0 \in R\) with \(0 + a = a\), (additive identity).
- (iii) \(a + b = b + a\), (commutativity of +).
- (iv) for each \(a \in R\) there exists \(b \in R\) with \(a + b = 0\), (additive inverse).
- (v) \(a(bc) = (ab)c\), (associativity of \(\cdot\)).
- (vi) there exists \(1 \in R\) with \(1a = a = a1\), (multiplicative identity).
- (vii) \(a(b + c) = ab + ac\) and \((b + c)a = ba + ca\). (distributivity).

A ring is said to be **commutative** if \(ab = ba\) for all all \(a, b \in R\).
Proposition 6.8. \( \mathbb{Z}_n \) is a commutative ring.

Proof. Since \( \mathbb{Z} \) is a ring, it is easy to check that \( \mathbb{Z}_n \) inherits all the necessary properties. For example, \([a] + [b] + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]). \)

A field is a commutative ring \( R \) in which every non-zero element has a multiplicative inverse; i.e., for all \( a \in R \setminus \{0\} \), there is some \( b \in R \) with \( ab = 1 \) (in this case, we write \( b = a^{-1} \)). The rings \( \mathbb{Q}, \mathbb{R} \) and \( \mathbb{C} \) are examples of fields. If \( a \in R \) has a multiplicative inverse, we call \( a \) a unit or say that it is invertible. We say \( a \in R \) is a zero-divisor if \( a \neq 0 \) and there exists some \( b \neq 0 \) in \( R \) with \( ab = 0 \).

The ring \( \mathbb{Z}_n \) is not always a field. For example, in \( \mathbb{Z}_6 \), \([3]\) has no multiplicative inverse.

Theorem 6.9. The congruence class \([a] \in \mathbb{Z}_n \) has a multiplicative inverse if and only if \( \gcd(a, n) = 1 \).

Proof. We know that \( \gcd(a, n) = 1 \) if and only if \( ba + cn = 1 \) for some \( b, c \in \mathbb{Z} \). Rearranging this formula we get, \( ba - 1 = cn \) (or equivalently \( ba \equiv 1 \pmod{n} \)) and therefore \([b][a] = [ba] = [1]\). Furthermore, one can follow this logic in reverse to show that if \([b][a] = [1]\) then there is some \( c \in \mathbb{Z} \) with \( ba + cn = 1 \) and hence \( \gcd(a, n) = 1 \).

When \( \gcd(a, n) = 1 \) we say \( a \) and \( n \) are relatively prime.

Theorem 6.10. Fix \( n \geq 2 \). The following statements are equivalent:

(a) Every non-zero element \([a] \in \mathbb{Z}_n \) has an inverse.

(b) \( \mathbb{Z}_n \) contains no zero-divisors.

(c) \( n \) is prime.

Proof. In order to prove a three-way equivalence like the above, it is enough to show that \((a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)\).

For \((a) \Rightarrow (b)\), assume that every non-zero element of \( \mathbb{Z}_n \) has an inverse. If \([a] \in \mathbb{Z}_n \) is a zero divisor then \([a] \neq 0 \) and there is some non-zero \([b] \in \mathbb{Z}_n \) with \([a][b] = [0]\). As \([a]\) is non-zero, it is invertible by our assumption.

So \([b] = [a]^{-1}[a][b] = [a]^{-1}[0] = [0]\), contradicting our assumption of \([b]\) as being a non-zero element. Therefore, assuming \((a)\), we have shown that \( \mathbb{Z}_n \) has no zero-divisors.
Instead of proving \((b) \Rightarrow (c)\), we prove its contrapositive \(\neg (c) \Rightarrow \neg (b)\).
Assume \(n\) is composite and therefore \(n = ab\) where \(1 < a < n\) and \(1 < b < n\).
Since \([a]\) and \([b]\) are non-zero elements of \(\mathbb{Z}_n\) and \([a] \cdot [b] = [ab] = [n] = [0]\),
we see that \([a]\) and \([b]\) are zero-divisors. Thus, we have proven \(\neg (b)\).
Since a statement and its contrapositive are logically equivalent, we have \((b) \Rightarrow (c)\).

Finally, to show \((c) \Rightarrow (a)\), assume that \(n\) is prime. Let \([a] \in \mathbb{Z}_n\) be an
arbitrary non-zero element. Since \([a] \neq [0]\), we see that \(n\) does not divide \(a\).
As \(n\) is prime, we have \(\gcd(a, n) = 1\) and therefore \([a] \in \mathbb{Z}_n\) is invertible by the
previous theorem. Thus, all non-zero elements of \(\mathbb{Z}_n\) are invertible when \(n\) is prime.

The equivalence of \((a)\) and \((c)\) in the above theorem tells us that \(\mathbb{Z}_n\) is a
field precisely when \(n\) is prime.

**Example 6.11.** Every non-zero congruence classes in \(\mathbb{Z}_5\) has an inverse.

\[
\begin{array}{c|cccc}
  \cdot & 0 & 1 & 2 & 3 & 4 \\
\hline
  0 & 0 & 0 & 0 & 0 & 0 \\
  1 & 0 & 1 & 2 & 3 & 4 \\
  2 & 0 & 2 & 4 & 1 & 3 \\
  3 & 0 & 3 & 1 & 4 & 2 \\
  4 & 0 & 4 & 3 & 2 & 1 \\
\end{array}
\]


Given any two invertible elements \([a], [b] \in \mathbb{Z}_n\), their product \([a][b]\) is also
invertible with inverse \([b]^{-1}[a]^{-1}\). Thus, powers of an invertible element are
always invertible.

**Lemma 6.12.** Given a unit \([a] \in \mathbb{Z}_n\), there is some \(m \in \mathbb{Z}\) with \([a]^m = [1]\).

**Proof.** Consider the sequence \([a], [a]^2, [a]^3\) and so on. Since there are a finite
number of elements in \(\mathbb{Z}_n\), at some point an element must repeat itself. That
is, there are some distinct integers \(1 \leq k < \ell\) with \([a]^k = [a]^\ell\). Since \([a]\) is
invertible we can multiply both sides by \([a]^{-k}\) to obtain \([1] = [a]^0 = [a]^\ell-k\).
Therefore \([a]^m = [1]\) where \(m = \ell - k\). \(\square\)

It is a natural question to ask which exponents \(m\) will give \([a]^m = [1]\).
Fermat’s little theorem and Euler’s theorem give us a choice of \(m\) which works
for all units in \(\mathbb{Z}_n\) simultaneously.
Theorem 6.13 (Fermat’s Little Theorem). If $p$ is prime and $[a] \in \mathbb{Z}_p$ is non-zero then

$$[a]^p = [a].$$

In the above theorem, we do not need to restrict ourselves to $[a] \neq [0]$ since $[0]^p = [0]$ for any $p \geq 1$. However, it is preferable to think of $[a] = [0]$ as a separate case, and focus instead on invertible elements. In $\mathbb{Z}_p$ with $p$ prime, every element other than zero is invertible.

Furthermore, if $[a]^p = [a]$ then we also have $[a]^{p-1} = [1]$ since $[a] \neq 0$ is invertible in $\mathbb{Z}_p$ for $p$ prime.

Fermat’s little theorem is often phrased using modular arithmetic: if $p$ is prime and $a \neq 0$ then $a^{p-1} \equiv 1 \pmod{p}$.

Example 6.14. We compute the remainder of $9^{1234}$ upon division by 11. By Fermat’s little theorem, $9^{10} \equiv 1 \pmod{11}$. Working modulo 11,

$$9^{1234} \equiv (9^{1230})(9^4) \equiv (9^{1230})(9^4) \equiv (9^{123})(9^4) \equiv (1)^{123}(9^4) \equiv 9^4 \equiv 81^2 \equiv 4^2 \equiv 16 \equiv 5.$$ Thus the remainder of $9^{1234}$ after division by 11 is 5.

We will come back and prove Fermat’s little theorem using some elementary group theory. Fermat’s little theorem is a short step away from Euler’s theorem:

Theorem 6.15 (Euler’s Theorem). If $[a]$ is a unit in $\mathbb{Z}_n$ then

$$[a]^\phi(n) = [1]$$

where $\phi(n)$ is the number of units in $\mathbb{Z}_n$.

In terms of modular arithmetic, Euler’s Theorem reads as follows:

Theorem 6.16 (Euler’s Theorem – alternative version). If $\gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n) = |\{b \in \mathbb{Z} \mid 1 \leq b \leq n \text{ and } \gcd(b, n) = 1\}|$.

The RSA cryptographic system is a clever method of sending securely encrypted messages. It relies on Euler’s theorem and the difficulty of factoring integers (see also Section 1.6 of the textbook).
Section 7: Groups

Definition 7.1 (Group). A non-empty set $G$ along with a binary operation $G \times G \to G$, written $(g, h) \to g \cdot h$, is called a group if it satisfies the following properties:

(i) Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.

(ii) Identity: There exists an element $e \in G$ such that $a \cdot e = a = e \cdot a$ for all $a \in G$. The element $e$ is called the identity of $G$. (We will prove that it is unique.)

(iii) Inverse: For any $a \in G$, there exists $b \in G$ such that $b \cdot a = a \cdot b = e$. We call $b$ the inverse of $a$ and write $b = a^{-1}$. (We will prove that any element $a \in G$ has a unique inverse.)

Implicit in saying that $\cdot$ is a binary operation $G \times G \to G$ is that given any $a, b \in G$, $a \cdot b$ must also be in $G$. We refer to this property by saying that $G$ is closed under $\cdot$.

Definition 7.2. A group $G$ is abelian (or commutative) if $a \cdot b = b \cdot a$ for all $a, b \in G$.

Definition 7.3. If $G$ is a group with a finite number of elements, then the number of elements in $G$ is called the order of $G$ and is denoted by $|G|$.

7.1 Examples

Example 7.4.

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are all abelian groups with $e = 0$.

(b) Any ring is an abelian group under addition. All the previous examples fall into this category, as do $\mathbb{Z}_n$ and the ring of polynomials.

(c) $(\mathbb{Q} \setminus \{0\}, \cdot)$, the set of all non-zero rational numbers under multiplication forms an abelian group with $e = 1$.

(d) For any field $k$, $(k \setminus \{0\}, \cdot)$ is an abelian group. (Think $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, Z_p\}$ for $p$ prime.)

(e) $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group because elements in $\mathbb{Z} \setminus \{0\}$ do not have multiplicative inverses.
(f) \( \{1, -1\}, \cdot \) is an abelian group. Here \( 1 \cdot 1 = 1 \), \( 1 \cdot (-1) = -1 \) and \( (-1) \cdot (-1) = 1 \).

(g) 
\[ \mathbb{Z}_n^* = \{ [a] \in \mathbb{Z}_n \mid [a] \text{ is a unit (i.e., invertible)} \} = \{ [a] \in \mathbb{Z}_n \mid \gcd(a, n) = 1 \} \]

is an abelian group under multiplication.

(h) If \( R \) is a ring then \( R^* = \{ a \in R \mid a \text{ is a unit} \} \) is a group under multiplication. It is an abelian group if \( R \) is a commutative ring. The last two examples fall into this case.

