Lecture notes for Math61: Introduction to Discrete Structures
Last revised March 10, 2020

Allen Gehret

Author address:

Department of Mathematics, University of California, Los Angeles, Los Angeles, CA 90095
E-mail address: allen@math.ucla.edu

Contents

Abstract

The goal of this class is to develop a basic level of mathematical literacy through the study of common structures and theories which often arise in mathematics and computer science.

I recommend you refer to these notes for learning the mathematical content of the course, and refer to the textbook for alternative explanations, examples, pictures, and additional exercises.

Note: these lecture notes are subject to revision, so the numbering of Lemmas, Theorems, etc. may change throughout the course and I do not recommend you print out too many pages beyond the section where we are in lecture. Any and all questions, comments, and corrections are enthusiastically welcome!

Last revised March 10, 2020.

2010 *Mathematics Subject Classification.* Primary .

The author is supported by the National Science Foundation under Award No. 1703709.

List of Figures

Introduction

We begin with a list of a few cardinal rules which you should always obey at all times if you want to be successful in this class and in future math classes.

(I) *Read.*

This rule is best explained by the following quote from Paul Halmos [**1**], where he is discussing how one is supposed to read mathematics:

> Don't just read it; fight it! Ask your own question, look for your own examples, discover your own proofs. Is the hypothesis necessary? Is the converse true? What happens in the classical special case? What about the degenerate cases? Where does the proof use the hypothesis?

Another way to think about reading is as follows: in real life when you read a novel (e.g., *Harry Potter*), it probably takes only a few minutes to read a single page, depending on how fast or slow a reader you are. In mathematics, it often takes a few minutes to read a *single sentence.* This is because you should constantly be employing the above advice from Halmos. Doing this might seem tedious at first, but it is the only way you can truly understand the material (and it becomes easier with practice!). If you don't do this, then you will only achieve a superficial understanding of the material and have to rely more on memorization.

(II) *Write in complete sentences.*

A mathematical proof is a form of communication where you are convincing a very skeptical (but otherwise mathematically literate) person that your argument is correct and the statement you claim is true is actually true. A proof is not a mess of scribbles and arrows and formulas on a page but instead is a reasoned and coherent argument that another human being can understand (and any two different human beings will understand in the same exact way). One easy way to force yourself to write a readable proof is to write in complete sentences. In this case, many times the verbs of the sentence might be equals signs or inequalities, and sometimes the nouns of the sentence will be mathematical objects or formulas. A more compelling way to say this is the following quote inspired by Quintilian (*Institutio Oratoria*, Book VIII, Chapter II, 24 from 95 AD.):

> Say what you mean. Mean what you say. Aim to make your work impossible to be misunderstood, rather than merely possible to be understood.

(III) *Always work from the definition.*

About a third of the content of the course is learning important definitions. Depending on who you ask, in mathematics the definitions are almost as important as the theorems themselves. Moreover, the definition of a particular word is the *only* thing that gives that word meaning, so you *must* always use the definition.

(IV) *Only write true statements.*

If you are writing something that is supposed to be a true statement, then it *better be* a true statement and you better know *why* it is a true statement. Really the only time you would ever knowingly write down something that is false is if you are doing a proof by contradiction; but even in this case, the introduction of the false statement is still in the service of justifying a true statement.

Conventions and notation

In this class the natural numbers is the set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ of nonnegative integers. In particular, we will consider 0 to be a natural number. Note: in the textbook the set $\mathbb{N}$ is denoted by $\mathbf{Z}^{nonneg}$, but we will not use this notation.

Unless stated otherwise, the following convention will be in force throughout the entire course:

Global Convention 0.0.1. Throughout, m and n range over $\mathbb{N} = \{0, 1, 2, \ldots\}$.

When we write "$X := Y$", we mean that the object X does not have any meaning or definition yet, and we are defining X to be the same thing as Y. When we write "$X = Y$" we typically mean that the objects X and Y both already are defined and are the same. In other words, when writing "$X := Y$" we are performing an action (giving meaning to X) and when we write "$X = Y$" we are making an assertion of sameness.

In making definitions, we will often use the word "if" in the form "We say that ... if ..." or "If ..., then we say that ...". When the word "if" is used in this way in *definitions*, it has the meaning of "if and only if" (but only in definitions!). For example:

Definition 0.0.2. Given integer $d, n \in \mathbb{Z}$, we say that d **divides** n if there exists an integer $k \in \mathbb{Z}$ such that $n = dk$.

This convention is followed in accordance with mathematical tradition. Also, we shall often write "iff" or "$\Leftrightarrow$" to abbreviate "if and only if."

Acknowledgements

I am grateful to Julian Ziegler Hunts for producing many of the figures in these lecture notes and to Ben Spitz for suggesting various exercises.

CHAPTER 1

Propositional Logic, Sets, and Induction

1.1. Propositional logic

Definition 1.1.1. A **proposition** is a sentence that is either true or false, but not both. In other words, a proposition is a statement for which it makes sense to assign a True/False value (of course, whether a proposition is actually true or false depends on context, definitions, interpretation, etc.).

Example 1.1.2. The following sentences are propositions:

(1) $2+2=5$.
(2) Winter is coming.
(3) I am the one who knocks.
(4) We were on a break.

The following sentences are *not* propositions:

(5) Should I stay or should I go now?
(6) May the force be with you.
(7) Is it too late now to say sorry?
(8) Everybody clap your hands!

In mathematics, and in language in general, more complicated propositions are built from simpler propositions by **(logical) operators** (and, or, not and implies).

Definition 1.1.3. Given propositions P and Q, the **conjunction** of P and Q (notation: $P \wedge Q$) is the proposition "P and Q". The truth value of the conjunction $P \wedge Q$ is determined by the individual truth values of P and Q separately in accordance with the following **truth table**:

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

In other words, $P \wedge Q$ is true precisely when both P and Q are true.

Definition 1.1.4. Given propositions P and Q, the **disjunction** of P and Q (notation: $P \vee Q$) is the proposition "P or Q". The truth table for $P \vee Q$ is as follows:

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

In other words, $P \vee Q$ is true precisely when at least one of P or Q is true.

Remark 1.1.5. In common language, there are two versions of "or". The version defined above is the so-called *inclusive or* because it includes the case when both P and Q are true. The other version is the *exclusive or* (notation: $P \texttt{ xor } Q$) which excludes the case when both P and Q are true:

P	Q	$P \texttt{ xor } Q$
T	T	F
T	F	T
F	T	T
F	F	F

In mathematics the exclusive or is rarely used and when people say "or" they almost always mean $P \vee Q$. In computer science both regularly get used. In this class, "or" will always mean "$P \vee Q$" and never "$P \texttt{ xor } Q$", so for us there will never be any ambiguity when we say "or". However in common everyday language, it is possible that this ambiguity might arise and it is good to be aware of it.

Definition 1.1.6. Given a proposition P, the **negation** of P (notation: $\neg P$) is the proposition "not P". Its truth table is as follows:

P	$\neg P$
T	F
F	T

In other words, $\neg P$ has the opposite truth value from P.

Definition 1.1.7. Given propositions P and Q, the proposition "if P, then Q" (notation: $P \to Q$) is called the **conditional proposition** with **hypothesis** (or **antecedent**) P and **conclusion** (or **consequent**) Q. Its truth table is as follows:

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

In other words, the only time $P \to Q$ is false is when the hypothesis P is true and the conclusion Q is false. One slightly counterintuitive feature of conditional propositions is that any time P is false, then $P \to Q$ is automatically true, *regardless of Q!* Whenever we encounter a conditional proposition $P \to Q$ which is true by virtue of P being false, then we say that $P \to Q$ is **vacuously true** (or **true by default**).

Definition 1.1.8. Given propositions P and Q, the proposition "P if and only if Q" (notation: $P \leftrightarrow Q$) is called a **biconditional proposition**. Its truth table is as follows:

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

In other words, $P \leftrightarrow Q$ is true precisely when P and Q have the same truth values. In writing, we will often abbreviate "if and only if" with the single word "iff".

Convention 1.1.9. For more complicated propositions we technically need to introduce parentheses to ensure *unique readability*. However, we wish to avoid a proliferation of parentheses in our propositions as much as possible. Therefore, we introduce the following convention of **operator precedence** (or *operator binding strength*) akin to "order of operations" for basic arithmetic. We agree that, in the absence of parentheses, we evaluate the operators in the following order of priority:

(1st) $\neg$
(2nd) $\wedge$
(3rd) $\vee$
(4th) $\to$
(5th) $\leftrightarrow$

For example, instead of writing

$$\big((\neg P) \wedge Q\big) \vee (\neg R)$$

we can just write

$$\neg P \wedge Q \vee \neg R.$$

In general we will not go too overboard with applying these conventions, since sometimes redundant parentheses can still assist in readability. For example, we might choose to write the above proposition as

$$(\neg P \wedge Q) \vee \neg R,$$

so that it is easier for the eye to see the grouping.

Since we will be in the business of reading/writing propositions and analyzing their truth values, one fundamental issue we need to address is the following: how can we tell when two propositions are actually saying the same thing? This is taken care of by the notion of *logical equivalence*:

Definition 1.1.10. Suppose we are given propositions P and Q which are both built from simpler propositions $p_1, \ldots, p_n$. Then we say that P and Q are **logically equivalent** (notation: $P \equiv Q$) if for all possible truth values for $p_1, \ldots, p_n$, the propositions P and Q have the same resulting truth value. In other words, $P \equiv Q$ means that in a truth table which contains both P and Q, the columns corresponding to P and Q are identical.

Example 1.1.11. Given propositions p_1 and p_2, define

$$P := p_1 \to p_2 \quad \text{and} \quad Q := \neg p_1 \vee p_2$$

(recall that $\neg p_1 \vee p_2$ is shorthand for $(\neg p_1) \vee p_2$ and not $\neg(p_1 \vee p_2)$, by our conventions for operator precedence). We claim that $P \equiv Q$.

Proof. To verify that $P \equiv Q$, we need to set up a truth table which contains both P and Q, and then observe that they have identical columns of truth values:

p_1	p_2	$\neg p_1$	$P := p_1 \to p_2$	$Q := \neg p_1 \vee p_2$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Since we observe that the columns for P and Q are the same ($TFTT$), we conclude that $P \equiv Q$. □

As the previous example shows, there is nothing difficult involved with proving that two propositions are equivalent. Indeed, it is a completely mechanical process of filling out a truth table in accordance with the rules for the various logical operators.

Remark 1.1.12. Logical equivalence is a so-called *equivalence relation* on the collection of propositions (see Definition 2.5.1) in the sense that given propositions P, Q, and R, the following always hold:

(1) $P \equiv P$,
(2) if $P \equiv Q$, then $Q \equiv P$, and
(3) if $P \equiv Q$ and $Q \equiv R$, then $P \equiv R$.

Furthermore, any time you know that two propositions are logically equivalent, then you are free to treat them as if they are *exactly the same* when doing proofs.

Sometimes we will encounter propositions which are *always true* and also propositions which are *always false*. These have special names:

Definition 1.1.13. A **tautology** (or **tautological statement**) is a proposition which is always true, for all possible truth assignments. In other words, a tautology is a proposition whose column in a truth table has all T's.

A **contradiction** (or **contradictory statement**) is a proposition which is always false, for all possible truth assignments (i.e., a contradiction has all F's in its column in a truth table).

We now record some common laws for propositional logic. The proofs of each of the laws follows by considering truth tables as in Example 1.1.11.

Boolean Algebra of Propositional Logic 1.1.14. *Given propositions P, Q, and R, a tautology T, and a contradiction F, the following logical equivalences always hold:*

(1) (Associative laws) $(P\vee Q)\vee R \equiv P\vee(Q\vee R)$ *and* $(P\wedge Q)\wedge R \equiv P\wedge(Q\wedge R)$
(2) (Commutative laws) $P \vee Q \equiv Q \vee P$ *and* $P \wedge Q \equiv Q \wedge P$
(3) (Distributive laws) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ *and* $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
(4) (Identity laws) $P \vee F \equiv P$ *and* $P \wedge T \equiv P$
(5) (Negation laws) $P \vee \neg P \equiv T$ *and* $P \wedge \neg P \equiv F$
(6) (Idempotent laws) $P \vee P \equiv P$ *and* $P \wedge P \equiv P$
(7) (Bound laws) $P \vee T \equiv T$ *and* $P \wedge F \equiv F$
(8) (Absorption laws) $P \vee (P \wedge Q) \equiv P$ *and* $P \wedge (P \vee Q) \equiv P$
(9) (Double negation law) $\neg(\neg P) \equiv P$
(10) (T/F laws) $\neg F \equiv T$ *and* $\neg T \equiv F$
(11) (De Morgan's laws) $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ *and* $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$

1.2. Sets and set constructions

A **set** is a collection of mathematical objects. Mathematical objects can be almost anything: numbers, other sets, functions, vectors, relations, matrices, graphs etc. For instance:

$$\{2, 5, 7\}, \quad \big\{3, 5, \{8, 9\}\big\}, \quad \text{and} \quad \{1, 3, 5, 7, \ldots\}$$

are all sets. A member of a set is called is called an **element** of the set. The membership relation is denoted with the symbol "$\in$", for instance, we write "$2 \in \{2, 5, 7\}$" (pronounced "2 is an element of the set $\{2, 5, 7\}$") to denote that the number 2 is a member of the set $\{2, 5, 7\}$. There are several ways to describe a set:

(1) by explicitly listing the elements in that set, i.e., the set $\{2, 5, 7\}$ is a set with three elements, the number 2, the number 5, and the number 7.

(2) by specifying a "membership requirement" that determines precisely which objects are in that set. For instance:

$$\big\{n \in \mathbb{Z} : \underbrace{n \text{ is positive and odd}}_{\text{membership requirement}}\big\}$$

is the set of all odd positive integers. The above set is pronounced "the set of all integers n such that n is positive and odd". The colon ":" is usually pronounced "such that", and the condition to the right of the colon is the membership requirement. Defining a set in this way is sometimes referred to as using **set-builder notation** since you are describing how the set is built (in the above example, the set is built by taking all integers and keeping the ones that are positive and odd), instead of explicitly specifying which elements are in the set. We could also choose to describe the set above by writing

$$\{1, 3, 5, 7, \ldots\},$$

although this might be a less ideal description because it requires the reader to guess or infer the meaning of "...".

The following is a very famous set:

Definition 1.2.1. The **emptyset** is the set which contains no elements (hence the name). It is denoted by either $\emptyset$ or $\{\}$.

The following are some of the main relationships two sets can have:

Definition 1.2.2. Suppose A and B are sets. We say that

(1) A is a **subset** of B (notation: $A \subseteq B$) if every element of A is also an element of B, i.e.,
  - For every x, if $x \in A$, then $x \in B$

(2) A is **equal** to B (notation: $A = B$) if A and B have exactly the same elements, i.e.,
  - For every x, $x \in A$ if and only if $x \in B$

  equivalently, $A = B$ means the same thing as $A \subseteq B$ and $B \subseteq A$

(3) A is a **proper subset** of B (notation: $A \subsetneq B$) if $A \subseteq B$ and $A \neq B$.

Note that for any set A, we automatically have $\emptyset \subseteq A$.

We now discuss how one might go about proving statements of the form "$A \subseteq B$" and "$A = B$" for sets A and B.

Question 1.2.3. *Suppose you are in a situation where you are asked to prove $A \subseteq B$ for some sets A and B. What is the general strategy?*

Answer. This depends on what the sets A and B actually are, but in general, you take an arbitrary element $x \in A$ and by some argument, conclude that x also has to be an element of B, i.e., that $x \in B$. Here, "arbitrary" means that you are not allowed to assume anything specific about the element x *except* that it belongs to A. We give an example from linear algebra. □

Another answer. Another strategy is to do a proof by contradiction. To do this, you first assume towards a contradiction that $A \not\subseteq B$ (i.e., it is not the case that

$A \subseteq B$). This means that there is at least one $x \in A$ such that $x \notin B$. Given an x like this, you then argue (using the specifics of whatever is assumed about A and B) to get some contradiction. Once you get a contradiction, you can conclude that it must actually be the case that $A \subseteq B$. □

Example 1.2.4. Prove that

$$\big\{(a,b,c) \in \mathbb{R}^3 : a = 0 \text{ and } b = 0\big\} \;\subseteq\; \big\{(a,b,c) \in \mathbb{R}^3 : a + b = 0\big\}$$

Proof. Call the first set A and the second set B. We want to prove that $A \subseteq B$. Let $(a,b,c) \in A$ be arbitrary. This means that $a = 0$ and $b = 0$. We want to show that (a,b,c) is an element of B. In order to be an element of B, it would have to be true that $a+b=0$. However, since $a = 0$ and $b = 0$, then we have $a+b = 0+0 = 0$. Thus (a,b,c) satisfies the membership requirement for B so we can conclude that $(a,b,c) \in B$. Since (a,b,c) was an arbitrary element of A, we can conclude that $A \subseteq B$. □

INCORRECT proof. We want to show that $A \subseteq B$. Let (a,b,c) be an element of A, for instance, $(0,0,2)$. The vector $(0,0,2)$ is also in B since $a+b = 0+0 = 0$ for this vector. Thus $A \subseteq B$. [Here, the crime is that we showed that a single specific vector from A is also in B. This does not constitute a proof that *all* vectors from A are also elements of B.] □

Question 1.2.5. *Suppose you are asked to prove that $A = B$ where A and B are sets (possibly with two different-seeming descriptions). How do you prove that $A = B$?*

Answer. This means you have to prove two separate things:

(1) prove $A \subseteq B$, and
(2) prove $B \subseteq A$.

So this breaks down to two different proofs, each one then reduces to answering Question 1.2.3 for those particular sets. □

Definition 1.2.6. Given sets A and B, we define their **union** (notation: $A \cup B$) to be the set of all elements that are in either A or B, i.e.,

$$A \cup B \;:=\; \{x : x \in A \text{ or } x \in B\}.$$

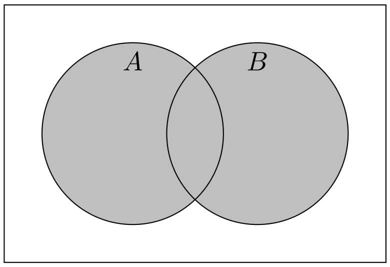

Figure 1.1: Venn diagram of the union $A \cup B$ of the sets A and B

Definition 1.2.7. Given sets A and B, we define their **intersection** (notation: $A \cap B$) to be the set of all elements they have in common, i.e.,

$$A \cap B \;:=\; \{x : x \in A \text{ and } x \in B\}.$$

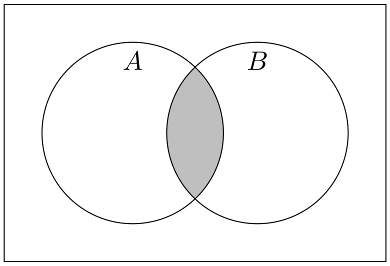

Figure 1.2: Venn diagram of the intersection $A \cap B$ of the sets A and B

Definition 1.2.8. Given sets A and B, we define their **(set) difference** (or **relative complement**) (notation: $A \setminus B$) to be the subset of A of all elements in A that are *not* in B, i.e.,

$$A \setminus B \ := \ \{x : x \in A \text{ and } x \notin B\}.$$

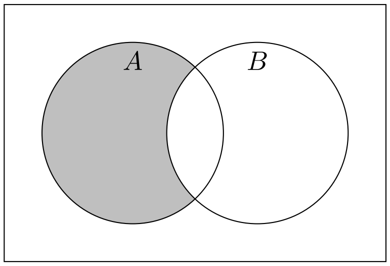

Figure 1.3: Venn diagram of the difference $A \setminus B$ of the sets A and B

Occasionally we will be in a mathematical situation where all relevant sets under discussion are subsets of one large sets. For example:

(1) In probability, all events E are subsets of the sample space Ω
(2) In real analysis, all relevant sets at a given moment might be subsets of the real numbers $\mathbb{R}$

In such situations, it is convenient to work with a so-called *universal set.* A **universal set** (or **universe**) is a set U such that all sets under discussion are implicitly assumed to be a subset of U. In such a situation, it makes sense to talk about the *complement* of a set:

Definition 1.2.9. Suppose U is a universal set, and $X \subseteq U$. We define the **complement** of X (notation: $\overline{X}$) to be the subset of U consisting of all elements which are *not* in X, i.e.,

$$\overline{X} \ := \ U \setminus X \ = \ \{x \in U : x \notin X\}.$$

Note that when we are working in a universal set, we can rewrite set difference in terms of intersection and complement:

$$A \setminus B \ = \ A \cap \overline{B}$$

Warning: the operation of *complement* only makes sense when it is clear what the universal set U is. Usually this will be explicitly told to you or easily inferred from the context. In some contexts there is no universal set, in which case complements don't make sense (but relative complements still do).

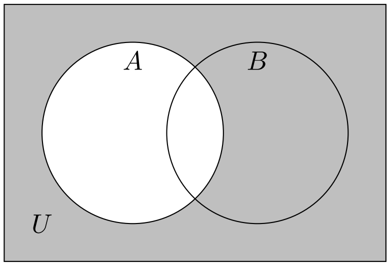

Figure 1.4: Venn diagram of the complement $\overline{A}$ of A in the universal set U

One very important invariant of a set is its *size* or *cardinality* (i.e., number of elements). The notion of *cardinality* is actually quite subtle, but for finite sets the following superficial definition is good enough for our current purposes:

Definition 1.2.10. Given a finite[1] set X, we define the **cardinality** of X (notation: $|X|$ or sometimes $\#X$) to be the number of elements of X.

Example 1.2.11. $|\emptyset| = 0$, $|\{\emptyset\}| = 1$ $\big|\{0,1,2,3\}\big| = 4$, and $\big|\{0,1,\{2,3\}\}\big| = 3$.

Definition 1.2.12. Given a set X, we define the **powerset of** X (notation: $\mathcal{P}(X)$) to be the set of all subsets of X:

$$\mathcal{P}(X) \ := \ \{A : A \text{ is a set and } A \subseteq X\}$$

Example 1.2.13. Suppose $X = \{0,1,2\}$. Then

$$\mathcal{P}(X) \ = \ \big\{\{0,1,2\},\{0,1\},\{0,2\},\{1,2\},\{0\},\{1\},\{2\},\emptyset\big\}$$

Note that $|X| = 3$ whereas $\big|\mathcal{P}(X)\big| = 8 = 2^3$.

Suppose we have elements a, b, c, d such that $\{a, b\} = \{c, d\}$. It is tempting in this situation to conclude that "$a = c$ and $b = d$", but in general this is *false*. Indeed, we have $\{1,2\} = \{2,1\}$, but $1 \neq 2$ and $2 \neq 1$. This is because elements of a set are *unordered*. To get an *ordered* version of a two-element set we introduce the so-called *ordered pair* construction.

Definition 1.2.14. Given objects a and b, we define their **ordered pair** to be the object:

$$(a,b) \ := \ \big\{\{a\},\{a,b\}\big\}$$

The righthand side of the definition might seem a little funny, but it guarantees the following:

Ordered Pair Property 1.2.15. *For every a, b, c, d,*

$$(a,b) \ = \ (c,d) \quad \textit{if and only if} \quad a = c \textit{ and } b = d.$$

Proof. This is Exercise 1.5.6. □

[1] See Definition 7.1.6 for the definition of a finite set.

In practice, the Ordered Pair Property 1.2.15 is really the only feature of ordered pairs that is ever relevant. You will almost never have to actually deal with the definition "$\big\{\{a\},\{a,b\}\big\}$", except when it comes proving the Ordered Pair Property.

Definition 1.2.16. Given sets X and Y, we define the **cartesian product (of X and Y)** (notation: $X \times Y$) to be the following set:

$$X \times Y \ := \ \big\{(x,y) : x \in X \text{ and } y \in Y\big\}$$

Example 1.2.17. Suppose $X = \{0,1\}$ and $Y = \{a,b,c\}$. Then the cartesian product of X and Y is

$$X \times Y \ = \ \big\{(0,a),(0,b),(0,c),(1,a),(1,b),(1,c)\big\}.$$

Note that $|X| = 2$, $|Y| = 3$, and $|X \times Y| = 2 \cdot 3 = 6$.

We conclude this section with the set-theoretic analogue of the identities in Boolean Algebra for Proposition Logic .

Boolean Algebra of Sets 1.2.18. *Given sets X, Y, and Z, and a universal set U, the following set equalities always hold:*

(1) (Associative laws) $(X\cup Y)\cup Z = X\cup(Y\cup Z)$ and $(X\cap Y)\cap Z = X\cap(Y\cap Z)$
(2) (Commutative laws) $X \cup Y = Y \cup X$ and $X \cap Y = Y \cap X$
(3) (Distributive laws) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ and $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$
(4) (Identity laws) $X \cup \emptyset = X$ and $X \cap U = X$
(5) (Complement laws) $X \cup \overline{X} = U$ and $X \cap \overline{X} = \emptyset$
(6) (Idempotent laws) $X \cup X = X$ and $X \cap X = X$
(7) (Bound laws) $X \cup U = U$ and $X \cap \emptyset = \emptyset$
(8) (Absorption laws) $X \cup (X \cap Y) = X$ and $X \cap (X \cup Y) = X$
(9) (Double complement law) $\overline{\overline{X}} = X$
(10) (0/1 laws) $\overline{\emptyset} = U$ and $\overline{U} = \emptyset$
(11) (De Morgan's laws) $\overline{(X \cup Y)} = \overline{X} \cap \overline{Y}$ and $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$

Proof. We will only give a proof for the first De Morgan's law:

$$\overline{(X \cup Y)} \ = \ \overline{X} \cap \overline{Y}.$$

This will also be an example of how to prove a *universal statement*. Recall from the definition of two sets being equal (i.e., having exactly the same elements), the statement we need to prove written out formally is:

$$\forall x \in U(x \in \overline{(X \cup Y)} \leftrightarrow x \in \overline{X} \cap \overline{Y}),$$

i.e., we need to show the "iff" statement is true for *every* $x \in U$. Let $x \in U$ be arbitrary. We will prove this by a trail of equivalences and definition-unwinding:

$$\begin{aligned}
x \in \overline{(X \cup Y)} &\Leftrightarrow x \notin X \cup Y \quad \text{(by def. of complement)}\\
&\Leftrightarrow \neg(x \in X \cup Y) \quad \text{(by def. of } \notin\text{)}\\
&\Leftrightarrow \neg(\underbrace{x \in X}_{P} \vee \underbrace{x \in Y}_{Q}) \quad \text{(by def. of union } \cup\text{)}\\
&\Leftrightarrow \neg(\underbrace{x \in X}_{P}) \wedge \neg(\underbrace{x \in Y}_{Q})\\
&\qquad \text{(by De Morgan's law for } \textit{Propositions}\text{: } \neg(P \vee Q) \equiv \neg P \wedge \neg Q\text{))}\\
&\Leftrightarrow x \notin X \wedge x \notin Y\\
&\Leftrightarrow x \in \overline{X} \wedge x \in \overline{Y}\\
&\Leftrightarrow x \in \overline{X} \cap \overline{Y}.
\end{aligned}$$

Comparing the first and last statement, we see that $x \in \overline{(X \cup Y)}$ iff $x \in \overline{X} \cap \overline{Y}$. Since $x \in U$ was arbitrary (i.e., we didn't assume anything special about x beyond the assumption $x \in U$), we conclude that this is true for all $x \in U$. [Note: In Answer to Question 1.2.5 we said you need to prove two set containments $A \subseteq B$ and $B \subseteq A$ separately to conclude $A = B$. The proof here is an exception because every step along the way was easily reversible, but in general that might not be the case.]

The proofs for the rest of the laws work exactly the same way: unwinding definitions, writing everything out fully in terms of logical operators, and applying the appropriate Propositional Logic equivalence. As an exercise, you are encouraged to prove the other laws. □

Remark 1.2.19. ($\Leftrightarrow$ vs. $\leftrightarrow$) In the above proof, $\Leftrightarrow$ is an abbreviation for "if and only if". So when we write "$x \in \overline{X} \wedge x \in \overline{Y} \Leftrightarrow x \in \overline{X} \cap \overline{Y}$", this is just shorthand for a longer English sentence asserting that whenever x makes the proposition on the lefthand side true, it also makes the proposition on the righthand side true, and vice-versa (in this case, because of the definition of intersection $\cap$). There is a subtle distinction between this usage of "if and only if" and the logical operator $\leftrightarrow$. Namely, when writing "if and only if" in a proof, we are *actually asserting* as the prover that two things are equivalent. The symbol $\leftrightarrow$ does not do this; given propositions P and Q (which each could either be true or false), the symbol $\leftrightarrow$ allows us to build a new proposition $P \leftrightarrow Q$ (which could also be either true or false). In other words, $\leftrightarrow$ is part of the *formal language* for writing propositions (it's a symbol which combines two propositions, equipped with a rule determining the overall truth value given the truth values of the individual propositions), whereas $\Leftrightarrow$ is part of the *meta-language* of English in which we are expressing our argument in.

We conclude this section with a few more constructions and definitions we will need later:

Definition 1.2.20. We define **ordered triples**, **ordered quadruples**, and more generally **ordered n-tuples** recursively as follows:

$$\begin{aligned}(a_1, a_2, a_3) &:= \big((a_1, a_2), a_3\big)\\ (a_1, a_2, a_3, a_4) &:= \big((a_1, a_2, a_3), a_4\big)\\ &\vdots\\ (a_1, \ldots, a_{n+1}) &:= \big((a_1, \ldots, a_n), a_{n+1}\big)\end{aligned}$$

for any objects $a_1, a_2, a_3, \ldots$. It follows that two ordered n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are equal iff $a_i = b_i$ for each $i \in \{1, \ldots, n\}$. Next, given sets $A_1, \ldots, A_n$, we define their **n-fold cartesian product** to be the set

$$A_1 \times \cdots \times A_n \;:=\; \big\{(a_1, \ldots, a_n) : a_i \in A_i \text{ for each } i = 1, \ldots, n\big\}.$$

Definition 1.2.21. (1) We say that two sets X and Y are **disjoint** if $X \cap Y = \emptyset$.

(2) Given a collection[2] of sets S. We say that the collection of sets in S is **pairwise disjoint** if for every $X, Y \in S$, if $X \neq Y$, then $X \cap Y = \emptyset$.

(3) Given a set X, we say that a collection S of subsets of X (so $S \subseteq \mathcal{P}(X)$) is a **partition of** X if

(a) for every $Y \in S$, $Y \neq \emptyset$,

(b) for every $x \in X$, there is exactly one $Y \in S$ such that $x \in Y$.

It follows that a partition of X is pairwise disjoint.

1.3. Familiar number systems and some basic features

In this section we review some familiar number systems and some of their basic features. In lieu of giving precise and formal definitions we opt instead for the following casual discussion. We relegate a more thorough discussion to Appendix A.

You have probably encountered the following number systems before:

$$\mathbb{N} \;=\; \{0, 1, 2, 3, \ldots\} \quad \text{(the \textbf{natural numbers})}$$

$$\mathbb{Z} \;=\; \{0, 1, -1, 2, -2, \ldots\} \quad \text{(the \textbf{integers})}$$

$$\mathbb{Q} \;=\; \{k/\ell : k, \ell \in \mathbb{Z}, \ell \neq 0\} \;=\; \{\text{all ``fractions''}\} \quad \text{(the \textbf{rational numbers})}$$

and finally:

$$\mathbb{R} \quad \text{(the set of all \textbf{real numbers})}$$

Furthermore, we know that these number systems contain one another:

$$\mathbb{N} \;\subseteq\; \mathbb{Z} \;\subseteq\; \mathbb{Q} \;\subseteq\; \mathbb{R}$$

i.e., every natural number *is an* integer, every integer *is a* rational number, and every rational number *is a* real number.

The development of these number systems somewhat reflects the stages in life you learned about them. For example:

(1) As a young child you probably first learned about the positive natural numbers (or "counting numbers"), i.e., $1, 2, 3, 4, 5, \ldots$ You also slowly learned how to add and multiply these numbers.

[2] *Collection* is a synonym for set. Often when discussing a set consisting of other sets, we will instead say *collection* of sets or *family* of sets.

(2) Later on in elementary school you learn about the numbers "0" as well as the negatives of the natural numbers $-1, -2, -3, \ldots$ You also learned how to add and multiply these numbers.
(3) At some point in elementary school you also start to learn about fractions $1/2, 2/3, 3/4, \ldots$ as well as how to add and multiply these numbers as well.
(4) Finally, later in middle school and high school, you start learning about "real numbers" which aren't fractions, like $\sqrt{2}, \pi$, and e. You were probably given a vague (and possibly incorrect) description of "what is the set of real numbers $\mathbb{R}$" suitable enough to learn how to do the computations in calculus. However, you probably didn't spend any time discussing what $\mathbb{R}$ "really is", as a mathematical object.

In this class we will assume familiarity with the basic properties of $\mathbb{R}$, if you want to really understand $\mathbb{R}$ you should take Math131a.

When it comes to arithmetic involving numbers, we will be interested in adding an arbitrary number of numbers together. The best way to make this precise is with *summation notation*:

Notation 1.3.1. Suppose $M, N \in \mathbb{Z}$ are integers such that $M \leq N$ and suppose we are given numbers $a_M, a_{M+1}, \ldots, a_N$ indexed by all integers between M and N. Then we denote the **finite summation** of the integers $a_M, \ldots, a_N$ by

$$\sum_{k=M}^{N} a_k \;:=\; a_M + a_{M+1} + \cdots + a_N.$$

The "k" in the expression $\sum_{k=M}^{N} a_k$ is referred to as the **index of summation** and it is a **dummy variable**, i.e., a variable which only exists and takes value inside the summation. This is analogous to the control variable of a `for-loop` in a computer program. Accordingly, the index of summation can be changed to any other variable which is not being used and the meaning will stay the same, i.e.,

$$\sum_{k=M}^{N} a_k \;=\; \sum_{\ell=M}^{N} a_\ell \;=\; \sum_{j=M}^{N} a_j \;=\; \cdots$$

The following is basic and obvious, but very useful for avoiding so-called *off-by-one errors*[3] in mathematics and computer science:

Remark 1.3.2 (Number of elements in a list)**.** Suppose $M, N \in \mathbb{Z}$ are integers such that $M \leq N$. Then there are $N - M + 1$ integers in the list $M, M+1, \ldots, N$. Put another way,

$$\sum_{k=M}^{N} 1 \;=\; N - M + 1.$$

A handy pneumonic device for remembering this is as follows: given a list

$$a_M, a_{M+1}, \ldots, a_N$$

with first index M and last index N, then the number of terms in the list is

Last (index) minus first (index) plus one.

The following two summation formulas are very useful in analysis and arithmetic.

