UC Irvine Math 13 Winter 2022
Introduction to Abstract Mathematics

Professor: Erik Walsberg
Teaching Assistant: Cheuk-Wai Yau
Notes: Timothy Cho

January 2024
Lecture Note Series #**4**

Introduction

These notes are roughly sorted chronologically, but sections are mainly organized by topic. The scope of these notes cover most lectures and some discussion. We should note that this iteration of Math 13 was quite unorthodox; hence, these do not exactly line up with the UC Irvine Math 13 official course notes (by Neil Donaldson); however, the material here is worth their weight in paper, at least for a review of Math 13. Some interesting exercises are included at the back of these notes to aid practice and readability.

1 Propositional Logic

In this section, we introduce the notion of a *proposition*, and we learn the basic logical connectives that will occur in this course.

Definition 1.1. A *proposition* is a statement that is definitively either true or false.

For example, "the sum of 2 and 2 is 4" is a true proposition, whereas "Eggs are tasty" is not even a proposition, as it is an *opinion* that is not definitively true or false. We represent propositions using capital letters, usually P or Q, the trueness or the falsity of a proposition is called its *truth value*. We write $|P| = 1$ to mean that P is true, and $|P| = 0$ to mean that P is false. We also write $P \equiv Q$ whenever P and Q have the same truth value. Doing so, we can build longer propositions out of short ones, using logical connectives.

Definition 1.2. Let P and Q be propositions. We define these propositions in terms of the truth values for P and Q:

1. The *conjunction* $P \wedge Q$, read "P and Q", is true exactly when P and Q are both true. It is false otherwise.
2. Then *disjunction* $P \vee Q$, read "P or Q", is false exactly when P and Q are both false. It is true otherwise.
3. The *negation* $\neg P$, read "not P," is true when P is false, and false when P is true.
4. The *implication* $P \implies Q$, read "if P then Q," is false exactly when P is true and Q is false. It is true otherwise.
5. The *equivalence* $P \iff Q$, read "P if and only if Q," is true whenever $P \equiv Q$. It is false otherwise.

We note that the equivalence is sometimes called the *biconditional*. We leave it to the reader to verify these fundamental identities.

Theorem 1.3 (Properties of Logical Connectives)**.** *Let P, Q, and R be propositions. Then the following properties hold:*

1. *Associativity of Conjunction:* $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$.
2. *Associativity of Disjunction:* $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$.
3. *Distributivity I:* $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.
4. *Distributivity II:* $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

5. *Double Negation Property:* $\neg(\neg P) \equiv P$.
6. *Commutativity of Conjunction:* $P \wedge Q \equiv Q \wedge P$.
7. *Commutativity of Disjunction:* $P \vee Q \equiv Q \vee P$.
8. *Decomposition of Implication:* $(P \implies Q) \equiv (\neg P) \vee Q \equiv \neg(P \wedge \neg Q)$.
9. *DeMorgan I:* $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.
10. *DeMorgan II:* $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$.
11. *Decomposition of Equivalence:* $(P \iff Q) \equiv (P \implies Q) \wedge (Q \implies P)$.
12. *Contrapositive:* $(P \implies Q) \equiv (\neg Q \implies \neg P)$.

With all of this being said, one fine detail should not be missed. Recall that we write $P \equiv Q$ whenever P and Q share the same truth value; we vocalize this as saying "P is *(logically) equivalent* to Q." **However, P is not necessarily equal to Q!** For example, if P is the statement $0 = 3$, and Q is the statement "the derivative of x^2 is e^x," then clearly $P \equiv Q$ as both statements are false, but $P \neq Q$ in that the statements P and Q are quite literally different words. In a slightly more subtle way, $P \wedge Q$ and $Q \wedge P$ are *not* the same statement in that the *order* of the words are different, but the notion of logical equivalence allows us to consider $P \wedge Q$ and $Q \wedge P$ to be "basically equivalent" for lack of a better term. Notice that if indeed $P \equiv Q$, then P and Q are also "basically equivalent" even if the sentential content in P and Q are vastly different: this is the limit to the logical system we are using, as it cannot distinguish propositions based on "related-ness," but merely on truth alone.

Here are some exercises to work through.

Exercise 1. Let P and Q be propositions. We define the *exclusive disjunction* $P + Q$, read "P exclusive or Q," to be true whenever exactly one of P and Q are true, and false otherwise. Prove the following for all propositions P, Q, R:

(a) $P + Q \equiv \neg(P \iff Q)$.

(b) $P + Q = Q + P$.

(c) $(P + Q) + R \equiv P + (Q + R)$.

(d) $P \wedge (Q + R) \equiv (P \wedge Q) + (P \wedge R)$.

Exercise 2. Let P and Q be propositions. We define the *not conjunction* $P \uparrow Q$, read "P nand[1] Q," to be true whenever $P \wedge Q$ is false, and false whenever $P \wedge Q$ is true. That is, we have

$$P \uparrow Q \equiv \neg(P \wedge Q).$$

Prove the following for all propositions P and Q:

(a) $\neg P \equiv P \uparrow P$.

(b) $P \wedge Q \equiv (P \uparrow Q) \uparrow (P \uparrow Q)$.

(c) $P \vee Q \equiv (P \uparrow P) \uparrow (Q \uparrow Q)$.

This exercise shows that the $\uparrow$ operation is *functionally complete*: all of our familiar operators can be written solely in terms of just the $\uparrow$.

[1] That is, "not and."

2 Sets I: Basic Definitions

In this class, logic is important as we need to discuss sets, which in some extent depend on whether a certain thing is "inside" the set or not.[2] To do this, we will make the following definition of a set, which is good enough for our purposes.

Definition 2.1. A *set* S is any collection of objects, called *elements* of the set. If x is included inside S, then we write $x \in S$ (read "x is in S") to denote this relationship. Similarly, if x is not included inside S, we write $x \notin S$.

What an object is really depends on the context. For example, $\{2, 5\}$ is a set containing the numbers 2 and 5, and so is the *singleton set* $\{e^x\}$, containing a function. We note that sets can contain other sets, such as $\{3, \pi, \{f, j\}\}$. Sets do not contain duplicate elements, so $\{3, 4, 3\}$ is the same set as $\{3, 4\}$. There is also a unique set containing nothing:

Definition 2.2. The *empty set*, denoted $\varnothing$, is the set containing no elements: $\varnothing := \{\}$.

We are able to specify elements of a set by explicitly listing them out (as we did above), or by using *set builder notation*:

$$A = \{x : P_x \text{ is true}\},$$

where P_x is some proposition that depends on the x you choose. For example, consider the set

$$E = \{x : x \text{ is an integer multiple of } 3\} = \{..., -6, -3, 0, 3, 6, ...\},$$

where P_x is the proposition "x is a multiple of 3." The set E thus contains exactly the elements x such that P_x is true; i.e., it contains all multiples of 3 and nothing else. Of course, now that we have propositions, we can build new sets out of old just like we built new propositions out of smaller ones.

Definition 2.3. Let A and B be sets. We define these new sets in terms of A and B:

1. The *union* $A \cup B$ is the set $A \cup B := \{x : (x \in A) \vee (x \in B)\}$.
2. The *intersection* $A \cap B$ is the set $A \cap B := \{x : (x \in A) \wedge (x \in B)\}$.
3. The *set difference* $A \setminus B$ is the set $A \setminus B := \{x : (x \in A) \wedge (x \notin B)\}$.
4. The *set sum* $A \oplus B$ is the set $A \oplus B := (A \cup B) \setminus (A \cap B)$.

We would also like to determine the "size" of two sets. There are two obvious ways to do this: count the number of elements in the set, leading to a notion of *cardinality* (which we will explore in detail later), or seeing if one set is entirely contained in another. Hence, we make the following definition.

Definition 2.4. Let A, B be sets. We say that A *is a subset of* B if $x \in A$ implies $x \in B$, for any $x \in A$. We write $A \subseteq B$ to denote this relationship. In the case that we want to stress $A \neq B$, we will write $A \subsetneq B$ and say that A *is a proper subset of* B.

Now, we can also define what it means for two sets to be equal:

[2] A more modern framework is that of *category theory*, which is not as concerned about the stuff inside a set.

Definition 2.5. Let A, B be sets. Then $A = B$ precisely if A and B contain the exact same elements.

For example, if $A = \{x : x \text{ is an even prime}\}$ and $B = \{2\}$, then $A = B$. That is, A and B are just names that represent the same object: the singleton set $\{2\}$. We also get the following proposition.

Proposition 2.6. *Let A, B be sets. Then $A = B$ if and only if both $A \subseteq B$ and $B \subseteq A$ are satisfied.*

Hence, in order to prove that two sets are equal, we show that they are mutually subsets of each other. From here, we get the following properties that should look a lot like what we did for logic.

Proposition 2.7 (Properties of Set Constructions)**.** *Let A, B, and C be sets. Then the following properties hold:*

1. *Associativity of Intersection:* $(A \cap B) \cap C = A \cap (B \cap C)$.
2. *Associativity of Union:* $(A \cup B) \cup C = A \cup (B \cup C)$.
3. *Distributivity I:* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. *Distributivity II:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
5. *Commutativity of Intersection:* $A \cap B = B \cap A$.
6. *Commutativity of Union:* $A \cup B = B \cup A$.

We note that we are dealing with true, honest *equality* here, not just *equivalence* as with the logic case. Also, a lot of the time, we will be thinking of sets as residing in some "collection of everything," usually denoted $\mathcal{U}$. We call $\mathcal{U}$ the *universal set*, which contains all the sets that we are interested in.[3] If we accept the existence of such a universal set $\mathcal{U}$, we make the following definitions.

Definition 2.8. Let A be a set contained in some universal set $\mathcal{U}$; i.e., $A \subseteq \mathcal{U}$. We define the *complement* of A to be the set $A^c := \mathcal{U} \setminus A$.

That is, the complement of A is the set of everything not in A, where our "everything" depends on what our universal set is. From this, we get a few more propositions that look a lot like logic once more.

Proposition 2.9 (Properties of the Complement)**.** *Let A, B be contained in some universal set $\mathcal{U}$. Then the following properties hold:*

1. *Double Complement Property:* $(A^c)^c = A$.
2. *DeMorgan I:* $(A \cup B)^c = A^c \cap B^c$.
3. *DeMorgan II:* $(A \cap B)^c = A^c \cup B^c$.

Here are some exercises for the reader to think about.

[3] The logician will have trouble accepting this, but this is good enough for our purposes.

Exercise 3. Let A and B be sets. Show that $A \cup B$ is the "smallest" set containing both A and B; i.e., if S is a set with $A \subseteq S$ and $B \subseteq S$, then we have $A \cup B \subseteq S$.

Exercise 4. Let A and B be sets. Show that $A \cap B$ is the "largest" set containing elements which are both in A and B; i.e., if S is a set such that $S \subseteq A$ and $S \subseteq B$, then $S \subseteq A \cap B$.

Exercise 5. Prove the following for sets A, B, and C. [Hint: use the exclusive disjunction.]

(a) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$;

(b) $A \oplus B = B \oplus A$;

(c) $A \oplus \varnothing = A$;

(d) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$.

This exercise shows that $\oplus$ and $\cap$ are set analogues of $+$ and $\times$ over the real numbers.

Exercise 6. Prove that for all sets A, B, one has $A \oplus B = (A \setminus B) \cup (B \setminus A)$.

3 Sets II: Advanced Constructions and Cardinality

We have already seen the sum and difference of two sets A and B. We will now define the notion of a *product* of sets.

Definition 3.1. Let A, B be sets. Then the *Cartesian product* of A and B, denoted $A \times B$, is the set of all *ordered pairs* where the first coordinate comes from A and the second coordinate comes from B:

$$A \times B := \{(x, y) : (x \in A) \wedge (y \in B)\}.$$

Notice that the elements of $A \times B$ fundamentally "look different" than that of A and B: those in A and B are specifically elements, while the elements in $A \times B$ are specifically ordered pairs of elements. Of course, we will also define Cartesian products of multiple sets in the obvious way: if $A_1, \ldots, A_n$ are sets, then we write

$$A_1 \times A_2 \times \cdots \times A_n := \{(x_1, \ldots, x_n) : (x_1 \in A_1) \wedge \cdots \wedge (x_n \in A_n)\}.$$

To see why $A \times B$ is called a "product," we introduce the notion of cardinality.