**Example 7.5.** Let \( X \) be a set and let \( \text{Aut}(X) = \{ f : X \to X \mid f \text{ is a bijection} \} \). Then \( \text{Aut}(X) \) along with composition is a group.

**Proof.** First \( (f, g) \mapsto f \circ g \) is a binary operation \( \text{Aut}(X) \times \text{Aut}(X) \to \text{Aut}(X) \) since the composition of two bijections is again a bijection.

Next \( (f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x) \) for all \( x \in X \). Therefore \( f \circ (g \circ h) = (f \circ g) \circ h \). So, composition is associative.

The identity map \( \text{id}_X \) on \( X \) is a bijection. So, \( \text{id}_X \in \text{Aut}(X) \). It has the property that \( \text{id}_X \circ f = f = f \circ \text{id}_X \) for all \( f \in \text{Aut}(X) \). Therefore \( G \) contains an identity. (We still have not proven that the identity of a group is unique.)

Finally, given any bijection \( f : X \to X \). We know that there exists an inverse function \( f^{-1} : X \to X \) with the property that \( f \circ f^{-1} = \text{id}_X = f^{-1} \circ f \). Thus, \( \text{Aut}(X) \) contains inverses. Therefore, \( \text{Aut}(X) \) is a group. \( \Box \)

It is not true that \( f \circ g = g \circ f \) for arbitrary \( f, g \in \text{Aut}(X) \), though it may happen in some cases. Therefore, \( \text{Aut}(X) \) is not abelian. (Caution: \( \text{Aut}(X) \) is abelian if \( |X| = 1 \) or \( |X| = 2 \).)

**Definition 7.6.** Let \( X = \{1, \ldots, n\} \). A permutation is a bijection \( \sigma : X \to X \). The set of all permutations of \( X \) along with composition is called the **symmetric group** and denoted by \( \mathfrak{S}_n \) (this symbol is a gothic \( S \)). Observe that \( \mathfrak{S}_n = \text{Aut}(\{1, \ldots, n\}) \).

**Example 7.7.** Let \( \text{GL}(2, \mathbb{k}) \) be the set of \( 2 \times 2 \) non-singular (i.e., invertible) matrices with entries in a field \( \mathbb{k} \). \( \text{GL}(2, \mathbb{k}) \) along with matrix multiplication is a (non-abelian) group.
Proof. The product of two non-singular matrices is also non-singular. For example, if \( A, B \in \text{GL}(2, k) \) then \( \det A \neq 0 \) and \( \det B \neq 0 \). So \( \det(AB) = \det(A)\det(B) \neq 0 \). Thus \( \text{GL}(2, k) \) is closed under matrix multiplication. Matrix multiplication is associative. The \( 2 \times 2 \) identity matrix \( I \) has the property that \( MI = M = IM \) for any \( M \in \text{GL}(2, k) \). The inverse of matrix

\[
M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}
\]

is

\[
M^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.
\]

It has the property that \( MM^{-1} = I = M^{-1}M \).

In fact \( \text{GL}(n, k) \), the set of all non-singular \( n \times n \) matrices, is a group under matrix multiplication.

The following are elementary properties of groups.

**Theorem 7.8.** Let \((G, \cdot)\) be a group.

(i) The identity of \( G \) is unique.

(ii) Every element \( a \in G \) has a unique inverse \( a^{-1} \in G \).

(iii) If \( a \in G \) then \((a^{-1})^{-1} = a\).

(iv) If \( e \) is the identity of \( G \) then \( e^{-1} = e \).

(v) If \( a, b \in G \) then \((a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \).

(vi) If \( a, b, c \in G \) with \( ab = ac \) (or \( ba = ca \)) then \( b = c \).

(Caution: if \( ab = ca \), it does not follow that \( b = c \).)

Proof.

(i) If \( e, f \in G \) both have the property that \( a \cdot e = a = e \cdot a \) and \( a \cdot f = a = f \cdot a \) for all \( a \in G \), then \( e = e \cdot f = f \). Therefore, the identity element of \( G \) is unique.

(ii) Fix \( a \in G \). If \( b, c \in G \) both have the property that \( a \cdot b = e = b \cdot a \) and \( a \cdot c = e = c \cdot a \) then \( b = e \cdot b = c \cdot a \cdot b = c \cdot e = c \). Therefore, \( a \) has a unique inverse. (We may now refer to \( b \) as the inverse of \( a \) and denote it by \( a^{-1} \).)

(iii) Since \( a \cdot a^{-1} = e = a^{-1} \cdot a \), we see that \( a \) is the inverse of \( a^{-1} \). Thus, \((a^{-1})^{-1} = a\).
(iv) As \( e \cdot e = e \), we have \( e^{-1} = e \).

(v) As \( a \cdot b \cdot b^{-1} \cdot a^{-1} = a \cdot e \cdot a^{-1} = e \) and \( b\cdot a \cdot a^{-1} \cdot b^{-1} = b \cdot e \cdot b^{-1} = b \cdot b^{-1} = e \), we see that \( a \cdot b \) and \( b^{-1} \cdot a^{-1} \) are inverses.

(vi) If \( ab = ac \) then by multiplying on the left by \( a^{-1} \) we get \( a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c \) and hence \( b = c \).

\[ \]

7.2 Cyclic Groups

Let \( G \) be a group written multiplicatively. For \( a \in G \) we write \( a^n \) for the \( n \)-fold product \( a \cdot a \cdot \ldots \cdot a \). Thus \( a^0 = e \), \( a^1 = a \), \( a^2 = a \cdot a \) and so on. We define \( a^{-n} = (a^{-1})^n \).

**Lemma 7.9.** Let \((G, \cdot)\) be a group and let \( a \in G \).

(i) \( (a^n)^{-1} = a^{-n} \) for all \( n \in \mathbb{Z} \),

(ii) \( a^n \cdot a^m = a^{n+m} \) for all \( n, m \in \mathbb{Z} \),

(iii) \( (a^n)^m = a^{nm} \) for all \( n, m \in \mathbb{Z} \), and

(iv) If \( ab = ba \) then \( ba^n = a^n b \) and \( (ab)^n = a^n b^n \).

**Definition 7.10.** Let \( G \) be a group and pick an element \( a \in G \). The **order** of \( a \) is the least positive integer \( n \) with \( a^n = e \). We write \( |a| = n \). If \( a^n \neq e \) for all \( n \geq 1 \), we say that \( a \) has **infinite order**.

**Example 7.11.** Consider \( [3] \in \mathbb{Z}_{11}^* = \mathbb{Z}_{11} \setminus \{0\} \). The powers of \( [3] \) are

\[
\begin{align*}
[3]^1 &= [3], \\
[3]^2 &= [9], \\
[3]^3 &= [27] = [5], \\
[3]^4 &= [3][5] = [15] = [4], \\
\end{align*}
\]

Therefore \( [3] \) has order 5.

**Proposition 7.12.** If \( G \) is a finite group and \( a \in G \), then there is some integer \( n \geq 1 \) with \( a^n = e \). Therefore every element in a finite group has a finite order.
Proof. Consider the map \( \mathbb{Z} \to G \) given by \( n \mapsto a^n \). This map is not injective as \( G \) is finite. Therefore there are two distinct integers \( k, \ell \) with \( a^k = a^\ell \).

Assume, without loss of generality, that \( k > \ell \). Multiplying \( a^k = a^\ell \) by \( a^{-\ell} \) gives \( a^{k-\ell} = a^0 = e \). Thus \( n = k - \ell \geq 1 \) has the property that \( a^n = e \).

We will improve the previous theorem by showing that \( |a| \) divides \( |G| \) (and hence \( a^{|G|} = e \)) for any finite group \( G \) (Lagrange’s Theorem).

**Proposition 7.13.** Let \( a, b \) be elements of a group \( G \). The equation \( a \cdot x = b \) has a unique solution given by \( x = a^{-1}b \). (Similarly, the equation \( x \cdot a = b \) has unique solution \( x = b \cdot a^{-1} \).)

**Proof.** Certainly \( x = a^{-1}b \) satisfies \( ax = aa^{-1}b = eb = b \). If \( a \cdot y = b \) then, multiplying by \( a^{-1} \) on the left gives \( a^{-1}ay = a^{-1}b \) and hence \( y = a^{-1}b = x \). Therefore, \( a^{-1}b \) is the unique solution. \( \Box \)

The multiplication table of a group is called its **Cayley table**.

**Corollary 7.14.** Every row (and every column) in the Cayley table for a group \( G \) contains every element of \( G \).

**Proof.** The rows of the Cayley table of \( G \) are indexed by elements in \( G \). Fix a row indexed by \( a \in G \). Then any element \( b \in G \) appears exactly once in the row of \( a \) since \( a \cdot x = b \) has a unique solution; \( x \) determines the column in which \( b \) appears. \( \Box \)

**Example 7.15.** Consider the multiplicative group \( \mathbb{Z}^*_n = \{[1], [3], [7], [9]\} \). The Cayley table of \( \mathbb{Z}^*_n \) is

\[
\begin{array}{c|cccc}
\end{array}
\]

**Definition 7.16.** Let \( C_n = \{e = a^0, a, a^2, \ldots, a^{n-1}\} \) be an \( n \)-element set and define \( a^i \cdot a^j = a^k \) where \( 0 \leq k < n \) is the remainder of \( i + j \) after division by \( n \). The set \( C_n \) along with this operation is called the **cyclic group** of order \( n \). The element \( a \) is called the **generator** of \( C_n \) and has order \( n \).

Note that \( C_n \) is nothing more than \( \mathbb{Z}_n \) written multiplicatively. Each \([i] \in \mathbb{Z}_n \) with \( 0 \leq i < n \), corresponds to \( a^i \in C_n \).
Section 8: Lagrange’s Theorem

8.1 Subgroups

Definition 8.1. A non-empty subset \( H \subseteq G \) of a group \((G, \cdot)\) is called a subgroup of \( G \) if \( H \) is a group using the multiplication as defined on \( G \). We write \( H \leq G \) when \( H \) is a subgroup of \( G \).

Given any subset \( H \subseteq G \) of a group \((G, \cdot)\) we can define a product \( \cdot_H \) on \( H \) by \( a \cdot_H b = a \cdot b \) where \( a, b \in H \) (the second product taken as the multiplication in \( G \)). This gives a map \( H \times H \to G \), since the product may not lie in \( H \). So, in order to check that \( H \) is subgroup of \( G \), we need to check that \( a \cdot b \in H \) for every \( a, b \in H \), so that \( \cdot_H \) is map \( H \times H \to H \).

As multiplication in \( G \) is associative, the inherited multiplication \( \cdot_H \) on \( H \) must also be associative.

Lemma 8.2. A non-empty subset \( H \subseteq G \) is a subgroup of \( G \) if and only if

(i) the identity \( e \in G \) is also in \( H \),
(ii) for all \( a, b \in H \), \( a \cdot b \in H \), and
(iii) for all \( a \in H \), \( a^{-1} \in H \).

(The multiplication in (ii) and the inverse in (iii) are taken in \( G \).)