[3] See `https://en.wikipedia.org/wiki/Off-by-one_error`

Difference of Powers Formula 1.3.3. *For any $n \in \mathbb{N}$ such that $n \geq 2$ and $a, b \in \mathbb{R}$,*

$$\begin{aligned} a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \\ &= (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k \end{aligned}$$

Proof. Start with the summation version of the righthand side:

$$(a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$$

distribute the $(a-b)$:

$$= a\left(\sum_{k=0}^{n-1} a^{n-1-k}b^k\right) - b\left(\sum_{k=0}^{n-1} a^{n-1-k}b^k\right) = \sum_{k=0}^{n-1} a^{n-k}b^k - \sum_{k=0}^{n-1} a^{n-1-k}b^{k+1}$$

Pull out the first term from the first sum and the last term from the second sum:

$$= a^n + \left(\sum_{k=1}^{n-1} a^{n-k}b^k - \sum_{k=0}^{n-2} a^{n-1-k}b^{k+1}\right) - b^n$$

Reindex the second sum so that it starts at $k = 1$:

$$= a^n + \left(\sum_{k=1}^{n-1} a^{n-k}b^k - \sum_{k=1}^{n-1} a^{n-k}b^k\right) - b^n = a^n - b^n,$$

which is the desired lefthand side of the formula. □

Geometric Sum Formula 1.3.4. *For any $n \in \mathbb{N}$ and $r \in \mathbb{R}$ such that $r \neq 1$,*

$$\sum_{k=0}^{n} r^k = 1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1-r}.$$

Proof. Setting $a = 1$ and $b = r$ in the Difference of Powers Formula 1.3.3 gives for $n+1$:

$$1 - r^{n+1} = (1-r)(1 + r + \cdots + r^n).$$

The Geometric Sum Formula follows from dividing both sides by $1 - r$, which is permitted since $1 - r \neq 0$. □

Factorials and binomial coefficients also play an important role in analysis and arithmetic:

Definition 1.3.5. For nonnegative integers n we define the **factorial** $n!$ of n recursively by setting

$$0! := 1 \quad \text{and} \quad n! := n \cdot (n-1)! \quad \text{if } n \geq 1.$$

In other words, for $n \geq 1$ we have

$$n! = n \cdot (n-1) \cdots 2 \cdot 1.$$

Given nonnegative integers n and k such that $0 \leq k \leq n$, we define the **binomial coefficient** $\binom{n}{k}$ via the formula

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

When the binomial coefficients are displayed as a triangular array as in Figure 1.5 below, this is commonly referred to as *Pascal's Triangle*. We chose to make our triangle left-justified (to make it easier to see the corresponding n and k values), but it is also common to display the triangle so that each line is centered above the line below it (see Figure 6.7.1 in [**2**]).

$\binom{n}{k}$	$k=0$	1	2	3	4	5	6	7	$\cdots$
$n=0$	1								
1	1	1							
2	1	2	1						
3	1	3	3	1					
4	1	4	6	4	1				
5	1	5	10	10	5	1			
6	1	6	15	20	15	6	1		
7	1	7	21	35	35	21	7	1	
$\vdots$	$\vdots$								$\ddots$

Figure 1.5: Pascal's Triangle: Table of binomial coefficients $\binom{n}{k}$

Factorials and binomial coefficients are fundamental in *combinatorics*, the field of mathematics devoted to counting. In analysis they show up quite naturally in many formulas and expansions (e.g., *Binomial Theorem* and *Taylor expansions*). The following easy identity relates adjacent binomial coefficients:

Pascal's Rule 1.3.6. *For $1 \le k < n$ we have*

$$\binom{n-1}{k} + \binom{n-1}{k-1} \; = \; \binom{n}{k}.$$

Proof. Note that for $1 \le k < n$ we have

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= (n-1)! \left[\frac{n-k}{k!(n-k)!} + \frac{k}{k!(n-k)!} \right] \\
&= (n-1)! \frac{n}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}.
\end{aligned}$$

□

In Figure 1.6 below, we demonstrate three instances of Pascal's Rule. From top to bottom they are:

$$\begin{aligned}
\binom{1}{0} + \binom{1}{1} &= \binom{2}{1} \quad \text{i.e.,} \quad 1+1 = 2 \\
\binom{4}{1} + \binom{4}{2} &= \binom{5}{2} \quad \text{i.e.,} \quad 4+6 = 10 \\
\binom{6}{4} + \binom{6}{5} &= \binom{7}{5} \quad \text{i.e.,} \quad 15+6 = 21
\end{aligned}$$

$\binom{n}{k}$	$k=0$	1	2	3	4	5	6	7	$\cdots$
$n=0$	1								
1	$\boxed{1 +}$	$\boxed{1}$							
		$=$							
2	1	$\boxed{2}$	1						
3	1	3	3	1					
4	1	$\boxed{4 +}$	$\boxed{6}$	4	1				
			$=$						
5	1	5	$\boxed{10}$	10	5	1			
6	1	6	15	20	$\boxed{15 +}$	$\boxed{6}$	1		
						$=$			
7	1	7	21	35	35	$\boxed{21}$	7	1	
$\vdots$	$\vdots$								$\ddots$

Figure 1.6: Demonstration of Pascal's Rule

1.4. The well-ordering principle and induction

Here is an important basic property about $\mathbb{N}$ which we will take for granted:

Well-Ordering Principle 1.4.1. *Suppose $S \subseteq \mathbb{N}$ is such that $S \neq \emptyset$. Then S has a least element, i.e., there is some $a \in S$ such that for all $b \in S$, $a \leq b$.*

The following fundamental theorem is more commonly referred to as *The Division Algorithm*:

Quotient-Remainder Theorem 1.4.2. *Suppose $d, n \in \mathbb{Z}$ and $d \neq 0$. Then:*

(1) (existence) there exists $q, r \in \mathbb{Z}$ such that

$$n = dq + r \quad \textit{and} \quad 0 \leq r < |d|$$

(2) (uniqueness) if $q_0, q_1, r_0, r_1 \in \mathbb{Z}$ are such that
(a) $n = dq_0 + r_0$ and $0 \leq r_0 < |d|$, and
(b) $n = dq_1 + r_1$ and $0 \leq r_1 < |d|$,
then $q_0 = q_1$ and $r_0 = r_1$.

Item (2) asserts that the q and r in (1) are *unique*, i.e., there are no other different options for q and r that also work. We shall call q the **quotient** and r the **remainder** resulting from dividing n by d.

Proof. We will prove two cases:

Case 1: $(d > 0)$. Consider the following set of all *candidate remainders*:

$$R \ := \ \{n - dq : q \in \mathbb{Z} \text{ and } n - dq \geq 0\} \ \subseteq \ \mathbb{N}.$$

We claim that $R \neq \emptyset$. Consider the following integer:

$$q \ := \ -|n|$$

Then we see that

$$n - dq \ = \ n - d(-|n|) \ = \ n + d|n| \ \geq n + |n| \ \geq 0 \quad (\text{using } d > 0 \text{ in first inequality})$$

and so $n - dq \in R$ (hence R is not empty).

By the Well-Ordering Principle 1.4.1, the set has a least element $r_0 = n - dq_0 \in R$ for some $q_0 \in \mathbb{Z}$. We claim that $0 \leq r_0 < d$. Assume towards a contradiction that $r_0 \geq d$. In this case the natural number $r_1 := n - d(q_0 + 1)$ is an even smaller element of R than r_0 is. Indeed, it is in R:

$$r_1 \ = \ n - d(q_0 + 1) \ = \ n - dq_0 - d \ = \ r_0 - d \ \geq \ 0 \quad (\text{since } r_0 \geq d)$$

and it is smaller than r_0:

$$r_1 - r_0 \ = \ n - d(q_0 + 1) - n - dq_0 \ = \ -d \ < \ 0.$$

This contradicts the assumption that $r_0 = \min R$. Since we arrived at a contradiction, we conclude that $0 \leq r_0 < d$. This finishes the proof of Existence for the case.

For Uniqueness, suppose we have $q_0, q_1 \in \mathbb{Z}$ and $r_0, r_1 \in \mathbb{N}$ such that

$$n \ = \ dq_0 + r_0 \ = \ dq_1 + r_1 \quad \text{and} \quad 0 \leq r_0, r_1 < d.$$

We can rewrite this as

$$r_1 - r_0 \ = \ d(q_0 - q_1)$$

and taking absolute values gives us

$$|r_1 - r_0| \ = \ d|q_0 - q_1|.$$

Next, since both $0 \leq r_0, r_1 < d$, we get that $|r_1 - r_0| < d$, and so

$$d|q_0 - q_1| \ < \ d.$$

Thus

$$0 \ \leq \ |q_0 - q_1| \ < \ 1.$$

This forces $|q_0 - q_1| = 0$ and so $q_0 = q_1$. From this it follows that $r_0 = r_1$ also.

Case 2: $(d < 0)$. In this case, apply Case 1 to the number "n" and "$-d$", and then multiply the q you get by -1. In more detail:

(Existence) By Case 1, there are $q', r' \in \mathbb{Z}$ such that $n = (-d)q' + r'$ and $0 \leq r' < |-d| = |d|$. Then for $q := -q'$ and $r := r'$ we have $n = dq + r$ and $0 \leq r \leq |d|$.

(Uniqueness) Suppose $q_0, q_1, r_0, r_1 \in \mathbb{Z}$ are such that $n = dq_0 + r_0$, $n = dq_1 + r_1$ and $0 \leq r_0, r_1 < |d|$. Then it is also the case that $n = (-d)(-q_0) + r_0$, $n = (-d)(-q_1) + r_1$ and $0 \leq r_0, r_1 < |d|$, so by the Uniqueness from Case 1, we conclude that $-q_0 = -q_1$ (so $q_0 = q_1$) and $r_0 = r_1$. □

We are now in a good position to provide a very sound definition for a concept you were already using as a young child (however going forward in life you should use this new definition!):

Definition 1.4.3. Suppose $n \in \mathbb{Z}$ is an integer. We say that n is **even** if there is $q \in \mathbb{Z}$ such that $n = 2q$ and we say that n is **odd** if there is $q \in \mathbb{Z}$ such that $n = 2q + 1$.

It follows from the Quotient-Remainder Theorem 1.4.2 that every integer n is either even or odd, but not both (why?).

The Well-Ordering Principle of $\mathbb{N}$ also gives us the following important *proof principle* (or *proof template*) about natural numbers:

Principle of Induction 1.4.4. *Suppose $P(n)$ is a property that a natural number n may or may not have. Suppose that*

(1) $P(0)$ holds (this is called the "base case for the induction"), and
(2) for every $n \in \mathbb{N}$, if $P(n)$ holds, then $P(n+1)$ holds (this is called the "inductive step").

Then $P(n)$ holds for every *natural number $n \in \mathbb{N}$.*

Proof. Define the set:

$$S \ := \ \big\{n \in \mathbb{N} : P(n) \text{ is false}\big\} \ \subseteq \ \mathbb{N}.$$

Assume towards a contradiction that $P(n)$ does not hold for every natural number $n \in \mathbb{N}$. Thus $S \neq \emptyset$. By the Well-Ordering Principle, the set S has a least element a. Since $P(0)$ holds by assumption, we know that $0 < a$ (so $a - 1 \in \mathbb{N}$). Since a is the least element of S, then the natural number $a - 1 \notin S$, so $P(a-1)$ holds. By assumption (2), this implies $P(a)$ holds, a contradiction. □

Warning 1.4.5. In part (2) of the Principle of Induction, it does *not* say you have to prove $P(n+1)$ is true outright. It says you have to prove that the following *implication* holds:

$$\big(P(n) \text{ is true}\big) \ \Longrightarrow \ \big(P(n+1) \text{ is true}\big)$$

Proving the implication is in general easier because you can use the assumption that $P(n)$ is true to help you prove that $P(n+1)$ is true. In other words, $P(n)$ is a precious gift you've been given, so don't squander it.

We now arrive at the very first example of a proof by induction. It is the canonical "first proof by induction that everybody should know" and it involves the so-called *triangular numbers*[4]:

Triangular Number Formula 1.4.6. *For every natural number $n \in \mathbb{N}$,*

$$0 + 1 + 2 + \cdots + n \ = \ \sum_{k=0}^{n} k \ = \ \frac{n(n+1)}{2} \ = \ \binom{n+1}{2}.$$

Proof. Let $P(n)$ be the assertion:

$$P(n): \quad \text{“}\textstyle\sum_{k=0}^{n} k = n(n+1)/2 \text{ is true.”}$$

We will show that $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

[4] https://en.wikipedia.org/wiki/Triangular_number

Base Case: First, we show that $P(0)$ holds outright. This is easy because $P(0)$ says "$0 = 0 \cdot 1/2$", which is obviously true.

Inductive Step: Next, we will suppose that for some $n \geq 0$ that $P(n)$ holds, and we will use it to prove that $P(n+1)$ also holds. Suppose $P(n)$ holds, i.e.,

$$\sum_{k=0}^{n} k \;=\; \frac{1}{2}n(n+1).$$

We must now show that $P(n+1)$ also holds. Note that:

$$\begin{aligned}\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1)\\ &= \frac{1}{2}n(n+1) + (n+1) \quad \text{since } P(n) \text{ is assumed to be true}\\ &= (n/2+1)(n+1)\\ &= \frac{1}{2}(n+2)(n+1)\\ &= \frac{1}{2}(n+1)\big((n+1)+1\big).\end{aligned}$$

Thus $P(n+1)$ holds as well. □

Notice how both "$n-1$" and "n" occurs in the statement of Pascal's Rule 1.3.6. This property makes Pascal's Rule useful in inductive proofs involving binomial coefficients, for instance, in the proof of the important *Binomial Theorem*:

Binomial Theorem 1.4.7. *Suppose $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$. Then*

$$(a+b)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Proof. The statement we will prove by induction is:

$$P(n): \quad \text{“For every } a, b \in \mathbb{R},\ (a+b)^n = \textstyle\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.\text{”}$$

Base Cases: First we will verify $P(0)$: $(a+b)^0 = 1 = \sum_{k=0}^{n} \binom{0}{k} a^{0-k} b^0$, thus $P(0)$ is true. For good measure (although not technically necessary), we will also verify $P(1)$ is true. Note that

$$\sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k \;=\; \binom{1}{0} a + \binom{1}{b} \;=\; a+b \;=\; (a+b)^1.$$

Inductive step: We assume that $P(n)$ is true for some $n \geq 1$ (this would have to be "for some $n \geq 0$" if we didn't do the base case $P(0)$ above). We will use this to prove that $P(n+1)$ is true. Note that

$$(a+b)^{n+1} \;=\; (a+b)(a+b)^n \;=\; (a+b)\left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k\right),$$

where the last equality uses the inductive assumption $P(n)$. Next, we distribute the $(a+b)$:

$$\begin{aligned}(a+b)\left(\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k\right) &= a\left(\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k\right)+b\left(\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k\right)\\ &=\sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1}\end{aligned}$$

Then we separate out the first term from the first sum and the last term from the second sum:

$$\sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1}$$

$$=a^{n+1}+\sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=0}^{n-1}\binom{n}{k}a^{n-k}b^{k+1}+b^{n+1}$$

Then we reindex the second sum so that it starts at $k=1$:

$$=a^{n+1}+\sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=1}^{n}\binom{n}{k-1}a^{n-k+1}b^k+b^{n+1}$$

Then we combine the two sums:

$$=a^{n+1}+\sum_{k=1}^{n}\left[\binom{n}{k}a^{n-k+1}b^k+\binom{n}{k-1}a^{n-k+1}b^k\right]+b^{n+1}$$

$$=a^{n+1}+\sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]a^{n-k+1}b^k+b^{n+1}$$

Then apply Pascal's Rule and also note that $\binom{n+1}{0}=\binom{n+1}{n+1}=0$:

$$=\binom{n+1}{0}a^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}a^{(n+1)-k}b^k+\binom{n+1}{n+1}b^{n+1}$$

Finally, reincorporate the first and last term into the summation:

$$=\sum_{k=0}^{n+1}\binom{n+1}{k}a^{(n+1)-k}b^k.$$

Thus we have shown $P(n+1)$ holds (see the first and last term in the sequence of equalities.) □

We also have the following variant of the Principle of Induction, which starts at some natural number (or integer!) other than 0:

Corollary 1.4.8 (Principle of Induction starting at N). *Let $N\in\mathbb{Z}$ and suppose $P(n)$ is a property that an integer $n\geq N$ may or may not have. Suppose that*

(1) $P(N)$ holds.
(2) for every $n\geq N$, if $P(n)$ holds, then $P(n+1)$ holds.

Then $P(n)$ holds for every integer $n\geq N$.

Proof. We will prove this by reducing it to the original Induction Principle by shifting. Let $Q(n)$ be the statement:

$$Q(n): \quad \text{“}P(n+N) \text{ holds.”}$$

Base Case: (1) implies that $Q(0)$ holds.

Inductive Step: Assume for some $n \geq 0$ that $Q(n)$ holds. We will use this to prove that $Q(n+1)$ holds. Since $Q(n)$ holds, this means that $P(n+N)$ holds. Since $n+N \geq N$, by assumption (2), we conclude that $P(n+N+1)$ holds. In other words, $Q(n+1)$ holds.

Thus $Q(n)$ is true for all $n \geq 1$ by the Principle of Induction. In other words, $P(n)$ is true for all $n \geq N$, which is what we wanted to prove. □

Sometimes, when proving $P(n+1)$ is true, it is not good enough to assume that only its immediate predecessor $P(n)$ is true. In such situations, the following variant of the Principle of Induction is useful:

Principle of Strong Induction 1.4.9. *Suppose $P(n)$ is a property that a natural number n may or may not have. Suppose that*

(1) $P(0)$ holds, and

(2) For every $n \geq 0$, if $P(k)$ holds for $k = 0, \ldots, n$, then $P(n+1)$ holds.

Then $P(n)$ holds for every natural number $n \in \mathbb{N}$.

Proof. The proof will follow from applying the (usual) Principle of Induction to a carefully chosen proposition. Specifically, for each $n \in \mathbb{N}$, let $Q(n)$ be the statement:

$$Q(n): \quad \text{“For each } k \in \{0, \ldots, n\},\ P(k) \text{ is true.”}$$

We will prove that $Q(n)$ is true for all $n \in \mathbb{N}$.

Base Case: By assumption (1), $P(0)$ holds. In other words, for all $k \in \{0\}$, $P(k)$ holds. This means that $Q(0)$ holds.

Inductive Step: Assume for some $n \in \mathbb{N}$ that $Q(n)$ holds. We want to show that $Q(n+1)$ holds. By definition of $Q(n)$, this means for every $k \in \{0, 1, \ldots, n\}$, $P(k)$ is true. By assumption (2), this implies that $P(n+1)$ is also true. Thus for $k \in \{0, 1, \ldots, n, n+1\}$, we have that $P(k)$ is true. This means that $Q(n+1)$ is true.

By the Principle of Induction, we conclude that $Q(n)$ is true for all $n \geq 0$. Since for each n, $Q(n)$ implies $P(n)$, we conclude that for every $n \geq 0$, $P(n)$ is true. □

Just like regular induction, strong induction can also start at another integer besides 0. Here is such an example of strong induction:

Example 1.4.10. Every natural number $n \geq 12$ is of the form $3x + 7y$ for some $x, y \in \mathbb{N}$.

Proof. For $n \geq 11$ we will consider the following statement:

$$P(n): \quad \text{“There exists } x, y \in \mathbb{N} \text{ such that } n = 3x + 7y\text{”}$$

Base Cases: We verify directly that $P(12)$, $P(13)$ and $P(14)$ are true. Indeed,

$$\begin{aligned} 12 &= 3 \cdot 4 + 7 \cdot 0 \quad (x = 4, y = 0) \\ 13 &= 3 \cdot 2 + 7 \cdot 1 \quad (x = 2, y = 1) \\ 14 &= 3 \cdot 0 + 7 \cdot 2 \quad (x = 0, y = 2) \end{aligned}$$

Inductive step: We will now assume that for some $n \geq 14$ and that $P(k)$ holds for $k \in \{12, 13, \ldots, n\}$. We now must show $P(n+1)$ is true. Since $n \geq 14$, $n-2 \geq 12$, so $P(n-2)$ holds by the inductive assumption. Thus we can take $x, y \in \mathbb{N}$ such that $n-2 = 3x + 7y$. Adding another "3" will give us the desired representation for $n+1$:

$$3(x+1) + y \;=\; 3x + y + 3 \;=\; n - 2 + 3 \;=\; n + 1.$$

By the Principle of Strong Induction 1.4.9, we conclude that $P(n)$ is true for every $n \geq 12$. □

1.5. Exercises

Exercise 1.5.1. The **Scheffer stroke** (or **nand**) (notation: $P|Q$) is the logical operator with the following truth table:

P	Q	$P\|Q$
T	T	F
T	F	T
F	T	T
F	F	T

Given propositions P and Q, show that each of the following propositions are logically equivalent to a proposition which uses *only* the Scheffer stroke $|$ (you might need to use multiple Scheffer strokes):

(1) $\neg P$
(2) $P \wedge Q$
(3) $P \vee Q$.

The **Peirce arrow** (or **nor**) (notation: $P \downarrow Q$) is the logical operator with the following truth table:

P	Q	$P \downarrow Q$
T	T	F
T	F	F
F	T	F
F	F	T

Given propositions P and Q, show that the following propositions are logically equivalent to a proposition which uses *only* the Peirce arrow $\downarrow$:

(4) $\neg P$
(5) $P \wedge Q$
(6) $P \vee Q$.

Exercise 1.5.2. Given propositions P, Q, and R, determine if the following propositions are tautologies, contradictions, or neither.

(1) $(P \leftrightarrow Q) \leftrightarrow ((P \wedge \neg Q) \vee (\neg P \wedge Q))$
(2) $(P \to Q) \vee (Q \to P)$
(3) $(\neg R \to ((P \vee Q) \to Q)) \vee R$
(4) $((P \to Q) \wedge (Q \to R)) \to (P \to R)$

Exercise 1.5.3. Recall that a proof is a finite sequence of logical steps. A natural question is "what counts as a logical step"? We won't answer this question in depth in this course, but at a basic level, there are three kinds of steps that can be written down in a proof:

- You can state any one of the premises of the proof
- You can state any tautology
- You can apply an *inference rule* to previous steps of the proof

We already know what all of these things are besides inference rules, which are what this question aims to introduce. The most basic example of an inference rule is called *Modus Ponens*: it says that if, at some point in a proof, we've deduced $P \to Q$ and P (where P and Q are some propositions), then we can also deduce Q. To see this inference rule in action, here is a formal proof in propositional logic:

Premises: $P \to Q$, $Q \to R$, and P

Step	Claim	Justification
1.	P	Premise
2.	$P \to Q$	Premise
3.	Q	Modus Ponens on steps 1 and 2
4.	$Q \to R$	Premise
5.	R	Modus Ponens on steps 3 and 4

Conclusion: R

Figure 1.7: A formal proof that $(P \to Q) \wedge (Q \to R) \wedge P \implies R$.

Inference rules are usually written in the following way:

$$\begin{array}{l} P \to Q \\ P \\ \hline Q \end{array}$$

Figure 1.8: The inference rule of Modus Ponens, written in standard form.

This just says that Modus Ponens is an inference rule which allows one to deduce "Q" whenever both "$P \to Q$" and "P" have already been deduced. One question we may have is "why is Modus Ponens a valid inference rule"? The answer is simply that $((P \to Q) \wedge P) \to Q$ is a tautology! In other words, if we've deduced $P \to Q$ and P, then it *must* be valid to conclude Q, regardless of the truth values of P and Q.

More generally, an inference rule

$$\begin{array}{c} A_1 \\ A_2 \\ \vdots \\ A_n \\ \hline B \end{array}$$

just says that $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ is a tautology. **Prove the following inference rules:**

(1) Modus Tollens:

$$\begin{array}{l} P \to Q \\ \neg Q \\ \hline \neg P \end{array}$$

(2) Hypothetical Syllogism:

$$\begin{array}{c} P \to Q \\ Q \to R \\ \hline P \to R \end{array}$$

(3) Conjuction:

$$\begin{array}{l} A \\ B \\ \hline A \wedge B \end{array}$$

Exercise 1.5.4. Given sets A and B, prove that the following two conditions are equivalent:

(1) $A \setminus B = B \setminus A$,
(2) $A = B$.

Exercise 1.5.5. Given sets X and Y, we define the **symmetric (set) difference** of X and Y (notation: $X \triangle Y$) to be the set $X \triangle Y := (X \cup Y) \setminus (X \cap Y)$. Do the following:

(1) Draw a Venn Diagram which illustrates the symmetric difference $X \triangle Y$ of X and Y.
(2) Prove that for any set X, $X \triangle X = \emptyset$.
(3) Prove that for any sets X and Y, $(X \cup Y) \setminus (X \triangle Y) = X \cap Y$.
(4) Prove that for any sets X, Y, and Z, $(X \triangle Y) \cap Z = (X \cap Z) \triangle (Y \cap Z)$.

Exercise 1.5.6. Prove the Ordered Pair Property: For every a, b, c, d,

$$(a, b) \; = \; (c, d) \quad \text{if and only if} \quad a = c \text{ and } b = d.$$

Exercise 1.5.7. Find the cardinalities of the following finite sets:

(1) $\{1, 2\} \cup \mathcal{P}(\{1, 2\})$
(2) $\{\{1\}, \{2\}\} \cup \mathcal{P}(\{1, 2\})$
(3) $\{0, 1, 2, 3\} \times \{\emptyset, \{0, 1, 2, 3\}\}$

Exercise 1.5.8. Prove the following fact by induction: for any natural number n,

$$\sum_{i=0}^{n} i^2 \; = \; \frac{n(n+1)(2n+1)}{6}.$$

Exercise 1.5.9. In this exercise we will prove the so-called *Hockey-Stick Identity*:

(1) Prove the following: For $0 \leq r \leq n$ we have

$$\sum_{i=r}^{n} \binom{i}{r} \; = \; \binom{n+1}{r+1}.$$

Hint: Fix $r \in \mathbb{N}$ and then do a proof by induction on n (so the base case will be $n = r$). Pascal's Rule might also be useful.

(2) Draw your own Pascal's Triangle with at least 8 rows and illustrate 3 instances of the Hockey-Stick Identity with $n - r \geq 2$.

Exercise 1.5.10. Let $f, g : \mathbb{R} \to \mathbb{R}$ be sufficiently nice functions (i.e., you can differentiate them as many times as you like). Recall the **product rule** from calculus:

$$D(fg) \; = \; fD(g) + D(f)g.$$

Let D^n denote taking the nth derivative. Prove the following analogue of the *Binomial Theorem* for derivatives: For every $n \geq 1$,

$$D^n(fg) \;=\; \sum_{k=0}^{n} \binom{n}{k} D^{n-k}(f) D^k(g).$$

Exercise 1.5.11. Use the Principle of Strong Induction to carefully prove the *Principle of Cauchy Induction*: Suppose $P(n)$ is a property that a natural number n may or may not have. Suppose that

(a) $P(2)$ holds,
(b) For every $n \geq 2$, if $P(n)$ holds, then $P(2n)$ holds, and
(c) For every $n \geq 3$, if $P(n)$ holds, then $P(n-1)$ holds.

Then $P(n)$ holds for every natural number $n \geq 2$.

Exercise 1.5.12. Let F_n be the sequence of **Fibonacci numbers**: $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all natural numbers n. For example, $F_2 = F_1 + F_0 = 1 + 0 = 1$ and $F_3 = F_2 + F_1 = 1 + 1 = 2$. Prove that

$$F_n \;=\; \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$$

for all natural numbers n, where

$$\alpha \;:=\; \frac{1+\sqrt{5}}{2}$$
$$\beta \;:=\; \frac{1-\sqrt{5}}{2}$$

Hint: Use strong induction. Notice that $\alpha + 1 = \alpha^2$ and $\beta + 1 = \beta^2$!

Exercise 1.5.13. The **Catalan numbers** C_n are defined by

$$C_n \;:=\; \frac{1}{n+1}\binom{2n}{n} \;=\; \frac{(2n)!}{n!(n+1)!}, \quad \text{for } n \in \mathbb{N},$$

forming a sequence $C_0 = 1, C_1 = 1, 2, 5, 14, 42, 132, \ldots$. For each $n \geq 1$ prove that

$$C_n \;=\; \frac{2(2n-1)}{n+1} C_{n-1}$$

Exercise 1.5.14. For each of the following pairs of integers $n, d \in \mathbb{Z}$ find the unique $q, r \in \mathbb{Z}$ such that $n = dq + r$ and $0 \leq r < |d|$:

(1) $n = 59$ and $d = 13$
(2) $n = 1188$ and $d = 385$
(3) $n = 832$ and $d = 10933$
(4) $n = 4131$ and $d = 2431$

Challenge: try to do the calculations by hand without a calculator!

Exercise 1.5.15. Use the Quotient-Remainder Theorem 1.4.2 to carefully prove the following:

(1) The square of any integer is either of the form $3k$ or $3k+1$ (i.e., prove that for every integer j there exists an integer k such that $j^2 = 3k$ or $j^2 = 3k+1$).
(2) The cube of any integer has one of the forms: $9k$, $9k+1$, or $9k+8$.

(3) Prove that $3k^2 - 1$ is never a perfect square (i.e., prove that for every integer j it is not the case that there exists an integer k such that $j^2 = 3k^2 - 1$).

Exercise 1.5.16. Use the Principle of Induction to prove the following for all $n \geq 1$:

$$\sum_{k=1}^{n} k \cdot k! \; = \; (n+1)! - 1.$$

Exercise 1.5.17. Use the Binomial Theorem to prove the following identities:

(1) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

(2) $\sum_{k=0}^{n} (-1)^n \binom{n}{k} = 0$

(3) $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$ [Hint: $n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$]

CHAPTER 2

Relations

2.1. Predicates and quantifiers

The primary role of propositional logic is to serve as a very robust backend for handling all the *boolean* logic which shows up (i.e., it tells us how to deal with *and*, *or*, *not*). However, propositional logic by itself is too crude of a language to really do or say anything useful about the mathematical structures we (will) care about. Indeed, it would be more natural and useful to work in a language which can also handle the following things:

quantifiers *variables* *relations* *functions* *predicates*

We will now give a brief introduction to the type of logic which can express these things (so-called *first-order logic*).

Definition 2.1.1. A **predicate** (or **propositional function**) is a statement $P(x)$ where x is a variable ranging over a set D (D is called the **domain of discourse**) such that for each specific $d \in D$, the statement $P(d)$ is a proposition (i.e., it is either true or false).

Example 2.1.2. Consider the predicate

$$P(x): \quad \text{“}x\text{ is a prime number”}$$

where x ranges over its domain of discourse $\mathbb{N}$. Then for each $k \in \mathbb{N}$, $P(k)$ is either true or false, for instance: $P(2), P(3), P(5)$ are true, whereas $P(1), P(4), P(6)$ are false. Note that it doesn't make sense to ask what the truth value of the predicate “$P(x)$” is since it has a free variable x. The predicate only obtains a definitive truth value once we plug a specific number in for x.

We can (and will) also talk about predicates $P(x_1, \dots, x_n)$ with multiple free variables, with each having its own domain of discourse (which could all be the same set, or not).

Definition 2.1.3. Suppose $P(x)$ is a predicate with domain of discourse D.

(1) The statement

$$\text{“for all } x,\ P(x)\text{”} \qquad (\text{notation: } \forall x P(x))$$

is a proposition which is true precisely when for each $d \in D$, the individual proposition $P(d)$ is true. This is called a **universally quantified statement** and the symbol $\forall$ is called a **universal quantifier**.

(2) The statement

$$\text{“there exists } x \text{ such that } P(x)\text{”} \qquad (\text{notation: } \exists x P(x))$$

is a proposition which is true precisely when there is at least one $d \in D$ such that $P(d)$ is a true proposition. This is called a **existentially quantified statement** and the symbol $\exists$ is called a **existential quantifier**.

Proving an existential statement is in general a *finding problem.* For example:

Example 2.1.4. The following proposition with domain of discourse $\mathbb{C}$ (the set of all *complex* numbers) is true:

$$\exists x\ (x^2 - 2x + 2 = 0)$$

This is because we observe that for the specific complex number $z := 1 + i$, we get an equality $z^2 - 2z + 2 = 0$ (so $P(1 + i)$ is true where $P(x)$ is the predicate "$x^2 - 2x + 2 = 0$"). How did we actually find the above number $1 + i$? For that we used actual math (the quadratic formula, for instance). Note that the domain of discourse also plays an important role in determining the truth value of the proposition. For instance, if our domain of discourse were instead $\mathbb{R}$, then the above proposition would be false since the polynomial $x^2 - 2x + 2$ does not have any real roots.

We are now in a position to give a very vague definition of *first-order logic*:

Informal Definition 2.1.5. The language of first-order logic consists of all statements which can be built up from:

- "simple[1] predicates" involving one or more free variables,
- the logical operators $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$ from Section 1.1, and
- quantifiers $\forall$ and $\exists$ quantifying over free variables.

Nearly all mathematical statements we have encountered so far can be converted into a first-order logic statement. As a general rule, we will continue to write mathematical statements as clear English sentences, however, we will often also choose to spell out our statements as a first-order logic statement in order to make clear what the precise logical structure of the statement is. For instance, the first part of the Quotient-Remainder Theorem says:

"Suppose $d, n \in \mathbb{Z}$ and $d \neq 0$.

Then there exists $q, r \in \mathbb{Z}$ such that $n = dq + r$ and $0 \leq r < |d|$."

We could write this in first-order logic as:

$$\forall d \forall n \big(d \neq 0 \rightarrow \exists q \exists r (n = dq + r \wedge 0 \leq r < |d|)\big)$$

where all domains of discourse are $\mathbb{Z}$, or even as

$$\forall d \neq 0 \forall n \exists q \exists r (n = dq + r \wedge 0 \leq r < |d|)$$

where the domain of discourse for d is $\{k \in \mathbb{Z} : k \neq 0\}$ and the domains of discourse for n, q, r are all $\mathbb{Z}$.

Just as in propositional logic, we also have a notion of *logical equivalence* in first-order logic:

[1] We won't define this term, but it includes statements like "x is prime" or "$x^2 - 2x + 2 = 0$".

Informal Definition 2.1.6. Given two propositions P and Q in first-order logic, we say that P and Q are **logically equivalent** (notation: $P \equiv Q$) if for all possible choices of domains of discourse, P and Q will always have the same truth value. In other words, $P \equiv Q$ means that P and Q are logically indistinguishable under any possible interpretation.