Definition 3.2. Let A be a set. The *cardinality* of A, denoted $|A|$, is the number of elements that A contains. We say that A is *finite* if $|A|$ is finite, and A is *infinite* otherwise.

Our next theorem tells us that Cartesian products cause the cardinality to be multiplicative.

Theorem 3.3. *Let A, B be both finite sets. Then $|A \times B| = |A| \cdot |B|$.*

Proof. By definition, we have $A \times B = \{(x, y) : x \in A \wedge y \in B\}$. That is, every element of $A \times B$ can be thought of as a choice of an element from A, followed by a choice of an element from B. If we have $|A| = m$ and $|B| = n$, we see that we have $m \cdot n$ choices for ordered pairs. This completes the proof. □

Our next construction gives us an analogue to *exponentiation* for sets.

Definition 3.4. Let A be a set. Then the *power set* of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A:

$$\mathcal{P}(A) := \{X : X \subseteq A\}.$$

Notice that the power set is a *set of sets*! The elements themselves are sets: for example, if $A = \{1, 2, 3\}$, then we see that $\{2, 3\} \in X$. **It would be incorrect to write** $\{2, 3\} \subseteq X$, as X is a set of sets. We have the following theorem about the size of a power set.

Theorem 3.5. *Let A be a finite set. Then $|\mathcal{P}(A)| = 2^{|A|}$.*

It is for this reason why we can think of a power set as raising 2 to some *power*.

Proof. Let $|A| = n$, so we write $A = \{a_1, \ldots, a_n\}$. [We are of course assuming the a_i are distinct.] We build a subset B of A by running through the a_i and deciding whether each a_i is in B or not. This is a *binary choice*: $a_i \in B$, or $a_i \notin B$. Since we have n choices to make, we end up with 2^n outcomes. Hence $|\mathcal{P}(A)| = 2^n = 2^{|A|}$. □

Example 3.6. If $A = \varnothing$, then $\varnothing \subseteq \varnothing$. Hence $P(\varnothing) = \{\varnothing\}$, which has cardinality $2^0 = 1$, as expected.

Here is perhaps a simpler way to think about the proof of Theorem 3.5. We define a *binary n-tuple* to be a ordered n-tuple whose entries are either 0 or 1. For example, $(1, 0, 0, 0, 1)$ is a binary 5-tuple while $(1, 2, 0, 1, 0)$ is not. Consider the set $A := \{1, 2, \ldots, n\}$, where $n \geq 1$. We can think of subsets of A to be binary n-tuples, based on whether something is in the set. For example, fixing $n = 3$, we have the correspondences

$$\{1, 2, 3\} \leftrightarrow (1, 1, 1)$$

$$\{1, 2\} \leftrightarrow (1, 1, 0)$$

$$\varnothing \leftrightarrow (0, 0, 0)$$

$$\{2\} \leftrightarrow (0, 1, 0).$$

Formally, there is an *isomorphism of sets* between subsets of $\{1, 2, 3\}$ and binary 3-tuples. Clearly, there are 8 possible binary 3-tuples, which is what we expect from Theorem 3.5.

The following proposition is occasionally useful.

Proposition 3.7. *Let A, B be sets. If $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.*

Proof. Suppose $A \subseteq B$. Take $X \in \mathcal{P}(A)$. Then $X \subseteq A$ by definition. Taking $x \in X$, we see $x \in A$. This implies $x \in B$ as $A \subseteq B$, so we have shown $X \subseteq B$. Hence $X \in \mathcal{P}(B)$ by definition, so we are done. □

Here is an exercise to think about.

Exercise 7. Prove or disprove the following propositions.

(a) $(A_1 \times A_2) \cup (B_1 \times B_2) = (A_1 \cup B_1) \times (A_2 \cup B_2)$ for all sets A_i, B_i.

(b) $(A_1 \times A_2) \cap (B_1 \times B_2) = (A_1 \cap B_1) \times (A_2 \cap B_2)$ for all sets A_i, B_i.

4 Functions

The study of mathematics focuses on sets, yes, but it is arguably more important to discuss relationships between sets. A common way to do this is through *functions*, which we have seen in high school. Informally, a function is a rule that sends one input to one output. We give a formal definition, due to Dirichlet, below.

Definition 4.1. A *function* f consists of the following information:

1. A set A, called the *domain*,
2. A set B, called the *codomain*,
3. An a subset Γ of $A \times B$, called the *graph* of f, such that for every $a \in A$, there is exactly one $b \in B$ such that $(a, b) \in \Gamma$.

Notationally, we will write $f : A \to B$ to denote a function with its domain and codomain, and if $(a, b) \in \Gamma$, we write $f(a) = b$. The element $b \in B$ is the *image* of a under f.

The reader should convince themselves that point (3) above is simply a restatement of the vertical line test from high-school algebra.

Example 4.2. Define the function $f : \mathbb{R} \to \mathbb{R}$ by $f(t) = 0$ if $t \in \mathbb{Q}$, and $f(t) = 1$ if $t \notin \mathbb{Q}$. [Here, $\mathbb{R}$ denotes the *real numbers* and $\mathbb{Q}$ denotes the *rational numbers*.] This definition makes sense, as certainly $\mathbb{Q} \subseteq \mathbb{R}$, so the domain of $\mathbb{R}$ is legal here. Now, the vertical line test is satisfied, as every real number is either rational, or not.

The notion of functions allows us to build upon our idea of trying to take "exponents" of sets.

Definition 4.3. Let A, B be sets. We define B^A to be the set of all functions $f : A \to B$.

Of course, this is reflected in the cardinalities of these sets.

Theorem 4.4. *Suppose A and B are finite. Then $|B^A| = |B|^{|A|}$. That is, if $|A| = n$ and $|B| = m$, then there are exactly m^n functions from A to B.*

Proof. The proof is similar to that of Theorem 3.5. [This is not a surprise; why?] Enumerate the elements in A and B; i.e., write $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$. We build a function $f : A \to B$ by running through the a_i's and assigning them to arbitrary b_j's, from which we have m choices for each b_j. We do this n times, so there are m^n functions by counting.

In the case that $B = \varnothing$ and A is nonempty, there are no functions $f : A \to B$, so we have $|B|^{|A|} = 0^n = 0$, which makes sense. If A and B are both empty, then there is a unique function $f : \varnothing \to \varnothing$, which sends nothing to nothing and is called the *empty function*. We thus allow ourselves the abuse of notation and write $|B|^{|A|} = |B|^0 = 1$. □

Similarly, we can build new functions out of old ones through composition.

Definition 4.5. Let $f : A \to B$ and $g : B \to C$ be functions. The *composition* $g \circ f$, read "g after f," is the function $g \circ f : A \to C$ defined by $(g \circ f)(a) = g(f(a))$.

Of course, the composition is only defined when the domain of g matches the codomain of f.

Our next order of business is to discuss special properties that a function can have. In precalculus, we may have seen a notion of a function passing the horizontal line test, so we could find the function's inverse. We now rigorously define these ideas.

Definition 4.6. Let $f : A \to B$ be a function.

1. We say f is *injective* if whenever $x, y \in A$ satisfy $f(x) = f(y)$, it follows that $x = y$. That is, for any $b \in B$, there is *at most one* $a \in A$ such that $f(a) = b$.

2. We say f is *surjective* if for any $b \in B$, we can find some $a \in A$ with $b = f(a)$. That is, for any $b \in B$, there is *at least one* $a \in A$ such that $f(a) = b$.

3. We say f is *bijective* if it is both injective and surjective. That is, for any $b \in B$, there is *exactly one* $a \in A$ such that $f(a) = b$.

The terms *injective* and *surjective* were originally French, so in older English texts, one may see the terms *one-to-one* and *onto* respectively. The category theory terms *monomorphism* and *epimorphism* derive from the English terms, but in these notes we will use the French terms as given in the definition above.

Example 4.7. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not surjective: for example, $-1 \in \mathbb{R}$, but there is no $x_0 \in \mathbb{R}$ such that $f(x_0) = -1$. However, the modified function $\tilde{f} : \mathbb{C} \to \mathbb{C}$ given by $\tilde{f}(z) = z^2$ *is* indeed surjective, as one can take the square root of any complex number.

Example 4.8. Define the *projection* $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi(x, y) = x$. We see that π is surjective: for any $x \in \mathbb{R}$, we have $\pi(x, 0) = x$. However, π is not injective, as $\pi(1, 2) = \pi(1, 0) = 1$ yet $(1, 2) \neq (1, 0)$.

Example 4.9. Let $g : \mathbb{Z} \to \mathbb{Z}$ be[4] the function $g(n) = 2n$. Then g is certainly injective, but it is not surjective: taking $5 \in \mathbb{Z}$, there is no $n_0 \in \mathbb{Z}$ such that $g(n_0) = 5$; we would need $n_0 = 5/2$ which is not an integer. However, the modified function $\tilde{g} : \mathbb{R} \to \mathbb{R}$ by $\tilde{g}(x) = 2x$ is surjective, and in fact bijective.

The above examples demonstrate that our choice of domain and codomain are very important for determining injectivity and surjectivity. Also, if a function is *bijective*, then we can define an inverse function:

Definition 4.10. Let $f : A \to B$ be a bijection. We define the *inverse* of f to be the function $f^{-1} : B \to A$, where $f^{-1}(b) := a$, where a is the unique value in A such that $f(a) = b$.

However, not all functions are bijective as we have seen, yet we would still like some notion of "invertibility," even if we do not get a true inverse. As such, we define the following terms.

Definition 4.11. Let $f : A \to B$ be a function. For any subset $X \subseteq A$, the *restriction of f to X* is the function $f|_X : X \to B$ given by $(f|_X)(a) := f(a)$ for every $a \in X \subseteq A$.

[4] $\mathbb{Z}$ denotes the set of integers.

The restriction is useful for building inverses, and we might have seen something similar in pre-calculus. For example, $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2$ is not injective, and thus not bijective and has no inverse. However, we see that the restriction $f|_{[0,\infty)}$ is at least *injective*, which gets us closer to our goal. To finish this, we define the *image* of a function.

Definition 4.12. Let $f : A \to B$ be a function, and take $X \subseteq A$. The *image* of X is the set $f(X) := \{f(a) : a \in X\}$. In the case that $X = A$, the image of A is called the *range (or image) of* f and is also denoted $\operatorname{im} f$.

Hence, we can rephrase what it means for a function to be surjective:

Proposition 4.13. *Let $f : A \to B$ be a function. Then f is surjective if and only if* $\operatorname{im} f = B$.

Exercise 8. Prove the above proposition.

Now, taking $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2$ to above, we see that we can restrict the domain and the codomain appropriately to obtain the function $\tilde{f} : [0, \infty) \to [0, \infty)$ by $\tilde{f}(x) = x^2$, which is injective and surjective. However, we can approach the problem of "forcing" an inverse differently, by defining what we call a *preimage*.

Definition 4.14. Let $f : A \to B$ be a function, and take $Y \subseteq B$. The *preimage of* Y (under f) is the set $f^{-1}(Y) := \{a \in A : f(a) \in Y\}$.

That is, the preimage of a set Y is the set of all things in the domain that map into Y. Also note the apparently unfortunate overloading of notation here: depending on the context, f^{-1} could mean the inverse function of a bijection f, or the preimage of an arbitrary function f. However, upon closer inspection, these two usages of the same symbol $f^{-1}(\cdot)$ are nearly synonymus: if Y is a singleton set $Y = \{b\}$, then if f is bijective, $f^{-1}(Y)$ is also a singleton set, say $\{a\}$. This is practically no different than saying $f^{-1}(b) = a$ as per the definition of inverse functions.

Special Types of Functions

In this class, we will highlight two important classes of functions, which we will use extensively in examples and proofs.

Definition 4.15. Let X be any set. A *sequence* is a function $f : \mathbb{Z}^+ \to X$. [Here, $\mathbb{Z}^+$ denotes the positive integers.]