The above lemma can be simplified via the following equivalent result.

Lemma 8.3. A non-empty subset \( H \subseteq G \) is a subgroup of \( G \) if and only if \( ab^{-1} \in H \) for all \( a, b \in H \).

Proof. If \( H \) is a subgroup of \( G \), then clearly \( ab^{-1} \in H \) for all \( a, b \in H \) by (ii) and (iii) of Lemma 8.2.

We next show the reverse direction by proving that all three conditions of Lemma 8.2 hold. For any \( a \in H \), take \( b = a \) and apply the condition \( ab^{-1} \in H \) to obtain that \( aa^{-1} = e \in H \); thus condition (i) of Lemma 8.2 holds. Now for \( b \in Ha \), apply the condition \( ab^{-1} \in H \) with \( a = e \) (as we now know that \( e \in H \)) to get that \( eb^{-1} = b^{-1} \in H \); thus condition (iii) of Lemma 8.2 holds. Finally, for \( c, d \in H \), we also know that \( d^{-1} \in H \) (just proven); so apply the condition \( ab^{-1} \in H \) with \( a = c \) and \( b = d^{-1} \) to yield that \( c(d^{-1})^{-1} = cd \in H \), thus proving condition (ii) of Lemma 8.2 and completing the proof. \( \square \)
Example 8.4. If $G$ is a group with identity $e$ then both $\{e\}$ and $G$ are subgroups of $G$. We call $\{e\}$ the **trivial subgroup** of $G$. A **proper subgroup** of $G$ is any subgroup $H \leq G$ with $H \neq G$. When $H$ is a proper subgroup of $G$, we write $H < G$.

Example 8.5. Recall the Cayley table of $\mathbb{Z}_10^\ast = \{[1], [3], [7], [9]\}$, given below. The set $H = \{[1], [9]\}$ is a subgroup of $\mathbb{Z}_10^\ast$.

<table>
<thead>
<tr>
<th></th>
<th>[1]</th>
<th>[3]</th>
<th>[7]</th>
<th>[9]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[3]</td>
<td>[7]</td>
<td>[9]</td>
</tr>
<tr>
<td>[3]</td>
<td>[3]</td>
<td>[9]</td>
<td>[1]</td>
<td>[7]</td>
</tr>
<tr>
<td>[7]</td>
<td>[7]</td>
<td>[1]</td>
<td>[9]</td>
<td>[3]</td>
</tr>
<tr>
<td>[9]</td>
<td>[9]</td>
<td>[7]</td>
<td>[3]</td>
<td>[1]</td>
</tr>
</tbody>
</table>

Observe that $H$ contains the identity $e = [1]$, products of elements in $H$ are in $H$ and the inverse of each element in $H$ is also in $H$. From the Cayley table for $H$, we can see that there is no real difference between $H$ and $C_2$.

Example 8.6. Let $G = \text{GL}(n, k)$ be the group of invertible $n \times n$ matrices. The set

$$H = \{ M \in \text{GL}(n, k) \mid M \text{ is diagonal} \}$$

$$= \left\{ \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix} : a_{11} \neq 0, \ldots, a_{nn} \neq 0 \right\}$$

is a subgroup of $G$. The group $H$ is essentially $k^\ast \times \cdots \times k^\ast$. (We will discuss “equivalent” groups in detail later.)

Example 8.7. Let $n\mathbb{Z} = \{ nk \mid k \in \mathbb{Z} \}$. The set $n\mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$ (i.e., a subgroup of $(\mathbb{Z}, +)$).

**Proof.** We need to check (by Lemma 8.2) that $n\mathbb{Z}$ contains the identity of $\mathbb{Z}$, is closed under addition and taking inverses.

As $0 \in n\mathbb{Z}$, it contains the identity of $\mathbb{Z}$. If $m \in n\mathbb{Z}$ and $\ell \in n\mathbb{Z}$ then $m = na$ and $\ell = nb$ for some $a, b \in \mathbb{Z}$. Therefore, $m + n = na + nb = n(a + b) \in n\mathbb{Z}$. Therefore $n\mathbb{Z}$ is closed under addition.

Finally, if $m \in n\mathbb{Z}$ then $m = nk$ for some $k \in \mathbb{Z}$. Therefore $-m = n(-k)$ and hence $-m \in n\mathbb{Z}$. Thus, the inverse of an element in $n\mathbb{Z}$ is also in $n\mathbb{Z}$. \qed
Example 8.8. Let \( G \) be a multiplicative group and let \( a \in G \). The set \( \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \) is a subgroup of \( G \) and is called the **cyclic subgroup** of \( G \) generated by \( a \).

**Proof.** By definition, \( a^0 = e \in \langle a \rangle \). Thus, \( \langle a \rangle \) contains the identity of \( G \). The set \( \langle a \rangle \) is clearly closed under multiplication (\( a^i \cdot a^j = a^{i+j} \in \langle a \rangle \)) and inverses (\( a^i \cdot a^{-i} = a^0 = e \)). Thus the proof is complete by Lemma 8.2 (an alternative proof consists of using Lemma 8.3 and is left as an exercise).

If a cyclic subgroup as defined in this example is finite, then \( \langle a \rangle = C_n \) where \( n = |a| \). If \( \langle a \rangle \) is not finite, then \( \langle a \rangle \) is essentially \( \mathbb{Z} \) (after replacing multiplication notation with addition).

**Lemma 8.9.** If \( H \) is a subset of a finite group \( G \) and \( H \) is non-empty and closed under multiplication, then \( H \) is a subgroup of \( G \).

**Proof.** Using Lemma 8.2, we need to show that \( H \) contains the identity and the inverse of each of its elements. Take \( a \in H \). As \( a \) has a finite order in \( G \), we know that \( a^n = e \) for some \( n \in \mathbb{Z} \). As \( H \) is closed under multiplication, \( e = a^n \in H \). Furthermore, the inverse of \( a \) is \( a^{n-1} \) and hence \( a^{-1} = a^{n-1} \in H \).

### 8.2 Cosets and Lagrange’s Theorem

**Definition 8.10.** Let \( H \leq G \) be a subgroup of \( G \). We define a relation \( \sim_H \) on \( G \) by the following: if \( a, b \in G \) then \( a \sim_H b \) if \( ab^{-1} \in H \).

**Lemma 8.11.** The relation \( \sim_H \) is an equivalence relation.

**Proof.** If we take \( a \in G \), then \( aa^{-1} = e \in H \). Therefore \( a \sim_H a \) for all \( a \in G \) (i.e., \( \sim_H \) is reflexive). Next if \( a, b \in G \) have \( a \sim_H b \), then \( ab^{-1} \in H \). The inverse of \( ab^{-1} \) is also in \( H \), so \( (ab^{-1})^{-1} = ba^{-1} \in H \). Thus \( a \sim_H b \) implies \( b \sim_H a \). Finally, if \( a \sim_H b \) and \( b \sim_H c \) then \( ab^{-1} \in H \) and \( bc^{-1} \in H \), so \( ab^{-1}bc^{-1} = ac^{-1} \in H \). Thus \( a \sim_H b \) and \( b \sim_H c \) imply \( a \sim_H c \).

**Example 8.12.** Consider the group \( \mathbb{Z} \) and the subgroup \( n\mathbb{Z} \). The relation \( \sim_{n\mathbb{Z}} \) gives \( a \sim_{n\mathbb{Z}} b \) if \( a - b \in n\mathbb{Z} \). That is, \( a \sim_{n\mathbb{Z}} b \) is simply congruence modulo \( n \).

**Definition 8.13.** Let \( H \leq G \) for a group \( G \) and let \( \sim_H \) be the relation defined above. The equivalence class of \( a \in G \) is called a **right coset** of \( H \) and is denoted \( Ha \).
Let us examine an equivalence class and see why this notation makes sense.

\[
[a] = \{b \in G \mid b \sim_H a\}
= \{b \in G \mid ba^{-1} \in H\}
= \{b \in G \mid \exists h \in H, ba^{-1} = h\}
= \{b \in G \mid \exists h \in H, b = ha\}
= \{ha \mid h \in H\}
= Ha
\]

**Remark 8.14.** A left coset of \(H\) is a set \(aH = \{ah \mid h \in H\} = \{b \in G \mid b^{-1}a \in H\}\) for some \(a \in G\). Thus, left cosets are equivalence classes under a similar (but different) equivalence relation on \(G\) given by \(a \sim b\) iff \(a^{-1}b \in H\).

**Lemma 8.15.** Let \(G\) be a group and \(H\) be a subgroup of \(G\). For \(a, b \in G\), either \(aH = bH\) or \(aH \cap bH = \emptyset\) (and similarly for right cosets). Furthermore, \(aH = bH\) if and only if \(a^{-1}b \in H\) and \(Ha = Hb\) if and only if \(ab^{-1} \in H\).

**Proof.** Right cosets are equivalence classes under the relation \(a \sim_H b\) if \(ab^{-1} \in H\). Thus, by Proposition 3.12, two cosets are either disjoint, or their representatives are related and hence the cosets are equal. The same holds for left cosets. \(\square\)

**Lemma 8.16.** Let \(G\) be a group and \(H\) be a subgroup of \(G\). For any \(a \in G\), \(|H| = |aH| = |Ha|\).

**Proof.** Consider the function \(\phi : H \to aH\) given by \(h \mapsto ah\). If \(\phi(h) = \phi(k)\) for some \(h, k \in H\) then \(ah = ak\) and hence \(h = k\) (cf. Theorem 7.8). Thus, \(\phi\) is injective. If we take an arbitrary element \(c \in aH\) then \(c = ah\) for some \(h \in H\) and hence \(c = \phi(h)\). Thus, \(\phi\) is surjective.

As \(\phi\) is a bijection between \(H\) and \(aH\), we have \(|H| = |aH|\). Similarly, the map \(h \mapsto ha\) is a bijection between \(|H|\) and \(|Ha|\) completing the proof. \(\square\)

**Theorem 8.17 (Lagrange’s Theorem).** Let \(G\) be a finite group and let \(H\) be a subgroup of \(G\). The order of \(H\) divides the order of \(G\) and there are \(|G|/|H|\) left cosets of \(H\) and \(|G|/|H|\) right cosets of \(H\).

**Proof.** There are a finite number of elements in \(G\), so there are a finite number of distinct left cosets \(a_1H, a_2H, \ldots, a_sH\). Here we have picked \(a_1, \ldots, a_s\) as their representatives. These cosets partition \(G\), meaning that they are pairwise
disjoint and their union is all of $G$. Therefore, $|G| = |a_1H| + |a_2H| + \cdots + |a_sH|$. As $|a_iH| = |H|$ for $1 \leq i \leq s$, we see $|G| = s|H|$ for some integer $s \geq 1$. Therefore $|H|$ divides $|G|$ and $s = |G|/|H|$ is the number of left cosets of $H$.

**Corollary 8.18.** Let $a \in G$ be an element in a finite group $G$. The order of $a$ divides the order of $G$.

**Proof.** The order of $a$ is the least integer $n \geq 1$ with $a^n = e$. Let $H = \langle a \rangle = \{e, a, \ldots, a^{n-1}\}$ be the cyclic subgroup generated by $a$. As $H$ is a subgroup of $G$, $|H|$ divides $|G|$ by Lagrange’s Theorem. As $|H| = n = |a|$, we are done.