Logical equivalences in propositional logic naturally give rise to logical equivalences in this setting, for instance:

$$\forall x\big(P(x) \to Q(x)\big) \;\equiv\; \forall x\big(\neg P(x) \vee Q(x)\big)$$

The following logical equivalences are essential when dealing with negating statements with quantifiers:

Fact 2.1.7. Suppose $P(x)$ is a predicate. The following logical equivalences show you how to negate a quantifier:

(1) $\neg\forall x P(x) \equiv \exists x\big(\neg P(x)\big)$,
(2) $\neg\exists x P(x) \equiv \forall x\big(\neg P(x)\big)$.

In other words, to move a negation sign past a quantifier, you have to switch the quantifier type.

Example 2.1.8. Recall that $A \subseteq B$ means

$$\forall x(x \in A \to x \in B)$$

where the domain of discourse is some universal set U. What $A \not\subseteq B$ (read "A is not a subset of B") mean? By negating and applying logical equivalences, we see that

$$\begin{aligned}
\neg\forall x(x \in A \to x \in B) \;&\equiv\; \exists x\neg(x \in A \to x \in B)\\
&\equiv\; \exists x\neg\big(\neg(x \in A) \vee x \in B\big) \quad \text{(by Example 1.1.11)}\\
&\equiv\; \exists x\big(\neg\neg(x \in A) \wedge \neg(x \in B)\big) \quad \text{(by De Morgan's Law)}\\
&\equiv\; \exists x\big(x \in A \wedge x \notin B\big).
\end{aligned}$$

In other words, $A \not\subseteq B$ means there exists at least one x such that $x \in A$ and $x \notin B$. This is the formal justification for the second answer we gave to Question 1.2.3.

We end this section with a friendly warning:

You can't switch the order of quantifiers of different type.

Consider the following proposition with domain of discourse $\mathbb{R}$:

$$\forall x\exists y\ (x = y)$$

This is clearly a true proposition since we can just take $y := x$ in a proof. However, the proposition

$$\exists y\forall x\ (x = y)$$

is clearly false since otherwise there would be a real number $y \in \mathbb{R}$ which is equal to all other real numbers, which can't happen since $\mathbb{R}$ has at least two elements in it. Occasionally you will encounter situations where the quantifiers can be switched, but this type of coincidence would only happen for some special mathematical reason. You can, however, always switch quantifiers of the same type, provided they are next to each other, for instance:

$$\forall x\forall y P(x,y) \;\equiv\; \forall y\forall x P(x,y) \quad\text{and}\quad \exists x\exists y Q(x,y) \;\equiv\; \exists y\exists x Q(x,y)$$

2.2. Relations

The mathematical structures we will deal with usually have more structure on it beyond the underlying set. For instance, we know that when we talk about the set $\mathbb{R}$, we also want to be able to talk about the linear order $\leq$ and the usual arithmetic binary functions $+$ and $\cdot$. If we didn't have these notions available to us, then there wouldn't be anything that special about the set $\mathbb{R}$ except that it's a very very large set. The formal way to make things like this is through *relations*.

Definition 2.2.1. Given sets X and Y, we define a **(binary) relation on** $X \times Y$ (or a **(binary) relation from** X **to** Y) to be a subset $R \subseteq X \times Y$. If R is a relation on $X \times Y$, then for an ordered pair $(x, y) \in X \times Y$ we will often write

$$\begin{aligned} &xRy \quad \text{instead of } (x,y) \in R, \text{ and} \\ &x\not{R}y \quad \text{instead of } (x,y) \notin R. \end{aligned}$$

(Note: xRy is pronounced "x is related to y (by R)"; and $x\not{R}y$ is pronounced "x is not related to y (by R)")

Remark 2.2.2. The word *binary* in Definition 2.2.1 refers to the fact that R is a relation on a cartesian product on *two* sets: X and Y. One can also define *ternary relations* on $X \times Y \times Z$ and every *n-ary relations* on $X_1 \times X_2 \times \cdots \times X_n$. In this class we will (for the most part) restrict our attention to binary relations.

Example 2.2.3. Consider $X := \{1, 2, 3, 4\}$ and $Y := \{a, b, c\}$ and the binary relation R on $X \times Y$ given by:

$$R = \big\{(1,a), (1,b), (2,a), (4,b), (4,c)\big\}$$

The relation R tells us, among other things, $1Ra$ but $3\not{R}y$ for every $y \in R$. We can picture all the relations specified by R with the following **arrow diagram**:

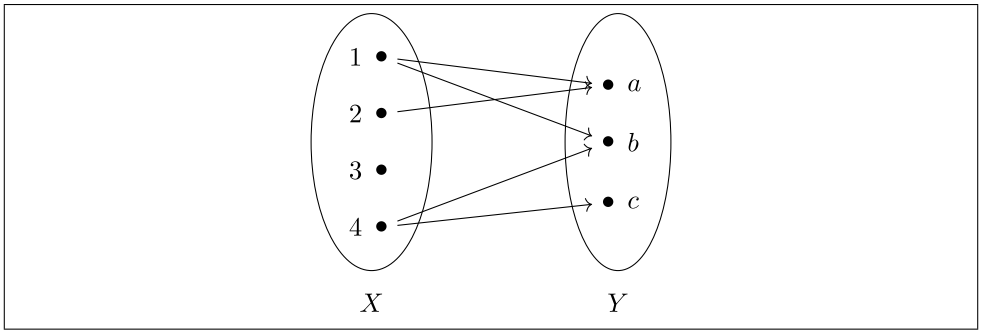

Figure 2.1: Arrow diagram from X to Y illustrating the relation R on $X \times Y$

We can also represent the relation R with the following **relation matrix**:

$$\begin{array}{c c} & \begin{array}{ccc} a & b & c \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \end{array}$$

The relation matrix is constructed by labelling the rows with the elements of X, labelling the columns with the elements of Y, and for each $x \in X$ and $y \in Y$, the entry of the matrix corresponding to (x, y) is 1 iff xRy and is 0 otherwise.

In the rest of this chapter we will study specific examples of relations.

2.3. Partial and total order relations

Many common relations have the property that the two sets X and Y are actually the same. In this case, we use the following terminology:

Definition 2.3.1. Given a set X, we say that R is a **relation on** X if $R \subseteq X \times X$ is a binary relation on $X \times X$ (i.e., a relation on $X \times Y$ as defined in the previous section, except that $X = Y$ is the same set).

Example 2.3.2. Suppose $X = \{a, b, c, d, e\}$ and R is a relation on X given by

$$R \ := \ \big\{(a,b),(b,a),(e,a),(e,c),(d,e),(d,d)\big\}.$$

In this situation, instead of representing R as an arrow diagram from X to X, since both the first set and the second set are the same set, we can represent R as a **directed graph** (or **digraph**) on X:

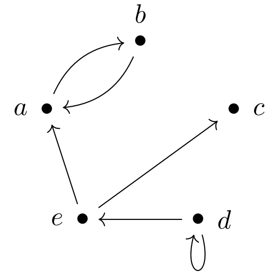

Figure 2.2: Digraph representing the relation R

We draw special attention to the following properties which a relation R on a set X may or may not enjoy:

Definition 2.3.3. Suppose R is a relation on X. We say that the relation R is

(1) **reflexive** if for every $x \in X$, $(x,x) \in R$:

$$\forall x \in X,\ xRx$$

(2) **antireflexive** if for every $x \in X$, $(x,x) \notin R$:

$$\forall x \in X,\ \neg(xRx)$$

(3) **symmetric** if for every $x, y \in X$, if $(x,y) \in R$, then $(y,x) \in R$:

$$\forall x \in X\ \forall y \in X,\ (xRy \to yRx)$$

(4) **antisymmetric** if for all $x, y \in X$, if $(x,y) \in R$ and $(y,x) \in R$, then $x = y$:

$$\forall x \in X\ \forall y \in X,\ (xRy \wedge yRx \to x = y)$$

(5) **transitive** if for all $x, y, z \in X$, if $(x,y) \in R$ and $(y,z) \in R$, then $(x,z) \in R$:

$$\forall x \in X\ \forall y \in X\ \forall z \in X,\ (xRy \wedge yRz \to xRz)$$

Note that in general, "antisymmetric" is not the negation of "symmetric"; same with "antireflexive" and "reflexive".

Definition 2.3.4. We say a relation R on X is a **partial order** if R is reflexive, antisymmetric, and transitive.

We interpret a partial ordering on X as a *comparing notion.* It is useful for encoding *hierarchical* structure, for example:

Example 2.3.5. Given a set X, the subset relation $\subseteq$ on the powerset $\mathcal{P}(X)$ of X is a partial order on $\mathcal{P}(X)$.

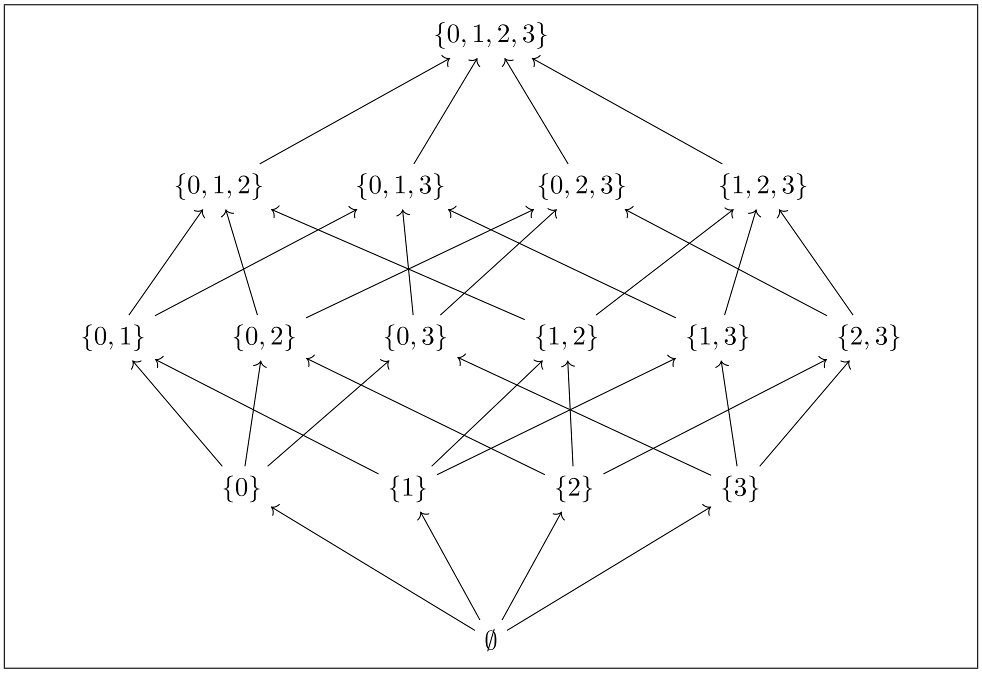

Figure 2.3: Partial digraph of the $\subseteq$ relation on $\mathcal{P}\big(\{0,1,2,3\}\big)$ (with self-loops and transitive arrows omitted)

One of the features of the subset relation $\subseteq$ on $\mathcal{P}\big(\{0,1,2,3\}\big)$ in the above example is that certain sets are unrelated to each other. For instance, $\{0,1\} \not\subseteq \{2,3\}$ and $\{2,3\} \not\subseteq \{0,1\}$, i.e., the sets $\{0,1\}$ and $\{1,2\}$ are *incomparable* with respect to the subset relation. We are also interested in partial orders where every pair of elements are related by the relation. First, some definitions:

Definition 2.3.6. Suppose R is a partial order on a set X. Given elements $x, y \in X$, we say they are

(1) **comparable** if xRy or yRx, and
(2) **incomparable** if $x \not R y$ and $y \not R x$.

We say that the partial order R on X is a **total order** (or **linear order**) if all pairs of elements are comparable, i.e., if R also satisfies:

(3) (**totality**) for every $x, y \in X$, either xRy or yRx:

$$\forall x \in X \ \forall y \in X, \ (xRy \vee yRx)$$

Example 2.3.7. The first and most important example of a total order is the usual "less than or equal" relation "$\leq$" on $\mathbb{R}$. This relation also restricts to a total order on $\mathbb{Q}, \mathbb{Z}, \mathbb{N}$ and really any subset of $\mathbb{R}$. In Figure 2.4 below we sketch the partial diagraph corresponding to the $\leq$ relation on $\mathbb{N}$. Since we know that $\leq$ is reflexive we chose to omit the self-loops on each number for the sake of clarity.

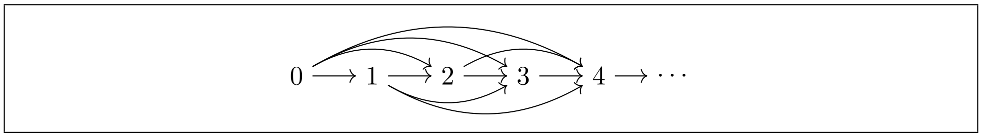

Figure 2.4: Partial digraph of the $\leq$ relation on $\mathbb{N}$ (with self-loops omitted)

Convention 2.3.8. If we refer to an object $(X; R)$ as a **partial order**, we mean that X is a set and $R \subseteq X \times X$ is a partial order on X. Likewise, if we refer to an object $(L; \leq)$ as a **linear order**, we mean that L is a set and $\leq$ is a total/linear order on L.

2.4. The *divides* relation

In this section we introduce the *divides* relation, an important and fundamental relation in number theory and arithmetic:

Definition 2.4.1. Suppose $d, n \in \mathbb{Z}$. We say that d **divides** n (notation: $d|n$) if there exists $q \in \mathbb{Z}$ such that $dq = n$; in symbols:

$$d|n \;:\Longleftrightarrow\; \exists q \in \mathbb{Z}\ (d \cdot q = n)$$

If $d|n$ and $q \in \mathbb{Z}$ is such that $dq = n$, then we shall call d a **divisor** (or **factor**) of n, and we shall call q the **quotient** of n divided by d. We shall construe $|$ as a relation on $\mathbb{Z}$, i.e., "$| \subseteq \mathbb{Z} \times \mathbb{Z}$".

In Figure 2.5 below, we illustrate how the digraph of the divides relation $|$ looks on the set $\mathbb{N}$. Since the divides relation is reflexive and transitive, for the sake of clarity we chose to omit all self-loops from the picture and any arrows resulting from applying transitivity to other arrows. We are now in a position to define one of the most important notions in all of mathematics:

Definition 2.4.2. A natural number $p \in \mathbb{N}$ is called a **prime number** if $p \neq 1$ and its only nonnegative divisors are 1 and p; in symbols:

$$p \text{ prime } :\Longleftrightarrow\; p \neq 1 \wedge \forall d \in \mathbb{N}(d|p \to d = 1 \vee d = p)$$

A natural number $n \geq 2$ which is not prime is called **composite**.

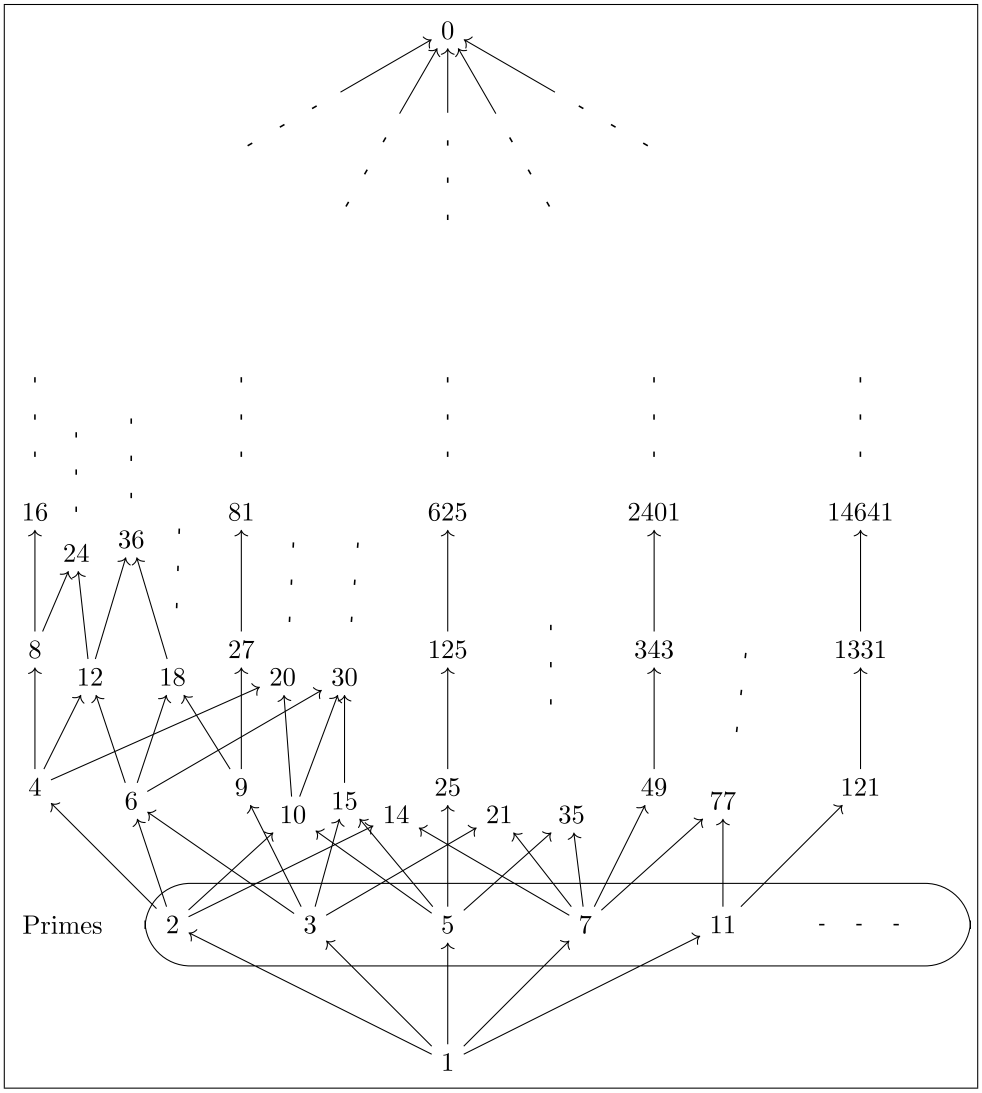

Figure 2.5: Partial digraph of the *divides* relation $|$ on $\mathbb{N}$ (with self-loops and transitive arrows omitted)

In order to prove that one number divides another number, you have to explicitly "find the q".

Example 2.4.3. $42|546$, i.e., 42 divides 546.

Proof. By the definition of "$d|n$", we have to show that there exists $q \in \mathbb{Z}$ such that $42q = 546$. We claim that $q := 13$ works. Indeed:

$$42q \;=\; 42 \cdot 13 \;=\; 546. \qquad \square$$

Officially speaking, we are under no obligation to show *how* we arrived at $q := 13$. Clearly the above proof shows that 42 does indeed divide 546. In the case where d does not divide n, a good strategy to rigorously prove this is to apply the Quotient-Remainder Theorem to n and d and then observe $r \neq 0$ (see next proof).

Example 2.4.4. $42 \nmid 547$, i.e., 42 does not divide 547.

PROOF. Note that for $q_1 := 13$ and $r_1 := 1$ we have

$$547 \ = \ 42 \cdot \underbrace{13}_{q_1} + \underbrace{1}_{r_1} \quad \text{and } 0 \leq r_1 = 1 < 42.$$

Suppose towards a contradiction that $42|547$, i.e., there is $q_2 \in \mathbb{Z}$ such that $42q_2 = 547$. Then for this q_2 and $r_2 := 0$ we would have

$$547 \ = \ 42 \cdot q_2 \ = \ 42 \cdot q_2 + \underbrace{0}_{r_2} \quad \text{and } 0 \leq r_2 = 0 < 42.$$

By the *uniqueness* part of the Quotient-Remainder Theorem 1.4.2(2), we conclude that $r_1 = r_2$, i.e., $1 = 0$, a contradiction. Thus $42 \nmid 547$. □

Clearly *divisibility* is a fundamental arithmetic relation we should (and do!) care about. Indeed, you implicitly use it all the time whenever you are mentally simplifying fractions. Consequently, it makes sense to establish a robust arsenal of useful properties about divisibility which we can just use anytime in the future without having to reprove them every time. Here it is:

Divisibility Properties 2.4.5. *For every $a, b, c \in \mathbb{Z}$ the following hold:*

(D1) $a|0$, $1|a$, $a|a$
(D2) $a|1$ *if and only if* $a = \pm 1$
(D3) *if* $a|b$ *and* $c|d$*, then* $ac|bd$
(D4) *if* $a|b$ *and* $b|c$*, then* $a|c$
(D5) $a|b$ *and* $b|a$ *if and only if* $a = \pm b$
(D6) *if* $a|b$ *and* $b \neq 0$*, then* $|a| \leq |b|$
(D7) *if* $a|b$ *and* $a|c$*, then for every* $x, y \in \mathbb{Z}$*,* $a|(bx + cy)$

In particular, the divides relation $|$ is reflexive (D1) and transitive (D4).

PROOF. The general strategy for proving these properties is to rewrite what you need to prove in terms of the *definition* of divides $|$. We provide a few examples and leave the rest as an exercise for the reader.

(D3) Assume that $a|b$ and $c|d$. By definition of the divides relation, this means there exists integers $q_0, q_1 \in \mathbb{Z}$ such that $aq_0 = b$ and $cq_1 = d$. Multiplying these equalities together yields:

$$bd \ = \ (aq_0)(cq_1) \ = \ (ac)(\underbrace{q_0 q_1}_{=:q}) \ = \ (ac)q$$

so we see that for the integer $q := q_0 q_1$ we have $bd = (ac) \cdot q$. Thus $ac|bd$, by definition of the divides relation.

(D7) Assume $a|b$ and $a|c$. By definition of the divides relation, this means there exists $q_0, q_1 \in \mathbb{Z}$ such that $b = aq_0$ and $c = aq_1$. Then for the integer $q := q_0 x + q_1 y$, we see that

$$bx + cy \ = \ aq_0 x + aq_1 y \ = \ a(q_0 x + q_1 y) \ = \ aq,$$

and so $a|bx + cy$ by definition of the divides relation. □

We would like to think of $|$ as a partial order, however (D5) shows that this is not the case. Indeed, $2|-2$ (because $2 \cdot (-1) = -2$) and $-2|2$ (because $(-2) \cdot (-1) = 2$), but $2 \neq -2$. However, if we restrict out attention to only considering nonnegative numbers, then this natural restriction of $|$ *is* a partial order.

Corollary 2.4.6. *The restriction of $|$ to the natural numbers, i.e., the relation on $\mathbb{N} \times \mathbb{N}$ defined by*

$$d|n \;:\Longleftrightarrow \textit{ there exists } q \in \mathbb{Z} \textit{ such that } dq = n$$

for $d, n \in \mathbb{N}$, is a partial order on $\mathbb{N}$.

(Note that if $d, n \in \mathbb{N}$ and $d|n$, then if $n = 0$, then $d \cdot 0 = n$ and if $n > 0$, then if $dq = n$ for some $q \in \mathbb{Z}$, then necessarily $q > 0$ since $d \geq 0$. Thus in either case, if $d|n$, then a "q" as in the definition of "$d|n$" can already be found in $\mathbb{N}$; not that it matters for the veracity of the corollary.)

Proof. Reflexivity is part of (D1), transitivity is (D4), and antisymmetry follows from (D5) since we are restricting to $\mathbb{N}$. □

We are now in a position to prove the following theorem by Euclid (c. 300 BCE) that there exists infinitely many prime numbers. This is another "very famous proof everyone should know".

Euclid's Theorem 2.4.7. *There exists infinitely many prime numbers.*

Proof. Let $\mathbb{P} := \{p \in \mathbb{N} : p \text{ prime}\}$ be the set of all prime numbers. It will be sufficient[2] to prove the following statement for every $n \geq 1$ by induction on $n \geq 1$:

$$P(n): \quad \text{"}\mathbb{P} \text{ has at least } n \text{ distinct elements in it (i.e., the cardinality } |\mathbb{P}| \text{ of } \mathbb{P} \text{ is } \geq n)\text{."}$$

Base Case: 2 is a prime number, so $2 \in \mathbb{P}$ which implies $|\mathbb{P}| \geq 1$. Thus $P(1)$ is true.

Induction Step: Suppose for some $n \geq 1$ that $P(n)$ is true. This means the set $\mathbb{P}$ contains at least n distinct primes. Let $p_1, \ldots, p_n$ be n distinct prime numbers (it doesn't matter what they are, $P(n)$ just assures us that they exist). We will show there must be another prime number which is not in this list already. Consider the positive integer

$$M \;:=\; p_1 \cdots p_n + 1.$$

By Exercise 2.8.7 there exists a prime number $p \in \mathbb{P}$ such that $p|M$. Since $p \nmid 1$, it follows from (D7) that $p \nmid M - 1$. However, for each $i \in \{1, \ldots, n\}$, we have $p_i | M - 1 = p_1 \cdots p_n$. Thus $p \neq p_i$. In particular, $|\{p_1, \ldots, p_n, p\}| = n + 1$, so $|\mathbb{P}| \geq n + 1$. Hence $P(n + 1)$ is proved. □

2.5. Equivalence relations and partitions

One of the amazing insights that permeates all of modern mathematics is the idea of relaxing the very strict and draconian relation of "equals" (i.e., being the same in every single possible way) to a relation of "equivalence" (i.e., being the same in only the ways we care about). For example, suppose you were deriving some rules about how the evenness/oddness of an integer gets affected by the usual arithmetic operations + and ×. You would probably come up with the following:

odd+odd=even   even+even=even   even+odd=odd

[2] We don't have a formal definition of what it means for a set to be *infinite*. However, knowing that the claim $P(n)$ is true for all $n \geq 1$ should at least convince you that the set is not finite (if it were finite, then it would have a fixed cardinality $n_0 \in \mathbb{N}$, but then $P(n_0 + 1)$ being true would contradict that).

$$\textit{odd}\times \textit{odd}=\textit{odd} \quad \textit{even}\times \textit{even}=\textit{even} \quad \textit{even}\times \textit{odd}=\textit{even}$$

You would probably discover in the course of your investigation that the *only thing* that matters about a number n in this context is whether $r = 0$ or 1, where $n = 2q + r$ is the result of applying the Quotient-Remainder Theorem 1.4.2 to n with $d = 2$. All other information (for instance, the precise value of q) is irrelevant in this context. The notion of *equivalence relation* gives us a way of making this feeling rigorous.

Definition 2.5.1. We say a relation E on X is a **equivalence relation** if E is reflexive, symmetric, and transitive. Recall this means:

(1) (reflexive) $\forall x\ (xEx)$
(2) (symmetric) $\forall x \forall y\ (xEy \to yEx)$
(3) (transitive) $\forall x \forall y \forall z\ (xEy \wedge yEz \to xEz)$

where the domain of discourse is X.

Example 2.5.2. (1) Given a set X, we can construe "=" as an equivalence relation on X in the obvious way, i.e.,

$$= := \big\{(x,x) : x \in X\big\} \ \subseteq\ X \times X.$$

(2) Given a set X, define the **trivial equivalence relation on** X to be the relation $E := X \times X$, i.e., for every $x, y \in X$, xEy. Then E is a (not particularly useful) equivalence relation with a single equivalence class.

(3) Let $X := \{a, b, c, d, e, f\}$. The following relation E on X is an equivalence relation:

$$E \ := \ \big\{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),$$

$$(a,b),(b,a),(a,c),(c,a),(b,c),(c,b),(d,e),(e,d)\big\}$$

E has the following digraph:

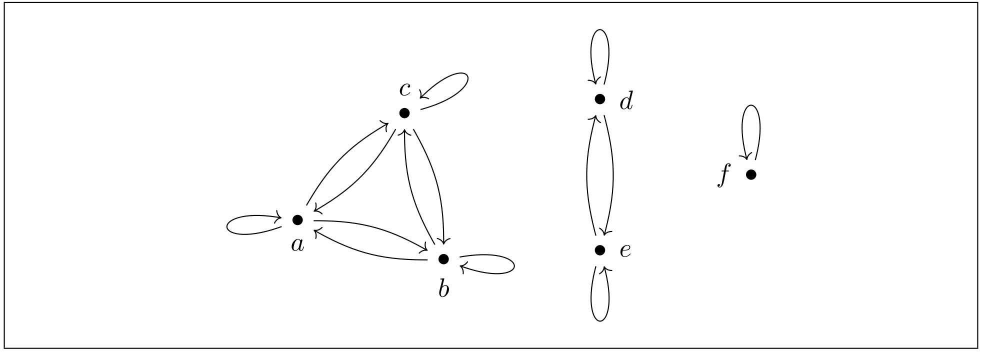

Figure 2.6: Digraph of the equivalence relation E on X

In general, equivalence relations are most useful when they are nontrivial and not the *equals* relation (although these are still perfectly valid examples of equivalence relations). Given an equivalence relation E on a set X, there is a natural construction which allows us to replace E with actual equality =, at the cost of modifying the objects we are talking about:

Definition 2.5.3. Suppose E is an equivalence relation on a set X. For each $a \in X$, define the **equivalence class** of a (with respect to E) to be

$$[a] \ = \ [a]_E \ := \ \{x \in X : xEa\}.$$

In other words, $[a]$ is the set of all things in X which E thinks is equivalent to a. Define the **quotient of** X **by** E (notation: X/E, read: "X mod E") to be the set

$$X/E \ := \ \big\{[a] : a \in X\big\}$$

There is a correspondence between partitions of a set X and equivalence relations on a set X. The following makes this clear:

Fact 2.5.4. Suppose E is an equivalence relation on a set X. Then

(1) X/E is a partition of X,

(2) if $\mathcal{S} \subseteq \mathcal{P}(X)$ is a partition of X, then the relation $E_{\mathcal{S}}$ on X defined by:

$$xE_{\mathcal{S}}y \ :\Longleftrightarrow \ \text{there exists } A \in \mathcal{S} \text{ such that } x \in A \text{ and } y \in A$$

is an equivalence relation on X and $X/E_{\mathcal{S}} = \mathcal{S}$,

(3) for every $x, y \in X$, xEy if and only if $[x] = [y]$.

Proof. (1) and (2) is Exercise 2.8.8. For (3) suppose $x, y \in X$ are arbitrary. If xEy, by definition of $[y]$ we have $x \in [y]$. Thus $x \in [x] \cap [y] \neq \emptyset$ is nonempty. Since X/E is a partition, it must be the case that $[x] = [y]$. Conversely, suppose $[x] = [y]$. Then $x \in [x] = [y]$ and so xEy. □

In other words, an equivalence relation partitions the set X into disjoint equivalence classes. The set X/E is basically the set X where we collapse each equivalence class into a single element. When studying the equivalence relation E, we can either use "E" and talk about "X", or use "=" and talk about X/E. Using both points of view and the interplay between them can be very fruitful.

Example 2.5.5. Let X and E be from Example 2.5.2(3). Then the partition X/E is the following set:

$$X/E \ = \ \big\{\{a, b, c\}, \{d, e\}, \{f\}\big\}$$

which we illustrate in Figure 2.7 below.

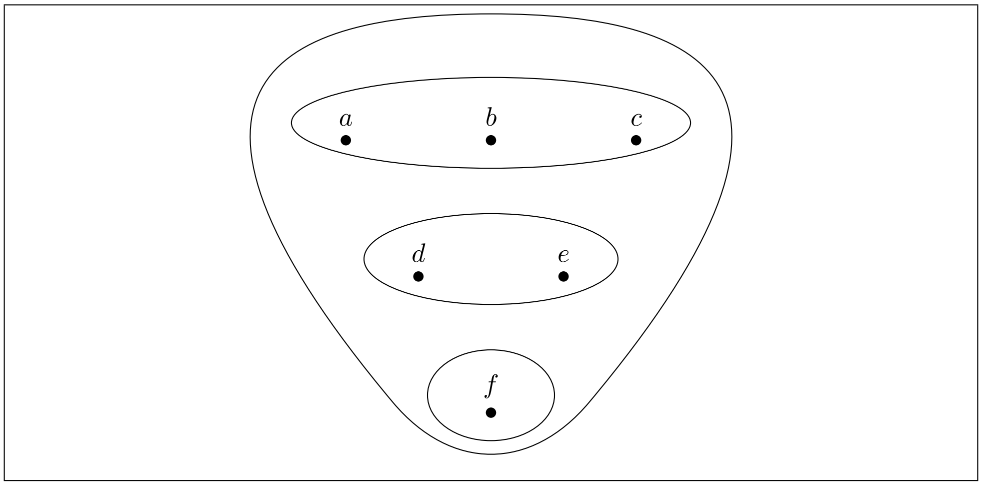

Figure 2.7: Partition X/E of X

2.6. The *mod* n congruence (equivalence) relation

In this section, fix a positive integer $n \geq 1$. We will define one of the most fundamental examples of an equivalence relation in all of mathematics. At its core its based on the divisibility relation:

Definition 2.6.1. We say that two integers $a, b \in \mathbb{Z}$ are **congruent modulo** n (notation: $a \equiv b \pmod{n}$) if $n | a - b$, i.e.,

$$\begin{aligned} a \equiv b \pmod{n} \ &:\Longleftrightarrow \ n | a - b \\ &\Longleftrightarrow \ \text{there exists } q \in \mathbb{Z} \text{ such that } nq = a - b \end{aligned}$$

We shall construe *congruence mod(ulo)* n as a binary relation on $\mathbb{Z} \times \mathbb{Z}$ in the natural way, i.e., the pair (a, b) is in the relation iff $a \equiv b \pmod{n}$.

Remark 2.6.2. Note that the n in the definition of *congruence modulo* n is fixed. In other words, we are actually defining infinitely many equivalence relations – one for each $n \geq 1$.

Example 2.6.3. (1) Suppose $n := 2$. Then for $k \in \mathbb{Z}$, we have either $k = 2q$ or $k = 2q + 1$, so either $2|k - 0$ or $2|k - 1$. Thus either $k \equiv 0 \pmod{2}$ or $k \equiv 1 \pmod{2}$ depending on whether k is even or odd. Thus congruence mod 2 captures the *evenness/oddness* of the numbers.

(2) Let's consider the case where $n := 1$. Suppose $a, b \in \mathbb{Z}$. Then $1 \cdot (a - b) = a - b$, so with $q := a - b$ we see that $1|a - b$ and thus $a \equiv b \pmod{1}$. Thus, congruence mod 1 is the trivial equivalence relation on $\mathbb{Z}^2$. Consequently, we will restrict our attention to congruence mod n where $n \geq 2$.

Congruence Properties 2.6.4. *Fix* $n \geq 1$. *Then for every* $a, b, c, d \in \mathbb{Z}$ *the following hold:*

(C1) $a \equiv a \pmod{n}$
(C2) *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$
(C3) *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$
(C4) *if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$
(C5) *if* $a \equiv b \pmod{n}$, *then* $a^m \equiv b^m \pmod{n}$ *for every* $m \in \mathbb{N}$.