Alternatively, one may think of a sequence as an infinite tuple; for example, we can write the sequence $f : \mathbb{Z}^+ \to \mathbb{Z}$ by $f(n) = 2n$ as $(2, 4, 6, 8, \ldots)$. This viewpoint is reversible, even for finite n-tuples: the ordered triplet of real numbers $(\pi, \sqrt{2}, 7)$ can be viewed as a function $f : \{1, 2, 3\} \to \mathbb{R}$ by $f(1) = \pi$, $f(2) = \sqrt{2}$, and $f(3) = 7$.

The second important set of functions we will use often are *real-valued functions*. These functions are the main objects of study in real analysis (Math 140AB).

Definition 4.16. Let $U \subseteq \mathbb{R}$. A function $f : U \to \mathbb{R}$ is called a *real-valued function*.

With this, we can define *sums* and *products* of functions.

Definition 4.17. Let $f, g : U \to \mathbb{R}$ be real-valued. We define the *sum* of f and g to be the function $(f + g)$, given by $(f + g)(a) = f(a) + g(a)$ for all $a \in U$. Similarly, we define the *product* of f and g to be the function fg, given by $fg(a) = f(a) \cdot g(a)$ for all $a \in U$.

We now leave the reader with some exercises to work through.

Exercise 9. Let $f : A \to B$ be a function, and take $X, Y \subseteq B$. Prove that $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$. Is it true that $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$?

Exercise 10. Are each of the following functions injective, surjective, or both?

(a) $f : \mathbb{Z} \to \mathbb{Z}$ by $f(a) = 2a + 1$.

(b) $g : \mathbb{R} \to \mathbb{R}$ by $g(a) = 2a + 1$.

(c) $h : \mathbb{R} \to [0, \infty)$ by $h(a) = a^2$.

(d) $k : \mathbb{Z} \to \mathbb{Z}$ by $k(a) = a^2$.

Exercise 11. Let A and B be sets. Define the set B^A to be the set of all functions $f : A \to B$. Construct an explicit bijection from $\mathcal{P}(A)$ to $\{0, 1\}^A$.

Exercise 12. Let $f : A \to A$ be *idempotent*, i.e., $f \circ f = f$. Show that f is injective if and only if it is surjective.

Exercise 13. Let B be the set of all infinite binary sequences. Give a bijection $f : B \to \mathcal{P}(\mathbb{N})$.

Exercise 14. Let X be a set and $A \subseteq X$. We define the *characteristic function* $\chi_A : X \to \{0, 1\}$ by $\chi_A(x) = 1$ if $x \in A$ and $\chi_A(x) = 0$ if $x \notin A$. If $A, B \subseteq X$, show that $\chi_A \chi_B = \chi_{A \cap B}$.

Exercise 15. Determine whether the following functions are injective, surjective, and/or bijective.

(a) $f : \mathbb{R} \to \mathbb{R}^2$: $x \mapsto (x, x^2)$,

(b) $g : \mathbb{R}^3 \to \mathbb{R}$: $(x, y, z) \mapsto x + y + z$,

(c) $h : \mathbb{R} \to \mathbb{R}$: $x \mapsto x^3 + 2$,

(d) $k : \mathbb{C} \to \mathbb{C}$: $z \mapsto z^3 + 2$.

For the next exercise, we need the following definitions.

Definition 4.18. Let X be a set. The *identity function* $\iota_X : X \to X$ is the function that sends each element to itself: i.e., $\iota_X(x) = x$ for every $x \in X$.

Definition 4.19. Let $f : A \to B$. A *left inverse* of f is a function $g : B \to A$ such that $g \circ f = \iota_A$, if it exists. Similarly, a *right inverse* of f is a function $h : A \to B$ such that $f \circ h = \iota_B$, if it exists.

These notions allow us to extend the notion of an inverse even further.

Exercise 16. Let $f : A \to B$ be a function. Prove the following:

(a) f is injective if and only if it has a left-inverse;

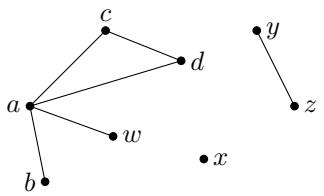
(b) f is surjective if and only if it has a right-inverse.

5 The Pigeonhole Principle: Graphs

In this section, we demonstrate the pigeonhole principle through exploring a basic result in graph theory. We first roughly define what a graph is. Informally, a *graph* (for the purposes of this section) consists of a set of *vertices* and *edges* connecting vertices, subject to the following rules:

- There is at most 1 edge between any pair of vertices.
- There are no loops from a vertex to itself.

For example, the following is a graph:



For the purposes of this discussion, a *finite graph* is a graph where the set of vertices V is finite. We first state the following definition.

Definition 5.1. Let G be a graph, and let v be a vertex. A *neighbor* of v is a vertex that is connected to v by an edge.

Example 5.2. In the graph above, a has the neighbors b, c, d, and w. Meanwhile, y has one neighbor z, and x has no neighbors.

We now state and prove our main theorem, which will demonstrate the pigeonhole principle. Notice that in the graph above, z and w have the same number of neighbors: just one. This is in fact an example of something more general:

Theorem 5.3. *Suppose G is a finite graph with at least 2 vertices. Then there exist 2 distinct vertices on the graph such that they have the same number of neighbors.*

Proof. Suppose G has n vertices, where $n \geq 2$. Thus, if v is a vertex, then v can have *at most* $n-1$ neighbors, as we have disallowed loops in our graphs. Suppose there is some vertex u with the maximum number of neighbors. This means that no vertex can have no neighbors, as u is connected to everything. Similarly, if there is some vertex w with no neighbors, then no vertex can have the maximum number of neighbors $n-1$, as each vertex will miss w as a possible neighbor. Thus, we have two cases:

1. Across all vertices, the number of neighbors is in the set $\{0, 1, \ldots, n-2\}$.
2. Across all vertices, the number of neighbors is in the set $\{1, 2, \ldots, n-1\}$.

However, in each case we have n vertices on our graph, and each vertices has $(n-1)$ possible choices of a number of neighbors to choose from. Hence, it is impossible for each vertex to have a distinct number of neighbors, so there must exist 2 distinct vertices with the same number of neighbors. □

The end of the argument above demonstrates the pigeonhole principle — the number of objects we have exceeds the number of choices, so two distinct objects must make the same choice. Alternatively stated in terms of functions:

Theorem 5.4 (Pigeonhole Principle)**.** *Let A, B be finite sets, and $f : A \to B$ be a function. If $|A| > |B|$, then f is not injective.*

This is illustrative of a more general principle:

Theorem 5.5 (Functions and Cardinality)**.** *Let A, B be finite sets.*

1. *If there exists an injection $f : A \to B$, then $|A| \leq |B|$.*[5]
2. *If there exists a surjection $f : A \to B$, then $|A| \geq |B|$.*
3. *If there exists a bijection $f : A \to B$, then $|A| = |B|$.*

6 Quantifiers

We have already seen the words "for every/all" and "there exists" in our previous work. These are what are known as *quantifiers* in logic, which we allow ourselves to use when writing complex propositions. First, we introduce some notation. Let P be some statement (usually some property), and $x \in X$ be some object. We write $P(x)$ to mean "P is true of x." Formally, we are defining a function $P : X \to \{\text{set of propositions}\}$.

Example 6.1. Let $P(n)$ be the propositions of the form "n is even." Then $P(2)$ is true, as 2 is even, and so is $\neg P(3)$, as it is not the case that 3 is even. We can use our familiar logical connectives to deduce that $P(2) \wedge P(4)$, $P(2) \vee P(-1)$, $P(2) \iff (3 = 3)$, and $P(2) \implies (2 + 2 = 4)$ are all logically true statements.

We extend this by defining quantifiers.

Definition 6.2. Let X be a set, and let P be a function $P : X \to \{\text{set of propositions}\}$. We define the following *quantifiers*:

1. The *existential quantifier* $\exists$, read "there exists," is used to assert that there is at least one $x \in X$ such that $P(x)$ is true:
$$(\exists x \in X)\, P(x) = \text{"there is an } x \text{ such that } P \text{ is true of } x\text{."}$$
2. The *universal quantifier* $\forall$, read "for every," is used to assert that for every $x \in X$, $P(x)$ is true:
$$(\forall x \in X)\, P(x) = \text{"for every } x, P \text{ is true."}$$

If the set X is clear from context, we write $\exists x$ and $\forall x$ instead of $\exists x \in X$ and $\forall x \in X$.

Quantifiers can be manipulated like the rest of our logical connectives. In particular, they play nicely with our negation operation, which we leave the reader to verify:

Proposition 6.3. *Let $P(x)$ be a set of propositions about elements in some set X. Then $\neg\exists x\, P(x) \equiv \forall x\, \neg P(x)$ and $\neg\forall x\, P(x) \equiv \exists x \neg P(x)$.*

[5] This is the contrapositive of the Pigeonhole Principle.

We also stress that the order of quantifiers, when there are many of them, is important. Consider the following example.

Example 6.4. Let us discuss these two statements about positive integers:

1. $(\forall m \in \mathbb{Z}^+)\,(\exists n \in \mathbb{Z}^+)\,(m < n)$;
2. $(\exists n \in \mathbb{Z}^+)\,(\forall m \in \mathbb{Z}^+)\,(m < n)$.

The first of these reads, "for every positive integer m, there exists another positive integer n such that n is greater than n," equivalently, "there is no largest integer." This is evidently true. However, the second of these reads "there exists a positive integer n, such that for every positive integer m, we have m is less than n," equivalently, "there *is* a largest integer," which is the negation of statement (1).

Try negating the following statements involving multiple quantifiers:

Exercise 17. Find the negation of the following two statements.

(a) $(\forall n \in \mathbb{Z}^+)\,(\exists x \in \mathbb{R})\,(x < 1/n)$;

(b) $(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})\,(xy = 1)$.

Which of these two statements is true?

7 Induction I: The Basic Principle

Now, we turn our attention to the case where $P(n)$ represents some property of positive integers, so we are picking $n \in \mathbb{Z}^+$. Often, we would like to prove a statement of the form $(\forall n \in \mathbb{Z}^+)\,P(n)$; however, it would seem like there is an infinite list of things to check. However, here we introduce the *principle of induction*, which boils down to showing two things.

Theorem 7.1 (Induction Principle)**.** *Suppose we would like to prove* $(\forall n \in \mathbb{Z}^+)P(n)$*. Then it suffices to prove* $P(1)$ *and* $P(n) \implies P(n+1)$ *for an arbitrary integer* n*. That is,*

$$\Big[P(1) \wedge \big(P(n) \implies P(n+1)\big)\Big] \implies \forall n\, P(n).$$

Intuitively, we have a *base case* $P(1)$ to fall back on, and proving the *inductive step* $P(n) \implies P(n+1)$, where n is *arbitrary*, means we can chain implications together:

$$P(1) \implies P(2), P(2) \implies P(3), P(3) \implies P(4), \ldots,$$

in order to show $P(1) \implies P(n)$ for every $n \in \mathbb{Z}^+$. Since $P(1)$ is true, $P(n)$ must also be true for the implication $P(1) \implies P(n)$ to be true. We view some examples.

Example 7.2. Prove that for all $n \in \mathbb{Z}^+$, we have $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof. We proceed by induction on n. First, we verify that the base case $n = 1$ holds:

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

Now, assume the induction hypothesis, that $1+2+\cdots+n = n(n+1)/2$ for some arbitrary n. We compute

$$\sum_{k=1}^{n+1} k = (1+2+\cdots+n)+(n+1) = (n+1)+\sum_{k=1}^{n} k,$$

so by our induction hypothesis, we have

$$\sum_{k=1}^{n+1} k = (n+1)+\frac{n(n+1)}{2} = \frac{(n+1)(n+2)}{2},$$

where the reader can check the algebra in this last equality. This completes the proof. □

Example 7.3. Prove that for every $n \geq 1$, we have

$$1\cdot 2 + 2\cdot 3 + \cdots + n(n+1) = \frac{1}{3}n(n+1)(n+2).$$

Proof. We prove by induction on n. We verify the base case $n = 1$:

$$1\cdot 2 = 2 = \frac{1}{3}(1)(1+1)(1+2) = \frac{1}{3}(2)(3).$$

Now, we assume the inductive hypothesis that $\displaystyle\sum_{k=1}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2)$ for some arbitrary $n \geq 1$, and we compute

$$\sum_{k=1}^{n+1} k(k+1) = (n+1)(n+2)+\sum_{k=1}^{n} k(k+1) = (n+1)(n+2)+\frac{1}{3}n(n+1)(n+2)$$

$$= (n+1)(n+2)\left[1+\frac{1}{3}n\right] = \frac{1}{3}(n+1)(n+2)(n+3),$$

which completes the proof. □

The above examples demonstrate an important principle when working with sums: split the sum appropriately. Here is an example with a different flavor.