**Corollary 8.19.** If $G$ is a finite group with $|G| = m$ then for any $a \in G$, $a^m = e$.

**Proof.** If we let $n = |a|$, then $a^n = e$. As $n$ divides $m$, there is some integer $k$ with $kn = m$. Thus $a^m = a^{kn} = (a^n)^k = e^k = e$.

**Corollary 8.20.** A group $G$ of prime order is cyclic.

**Proof.** Take $a \in G$ with $a \neq e$. The cyclic group generated by $a$ has $|a| > 1$ elements, but $|a|$ must divides $|G|$ which is prime. Therefore $|a| = |G|$ and hence $\langle a \rangle = G$.

**Theorem 8.21 (Euler’s Theorem).** If $\gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n) = |\{b \in \mathbb{Z} \mid 1 \leq b \leq n \text{ and } \gcd(b, n) = 1\}|$.

**Proof.** Let $\mathbb{Z}_n^*$ be the group of units in $\mathbb{Z}_n$. An element $[a] \in \mathbb{Z}_n$ is a unit if it is represented by an integer $a$ with $\gcd(a, n) = 1$. Thus, $\phi(n) = |\mathbb{Z}_n^*|$. Therefore, if $[a] \in \mathbb{Z}_n^*$, we have $[a]^{\phi(n)} = [1]$ by Corollary 8.19. In terms of congruence, this says $a^{\phi(n)} \equiv 1 \pmod{n}$.

**Theorem 8.22 (Fermat’s Little Theorem).** If $p$ is prime and $[a] \in \mathbb{Z}_p$ then

$$[a]^p = [a].$$

**Proof.** As $[0]^p = [0]$, the result is clear for $[a] = [0]$. Now suppose that $[a] \neq [0]$, and therefore $[a] \in \mathbb{Z}_p^*$. As $|\mathbb{Z}_p^*| = p - 1$, Euler’s theorem says $[a]^{p-1} = [1]$. Multiplying by $[a]$ gives $[a]^p = [a]$.
Section 9: Group Quotients

9.1 Normal Subgroups

Definition 9.1. Let $G$ be a group and let $H \leq G$ (i.e., $H$ is a subgroup of $G$) and $g \in G$. The conjugation of $H$ by $g$ is the set

$$gHg^{-1} = \{ ghg^{-1} \mid h \in H \}$$

Lemma 9.2. If $H \leq G$ and $g \in G$ then $gHg^{-1}$ is a subgroup of $G$.

Proof. By Lemma 8.3, we show that if $a,b \in gHg^{-1}$, then $ab^{-1} \in gHg^{-1}$ to conclude that $gHg^{-1}$ is a subgroup of $G$.

Since $a,b \in gHg^{-1}$, we can write $a = gh_1g^{-1}$ and $b = gh_2g^{-1}$ for some $h_1,h_2 \in H$. Then

$$ab^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1}.$$ 

Since both $h_1$ and $h_2$ belong to $H$, then $h_1h_2^{-1} \in H$ (as $H$ is a subgroup). Hence $ab^{-1} \in gHg^{-1}$; this completes the proof. 

Definition 9.3. A subgroup $H \leq G$ is normal if $gHg^{-1} = H$ for all $g \in G$. We write $H \trianglelefteq G$ when $H$ is a normal subgroup of $G$.

Lemma 9.4. Every subgroup of an abelian group is normal.

Proof. If $H \leq G$ and $G$ is abelian, then for every $g \in G$ and $ghg^{-1} \in gHg^{-1}$, we have $ghg^{-1} = gg^{-1}h = h \in H$. Therefore $gHg^{-1} \subseteq H$. Similarly, if $h \in H$ then $h = gg^{-1}h = ghg^{-1} \in gHg^{-1}$. Thus $gHg^{-1} = H$. As this holds for all $g \in G$, we conclude that $H$ is normal. 

Example 9.5.

Consider (under matrix multiplication) the subgroup $H \leq \text{GL}(2, \mathbb{R})$ given by

$$H = \left\{ \begin{bmatrix} 2^n & 0 \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}.$$ 

Let $g = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Note that $g^{-1} = g$. Thus,

$$gHg^{-1} = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2^n & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mid n \in \mathbb{Z} \right\}.$$
Thus $H$ is not a normal subgroup $\text{GL}(2, \mathbb{R})$, as we have an example of an element $g \in G$ with $gHg^{-1} \neq H$. If, instead, we let $k = 3I_{2\times2}$ (where $I_{2\times2}$ is the $2 \times 2$ identity matrix), then you can check that $kHk^{-1} = H$.

This does not, however, make $H$ normal.

**Lemma 9.6.** Let $H \leq G$ be a subgroup of $G$. The following are equivalent:

(i) $H$ is a normal subgroup of $G$.

(ii) For all $a \in G$ and $h \in H$, there is some $k \in H$ with $ah = ka$.

(iii) For all $a \in G$ and $k \in H$, there is some $h \in H$ with $ah = ka$.

(iv) $aH = Ha$ for all $a \in G$.

**Proof.** First assume that $H$ is a normal subgroup of $G$. Take any $a \in G$ and any $h \in H$. As $H$ is normal, $H = aHa^{-1}$ for all $a \in G$. Since $aha^{-1} \in aHa^{-1}$, we also know $aha^{-1} \in H$. Thus, there exists some element $k \in H$ with $aha^{-1} = k$.

Multiplying on the right by $a$ gives $ah = ka$. Thus (i) implies (ii).

Now assume (ii) holds. If $aha^{-1} \in aHa^{-1}$ then $aha^{-1} = kaa^{-1} = k$ for some $k \in H$. Thus $aHa^{-1} \subseteq H$. Also, if $h \in H$ then $h = aa^{-1}k = aka^{-1}$ for some $k \in H$ using (ii) applied to $h$ and $a^{-1}$. Thus $H \subseteq aHa^{-1}$, giving equality. Thus (ii) implies (i).

The remaining equivalences follow similarly and are left as an exercise. □

### 9.2 Group Quotients

**Proposition 9.7.** Let $H \trianglelefteq G$ be a normal subgroup of a group $G$. The set $G/H = \{aH \mid a \in G\}$ along with the binary operation on $G/H$ defined by $(aH) \cdot (bH) = abH$ makes $G/H$ a group; it is called the **quotient (or factor)** group of $G$ by $H$.

**Proof.** First, we check that this multiplication operation is well-defined. Let $a_1, a_2$ be two representatives for the same coset $a_1H = a_2H$ and similarly let $b_1, b_2$ be two representatives for another coset $b_1H = b_2H$. We will show that $(a_1H)(b_1H) = a_1b_1H = a_2b_2H = (a_2H)(b_2H)$, and therefore multiplication of cosets does not depend on the choice of representative.
By Lemma 8.15 (see also Remark 8.14), as \( b_1H = b_2H \), we have \( b_1^{-1}b_2 \in H \) and since \( a_1H = a_2H \), we know \( a_1^{-1}a_2 \in H \). To conclude that \( a_1b_1 \sim a_2b_2 \) or, in other words, we need to check that \((a_1b_1)^{-1}(a_2b_2) \in H:\)

\[
(a_1b_1)^{-1}a_2b_2 = b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}hb_2, \quad \text{letting } h = a_1^{-1}a_2 \in H,
\]

\[
= kb_1^{-1}b_2, \quad \text{for some } k \in H \text{ as } H \text{ is normal (Lemma 9.6)},
\]

as \( k \in H \) and \( b_1^{-1}b_2 \in H \). Thus, multiplication of cosets of a normal subgroup is a well-defined operation. Also, \( G/H \) is closed under this operation.

Multiplication of cosets is associative since \((aH)((bH)(cH)) = (aH)(bcH) = abcH = (abH)(cH) = ((aH)(bH))(cH)\). Next \((eH)(aH) = (ea)H = aH = (ae)H = (aH)(eH)\) for all \( a \in G \). So, \( eH \) is the identity of \( G/H \). Finally the inverse of \( aH \) is \( a^{-1}H \) as one can easily check. Thus \( G/H \) is a group.

\[\square\]

**Remark 9.8.** Every subgroup of an abelian group is normal. Therefore, \( G/H \) is a group for every subgroup \( H \) of an abelian group \( G \).

**Remark 9.9.** Another (similar) quotient group given by \( G/H = \{Ha \mid a \in G\} \) can be formed under the binary operation \((Ha) \cdot (Hb) = H(ab)\).

**Example 9.10.** Let \( G = \mathbb{Z} \) and \( H = n\mathbb{Z} \) for some \( n \geq 2 \). Since \( G = \mathbb{Z} \) is an additive group, the cosets of \( H \) are \( G/H = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} \). As \( G = \mathbb{Z} \) is abelian, \( H \) is a normal subgroup (you only need to check that it is a subgroup). The sum of two cosets is given by taking the sum of their representatives: \((a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}\). We see that \( G/H = \mathbb{Z}/n\mathbb{Z} \) is precisely \( \mathbb{Z}_n \).

**Example 9.11.** Let \( G = \mathbb{Z}_6 \) and \( H = \{[0], [3]\} \). By Lagrange’s theorem \(|G/H| = |G|/|H| = 6/2 = 3\). So, we expect three cosets of \( H \). They are, \([0] + H, [1] + H \) and \([2] + H\). The multiplication table for \( G/H = \mathbb{Z}_6/\{[0], [3]\} \) is precisely that of \( \mathbb{Z}_3 \).

### 9.3 Permutations

We will form some interesting examples from permutations. Recall the definition of the symmetric group:
Definition 9.12. A permutation of the set $[n] = \{1, \ldots, n\}$ is a bijection $\sigma : [n] \to [n]$. The symmetric group $\mathfrak{S}_n$ is the set of all permutations with composition as the operation.

We can write specific permutation $\sigma : [n] \to [n]$ in two-line notation:

$$
\begin{pmatrix}
1 & 2 & 3 & \cdots & n \\
\sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n)
\end{pmatrix}
$$

For example the permutation $\sigma \in \mathfrak{S}_6$ with $\sigma(1) = 4$, $\sigma(2) = 6$, $\sigma(3) = 5$, $\sigma(4) = 2$, $\sigma(5) = 3$, $\sigma(6) = 1$ can be written as

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

Furthermore, this permutation can be expressed in terms of its cycles:

$$
\sigma = (1\,4\,2\,6)(3\,5).
$$

The cycle $(1\,4\,2\,6)$ should be read as $\sigma(1) = 4$, $\sigma(4) = 2$, $\sigma(2) = 6$, and $\sigma(6) = 1$ (it wraps). Similarly, the cycle $(3\,5)$ reads as $\sigma(3) = 5$ and $\sigma(5) = 3$.