Proof. The general strategy for proving things about $\equiv$ is to rewrite what you are doing in terms of the divides relation $|$ (i.e., in terms of the definition of $\equiv$), and then if necessary rewrite what you are doing in terms of the definition of divides. We prove (C4) like this and leave the rest as an exercise for the reader (for (C5) use induction on $m \in \mathbb{N}$).

(C4) Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By definition, this means that $n|a - b$ and $n|c - d$. By (D7) (with $x = y = 1$), we have

$$n|(a - b) + (c - d)$$

which we can rewrite as

$$n|(a + c) - (b + d).$$

We conclude that $a + c \equiv b + d \pmod{n}$, by definition of $\equiv$. For the second part, applying the definition of divides we get integers $q_0, q_1 \in \mathbb{Z}$ such that $nq_0 = a - b$ and $nq_1 = c - d$, i.e., $a = b + nq_0$ and $c = d + nq_1$. Note that

$$ac \ = \ (b + nq_0)(d + nq_1) \ = \ bd + (bq_1 + dq_0 + q_0q_1n)n$$

which we rewrite as

$$ac - bd \;=\; \underbrace{(bq_1 + dq_0 + q_0q_1n)}_{\text{an integer}}\, n$$

which implies $n|ac{-}bd$, by definition of divides. We conclude that $ac \equiv bd \pmod{n}$, by definition of $\equiv$. □

It follows from (C1), (C2), and (C3) that (for a fixed $n \geq 1$) congruence is an equivalence relation:

Corollary 2.6.5. *For fixed $n \geq 1$, the relation "$a \equiv b \pmod{n}$" is an equivalence relation on $\mathbb{Z}$.*

We conclude this section with an example which shows what the quotient of $\mathbb{Z}$ with a congruence relation looks like.

Example 2.6.6. Suppose $n = 5$. Then the equivalence relation $x \equiv y \pmod{5}$ partitions $\mathbb{Z}$ into five distinct equivalence classes: [0], [1], [2], [3], and [4]. We illustrate these five equivalence classes in Figure 2.8 below.

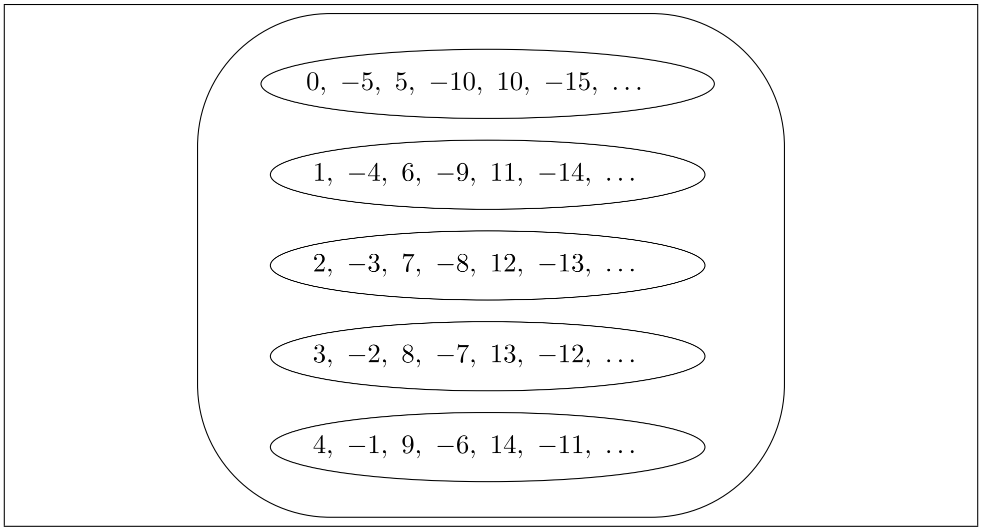

Figure 2.8: Partition $\mathbb{Z}/(\operatorname{mod} 5) = \{[0], [1], [2], [3], [4]\}$ of $\mathbb{Z}$ into equivalence classes

2.7. More abstract nonsense

We conclude this chapter with a few more general constructions for relations. The first is a way to construct a relation on $X \times Z$ given a relation on $X \times Y$ and a relation on $Y \times Z$:

Definition 2.7.1. Suppose R is a relation on $X \times Y$ and S is a relation on $Y \times Z$. We define the **composition (of R with S)** (notation: $S \circ R$) to be the following relation on $X \times Z$:

$$S \circ R \;:=\; \big\{(x, z) \in X \times Z : \exists y \in Y \text{ such that } (x, y) \in R \text{ and } (y, z) \in S\big\} \;\subseteq\; X \times Z.$$

The second is a way to get a relation on $Y \times X$ given a relation on $X \times Y$:

Definition 2.7.2. Suppose R is a relation on $X \times Y$. We define the **inverse** of R (notation: R^{-1}) to be the following relation on $Y \times X$:

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

These notions of *composition* and *inverse* will be more important for functions (special type of relation) in the next chapter. Although they can still be quite useful for relations which aren't functions.

2.8. Exercises

Exercise 2.8.1. This exercise is about writing natural statements in first-order logic, and then negating those statements. These examples come from Math131a and Math115a, although you don't need to know anything from those subjects to do this problem.

(1) Suppose $(a_n)_{n\in\mathbb{N}} = a_0, a_1, a_2, \ldots$ is a sequence of real numbers indexed by $n \in \mathbb{N}$ and $a \in \mathbb{R}$ is a fixed real number. We say the sequence $(a_n)_{n\in\mathbb{N}}$ **converges** to a (notation: $\lim_{n\to\infty} a_n = a$) if: for every real number $\epsilon > 0$, there is an index $N \in \mathbb{N}$ such that for all indices $n \geq N$ we have $|a_n - a| < \epsilon$.
   (a) Write the statement "$(a_n)_{n\in\mathbb{N}}$ converges to a" as a statement in first-order logic. Indicate what the domain of discourse is for each variable.
   (b) Write the negation of the statement from (a) as a statement in first-order logic. Write it in an equivalent form which does not require the negation symbol "$\neg$".
   (c) Rewrite the symbolic statement from (b) as a statement using natural language.

(2) Suppose $f : \mathbb{R} \to \mathbb{R}$ is a function. We say that f is a **continuous** function if: for every point $a \in \mathbb{R}$, for every real number $\epsilon > 0$, there is a real number $\delta > 0$ such that for every $b \in \mathbb{R}$, if $|a - b| < \delta$, then $|f(a) - f(b)| < \epsilon$. Repeat steps (a)-(c) for the statement "$f : \mathbb{R} \to \mathbb{R}$ is a continuous function".

(3) Suppose V is a vector space over $\mathbb{R}$. Given vectors $v_1, \ldots, v_n \in V$, we say that $v_1, \ldots, v_n$ are **linearly independent** if: for all coefficients $c_1, \ldots, c_n \in \mathbb{R}$, if $c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$, then $c_i = 0$ for each $i = 1, \ldots, n$. Repeat steps (a)-(c) for the statement "$v_1, \ldots, v_n$ are linearly independent".

Exercise 2.8.2. Let $A = \{2, 4\}$ and $B = \{6, 8, 10\}$ and define relations R and S from A to B as follows: For all $(x, y) \in A \times B$, xRy iff $x|y$, and xSy iff $y - 4 = x$. State explicitly which ordered pairs are in $A \times B$, R, S, $R \cup S$, and $R \cap S$.

Exercise 2.8.3. For each of the following relations, determine (with justification) whether each one is reflexive, symmetric, and/or transitive:

(1) Define the relation I on $\mathbb{R}$ by: xIy iff $x - y \in \mathbb{R} \setminus \mathbb{Q}$ (i.e., iff $x - y$ is irrational).
(2) Let P be the set of all propositions (in some fixed setting). Define the relation R on P by: pRq iff the proposition "$p \to q$" is true.
(3) Define the relation P on $\mathbb{Z}$ by: $kP\ell$ iff there exists a prime number $p \in \mathbb{N}$ such that $p|k$ and $p|\ell$.

Exercise 2.8.4. Prove by induction that for every $n \geq 1$ we have $15|2^{4n} - 1$.

Exercise 2.8.5. Prove that for all $d, n \in \mathbb{N}$, if $d|n$, then $2^d - 1|2^n - 1$ [Hint: use Difference-of-Powers Formula]. Then justify why $31|2^{35} - 1$ and $127|2^{35} - 1$.

Exercise 2.8.6. For every $a \in \mathbb{Z}$, show the following:

(1) $2|a(a+1)$
(2) $3|a(a+1)(a+2)$
(3) $3|a(2a^2+7)$

Exercise 2.8.7. Prove that every natural number $n \geq 2$ has a prime divisor. Hint: Apply the Well-Ordering Principle to a carefully chosen set of divisors of n; you can also do this with Strong Induction.

Exercise 2.8.8. Prove parts (1) and (2) of Fact 2.5.4.

Exercise 2.8.9. Let $n \geq 1$ and suppose $a, b \in \mathbb{Z}$. Prove the following are equivalent:

(1) $a \equiv b \pmod{n}$,
(2) $n|a - b$,
(3) if $q_0, q_1, r_0, r_1 \in \mathbb{Z}$ are such that $a = nq_0 + r_0$, $b = nq_1 + r_1$ and $0 \leq r_0, r_1 < n$, then $r_0 = r_1$ (i.e., a and b leave the same remainder when divided by n).

Exercise 2.8.10. For $n \geq 1$ let p_n denote the nth prime number (so the sequence $p_1, p_2, p_3, \ldots$ begins $2, 3, 5, \ldots$). Use strong induction to prove the following: For each $n \geq 1$, $p_n \leq 2^{2^{n-1}}$. [Hint: study the proof of Euclid's Theorem.]

Exercise 2.8.11. Prove the *existence* part of the Fundamental Theorem of Arithmetic by strong induction:

For each $n \geq 2$ there exists $m \geq 1$, prime numbers $p_1 < p_2 < \cdots < p_m$ and positive integers $k_1, \ldots, k_m$ such that

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}.$$

Exercise 2.8.12. Suppose X, Y, Z, W are sets sets and $R \subseteq X \times Y$, $S \subseteq Y \times Z$ and $T \subseteq Z \times W$ are binary relations. Prove that relational composition is associative:

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Exercise 2.8.13. Suppose R is a relation on a set X. For each $n \geq 1$ define the **n-fold composition** $R^{\circ n}$ as follows: for $n = 1$ we set $R^{\circ 1} := R$ and for $n \geq 1$ we define $R^{\circ(n+1)} := R^{\circ n} \circ R$. Define the **transitive closure** R^{tc} of R to be the following relation on X:

$$R^{\text{tc}} := \bigcup_{n=1}^{\infty} R^{\circ n} := \{(x,y) \in X \times X : \text{there exists } n \geq 1 \text{ such that } (x,y) \in R^{\circ n}\}$$

Prove the following:

(1) $R \subseteq R^{\text{tc}}$,
(2) R^{tc} is a transitive relation on X,
(3) for every relation S on X, if
  (a) $R \subseteq S$ and
  (b) S is transitive,
then $R^{\text{tc}} \subseteq S$.

This essentially says that R^{tc} is the transitive relation "generated" by R, and it is the smallest transitive relation on X which contains R.

Exercise 2.8.14. This problem is the sequel to the "transitive closure" exercise above (and you can freely cite parts of that problem here if it helps). Given $S \subseteq X \times X$ define the following operations:

$$\begin{aligned} \rho(S) &:= S \cup \big\{(x,x) : x \in X\big\} \\ \sigma(S) &:= S \cup S^{-1} \\ S^{\mathrm{tc}} &:= \bigcup_{n=1}^{\infty} S^{\circ n} \end{aligned}$$

Now suppose $R \subseteq X \times X$.

(1) Show that $(\sigma(\rho(R)))^{\mathrm{tc}}$ is an equivalence relation on X which contains R.
(2) Show that if $R' \subseteq X \times X$ is an equivalence relation on X which contains R (i.e., $R \subseteq R'$), then $R' \supseteq (\sigma(\rho(R)))^{\mathrm{tc}}$. In other words, $(\sigma(\rho(R)))^{\mathrm{tc}}$ is the smallest equivalence relation which contains R. (One could perhaps call this the "equivalence relation closure" of R.)

[Hint: For this problem, it might help to state and prove several smaller claims.]

Exercise 2.8.15. True or False (with justification):

(1) $17 \equiv 2 \pmod 5$
(2) $14 \equiv -6 \pmod{10}$
(3) $97 \equiv 5 \pmod{13}$
(4) $3 \cdot 4 \equiv 3 \cdot 14 \pmod 6$
(5) $4 \equiv 14 \pmod 6$
(6) For all $a, b, c \in \mathbb{Z}$ and $n \geq 1$, if $ab \equiv ac \pmod n$, then $b \equiv c \pmod n$.

Exercise 2.8.16. This problem is about prime numbers.

(1) Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$. [Hint: Consider $n! - 1$].
(2) Prove that if $2^n - 1$ is prime, then n is prime.
(3) Prove that if $2^n + 1$ is prime, then n is a power of 2.

CHAPTER 3

Functions

3.1. Functions

We are already familiar with functions $f : X \to Y$ as being some sort of machine that assigns to each input $x \in X$ a unique output $y \in Y$. The formal way to view functions is as a special case of relations:

Definition 3.1.1. Suppose f is a relation on $X \times Y$. We say that f is a **function from X to Y** (notation: $f : X \to Y$) if for every $x \in X$ there is exactly one $y \in Y$ such that $(x, y) \in f$, i.e.,

(i) For each $x \in X$, there exists $y \in Y$ such that $(x, y) \in f$:

$$\forall x \in X \ \exists y \in Y \ \big((x, y) \in f\big)$$

(ii) For each $x \in X$, and for every $y_1, y_2 \in Y$, if $(x, y_1) \in f$ and $(x, y_2) \in f$, then $y_1 = y_2$:

$$\forall x \in X \ \forall y_1 \in Y \ \forall y_2 \in Y \ \big((x, y_1) \in f \wedge (x, y_2) \in f \to y_1 = y_2\big)$$

Note: (i) asserts there is *at least one* $y \in Y$, and (ii) asserts there is *at most one* $y \in Y$. Taken together, (i) and (ii) assert there is *exactly one* $y \in Y$ (with the property $(x, y) \in f$).

Suppose $f : X \to Y$. Then:

(1) We shall use the notation $f(x) = y$ to indicate that $(x, y) \in f$

(2) The set X is called the **domain** of f (notation: $\mathrm{domain}(f) = X$)

(3) The set Y is called the **codomain** of f (notation: $\mathrm{codomain}(f) = Y$)

(4) The following subset of Y

$$\mathrm{range}(f) \ := \ \big\{f(x) : x \in X\big\} \ = \ \big\{y \in Y : \text{there exists } x \in X \text{ such that } f(x) = y\big\}$$

is called the **range** of f

(5) We also may use the notation "$x \mapsto f(x) : X \to Y$" instead of $f : X \to Y$, especially when the function f is determined by a formula in x and/or it is not necessary to give a name to the function; see Example 3.1.2(2) below.

Example 3.1.2. (1) Given a set X we define the **identity function** on X (notation: $\mathrm{id}_X : X \to X$) to be the function that sends every $x \in X$ to itself, i.e.,

$$\mathrm{id}_X(x) \ := \ x, \quad \text{for every } x \in X.$$

Note that in this case, $\mathrm{domain}(\mathrm{id}_X) = \mathrm{codomain}(\mathrm{id}_X) = \mathrm{range}(\mathrm{id}_X) = X$.

(2) The function:

$$k \mapsto k^2 : \mathbb{Z} \to \mathbb{Z}$$

has domain $\mathbb{Z}$, codomain $\mathbb{Z}$ and range $\{0, 1, 4, 9, 16, \ldots\}$.

(3) We define the **floor function** to be the function $x \mapsto \lfloor x \rfloor : \mathbb{R} \to \mathbb{Z}$ defined by

$$x \mapsto \lfloor x \rfloor \ := \ \text{the unique } k \in \mathbb{Z} \text{ such that } k \leq x < k+1,$$

i.e., the floor of a real number x is the greatest integer less than or equal to x.

(4) Likewise, we define the **ceiling function** to be the function $x \mapsto \lceil x \rceil : \mathbb{R} \to \mathbb{Z}$ defined by

$$x \mapsto \lceil x \rceil \ := \ \text{the unique } k \in \mathbb{Z} \text{ such that } k-1 < x \leq k,$$

i.e., the ceiling of a real number x is the least integer greater than or equal to x.

Question 3.1.3. *What is the codomain of the following function:*

$$f \ := \ \big\{(1,a),(2,c),(3,c),(4,b)\big\}$$

Answer 3.1.4. Trick question! The domain is definitely the set $X := \{1,2,3,4\}$, however, the *codomain* can technically be any set which contains $Y := \{a,b,c\}$. Indeed, f is a valid function of type "$X \to Y$" (in which case, the codomain would be Y), but it is also a valid function of type "$X \to Y \cup \{d,e,f\}$" (in which case, the codomain would be $Y \cup \{d,e,f\} = \{a,b,c,d,e,f\}$). The lesson here is that the codomain is determined by what we say it is when we are specifying the function as either $f : X \to Y$ or $f : X \to Y \cup \{d,e,f\}$. This annoyance only occurs for the *codomain*. The *domain* is always uniquely determined (as mentioned above) from the underlying set of ordered pairs, as is the *range* (which in this case is Y).

Just as with relations, we can form a new function from two given functions by *composition*.

Definition 3.1.5. Suppose $f : X \to Y$ and $g : Y \to Z$ are functions. Then the relational composition $g \circ f \subseteq X \times Z$ is a function[1] $g \circ f : X \to Z$ called the **composition of** g **with** f. Recall that $g \circ f : X \to Z$ is defined by:

$$\begin{aligned}(g \circ f)(x) \ := \ g\big(f(x)\big) \ := \ &\text{the unique } z \in Z \text{ such that } \exists y \in Y \\ &\text{such that } f(x) = y \text{ and } g(y) = z.\end{aligned}$$

Remark 3.1.6. (1) Suppose we have three function $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$. Then we can create two new functions through composition: $g \circ f : X \to Z$ and $h \circ g : Y \to W$. Finally, we can create two new functions:

$$h \circ (g \circ f) : X \to W \quad \text{and} \quad (h \circ g) \circ f : X \to W.$$

By Exercise 2.8.12, it follows that these functions are the same, i.e.,

$$h \circ (g \circ f) \ = \ (h \circ g) \circ f.$$

Thus we say that functional composition is *associative*.

(2) Functional composition allows us to highlight the two main properties of the identity function $\mathrm{id}_X : X \to X$:

(a) For every function $f : X \to Y$ we have $f \circ \mathrm{id}_X = f$,

(b) For every function $g : W \to X$ we have $\mathrm{id}_X \circ g = g$.

[1] See Exercise 3.5.1.

We can also (sometimes) consider the *inverse* of a function. However, we will define the inverse of a function in a more compelling way than just considering the inverse f^{-1} of the underlying relation f (our definition will turn out to mean the same thing).

Definition 3.1.7. Suppose $f : X \to Y$ is a function. We say that a function $g : Y \to X$ is an **inverse** to f if $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. We say that $f : X \to Y$ is an **invertible** function if there exists an inverse $g : Y \to X$.

At this point, it is not clear whether every function has an inverse (answer: no), or even in the cases when a function does have an inverse whether that inverse is unique (answer: yes). The following clears up the latter issue:

Lemma 3.1.8 (Uniqueness of function inverse)**.** *Suppose $f : X \to Y$ is a function and $g, h : Y \to X$ are inverses to f. Then $g = h$.*

Proof. Note that

$$\begin{aligned} g &= g \circ \mathrm{id}_Y \quad \text{by Remark 3.1.6(2)} \\ &= g \circ (f \circ h) \quad \text{since } h \text{ is an inverse of } f \\ &= (g \circ f) \circ h \quad \text{since composition is associative} \\ &= \mathrm{id}_X \circ h \quad \text{since } g \text{ is an inverse of } f \\ &= h \quad \text{by Remark 3.1.6(2).} \end{aligned}$$ □

One special feature of the proof of Lemma 3.1.8 is that it used very general principles (compositional property of identity, definition of inverse, associativity) and did not mention specific elements $x \in X$ at all. Analogues of this argument show up in many other areas of math, for example, in the proof that the inverse of an invertible matrix is unique. At any rate, we can now unambiguously define the inverse f^{-1} of an invertible function f:

Definition 3.1.9. Suppose $f : X \to Y$ is an invertible function. Then we define $f^{-1} : Y \to X$ to be the (unique) inverse of f.

At this point, given an invertible function f we have two meanings to "f^{-1}", the one given by Definition 2.7.2 (if we were viewing f as a relation) and the one given by Definition 3.1.9 (if we are viewing f as an invertible function). Fortunately these two meanings coincide so there is no issue (see Exercise 3.5.3).

3.2. Three special types of functions

There are three special flavors of functions which permeate all of mathematics:

Definition 3.2.1. A function $f : X \to Y$ is called

(1) **injective** (or **one-to-one**) if for every $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$:

$$\forall x_1 \in X\ \forall x_2 \in X\ \big(f(x_1) = f(x_2) \to x_1 = x_2\big)$$

(2) **surjective** (tacitly[2]: **surjective onto** Y)(or **onto**) if for every $y \in Y$ there exists an $x \in X$ such that $f(x) = y$:

$$\forall y \in Y \; \exists x \in X \; \big(f(x) = y\big)$$

Equivalently, f is surjective if range(f) = codomain(f).

(3) **bijective** (or a **bijection**, or **one-to-one and onto**) if f is both injective and surjective

We give some simple examples of functions which either have or do not have each of these properties:

Example 3.2.2. (1) Suppose $X = \{a, b, c\}$ and $Y = \{d, e, f\}$. Then the function $f : X \to Y$ specified in Figure 3.1 is a bijection, i.e., it is both injective and surjective.

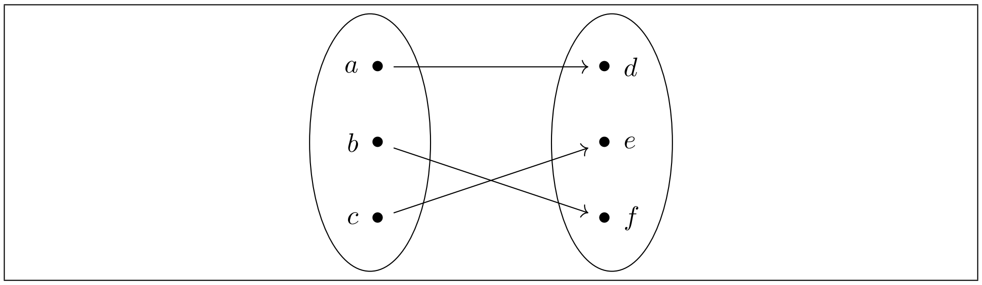

Figure 3.1: A bijective (i.e., an injective and surjective) function

(2) Suppose $X = \{a, b, c\}$ and $Y = \{d, e\}$. Then the function $f : X \to Y$ specified in Figure 3.2 is a surjective function but it is not injective.

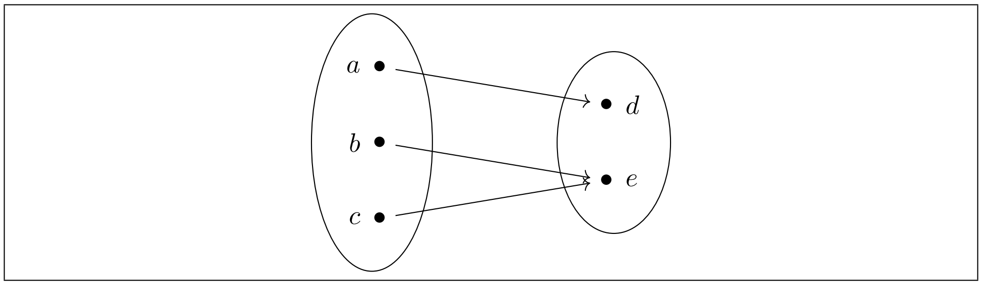

Figure 3.2: A surjective function that is not bijective

(3) Suppose $X = \{a, b\}$ and $Y = \{c, d, e\}$. Then the function $f : X \to Y$ specified in Figure 3.3 is an injective function but it is not surjective.

[2] The notion of *surjective* (as well as *bijective*) only makes sense when it is clear what the codomain is. If you change what the codomain is, the function might change whether it is surjective or not. For instance, in Question 3.1.3, the function $f : X \to Y$ is surjective, but the function $f : X \to Y \cup \{d, e, f\}$ is not surjective, even though the two f's have the same underlying set!

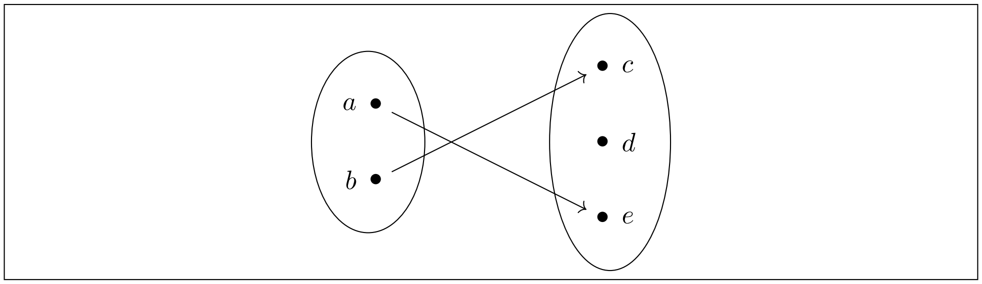

Figure 3.3: An injective function that is not surjective

(4) Suppose $X = \{a, b\}$ and $Y = \{c, d\}$. Then the function $f : X \to Y$ specified in Figure 3.4 is neither injective nor surjective.

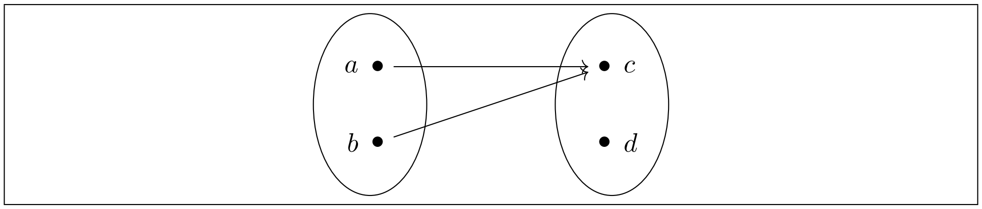

Figure 3.4: A function that is neither injective nor surjective

These notions allow us to characterize which functions are invertible:

Theorem 3.2.3. *Suppose $f : X \to Y$ is a function. The following are equivalent:*

(1) f is a bijection.
(2) f is invertible.

Proof. This is Exercise 3.5.5. □

For finite domains and codomains, the notions of *injective*, *surjective*, and *bijective* are intimately tied to the concept of *cardinality*. We begin with introducing the following (obvious) fact about cardinality which we will take for granted:

Cardinality Fact 3.2.4. *Suppose X is a finite set and $a \notin X$. Then $|X \cup \{a\}| = |X| + 1$.*

We also need to introduce the following:

Definition 3.2.5. Suppose $f : X \to Y$ is a function. Then we define the **inverse image function (of f)** to be the set-valued function

$$f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$$

defined by

$$f^{-1}(A) \;:=\; \{x \in X : f(x) \in A\}$$

for every $A \subseteq Y$. Here are some basic facts about the inverse image function:

(1) a function $f : X \to Y$ is an injection iff for every $b \in Y$, $|f^{-1}(\{b\})| \leq 1$,
(2) a function $f : X \to Y$ is a surjection iff for every $b \in Y$, $|f^{-1}(\{b\})| \geq 1$,
(3) if $f : X \to Y$ is a function and X is finite, then

$$|X| \;=\; \sum_{b \in Y} |f^{-1}(\{b\})|.$$

Remark 3.2.6. Note that *every* function $f : X \to Y$ admits an inverse image function $f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$, regardless of whether f is invertible or not. If f is invertible, then its inverse $f^{-1} : Y \to X$ also has the name "f^{-1}", although this should not cause any confusion since the inverse image function takes as input *subsets* of Y whereas the inverse of f (should it exist), takes as input *elements* of Y. Thus the context should always make clear what "f^{-1}" means, depending on what type of object the input and output of the function is supposed to be.

Lemma 3.2.7. *Suppose $f : X \to Y$ is a function. Then*

(1) if X is finite and f is an injection, then $|X| \leq |Y|$.

(2) if f is a surjection, then there exists an injection $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$, and thus $|Y| \leq |X|$ if Y is finite.

Proof. (1) We will prove this statement by induction on $|X|$. Specifically, we will prove the following for every $n \geq 0$:

$$P(n): \quad \text{“if } |X| = n \text{ and } f : X \to Y \text{ is an injection, then } |X| \leq |Y|.\text{”}$$

Base Case: Suppose $n = 0$, then automatically $|X| = 0 \leq |Y|$.

Inductive Step: Suppose for some $n \geq 0$ we know that $P(n)$ is true. We will show that $P(n+1)$ is true. Suppose $f : X \to Y$ is an injection with $|X| = n+1$. Select some $a \in X$ and consider $X' := X \setminus \{a\}$, so $|X'| = n$. Also define $Y' := Y \setminus \{f(a)\}$. Then the relation $f \setminus \{(a, f(a))\} \subseteq X' \times Y'$ is also an injective function. Thus by $P(n)$ it follows that $|X'| \leq |Y'|$. By Cardinality Fact 3.2.4, it follows that $|X| = |X'| + 1 \leq |Y'| + 1 = |Y|$. Thus $P(n+1)$ is proven.

(2) Suppose $f : X \to Y$ is a surjection. Since f is surjective, for each $b \in Y$, the set $f^{-1}(\{b\})$ is nonempty. Thus define $g(b)$ arbitrarily such that $g(b) \in f^{-1}(\{b\})$. Then $f\big(g(b)\big) = b$ for every $b \in Y$ so $f \circ g = \mathrm{id}_Y$. Furthermore, the function $g : Y \to X$ is an injection. Indeed, suppose $b_1, b_2 \in Y$ are arbitrary such that $g(b_1) = g(b_2)$. Applying f to both sides yields $b_1 = f\big(g(b_1)\big) = f\big(g(b_2)\big) = b_2$. □

Theorem 3.2.8. *Suppose $f : X \to Y$ is a function, X and Y are finite sets and $|X| = |Y|$. Then the following are equivalent:*

(1) f is injective.

(2) f is surjective.

(3) f is bijective.

(4) f is invertible.

Proof. (3)⇔(4) follows from Theorem 3.2.3. (3)⇒(1) and (3)⇒(2) follows from the definition of *bijection*.

(1)⇒(2) Suppose $f : X \to Y$ is an injection. Then $f : X \to \mathrm{range}(f)$ is also an injection and so $|X| \leq |\mathrm{range}(f)| \leq |Y|$. However, since $|X| = |Y|$ and these sets are finite, it follows that $|Y| = |\mathrm{range}(f)|$ and so $Y = \mathrm{range}(f)$. Thus f is surjective.

(2)⇒(1) Suppose $f : X \to Y$ is surjective. By Lemma 3.2.7(2) there exists an injective function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$. Since we already know (1)⇒(2) is true, we know that g is surjective and so $g : Y \to X$ is bijective, and thus invertible (by (3)⇔(4)). Let $h : X \to Y$ be an inverse of g, which is also injective since it is invertible. Note that

$$h = \mathrm{id}_Y \circ h = (f \circ g) \circ h = f \circ (g \circ h) = f \circ \mathrm{id}_X = f.$$

Thus f is also injective.

Now that we've established (1)⇔(2), we know that an injective function $f : X \to Y$ is automatically surjective, hence bijective. Thus (1)⇒(3) is also true. □

The contrapositive of Lemma 3.2.7(1) is of special importance:

Pigeonhole Principle 3.2.9 (Abstract Form)**.** *Suppose $f : X \to Y$ is a function, X and Y are finite sets and $|X| > |Y|$. Then f is not injective, i.e., there are $x_1, x_2 \in X$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.*

Note: the previous three results are in some sense an *embryonic form* of the arguments needed for basic dimension-theoretic results concerning linear transformations between finite-dimensional vector spaces.

3.3. The *mod* n function and the *greatest common divisor* function

In this section we continue our study of basic number theory. In section 2.6 we encountered the $a \equiv b \pmod n$ congruence (equivalence) relation on $\mathbb{Z}^2$. Given integers $a, b \in \mathbb{Z}$, the relation $a \equiv b \pmod n$ says that a and b leave the same remainder when divided by n. Many times, it is convenient to know what the remainder actually is. For instance, it is nice to know that $432 \equiv 7495 \pmod 7$, but it is perhaps more informative to know that $432 \equiv 5 \pmod 7$ and $7495 \equiv 5 \pmod 7$, This is because in our minds we picture the equivalence classes (mod 7) as being labeled by some number from $\{0, 1, 2, \ldots, 6\}$ (the remainder when divided by 7), so we somehow know more information if we are told both 432 and 7495 are $\equiv 5 \pmod 7$ because it tells us which specific equivalence class these numbers belong to, which could be useful when comparing them to other numbers later which come along.

Definition 3.3.1. Fix an $n \geq 1$. Define the **modulus operator** (with respect to n) to be the function

$$k \mapsto k\%n \ : \ \mathbb{Z} \to \{0, 1, \ldots, n-1\}$$

defined for $k \in \mathbb{Z}$ by

$$k\%n \ := \ \text{the unique } r \in \{0, \ldots, n-1\} \text{ such that } k \equiv r \pmod n.$$

In the textbook, $k\%n$ is denoted instead "$k \bmod n$", however we will stick to the notation $k\%n$ to emphasize that we are talking about a function, to acknowledge the computer science connection, and to distinguish it from the equivalence relation $a \equiv b \pmod n$ (which is *not* a function)

When simplifying fractions a/b, we want to know what is the best divisor which we can factor out of both a and b simultaneously, to then cancel out. For instance,

$$\frac{15}{21} \ = \ \frac{3 \cdot 5}{3 \cdot 7} \ = \ \frac{5}{7}.$$

The divisor we are looking for is called the *greatest common divisor* of a and b. In order to make this definition precise, first we need to observe the following:

Lemma 3.3.2. *Suppose $a, b \in \mathbb{Z}$ are such that either $a \neq 0$ or $b \neq 0$, i.e., suppose $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Then the set of common divisors*

$$\mathrm{CD}(a, b) \ := \ \{d \in \mathbb{N} : d|a \text{ and } d|b\}$$

has the properties:

(1) $1 \in \mathrm{CD}(a, b)$ (so $\mathrm{CD}(a, b)$ is nonempty), and

(2) for every $d \in \mathrm{CD}(a,b)$, $d \le \max(|a|,|b|)$ (so $\mathrm{CD}(a,b)$ is bounded above).
Thus the set $\mathrm{CD}(a,b)$ has a largest element.