Example 7.4. Prove that for every $n \in \mathbb{Z}^+$, we have $n+(n+1)+\cdots+2n = \frac{3}{2}n(n+1)$.

Proof. We prove by induction on $n \in \mathbb{Z}^+$. The base case $n = 1$ is easy to verify:

$$1+2 = 3 = \frac{3}{2}(1)(2).$$

Now, assume that our statement is true for some arbitrary $n \geq 1$. We compute

$$S := (n+1)+(n+2)+\cdots+2(n+1) = [(n+1)+(n+2)+\cdots+2n]+(2n+1)+(2n+2).$$

The induction hypothesis almost applies, so we make a slight adjustment:

$$S = \left[\frac{3}{2}n(n+1) - n\right] + (4n+3) = \frac{3}{2}n(n+1) + 3n + 3 = \frac{3}{2}n^2 + \frac{3}{2}n + 3n + 3$$

$$= \frac{3}{2}n^2 + \frac{9}{2}n + 3 = \frac{3}{2}(n^2 + 3n + 2) = \frac{3}{2}(n+1)(n+2),$$

so we are done. □

Induction can be used to prove more than just sums:

Example 7.5. Prove that for any $n \in \mathbb{Z}$, $n^5 - n$ is a multiple of 5.

Proof. We first take the case where $n \geq 0$. Here, we apply induction on all non-negative n. Our base case starts at $n = 0$, and we see that $0^5 - 0 = 0$, which is a multiple of 5. Now, suppose that $n^5 - n$ is a multiple of 5, where $n \geq 0$ is arbitrary. Then

$$(n+1)^5 - (n+1) = (n^5 + 5n^4 + 10n^3 + 10n^2 + 10n + 1) - n - 1$$

$$= (n^5 - n) + 5(n^4 + 2n^3 + 2n^2 + n).$$

The first of these terms is divisible by 5 by the induction hypothesis, and the second of these terms is obviously divisible by 5. Hence, we are done when $n \geq 0$.

If $n \leq 0$, note that $-n \geq 0$, so that $(-n)^5 - (-n) = -(n^5 - n)$ is divisible by 5 by our previous case. Flipping signs gives us what we need, so we are done for all $n \in \mathbb{Z}$. □

Example 7.6. Prove that for all $n \in \mathbb{Z}^+$, we have $4^n < (n+2)!$.

Proof. We prove by induction on $n \in \mathbb{Z}^+$. For the base case $n = 1$, we have $4^1 = 4 < 6 = (1+2)!$. Assume that $4^n < (n+2)!$ for an arbitrary $n \in \mathbb{Z}^+$. Then

$$4^{n+1} = 4 \cdot 4^n < 4 \cdot (n+1)!$$

by the induction hypothesis, but now since $n \geq 1$, we must have $n + 3 \geq 4$, so we may replace and write

$$4^{n+1} < 4 \cdot (n+1)! \leq (n+3)(n+2)! = (n+3)! = [(n+2)+1]!,$$

so by induction, we are done. □

We leave these exercises for the reader to try.

Exercise 18. Prove that every finite subset of $\mathbb{R}$ has a minimum element.

Exercise 19. Show that for all positive integers, we have

$$\sum_{k=0}^{n} q^k = \frac{q^{n+1} - 1}{q - 1}$$

as long as $q \neq 1$.

Exercise 20. Show that the sum of the first n odd positive integers is n^2, more precisely that

$$n^2 = \sum_{k=1}^{n} (2k-1) \text{ for all } n \in \mathbb{Z}^+.$$

Exercise 21. Prove that for all $n \in \mathbb{Z}^+$, we have $2^n + n \leq 3^n$.

Exercise 22. The *gamma function* $\Gamma : (0, \infty) \to \mathbb{R}$ is defined by

$$\Gamma(x) := \int_0^\infty t^{s-1} e^{-t}\, dt.$$

Show that $\Gamma(n) = (n-1)!$ for every $n \geq 1$.

8 Induction II: Strong Induction

Sometimes, induction is not enough to prove a statement of the form $(\forall n \in \mathbb{Z}^+)\, P(n)$, due to the way the problem requires more assumptions. However, there is a (relatively) easy fix: just assume more assumptions when we do the induction step.

Theorem 8.1 (Strong Induction Principle)**.** *Suppose we would like to prove* $(\forall n \in \mathbb{Z}^+)P(n)$*. Then it suffices to prove* $P(1)$*, and that* $[P(1) \wedge P(2) \wedge \cdots \wedge P(n)] \implies P(n+1)$*.*

That is, we show $P(1)$, and we assume the statements $P(k)$ are all true for all $1 \leq k \leq n$, from which we deduce $P(n+1)$. We view an example, which is an important theorem we will use later on.

Theorem 8.2 (Fundamental Theorem of Arithmetic)**.** *Every natural number* $n \geq 2$ *can be factored into primes, and this factorization is unique up to changing the order of the factors.*

We will prove existence via strong induction.

Proof of Existence of Factorization. We check our base case $n = 2$: the number 2 is prime, so our factorization is simply $2 = 2$. Now, assume the strong induction hypothesis that every integer k, with $2 \leq k \leq n$, can be factored as a product of primes. Consider the integer $n+1$. If $n+1$ is prime, then $n+1 = n+1$ is a factorization into primes. Otherwise, $n+1$ is composite and there exist integers a, b with $2 < a, b < n+1$ such that $n+1 = ab$. By the inductive hypothesis, factor both a and b into primes:

$$a = p_1 p_2 \cdots p_m, b = q_1 q_2 \cdots q_\ell,$$

where the q_i's and q_j's are all prime. Hence

$$n+1 = (p_1 p_2 \cdots p_m)(q_1 q_2 \cdots q_\ell) = \prod_{i=1}^{m} p_i \prod_{j=1}^{\ell} q_j$$

is a factorization of $n+1$ into primes. □

Notice that the strong induction hypothesis was actually necessary here: we did not know *exactly* what a and b were, only that they were in the range to apply the strong induction hypothesis on.

Strong induction is often used when we have a *recursive* definition of a sequence $f : \mathbb{Z}^+ \to X$. One prototypical example of this is the Fibonacci sequence:

Definition 8.3. The *Fibonacci sequence* is the function $F : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined as follows: $F(1) = F(2) = 1$, and $F(n) = F(n-1) + F(n-2)$ for every $n \geq 3$.

We often write F_n in place of $F(n)$ for sequences such as this one.

Example 8.4. For every $n \in \mathbb{Z}^+$, define S_n to be the set of sequences of 1's and 2's that sum to n. For example, $S_1 = \{(1)\}$, $S_2 = \{(2), (1,1)\}$, and $S_3 = \{(1,1,1), (1,2), (2,1)\}$. Show that $|S_n| = F_{n+1}$ for every $n \in \mathbb{Z}^+$.

Proof. We prove by strong induction. Here, we need to check two base cases, due to how the Fibonacci sequence is defined. Clearly, the example above shows that $|S_1| = 1 = F_2$ and $|S_2| = 2 = F_3$, so the base cases hold. Now, assume $n \geq 3$, and that the induction hypothesis holds for all $k < n$. [Note that this is simply a different way of phrasing the induction step in strong induction.] Let $(s_1, \ldots, s_k)$ be a sequence of 1's and 2's that sum to n. If $s_1 = 1$, then the subsequence $(s_2, \ldots, s_k)$ sums to $n-1$; similarly, if $s_1 = 2$, then the subsequence $(s_2, \ldots, s_k)$ sums to $n-2$. Alternatively stated, every sequence in S_n is of the form $(1, s_2, \ldots, s_k)$ or $(2, t_2, \ldots, t_k)$, where $(s_2, \ldots, s_k) \in S_{n-1}$ and $(t_2, \ldots, t_k) \in S_{n-2}$. By counting and the induction hypothesis, we see that $|S_n| = |S_{n-1}| + |S_{n-2}| = F_n + F_{n-1} = F_{n+1}$. □

Example 8.5. We show that any $k \in \mathbb{Z}^+$ has a *binary expansion*: i.e., for every $k \in \mathbb{Z}^+$, there exist integers $0 \leq k_1 < k_2 < \cdots < k_\ell$ such that $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_\ell}$.

Proof. We prove by strong induction. The base case $n = 1$ is simple enough: $1 = 2^0$. Now, assume for some $k \geq 1$, the statement holds for all integers less than or equal to k. Let $n := k + 1$. Let $j \in \mathbb{N}$ be such that $2^j \leq n$ but $2^{j+1} > n$; that is, $j := \lfloor \log_2 n \rfloor$, and set $m := n - 2^j$. Clearly, $m \geq 0$. If $m = 0$, then $n = 2^j$ and we are done.

In the case that $m > 0$, we note that $m = n - 2^j = j + 1 - 2^j \leq k + 1 - 1 = k$, so the induction hypothesis applies, so there exist $0 \leq k_1 < k_2 < \cdots < k_\ell$, all integers, such that $m = 2^{k_1} + \cdots + 2^{k_\ell}$. We make the claim that $j \neq k_i$ for any $i = 1, 2, \ldots, \ell$. Otherwise, if $j = k_i$ for some k_i, we would have $n = m + 2^j = m + 2^{k_i} = (2^{k_1} + \cdots + 2^{k_i} + \cdots + 2^{k_\ell}) + 2^{k_i} \geq 2 \cdot 2^{k_i} = 2^{k_i+1} = 2^{j+1}$, but this would contradict our definition of j. Thus

$$n = m + 2^j = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_\ell} + 2^j,$$

where each integer is distinct. Now, put the integers $j, k_1, k_2, \ldots, k_\ell$ in order to complete the proof. □

Here are two strong induction exercises.

Exercise 23. Let $a_1 = 3/2$, $a_2 = 7/12$ and $6a_{k+2} = 5a_{k+1} - a_k$ for all $k \geq 1$. Prove that

$$a_k = \frac{1}{2^k} + \frac{1}{3^{k-1}}.$$

Exercise 24. Let $x_1 = 2$, $x_2 = 12$ and for any positive integer n, define $x_{n+2} = 2x_{n+1} + 4x_n$. Show that x^n is a multiple of 2^n for all n.

9 Induction III: The Binomial Coefficient

One particular function often arises in combinatorics, but also in other unexpected areas. In this section, we explore the *binomial coefficient* and its relationship to induction.

Definition 9.1. Let $n, k \in \mathbb{Z}_{\geq 0}$, with $k \leq n$. We define the *binomial coefficient* $\binom{n}{k}$ by $\binom{n}{0} = 1 = \binom{n}{n}$ if $k = 0, n$, and recursively by $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ otherwise.

For us, binomial coefficients have one major interpretation.

Proposition 9.2. *There are* $\binom{n}{k}$ *subsets of cardinality* k *of* $\{1, 2, \ldots, n\}$.

Proof. We apply a "double induction" on n and k. In the case that $k = 0$ or $k = n$, this is obvious: there is one subset of zero elements ($\varnothing$) and one subset containing n elements (the whole set). Of course, we have $\binom{n}{0} = \binom{n}{n} = 1$. For the inductive step, suppose $1 \leq k \leq n-1$ and suppose $\binom{m}{j}$ is the number of j-element subsets of an m-element set, whenever $j < k$ or $m < n$. Consider a k-element subset of $\{1, 2, \ldots, n\}$; call this subset X. We consider two disjoint cases.

Case I: $1 \notin X$. In this case, $X \subseteq \{2, 3, \ldots, n\}$, which is a set of $n-1$ elements. Apply the inductive hypothesis, and there are such $\binom{n-1}{k}$ sets of size k inside $\{2, 3, \ldots, n\}$.

Case II: $1 \in X$. In this case, let $Y := X \setminus \{1\}$. Then $|Y| = k - 1$, and $Y \subseteq \{2, \ldots, n\}$. By induction, there are $\binom{n-1}{k-1}$ such sets.