The product of two permutations is their composition, and should therefore be read right to left. For example,

$$
\sigma = \begin{pmatrix}
1 & 2 & 3 & 4 \\
4 & 1 & 3 & 2
\end{pmatrix},
\quad
\tau = \begin{pmatrix}
1 & 2 & 3 & 4 \\
3 & 1 & 2 & 4
\end{pmatrix}, \text{ and }
\quad
\sigma\tau = \begin{pmatrix}
1 & 2 & 3 & 4 \\
3 & 4 & 1 & 2
\end{pmatrix}.
$$

For example $\tau(1) = 3$ and $\sigma(3) = 3$, so $\sigma\tau(1) = \sigma(3) = 3$. Also, $\tau(2) = 1$ and $\sigma(1) = 4$, so $\sigma\tau(2) = \sigma(1) = 4$.

In cycle notation, this same example reads $\sigma = (1\,4\,2)$ where integer 3 is not listed as it is “fixed” by $\sigma$ (i.e., $\sigma(3) = 3$), $\tau = (1\,3\,2)$ and $\sigma\tau = (1\,3)(2\,4)$.

We can easily write $\mathfrak{S}_3$ in cycle notation:

$$
\mathfrak{S}_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.
$$
Consider the subgroup $K = \{e, (1 2)\}$ of $\mathfrak{S}_3$. This is the cyclic subgroup generated by $(1 2)$ since $(1 2)^2 = e$. The left cosets of $K$ are

$$eK = (1 2)K = \{e, (1 2)\}$$

$$\begin{align*}
(2 3)K &= (1 3 2) = \{(2 3), (1 3 2)\} \\
(1 3)K &= (1 2 3) = \{(1 3), (1 2 3)\}
\end{align*}$$

and they are different from the right cosets,

$$\begin{align*}
Ke &= K(1 2) = \{e, (1 2)\} \\
K(2 3) &= K(1 2 3) = \{(2 3), (1 2 3)\} \\
K(1 3) &= K(1 3 2) = \{(1 3), (1 3 2)\}.
\end{align*}$$

A subgroup $H \leq G$ is normal if $aHa^{-1} = H$ for all $a \in G$. This subgroup $K \leq \mathfrak{S}_3$ is not normal since

$$\begin{align*}
(1 3)K(1 3) &= \{(1 3)e(1 3), (1 3)(1 2)(1 3)\} = \{e, (2 3)\}.
\end{align*}$$

Let $H = \{e, (1 2 3), (1 3 2)\} \leq \mathfrak{S}_3$. This subgroup is the cyclic subgroup generated by $(1 2 3)$ since $(1 2 3)^2 = (1 2 3)(1 2 3) = (1 3 2)$ and $(1 2 3)^3 = (1 3 2)(1 2 3) = (1)(2)(3) = e$. So $|1 2 3| = |H| = 3$.

There are only two left cosets of $H$ and they are the same as the right cosets:

$$\begin{align*}
\{e, (1 2 3), (1 3 2)\} &= He = H(1 2 3) = H(1 3 2) = eH = (1 2 3)H = (1 3 2)H \\
\{(1 2), (2 3), (1 3)\} &= H(1 2) = H(2 3) = H(1 3) = (1 2)H = (2 3)H = (1 3)H
\end{align*}$$

You can check that $H$ is a normal subgroup.
Section 10: Group Homomorphisms

10.1 Group Homomorphisms

In this section we will be discussing maps between groups. For this purpose, we will use $G$ and $H$ to denote separate groups. So, unlike in the previous section, $H$ will not refer to a subgroup of $G$.

Definition 10.1. Let $G$ and $H$ be two groups. A function $\phi : G \to H$ is called a homomorphism if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Example 10.2.

(i) Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$. The function $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ is a group homomorphism since $\ln(ab) = \ln(a) + \ln(b)$. The function $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ is also a group homomorphism since $\exp(a + b) = \exp(a)\exp(b)$.

(ii) The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ (both additive groups) given by $\phi(a) = [a]$ is a group homomorphism since $\phi(a + b) = [a + b] = [a] + [b] = \phi(a) + \phi(b)$.

(iii) The map $\det : \text{GL}(n, \mathbb{R}) \to \mathbb{R}$ is a group homomorphism since $\det(MN) = \det(M)\det(N)$.

(iv) Take any group $G$ and an element $a \in G$. The map $f : \mathbb{Z} \to G$ given by $f(n) = a^n$ is a group homomorphism since $f(n + m) = a^{n+m} = a^na^m = f(n)f(m)$.

Proposition 10.3. Suppose $\alpha : G \to H$ and $\beta : H \to K$ are group homomorphisms. Their composition $\beta \circ \alpha : G \to K$ is also a group homomorphism.

Proof. Take $a, b \in G$. Apply $\beta \circ \alpha$ to $ab$ gives $\beta \circ \alpha(ab) = \beta(\alpha(ab)) = \beta(\alpha(a)\alpha(b)) = \beta(\alpha(a))\beta(\alpha(b)) = (\beta \circ \alpha(a))(\beta \circ \alpha(b))$. Therefore $\beta \circ \alpha$ is a group homomorphism. \qed

Lemma 10.4. Suppose that $\phi : G \to H$ is a group homomorphism.

(i) If $e_G$ is the identity of $G$ then $\phi(e_G) = e_H$ is the identity of $H$.

(ii) For $a \in G$, $\phi(a^{-1}) = (\phi(a))^{-1}$.

(iii) For $a \in G$, $\phi(a^n) = (\phi(a))^n$ for any integer $n$. 

Proof. For (i), consider \( \phi(e_G) = \phi(e_G e_G) = \phi(e_G) \phi(e_G) \). Multiplying both sides by the inverse of \( \phi(e_G) \in H \) gives \( e_H = \phi(e_G) \).

Now consider the product of \( \phi(a^{-1}) \) and \( \phi(a) \):

\[
\phi(a^{-1}) \phi(a) = \phi(a^{-1} a) = \phi(e_G) = e_H.
\]

Similarly, \( \phi(a) \phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_G) = e_H \). Therefore \( \phi(a) \) and \( \phi(a^{-1}) \) are inverses, proving (ii).

Finally for part (iii), if \( a \in G \) and \( n > 0 \) then

\[
\phi(a^n) = \phi(\underbrace{a \cdots a}_{n \text{ times}}) = \underbrace{\phi(a) \phi(a) \cdots \phi(a)}_{n \text{ times}} = (\phi(a))^n.
\]

If \( n < 0 \) then let \( m = -n \geq 0 \), so

\[
\phi(a^n) = \phi(a^{-m}) = \phi((a^m)^{-1}) = ((\phi(a))^m)^{-1} = (\phi(a))^{-m} = (\phi(a))^n.
\]

The last case, where \( n = 0 \), follows from part (i).

\[\square\]

**Proposition 10.5.** Suppose that \( \phi : G \to H \) is a group homomorphism. If \( a \in G \) has finite order then \( |\phi(a)| \) divides \( |a| \).

**Proof.** Let \( n = |a| \) and \( k = |\phi(a)| \). Since \( a^n = e_G \), we have \( \phi(a)^n = \phi(a^n) = \phi(e_G) = e_H \). Since \( \phi(a)^n = e_H \) we know that \( k = |\phi(a)| \) is less than or equal to \( n \).

The division algorithm tells us that we can express \( n \) as \( n = qk + r \) for some \( 0 \leq r < k \). Observe that \( e = \phi(a)^n = \phi(a)^{qk+r} = (\phi(a)^k)^q \phi(a)^r = e_H^q \phi(a)^r = \phi(a)^r \). But, \( \phi(a)^r = e_H \) and \( r < k \). Therefore, we must have \( r = 0 \) and hence \( n = qk \). That is, the order of \( \phi(a) \) divides the order of \( a \).

\[\square\]

**Lemma 10.6.** Suppose that \( \phi : G \to H \) is a group homomorphism. The image \( \phi(K) = \{ \phi(k) \mid k \in K \} \) of a subgroup \( K \leq G \) is a subgroup of \( H \). The pre-image \( \phi^{-1}(L) = \{ g \in G \mid \phi(g) \in L \} \) of a subgroup \( L \leq H \) is a subgroup of \( G \).

**Proof.** Assume \( K \leq G \) is a subgroup of \( G \). Since \( e_G \in K \), we know that \( \phi(e_G) = e_H \in \phi(K) \). For any two elements \( x, y \in \phi(K) \) in the image of \( K \), there are \( a, b \in K \) with \( \phi(a) = x \) and \( \phi(b) = y \). Since \( K \) is closed under multiplication, \( ab \in K \) and hence \( \phi(a) \phi(b) = \phi(ab) \in \phi(K) \). For \( a \in K \), the inverse of \( a \) is also in \( K \). Therefore \( \phi(a)^{-1} = \phi(a^{-1}) \in \phi(K) \). Thus, by Lemma 8.2, \( \phi(K) \) is a subgroup of \( H \).
Assume that $L \leq H$ is a subgroup of $H$. As $\phi(e_G) = e_H \in L$, we see that $e_G \in \phi^{-1}(L)$. Furthermore, if $a, b \in \phi^{-1}(L)$ then $\phi(ab) = \phi(a)\phi(b) \in L$ as $\phi(a) \in L$ and $\phi(b) \in L$. Consequently, $ab \in \phi^{-1}(L)$. And last, if $a \in \phi^{-1}(L)$ then $\phi(a) \in L$ and hence $\phi(a^{-1}) = \phi(a)^{-1} \in L$. Thus, $a^{-1} \in \phi^{-1}(L)$. Thus, the pre-image of $L$ is a subgroup of $G$.

**Definition 10.7.** Let $\alpha : G \to H$ be a group homomorphism. The kernel of $\alpha$ is $\text{Ker } \alpha = \{a \in G \mid \alpha(a) = e_H\}$. The image of $\alpha$ is $\text{Im } \alpha = \{b \in H \mid \exists a \in G, \alpha(a) = b\}$ (i.e., the image of $\alpha$ as a function).

**Proposition 10.8.** The kernel of a group homomorphism $\alpha : G \to H$ is a normal subgroup of $G$. The image of $\alpha$ is a subgroup of $H$.

**Proof.** We start with the image. Since $\text{Im } \alpha = \alpha(G)$, we see from the previous lemma that $\text{Im } \alpha$ is a subgroup of $H$.

The kernel of $\alpha$ is the pre-image of the subgroup $K = \{e_H\} \leq H$. That is, $\text{Ker } \alpha = \alpha^{-1}(e_H) = \{a \in G \mid \alpha(a) = e_H\}$. Therefore, by the previous lemma, $\text{Ker } \alpha$ is a subgroup of $G$. We now check that it is normal. Take any $a \in G$. We want to show that $a(\text{Ker } \alpha)a^{-1} = \text{Ker } \alpha$. If $aka^{-1} \in a(\text{Ker } \alpha)a^{-1}$ then $\phi(aka^{-1}) = \phi(a)\phi(k)\phi(a)^{-1} = \phi(a)e_H\phi(a)^{-1} = e_H$. Therefore $aka^{-1} \in \text{Ker } \alpha$ and hence $a(\text{Ker } \alpha)a^{-1} \subseteq \text{Ker } \alpha$. For the opposite containment, take $k \in \text{Ker } \alpha$. Since $k = aa^{-1}kaa^{-1}$, it suffices to show that $a^{-1}ka \in \text{Ker } \alpha$ (verify it).