Proof. (1) follows from 2.4.5(D1) and (2) follows from (D6). □

Definition 3.3.3. Define the **greatest common divisor** function of two integers to be the function

$$(a,b) \mapsto \gcd(a,b) \;:\; \mathbb{Z}^2 \setminus \{(0,0)\} \to \mathbb{N}$$

defined by

$$\gcd(a,b) \;:=\; \max \mathrm{CD}(a,b).$$

In other words, $\gcd(a,b) = d$ means:

(1) $d|a$ and $d|b$, in symbols:

$$d|a \wedge d|b$$

(2) for all $e \in \mathbb{N}$, if $e|a$ and $e|b$, then $e \le d$, in symbols:

$$\forall e\ (e|a \wedge e|b \to e \le d)$$

[Note: (1) asserts that d is a common divisor, and (2) asserts that d is greater than or equal to all other common divisors, taken together this means that d is the greatest common divisor.]

For small integers, the gcd is easy to compute by brute-force:

Example 3.3.4. Suppose $a = 24$ and $b = 45$. Then the set of positive divisors are respectively

$$\{1,2,3,4,6,8,12,24\} \quad \text{and} \quad \{1,3,5,9,15,45\}.$$

Thus the common divisors are

$$\mathrm{CD}(24,45) \;=\; \{1,3\}$$

and so $\gcd(24,45) = 3$.

We will study more efficient ways of computing $\gcd(a,b)$. First we give a useful and more abstract characterization of $\gcd(a,b)$:

Theorem 3.3.5. *Suppose $a,b \in \mathbb{Z}$ and $(a,b) \ne (0,0)$. Consider the nonempty set of natural numbers:*

$$S \;:=\; \{ax + by : x,y \in \mathbb{Z} \text{ and } ax + by > 0\}$$

Then $\gcd(a,b) = \min S$. Furthermore,

$$\{ax + by : x,y \in \mathbb{Z}\} \;=\; \big\{k\gcd(a,b) : k \in \mathbb{Z}\big\},$$

i.e., the set of all integer combinations of a and b is the same as the set of all integer multiples of $\gcd(a,b)$.

Proof. Let $d := \min S$ (by the Well-Ordering Principle, S has a least element since it is nonempty; indeed, consider $x = \pm 1$ and $y = \pm 1$, at least one of these choices of x and y will work). Let $x,y \in \mathbb{Z}$ be such that $d = ax + by$.

By the Quotient-Remainder Theorem, we get $q,r \in \mathbb{Z}$ such that $a = qd + r$ where $0 \le r < d$. Then we have

$$r \;=\; a - qd \;=\; a - q(ax+by) \;=\; a(1-qx) + b(-qy).$$

Since $0 \leq r < d$, this forces $r = 0$ (otherwise r would be an even smaller element of S than d). Thus $d|a$. By a similar argument we also get $d|b$. Thus d is a positive common divisor of a and b.

Next, suppose $c \in \mathbb{N}$ is such that $c \geq 1$ and $c|a$ and $c|b$. Then $c|ax + by = d$, so $c \leq d$. We conclude that $d = \gcd(a, b)$.

For the second property, define $T := \{ax + by : x, y \in \mathbb{Z}\}$ and $W := \big\{kd : k \in \mathbb{Z}\big\}$. Since $d|a$ and $d|b$, if follows that $d|ax + by$ for all $x, y \in \mathbb{Z}$ and so $T \subseteq W$. Conversely, since $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$ (by the first part), it follows that $kd = a(kx_0) + b(ky_0) \in T$. Thus $W \subseteq T$. □

Definition 3.3.6. Given $a, b \in \mathbb{Z}$ such that $(a, b) \neq (0, 0)$, we say that a and b are **relatively prime** if $\gcd(a, b) = 1$.

Euclid's Lemma 3.3.7. *Suppose $a, b, c \in \mathbb{Z}$ are such that $(a, b) \neq (0, 0)$ and $\gcd(a, b) = 1$. If $a|bc$, then $a|c$.*

Proof. Since $\gcd(a, b) = 1$, by Theorem 3.3.5 there are $x, y \in \mathbb{Z}$ such that $ax+by = 1$. Thus $c = c \cdot 1 = acx + bcy$. Since $a|acx$ and $a|bcy$, it follows that $a|c$. □

We now summarize many of the relevant divisibility properties concerning prime numbers:

Lemma 3.3.8. *Suppose p is a prime number. Then*

(1) for every $a \in \mathbb{Z}$, if $p \nmid a$, then $\gcd(p, a) = 1$,
(2) for every $0 < k < p$, $\gcd(p, k) = 1$,
(3) for every $a, b \in \mathbb{Z}$, if $p|ab$, then $p|a$ or $p|b$,
(4) for every $a_1, \ldots, a_n \in \mathbb{Z}$, if $p|a_1 \cdots a_n$, then $p|a_i$ for some $i \in \{1, \ldots, n\}$.

Proof. (1) Suppose $d := \gcd(p, a)$. Then $d|p$ so either $d = p$ or $d = 1$. However, since $d|a$ it must be the case that $d \neq p$. Thus $d = 1$.

(2) follows from (1) since if $0 < k < p$, then $p \nmid k$ by Divisibility Property (D6).

(3) Assume $p|ab$ and $p \nmid a$. Then $\gcd(p, a) = 1$ by part (1), so $p|b$ by Euclid's Lemma 3.3.7.

(4) follows from (3) by induction on n. □

We are now in a good position to prove the *Fundamental Theorem of Arithmetic* which says that every integer $n \geq 2$ has a unique prime factorization:

Fundamental Theorem of Arithmetic 3.3.9. *Suppose $n \geq 2$. Then*

(1) (Existence) there exists $r \geq 1$, prime numbers $p_1 < p_2 < \cdots < p_r$ and positive integers $k_1, \ldots, k_r$ such that

$$n \;=\; p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}.$$

(2) (Uniqueness) for every $r, s \geq 1$, prime numbers $p_1 < p_2 < \cdots < p_r$, $q_1 < q_2 < \cdots < q_s$ and positive integers $k_1, \ldots, k_r$ and $\ell_1, \ldots, \ell_s$, if

$$n \;=\; p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \;=\; q_1^{\ell_1} q_2^{\ell_2} \cdots q_s^{\ell_s}$$

then $r = s$, and for each $i \in \{1, \ldots, r\}$, $p_i = q_i$ and $k_i = \ell_i$.

Proof. (1) This is Exercise 2.8.11.

(2) We will prove the following statement by induction on $n \geq 1$:

$P(n)$: "for every $r, s \geq 1$, prime numbers $p_1 < p_2 < \cdots < p_r$, $q_1 < q_2 < \cdots < q_s$

and positive integers $k_1, \dots, k_r$ and $\ell_1, \dots, \ell_s$, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1^{\ell_1} q_2^{\ell_2} \cdots q_s^{\ell_s}$,
then $r = s$, and for each $i \in \{1, \dots, r\}$, $p_i = q_i$ and $k_i = \ell_i$.”

We will prove this by strong induction.

Base Case: Suppose $n \geq 2$ is a prime number (this includes the true base case of $n = 2$). We claim that $n = p_1^{k_1}$ (where $p_1 := n$, $k_1 = 1$, and $r := 1$) is the unique prime factorization of n. Suppose we are given $s \geq 1$, primes $q_1 < \cdots < q_s$ and natural numbers $\ell_1, \dots, \ell_s$ such that

$$n \;=\; p_1^{k_1} \;=\; q_1^{\ell_1} \cdots q_s^{\ell_s}.$$

Then since n is composite, it must be the case that $s = 1$, that ℓ_1 (otherwise n would have too many divisors). Thus $n = p_1^1 = q_1^1$, so $p_1 = q_1$ as well.

Inductive Step: Assume for some $n \geq 2$ that $n+1$ is composite and we know that $P(2), \dots, P(n)$ hold. We will prove that $P(n+1)$ is true. Suppose we have $r, s \geq 1$, primes $p_1 < \cdots < p_r$, $q_1 < \cdots < q_s$, and positive integers $k_1, \dots, k_r$ and $\ell_1, \dots, \ell_s$ such that

$$n+1 \;=\; p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \;=\; q_1^{\ell_1} q_2^{\ell_2} \cdots q_s^{\ell_s}$$

Then $p_1 | n+1 = q_1^{\ell_1} \cdots q_s^{\ell_s}$. By Lemma 3.3.8(4), it follows that there is some $i \in \{1, \dots, s\}$ such that $p_1 | q_i$ and thus $p_1 = q_i$ since q_i is prime. Thus $q_1 \leq p_1$. A similar argument dividing q_1 into $n+1$ shows that $p_1 \leq q_1$. Thus $p_1 = q_1$. Consider the integer:

$$n' \;:=\; \frac{n+1}{p_1} \;=\; p_1^{k_1 - 1} p_2^{k_2} \cdots p_r^{k_r} \;=\; q_1^{\ell_1 - 1} q_2^{\ell_2} \cdots q_s^{\ell_s}.$$

Since $2 \leq n' \leq n$, we know that $P(n')$ is true. Thus $r = s$, $k_i = \ell_i$ and $p_i = q_i$ for each $i \in \{1, \dots, r\}$. Officially, we should do a case distinction to conclude this:

Case 1: *Suppose* $k_1 = 1$ Then $k_1 - 1 = 0$, so $p_1 \nmid n'$. Thus $q_1 \nmid n'$, so $\ell_1 - 1 = 0$, so $\ell_1 = 1$. In this case, the true prime factorization (with all positive exponents) is actually

$$n' \;:=\; \frac{n+1}{p_1} \;=\; p_2^{k_2} \cdots p_r^{k_r} \;=\; q_2^{\ell_2} \cdots q_s^{\ell_s}.$$

where there are $r-1$ and $s-1$ distinct primes in each, respectively. By $P(n')$, it follows that $r - 1 = s - 1$ and thus $r - s$. Furthermore, it follows from $P(n')$ that $p_i = q_i$ and $k_i = \ell_i$ for every $i \in \{2, \dots, r\}$.

Case 2: *Suppose* $k_1 > 1$ Then $k_1 - 1 > 0$ is a positive integer, so $p_1 | n'$. Thus $q_1 | n'$, so $\ell_1 - 1 \geq 1$ is also a positive integer. Thus the true prime factorization in this case (with all positive exponents) is

$$n' \;:=\; \frac{n+1}{p_1} \;=\; p_1^{k_1 - 1} p_2^{k_2} \cdots p_r^{k_r} \;=\; q_1^{\ell_1 - 1} q_2^{\ell_2} \cdots q_s^{\ell_s}.$$

and so by $P(n')$, we have that $r = s$, $p_i = q_i$ for every $i \in \{1, \dots, r\}$, $k_1 - 1 = \ell_1 - 1$, so $k_1 = \ell_1$, and $k_i = \ell_i$ for every $i \in \{2, \dots, r\}$. □

3.4. The Euclidean Algorithm

In this section we will present a recursive algorithm for computing $\gcd(a, b)$. This algorithm is based on the following properties of gcd:

Lemma 3.4.1. *Suppose* $a, b \in \mathbb{Z}$ *are such that* $(a, b) \neq (0, 0)$. *Then:*

(1) (Symmetry) $\gcd(a, b) = \gcd(b, a)$
(2) (Reduction) if $b \neq 0$, *then* $\gcd(a, b) = \gcd(b, a\%b)$

(3) (Stopping Conditions) $\gcd(a,1) = 1$ *and* $\gcd(a,0) = |a|$ *if* $a \neq 0$.

Proof. (1) Since $\mathrm{CD}(a,b) = \mathrm{CD}(b,a)$, it follows that

$$\gcd(a,b) \;=\; \max \mathrm{CD}(a,b) \;=\; \max \mathrm{CD}(b,a) \;=\; \gcd(b,a).$$

(2) Let $q \in \mathbb{Z}$ be such that $a = qb + a\%b$ and suppose $d \in \mathrm{CD}(a,b)$ is arbitrary. Then $d|a - qb = a\%b$, so $d \in \mathrm{CD}(b, a\%b)$. Conversely, if $d \in \mathrm{CD}(b, a\%b)$, then $d|qb + a\%b = a$, so $d \in \mathrm{CD}(a,b)$. Thus $\mathrm{CD}(a,b) = \mathrm{CD}(a, b\%a)$, and so $\gcd(a,b) = \gcd(a, a\%b)$.

(3) The only positive divisor of 1 is 1, so $\mathrm{CD}(a,1) = \{1\}$ and $\gcd(a,1) = 1$. Since $|a||a$ and $|a||0$, and $\gcd(a,0) \leq \max\{|a|, |0|\} = |a|$, it follows that $\gcd(a,0) = |a|$. □

Before formally introducing the *Euclidean Algorithm*, we will work out an example of its usage:

Example 3.4.2. What is $\gcd(157,30)$? Also, find integers $x, y \in \mathbb{Z}$ such that $\gcd(157,30) = 157x + 30y$.

Answer. We will iterate the (Reduction) property by continually dividing the new remainder (r) into the old smaller number (d) using the Quotient-Remainder Theorem, until we reach a (Stopping Condition). We agree to stop at 0 even if a remainder of 1 shows up (we display d, q, r only to show which numbers are playing which role in each application of the Quotient-Remainder Theorem):

$$\begin{array}{rcl@{\qquad}ccc}
a & = & b \cdot q + r & d & q & r \\
157 & = & 30 \cdot 5 + 7 & 30 & 5 & 7 \\
30 & = & 7 \cdot 4 + 2 & 7 & 4 & 2 \\
7 & = & 2 \cdot 3 + \boxed{1} & 2 & 3 & 1 \\
2 & = & 1 \cdot 2 + 0 & 1 & 2 & 0
\end{array}$$

Note that by (Reduction) the above computation shows

$$\gcd(157,30) \;=\; \gcd(30,7) \;=\; \gcd(7,2) \;=\; \gcd(2,1) \;=\; \gcd(1,0) \;=\; 1.$$

Thus $\gcd(157,30) = 1$. We will use back-substitution on the above computation to find integers x and y:

$$\begin{aligned}
1 &= 7 - 2 \cdot 3 \quad \text{(from fourth row)} \\
&= 7 - (30 - 7 \cdot 4) \cdot 3 \quad \text{(from third row)} \\
&= 7 \cdot 13 - 30 \cdot 3 \\
&= (157 - 30 \cdot 5) \cdot 13 - 30 \cdot 3 \quad \text{(from second row)} \\
&= 157 \cdot 13 - 30 \cdot 68.
\end{aligned}$$

Thus $x := 13$ and $y := -68$ suffice. □

The Euclidean Algorithm works exactly as in the above example:

Euclidean Algorithm 3.4.3. *Suppose $a > b \geq 1$. Then there are $n \geq 1$, a strictly decreasing sequence $r_1 > r_2 > \cdots > r_n = 0$ and integers $q_1, \ldots, q_n \in \mathbb{Z}$ such that*

$$
(\dagger)\qquad
\begin{array}{rcl@{\qquad\qquad}ccccc}
a &=& bq_1 + r_1 & 0 &\leq& r_1 &<& b \\
b &=& r_1 q_2 + r_2 & 0 &\leq& r_2 &<& r_1 \\
r_1 &=& r_2 q_3 + r_3 & 0 &\leq& r_3 &<& r_2 \\
 & \vdots & & & & & & \\
r_{n-3} &=& r_{n-2}q_{n-1} + \boxed{r_{n-1}} & 0 &\leq& r_{n-1} &<& r_{n-2} \\
r_{n-2} &=& r_{n-1}q_n + \underbrace{r_n}_{=0} & 0 &=& r_n. & &
\end{array}
$$

Furthermore,

1. *(1)* $\gcd(a,b) = r_{n-1}$*, with* $r_0 := b$*,*
2. *(2) for each* $k \in \{1, \ldots, n\}$*,* $r_k = r_{k-2}\%r_{k-1}$*, with* $r_{-1} := a$*,*
3. *(3) the numbers* $(n, r_1, \ldots, r_n, q_1, \ldots, q_n)$ *with property* $(\dagger)$ *are unique.*

[We suggestively call the number n in the Euclidean Algorithm the *number of recursive calls to the Quotient-Remainder Theorem for input* (a,b).]

Proof (Sketch). Given all the results we've developed so far, there is nothing inherently difficult about this proof other than the fact that the statement we are proving by induction is quite a mouthful. (Indeed, saying "are unique" in item (3) is really shorthand for a *much* longer statement.) We will prove the following statement for every $b \geq 1$ by strong induction on b:

$$P(b): \quad \text{For every } a > b \text{ there exists } (n, r_1, \ldots, r_n, q_1, \ldots, q_n)$$

$$\text{which satisfies } (\dagger) \text{ and } (1), (2), \text{ and } (3).$$

Base Case: Suppose $b = 1$. Then by the Quotient-Remainder Theorem 1.4.2 we have $q_1 := a \in \mathbb{Z}$ and $r_1 := a\%1 = 0$ such that $a = bq_1 + r_1$. Thus the data $(1, 0, a)$ have properties $(\dagger)$. Furthermore, $\gcd(a, 1) = 1$ by the (Stopping Condition) so item (1) holds. Item (2) holds by construction and (3) follows from the *Uniqueness* part of the Quotient-Remainder Theorem.

Inductive Step: Suppose for some $b \geq 1$ we know that $P(1), \ldots, P(b)$ are true. We must show that $P(b+1)$ is true. Suppose $a > b+1$ is arbitrary. By the Quotient-Remainder Theorem, get $q_1 \in \mathbb{Z}$ and $r_1 := a\%b$ such that $a = bq_1 + r_1$ and $0 \leq r_1 < b+1$.

If $r_1 = 0$, then $\gcd(a,b) = \gcd(b, a\%b) = \gcd(a, 0) = a$ by Lemma 3.4.1. Thus the data $(1, 0, q_1)$ has property $(\dagger)$ and satisfies items (1) and (2). Item (3) follows again from the *Uniqueness* part of the Quotient-Remainder Theorem.

If $1 \leq r_1 < b+1$, then by the inductive hypothesis $P(r_1)$ is true. Furthermore, by Lemma 3.4.1 we have $\gcd(a,b) = \gcd(a, r_1)$, so we can use $P(r_1)$ to compute $\gcd(a, r_1)$. Doing this yields data $(m, q'_1, \ldots, q'_m, r'_1, \ldots, r'_n)$ with the appropriate properties. Then the data $(m+1, q_1, q'_1, \ldots, q'_m, r_1, r'_1, \ldots, r'_n)$ works for computing $\gcd(a,b)$, i.e., it has properties $(\dagger)$ and satisfies items (1), (2), and (3) for the initial pair (a,b). □

3.5. Exercises

Exercise 3.5.1. Suppose we have two functions $f : X \to Y$ and $g : Y \to Z$. Since f and g are relations, we can consider their composition $g \circ f$ which is a relation on $X \times Z$ (see Definition 2.7.1). Prove that $g \circ f$ is a function $X \to Z$.

Exercise 3.5.2. Suppose $i : X \to X$ is a function with the following two properties:

(1) For every set Y and every function $f : X \to Y$ we have $f \circ i = f$, and
(2) For every set W and every function $g : W \to X$ we have $i \circ g = g$.

Prove that $i = \mathrm{id}_X$, i.e., prove that for every $x \in X$, that $i(x) = x$.

Exercise 3.5.3. Suppose $f : X \to Y$ is an invertible function with inverse $g : Y \to X$. Also consider the relation

$$h \ := \ \big\{(y, x) \in Y \times X : f(x) = y\big\}$$

on $Y \to X$. Prove that h is a function $Y \to X$ and that $g = h$.

Exercise 3.5.4. In this problem we will give alternative characterizations for injections and surjections. Suppose $f : X \to Y$ is a function.

(1) Prove the following are equivalent:
 (a) $f : X \to Y$ is an injection.
 (b) for every pair of functions $g, h : W \to X$, if $f \circ g = f \circ h$, then $g = h$.
(2) Prove the following are equivalent:
 (a) $f : X \to Y$ is a surjection.
 (b) for every pair of functions $g, h : Y \to Z$, if $g \circ f = h \circ f$, then $g = h$.

Exercise 3.5.5. Suppose $f : X \to Y$ is a function. The following are equivalent:

(1) f is a bijection.
(2) f is invertible.

Exercise 3.5.6. Suppose $f : X \to Y$ and $g : Y \to Z$ are invertible functions. Prove the following:

(1) $g \circ f : X \to Z$ is invertible, and
(2) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Exercise 3.5.7. Suppose $f : X \to Y$ is a function. We will show that f can be "factored" as a surjection followed by an injection in an essentially unique way.

(1) Show that $E_f \subseteq X \times X$ defined by aE_fb iff $f(a) = f(b)$ is an equivalence relation on X.
(2) Show that $\pi \subseteq X \times X/E_f$ defined by

$$\pi \ := \ \big\{(a, [a]) : a \in X\big\}$$

is a function $\pi : X \to X/E_f$ and this function is surjective.
(3) Show that $\overline{f} \subseteq X/E_f \times Y$ defined by

$$\overline{f} \ := \ \big\{([a], f(a)) : a \in X\big\}$$

is a function $\overline{f} : X/E_f \to Y$ and this function is injective.

(4) Show that $f = \overline{f} \circ \pi : X \to Y$. Here is the diagram illustrating the situation:

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\pi"'] & & Y \\
& X/E_f \arrow[ur, "\overline{f}"'] &
\end{tikzcd}$$

(5) Suppose we have functions $g : X \to Q$ and $h : Q \to Y$ such that
   (a) g is a surjection,
   (b) h is an injection, and
   (c) $f = h \circ g : X \to Y$.

   Prove that there exists a bijection $b : X/E_f \to Q$ such that $b \circ \pi = g$ and $h \circ b = \overline{f}$. Here is a diagram illustrating the situation:

$$\begin{tikzcd}
X \arrow[r, "\pi"] \arrow[dr, "g"'] & X/E_f \arrow[r, "\overline{f}"] \arrow[d, "b"] & Y \\
& Q \arrow[ur, "h"'] &
\end{tikzcd}$$

Exercise 3.5.8. Prove for every real number $x \in \mathbb{R}$, if $x \geq 0$, then

$$\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor \;=\; \lfloor \sqrt{x} \rfloor.$$

Exercise 3.5.9 (Freshman's Dream)**.** In this exercise we will prove an important and useful fact about arithmetic mod p (where p is a prime).

(1) For $0 \leq k \leq n$, by definition $\binom{n}{k} = \frac{n!}{k!(n-k)!} \in \mathbb{Q}$ is a rational number. Prove that in fact $\binom{n}{k} \in \mathbb{Z}$. [Hint: Use induction on n and for the cases $0 < k < n$ use Pascal's Rule]. Conclude that $k!(n-k)!|n!$.

(2) Suppose p is a prime and $0 < k < p$. Prove that $k!(p-k)!|(p-1)!$. Conclude that $p|\binom{p}{k}$.

(3) Let $x, y \in \mathbb{Z}$ be arbitrary and suppose p is a prime. Prove that

$$(x+y)^p \;\equiv\; x^p + y^p \pmod{p}.$$

Exercise 3.5.10. Suppose $a, b \in \mathbb{Z}$ are such that $\gcd(a, b) = d$. Prove that $\gcd(a/d, b/d) = 1$ (this includes justifying first why $a/d, b/d \in \mathbb{Z}$).

Exercise 3.5.11. Suppose $a, b, c \in \mathbb{Z}$ are such that $a|c$, $b|c$, and $\gcd(a, b) = 1$. Prove that $ab|c$.

Exercise 3.5.12. Suppose $a, b \in \mathbb{Z}$ are such that $\gcd(a, b) = 1$. Prove that for every $m, n \geq 1$ that $\gcd(a^m, b^n) = 1$ [Hint: use the "$ax + by = 1$" characterization of $\gcd(a, b) = 1$ and the Binomial Theorem.]

Exercise 3.5.13. Suppose $a, b, c \in \mathbb{Z}$ (with at least two of these numbers being nonzero). Prove that gcd is associative:

$$\gcd\big(a, \gcd(b, c)\big) \;=\; \gcd\big(\gcd(a, b), c\big).$$

Exercise 3.5.14. For all integers $a, b \in \mathbb{Z}$ such that $(a, b) \neq (0, 0)$, prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

Exercise 3.5.15. In each of the following, use the Euclidean algorithm to calculate the gcd and to find appropriate integers $x, y \in \mathbb{Z}$:

(1) Find integers $x, y \in \mathbb{Z}$ such that $547x + 632y = \gcd(547, 632)$.
(2) Find integers $x, y \in \mathbb{Z}$ such that $398x + 600y = \gcd(398, 600)$.
(3) Find integers $x, y \in \mathbb{Z}$ such that $922x + 2163y = \gcd(922, 2163)$.

Exercise 3.5.16. Find integers x, y, z such that

$$\gcd(198, 288, 512) \;=\; 198x + 288y + 512z.$$

Exercise 3.5.17. This problem is about gcd. Prove the following:

(1) If $\gcd(a, b) = 1$ and if $d|(a + b)$, then $\gcd(a, d) = \gcd(b, d) = 1$.
(2) If $a > 1$, then $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

CHAPTER 4

Counting

We begin with an analogy. Recall that prior to learning linear algebra, you could probably still solve simple linear equations

$$\begin{aligned} x + y &= 1 \\ x + 3y &= 2 \end{aligned}$$

just by thinking hard enough and coming up with some heuristic argument. However, linear equations are often much more complicated and the subject of linear algebra gives us (among many other things) a very systematic way to approach more complicated linear equations (and the simpler ones too)!

The subject of *counting* has a similar feeling to it. For instance, you can probably come up with the answer to the following counting problem

How many 5-card poker hands are a full-house?

just by thinking about it long enough and coming up with some heuristic argument. However, the subject of *counting* teaches us various systematic ways to view and count large sets as well as several very general principles we can apply when faced with a new problem.

4.1. Basic counting principles

In this section we introduce two fundamental counting principles. I claim that these principles are obvious and you've been using them your entire life. The novelty here is that we are making these principles explicit when usually we don't think about them when we are using them. Consequently, we'll give an example of the principle in action first, then discuss the principle itself.

Example 4.1.1 (License Plates)**.** Suppose in some state every license plate is of the form `ABC123` (i.e., three letters from the 26-letter alphabet and three non-zero digits from $\{1, 2, \ldots, 9\}$). Letters and numbers are allowed to appear more than once on the same license plate, so `CCD363` is also valid, for instance. A natural counting question to ask is:

How many distinct license plates can be made?

To answer this question, we think of how we might go about creating/constructing a particular license plate. This can be done in a series of choices:

(Step 1) Choose the first letter: 26 choices
(Step 2) Choose the second letter: 26 choices
(Step 3) Choose the third letter: 26 choices
(Step 4) Choose the first digit: 9 choices
(Step 5) Choose the second digit: 9 choices

(Step 6) Choose the third digit: 9 choices

In each step, so we are free to make any choice we want, independent of the previous steps, we should convince ourselves that there are

$$26 \cdot 26 \cdot 26 \cdot 9 \cdot 9 \cdot 9 \;=\; 12{,}812{,}904 \text{ total license plates.}$$

The following is the underlying principle which we used in the above example:

Multiplication Principle 4.1.2. *Suppose an object/activity/thing can be constructed/specified/created in t successive steps, where for each $i \in \{1, \dots, t\}$ Step i can be done in $n_i \in \mathbb{N}$ different ways, then the total number of possible objects/activities/things is*

$$n_1 \cdot n_2 \cdots n_t.$$

The Multiplication Principle is equivalent to the following abstract form involving finite sets and cardinalities:

Multiplication Principle 4.1.3 (Abstract Form)**.** *Suppose $A_1, A_2, \dots, A_t$ are finite sets. Then*

$$|A_1 \times A_2 \times \cdots \times A_t| \;=\; |A_1| \cdot |A_2| \cdots |A_t|.$$

Proof. We won't give a proof of this (we can't anyway unless we give a more formal definition of cardinality). However, you should have no problem taking this principle on faith. To convince yourself that it is true, use induction on t and recall the "multiplication is repeated addition" characterization of multiplication in $\mathbb{N}$. □

Our next principle is also straightforward. We give an example first:

Example 4.1.4 (Choosing flights)**.** Suppose we want to purchase an airline ticket for a flight from Los Angeles to Chicago. For the particular day we are interested in flying, there are three airlines offering flights throughout the day:

- Airline A has a total of 3 flights
- Airline B has a total of 5 flights
- Airline C has a total of 2 flights

The question we ask is the following:

How many total flights are there?

To answer this, we add up the total number of flights which each airline is offering:

$$3 + 5 + 2 \;=\; 10.$$

Thus there are 10 total flights to choose from.

The previous example illustrates a simple case of the *Addition Principle*:

Addition Principle 4.1.5. *Suppose the objects we are counting/constructing are partitioned into t disjoint categories, where for each $i \in \{1, \dots, t\}$ the ith category has $n_i \in \mathbb{N}$ objects in it. Then the total number of objects is*

$$n_1 + n_2 + \cdots + n_t.$$

The Addition Principle is also equivalent to a form involving finite sets and cardinalities (proof also omitted):

Addition Principle 4.1.6 (Abstract Form)**.** *Suppose $A_1, A_2, \dots, A_t$ are pairwise disjoint finite sets. Then*

$$|A_1 \cup A_2 \cup \cdots \cup A_t| \;=\; |A_1| + |A_2| + \cdots + |A_t|.$$

The Addition Principle only works when the sets in question are disjoint. For non-disjoint unions, the following is essential:

Inclusion-Exclusion Principle 4.1.7. *Suppose X and Y are finite sets. Then*

$$|X \cup Y| \;=\; |X| + |Y| - |X \cap Y|$$

Proof. We have the following decompositions of X, Y and $X \cup Y$ into disjoint unions:

(1) $X = (X \setminus Y) \cup (X \cap Y)$ (disjoint union)
(2) $Y = (X \cap Y) \cup (Y \setminus X)$ (disjoint union)
(3) $X \cup Y = (X \setminus Y) \cup (X \cap Y) \cup (Y \setminus X)$ (disjoint union)

Since these unions are disjoint, the Addition Principle 4.1.6 yields:

(4) $|X| = |X \setminus Y| + |X \cap Y|$
(5) $|Y| = |X \cap Y| + |Y \setminus X|$
(6) $|X \cup Y| = |X \setminus Y| + |X \cap Y| + |Y \setminus X|$

Finally, adding (4) and (5) and then using (6) yields:

$$|X| + |Y| \;=\; |X \setminus Y| + 2|X \cap Y| + |Y \setminus X| \;=\; |X \cup Y| + |X \cap Y|.$$

Subtracting $|X \cap Y|$ from both sides yields the desired formula. □

The Inclusion-Exclusion Principle works any time you would like to use the addition principle, but are forced to double-count something. Then the Inclusion-Exclusion Principle says that you should subtract out the double-counted group "$-|X \cap Y|$" to get the correct count.

Example 4.1.8 (CS vs. Math majors)**.** In a particular class containing only CS and Math majors we are told the following information:

- 100 students have a major in CS
- 90 students have a major in Math
- among the above students, 30 students are majoring in both CS and Math

We want to determine:

How many total students are in the class?

The Inclusion-Exclusion Principle tells us that to count the total number of students we need to add the first two groups together, and then subtract out the third group because that third group was counted twice:

$$\#\text{CS majors} \;+\; \#\text{Math majors} \;-\; \#\text{Double majors}$$

$$=\; 100 \;+\; 90 \;-\; 30 \;=\; 160 \text{ total students.}$$

4.2. Permutations and combinations

The Multiplication and Addition Principles give rise to various counting motifs that deserve special attention.

Example 4.2.1 (Class Rank)**.** Suppose a class has five students, A, B, C, D and E. At the end of the class the students will be ranked 1st to 5th (no ties) depending on their academic performance.

How many possible rankings are there?

Keeping in line with the previous examples, let's take a look at what decisions we need to make if we were to specify a particular ranking.

(1st) We need to choose which student is ranked 1st. There are five choices: any student from the set $\{A, B, C, D, E\}$. Let's choose student D. Now our ranking mid-construction looks like $(D, ?, ?, ?, ?)$.

(2nd) Next we need to choose which student is ranked 2nd. There are now four choices: any student from the set $\{A, B, C, E\}$. Let's choose student B. Now our ranking mid-construction looks like $(D, B, ?, ?, ?)$.

(3rd) Now we need to choose which student is ranked 3rd. There are now three choices: any student from the set $\{A, C, E\}$. Let's choose student A. Now our ranking mid-construction looks like $(D, B, A, ?, ?)$.

(4th) Now we choose which student is ranked 4th among the remaining two choices: any student from the set $\{C, E\}$. Let's choose student E. Now our ranking mid-construction looks like $(D, B, A, E, ?)$.

(5th) Finally we "choose" which student is 5th. There is one choice: C. We now arrive at our ranking (D, B, A, E, C).

In the above line of reasoning, *what* choices we have available to us at each step depends on the previous choices we made. However, the *number* of choices in each step does not. Indeed, no matter which choice we made in the first step, we would still have four different choices in the 2nd step, and so on. This suggests that the total number of possible rankings is

$$5 \times 4 \times 3 \times 2 \times 1 \;=\; 5! \;=\; 120.$$

This is indeed the correct answer, as justified by Lemma 4.2.4 below. First we shall make a some definitions.

Definition 4.2.2. Suppose $X = \{x_1, \ldots, x_n\}$ is a set such that $|X| = n$.

(1) A **permutation** (or **ordering**) of X is a tuple $(y_1, \ldots, y_n) \in X^n$ such that for each $i, j \in \{1, \ldots, n\}$, if $y_i = y_j$, then $i = j$.

(2) We define the set $\mathcal{O}(X)$ of all permutations of X to be:

$$\mathcal{O}(X) \;:=\; \big\{(y_1, \ldots, y_n) \in X^n : (y_1, \ldots, y_n) \text{ is a permutation of } X\big\} \;\subseteq\; X^n.$$

Clearly $|\mathcal{O}(X)| \leq |X^n| = n^n$.

Example 4.2.3. Suppose $X = \{a, b, c\}$ with $|X| = 3$. Then the collection of all permutations of X is

$$\mathcal{O}(X) \;=\; \big\{(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)\big\}$$

Thus $|\mathcal{O}(X)| = 6 = 3!$.

Lemma 4.2.4. *Suppose $|X| = n$. Then the total number of permutations of X is $n!$, i.e., $|\mathcal{O}(X)| = n!$.*

Proof. We will actually prove this using the *Addition Principle* and induction. The statement we will prove by induction is:

$$P(n): \quad \text{“Every set } X \text{ of size } n \text{ has } n! \text{ total permutations.”}$$

To emphasize a point about $n = 0$, we will prove two base cases:

Base Case: ($n = 0$) Suppose X has size 0. Then $X = \emptyset$. By convention, the empty-tuple () is considered an ordering of the emptyset. Thus there is only one ordering, so $|\mathcal{O}(\emptyset)| = 1 = 0!$.