Now, adding together the disjoint cases, we have $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$ such k-element subsets of $\{1, 2, \ldots, n\}$. □

Next, we prove an important theorem from algebra, using induction.

Theorem 9.3 (Binomial Theorem)**.** *For all* $x, y \in \mathbb{C}$ *and* $n \in \mathbb{Z}^+$*, we have*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proof. We prove by induction on n. The base case $n = 1$ is easy to verify: $(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y$. Now, suppose the theorem holds for some $n \geq 1$. We expand $(x+y)^{n+1}$:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n && (1)\\
&= (x+y)\left[\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right] && (2)\\
&= x\left[\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right] + y\left[\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right] && (3)\\
&= \left[x^{n+1} + \binom{n}{1} x^n y + \cdots + xy^n\right] + \left[x^n y + \binom{n}{1} x^{n-1} y^2 + \cdots + y^{n+1}\right] && (4)\\
&= x^{n+1} + \left[\binom{n}{0} + \binom{n}{1}\right] x^n y + \left[\binom{n}{1} + \binom{n}{2}\right] x^{n-1} y^2 + \cdots + y^{n+1} && (5)\\
&= \binom{n+1}{0} x^{n+1} + \binom{n+1}{1} x^n y + \binom{n+1}{x}^{n-1} y^2 + \cdots + \binom{n+1}{n+1} y^{n+1}, && (6)
\end{aligned}$$

where (2) comes from the inductive hypothesis and (6) comes from the definition of the binomial coefficient. This completes the proof. □

Next, we give some examples of manipulating the binomial coefficient effectively.

Example 9.4. We claim that $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Proof. We prove by induction on n. The base case $n = 1$ is obvious: $\sum_{k=0}^{1} \binom{1}{k} = \binom{1}{0} + \binom{1}{1} = 1 + 1 = 2 = 2^1$. Now, suppose the claim holds for some $n \geq 1$. Then we expand:

We have, noting that $\binom{j}{0} = \binom{j}{j} = 1$ for all $j \in \mathbb{Z}^+$,

$$\begin{aligned}\sum_{k=0}^{n+1} \binom{n+1}{k} &= \binom{n+1}{0} + \binom{n+1}{1} + \cdots + \binom{n+1}{n} + \binom{n+1}{n+1} \\ &= \binom{n}{0} + \left[\binom{n}{0} + \binom{n}{1}\right] + \cdots + \left[\binom{n}{n-1} + \binom{n}{n}\right] + \binom{n}{n} \\ &= 2\binom{n}{0} + 2\binom{n}{1} + \cdots + 2\binom{n}{n-1} + 2\binom{n}{n} = 2\sum_{k=0}^{n} \binom{n}{k},\end{aligned}$$

For the second step, we used the definition of the binomial coefficient. Now, the inductive step finishes the proof:

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = 2\sum_{k=0}^{n} \binom{n}{k} = 2 \cdot 2^n = 2^{n+1},$$

so we are done. □

Exercise 25. Give an alternative proof of the above example by appealing to Theorem 3.5.

Our final example relates our definition of the binomial coefficient to a common alternate definition often used by textbooks.

Proposition 9.5. *For all $n, k \in \mathbb{Z}_{\geq 0}$ with $n \geq k$, we have* $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

Proof. We prove by "double induction" on n and k. We check two base cases: $\binom{n}{0} = 1 = n!/(n! \cdot 0!) = \binom{n}{n}$. For the induction hypothesis, assume that

$$\binom{m}{j} = \frac{m!}{j!(n-j)!}$$

for all $m < n$ and $j < k$. Now

$$\begin{aligned}\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= \frac{(n-1)!}{k!(n-k-1)!} \cdot \frac{n-k}{n-k} + \frac{(n-1)!}{(k-1)!(n-k)!} \cdot \frac{k}{k} \\ &= \frac{(n-1)!(n-k) + (n-1)!k}{k!(n-k)!} = \frac{(n-1)!(n-k+k)}{k!(n-k)!} \\ &= \frac{n!}{k!(n-k)!},\end{aligned}$$

which completes the proof. □

Here are some slightly more interesting examples for the reader to solve.

Exercise 26. Let $0 \leq k \leq m \leq n$. Show that $\binom{m}{k}\binom{n}{m} = \binom{n}{k}\binom{n-k}{m-k}$.

Exercise 27. Let $n \geq 1$. Show that $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$.

Exercise 28. Let $n \geq 1$. Show that $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$.

Exercise 29. Let $n \geq 1$. Show that $\sum_{k=1}^{n} k(-1)^k 2^{n-k}\binom{n}{k} = -n$.

Exercise 30. Using the fact that $(1+x)^n(1+x)^n = (1+x)^{2n}$, show that

$$\sum_{r=0}^{k} \binom{n}{r}\binom{n}{k-r} = \binom{2n}{k}.$$

10 Divisibility I: Basic Principles

We now move into the number theory part of Math 13. A lot of number theory is based on the idea of *divisibility*, which we will discuss later, but first, let us consider a special case: divisibility by 2.

Definition 10.1. Let $n \in \mathbb{Z}$.[6] We say that n is *even* if $n = 2k$ for some $k \in \mathbb{Z}$. Similarly, we say that n is *odd* if $n = 2k+1$ for some $k \in \mathbb{Z}$.

Alternatively worded, n is even if it is "divisible by 2," whatever that means. We first note an obvious-sounding property of evenness and oddness, which will have important ramifications later — which is to say, do not skip this proof!

Proposition 10.2. *Every integer is either even or odd, and no integer is both even and odd.*

Proof. We first prove the statement that every integer is either even or odd. Let $n \in \mathbb{Z}$. We need only consider the non-negative integers, as we can just "flip" things around for negative integers. Hence, we apply induction on all $n \geq 0$. The base case $n = 0$ is obvious: $0 = 2 \cdot 0$, so 0 is even. Now, suppose that n is either even or odd, for some $n \geq 0$. We consider 2 cases.

Case I: n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. But then $n+1 = 2k+1$, so $n+1$ is odd.

Case II: n is odd. Then $n = 2j+1$ for some $j \in \mathbb{Z}$. But then $n+1 = 2j+2 = 2(j+1)$. Letting $m := j+1$, we see $n+1 = 2m$, so $n+1$ is even.

Thus, every integer (reflecting this for negative integers) is either even or odd.

Now, we show that no integer is both even and odd. Suppose for contradiction that $n \in \mathbb{Z}$ is both even and odd. Then $n = 2k$ and $n = 2j+1$ for $j, k \in \mathbb{Z}$.[7] Thus, $n = 2k = 2j+1$, which implies $2(k-j) = 1 \iff k - j = 1/2$. But since $k, j \in \mathbb{Z}$, we have $1/2 \in \mathbb{Z}$, which is impossible. Hence, no integer is both even and odd. □

We now take a look at the more general notion of divisibility by any number.

[6] We again remind the reader that $\mathbb{Z}$ denotes the integers. We will be seeing a lot of $\mathbb{Z}$'s in this part of the course.

[7] Notice that we really need two distinct variables here!

Definition 10.3. Let $m, n \in \mathbb{Z}$. We say that m *divides* n if there exists a $k \in \mathbb{Z}$ such that $n = km$. We write $m \mid n$ when m divides n, and $m \nmid n$ otherwise.

This allows us to rewrite the definition of an even integer: n is even if and only if $2 \mid n$.

Grade-School Division

Recall the type of division we learned in 3rd grade prior to learning about fractions — given a number, say 27 apples, we wanted to know how we can split that evenly amongst, say 5 friends. Clearly, each friend gets 5 apples, with 2 leftover — that is, our division had a quotient and remainder. It is this sort of division that we will interest ourselves with for the rest of the course.

Theorem 10.4 (Division Algorithm)**.** *Let $k \geq 2$ be an integer. For any $n \in \mathbb{Z}$, there exist $q \in \mathbb{N}$ and $r \in \{0, 1, \ldots, k-1\}$, both unique, such that $n = qk + r$.*

That is to say, the quotient and remainder from grade-school are always unique — intuitively, we know this to be true, but let us see the proof.

Proof. We first prove the existence of q and r. Fix $k \geq 2$, and we apply induction on non-negative $n \in \mathbb{Z}$. [Of course, we flip everything around as necessary when $n < 0$.] For $n = 0$, we simply set $q = r = 0$. Now, assume the inductive hypothesis, and $n = kq + r$ for $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, k-1\}$. We then see that $n + 1 = kq + r + 1$, and we consider 2 cases.

Case I: $r < k - 1$. In this case, there is nothing to do, simply set $q' = q$ and $r' = r + 1$. Notice that $r' \in \{0, 1, \ldots, k-1\}$ in this case, so this is legal. Hence $n + 1 = q'k + r'$.

Case II: $r = k - 1$. Then $n + 1 = kq + r + 1 = kq + (k-1) + 1 = k(q+1)$. Hence, set $r' = 0$ and $q' = q + 1$, so $n + 1 = q'k + r'$.

Now, we prove uniqueness. Fixing $k \geq 2$ and some $n \in \mathbb{Z}$, suppose $n = qk + r = q'k + r'$ for $q, q' \in \mathbb{Z}$ and $r, r' \in \{0, 1, \ldots, k-1\}$. It suffices to show $q = q'$ and $r = r'$.

First, we have $n = qk + r = q'k + r'$. By some algebra, we write this as $k(q - q') = r' - r$. Since $q - q'$ is an integer, we see by the definition of divisibility that $k \mid (r' - r)$. Without loss of generality, assume $r' \geq r$. But then $r', r \in \{0, 1, \ldots, k-1\}$ implies $r' - r \in \{0, 1, \ldots, k-1\}$, so the divisibility condition is impossible unless $r' = r$.

From the fact that $r' = r$, we simply have $qk + r = q'k + r' \implies qk = q'k \implies q = q'$, so we are done. □

Notice that the assumption that r was taken from $\{0, 1, \ldots, k-1\}$ is very important!

Exercise 31. Replace $r \in \{0, 1, \ldots, k-1\}$ from the statement of the Division Algorithm with $r \in \mathbb{Z}$. Give a counterexample to show that uniqueness fails.

With the Division Algorithm in place, we now show that our way of writing numerics makes sense. For example, the number 123 is literally a string of digits, but we take this to mean

$$123 = 1 \times 10^2 + 2 \times 10^1 + 3 \times 10^0.$$

In fact, the representation of this number is unique in base 10, as the following theorem shows.

Theorem 10.5. *For any $n \geq 1$ and $k \geq 2$, there exist unique $r \in \mathbb{Z}^+$ and $d_0, d_1, \ldots, d_r \in \{0, 1, \ldots k-1\}$ such that $n = d_r k^r + d_{r-1} k^{r-1} + \cdots + d_1 k + d_0$ and $d_r \neq 0$.*

Taking $k = 10$, this simply says a number can be written uniquely in base 10. We prove existence and leave uniqueness to the reader.

Proof (of existence). We apply strong induction on $n \geq 1$. For our base case, we check n satisfying $1 \leq n \leq k-1$. In this case, we take $r = 0$ and $d_0 = n$.

Now, assume the inductive hypothesis, that the theorem holds for all $\ell < n$, where $n \geq 1$ is some integer. Now, we apply the Division Algorithm to n to write $n = kq + d_0$, where $d_0 \in \{0, 1, \ldots, k-1\}$. Suppose $n \geq k$, so $q \geq 1$. We apply the inductive hypothesis on q: write

$$q = d_r k^{r-1} + d_{r-1} k^{r-2} + \cdots + d_2 k + d_1,$$

for appropriate $d_1, \ldots, d_r \in \{0, 1, \ldots, k-1\}$ and $d_r \neq 0$. Hence

$$\begin{aligned} n = kq + d_0 &= k(d_r k^{r-1} + d_{r-1} k^{r-2} + \cdots + d_2 k + d_1) + d_0 \\ &= d_r k^r + d_{r-1} k^{r-1} + \cdots + d_2 k^2 + d_1 k + d_0, \end{aligned}$$

as expected. □

Exercise 32. The uniqueness proof is hidden inside the existence proof above. Rephrase the proof to account for uniqueness.