**Proposition 10.9.** A group homomorphism $\phi : G \to H$ is injective if and only if $\text{Ker } \phi = \{e_G\}$.

**Proof.** First assume that $\phi$ is injective. We know $\phi(e_G) = e_H$ by Lemma 10.4 and hence $e_G \in \text{Ker } \phi$. If $a \in \text{Ker } \phi$ then $\phi(a) = e_H$ and hence $a = e_G$ as $\phi$ is injective. Therefore $\text{Ker } \phi = \{e_G\}$.

Now assume that $\text{Ker } \phi = \{e_G\}$. If $a, b \in G$ have $\phi(a) = \phi(b)$ then $e_H = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1})$. Therefore $ab^{-1} \in \text{Ker } \phi$. As we have assumed $\text{Ker } \phi = \{e_G\}$, we must have $ab^{-1} = e_G$ and hence $a = b$. Thus, $\phi$ is injective.

### 10.2 Group Isomorphisms

**Definition 10.10.** A group isomorphism is a group homomorphism $\phi : G \to H$ that is also a bijection. If $\phi : G \to H$ is an isomorphism, we say that $G$ and $H$ are isomorphic and write $G \cong H$. 

Two isomorphic groups are essentially the same in that they have the same multiplication tables after a relabeling of their elements.

**Proposition 10.11.** If \( \phi : G \to H \) is a group isomorphism, then the compositional inverse \( \phi^{-1} : H \to G \) is also an isomorphism.

*Proof.* As \( \phi \) is a bijection, its compositional inverse \( \phi^{-1} \) is also a bijection. So, it suffices to check that \( \phi^{-1} \) is a group homomorphism. Let \( c,d \in H \) and let \( a = \phi^{-1}(c) \) and \( b = \phi^{-1}(d) \). As \( \phi \) is a group homomorphism, we have \( \phi(ab) = \phi(a)\phi(b) = cd \). Applying \( \phi^{-1} \) to this, we obtain \( \phi^{-1}(cd) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(c)\phi^{-1}(d) \). Therefore, \( \phi^{-1} \) is a group homomorphism and hence an isomorphism.

The next theorem is often called the **first isomorphism theorem**.

**Theorem 10.12.** Let \( \phi : G \to H \) be a group homomorphism and let \( K = \ker \phi \). The function \( \overline{\phi} : G/K \to \im \phi \) given by \( \overline{\phi}(aK) = \phi(a) \) is a well-defined group isomorphism. In particular \( G/\ker \phi \cong \im \phi \).

*Proof.* Since the kernel of any group homomorphism is a normal subgroup, we know by Proposition 9.7 that \( G/K \) is a group (and not just a collection of cosets).

Next, we need to show that \( \overline{\phi} \) is a well-defined function. Take \( a,b \in G \) which are representatives for the same coset of \( K \): \( aK = bK \). Since \( aK = bK \), we know that \( b^{-1}a \in K = \ker \phi \) and hence \( e_H = \phi(b^{-1}a) = \phi(b^{-1})\phi(a) = \phi(b)^{-1}\phi(a) \). Multiplying on the left by \( \phi(b) \) gives \( \phi(b) = \phi(a) \). Therefore \( \overline{\phi} \) is well defined.

Since \( \phi \) is a group homomorphism, we have \( \overline{\phi}((aK)(bK)) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK) \). Thus, \( \overline{\phi} \) is also a homomorphism.

The map \( \overline{\phi} \) is surjective since if \( b \in \im \phi \) then there is \( a \in G \) with \( \phi(a) = b \) and hence \( \overline{\phi}(aK) = \phi(a) = b \).

Finally, if \( aK \in \ker \overline{\phi} \), then \( e_H = \overline{\phi}(aK) = \phi(a) \). Thus, \( a \in K \) and hence \( aK = K = e_{G/K} \), the identity of \( G/K \). Therefore \( \ker \overline{\phi} = \{ e_{G/K} \} \) and hence \( \overline{\phi} \) is injective by Proposition 10.9.

We conclude that \( \overline{\phi} \) is a well-defined bijective group homomorphism; thus \( G/\ker \phi \cong \im \phi \). \( \Box \)

**Lemma 10.13.** If \( G \cong H \) are two isomorphic groups then \( G \) is abelian if and only if \( H \) is abelian.
Proof. Due to symmetry, it suffices to assume that $G$ is abelian and show that $H$ is abelian. Let $\phi : G \rightarrow H$ be an isomorphism. For $a, b \in H$, there exist $c, d \in G$ with $\phi(c) = a$ and $\phi(d) = b$. Thus, $ab = \phi(c)\phi(d) = \phi(cd) = \phi(dc) = \phi(d)\phi(c) = ba$. So, $H$ is abelian.

**Theorem 10.14.** If $\phi : G \rightarrow H$ is a group homomorphism and $H$ is abelian, then $G/\text{Ker} \phi$ is abelian.

**Proof.** From the first isomorphism theorem (Theorem 10.12), $G/\text{Ker} \phi \cong \text{Im} \phi$. Since $\text{Im} \phi \leq H$ is a subgroup of an abelian group, it is also abelian. Since $G/\text{Ker} \phi$ is isomorphic to the abelian group $\text{Im} \phi$, it is also abelian (by the previous lemma, Lemma 10.13).

**Theorem 10.15.** If $\phi : G \rightarrow H$ is a surjective group homomorphism and $G$ is abelian, then $H$ is abelian.

**Proof.** Since $G$ is a abelian, 
\[(a \text{ Ker} \phi)(b \text{ Ker} \phi) = (ab) \text{ Ker} \phi = (ba) \text{ Ker} \phi = (b \text{ Ker} \phi)(a \text{ Ker} \phi)\] and hence $G/\text{Ker} \phi$ is abelian. Since $G/\text{Ker} \phi \cong \text{Im} \phi = H$ by the first isomorphism theorem and the fact that $\phi$ is surjective, we see that $H$ must be abelian as well (by Lemma 10.13).

**Alternate Proof.** In fact, we do not need the first isomorphism theorem for this proof. As $\phi$ is surjective, given $a, b \in H$ there are $c, d \in G$ with $\phi(c) = a$ and $\phi(d) = b$. Thus, $ab = \phi(c)\phi(d) = \phi(cd) = \phi(dc) = \phi(d)\phi(c) = ba$. So, $H$ is abelian.
Section 11: Coding Theory

Digital data, such as audio, images, video and text, are often sent over electronic communication channels that are subject to distortions of various kinds: wave interference, atmospheric noise, fading, multipath propagation effects, thermal noise, etc. Storage devices are also subject to magnetic fields and static which can corrupt data.

The theory and practice of error-correcting codes are intimately connected to the field of information theory, also known as the mathematical theory of communication, which was established by Claude Elwood Shannon.

Error-correcting codes are used to establish reliable transmission of information over noisy communication channels. They provide two capabilities. First, coding messages allows you to detect whether an error has occurred during transmission, assuming that the number of errors is below a certain threshold. A common response to receiving a message containing errors is to ask for the message to be retransmitted, so often detecting errors is enough. The second feature of coded messages is that they can allow for correction and recovery of the original message if the number of errors in the transmitted message is below a tighter threshold.

Different coding schemes provide different tolerances for errors. Generally, if you require more error tolerance, you will need to send longer messages.

From now on, we will be working with binary data. Let $\mathbb{B} = \mathbb{Z}_2 = \{[0], [1]\}$ thought of as bits (i.e., binary digits). We set $0 = [0]$ and $1 = [1]$ for notational convenience. We let $\mathbb{B}^n = \mathbb{B} \times \cdots \times \mathbb{B}$ be the set of $n$-tuples with entries in $\mathbb{B} = \{0, 1\}$. Instead of writing $a = (0, 1, 1, 0, 1) \in \mathbb{B}^5$ we will write $a = 01101$. The set $\mathbb{B}^n$ is a group with unity element given by the all-zero word of length $n$, $0^n = \underbrace{0 \cdots 0}_n$, under coordinate-wise (i.e., component-wise) addition:

$$01101 + 01011 = (0, 1, 1, 0, 1) + (0, 1, 0, 1, 1)$$
\[ (0 + 0, 1 + 1, 1 + 0, 0 + 1, 1 + 1) \]
\[ = (0, 0, 1, 1, 0) \]
\[ = 00110. \]

We call this bitwise addition, and it corresponds to the logical operation xor (exclusive or).

An element \( w \in \mathbb{B}^n \) is called a \textbf{binary word} of length \( n \).

**Definition 11.1.** Given positive integers \( k \) and \( n \), a \textbf{binary coding (or encoding) function} is an injective (i.e., one-to-one) function \( f : \mathbb{B}^k \rightarrow \mathbb{B}^n \). A binary word in \( w \in \mathbb{B}^k \) is called a \textbf{message}, while any binary word \( c \in \mathbb{B}^n \) that is in the image of \( f \) is called a \textbf{codeword}. The set \( \mathcal{C} = \text{Im} f = f(\mathbb{B}^k) \) is called an \((n, k)\)-binary code.

A binary coding function needs to be injective so that different messages get sent to different codewords before those codewords are sent across the noisy channel. If two codewords represented the same message, then the message would not be able to be correctly recovered by the recipient.

**Definition 11.2.** The \textbf{rate} of an \((n, k)\)-binary code is \( R = k/n \), measured in message bits/code bit.

Since encoding functions have to be injective, \( n \geq k \). Thus the rate of any code is bounded by 1: \( R \leq 1 \). The rate gives the amount of information (i.e., message bits) sent per code bit, so larger rates (with an appropriate error tolerance) are preferable.
Example 11.3. The \((n, 1)\) repetition binary code is given by the coding function \(f : \mathbb{B} \to \mathbb{B}^n\), with \(f(w) = \underbrace{ww \cdots w}_{n \text{ times}}\). For example, if \(n = 4\) then \(f(0) = 0000\) and \(f(1) = 1111\). The rate of \(f\) is \(R = k/n = 1/n\). The codewords are \(C = \{00 \cdots 0, 11 \cdots 1\}\). Since \(f\) is injective, the number of codewords equals the size of the domain which is \(|\mathbb{B}| = 2\).

If a message bit is sent using this code, and the codeword is subject to \(n-1\) or fewer errors, then we can tell that an error has occurred since the bits will not all be equal. If \(n = 2\ell + 1\) or \(n = 2\ell + 2\) and \(\ell\) or fewer errors occur, then we can also tell what the original message was. Thus, we can detect \(n-1\) errors, and correct \(\ell = \left\lfloor \frac{n-1}{2} \right\rfloor\) errors, where \(\lfloor x \rfloor\) is the largest integer less than or equal to \(x\).