Base Case: ($n = 1$) Suppose $X = \{x_1\}$ has size 1. Then (x_1) is the only permutation so the total number of permutations in this case is $|\mathcal{O}(X)| = 1! = 1$.

Inductive Step: Suppose for some $n \geq 1$ we know that $P(n)$ is true. We want to show that $P(n+1)$ is true. Let $X = \{x_1, \ldots, x_{n+1}\}$ be an arbitrary set of size $n+1$. We can partition $\mathcal{O}(X)$ into $n+1$ disjoint subsets. For each $i \in \{1, \ldots, n+1\}$ define

$$\mathcal{O}(X)_i \ := \ \big\{(y_1, \ldots, y_{n+1}) \in \mathcal{O}(X) : y_1 = x_i\big\},$$

i.e., $\mathcal{O}(X)_i$ is the set of all orderings where x_i is first. This gives us a partition of $\mathcal{O}(X)$:

$$\mathcal{O}(X) \ = \ \mathcal{O}(X)_1 \cup \cdots \cup \mathcal{O}(X)_{n+1} \quad \text{(disjoint union).}$$

Next note that $\mathcal{O}(X)_i$ is really the cartesian product

$$\mathcal{O}(X)_i \ = \ \{x_i\} \times \mathcal{O}(X \setminus \{x_i\})$$

since every permutation of X starting with x_1 is the same thing as x_1 followed by a permutation of $X \setminus \{x_i\}$, so it has the same cardinality as the set $\mathcal{O}(X \setminus \{x_i\})$ which by $P(n)$ has size $n!$. By the *Addition Principle*, we compute

$$|\mathcal{O}(X)| \ = \ \sum_{i=1}^{n+1} |\mathcal{O}(X)_i| \ = \ \sum_{i=1}^{n+1} n! \ = \ (n+1)n! \ = \ (n+1)!. \qquad \square$$

The next type of common counting question we would like to answer is exemplified by the following:

Example 4.2.5 (Committees)**.** Suppose a group has 100 people and they want to form a leadership committee formed by 7 people from the group.

How many possible committees can be formed?

We will see below that the answer is $\binom{100}{7}$. To answer this, we will consider a more general question.

Definition 4.2.6. Suppose $0 \leq k \leq n$ and X is a set such that $|X| = n$.

(1) A k-**combination** (or k-**subset**) of X is a set $Y \subseteq X$ such that $|Y| = k$.
(2) We denote the set of all k-combinations of X as

$$\mathcal{P}_k(X) \ := \ \{Y \subseteq X : |Y| = k\}.$$

The notation suggests that $\mathcal{P}_k(X)$ is a certain “slice” of the full powerset $\mathcal{P}(X)$ where we keep only the k-subsets. Indeed, these sets give us a partition of the powerset:

$$\mathcal{P}(X) \ = \ \mathcal{P}_0(X) \cup \mathcal{P}_1(X) \cup \cdots \cup \mathcal{P}_n(X).$$

The general question we want to ask is:

How many k-combinations does an n-element set have?

This is answered by the following lemma:

Lemma 4.2.7. *Suppose $0 \leq k \leq n$ and X is a set of size n. Then the total number of k-combinations of X is $\binom{n}{k}$, i.e., $|\mathcal{P}_k(X)| = \binom{n}{k}$.*

Proof. We will prove this by induction, the *Addition Principle*, and Pascal's Rule. The statement we will prove by induction is:

$$P(n): \quad \text{“For every } X \text{ with } |X| = n, \text{ and every } 0 \leq k \leq n,$$
$$\text{we have } |\mathcal{P}_k(X)| = \binom{n}{k}.\text{”}$$

Again we will prove two base cases.

Base Case: ($n = 0$) In this case, $0 = k = n$ and we are asking how many 0-element subsets are there of the emptyset $\emptyset$. Since $\emptyset \subseteq \emptyset$ is the only subset of $\emptyset$, and it has 0 elements, the answer is $1 = \binom{0}{0} = |\mathcal{P}_0(\emptyset)|$.

Base Case: ($n = 1$) In this case, there are two options for $0 \leq k \leq 1$. Either $k = 0$ or $k = 1$. Suppose $X = \{x\}$ is a 1-element set. Then

$$\mathcal{P}(\{x\}) \;=\; \underbrace{\{\emptyset\}}_{=\mathcal{P}_0(\{x\})} \;\cup\; \underbrace{\{\{x\}\}}_{=\mathcal{P}_1(\{x\})} \qquad \text{(disjoint union)}$$

Thus $|\mathcal{P}_0(X)| = 1 = \binom{1}{0}$ and $|\mathcal{P}_1(X)| = 1 = \binom{1}{1}$.

Induction Step: Suppose for some $n \geq 1$ we know that $P(n)$ is true. We will use this to prove $P(n+1)$. Let $X = \{x_1, \ldots, x_{n+1}\}$ be an arbitrary $n+1$-element set. Let $k \in \{0, \ldots, n+1\}$. We will consider several cases.

If $k = 0$, then $\mathcal{P}_0(X) = \{\emptyset\}$ and so $|\mathcal{P}_0(X)| = 1 = \binom{n+1}{0}$.

If $k = n+1$, then $\mathcal{P}_{n+1}(X) = \{X\}$ and so $|\mathcal{P}_{n+1}(X)| = 1 = \binom{n+1}{n+1}$.

Now suppose $0 < k < n+1$. Note that we can partition $P_k(X)$ into two disjoint subsets depending on whether the set contains x_1 or not:

$$A \;:=\; \{Y \in \mathcal{P}_k(X) : x_1 \in Y\} \quad \text{and} \quad B \;:=\; \{Y \in \mathcal{P}_k(X) : x_1 \notin Y\},$$

with $\mathcal{P}_k(X) = A \cup B$ (disjoint union). One can also check (Exercise 4.3.2) that the following two functions are bijections:

- $f : \mathcal{P}_{k-1}(X \setminus \{x_1\}) \to A$ given by $f(Y) := Y \cup \{x_1\}$ and
- $g : \mathcal{P}_k(X \setminus \{x_1\}) \to B$ given by $g(Y) := Y$.

Thus, by $P(n)$, the cardinalities of A and B are

$$|A| \;=\; |\mathcal{P}_k(X \setminus \{x_1\})| \;=\; \binom{n}{k} \quad \text{and} \quad |B| \;=\; |\mathcal{P}_{k-1}(X \setminus \{x_1\})| \;=\; \binom{n}{k-1}.$$

Thus by the *Addition Principle* and Pascal's Rule:

$$|\mathcal{P}_k(X)| \;=\; |A| + |B| \;=\; \binom{n}{k} + \binom{n}{k-1} \;=\; \binom{n+1}{k}. \qquad \square$$

We can now give a *combinatorial proof* of an identity established in Exercise 1.5.17:

Theorem 4.2.8. *Suppose X is a finite set such that $|X| = n$. Then the cardinality of its powerset is*

$$|\mathcal{P}(X)| \;=\; 2^n \;=\; \sum_{k=0}^{n} \binom{n}{k}.$$

Proof. Suppose $X = \{x_1, \ldots, x_n\}$ has size n. We will count the cardinality of $\mathcal{P}(X)$ in two different ways.

Method 1: To construct a specific $Y \subseteq X$, for each of the n elements x_i, we can choose "yes" or "no" whether we want $x_i \in Y$. Specifically, there is a bijection (see Exercise 4.3.3):

$$f : \mathcal{P}(X) \to \{0,1\}^n$$

defined by

$$f(Y) \;:=\; (\epsilon_1, \ldots, \epsilon_n) \quad \text{where for each } i \in \{1, \ldots, n\},\ \epsilon_i \;:=\; \begin{cases} 1 & \text{if } x_i \in Y \\ 0 & \text{if } x_i \notin Y. \end{cases}$$

Thus $|\mathcal{P}(X)| = |\{0,1\}^n| = 2^n$ by the Multiplication Principle.

Method 2: Using the Addition Principle, we partition $\mathcal{P}(X)$ into the various $\mathcal{P}_k(X)$'s and count:

$$|\mathcal{P}(X)| \;=\; |\mathcal{P}_0(X) \cup \cdots \cup \mathcal{P}_n(X)| \;=\; \sum_{k=0}^{n} |\mathcal{P}_k(X)| \;=\; \sum_{k=0}^{n} \binom{n}{k},$$

using Lemma 4.2.7 for the last step. □

Remark 4.2.9. Note that the above proof essentially gives another proof of the identity:

$$(\ddagger) \qquad 2^n \;=\; \sum_{k=0}^{n} \binom{n}{k}.$$

Of course, this was originally proved using the Binomial Theorem with $x = y := 1$. Instead, we proved it here by counting the set $\mathcal{P}(X)$ in two different ways, and knowing that we *must* get the same answer either way. Many identities involving binomial coefficients are like this, where we just find the right set and count it in two different (and possibly clever) ways.

We have one more type of general counting question that we want to address.

Example 4.2.10 (Track meet placements)**.** Suppose there is a track meet with 100 athletes competing in a certain event. Only the top 10 finalists get ranked 1st through 10th (the bottom 90 don't get ranked).

How many different rankings are possible?

This is a lot like a permutation of all 100 athletes, except that we stop after our first ten choices of who goes 1st through 10th. Thus, we guess that the answer is:

$$100 \cdot 99 \cdot 98 \cdot 97 \cdot 96 \cdot 95 \cdot 94 \cdot 93 \cdot 92 \cdot 91 \;=\; \frac{100!}{90!} \;=\; 62\,815\,650\,955\,529\,472\,000.$$

This is correct, as Lemma 4.2.13 shows.

Definition 4.2.11. Suppose $0 \leq k \leq n$ and X is a set such that $|X| = n$.

(1) A **k-permutation** (or **k-ordering**) of X is an ordering of a k-element subset of X, i.e., it is a tuple $(y_1, \ldots, y_k) \in X^k$ such that if $i \neq j$, then $y_i \neq y_j$.

(2) We denote the set of all k-permutations of X as

$$\mathcal{O}_k(X) \;:=\; \big\{(y_1, \ldots, y_k) \in X^k : (y_1, \ldots, y_k) \text{ is a } k\text{-permutation of } X.\big\}$$

Note that $\mathcal{O}(X) = \mathcal{O}_n(X)$.

Example 4.2.12. Suppose $X = \{a, b, c, d\}$. The set of all 2-permutations of X is

$$\begin{aligned}\mathcal{O}_2(X) \;&=\; \big\{(a,b),(a,c),(a,d),(b,a),(b,c),(b,d),\\ &\qquad (c,a),(c,b),(c,d),(d,a),(d,b),(d,c)\big\}\end{aligned}$$

Lemma 4.2.13. *Suppose* $0 \leq k \leq n$ *and* $|X| = n$. *The total number of* k-*permutations of* X *objects is*

$$|\mathcal{O}_k(X)| \;=\; n(n-1)\cdots(n-k+1) \;=\; \frac{n!}{(n-k)!}.$$

Proof. To motivate the proof, we ask the question "how does one create a k-permutation?" One reasonable answer is that given X, first one chooses a k-subset $Y \subseteq X$ with $|Y| = k$ and then gives it an ordering (i.e., picks an element of $\mathcal{O}(Y)$). This is what we will do.

First note that we can partition $\mathcal{O}_k(X)$ according to which k-elements of X are involved in the k-permutation, i.e.,

$$\mathcal{O}_k \;=\; \bigcup_{Y \in \mathcal{P}_k(X)} \mathcal{O}(Y) \quad \text{(disjoint union)}$$

(note, the union ranges over all subsets of Y of size k). Lemma 4.2.4 for each $Y \in \mathcal{P}_k(X)$ it follows that that $|\mathcal{O}(Y)| = k!$ since $|Y| = k$. Furthermore, Lemma 4.2.7 tells us that $|\mathcal{P}_k(X)| = \binom{n}{k}$. Thus

$$\begin{aligned}|\mathcal{O}_k(X)| \;&=\; \left|\bigcup_{Y \in \mathcal{P}_k(X)} \mathcal{O}(Y)\right| \;=\; \sum_{Y \in \mathcal{P}_k(X)} |\mathcal{O}(Y)| \quad \text{by Addition Principle}\\ &=\; \sum_{Y \in \mathcal{P}_k(X)} k! \;=\; k! \sum_{Y \in \mathcal{P}_k(X)} 1 \;=\; k!|\mathcal{P}_k(X)|\\ &=\; k!\binom{n}{k} \;=\; \frac{n!}{(n-k)!}.\end{aligned}$$

□

4.3. Exercises

Exercise 4.3.1. How many integers are there in the set $\{1, 2, 3, \ldots, 1000\}$ that are not divisible by either 6 or 8?

Exercise 4.3.2. Show that the functions $f : \mathcal{P}_{k-1}(X \setminus \{x_1\}) \to A$ and $g : \mathcal{P}_k(X \setminus \{x_1\}) \to B$ from the proof of Lemma 4.2.7 are bijections.

Exercise 4.3.3. Show that the function $f : \mathcal{P}(X) \to \{0,1\}^n$ defined in the proof of Theorem 4.2.8 is a bijection.

Exercise 4.3.4. Suppose A and B are sets such that $|A| = 50$ and $|B| = 100$.

(1) how many total functions $f : A \to B$ are there?

(2) how many *one-to-one* functions $f : A \to B$ are there? A function $f : A \to B$ is one-to-one if for all $x, y \in A$, if $f(x) = f(y)$, then $x = y$.

Exercise 4.3.5. If 12 people are to be divided into 3 committees of respective sizes 3, 4, and 5, how many divisions are possible?

Exercise 4.3.6. A student has to sell 2 books from a collection of 6 math, 7 science, and 4 economics books. How many choices are possible if

(1) both books are to be on the same subjects?

(2) the books are to be on different subjects?

Exercise 4.3.7. Seven blue and four red balls are to be arranged in order. How many ways can this be done if

(1) The blue balls are distinguishable (e.g. numbered) as are the red balls.
(2) Blue balls are distinguishable, but the red balls are identical.
(3) The balls of each color are indistinguishable.

Exercise 4.3.8. How many ways can we distribute n balls among k bags if

(1) the balls and bags are distinguishable (e.g. numbered).
(2) the bags are distinguishable; the balls are not.
(3) balls and bags are distinguishable, but the bags can contain at most one ball (necessarily, $k \geq n$).
(4) the bags are distinguishable, the balls are not, and the bags can contain at most one ball

Exercise 4.3.9. A candy factory has an endless supply of red, orange, yellow, green, blue, and violet jelly beans. The factory packages the jelly beans into jars of 100 jelly beans each. One possible color distribution, for example, is a jar of 58 red, 22 yellow, and 20 green jelly beans. As a marketing gimmick, the factory guarantees that no two jars have the same color distribution. What is the maximum number of jars the factory can produce.

Exercise 4.3.10. How many ways can we order the twenty-six letters of the alphabet together with seven (indistinguishable) # symbols?

Exercise 4.3.11. This problem involves counting.

(1) Suppose there are 50 customers at a supermarket and there are 5 checkout lines. How many ways can all 50 customers get into these 5 lines? The order in each line matters and lines are allowed to be empty.
(2) In how many ways can 5 identical chess pieces be placed on an 8×8 chessboard so that four of them form the corners of a rectangle with sides parallel to the sides of the board?

CHAPTER 5

Sequences

5.1. Sequences and recurrence relations

So far we have only encountered *sequences* at a casual level. Informally, a *sequence* is some list of objects indexed by natural numbers (or integers). We now give the formal definition:

Definition 5.1.1. A **sequence** s is a function whose domain D is subset of $\mathbb{Z}$.

As this is a very general definition, some remarks are in order:

Remark 5.1.2. (1) Given a sequence $s : D \to X$, we will often denote it by $\{s_n\}_{n \in D}$, where $s_n := s(n)$. In particular, when using sequences we will use the more common subscript notation "s_n" instead of usual function notation "$s(n)$" to emphasize the role of D as an **index set**.

(2) Most of the time, the domain D of a sequence is either a finite set of the form $\{0, 1, \ldots, n\}$ or $\{1, \ldots, n\}$, or an infinite set of the form $\mathbb{N}$ or $\mathbb{N} \setminus \{0\}$. Sequences where D is finite are called **finite sequences** and sequences where D is infinite are called **infinite sequences**.

(3) We put no restriction on what the codomain of a sequence is allowed to be. In general we might wish to consider sequences of real numbers (sequences of the form $s : D \to \mathbb{R}$), sequences of rational numbers (sequences of the form $s : D \to \mathbb{Q}$), and really for any set X we might wish to consider sequences in X (sequences of the form $s : D \to X$). In this class we will primarily consider sequences of numbers of some kind.

The following is a famous example of the type of sequence we wish to study:

Example 5.1.3 (Tower of Hanoi)**.** Suppose we have three vertical pegs and n disks of decreasing radius. At the start of game the disks have the initial setup:

(Start) All n disks are placed on the first peg. Disks of smaller radius are above disks of bigger radius.

The objective of the game is to move all n disks to the third peg subject to the following two rules:

(Rule 1) One "move" consists of moving the top-most disk from one peg to another peg.

(Rule 2) At no point can a disk of larger radius be placed above a disk of smaller radius.

Associated to this game is a sequence $(c_n)_{n \geq 1}$ in $\mathbb{N}$ we wish to study:

$$c_n \; := \; \text{number of moves it takes to move all } n \text{ disks to the third peg.}$$

Clearly $c_1 = 1$. Indeed, if there is only one disk, then we can legally move it directly to the third peg in one move. What about c_n for arbitrary $n \geq 1$?

For this, we need to think *inductively/recursively.* Suppose for some $n \geq 1$ we already know c_n. Moreover, suppose for this n we already have some method of legally moving n disks in c_n many moves. Then we can use this to move $n+1$ disks:

(Step 1) Move the top n disks from the first peg to the second peg (c_n total moves).

(Step 2) Now the first peg has only the largest $n+1$st disk on it. Move this directly to the third peg (1 total move).

(Step 3) Move the n disks from the second peg to the third peg on top of the largest $n+1$st disk (c_n total moves).

Thus, we can accomplish legally moving $n+1$ disks in $2c_n + 1$ moves. In other words, $c_{n+1} = 2c_n + 1$. In the parlance of this chapter, we summarize this by saying that the sequence $(c_n)_{n\geq 1}$ satisfies the following *recurrence relation*:

- (Initial condition) $c_1 = 1$
- (Recurrence relation) $c_{n+1} = 2c_n + 1$ for $n \geq 1$.

There are many variants of how a sequence might be recursively defined, but in general it takes the following form:

Definition 5.1.4. A sequence $(c_n)_{n\geq 1}$ is **recursively defined** if we have the following:

(1) One or more **initial conditions**, i.e., for some fixed $N \geq 1$ we are told the specific values of $c_1, c_2, \ldots, c_N$ (usually $N = 1$ or 2 for us).

(2) A **recurrence relation**: for each $n \geq N$ there is a function f_n such that

$$c_{n+1} \;=\; f_n(c_1, \ldots, c_n)$$

i.e., the $n+1$st value of the sequence is completely determined by the first n values of the sequence in a way we understand. Note: the function f_n is allowed to depend on $c_1, \ldots, c_n$, but it doesn't actually have to reference all of them. Indeed, in the Tower of Hanoi example above, the function giving c_{n+1} only depends on c_n (which we view as a special case of depending on $c_1, \ldots, c_n$).

Here are the main things one might want to do with a recursively defined sequence:

(I) *Study its properties.* This is vague, but the point is that from the recursive definition alone you can usually prove many things about c_n using induction, even if you don't yet have a full understanding of the sequence.

(II) *Find an explicit formula for c_n.* Initially, to compute c_n you might have to first compute $c_1, \ldots, c_{n-1}$, which could be labor-intensive. It's often nice to have a formula for c_n which can be computed from the value of n alone, without knowing all the previous values in the sequence. For example, we will show in the Tower of Hanoi example that

$$c_n \;=\; 2^n - 1 \quad \text{for every } n \geq 1,$$

which in many ways is a "better" formula for c_n than the recursive definition (see Example 5.2.2 below).

(III) *Study its asymptotics as $n \to \infty$.* For instance, does $\lim_{n\to\infty} c_n$ exist? If $c_n \to \infty$ as $n \to \infty$, how fast or slow does c_n grow? These questions involve analysis and we won't address them in this class. However, it's good to be aware that this type of information about a sequence is also very desirable. This is because in many applications when n is really large and c_n is also very large, it is often sufficient for practical purposes to have a good estimate of the value of c_n, as opposed to the exact value of c_n itself.

5.2. Solving recurrence relations I: first-order linear (in)homogeneous recurrence relations

In this section we will show how to *solve* (i.e., *find an explicit formula for*, as in (II) above) several very simple recurrence relations of a general form.

Definition 5.2.1. We say that a recursively defined sequence $(a_n)_{n\geq 1}$ is **first-order linear** if it has a recursive definition of the following form:

(i) the value of a_1 is given as an initial condition,

(ii) there exists $c, d \in \mathbb{R}$ such that for every $n \geq 1$,

$$a_{n+1} \;=\; ca_n + d.$$

If $d = 0$, then we say that the recurrence relation is **homogeneous**. Otherwise, we say that the recurrence relation is **inhomogeneous**.

The term *first-order* refers to the fact that the recursive definition for a_{n+1} in (ii) only depends on a_n (it's *first* predecessor) and not on any additional terms (like a_{n-1}, a_{n-2}, etc).

First-order linear recurrence relations can generally be solved from scratch with the following strategy (which might also work for other recurrence relations):

(1) Compute the first few terms in the sequence.

(2) Guess a general pattern for the nth term.

(3) Prove that your formula from (2) is correct by induction and using the original recursive definition of the sequence.

We will use this strategy to solve the Towers of Hanoi recurrence relation, then look at the general situation:

Example 5.2.2 (Towers of Hanoi)**.** The recursively defined sequence $(c_n)_{n\geq 1}$ given by

(i) $c_1 = 1$,

(ii) for every $n \geq 1$, $c_{n+1} = 2c_n + 1$,

satisfies the formula

$$c_n \;=\; 2^n - 1.$$

Solution. We begin by computing the first few terms:

$$\begin{aligned} c_1 &= 1 \\ c_2 &= 2 + 1 \\ c_3 &= 2(2+1) + 1 \;=\; 2^2 + 2^1 + 2^0 \\ c_4 &= 2(2^2 + 2^1 + 2^0) + 1 \;=\; 2^3 + 2^2 + 2^1 + 2^0. \end{aligned}$$

It looks like the general pattern is that the nth term is equal to

$$d_n \;=\; \sum_{k=0}^{n-1} 2^k \;=\; 2^n - 1.$$

We can prove this is true by induction on the following statement:

$$P(n): \quad \text{“}c_n = d_n\text{, i.e., } c_n = 2^n - 1.\text{”}$$

Base Case: If $n = 1$, then $c_n = 1$ and $d_n = 2^1 - 1 = 1$. Thus $P(1)$ is true.

Inductive Step: Suppose we know $P(n)$ is true for some $n \geq 1$. We will show $P(n+1)$ is true. Note that

$$\begin{aligned} c_{n+1} &= 2c_n + 1 \\ &= 2(2^n - 1) + 1 \quad \text{since } P(n) \text{ is true} \\ &= 2^{n+1} - 2 + 1 \\ &= 2^{n+1} - 1 \\ &= d_{n+1}. \end{aligned}$$

Thus $P(n+1)$ is true. □

We now look at the arbitrary situation:

Example 5.2.3. Suppose $(a_n)_{n\geq 1}$ is a recursively defined sequence with definition:

(1) a_1 is given,
(2) there are $c, d \in \mathbb{R}$ such that for every $n \geq 1$, $a_{n+1} = ca_n + d$.

Proof. We begin by writing down the first few terms:

$$\begin{aligned} a_1 &= a_1 \\ a_2 &= ca_1 + d \\ a_3 &= c(ca_1 + d) + d \;=\; c^2a_1 + (c+1)d \\ a_4 &= c(c^2a_1 + (c+1)d) + d \;=\; c^3a_1 + (c^2 + c + 1)d. \end{aligned}$$

We make a guess that the general form of the nth term is:

$$b_n \;=\; c^{n-1}a_1 + d\sum_{k=0}^{n-2} c^k.$$

In fact, this is correct, according to the next theorem. □

Theorem 5.2.4. *Suppose $(a_n)_{n\geq 1}$ is a recursively defined linear first-order (in)homogeneous equation with definition:*

(1) a_1 is given,
(2) there are $c, d \in \mathbb{R}$ such that for every $n \geq 1$, $a_{n+1} = ca_n + d$.

Then the nth term of the sequence can be explicitly computed as follows:

$$a_n \;=\; \begin{cases} c^{n-1}a_1 + d\left(\frac{c^{n-1}-1}{c-1}\right) & \text{if } c \neq 1, \\ c^{n-1}a_1 + (n-1)d & \text{if } c = 1. \end{cases}$$

Proof. See Exercise 5.4.2. □

5.3. Solving recurrence relations II: second-order linear homogeneous recurrence relations

In this section we will show how to solve the following type of recurrence relation:

Definition 5.3.1. We say that a recursively defined sequence $(a_n)_{n\geq 0}$ is **second-order linear homogeneous** if it has a recursive definition of the following form:

(i) the values of a_0, a_1 are given,

(ii) there exists $c_1, c_2 \in \mathbb{R}$ such that for every $n \geq 1$,

$$a_{n+1} \;=\; c_1 a_n + c_2 a_{n-1}.$$

The most famous example of this type of recurrence relation is the sequence of *Fibonacci numbers*:

Example 5.3.2 (Fibonacci numbers)**.** Consider the sequence of **Fibonacci numbers** defined by the recurrence:

(i) $F_0 := 0$ and $F_1 := 1$ (two initial conditions),
(ii) for every $n \geq 1$, $F_{n+1} := F_n + F_{n-1}$ (recurrence relation).

Ideally we would like to have a formula which computes F_n directly, i.e., without requiring us to compute $F_0, \ldots, F_{n-1}$ first. Of course, Exercise 1.5.12 already tells us the answer:

$$(\dagger) \qquad F_n \;=\; \frac{1}{\sqrt{5}}(\alpha^n - \beta^n), \quad \text{for every } n \geq 0,$$

where

$$\alpha \;:=\; \frac{1+\sqrt{5}}{2}$$
$$\beta \;:=\; \frac{1-\sqrt{5}}{2}.$$

However, this answer seems like we pulled a rabbit out of a habit. How does one actually *get* this answer if they don't guess it in advance? It turns out this can be done quite systematically utilizing the tools of calculus[1]:

Derivation. We will show how to derive (†) if you don't know it in advance. This will require several ingenious tricks that might be new to you, but in the subject of recursive sequences they are standard techniques:

Step 1: *Encode the sequence $(F_n)_{n\geq 0}$ into the DNA of a single object we can do calculus with.* This might sound vague, but what we mean by this is that we *define* some function[2] $F(x)$ by declaring that the coefficients of its Taylor series expansion (around $x = 0$) is precisely the sequence $(F_n)_{n\geq 0}$, i.e.,

$$F(x) \;:=\; \sum_{n=0}^{\infty} F_n x^n \;=\; 0 + x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^6 + 21x^7 + \cdots.$$

It might seem that we made the problem more complicated. However, provided the above power series has a positive radius of convergence[3], then we can recover the coefficients via the usual Taylor-series formula:

$$F_n \;=\; \frac{F^{(n)}(0)}{n!}, \quad \text{for every } n \geq 0.$$

Perhaps this doesn't seem much better, but at least it gives a possible alternative method of computing the nth coefficient F_n, which is what we want. [Note: at the moment, we have *zero* interest in the geometric properties of the graph of the

[1] You will never be asked to do partial fractions or anything involving Taylor/power series on an exam in this class.

[2] This function $F(x)$ is called the **generating function** for the sequence $(F_n)_{n\geq 0}$. See `https://en.wikipedia.org/wiki/Generating_function`.

[3] We will ignore issues of convergence, you'll study such things in an (complex) analysis course.

function F. It's role here is basically as a sneaky "data type" which allows us to encode an entire infinite sequence into one "object".]

Step 2: *Use the recursive definition of F_n to get a better description of $F(x)$.* First note that multiplying F by x and x^2 has the effect of shifting all of the coefficients:

$$\begin{aligned} xF(x) &= x\sum_{n=0}^{\infty} F_n x^n = \sum_{n=0}^{\infty} F_n x^{n+1} = \sum_{n=1}^{\infty} F_{n-1} x^n \\ x^2F(x) &= x^2\sum_{n=0}^{\infty} F_n x^n = \sum_{n=0}^{\infty} F_n x^{n+2} = \sum_{n=2}^{\infty} F_{n-2} x^n. \end{aligned}$$

The recursive definition of $(F_n)_{n\geq 0}$ then yields

$$F(x) - x = \sum_{n=2}^{\infty} F_n x^n = \sum_{n=2}^{\infty} F_{n-1}x^n + \sum_{n=2}^{\infty} F_{n-2}x^n = xF(x) + x^2F(x)$$

(the recursive definition is used in the second equality above, this also takes into account the initial conditions). This allows us to solve for the function $F(x)$:

$$F(x) = \frac{x}{1-x-x^2}.$$

The problem is a little more tractable now, we just need a way to compute the Taylor coefficients of F above.

Step 3: *Decompose F via partial fractions into a sum of functions which have nice Taylor expansions.* The first thing to do is to factor the denominator. The quadratic equation tells us that

$$x^2 + x - 1 = (x+\alpha)(x+\beta),$$

where α, β are defined as above. Thus we are looking for coefficients $A, B \in \mathbb{R}$ such that

$$\frac{-x}{(x+\alpha)(x+\beta)} = \frac{A}{x+\alpha} + \frac{B}{x+\beta}.$$

Cross-multiplying and equating the numerators gives us the system:

$$\begin{cases} A + B = -1 \\ A\beta + B\alpha = 0. \end{cases}$$

Which has unique solution $A = -(5+\sqrt{5})/10 = -\alpha/\sqrt{5}$ and $B = -(5-\sqrt{5})/10 = \beta/\sqrt{5}$. Thus

$$F(x) = -\frac{\alpha}{\sqrt{5}} \cdot \frac{1}{x+\alpha} + \frac{\beta}{\sqrt{5}} \cdot \frac{1}{x+\beta}$$

By Exercise 5.4.4 and linearity of the derivative, we get

$$\begin{aligned} F_n &= \frac{F^{(n)}(0)}{n!} = -\frac{\alpha}{\sqrt{5}}\frac{d^n}{dx^n}\left(\frac{1}{x+\alpha}\right)\Big|_{x=0}/n! + \frac{\beta}{\sqrt{5}}\frac{d^n}{dx^n}\left(\frac{1}{x+\beta}\right)\Big|_{x=0}/n! \\ &= -\frac{\alpha}{\sqrt{5}}\left(-\frac{1}{(-\alpha)^{n+1}}\right) + \frac{\beta}{\sqrt{5}}\left(-\frac{1}{(-\beta)^{n+1}}\right) = \frac{1}{\sqrt{5}}\left(-\frac{1}{(-\alpha)^n} + \frac{1}{(-\beta)^n}\right) \\ &= \frac{1}{\sqrt{5}}(\alpha^n - \beta^n), \end{aligned}$$

using $-1/\alpha = \beta$ and $-1/\beta = \alpha$. □

As it turns out, this is basically how the general case works:

Theorem 5.3.3. *Consider the second-order homogeneous linear equation:*

$$(A) \qquad a_{n+1} \;=\; c_1 a_n + c_2 a_{n-1}$$

Define the ***characteristic polynomial*** $p(x) := x^2 - c_1 x - c_2$. *Suppose* $p(x)$ *has roots*[4] r_1, r_2.

(1) *(Distinct roots) If* $r_1 \neq r_2$, *then equation (A) has two basic solutions:*
   (a) $(r_1^n)_{n\geq 0}$, *i.e., the sequence* $1, r_1, r_1^2, r_1^3, \ldots$, *and*
   (b) $(r_2^n)_{n\geq 0}$.

(2) *(Double root) If* $r_1 = r_2$, *then equation (A) has two basic solutions:*
   (a) $(r_1^n)_{n\geq 0}$, *and*
   (b) $(nr_1^n)_{n\geq 0}$, *i.e., the sequence* $0, r_1, 2r_1^2, 3r_1^3, \ldots$.

(3) *Given a sequence* $(a_n)_{n\geq 0}$ *which satisfies equation (A), there exists unique constants* $b, d \in \mathbb{R}$ *such that*

$$a_n \;=\; b \cdot (\textit{first basic solution}) + d \cdot (\textit{second basic solution}).$$

The constants b *and* d *are determined by the two initial conditions given with* $(a_n)_{n\geq 0}$. *Specifically, in (1) they are determined by the system:*

$$\begin{aligned} b + d &= a_0 \\ br_1 + dr_2 &= a_1 \end{aligned}$$

and in (2) they are determined by the system:

$$\begin{aligned} b &= a_0 \\ br_1 + dr_2 &= a_1. \end{aligned}$$

Note that (3) says that the set of solutions to equation (A) forms a two-dimensional vector space over $\mathbb{R}$.

Proof. (1) and (2) are done in Exercise 5.4.5. (3) requires basic linear algebra. □

The following example shows that, even if we are interested in sequences in $\mathbb{R}$, complex numbers are still convenient for giving explicit formulas:

Example 5.3.4. Consider the recurrence relation given by:

$$(\dagger) \qquad a_{n+1} \;=\; 0a_n - a_{n-1}.$$

It is clear that (†) has the following two sequences as solutions:

$$s_0 \;:=\; (1, 0, -1, 0, 1, 0, -1, \ldots) \quad \text{and} \quad s_1 \;:=\; (0, 1, 0, -1, 0, 1, 0, -1 \ldots)$$

By Theorem 5.3.3, both of these solutions are linear combinations of the two basic solutions corresponding to (†). We will show how this is.

First, define the characteristic polynomial $p(x) = x^2 + 1$. This has imaginary roots $\pm i$:

$$x^2 + 1 \;=\; (x - i)(x + i).$$

Since these roots are distinct, it gives two basic solutions $(i^n)_{n\geq 0}$ and $\big((-i)^n\big)_{n\geq 0}$. We will show that the solution s_0 is a linear combination of these two solutions. We are looking for $b, d \in \mathbb{R}$ such that

$$s_{0,n} \;=\; bi^n + d(-i)^n,$$

[4] These roots in general could be complex numbers in $\mathbb{C}$, but most of the time for us they'll be in $\mathbb{R}$.

where $s_{0,n}$ is the nth term of s_0. In particular, for the first two terms ($n = 0$ and $n = 1$) this gives the system:

$$\begin{aligned} b + d &= 1 \\ bi - di &= 0. \end{aligned}$$

Multiplying the bottom equation by i and then adding the two equations yields $2d = 1$, so $d = 1/2$. Furthermore, it follows that $b = 1/2$ as well. Thus

$$s_{0,n} = \frac{1}{2}\big(i^n + (-i)^n\big).$$

This illustrates how oscillation in *real* sequences can be explained by geometric progressions of *complex* numbers. We will not explore this idea any further.