Modular Arithmetic

The division algorithm also justifies another important construction, which allows us to tell the time. In a 12-hour system, we say that 5 hours after 9:00 is not 14:00, but rather 2:00. In some sense, the clock "wraps around" after 12:00. We generalize this into *modular arithmetic*, which is ubiquitous across most of abstract algebra.

Definition 10.6. Let $k \geq 2$, and let $n \in \mathbb{Z}$, so by the Division Algorithm we write $n = kq + r$ for $r \in \{0, 1, \ldots, k-1\}$. The *remainder of n modulo k* is the number r, and we say that $m, n \in \mathbb{Z}$ are *congruent modulo k* if they have the same remainder modulo k.

Notice that we are justified in saying **the** remainder due to the uniqueness condition of the Division Algorithm. In speech, we often abbreviate "modulo" by simply saying "mod"; hence we write $m \equiv n \pmod{k}$ to mean m and n are congruent modulo k. Of course, when k is clear from context, we will be lazy and say "m and n are congruent."

Example 10.7. Let $k = 10$. Then $m \equiv n \pmod{10}$ if and only if m and n have the same last digit: e.g., $17 \equiv 7 \pmod{10}$. The reason for this follows from Theorem 10.5.

Example 10.8. Let $k = 2$. Then $n \equiv 0$ if and only if n is even, and $n \equiv 1$ if and only if n is odd.

The two following propositions are very important.

Proposition 10.9. *Let $k \geq 2$, and let $m, n \in \mathbb{Z}$. Then $m \equiv n \pmod{k}$ if and only if $k \mid (m-n)$. In particular, $n \equiv 0 \pmod{k}$ if and only if $k \mid n$.*

Proof. ($\implies$): Suppose $m \equiv n \pmod{k}$. Then $m = q_1 k + r$ and $n = q_2 k + r$ for $r \in \{0, 1, \ldots, k-1\}$ and $q_1, q_2 \in \mathbb{Z}$. Now $m - n = q_1 k - q_2 k = k(q_1 - q_2)$, which is a multiple of k.

($\impliedby$): Suppose $k \mid (m-n)$. Write $m = q_1 k + r_1$ and $n = q_2 k + r_2$ by the Division Algorithm. Now $m - n = (q_1 - q_2)k + (r_1 - r_2)$. Since $k \mid (m-n)$, we have $k \mid (r_1 - r_2)$, but by the fact we chose $r_1, r_2 \in \{0, 1, \ldots, k-1\}$ by the Division Algorithm, we must have $r_1 - r_2 = 0$. Hence $r_1 = r_2$, so that $m \equiv n \pmod{k}$. □

Proposition 10.10. *Let $k \geq 2$. Suppose $m \equiv m'$ and $n \equiv n' \pmod{k}$. Then $m+n \equiv m'+n'$ and $mn \equiv m'n' \pmod{k}$.*

Exercise 33. Prove the above proposition.

Example 10.11. Let $k = 10$. Then $13 + 202 \equiv 3 + 2 = 5 \pmod{10}$. Similarly, $2 \cdot 13 \equiv 2 \cdot 6 \pmod{10}$.

Here is an interesting example: the divisibility rule for 3. Notice that this *only* works if we are in base 10.

Proposition 10.12 (Divisibility Rule for 3)**.** *Let $n \in \mathbb{Z}_{\geq 0}$. Then $3 \mid n$ if and only if the sum of the digits of n is also divisible by 3.*

Proof. By Theorem 10.5, write $n = d_r(10)^r + d_{r-1}(10)^{r-1} + \cdots d_1(10) + d_0$. Now, by the previous proposition, we see that $10 \equiv 1 \pmod{3}$, so that $10^j \equiv 1^j = 1 \pmod{3}$ for any $j \in \mathbb{Z}^+$. Hence, the above reduces to

$$\begin{aligned} n &\equiv d_r(1)^k + d_{r-1}(1)^{k-1} + \cdots + d_1(1) + d_0 \pmod{3} \\ &\implies n \equiv d_r + d_{r-1} + \cdots + d_1 + d_0 \pmod{3}, \end{aligned}$$

hence n is congruent to the sum of its digits in base 10, modulo 3. Now, Proposition 10.9 finishes the proof. □

We end with some exercises.

Exercise 34. Prove for any $n \in \mathbb{Z}^+$, we have $7 \mid (5^{2n} + 3 \cdot 2^{5n-2})$.

Exercise 35. Prove that $25 \mid (4^{200} - 1)$.

Exercise 36. Find the remainder of $1^5 + 2^5 + \cdots + 2022^5$ when divided by 4.

11 Divisibility II: Common Divisors

We start with a definition.

Definition 11.1. Let $m, n \in \mathbb{Z}$. The *greatest common divisor* (GCD) of m and n is the largest $d \in \mathbb{Z}^+$ such that $d \mid m$ and $d \mid n$. We denote the GCD of m and n by $\gcd(m, n)$.

We note that some algebra texts simply write "(m, n)" for the GCD of m and n. Alternatively stating the definition, $d_0 = \gcd(m, n)$ if and only if the following conditional holds:

$$\text{If } d \mid m \text{ and } d \mid n, \text{ then } d \leq d_0.$$

We view some examples.

Example 11.2. We have $\gcd(24, 21) = 3$, as $24 = 2^3 \times 3$ and $21 = 3 \times 7$. Similarly, $\gcd(36, 54) = 2 \times 3^2 = 18$, as $36 = 2^2 \times 3^2$ and $54 = 2 \times 3^3$.

Example 11.3. Let p, q be distinct prime numbers. Then $\gcd(p, q) = 1$ by their primality, as expected. However, the converse is not true: $\gcd(25, 49) = 1$, but neither 25 nor 49 are prime. However, this does suggest to us the following definition.

Definition 11.4. Let $m, n \in \mathbb{Z}$. We say m, n are *relatively prime* (or *coprime*) if $\gcd(m, n) = 1$; that is, they have no common prime factors.

Hence, the previous example tells us that any two prime numbers are coprime, but composite numbers can form coprime pairs as well.

Bezout's Lemma

Consider the following equation of a line: $ax + by = c$, where $a, b, c \in \mathbb{Z}$. In applications, we often care about whether this line passes through a *lattice point*, i.e., a point in the xy-plane where both coordinates are integers. Let us consider two exmaples firsts, before we develop the theory.

Example 11.5. Does $2x + 6y = 5$ pass through any lattice points?

Solution. No: notice we can write $5 = 2x + 6y = 2(x + 3y)$. If (x, y) is a lattice point on the line, then we must that 5 is an integer multiple of 2; i.e., 5 is even. This is impossible. •

Example 11.6. Does $23x + 24y = 17$ pass through any lattice points?

Solution. Yes, easily: first notice that $23(-1) + 24(1) = 1$. Now, multiplying by 17 gives the desired result: $(-17, 17)$ sits on the line. •

For the first of these examples, notice that the coefficients $a = 2$ and $b = 6$ satisfied $\gcd(a, b) = 2$, which ended up showing up in our proof of impossibility. On the other hand, in the second example, $\gcd(a = 23, b = 24) = 1$, which nicely divides 17 (obviously) and thus gave us a lattice point. Hence, the GCD is closely related with the lattice point problem. While comparing prime factors is easy for computing the GCD for small numbers, it falls off quickly as factorization becomes increasingly more difficult for larger numbers. However, we introduce an efficient method to find the GCD, which does not involve factorization, only long division, which is far less expensive.

Theorem 11.7 (Euclidean Algorithm)**.** *Suppose $a, b \in \mathbb{Z}^+$ and $a \geq b$. Then this algorithm gives the* $\gcd(a, b)$ *when it terminates:*

(1) *Firstly, if $a = b$, then clearly* $\gcd(a, b) = a = b$.

(2) *Otherwise, use the Division Algorithm to write $a = q_0 b + r_0$, for some $q \in \mathbb{Z}^+$ and $r_0 \in \{0, 1, \ldots, b - 1\}$. If $r_0 = 0$, then the algorithm terminates and* $\gcd(a, b) = b$.

(3) *Else if $r_0 > 0$, find q_1, r_1 by the Division Algorithm with $b = q_1 r_0 + r_1$. If $r_1 = 0$, then* $\gcd(a, b) = r_0$.

...

$(k + 2)$ *Else if $r_k > 0$, find q_{k+1}, r_{k+1} by the Division Algorithm with $r_{k-1} = q_{k+1} r_k + r_{k+1}$...*

At the point of termination, we have $\gcd(a, b) = r_j$*, where j is the last index k such that $r_k > 0$.*

The proof of the Euclidean algorithm is left in the official Math 13 notes, Exercise 4.2.8, and of course, the algorithm could be used for negative integers in the obvious way. Hopefully, these examples are convincing enough to show that this theorem holds.

Example 11.8. We compute $\gcd(32, 60)$. Setting $a = 60$ and $b = 32$, we write

$$\begin{aligned} 60 &= 1 \cdot \mathbf{32} + 28 \\ 32 &= 1 \cdot \mathbf{28} + 4 \\ 28 &= 7 \cdot \mathbf{4} + 0. \end{aligned}$$

Hence $\gcd(60, 32) = 4$.

Example 11.9. We compute $\gcd(657, 306)$. Setting $a = 657$ and $b = 306$, we write

$$\begin{aligned} 657 &= 2 \cdot 306 + 45 \\ 306 &= 6 \cdot 45 + 36 \\ 45 &= 1 \cdot 36 + 9 \\ 36 &= 4 \cdot 9 + 0. \end{aligned}$$

Hence $\gcd(657, 306) = 9$.

It turns out that the solution to our lattice point problem is a corollary of this GCD-finding technique.

Theorem 11.10 (Bezout's Lemma)**.** *Let $a, b, c \in \mathbb{Z}$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $\gcd(a, b) \mid c$.*

Proof. ($\implies$): Suppose for contradiction that there exist $x, y \in \mathbb{Z}$ such that $ax+by = c$, yet $\gcd(a, b) \nmid c$. Since $\gcd(a, b) \mid a, b$ by definition, we have $\gcd(a, b) \mid (ax+by)$, but $c = ax+by$, a contradiction.

($\impliedby$): Use the Euclidean algorithm to find $\gcd(a, b) = r_j$ for the integers $r_0, r_1, \ldots, r_j$. Notice that each r_i is a linear combination of a's and b's, so "reversing" the algorithm as appropriate[8] allows us to find $x', y' \in \mathbb{Z}$ such that $\gcd(a, b) = ax' + by'$. Since $\gcd(a, b) \mid c$, multiplying through by $c/\gcd(a, b)$ finishes the proof. □

If this proof was unsatisfying, see the exercises at the end of this section for a different proof. We now give important corollaries of Bezout's Lemma.

Corollary 11.11. *Let $a, b \in \mathbb{Z}$. Then a, b are coprime if and only if there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$.*

Proof. ($\implies$): This follows from Bezout's Lemma with $\gcd(a, b) = 1$.

($\impliedby$): Let $d = \gcd(a, b)$. Suppose there exist $x, y \in \mathbb{Z}$ with $1 = ax + by$. Then $d|a$ and $d|b$, so that $a = dm$ and $b = dn$ for some $m, n \in \mathbb{Z}$. Hence $1 = dmx + dny = d(mx + ny)$, so that 1 is a multiple of d. Hence $d = 1$; i.e., $\gcd(a, b) = 1$. □

Corollary 11.12. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and a, b are coprime, then $a \mid c$.*

Proof. Suppose $a \mid bc$ and a, b are coprime. By the previous corollary, there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$, so that $c = acx + bcy$. However, $a \mid bc$, so $bc = an$ for some $n \in \mathbb{Z}$. It follows that $c = acx + bcy = acx + y \cdot an = a(cn + ny)$, so $a \mid c$. □

In particular, we get these results when a is prime in the corollary above.

Proposition 11.13. *Let p be prime, and let $a \in \mathbb{Z}$. Then $\gcd(a, p) = 1$ if and only if $p \nmid a$.*

Proof. We know that $\gcd(a, p) \mid p$. But p is prime, so either $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. The proposition easily follows from this. □

Theorem 11.14 (Euclid's Lemma)**.** *Let p be prime, and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$. Alternatively stated, $ab \equiv 0 \pmod{p}$ implies $a \equiv 0$ or $b \equiv 0 \pmod{p}$.*

Proof. Suppose $p \mid ab$. If $p \mid a$, then we are done. Else if $p \nmid a$, we see by Corollary 11.12 and the previous proposition that $\gcd(p, a) = 1$, so that $p \mid b$. □

[8] See Math 13 official notes, p. 120-121.