Example 11.4. Let \(n = k + 1\). The \((k + 1, k)\) parity-check code is given by \(f : \mathbb{B}^k \to \mathbb{B}^{k+1}\) with \(f(x_1 x_2 \cdots x_k) = x_1 x_2 \cdots x_k y\) where \(y = x_1 + \cdots + x_k \in \mathbb{B}\) is called the parity bit. For example, if \(k = 4\) then some of the codewords are

\[f(0000) = 00000\]
\[f(1000) = 10001\]
\[f(0110) = 01100\]
\[f(0111) = 01111.\]

The codewords of \(f\) are

\[C = \{b_1 b_2 \cdots b_k b_{k+1} \in \mathbb{B}^k \mid b_1 + \cdots + b_{k+1} \equiv 0 \pmod{2}\}\]
\[= \{ \text{binary words of length } k + 1 \text{ with an even number of ones} \}.\]

If a message is sent using the parity-check code, then we can detect a single error in the codeword. If there are two errors in the codeword, or any even number of errors, then they will go undetected. Even though we can tell if a single error is made during transmission, we cannot correct the error: any given word in \(\mathbb{B}^{k+1} \setminus C\) (i.e., any erroneous codeword) is adjacent to \(k + 1\) codewords.

Definition 11.5. The **Hamming weight** of a binary word \(w \in \mathbb{B}^n\) is the number of 1’s in its expression. We use \(\text{wt}(w)\) to denote the weight.

For example, \(\text{wt}(10101) = 3\) while \(\text{wt}(00000) = 0\).
Definition 11.6. The Hamming distance between two words \( v, w \in B^n \) is
\[
d(v, w) = wt(v - w) \\
= wt(v + w) \\
= \text{the number of places where } v \text{ and } w \text{ disagree.}
\]
For example, \( d(111, 010) = wt(111 + 010) = wt(101) = 2 \). For any word \( w \in B^n \), \( d(w, w) = wt(w + w) = wt(0^n) = 0 \). Also, \( d(w, 0^n) = wt(w + 0^n) = wt(w) \).

Lemma 11.7. For any \( u, v, w \in B^n \),
\[
(i) \ d(v, w) = d(w, v), \\
(ii) \ d(v, w) = 0 \text{ if and only if } v = w, \\
(iii) \ d(u, w) \leq d(u, v) + d(v, w), \text{ and} \\
(iv) \ d(v, w) \geq 0.
\]
Consequently, the Hamming distance is said to be a metric on \( B^n \).

11.1 Nearest Neighbour Decoding

The recipient of a coded message needs a decoding function to recover the original message. If the encoder is the map \( f : B^k \to B^n \) and \( C = \{ f(w) \mid w \in B^k \} \) is the set of codewords, then a simple decoder is the function \( g : B^n \to B^k \),
\[
g(v) = \begin{cases} 
    m & v \in C \text{ and } f(m) = v, \\
    \text{bork!} & v \notin C.
\end{cases}
\]
Rather than giving an error when you receive a message that is not a codeword, we instead use a nearest neighbour decoder.

Definition 11.8. Given a binary code \( C \subseteq B^n \), a nearest neighbour decoder is a function \( g : B^n \to C \) with the following property: For any word \( v \in B^n \), \( d(g(v), v) \leq d(c, v) \) for all \( c \in C \).

This decoder is optimal (in terms of minimizing the decoding error probability) for commonly used channels such as the memoryless binary symmetric channel (with “crossover” probability less than 1/2).
A nearest neighbour decoder is simply a function which takes a word to the nearest codeword. Since \( f : \mathbb{B}^k \rightarrow \mathcal{C} \) is a bijection, we can decode \( v \in \mathbb{B}^n \) as \( f^{-1}(g(v)) \), i.e., the reconstructed message, since \( f^{-1} : \mathcal{C} \rightarrow \mathbb{B}^k \).

**Proposition 11.9.** If \( \mathcal{C} \subseteq \mathbb{B}^n \) is a binary code and \( g : \mathbb{B}^n \rightarrow \mathcal{C} \) is a nearest neighbour decoder, then \( g(c) = c \) for all \( c \in \mathcal{C} \).

**Proof.** We know that for any codeword \( c' \in \mathcal{C} \), \( d(g(c), c) \leq d(c', c) \). In particular, for \( c' = c \), \( d(g(c), c) \leq d(c, c) = 0 \). Thus, \( d(g(c), c) = 0 \) and hence \( g(c) = c \).

**Definition 11.10.** The minimum distance of a binary code \( \mathcal{C} \subseteq \mathbb{B}^n \) is

\[
d = \min\{d(c, c') \mid c, c' \in \mathcal{C}, c \neq c'\}.
\]

**Example 11.11.** The \((n, 1)\) repetition code \( \mathcal{C} = \{00\cdots0, 11\cdots1\} \) has only two codewords, so its minimum distance is \( d = d(00\cdots0, 11\cdots1) = \text{wt}(00\cdots0+11\cdots1) = \text{wt}(11\cdots1) = n \).

The \((k + 1, k)\) parity check code \( \mathcal{C} = \{w \in \mathbb{B}^{k+1} \mid \text{wt}(w) \text{ is even}\} \) has minimum distance \( d = 2 \): Clearly \( 00\cdots0 \) and \( 110\cdots0 \) are distance two apart, and no pair of words with even weight can be distance 1 apart.

**Definition 11.12.** A code \( \mathcal{C} \subseteq \mathbb{B}^n \) can detect \( s \) errors if for all \( c \in \mathcal{C} \) and all \( r \in \mathbb{B}^n \) with \( 1 \leq \text{wt}(r) \leq s \) (We think of the word \( r \) as the transmission error.)

**Theorem 11.13.** If \( \mathcal{C} \subseteq \mathbb{B}^n \) is a binary code with minimum distance \( d \), then \( \mathcal{C} \) can detect \( s \) errors if and only if \( d \geq s + 1 \).

**Proof.** Suppose \( d \geq s + 1 \). If \( c \in \mathcal{C} \) and \( r \in \mathbb{B}^n \) with \( 1 \leq \text{wt}(r) \leq s \) then \( d(c, c + r) = \text{wt}(c + c + r) = \text{wt}(r) \leq s \). Therefore \( c + r \notin \mathcal{C} \) since the smallest distance between between any two distinct elements of \( c \) is \( d \geq d(c, c + r) \). Thus if \( d \geq s + 1 \) then \( \mathcal{C} \) can detect \( s \) errors.

If \( d \leq s \), then there is a pair of words \( c, c' \in \mathcal{C} \) with \( d = d(c, c') = \text{wt}(c + c') \). Let \( r = c + c' \). Since \( \text{wt}(r) = d \) and \( c + r = c + c + c' = c' \in \mathcal{C} \), we see that \( \mathcal{C} \) cannot detect \( s \) errors. Thus we have proven that if \( \mathcal{C} \) can detect \( s \) errors then \( d \geq s + 1 \).

**Definition 11.14.** A code \( \mathcal{C} \subseteq \mathbb{B}^n \) can correct \( s \) errors if for all \( c \in \mathcal{C} \) and for every word \( w \in \mathbb{B}^n \) with \( d(c, w) \leq s \), \( c \) is closer to \( w \) than all other codewords. That is, \( d(c, w) < d(c', w) \) for all \( c' \in \mathcal{C} \) with \( c \neq c' \).
If a code can correct $s$ errors then a nearest neighbour decoder $g : \mathbb{B}^n \rightarrow \mathcal{C}$ will map $g(w) = c$ for all words $w$ with $d(c, w) \leq s$.

**Theorem 11.15.** If $\mathcal{C} \subseteq \mathbb{B}^n$ is a binary code with minimum distance $d$, then $\mathcal{C}$ can correct $s$ errors if and only if $d \geq 2s + 1$.

**Proof.** If the smallest distance between any two codewords is $d$ and $d \geq 2s + 1$, then any word $v$ which is distance $s$ from a codeword $c$ must be at least distance $s + 1$ from any other codeword. Otherwise, there is some $c'$ with $d(v, c') \leq s$ and hence $d(c, c') \leq d(c, v) + d(v, c') \leq s + s = 2s < d$, a contradiction to our choice of $d$. Therefore if $d \geq 2s + 1$ then $\mathcal{C}$ can correct $s$ errors.

If $\mathcal{C}$ can correct $s$ errors, then any two codewords must be more than $2s$ apart. Otherwise, there are two codewords $c, c'$ with $d(c, c') \leq 2s$ and hence there is a word between them that is within a distance of $s$ from each. So, $\mathcal{C}$ cannot correct $s$ codewords, a contradiction. \qed

### 11.2 Group Codes

**Definition 11.16.** A group code (or linear code) $\mathcal{C} \subseteq \mathbb{B}^n$ is a binary code which is a subgroup of $\mathbb{B}^n$.

Our encoding function has been the map $\mathbb{B}^k \rightarrow \mathbb{B}^n$. A more general encoding function would be a map $G^k \rightarrow G^n$ for some group $G$. In this more general setting, a group code is the image of a group homomorphism $G^k \rightarrow G^n$. The image of a group homomorphism $G^k \rightarrow G^n$ is a subgroup of $G^n$, this definition of a group code corresponds to the one above. We could also consider linear maps $\mathbb{k}^k \rightarrow \mathbb{k}^n$ over an arbitrary (finite) field $\mathbb{k}$. These produce codes $\mathcal{C} \subseteq \mathbb{k}^n$ which are subspaces. Since all group homomorphisms are $\mathbb{k}$-linear maps where $\mathbb{k} = \mathbb{Z}_2 = \mathbb{B}$, these definitions coincide in our case.

Since $\mathbb{B}^n$ is a group of order $2^n$, we know that any subgroup has to have order $2^k$ for some $k$ by Lagrange’s theorem. To determine whether a non-empty subset of $\mathbb{B}^n$ is a subgroup, it suffices to check that it is closed under addition; every element is its own inverse, so every non-empty subset that is closed under addition is also closed under taking inverses and contains the zero element (i.e., $0^n = 00 \cdots 0$).

**Example 11.17.** The following are $(n, k)$ group codes.

(a) $n = 5$, $k = 1$, $\mathcal{C} = \{00000, 11111\} = \text{span}_B\{11111\}$. 

(b) \( n = 4, k = 2, C = \{0000, 0101, 1010, 1111\} = \text{span}_B\{0101, 1010\} \).

(c) \( n = 4, k = 3, \)
\[
C = \{0000, 0010, 0101, 0111, 1000, 1010, 1101, 1111\}
= \text{span}_B\{0010, 0101, 1000\}.
\]

**Proposition 11.18.** If \( C \subseteq \mathbb{F}^n \) is a group code then its minimum distance \( d \) equals \( \min\{\text{wt}(w) \mid w \in C \setminus \{0^n\}\} \).

**Proof.** Since \( \text{wt}(w) = d(0^n, w) \) and \( 0^n \in C \), \( d \leq \min\{\text{wt}(w) \mid w \in C \setminus \{0^n\}\} \). For \( c, c' \in C \), \( d(c, c') = \text{wt}(c + c') = d(0^n, c + c') \). Therefore
\[
d = \min\{d(c, c') \mid c, c' \in C, c \neq c'\}
= \min\{\text{wt}(c + c') \mid c, c' \in C, c \neq c'\}
\geq \min\{\text{wt}(c'') \mid c'' \in C \setminus \{0\}\}
\]
Therefore \( d = \min\{\text{wt}(c'') \mid c'' \in C \setminus \{0\}\} \). \( \square \)
Section 12: Encoding and Decoding Group Codes

12.1 Coset Decoding

Let \( r \in \mathbb{B}^n \) be an error word which can be applied during transmission to a codeword \( c \in C \) where \( C \subseteq \mathbb{B}^n \) is a group code. The set \( \{ c + r \mid c \in C \} = r + C \), of this error applied to all codewords in \( C \) is a coset of \( C \). Since there are many representatives for a coset, there are many different ways to represent the elements in \( r + C \) as a codeword plus an error term.