Here is an example of the *Double root* case:

Example 5.3.5. Solve the following recurrence relation:

(i) $d_0 = 1$, $d_1 = 1$
(ii) for every $n \geq 1$, $d_{n+1} = 4d_n - 4d_{n-1}$.

Solution. First we define the characteristic polynomial:

$$p(x) = x^2 - 4x + 4.$$

This factors as $p(x) = (x - 2)^2$ (by inspection or the quadratic equation). Thus $r_1 = r_2 = 2$, so we are in the *Double root* case of Theorem 5.3.3. Thus the two basic solutions are $(2^n)_{n\geq 0}$ and $(n2^n)_{n\geq 0}$. Next, we use the initial conditions to figure out what linear combination of the two basic solutions is the solution to our specific recurrence relation. This gives us the system:

$$\begin{aligned} b &= 1 \\ 2b + 2d &= 1 \end{aligned}$$

Thus $b = 1$ and $d = -1/2$. We conclude that

$$d_n = 2^n - n2^{n-1}$$

is the solution to the recurrence relation we are looking for. □

5.4. Exercises

Exercise 5.4.1 (The Ackermann function)**.** The **Ackermann function** is a very important function in theoretical computer science and logic. It is a two-variable function $A : \mathbb{N}^2 \to \mathbb{N}$ defined recursively by the following conditions:

(i) $A(0, y) = y + 1$ for every $y \in \mathbb{N}$,
(ii) $A(n + 1, 0) = A(n, 1)$ for every $n \in \mathbb{N}$,
(iii) $A(n + 1, y + 1) = A\big(n, A(n + 1, y)\big)$ for every $n, y \in \mathbb{N}$.

The theoretical importance of the Ackermann function is the following: For any *primitive recursive* function $F : \mathbb{N} \to \mathbb{N}$, there is a fixed $n_F \in \mathbb{N}$ such that $F(x) \leq A(n_F, x)$ for every $x \in \mathbb{N}$ (here, a *primitive recursive* function is essentially any function that can be built up from constants, basic arithmetic $+, \cdot$ operations, composition, and *one-variable* recursive definitions with other primitive recursive functions, the specifics don't really matter for this problem. The point is that it's a large class of functions, but the Ackermann function is capable of growing faster than all of them! This shows that *two-variable* recursion is way more powerful than *one-variable* recursion). The following properties will give you practice with recursive definitions and induction. Prove the following:

(1) For every $n, x \in \mathbb{N}$, $A(n,x) < A(n+1,x)$.
(2) For every $n, x \in \mathbb{N}$, $A(n,x) < A(n,x+1)$.
(3) For every $n, x, y \in \mathbb{N}$, $A(n,x+y) \geq A(n,x) + y$. Hint: do induction first on n, then on y.
(4) For every $n, y \in \mathbb{N}$, if $n \geq 1$, then $A(n+1,y) > A(n,y) + y$. Hint: do a similar type of double-induction as in (3).
(5) For every $n, y \in \mathbb{N}$, $A(n+1,y) \geq A(n,y+1)$. Hint: do induction on y.
(6) For every $n, y \in \mathbb{N}$, $2A(n,y) < A(n+2,y)$. Hint: for $n > 0$ use (3), (4), and (5) above.
(7) For every $n, x, y \in \mathbb{N}$, if $x < y$, then $A(n,x+y) \leq A(n+2,y)$. Hint: do induction on n. In the inductive step, consider two cases separately: $x = y$ and $x < y$.

Exercise 5.4.2. Prove Theorem 5.2.4.

Exercise 5.4.3. Suppose $(a_n)_{n\geq 0}$ is a recursively defined sequence with recursive definition:

(i) $a_0 = 1$,
(ii) For every $n \geq 0$, $a_{n+1} = 2(n+1)a_n$

Solve this recurrence relation, i.e., find an explicit formula for the nth term and verify your formula is correct by induction.

Exercise 5.4.4. Fix $\alpha \in \mathbb{R}$ such that $\alpha \neq 0$, and define the function:

$$f(x) \ := \ \frac{1}{x-\alpha}$$

(this function is defined $\mathbb{R} \setminus \{\alpha\} \to \mathbb{R}$. For this problem, the relevant feature is that it is infinitely differentiable on some tiny interval containing $x = 0$). Prove the following:

(1) For every $n \geq 0$:

$$f^{(n)}(x) \ = \ (-1)^n \frac{n!}{(x-\alpha)^{n+1}}.$$

Here $f^{(n)}$ denotes the nth derivative of f, wherever it may be defined.

(2) For every $n \geq 0$:

$$\frac{f^{(n)}(0)}{n!} \ = \ -\frac{1}{\alpha^{n+1}}.$$

Exercise 5.4.5. Consider the second-order homogeneous linear equation:

$$\text{(A)} \qquad a_{n+1} \ = \ c_1 a_n + c_2 a_{n-1}.$$

Define the characteristic polynomial $p(x) := x^2 - c_1 x - c_2$.

(1) Suppose $p(r) = 0$, i.e., r is a root of p. Verify that the sequence $(r^n)_{n\geq 0}$ is a solution to (A).
(2) Suppose $p(x) = (x-r)^2$, i.e., r is a double root of p. Verify that the sequence $(nr^n)_{n\geq 0}$ is also a solution to (A).

Exercise 5.4.6. The **Lucas numbers** are a sequence $(\ell_n)_{n\geq 0}$ satisfying the following second-order linear homogeneous relation:

(i) $\ell_0 = 2$, $\ell_1 = 1$,
(ii) for $n \geq 1$, $\ell_{n+1} = \ell_n + \ell_{n-1}$.

Prove the following:

1. For $n \geq 1$, $\ell_n = F_{n-1} + F_{n+1}$, where $(F_n)_{n \geq 0}$ is the sequence of Fibonacci numbers.
2. For $n \geq 0$, $\sum_{k=0}^{n} \ell_k^2 = \ell_n \ell_{n+1} + 2$.

Exercise 5.4.7. Solve each of the following recurrence relations:

(1) Give an explicit formula for the nth term of the sequence $(a_n)_{n \geq 0}$ which has recursive definition:
   (i) $a_0 = 4$, $a_1 = 10$
   (ii) for $n \geq 1$, $a_{n+1} = 2a_n + 8a_{n-1}$.

(2) Do the same thing for the sequence $(b_n)_{n \geq 0}$ given by:
   (i) $b_0 = 5$, $b_1 = 16$,
   (ii) for $n \geq 1$, $b_{n+1} = 7b_n - 10b_{n-1}$.

Exercise 5.4.8. The following question is about straight lines drawn in $\mathbb{R}^2$.

1. n straight lines are drawn on the plane, no two being parallel and no three intersecting at one point. How many intersection points are there in this configuration?
2. What is the largest number of parts into which n straight lines can subdivide the plane?

CHAPTER 6

Graphs and trees

6.1. Graphs

In this class we will only consider the simplest type of graph: an *undirected simple graph.* Since we will not talk about other types of graphs (directed graphs, graphs with self-loops, graphs with parallel edges, graphs with weights attached to each edge, etc.) we will use the term *graph* to mean the narrow definition which we will give below. However you should be aware that in other contexts the definition of "graph" might be different and more general.

Definition 6.1.1. A **graph** is a pair $G = (V, E)$ consisting of a set V of **vertices** and a set $E \subseteq \mathcal{P}_2(V)$ of **edges**. (Recall that $\mathcal{P}_2(V)$ is the set of 2-subsets of V, i.e., the set of all *unordered* pairs from V).

Before we go any further, here is an example of a graph:

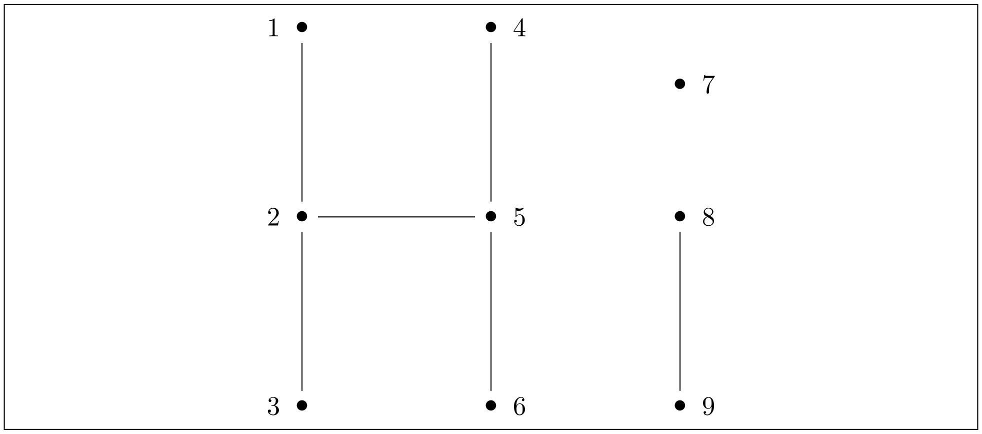

Figure 6.1: A graph with vertex set $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and edges $E = \big\{\{1, 2\}, \{2, 3\}, \{2, 5\}, \{4, 5\}, \{5, 6\}, \{8, 9\}\big\}$

Notation 6.1.2. By convention, we will denote an edge $\{v, w\}$ instead as vw, when no confusion should arise.

Here are some more basic graph-theory definitions:

Definition 6.1.3. Let $G = (V, E)$ be a graph.

(1) A vertex $v \in V$ and an edge $e \in E$ are said to be **incident** if $v \in e$, i.e., if v is one of the endpoints of e.
(2) Two vertices $v_0, v_1 \in V$ are **adjacent**, or are **neighbors**, if $v_0v_1 \in E$, i.e., if there is an edge connecting them.

(3) The **order** $|G|$ of G is the total number of vertices, i.e., $|G| = |V|$.

(4) Given a vertex $v \in V$, we define $E(v)$ to be the set of all edges incident to v, i.e.,

$$E(v) \; := \; \{e \in E : v \in e\}.$$

(5) Given a vertex $v \in V$, we define $N(v)$ to be the set of all neighbors of v, i.e.,

$$N(v) \; := \; \{w \in V : vw \in E\}$$

(6) Given a vertex $v \in V$, we define the **degree** of v to be the total number of neighbors (equivalently, number of incident edges) that v has, i.e.,

$$d(v) \; := \; \#N(v) \; = \; \#E(v)$$

Here are some examples of special graphs which have their own names.

Example 6.1.4. (1) A **complete graph** on n vertices, is a graph $G = (V, E)$ such that $|V| = n$ and $E = \mathcal{P}_2(V)$, i.e., it contains every possible edge between pairs of vertices. We denote a complete graph on n vertices as K_n. Figure 6.2 shows an example of a complete graph on 4 vertices.

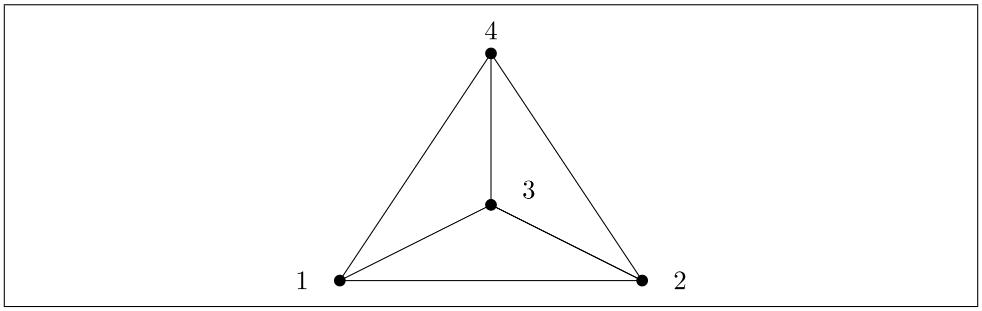

Figure 6.2: The complete graph K_4 with vertex set $V = \{1, 2, 3, 4\}$

(2) A **bipartite graph** is a graph $G = (V, E)$ such that the vertex set can be partitioned into two classes $V = V_1 \cup V_2$ such that each edge $e \in E$ is of the form $e = v_1 v_2$ where $v_1 \in V_1$ and $v_2 \in V_2$.

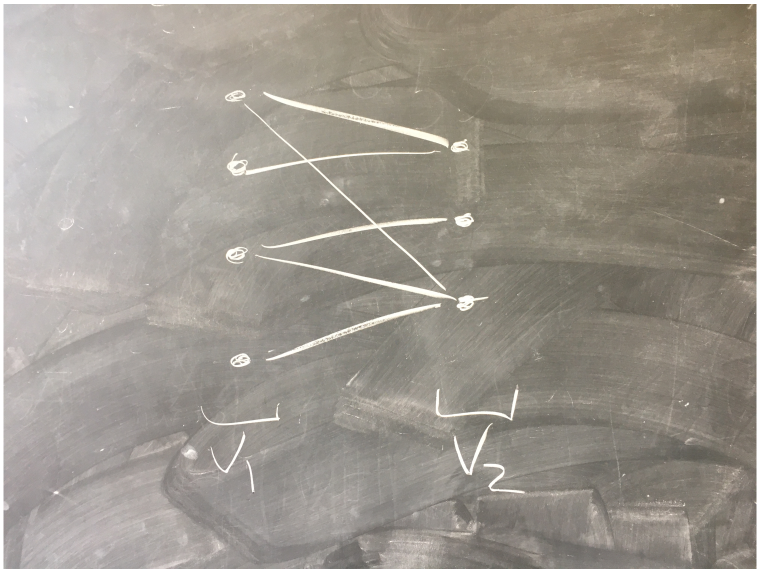

Figure 6.3: An example of a bipartite graph with partition $V = V_1 \cup V_2$

We say a bipartite graph is a **complete bipartite graph** if it contains all possible edges between V_1 and V_2. Given $m, n \geq 1$, we define $K_{m,n}$ to be the complete bipartite graph with

$$\begin{aligned} V &= \underbrace{\{u_1, \ldots, u_m\}}_{V_1} \cup \underbrace{\{v_1, \ldots, v_n\}}_{V_2} \\ E &= \{u_i v_j : i = 1, \ldots, m, j = 1, \ldots, n\}. \end{aligned}$$

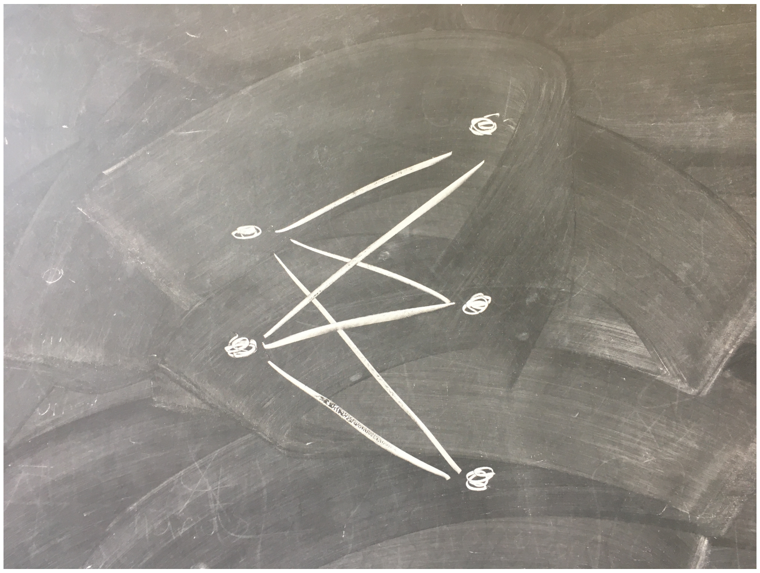

Figure 6.4: The complete bipartite graph $K_{2,3}$

The following observation is elementary, but it is the first result of the following form: a *global* conclusion (# of total odd-degree vertices) can be obtained from *local* information (degrees at each vertex).

Handshake Lemma 6.1.5. *Suppose $G = (V, E)$ is a graph. Then*

(1) $\sum_{v \in V} d(v) \;=\; 2|E|$,

(2) thus, the number of odd-degree vertices is even.

[Note: (2) can be interpreted as saying: at a party where guests greet other guests with handshakes, the total number of people that shook hands an odd number of times is even.]

Proof. (1) This follows from the observation that if you sum each degree of each vertex, then you are double-counting every edge. In more detail:

$$\begin{aligned}\sum_{v\in V} d(v) &= \sum_{v\in V} \#E(v)\\ &= \sum_{v\in V}\sum_{e\in E}\begin{cases}1 & \text{if } v\in e\\ 0 & \text{if } v\notin e\end{cases}\\ &= \sum_{e\in E}\sum_{v\in V}\begin{cases}1 & \text{if } v\in e\\ 0 & \text{if } v\notin e\end{cases}\\ &= \sum_{e\in E} 2\\ &= 2|E|,\end{aligned}$$

using in the fourth equality that each edge contains exactly two vertices.

(2) This is because if an odd number of vertices had odd degree, the sum in (1) would be odd. In more detail, taking the equality mod 2 gives:

$$\begin{aligned}0 \;\equiv\; 2|E| \;\equiv\; \sum_{v\in V} d(v) &\equiv \sum_{\substack{v\in V,\\ d(v)\equiv 0 \pmod 2}} d(v) + \sum_{\substack{v\in V,\\ d(v)\equiv 1 \pmod 2}} d(v)\\ &\equiv \sum_{\substack{v\in V,\\ d(v)\equiv 0 \pmod 2}} 0 + \sum_{\substack{v\in V,\\ d(v)\equiv 1 \pmod 2}} 1\\ &\equiv \#\{v\in V : d(v) \text{ odd}\} \pmod 2.\end{aligned}$$

□

One of the things we are interested in is how connected the graph is globally. For this, the following is an essential definition:

Definition 6.1.6. Given a graph $G = (V, E)$, a **path** (specifically, a **path from v_0 to v_n**) is a finite sequence of vertices and edges

$$(v_0, e_1, v_1 \ldots, v_{n-1}, e_n, v_n) \quad (\text{for some } n \geq 0)$$

such that for each $i = 0, \ldots, n-1$, $e_{i+1} = v_i v_{i+1} \in E$ (i.e., consecutive vertices are connected). [Note: for each $v \in V$ we regard (v) to be a path from v to v of length zero. This convention is to ensure the equivalence relation defined in Definition 6.1.13 is actually reflexive.] The **length** of a path $(v_0, e_1, v_1 \ldots, v_{n-1}, e_n, v_n)$ is n, the number of edges traversed (counted with multiplicity).

If a path $P = (v_0, e_1, \ldots, e_n, v_n)$ has the property that $v_0 = v_n$, then we say that P is a **cycle**. We call a cycle of the form (v) a **trivial cycle**.

Definition 6.1.7. We say a graph $G = (V, E)$ is **connected** if for every $x, y \in V$ there is a path from x to y.

The Königsberg Bridge Problem 6.1.8. This is a problem solved by Euler in 1736[1]. Is there a cycle on the graph in Figure 6.5 which traverses each edge exactly once?

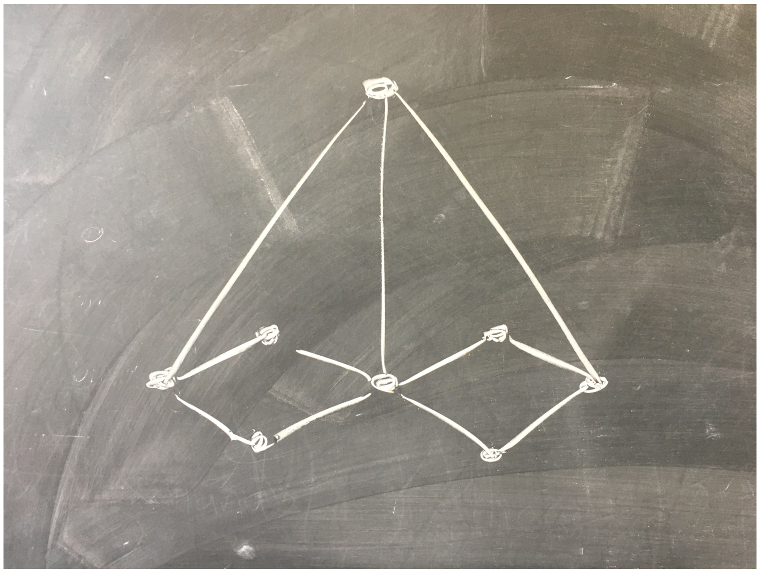

Figure 6.5: The Königsberg Graph

It's not obvious upon inspection whether there is or is not such a cycle on this graph. Perhaps after several attempts you will guess "no", but how can we *prove* there is no such cycle? This will be done in the Eulerian Graph Theorem 6.1.10 below.

First we will define precisely what type of cycle we are interested in:

Definition 6.1.9. Suppose $G = (V, E)$ is a graph.

(1) An **Euler cycle** is a cycle $C = (v_0, e_1, \dots, e_n, v_0)$ in G such that
   (a) each edge $e \in E$ occurs exactly once
   (b) each vertex $v \in V$ occurs at least once (this is implied by (a) if G is connected, we allow vertices to be repeated).

(2) We say G is **Eulerian** if it contains an Euler cycle.

Eulerian Graph Theorem 6.1.10. *Suppose $G = (V, E)$ is a graph. The following are equivalent:*

(1) G is an Eulerian graph.
(2) G is connected and for every $v \in V$, $d(v)$ is even.

For the proof we will need the following useful lemma:

[1] See `https://en.wikipedia.org/wiki/Seven_Bridges_of_K%C3%B6nigsberg` for a full discussion.

Boundary-Crossing Lemma 6.1.11. *Suppose $G = (V, E)$ is a graph, and $S \subseteq V$ some subset of vertices. If there are two vertices $v_0 \in S$ and $v_n \notin S$ and a path*

$$(v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$$

which connects v_0 to v_n, then there is some i such that $v_i \in S$ and $v_{i+1} \notin S$, i.e., the edge $e_{i+1} = v_i v_{i+1}$ crosses the "boundary" from being inside of S to outside of S. [See Figure 6.1.11]

Proof. Consider:

$$i \;=\; \max\{j : v_j \in S\}.$$

Then $i \geq 0$ and $i < n$ since $v_0 \in S$ and $v_n \notin S$. Thus $v_i \in S$ and $v_{i+1} \notin S$ by maximality of i. □

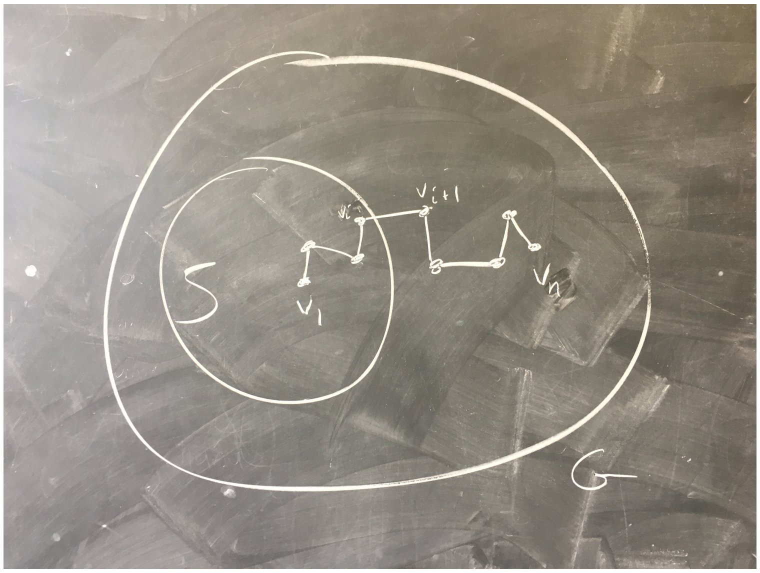

Figure 6.6: An illustration of the Boundary-Crossing Lemma

Proof of 6.1.10. (1)⇒(2) Suppose G is Eulerian with Euler cycle:

$$C \;=\; (v_0, e_1, \ldots, e_n, v_0).$$

(G connected) Suppose $x, y \in V$ are arbitrary. Since C is an Euler cycle, it contains every vertex. Thus there are $i, j \leq n-1$ such that $v_i = x$ and $v_j = y$. If $i \leq j$, then

$$P \;=\; (v_i, e_{i+1}, \ldots, e_j, v_j)$$

(i.e., the restriction of C to the part connecting x to y) is a path from v_i to v_j. If $j < i$, then the reverse of P is the desired path.

(even degrees) Let $x \in V$ be arbitrary. Then we must show $E(x)$ has even cardinality. In the Euler cycle C the vertex x occurs at least once, but possibly multiple times. Every edge in $E(x)$ occurs exactly once. Partition the set $E(x)$ into two subsets:

$$E(x)_{\text{ingoing}} \;:=\; \big\{e \in E(x) : \exists i \in \{1, \ldots, n\} \text{ such that } e = e_i \text{ in } C \text{ and } v_i = x\big\}$$
$$E(x)_{\text{outgoing}} \;:=\; \big\{e \in E(x) : \exists i \in \{1, \ldots, n\} \text{ such that } e = e_i \text{ in } C \text{ and } v_{i-1} = x\big\}$$

(using the convention that $v_n := v_0$), i.e., an edge is "ingoing" if it occurs immediately before x in the cycle, and "outgoing" if it occurs immediately after x in the cycle. Define the following function:

$$f : E(x)_{\text{ingoing}} \to E(x)_{\text{outgoing}}$$

by declaring for $e \in E(x)_{\text{ingoing}}$:

$$f(e) \ := \ e_{i+1} \quad \text{if there exists } i \in \{1, \ldots, n\} \text{ such that } e = e_i$$

(using the convention that $e_{n+1} := e_1$). Then f is a bijection (HW), and so $E(x)$ is even.

(2)⇒(1) Suppose G is connected and $\deg(x)$ is even for every $x \in V$. Consider the finite set:

$$\Sigma \ := \ \big\{P : P \text{ is a path in } G \text{ with no repeated edges}\big\}$$

Choose from Σ a path $P = (v_0, e_1, \ldots, e_n, v_n)$ of maximal length.

Claim. *P is a cycle, i.e., $v_0 = v_n$.*

Proof of claim. Suppose towards a contradiction that $v_0 \neq v_n$. Then v_0 is incident to an odd number of edges in P. Since $\deg(v_0)$ is even, there exists an edge $e = vv_0 \in E(v_0)$ not already occurring in P. Then

$$(v, e, v_0, e_1, \ldots, e_n, v_n)$$

is a strictly longer path which contains no repeated edges, a contradiction. □

We can now assume $v_0 = v_n$. Define $V(P)$ and $E(P)$ to be the sets of all vertices and edges occurring in P.

Claim. *P contains all vertices in V, i.e., $V = V(P)$.*

Proof of claim. Assume towards a contradiction that $V(P) \neq V$. Then there is $v' \in V \setminus V(P)$. Since G is connected, there is a path from v_0 to v'. By the Boundary-Crossing Lemma 6.6, there is a vertex $v_i \in V(P)$ and $v \in V \setminus V(P)$ such that $e = v_i v \in E$. This yields a longer path with no repeated edges:

$$(v, e, \underbrace{v_i, e_{i+1} \ldots, e_n, v_0, e_1, \ldots, e_i, v_i}_{\text{original } P\text{, starting and ending at } v_i})$$

This is a contradiction, see Figure 6.7. □

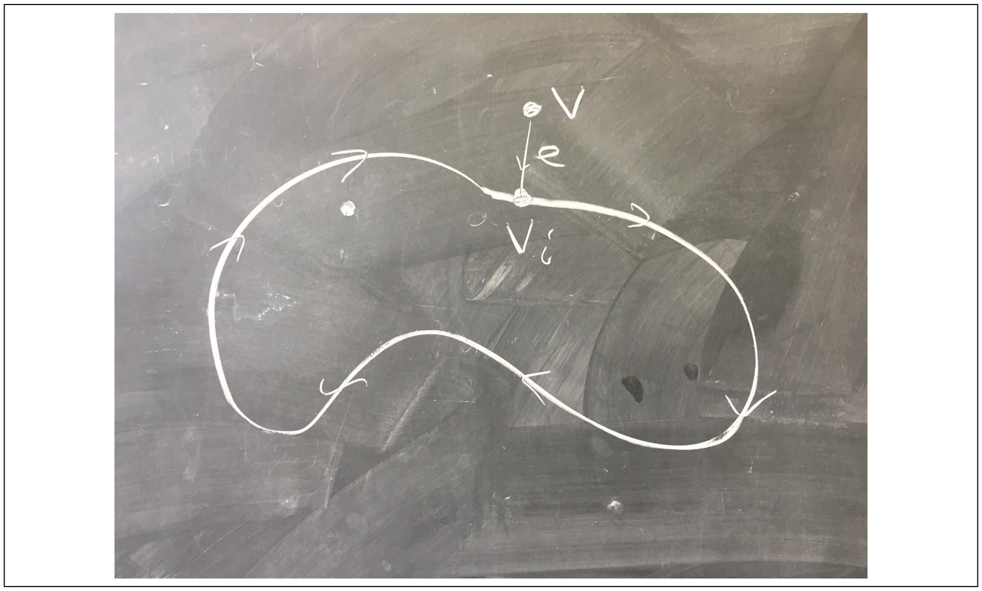

Figure 6.7: The proof that $V(P) = V$

Thus we may now assume $V(P) = V$.

Claim. *P contains every edge in E, i.e., $E(P) = E$.*

Proof of claim. Assume towards a contradiction that $E(P) \neq E$. Then there is some $e \in E \setminus E(P)$. Since $V = V(P)$, then e is of the form $e = v_i v_j$ for some $i < j$. This also yields a longer path with no repeated edges:

$$(v_i, e, \underbrace{v_j, v_{j+1}, \ldots, e_n, v_0, e_1, \ldots, e_j, v_j}_{\text{original } P\text{, starting and ending at } v_j})$$

This is a contradiction, see Figure 6.8. □

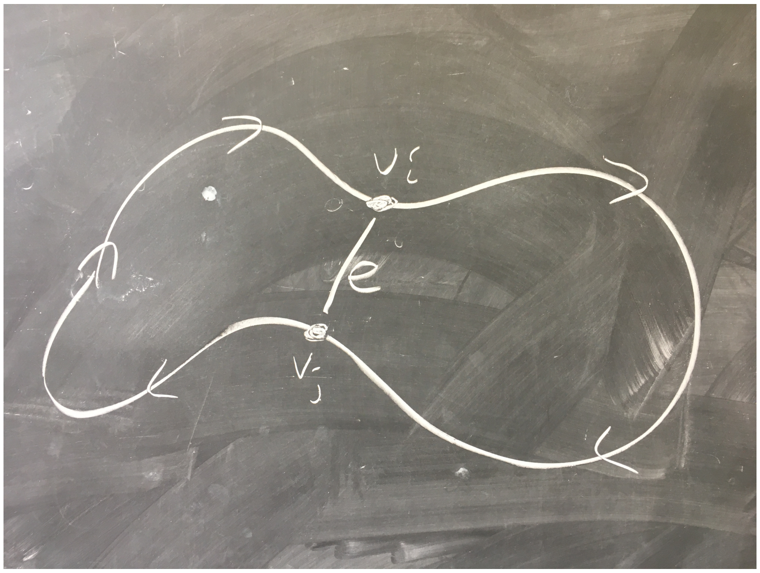

Figure 6.8: The proof that $V(P) = V$

We conclude that G is Eulerian. □

Definition 6.1.12. Suppose $G = (V, E)$ and $G' = (V', E')$ are graphs.

(1) We say that G' is a **subgraph** of G if $V' \subseteq V$ and $E' \subseteq E$.
(2) We say that G' is an **induced subgraph** of G is $V' \subseteq V$ and $E' = E \cap \mathcal{P}_2(V')$.

In other words, an induced subgraph of G is a graph G' which results from deleting some vertices of V to get a vertex-set V', but keeping all edges from the original graph involving only vertices in V'. In an arbitrary subgraph, you are allowed to further delete edges between vertices in V'.

Definition 6.1.13. Suppose $G = (V, E)$ is a graph.

(1) Define an equivalence relation $\sim$ on V by declaring:

$$x \sim y \;:\Longleftrightarrow\; \text{there is a path from } x \text{ to } y$$

Note: This relation is reflexive because for each $x \in V$, we regard (x) to be a path from x to x of length zero.

(2) This equivalence relation partitions V into subsets $V_1, \ldots, V_m$.
(3) The induced subgraphs on these subsets

$$(V_1, E_1), \ldots, (V_m, E_m)$$

are called the **connected components** of V. Note that

(a) $E_1 \cup \cdots \cup E_m = E$, and
(b) if G is connected, then there is only one connected component, namely $G = (V, E)$ itself.

6.2. Trees and forests

Definition 6.2.1. Let $G = (V, E)$ be a graph.

(1) We call a path $P = (v_0, e_1, \dots, e_n, v_n)$ in G a **simple path** if it does not repeat any edges (i.e., each edge $e \in E$ occurs at most once in P) .
(2) We call a cycle $C = (v_0, e_1, \dots, e_n, v_0)$ in G a **simple cycle** if it does not repeat any edges.
(3) We call G an **acyclic** graph (or a **forest**) if it does not contain any nontrivial simple cycles.
(4) We call G a **tree** if it is a connected acyclic graph (i.e., a connected forest).

In Figure 6.9 we illustrate a forest with four trees (i.e., each connected component is a tree).