Fundamental Theorem of Arithmetic: Uniqueness

With all of this in place, we are now ready to prove the uniqueness part of the Fundamental Theorem of Arithmetic (FTA, Theorem 8.2). We first state a generalization of Euclid's Lemma, which can be proved by induction.

Proposition 11.15. *Let p be prime and $a_1, \ldots, a_n \in \mathbb{Z}$. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some $i = 1, 2, \ldots, n$.*

We now proceed with the proof of the uniqueness of the factorization in the FTA.

Proof of Uniqueness of Factorization. Suppose $n \geq 2$ and $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ for primes $p_1, \ldots, p_k, q_1, \ldots, q_\ell$. Without loss of generality, consider the prime q_1 on the factorization. We claim $q_1 = p_i$ for some $1 \leq i \leq k$. We know $q_1 \mid n = p_1 p_2 \cdots p_k$. Hence $q_1 \mid p_i$ for some $i = 1, 2, \ldots, n$ by the proposition above. Since q_1 and p_i are both prime, we must have $q_1 = p_i$. Of course, this argument works for any q_j, $1 \leq j \leq \ell$, so we are done. □

The uniqueness in FTA allows a quick proof of the irrationality of $\sqrt{2}$.

Theorem 11.16. *We have $\sqrt{2} \notin \mathbb{Q}$.*

Proof. Assume for contradiction that $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = m/n$ for some $m, n \in \mathbb{Z}$, $n \geq 0$. Since $\sqrt{2} > 0$, we may assume $m, n > 0$, so that

$$\sqrt{2} = \frac{m}{n} \implies 2 = \frac{m^2}{n^2} \implies 2n^2 = m^2.$$

Write $n = p_1 p_2 \ldots p_k$ and $m = q_1 q_2 \ldots q_\ell$ for primes p_i, q_j. Hence $n^2 = \prod p_i^2$ and $m = \prod q_j^2$. In particular, each prime q_j in the factorization m^2 is doubled, so if $2 = q_j$ for some $j \leq \ell$, it must show up an even number of times in the factorization of m^2, and similarly for n^2. [Of course, if 2 does not show up as one of the q_j, then it occurs 0 times, which is still even.] But now $2n^2$ has an odd number of 2's in its factorization, but $2n^2 = m^2$. By the uniqueness part of FTA, we have a contradiction, so $\sqrt{2} \notin \mathbb{Q}$. □

Here are some exercises to try.

Exercise 37. Prove that if $\gcd(a, b) = 1$, then $a \mid c$ and $b \mid c$ implies $ab \mid c$.

Exercise 38. Use the following steps to give an alternative proof of Bezout's Lemma. Fix $m, n \in \mathbb{Z}^+$. We define $I := \{xm + yn : x, y \in \mathbb{Z}\}$.

(a) Show that if $a, b \in I$, then $ka + \ell b \in I$ for all $k, \ell \in \mathbb{Z}$.

(b) Show that I contains an element of $\mathbb{Z}^+$.

By part (b), well-ordering tells us that there exists a minimal element in $I \cap \mathbb{Z}^+$; call it d.

(c) Show $d\mathbb{Z} \subseteq I$.

(d) Show that if $d' \in I$, then the remainder of d' modulo d is also in I.

(e) Show that $d\mathbb{Z} = I$.

(f) Show $d \mid m$ and $d \mid n$.

(g) Show that if c is a common divisor of m and n, then $c \mid k$ for every $k \in I$.

(h) Show that $d = \gcd(m, n)$, and deduce Bezout's Lemma: $xm + yn = k$ only has integer solutions $(x, y) \in \mathbb{Z}^2$ if and only if $\gcd(m, n) \mid k$.

Exercise 39. Let $A = \{0\} \cup \{2^n : 0 \leq n \leq 9\}$, $B = \{2n : 0 \leq n \leq 10\}$, and $C = \{0, 1, \ldots, 10\}$. Define $f : A \to C$ and $g : B \to C$ by

$$f(a) = c \text{ if } 11 \mid (a - c),$$

$$g(b) = c \text{ if } 11 \mid (b - c).$$

Prove that both f and g are well-defined and bijective.

Exercise 40. Give an example of $a, b, j, k, n \in \mathbb{Z}^+$ such that $a^k \equiv b^k \pmod{n}$ and $k \equiv j \pmod{n}$ but $a^j \not\equiv b^k \pmod{n}$.

Exercise 41. Let p be a prime. Show that $\binom{p}{r}$ is a multiple of p for $1 \leq r \leq p - 1$, and use induction and this fact to prove Fermat's Little Theorem: if p is prime, then $a^p \equiv a \pmod{p}$ for any $a \in \mathbb{Z}$.

Exercise 42. Show that the only prime number having the form $n^2 - 4$, $n \in \mathbb{Z}^+$, is 5.

Exercise 43. Use the following steps to prove Wilson's Theorem. Let p be a prime.

(a) Show that if $1 \leq k \leq p - 1$, then the linear congruence $ax \equiv 1 \pmod{p}$ has a unique solution modulo p.

(b) Show that $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

(c) Show that $(p - 1)! \equiv -1 \pmod{p}$.

(d) Now, let $n \in \mathbb{Z}^+$. Show that $(n - 1)! \equiv 0 \pmod{n}$.

Exercise 44. Show that every integer $n > 1$ can be decomposed into $n = st$, where t is a perfect square and s is *squarefree*: i.e., s is not divisible by any perfect square other than 1.

Exercise 45. Let $a, b \in \mathbb{Z}$, and write $a = p_1 p_2 \cdots p_m$, $b = q_1 q_2 \cdots q_n$ by FTA. Prove that if $\gcd(a, b) = 1$, then $p_i \neq q_j$ for all $1 \leq i \leq m$, $1 \leq j \leq n$.

12 Divisibility III: Miscellaneous Topics

In this section, we give a few more classic proofs that may be skipped in most Math 13 classes. The first of these is an ancient argument, dating to Euclid's *Elements*, that all math students should see at some point in their careers.

Theorem 12.1 (Euclid's Theorem)**.** *There are infinitely many prime numbers.*[9]

Proof. Suppose for contradiction that there are only finitely many primes $p_1, \ldots, p_n$. Define $n := p_1 p_2 \cdots p_n + 1$. Then $n \equiv 1 \pmod{p_i}$ for all $i \in \{1, 2, \ldots, n\}$, so $p_i \nmid n$. However, FTA tells us that n must factor into a product of primes, so the list of primes $p_1, \ldots, p_n$ is missing at least one prime number. Thus, there must be infinitely many primes. □

[9] Not to be confused with Euclid's Lemma (Theorem 11.14). Sometimes, Euclid's Lemma is called Euclid's 1st Theorem, and this statement is called Euclid's 2nd Theorem.

The next theorem is also ancient, and is usually skipped in Math 13, yet appears often in Math 120B and higher abstract algebra (albeit in generalized forms).

Theorem 12.2 (Chinese Remainder Theorem)**.** *Suppose $k_1, \ldots, k_n \geq 2$ are pairwise relatively prime; i.e.,* $\gcd(k_i, k_j) = 1$ *for all $i \neq j$, $i, j \in \{1, 2, \ldots, n\}$, and let $r_1, r_2, \ldots, r_n \in \mathbb{Z}$. Then there exists some $x \in \mathbb{Z}$ such that*

$$\begin{aligned} x &\equiv r_1 \pmod{k_1} \\ x &\equiv r_2 \pmod{k_2} \\ &\cdots \\ x &\equiv r_n \pmod{k_n}. \end{aligned}$$

We prove the case where $n = 2$, but the general case follows the same proof idea.

Proof for $n = 2$. Let k_1, k_2 be coprime, and take $r_1, r_2 \in \mathbb{Z}$. We construct an x such that $x \equiv r_1 \pmod{k_1}$ and $x \equiv r_2 \pmod{k_2}$.

By Bezout's Lemma, there exist $y, z \in \mathbb{Z}$ such that $yk_1 + zk_2 = 1$. Hence $yk_1 \equiv 1 \pmod{k_2}$ and $zk_2 \equiv 1 \pmod{k_1}$. Let $x := r_2 yk_1 + r_1 zk_2$. Now, we verify

$$x \equiv r_2(yk_1) \equiv r_2 \cdot 1 = 1 \pmod{k_2},$$

$$x \equiv r_1(zk_2) \equiv r_1 \cdot 1 = 1 \pmod{k_1},$$

so we are done. □

Note that the solution x in the proof above is not necessarily unique, but it is unique *modulo* $k_1 k_2$, so once we have determined a solution x, we immediately know that $x + ak_1k_2$ is also a solution for any $a \in \mathbb{Z}$. Try to find the general solution in the exercises below.

Exercise 46. Solve this system of congruence if a solution exists: $\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{13}. \end{cases}$

Exercise 47. Solve this system of congruence if a solution exists: $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 5 \pmod{15}. \end{cases}$

Exercise 48. Prove the general case of the Chinese Remainder Theorem.

13 Well-Ordering

In this section, we give a basis to *why* our method of proof by induction "works." The material here is slightly more philosophical in nature, but it is of interest. We first state this property of the natural numbers $\mathbb{N} := \mathbb{Z}_{\geq 0}$:

Fact 13.1 (Well-Ordering of $\mathbb{N}$)**.** *Let $X \subseteq \mathbb{N}$ be nonempty. Then X has a minimum, i.e., there exists some $n \in X$ such that if $m \in X$, then $n \leq m$.*

Notice that we are careful with labeling this statement as merely a "fact" — depending on your axioms, this is either assumed to be true, or is a provable theorem about the natural numbers $\mathbb{N}$. Equivalently, we can also state well-ordering as follows: *there is no infinite descending sequence of natural numbers*, as otherwise if $a_1 > a_2 > \cdots$ is such a sequence, the set $\{a_1, a_2, \ldots, \}$ has no minimum.

Using this, we now turn our attention to the inductive argument once more. Suppose we want to prove $(\forall n \in \mathbb{N})\, P(n)$, for some property $P(n)$ depending on n. That is, if we define $Y := \{n \in \mathbb{N} : P(n) \text{ is true}\}$, induction is really showing $Y = \mathbb{N}$. More precisely, induction is showing $\mathbb{N} \subseteq Y$, as the other direction follows from definition. From induction, we have a base case: $0 \in Y$. Second, induction tells us that if $n \geq 0$ and $n \in Y$, then $n + 1 \in Y$. But this tells us that $X := \mathbb{N} \setminus Y$ has no minimum, so $X = \varnothing$ by well-ordering. Hence $Y = \mathbb{N}$ as desired, and we have just proven induction.

Appealing to the well-ordering property of $\mathbb{N}$ has more uses than just for doing induction. We demonstrate the *contradiction of minimality* technique which can be invoked once we have well-ordering by giving two proofs of the irrationality of $\sqrt{2}$ (which we proved before using FTA).

Proof 1. Suppose for contradiction that $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = p/q$ for some $p, q \in \mathbb{N}$, $q \neq 0$. By the well-ordering property of $\mathbb{N}$, we can suppose that q is minimally chosen. Clearly, $q > 1$, as $q = 1$ implies $\sqrt{2} \in \mathbb{N}$, which we know to be untrue. We note the identity

$$\sqrt{2} = \frac{2 - \sqrt{2}}{\sqrt{2} - 1} \iff \frac{p}{q} = \frac{2 - p/q}{p/q - 1} = \frac{2q - p}{p - q}.$$

Noting that $1 < \sqrt{2} < 2$, we see that $1 < p/q < 2 \implies q < p < 2q$. Hence $0 < p - q < q$, which contradicts minimality of q: we saw $\sqrt{2} = (2q - p)/(p - q)$. □

Proof 2. Suppose for contradiction that $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = p/q$ for some $p, q \in \mathbb{N}$, $q \neq 0$. By the well-ordering property of $\mathbb{N}$, we can suppose that q is minimally chosen. Clearly, $q > 1$, as $q = 1$ implies $\sqrt{2} \in \mathbb{N}$, which we know to be untrue. Now, $2 = p^2/q^2 \implies 2q^2 = p^2$, so $2 \mid p^2$. By Euclid's Lemma, $2 \mid p$. Hence $p = 2p_1$ for some $p_1 \in \mathbb{N}$, so that $2q^2 = p^2 = 4p_1^2$. Simplifying, we see $q^2 = 2p_1^2$, so $2 \mid q$. Hence $\sqrt{2} = \frac{p/2}{q/2}$, where both the top and bottom are integers, but $q/2 < q$, contradicting minimality. □

14 Relations I: The Basic Theory

Let A, B be sets. Recall that the Cartesian product $A \times B$ is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. Subsets of $A \times B$ have a special name: relations.