**Definition 12.1.** Let \( C \subseteq \mathbb{B}^n \) be a group code. For each coset of \( C \), we choose an element in that coset of smallest Hamming weight and call it the **coset leader**.

Not only is the coset leader the closest word in the coset to \( 0^n \), but it also gives the shortest distance from any element of the coset to a codeword (i.e., an element in \( C \)).

**Definition 12.2.** A **coset decoding table** of an \((n,k)\) group code \( C \subseteq \mathbb{B}^n \) is a table with \( 2^k \) columns and \( 2^n - k \) rows. The first row starts with \( 0^n \) and is followed by all other words in \( C \). Each of the remaining rows contains a coset of \( C \). The first entry in each row is a coset leader and the following entries are obtained by multiplying the coset leader (from the start of the row) by the element of \( C \) at the top of the column.

The following algorithm constructs the coset decoding table of a group code.

**Algorithm 12.3 (Coset Decoding Table Construction).**

(i) Write \( C \) as a row starting with \( 0^n \).

(ii) Pick a word \( w \in \mathbb{B}^n \) which is not in any of the previous rows, and which has smallest Hamming weight. Write this word in a new row below \( 0^n \).

(iii) Multiply\(^4 \) \( w \) by every element in \( C \), coming from the first column, and write the result in that column in the new row. This new row will contain \( w + C \) and \( w \) will be of smallest weight; \( w \) is our coset leader for \( w + C \).

(iv) Repeat steps 2 and 3, until you have used up all elements in \( \mathbb{B}^n \). There will be \( 2^{n-k} \) rows and \( 2^k \) columns in the table.

\(^4\)Note that “multiplication” in this case is nothing but component-wise addition in \( \mathbb{B}^n \).
Example 12.4. Consider the $(4, 2)$ group code $C = \{0000, 1011, 0110, 1101\}$. The first row of our coset table is

$$C : 0000, 1011, 0110, 1101.$$ 

The word 1000 has the least weight of all words in $B^4 \setminus C$. There are other words of weight 1, but we pick 1000 arbitrarily. Adding 1000 to our first row gives

$$1000 + C : 1000, 0011, 1110, 1101.$$ 

Notice that 0100 has not appeared in either of the first two rows and it has weight one – that is, lowest weight out of the remaining words. We now construct the third row:

$$0100 + C : 0100, 1111, 0010, 1001.$$ 

The smallest weight word remaining is 0001, which gives the row,

$$0001 + C : 0001, 1010, 0111, 1100.$$ 

Our entire table is now:

$$C : 0000, 1011, 0110, 1101$$

$$1000 + C : 1000, 0011, 1110, 1101$$

$$0100 + C : 0100, 1111, 0010, 1001$$

$$0001 + C : 0001, 1010, 0111, 1100$$

Here is how we use this table: If we receive message 1111, we look up which column it appears in our decoding table. In this case, 1111 appears in column 1011, so 1011 is the decoded message. The row of 1111 is labeled by the coset leader 0100, which is the error that was (mostly likely) applied to the original coded message 1011 to obtain 1111; $1111 = w = c + r = 1011 + 0100$.

Proposition 12.5. A coset decoding table gives a nearest neighbour decoding.

Proof. Suppose $w \in B^n$ is a word received at the channel output which appears in coset $r + C$ where $r$ is the coset leader of $r + C$. That is, $\text{wt}(r) \leq \text{wt}(u)$ for all $u \in r + C$. The coset decoding table’s decoding function $g : B^n \to C$ maps $g(w) = w + r$; it removes $r$, the error, from $w$.

In order to show that $g$ is a nearest neighbour decoder, we need to show that $d(g(w), w) \leq d(c, w)$ for all $c \in C$. Since $c \in C$, and $w \in r + C$, we can
write \( w = r + c' \) for some \( c' \in \mathcal{C} \) and hence \( c + w = c + r + c' = r + (c + c') \in r + \mathcal{C} \) as \( c + c' \in \mathcal{C} \). Therefore, \( \text{wt}(r) \leq \text{wt}(c + w) \) as \( r \) is a coset leader for \( r + \mathcal{C} \). Thus,

\[
d(g(w), w) = d(w + r, w) \\
= \text{wt}(w + r + w) \\
= \text{wt}(r) \\
\leq \text{wt}(c + w) \\
= d(c, w)
\]

and therefore \( g \) is a nearest neighbour decoder.

\[\square\]

### 12.2 Systematic Codes and Parity Check Matrices

Rather than record the whole table of cosets and coset leaders, we will construct a fast way to compute the coset leader of a given message. First we examine how a group code can be generated via a binary-valued matrix.

**Definition 12.6.** An \((n, k)\) group code \( \mathcal{C} \) is called **systematic** if each message \( w \in \mathbb{B}^k \) appears in the first \( k \) digits of exactly one codeword in \( \mathcal{C} \). In other words, a systematic group code is one in which each message appears at the beginning of its codeword.

For example, the parity check code which sends \( w \mapsto wp \) where \( p \) is the parity of \( w \), is a systematic group code.

**Definition 12.7.** A **systematic generator matrix** is a \( k \times n \) binary matrix \( M \) of the form \( [I_k \mid A] \) where \( A \) is \( k \times (n-k) \). The code \( \mathcal{C} = \mathcal{C}(M) \) associated to such a matrix is given by the span of its rows. The coding function of \( M \) is \( f_M : \mathbb{B}^k \to \mathbb{B}^n \) and is given by \( f_M(u) = uM \) under matrix multiplication in \( \mathbb{B} \) where the message word \( u \) is considered a row vector of size \( k \) (i.e., a \( 1 \times k \) matrix).

Systematic generator matrices send message \( u \) to the concatenation of \( u \) with \( uA \), yielding the codeword \( w = [u \ uA] \).

**Example 12.8.** Let \( M \) be the systematic generating matrix,

\[
M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.
\]
This matrix encodes messages in $\mathbb{B}^2$ as

\[
\begin{align*}
 f_M(00) &= (00)M = (0000) = 0000 \\
f_M(10) &= (10)M = (1011) = 1011 \\
f_M(01) &= (01)M = (0110) = 0110 \\
f_M(11) &= (11)M = (1101) = 1101,
\end{align*}
\]

and thus $C = \{1011, 0110, 0000, 1101\}$.

**Definition 12.9.** If $M = [I_k \mid A]$ is a $k \times n$ systematic generating matrix (where $I_k$ is the $k \times k$ identity matrix), then the **parity check matrix** of $M$ is the $n \times (n-k)$ matrix $H = \begin{bmatrix} A \\ I_{n-k} \end{bmatrix}$. The matrix $H$ defines a surjective (i.e., onto) map $\mathbb{B}^n \to \mathbb{B}^{n-k}$ by $w \mapsto wH$. The word $wH \in \mathbb{B}^{n-k}$ is called the **syndrome** of $w \in \mathbb{B}^n$.

**Theorem 12.10 (Orthogonality Theorem).** Let $C$ is an $(n,k)$ systematic group code. A word $w \in \mathbb{B}^n$ is a codeword if and only if the syndrome of $w$ is equal to the zero word of length $n-k$ (i.e., the all zero matrix $0_{1 \times (n-k)}$ of size $1 \times (n-k)$).

**Proof.** Note that $w$ is a codeword in the systematic group code $C$ iff $w = [u \ v]$ such that $v = uA$, where $v$ has size $1 \times (n-k)$, $u$ has size $1 \times k$ and $A$ has size $k \times (n-k)$. This is equivalent to

\[
0_{1 \times (n-k)} = uA - v \\
= uA - vI_{n-k} \\
= uA + vI_{n-k} \\
= [u \ v] \begin{bmatrix} A \\ I_{n-k} \end{bmatrix} \\
= [u \ v]H \\
= wH.
\]

Thus $w \in C$ iff $wH = 0_{1 \times (n-k)}$. □

**Corollary 12.11.** Suppose $C$ is a systematic group code. Two words $u, v \in \mathbb{B}^n$ are in the same coset of $C$ if and only if they have the same syndrome.
Proof. Two words $u$ and $v$ are in the same coset of $C$ if and only if $u - v \in C$. But $u - v \in C$ if and only if $(u - v)H = 0$, or equivalently $uH = vH$. (In this proof, we could have used plus instead of minus, but the negatives were kept for clarity.)

What’s really going on here is that we are identifying cosets of $C$ with elements of $B^{n-k}$ through the first isomorphism theorem: the map $\phi : B^n \to B^{n-k}$ given by $\phi(w) = wH$ has kernel $C$ and hence $\overline{\phi} : B^n/C \to B^{n-k}$ is an isomorphism. So, if we want to take a word $w \in B^n$ and determine which coset it’s in, it suffices to map $w$ to $wH \in B^{n-k}$ since elements of $B^{n-k}$ are in correspondence with the cosets of $C$.

Example 12.12. We already constructed the coset decoding table for $C = \{0000, 1011, 0110, 1101\}$:

$\begin{align*}
C &: 0000, 1011, 0110, 1101 \\
1000 + C &: 1000, 0011, 1110, 1101 \\
0100 + C &: 0100, 1111, 0010, 1001 \\
0001 + C &: 0001, 1010, 0111, 1100
\end{align*}$

The group code $C$ is a systematic group code coming from the matrix

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

The parity check matrix of $C$ is

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

Multiplying $H$ by the elements of $B^4$ we get

$$\begin{align*}
0000H &= 1011H = 0110H = 1101H = 00 \\
1000H &= 0011H = 1110H = 1101H = 11 \\
0100H &= 1111H = 0010H = 1001H = 10 \\
0001H &= 1010H = 0111H = 1100H = 01
\end{align*}$$
and thus we can see the syndrome of each coset. We now reduce our table down to a list of coset leaders and syndromes:

<table>
<thead>
<tr>
<th>Syndrome</th>
<th>Coset Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0000</td>
</tr>
<tr>
<td>11</td>
<td>1000</td>
</tr>
<tr>
<td>10</td>
<td>0100</td>
</tr>
<tr>
<td>01</td>
<td>0001</td>
</tr>
</tbody>
</table>

Algorithm 12.13 (Syndrome Decoding).

(i) Receive a word \( w \in \mathbb{B}^n \) as input.

(ii) Compute its syndrome \( h = wH \).

(iii) Use the table to lookup the coset leader \( r \) which goes with syndrome \( h \).

(iv) The corrected word is \( w + r \in \mathcal{C} \).

In the previous example, if we were to receive the word \( w = 1111 \), then \( h = 1111H = 10 \) and hence \( r = 0100 \). The decoded word is \( c = w + r = 1111 + 0100 = 1011 \).