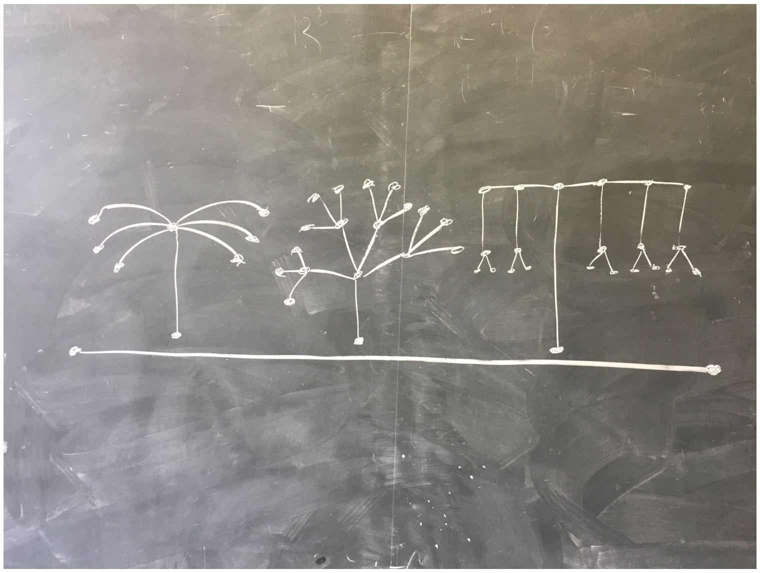

Figure 6.9: A forest with four trees

In terms of showing connectivity, simple paths are just as good as paths:

Lemma 6.2.2. *Suppose $G = (V, E)$ and $x, y \in V$ are such that there is a path in G from x to y. Then there is a simple path from x to y.*

Proof. Exercise. Hint: Prove the following statement by strong induction:

$$P(n): \quad \text{“For every graph } G\text{, for every } x, y \in G\text{,}$$
$$\text{if there is a path from } x \text{ to } y \text{ of length} \leq n\text{,}$$
$$\text{then there is a simple path from } x \text{ to } y\text{”}$$ □

Tree Characterization Theorem 6.2.3. *Suppose $G = (V, E)$ is a graph. The following are equivalent:*

(1) G is a tree.
(2) (Unique paths) for every $x, y \in V$, there exists a unique simple path from x to y.
(3) (Minimally connected) G is connected, however, for every $e \in E$, $G \setminus e := \big(V, E \setminus \{e\}\big)$ is disconnected.

(4) (Maximally acyclic) G is acyclic, however, for every $e \in \mathcal{P}_2(V) \setminus E$, $G + e := \big(V, E \cup \{e\}\big)$ contains a nontrivial simple cycle.
(5) (Euler's formula) G is connected and if $|G| \geq 1$, then $|V| = |E| + 1$

Before we proceed with our proof of 6.2.3, we need a definition and some lemmas.

Definition 6.2.4. Suppose $G = (V, E)$ is a graph. We call a vertex $v \in V$ a **leaf** (of G) if $d(v) = 1$.

Trees of order ≥ 2 are guaranteed to have at least two leaves:

Leaf Lemma 6.2.5. *Every tree with at least 2 vertices contains at least 2 leaves.*

Proof. This is essentially Exercise 8 on HW9. Hint: use the strategy employed in the proof of (2)⇒(1) in the Eulerian Graph Theorem 6.1.10. □

The following is essential to our inductive proof of 6.2.3:

Tree-Pruning Lemma 6.2.6. *Suppose $G = (V, E)$ is a graph, $v \in V$ is a leaf, and $e \in E$ is the unique edge incident to v. The following are equivalent:*
(1) G is a tree.
(2) $G \setminus v := \big(V \setminus \{v\}, E \setminus \{e\}\big)$ is a tree.

Proof. (1)⇒(2) Suppose G is a tree. Then G does not contain any nontrivial simple cycles so neither does $G \setminus v$. Furthermore, suppose $x, y \in V \setminus \{v\}$. Since G is connected, there is a path $P = (x = v_0, e_1, \ldots, e_n, v_n = y)$ from x to y in G. By Lemma 6.2.2 we may assume that P is a simple path. In particular, every vertex in P, except possibly x and y, have degree ≥ 2, and thus $\neq v$. Thus P is a path in $G \setminus v$. This shows that $G \setminus v$ is also connected.

(2)⇒(1) Suppose $G \setminus v$ is a tree. Adding in v and e can't create a nontrivial cycle since v and e can't be involved in such a cycle since v has degree 1. Thus G is acyclic. Since $G \setminus v$ is connected, so is G, since e connects the new vertex v to $G \setminus v$. □

Proof of 6.2.3. We will prove these equivalences by induction on the order of G:

$$P(n): \quad \text{“For every graph } G \text{ of order} \leq n, \text{(1)-(5) are equivalent.”}$$

Base Cases: For $n = 0$ the empty graph $(\emptyset, \emptyset)$ satisfies (1)-(5). Thus $P(0)$ is true. For $n = 1$, every graph of order 1 must be a single vertex: $G = (\{v\}, \emptyset)$. (1)-(5) are also all true for this graph (in particular, they are all equivalent).

Inductive Step: Assume for some $n \geq 1$ we know that $P(n)$ is true. We will prove $P(n+1)$. Let $G = (V, E)$ be a graph of order $n + 1$.

We will first prove that (1) implies (2)-(5). Suppose G is a tree. By the Leaf Lemma 6.2.5 there is a vertex $v \in V$ such that $d(v) = 1$. Let $e \in E$ be the unique edge incident to v. By the Tree-Pruning Lemma 6.2.6 the graph $G \setminus v$ is also a tree. In particular, $G \setminus v$ satisfies (2)-(5) by $P(n)$. We need to verify that G also satisfies (2)-(5):

(2) Suppose $x, y \in G$. If $x, y \in V \setminus \{v\}$, then the unique simple path from x to y in $G \setminus v$ is still the only simple path from x to y in G (any path that includes v or e but doesn't start or end at v can't be simple). Now suppose $x \in G \setminus v$. Furthermore, let $w \in V$ be such that $e = vw$. Then there is a unique path from x to w in $G \setminus v$. Continuing this path along e to v yields the unique path from x to v.

(3) If we remove the edge e, then v will not be connected to $V \setminus \{v\}$, since $d(v) = 1$. If we remove an edge from $V \setminus \{v\}$, then the graph $G \setminus v$ will become disconnected, by the inductive assumption. Then adding back in v and e to this disconnected graph can't connect it since $d(v) = 1$.

(4) Let $x \neq y \in V$ be such that $xy \notin E$. Since G is connected, there is a unique path from x to y. If we add in the edge xy, then we can create a nontrivial simple cycle with this new edge plus this path. [Note: this implication doesn't use the inductive hypothesis.]

(5) By (5) for $G \setminus v$, we know that $|V \setminus v| = |E \setminus e| + 1$. If we add in one vertex and one edge the equality is preserved and so $|V| = |E| + 1$.

Next we will prove that each of (2)-(5) separately implies (1).

(2)⇒(1) By the path assumption, G is connected. Furthermore, G cannot contain a nontrivial simple cycle, for if it did, this would give at least two simple paths connecting any two vertices on that simple cycle.

(3)⇒(1) G is also assumed to be connected here. We claim that G is acyclic. If G contained a nontrivial simple cycle, then we could delete one edge in that cycle and still have a connected graph, contradicting (3).

(4)⇒(1) We need to check that G is connected. Let $x, y \in V$ be two distinct vertices. We have two cases: (Case 1) suppose $xy \in E$. Then there is obviously a path from x to y. (Case 2) suppose $xy \notin E$. Then by assumption, the graph $G + xy$ must contain a nontrivial simple cycle, and this nontrivial simple cycle must contain xy. Deleting xy from this cycle yields a path connecting x and y.

(5)⇒(1) Suppose $|V| = |E| + 1 \geq 2$ and G is connected. By the Handshake Lemma 6.1.5 the sum of the degrees of all the vertices is $2|V| - 2$. Since $d(x) \geq 1$ for every $x \in V$, it follows that it cannot be the case that $d(x) \geq 2$ for every $x \in V$. Thus there is some $v \in V$ such that $d(v) = 1$ (i.e., v is a leaf). Deleting v and the edge adjacent to it yields a connected graph $G \setminus v$ satisfying $|V(G \setminus v)| = |E(G \setminus v)| + 1$, so $G \setminus v$ is a tree by $P(n)$. Thus G is also a tree by the Tree-Pruning Lemma 6.2.6. □

Definition 6.2.7. Suppose $G = (V, E)$ is a graph. A **spanning tree** of G is a subgraph $T = (V', E')$ of G such that:

(1) $V' = V$, i.e., T contains all the same vertices as G, and
(2) T is a tree.

Every connected graph has a spanning tree:

Spanning Tree Algorithm 6.2.8. *Suppose $G = (V, E)$ is a connected graph with m vertices which we order $(e_1, \ldots, e_m)$, for some $m \geq 1$. Recursively define a sequence of sets of edges $E_0, E_1, \ldots, E_m$ as follows:*

(1) $E_0 := \emptyset$
(2) if $i < m$ and E_i is already defined, then set:

$$E_{i+1} \;:=\; \begin{cases} E_i \cup \{e_{i+1}\} & \textit{if } (V, E_i \cup \{e_{i+1}\}) \textit{ is acyclic} \\ E_i & \textit{otherwise.} \end{cases}$$

Then (V, E_m) is a spanning tree of G.

Proof. □

6.3. Exercises

CHAPTER 7

A glimpse of infinity

In this chapter we are going to say a few things about infinite sets.

7.1. Infinite sets and cardinality

The first order of business is to come to grips with the *cardinality* of infinite sets. To motivate our definitions, let's take a careful look at how we reason about the cardinality of *finite* sets.

Question 7.1.1. *Which of the following sets is greater in cardinality:*

$$A := \{0,1,2\} \quad \textit{or} \quad B := \{0,1,2,3,4\}.$$

Answer 7.1.2. We shall reason as follows:

(1) First count the number of elements in A. There are three elements so we conclude $|A| = 3$.
(2) Then count the number of elements of B. There are five elements so we conclude $|B| = 5$.
(3) Then we compare the two numbers 3 and 5. Since $3 < 5$, we conclude that $|A| < |B|$, i.e., the set B has strictly greater cardinality than the set A.

We make the following observations about the above thought process:

(I) *First* we determine the cardinalities of the sets A and B separately, i.e., we associate A to $|A| = 3$ and associate B to $|B| = 5$.
(II) *After* we have determined the cardinalities, then we compare the cardinalities with each other to determine that B is larger.

In other words, the relation "$|A| < |B|$" is a consequence of first defining what $|A|$ and $|B|$ mean separately. For infinite sets, we need to think about cardinality the other way around, i.e., *first* we will define the relations "$|A| = |B|$", "$|A| \leq |B|$", and "$|A| < |B|$", and *then* we define what $|A|$ and $|B|$ mean from this. In the definitions below, while we have infinite sets in mind, they hold for both finite and infinite sets:

Definition 7.1.3. Suppose A and B are sets. Then we say that

(1) A and B are **equal in cardinality** (or **equinumerous**) (notation: $|A| = |B|$) if there exists a bijection from A to B, i.e.,

$$|A| = |B| \;:\Longleftrightarrow\; \text{there exists a function } f : A \to B \text{ such that } f \text{ is one-to-one and onto}$$

(2) A is **less than or equal in cardinality** to B (notation: $|A| \leq |B|$) if there exists a one-to-one function from A to B, i.e.,

$$|A| \leq |B| \;:\Longleftrightarrow\; \text{there exists a function } f : A \to B \text{ such that } f \text{ is one-to-one}$$

(3) A is **less than in cardinality** to B (notation: $|A| < |B|$) if $|A| \leq |B|$ and $|A| \neq |B|$.

The relation $|A| \leq |B|$ is actually a partial order on sets. Reflexivity and transitivity are obvious, anti-symmetry is not:

Lemma 7.1.4. *Let A, B, C be sets.*

(1) (Reflexivity) $|A| \leq |A|$,

(2) (Transitivity) if $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

PROOF. (1) is true since $\mathrm{id}_A : A \to A$ is an injection.

(2) Assume $|A| \leq |B|$ and $|B| \leq |C|$. By definition, this means there exists injections $f : A \to B$ and $g : B \to C$. Then the composition $g \circ f : A \to C$ is also an injection, hence $|A| \leq |C|$. □

The property of anti-symmetry is far from obvious because it is not clear how to create a single bijection from two injections going both ways. This construction is accomplished in the proof of the next theorem:

Schröder-Bernstein Theorem 7.1.5. *Let A and B be sets such that $|A| \leq |B|$ and $|B| \leq |A|$. Then $|A| = |B|$.*

PROOF. Suppose $f_1 : A \to B$ and $f_2 : B \to A$ are injections. Define $B' := f_2(B)$ and $A_1 := f_2(f_1(A))$. Then $A_1 \subseteq B' \subseteq A$. Furthermore, $f_2 : B \to B'$ is a bijection, so we might as well prove that $|B'| = |B|$. □

Definition 7.1.6. Given a set A, we say that A is **finite** if there exists a natural number $n \in \mathbb{N}$ such that

$$|A| \ = \ \big|\{0, 1, \ldots, n-1\}\big|.$$

We say that A is **infinite** if A is not finite.

If A is an infinite set, then we can construct an injection $i : \mathbb{N} \to A$ recursively by at each step getting a different counterexample to finiteness. Thus $|\mathbb{N}| \leq |A|$ if A is infinite.

Definition 7.1.7. Given a set A, we say that A is **countable** if $|A| \leq |\mathbb{N}|$. If A is countable and infinite, then we say that A is **countably infinite**. Otherwise, if $|\mathbb{N}| < |A|$, then we say that A is **uncountable**.

In view of the Schröder-Bernstein Theorem 7.1.5 above, if A is countably infinite, then $|A| = |\mathbb{N}|$, i.e.,

"A is the same size as $\mathbb{N}$."

The next theorem shows that both $\mathbb{Z}$ and $\mathbb{Q}$ are the "same size" as $\mathbb{N}$. This should seem paradoxical at first since the sets $\mathbb{Z}$ and $\mathbb{Q}$ strictly contain $\mathbb{N}$. This is one of the quirks of *infinite* cardinality that makes it different from *finite* cardinality. Specifically, for finite sets the following statement is true:

Given finite sets A and B, if $A \subseteq B$ and $A \neq B$, then $|A| < |B|$.

However, this is **COMPLETELY FALSE** for infinite sets:

Theorem 7.1.8. *The sets $\mathbb{Z}$ and $\mathbb{Q}$ are countably infinite and so $|\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N}|$. In particular,*

(1) There exists an injection $f : \mathbb{Z} \to \mathbb{N}$, and thus $|\mathbb{Z}| = |\mathbb{N}|$.

(2) There exists an injection $g : \mathbb{Q} \to \mathbb{N}$, and thus $|\mathbb{Q}| = |\mathbb{N}|$.

Proof. □

After the previous theorem, you might be tempted to think "so what? maybe this is true for *all* sets which contain $\mathbb{N}$ and infinite cardinality doesn't really tell us anything new." The next theorem shows that this is definitely *not* the case.

Theorem 7.1.9. $|\mathbb{N}| < |\mathbb{R}|$.

Proof. □

Thus $\mathbb{R}$ is uncountably infinite, whereas $\mathbb{N}, \mathbb{Z}$, and $\mathbb{Q}$ are countably infinite. Is there any infinity larger than $\mathbb{R}$? Then next theorem shows that there is no largest size of infinity, i.e., there is always a larger one:

Theorem 7.1.10 (Cantor)**.** *For every set X,*

$$|X| \ < \ |\mathcal{P}(X)|.$$

[Note that this theorem holds for all sets X, finite or infinite.]

Proof. Let $f : X \to \mathcal{P}(X)$ be an arbitrary function. It suffices to show that f is not a surjection. Consider the following element of the codomain:

$$Y \ := \ \big\{x \in X : x \notin f(x)\big\} \ \in \ \mathcal{P}(X).$$

Suppose towards a contradiction that there is $z \in X$ such that $f(z) = Y$. Is z an element of Y? Note that

$$z \in Y \ \Leftrightarrow \ z \notin f(z) \ \Leftrightarrow \ z \notin Y,$$

a contradiction. Thus Y is not in the range of f, and so f is not a surjection. □

7.2. Cantor's Theorem on dense linear orders

In this section we prove a theorem about linear orders which combines many topics from this course: sets, induction, relations, functions, and cardinality.

Definition 7.2.1. Suppose

7.3. Exercises

Exercise 7.3.1. Suppose $A_1, \ldots, A_n$ are countable sets, i.e., $|A_i| \leq |\mathbb{N}|$ for each $i = 1, \ldots, n$. Prove that

$$|A_1 \times \cdots \times A_n| \ \leq \ |\mathbb{N}|,$$

i.e., the cartesian product $A_1 \times \cdots \times A_n$ is also countable. This shows that for infinite cardinality, taking cartesian products does not necessarily increase your cardinality (as opposed to *finite* cardinality; see the Multiplication Principle 4.1.3).

Exercise 7.3.2. Give an explicit example of a bijection $f : \mathbb{Q} \to \mathbb{Q}^{>0} := \{q \in \mathbb{Q} : q > 0\}$ which induces an isomorphism of total orders $(\mathbb{Q}, <) \cong (\mathbb{Q}^{>0}, <)$. Prove that your function f is a bijection and strictly increasing.

APPENDIX A

Appendix

A.1. The natural numbers and Peano arithmetic

This section summarizes the the construction and basic properties of the natural numbers. For a deeper discussion, we refer the reader to [**3**, Ch. 5]. We are already familiar with the natural numbers

$$\mathbb{N} \; = \; \{0, 1, 2, 3, \ldots\}$$

but what exactly do we mean by "0", or "1", or "2"? There is a certain philosophy in math that *everything* can be built out of pure set-theoretic operations, starting from the emptyset. Following in this tradition, we can define the natural numbers as follows:

$$\begin{aligned} 0 \; &:= \; \emptyset \\ 1 \; &:= \; 0 \cup \{0\} \; = \; \{\emptyset\} \\ 2 \; &:= \; 1 \cup \{1\} \; = \; \big\{\emptyset, \{\emptyset\}\big\} \\ 3 \; &:= \; 2 \cup \{2\} \; = \; \big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\big\} \\ &\;\vdots \end{aligned}$$

More precisely, we define the natural numbers recursively by setting $0 := \emptyset$ and for each $n \geq 0$:

$$n + 1 \; := \; S(n) \quad \text{where } S(X) := X \cup \{X\} \text{ for any set } X.$$

We define the set $\mathbb{N}$ to be the set $\{0, 1, 2, 3, \ldots\}$ (a fancy way of defining $\mathbb{N}$ is to declare it to be the smallest set which contains 0 and is closed under the operation S). The operation S restricts to a function $S : \mathbb{N} \to \mathbb{N}$ called the **successor function**. We illustrate the action of the successor function in Figure A.1 below.

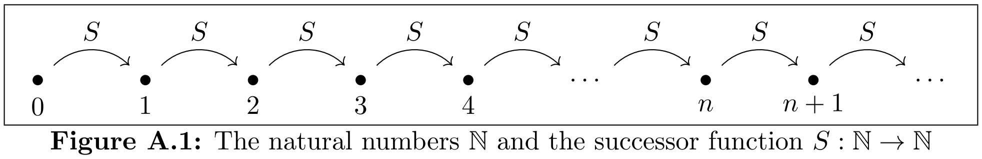

Figure A.1: The natural numbers $\mathbb{N}$ and the successor function $S : \mathbb{N} \to \mathbb{N}$

The natural numbers, together with the function S satisfies the following (remember, $S(n)$ is the function $n \mapsto n + 1$):

Peano Axioms A.1.1. *The following are true for the structure* $(\mathbb{N}; S)$*:*

(1) $0 \in \mathbb{N}$,
(2) *for every* $n \in \mathbb{N}$, $S(n) \in \mathbb{N}$,

(3) *for every $m, n \in \mathbb{N}$, if $S(m) = S(n)$, then $m = n$ (i.e., S is an injective function),*

(4) *(Induction Principle) for every $X \subseteq \mathbb{N}$,*

$$\big(0 \in X \wedge \forall n \in X(S(n) \in X)\big) \to X = \mathbb{N}$$

Justification. One can show, using elementary but technical set-theoretic arguments that the recursive construction of $(\mathbb{N}; S)$ satisfies (1)-(4). The justification for (4) actually looks a lot like our proof of the Principle of Induction 1.4.4. □

There are other operations on $\mathbb{N}$ we also care about, namely *addition* and *multiplication*. These can be defined from the successor function:

Definition A.1.2. We define the function $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ to be the unique function with the following properties:

(1) for every $n \in \mathbb{N}$, $0 + n := n$, and

(2) for every $m, n \in \mathbb{N}$, $S(m) + n := S(m + n)$.

and we define the function $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ to be the unique function with the following properties:

(3) for every $n \in \mathbb{N}$, $0 \cdot n := 0$, and

(4) for every $m, n \in \mathbb{N}$, $S(m) \cdot n := m \cdot n + n$.

Note: (as you are well aware) when dealing with the functions $+$ and $\cdot$, we always use the notation $a + b = c$ instead of $+(a, b) = c$ and $a \cdot b = c$ instead of $\cdot(a, b) = c$.

With *lots* of induction, one can prove that addition and multiplication have the following properties:

Fact A.1.3. For every $\ell, m, n \in \mathbb{N}$ we have

(1) (Associativity) $(\ell + m) + n = \ell + (m + n)$ and $\ell \cdot (m \cdot n) = (\ell \cdot m) \cdot n$

(2) (Commutativity) $m + n = n + m$ and $m \cdot n = n \cdot m$

(3) (Distributivity) $\ell \cdot (m + n) = \ell \cdot m + \ell \cdot n$ and $(\ell + m) \cdot n = \ell \cdot n + m \cdot n$

(4) (Additive identity) $0 + n = n + 0 = n$

(5) (Multiplicative identity) $1 \cdot n = n \cdot 1 = n$

One convenient feature of our construction of $\mathbb{N}$ is that we get the usual inequality $\leq$ essentially for free: given $m, n \in \mathbb{N}$, we define

$$m \leq n \quad \text{if and only if} \quad m = n \text{ or } m \in n$$

We construe $\leq$ as a binary relation on $\mathbb{N}$. One can prove that this binary relation satisfies the following:

Fact A.1.4. For every $\ell, m, n \in \mathbb{N}$,

(1) $\leq$ is a total order:
   (a) $n \leq n$
   (b) if $m \leq n$ and $n \leq m$, then $m = n$
   (c) if $\ell \leq m$ and $m \leq n$, then $\ell \leq n$

(2) $0 \leq n$

(3) $n \leq S(n)$

(4) if $m \leq n$ and $m \neq n$, then $S(m) \leq n$

(5) if $\ell \leq m$, then $\ell + n \leq m + n$

(6) if $\ell \leq m$, then $\ell \cdot n \leq m \cdot n$

In general, when we refer to the basic arithmetic structure of the natural numbers, we are referring to the structure $(\mathbb{N}; S, +, \cdot, \leq)$. We will freely assume and use all of the above facts and their basic consequences when dealing with the natural numbers.

A.2. The (ordered) ring of integers

The primary defect of the natural numbers $\mathbb{N}$ is that not every *addition equation* with coefficients from $\mathbb{N}$ has a solution (in $\mathbb{N}$). For example:

(1) $x + 3 = 5$ has a solution ($x := 2$), however
(2) $x + 5 = 3$ does not have a solution, i.e., there does not exist $x \in \mathbb{N}$ such that $x + 5 = 3$.

The remedy to this situation is to extend the natural number system $\mathbb{N}$ to a larger number system which does include all solutions to all addition equations. This larger number system is the integers

$$\mathbb{Z} \;=\; \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

which we will construct in this section. Before we do that, we give an additional reason for wanting to enlarge the number system $\mathbb{N}$ to the number system $\mathbb{Z}$:

Question A.2.1. *Suppose we have zero interest and desire to solve unsolvable addition equations and we only want to talk exclusively about natural numbers. In this case why would it still be beneficial to consider $\mathbb{Z}$?*

Answer. Even if we only want to answer questions only involving natural numbers, allowing ourselves to still work with negative numbers often simplifies the math and logic by eliminating various case distinctions. For example, suppose we have two natural numbers $a, b \in \mathbb{N}$ such that $(a, b) \neq (0, 0)$ and we are interested in calculating $r := \gcd(a, b)$. If we allow ourselves to use negative numbers in our calculations, we will be able to use the following fact:

$$\gcd(a,b) \text{ is the least } r \in \mathbb{N} \text{ such that there exists } x, y \in \mathbb{Z} \text{ such that } r = ax + by$$

If we are only allowing natural numbers, then we would be forced to work with the "natural number version" of this fact:

$$\gcd(a,b) \text{ is the least } r \in \mathbb{N} \text{ such that there exists } x, y \in \mathbb{N}$$

$$\text{such that } ax = by + r \text{ or } by = ax + r$$

The natural number version is a little more complicated than the integer version since the "or" will result in various case distinctions which are avoided if we allow calculations with (negative) integers. □

We now proceed with the construction of $\mathbb{Z}$. Recall we want to have all solutions of addition equations of the form $x + m = n$, where $m, n \in \mathbb{N}$. This motivates the following definition:

Definition A.2.2. For $m, n \in \mathbb{N}$, define the **pre-integer**[1] corresponding to the equation $x + n = m$ to be the ordered pair $(m, n) \in \mathbb{N} \times \mathbb{N}$. We think of the ordered pair (m, n) as representing a solution to $x + n = m$ (so (m, n) will represent the integer "$m - n$" in some sense). The set of all pre-integers is $\mathbb{N} \times \mathbb{N}$.

[1] This is provisional terminology.

The issue with pre-integers is that there are too many of them. Indeed, the pre-integer associated to $x+5=3$ is $(3,5)$ and the pre-integer associated to $x+6=4$ is $(4,6)$. The pre-integers $(3,5)\neq(4,6)$ are not equal, however, we definitely want $x+5=3$ and $x+6=4$ to have the same solution (since we get the second equation from the first equation by adding 1 to both sides, so an x which works for the first equation should also work for the second equation).

To remedy this, we define an equivalence relation $\sim$ on the set of all pre-integers $\mathbb{N}\times\mathbb{N}$ to capture when two pre-integers "ought to" represent the same integer. To motivate the definition, suppose we have natural numbers $m,n,m',n'\in\mathbb{N}$ and we want to say when "$m-n$" is equal to "$m'-n'$". We aren't allowed to talk about negative numbers or subtraction yet, but if we were, we would notice that

$$m-n \;=\; m'-n' \quad\text{if and only if}\quad m+n' \;=\; m'+n.$$

The second condition "$m+n'=m'+n$" doesn't mention negative numbers or subtraction at all and takes place entirely within $\mathbb{N}$. We will use this as the definition for our equivalence relation:

Definition A.2.3. Given two pre-integers $(m,n),(m',n')\in\mathbb{N}\times\mathbb{N}$, we say that (m,n) is **equivalent** to (m',n') (notation: $(m,n)\sim(m',n')$) if $m+n'=m'+n$, i.e.,

$$(m,n)\sim(m',n') \;:\Longleftrightarrow\; m+n'=m'+n.$$

For example, the pre-integer $(3,5)$ which is supposed to in some sense "represent" the integer $3-5=-2$ is equivalent to the following pre-integers:

$$(0,2)\sim(1,3)\sim(2,4)\sim(3,5)\sim(4,6)\sim\cdots$$

All of these pre-integers are also "representations" of -2 in the same sense that $(3,5)$ is, which is reassuring. In fact, we have the following:

Lemma A.2.4. *Let $(m,n)\in\mathbb{N}\times\mathbb{N}$ be arbitrary. Then:*

(1) $(m,n)\sim(m+1,n+1)$*,*
(2) the equivalence class $[(m,n)]$ *is infinite, and*
(3) there exists $r\in\mathbb{N}$ *such that either* $(m,n)\sim(r,0)$ *or* $(m,n)\sim(0,r)$*.*

By collapsing the set of all pre-integers into their equivalence classes, we arrive at our definition of the set of **integers**:

$$\mathbb{Z} \;:=\; \mathbb{N}\times\mathbb{N}/\sim \qquad \text{(The quotient of } \mathbb{N}\times\mathbb{N} \text{ by the equivalence relation } \sim)$$

At this point we should immediately raise the following objection:

Objection A.2.5. By construction it is clear that the sets $\mathbb{N}$ (defined as in Section A.1) and $\mathbb{Z}$ are disjoint. Indeed, each $n\in\mathbb{N}$ is a technically a finite set (e.g., $3=\big\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\big\}$ so $|3|=3$) whereas each $k\in\mathbb{Z}$ is an infinite set by Lemma A.2.4. However, we have always been operating under the tacit assumption in these notes that $\mathbb{N}\subseteq\mathbb{Z}$. How do we reconcile this?

The answer is we cheat a little and *redefine* the set of all natural numbers now as a subset of $\mathbb{Z}$:

- For each $n\in\mathbb{N}$, redefine $n:=[(n,0)]\in\mathbb{Z}$
- For each $n\in\mathbb{N}$ such that $n\geq 1$, define $-n:=[(0,n)]\in\mathbb{Z}$ ($-n$ is pronounced "negative n")

- We also use the symbol $\mathbb{N}$ as the name for the subset of integers which are natural numbers:
$$\mathbb{N} \;:=\; \big\{[(n,0)] : n \in \mathbb{N}\big\} \;\subseteq\; \mathbb{Z}.$$

It might seem we are asking for trouble by giving two definitions to $\mathbb{N}$ and to each $n \in \mathbb{N}$. However, keeping in mind that everything we do has a precise first-order logic underpinning, we naturally arrive at the following rule: if the domain of discourse is $\mathbb{N}$ (and it really matters to know which definition you are using), then we are using the definition in Section A.1, and if the domain of discourse is $\mathbb{Z}$ (and it also really matters which definition you are using), then we are using the definition from the current section. In general it never matters.

The following illustrates our new definition of the natural numbers and what the equivalence classes look like:

$$\begin{aligned}
&\vdots\\
-2 \;&=\; \big\{(0,2),(1,3),(2,4),(3,5),(4,5),\ldots\big\}\\
-1 \;&=\; \big\{(0,1),(1,2),(2,3),(3,4),(4,5),\ldots\big\}\\
0 \;&=\; \big\{(0,0),(1,1),(2,2),(3,3),(4,4),\ldots\big\}\\
1 \;&=\; \big\{(1,0),(2,1),(3,2),(4,3),(5,4),\ldots\big\}\\
2 \;&=\; \big\{(2,0),(3,1),(4,2),(5,3),(6,4),\ldots\big\}\\
&\vdots
\end{aligned}$$

The next order of business is to show that $\mathbb{Z}$ contains all solutions to addition equations. Before we can do that, we need to define what $+$ means for integers. This is a delicate issue since we need to do this in terms of what $+$ means for $\mathbb{N}$ (as defined in Section A.1) but the elements of $\mathbb{Z}$ are equivalence classes of pairs of natural numbers. The following lemma helps us with this:

Lemma A.2.6. *Suppose $(a,b),(c,d),(a',b'),(c',d')$ are pre-integers such that*

(1) $(a,b) \sim (a',b')$
(2) $(c,d) \sim (c',d')$

Then:
$$(a+c,b+d) \sim (a'+c',b'+d').$$

The previous lemma permits us to make the following definition (see Exercise A.6.1):

Definition A.2.7. We define **integer addition** to be the function $+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ defined by
$$[(a,b)] + [(c,d)] \;:=\; [(a+c,b+d)]$$

Integer addition has the following properties:

Lemma A.2.8. *For every $n \in \mathbb{N}$ such that $n > 0$ we have*

(1) $n + (-n) = 0$

and for every $a,b,c \in \mathbb{Z}$ we have

(2) (Associativity) $(a+b)+c = a+(b+c)$

(3) *(Commutativity)* $a + b = b + a$
(4) *(Additive Identity)* $a + 0 = 0 + a = a$
(5) *(Additive Inverse) there exists an integer* $d \in \mathbb{Z}$ *such that* $a + d = 0$ *(such an integer* d *is called an* ***additive inverse*** *of* a*)*

The first observation is that additive inverses are unique:

Lemma A.2.9. *Suppose* $a \in \mathbb{Z}$ *and* $b, c \in \mathbb{Z}$ *are additive inverses of* a*. Then* $b = c$*.*

For each $k \in \mathbb{Z}$, we define $-k$ to be the unique $d \in \mathbb{Z}$ such that $k + d = 0$. Note that by Lemma A.2.8(1), for $n > 0$ the notation $-n$ is defined to be both $[(0, n)]$ and the additive inverse of $n = [(n, 0)]$, which are the same so there is no issue to giving two meanings to "$-n$". For $a, b \in \mathbb{Z}$ we will also abbreviate $a + (-b)$ as just $a - b$.

It is easy to verify that with this definition we can solve all integer equations:

Lemma A.2.10. *Given* $m, n \in \mathbb{Z}$*, the integer* $x := m - n$ *satisfies the equation*

$$x + n \ = \ m.$$

In particular, since we are now viewing $\mathbb{N}$ *as a subset of* $\mathbb{Z}$*,* $\mathbb{Z}$ *contains all solutions to equations* $x + n = m$ *for every* $m, n \in \mathbb{N}$*.*

Now that *integer addition* is taken care of, we need to define *integer multiplication.* For this we need the following analogue of Lemma A.2.6 for multiplication:

Lemma A.2.11. *Suppose* $(a, b), (c, d), (a', b'), (c', d')$ *are pre-integers such that*

(1) $(a, b) \sim (a', b')$
(2) $(c, d) \sim (c', d')$

Then:

$$(ac + bd, ad + bc) \ \sim \ (a'c' + b'd', a'd' + b'c').$$

This permits us to make the following definition:

Definition A.2.12. We define **integer multiplication** to be the function

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

defined by

$$[(a, b)] \cdot [(c, d)] \ := \ [(ac + bd, ad + bc)]$$

This definition of integer multiplication comes from the observation that (anticipating how things "ought to" work), if $a, b, c, d \in \mathbb{N}$, then

$$(a - b)(c - d) \ = \ (ac + bd) - (ad + bc).$$

Thus the product of $[(a, b)]$ and $[(c, d)]$ better equal $[(ac + bd, ad + bc)]$ if our interpretation of pre-integers and integers is going to be correct.
The main properties of integer multiplication, and its interaction with integer addition, are the following:

Lemma A.2.13.

A.3. The (ordered) field of rational numbers

A.4. The (ordered) field of real numbers

A.5. The field of complex numbers

A.6. Exercises

Exercise A.6.1. Suppose $f : X \times Y \to Z$ is a binary function and E_1, E_2, E_3 are equivalence relations on X, Y, Z respectively. Show the following are equivalent:

(1) For every $x, x' \in X$ and $y, y' \in Y$, if
  (a) xE_1x', and
  (b) yE_2y',
  then
$$f(x,y)\ E_3\ f(x',y').$$

(2) The (ternary) relation
$$\overline{f} \;:=\; \big\{([x]_{E_1}, [y]_{E_2}, [f(x,y)]_{E_3}) : (x,y) \in X \times Y\big\} \;\subseteq\; X/E_1 \times Y/E_2 \times Z/E_3$$
is a function $X/E_1 \times Y/E_2 \to Z/E_3$.

Bibliography

1. Paul R. Halmos, *I want to be a mathematician*, Springer-Verlag, New York, 1985, An automathography. MR 789980
2. Richard Johnsonbaugh, *Discrete mathematics*, eighth ed., Pearson, 2018.
3. Yiannis Moschovakis, *Notes on set theory*, second ed., Undergraduate Texts in Mathematics, Springer, New York, 2006. MR 2192215

Index