Definition 14.1. Let A, B be sets. A *binary relation* $\mathcal{R}$ *over* A *and* B is a subset $\mathcal{R} \subseteq A \times B$. Similarly, if A is a set, a *binary relation* $\mathcal{R}$ *on* A is a subset $\mathcal{R} \subseteq A \times A =: A^2$. In place of $(a, b) \in \mathcal{R}$, we will often write $a \,\mathcal{R}\, b$.

Of course, this definition generalizes.

Definition 14.2. Let A be a set. An *n-ary relation on A* is any subset of A^n.

Example 14.3. Let A be a set. The following are common relations we see.

1. The *empty relation* on A is given by $\mathcal{R} = \varnothing \subseteq A^2$.
2. The *total relation* on A is given by $\mathcal{R} = A^2$.
3. Equality is a relation on A, when viewed as the set $\mathcal{R}_= = \{(a, a) : a \in A\}$.
4. Inequality is a relation on A, when viewed as the set $\mathcal{R}_\neq = A^2 \setminus \mathcal{R}_=$.

5. Order $(<, \leq)$ is a relation on $\mathbb{R}$.

6. Equivalence modulo $k \geq 2$ $(\equiv)$ is a relation on $\mathbb{Z}$.

Here is an example of a 3-ary, or ternary relation.

Example 14.4. Let $\mathcal{R} \subseteq \mathbb{R}^3$ be the relation on $\mathbb{R}$ given by $(x, y, z) \in \mathcal{R}$ if $x + y = z$, that is,

$$\mathcal{R} = \{(x, y, z) \in \mathbb{R}^3 : x + y = z\}.$$

Then $\mathcal{R}$ is a ternary relation on $\mathbb{R}$.

Often, we are concerned about whether our relations specify certain properties. Here are some common ones:

Definition 14.5. Let A be a set, and let $\mathcal{R} \subseteq A \times A$ be a binary relation on A. We say that $\mathcal{R}$ is *reflexive* if $a \mathcal{R} a$ for all $a \in A$. In contrast, $\mathcal{R}$ is *irreflexive* if $a \mathcal{R} a$ is never true for any $a \in A$.

Definition 14.6. Let A be a set, and let $\mathcal{R} \subseteq A \times A$ be a binary relation on A. We say that $\mathcal{R}$ is *symmetric* in the case that for any $a, b \in A$, $a \mathcal{R} b$ if and only if $b \mathcal{R} a$.

Exercise 49. Refer back to Example 14.3. Which of these six relations are reflexive? ...irreflexive? ...symmetric?

Finally, we have one more important property.

Definition 14.7. Let A be a set, and let $\mathcal{R} \subseteq A \times A$ be a binary relation on A. We say that $\mathcal{R}$ is *transitive* in the case that for any $a, b, c \in A$, if $a \mathcal{R} b$ and $b \mathcal{R} c$, then $a \mathcal{R} c$.

In particular, the equality relation "=" on a set is reflexive, symmetric, and transitive. Relations that have these three properties allow us to generalize our notion of "equality" on a certain set, and thus they are named appropriately.

Definition 14.8. Let A be a set, and let $\mathcal{R} \subseteq A \times A$ be a binary relation on A. We say that $\mathcal{R}$ is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Often, instead of using the symbol $\mathcal{R}$, we use the tilde "$\sim$" instead when we are discussing equivalence relations. Additionally, when we have $a \sim b$ for some $a, b \in A$, we say that a and b are *equivalent*. **We do not say "a and b are equal"** — notice the difference in meaning between *equivalence* and *equality*! We now view some examples of equivalence relations.

Example 14.9. Fix an integer $k \geq 2$. We claim congruence modulo k is an equivalence relation on $\mathbb{Z}$:

Proof. To show that $\equiv$ is an equivalence relation, we need to show that it is reflexive, symmetric, and transitive. Reflexivity and symmetry are obvious. Now, suppose $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b$ and $b \equiv c \pmod{k}$. Then $k \mid (a-b)$ and $k \mid (b-c)$. But then $(a-b)+(b-c) = a - c$ is also a multiple of a, so $k \mid (a - c) \iff a \equiv c \pmod{k}$, so $\equiv$ is transitive. $\square$

Exercise 50. Define a relation $\sim$ on $\mathbb{R}$ by $x \sim y$ if and only if $x - y \sim \mathbb{Z}$. Show that $\sim$ is an equivalence relation on $\mathbb{R}$. How can you view this exercise as a generalization of the previous one?

Example 14.10. Let $f : A \to B$ be a function. Define the binary relation $\sim$ on A given by $a \sim b$ if $f(a) = f(b)$. We show that $\sim$ is an equivalence relation.

Proof. Again, we show that $\sim$ is reflexive, symmetric, and transitive. Clearly, $a \sim a$ as $f(a) = f(a)$, and $a \sim b \iff b \sim a$ as $f(a) = f(b) \iff f(b) = f(a)$. Now, take $a, b, c \in A$ such that $a \sim b$ and $b \sim c$. Then $f(a) = f(b)$ and $f(b) = f(c)$. But this implies $f(a) = f(c)$, so $\sim$ is transitive. Hence, $\sim$ is an equivalence relation on A. □

Example 14.11. Here is a nontrivial example of an equivalence relation. Let $A := [0, 1] \times [0, 1]$, the unit square in the xy-plane. Define a binary relation $\sim$ on A by $(a, b) \sim (c, d)$ if $|a - c|, |b - d| \in \{0, 1\}$. Again, we claim that $\sim$ is an equivalence relation.

Proof. Symmetry is obvious, so we check reflexivity first. Certainly, we have $|a - a| = |b - b| = 0 \in \{0, 1\}$, so that $(a, b) \sim (a, b)$.

For transitivity, suppose $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$. We check that $|a_1 - a_3| \in \{0, 1\}$; a similar argument works for showing $|b_1 - b_3| \in \{0, 1\}$. We have $|a_1 - a_2|, |a_2 - a_3| \in \{0, 1\}$. Now, we split cases:

Case I: $|a_1 - a_2| = |a_2 - a_3| = 0$. In this case, we have $a_1 = a_2 = a_3$, so that $|a_1 - a_3| = 0 \in \{0, 1\}$.

Case II: $|a_1 - a_2| = 1$ and $|a_2 - a_3| = 0$. In this case, $a_2 - a_3$, so that $|a_1 - a_2| = |a_1 - a_3| = 1 \in \{0, 1\}$.

Case III: $|a_1 - a_2| = 0$ and $|a_2 - a_3| = 1$. Similar to the previous case.

Case IV: $|a_1 - a_2| = |a_2 - a_3| = 1$. Here, we must utilize our assumption that our equivalence relation is defined on the set $A = [0, 1]^2$. Hence, the only way for $|a_1 - a_2| = |a_2 - a_3| = 1$ to occur is if $a_1, a_2, a_3 \in \{0, 1\}$. Hence, if $a_1 = 0$, we immediately see $a_2 = 1$ and $a_3 = 0$, and if $a_1 = 1$, then $a_2 = 0$ and $a_3 = 1$. Hence $|a_1 - a_3| = 0 \in \{0, 1\}$.

This shows that $\sim$ is transitive, so that $\sim$ is an equivalence relation on A. □

In topology, the equivalence relation above describes how to build a 2-*torus* (a donut) from a unit square. A few more interesting examples are given in the exercises below.

Exercise 51. Let X be an infinite set, and define the relation $\sim$ on $\mathcal{P}(X)$ where $A \sim B$ if and only if $A \oplus B$ is finite. Prove that $\sim$ is an equivalence relation.

Exercise 52. Let A be a set, and define a relation $\sim$ on A^A by $f \sim g$ if and only if f and g are *conjugate*, i.e., there exists an invertible map $\varphi \in A^A$ satisfying $g = \varphi^{-1} \circ f \circ \varphi$. Show that $\sim$ is an equivalence relation, and find all elements equivalent to the identity function on A.

Exercise 53. Define a relation $\sim$ on $\mathbb{R}^2 \setminus \{(0, 0)\}$ given by $u \sim v$ if and only if there exists some $k \in \mathbb{R} \setminus \{0\}$ such that $u = kv$. That is, $u \equiv v$ if and only if u is a *scalar multiple* of v. Show that $\sim$ is an equivalence relation. The equivalence classes of $\sim$ define what is called *projective space* in algebraic geometry.

15 Relations II: Partitions and Well-Definition

Recall that an equivalence relation on a set A is a binary relation that is reflexive, symmetric, and transitive. In this section, we will justify the naming of these relations as "equivalent" by seeing how it "collapses" the set A into something simpler to analyze. We start with a definition.

Definition 15.1. Let $\sim$ be an equivalence relation on a set A, and let $a \in A$. The *equivalence class of* a is the set of all $b \in A$ such that $a \sim b$. Notationally:

$$[a] := \{b \in A : a \sim b\}.$$

The element a is called a *representative* of the equivalence class $[a]$.

Example 15.2. Consider the equivalence relation $\equiv$ on $\mathbb{Z}$ given by congruence modulo 5. Then we have 5 equivalence classes, corresponding to the remainders modulo 5: $[0], [1], [2], [3], [4]$. More generally, congruence modulo k gives us k equivalence classes, corresponding to the remainders modulo k.

We should notice that each equivalence class above is disjoint: for example, $[0] \cap [3] = \varnothing$. Also, equivalence classes are not uniquely specified by representative: for example, $[3] = [8]$ under congruence modulo 5. Furthermore, the union of every equivalence class gives the whole set:

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4].$$

Hence, we say that the equivalence classes of $\equiv$ *partition* the set, as we define below.

Definition 15.3. Let A be a set. A *partition of* A is a collection $\mathcal{C}$ of subsets of A such that:

- For every $a \in A$, then there exists some P such that $a \in P$ for some $P \in \mathcal{C}$. That is, every element of a lies in some set P inside $\mathcal{C}$.
- For any pair of sets $P, Q \in \mathcal{C}$, either $P \cap Q = \varnothing$ or $P = Q$.

The sets $P \in \mathcal{C}$ are called *pieces of the partition* $\mathcal{C}$ of A.

Partitions essentially form an equivalence relation on a set, as demonstrated below.

Theorem 15.4. *Let $\sim$ be an equivalence relation on a set A. Then*

(1) *The equivalence classes of $\sim$ form a partition of A;*

(2) *If $\mathcal{C}$ is any partition of A, then $\mathcal{C}$ defines a natural equivalence relation $\sim$ on A.*

Proof. We prove (1). First, notice that for any $a \in A$, we have $a \in [a]$ as $a \sim a$ [reflexivity of $\sim$]. This gives us the first condition for being a partition. Now, take $[a], [b]$ to be equivalence classes, and suppose $[a] \cap [b] \neq \varnothing$. Then there exists some $c \in [a] \cap [b]$, so we have $a \sim c$ and $c \sim b$. By transitivity, we have $a \sim b$, so $[a] = [b]$.

Now, for (2), define the relation $\sim$ on A given by $a \sim b$ if there exists $P \in \mathcal{C}$ such that $a \in P$ and $b \in P$ — i.e., a and b lie in the same piece of the partition. The reader can show that $\sim$ is reflexive, symmetric, and transitive. □

The partition determined by the equivalence classes of some relation $\sim$ on A is given a special name.

Definition 15.5. Let A be a set, and let $\sim$ be an equivalence relation on A. The *quotient of A by $\sim$* is the set of all equivalence classes of $\sim$. Notationally:

$$A/\sim := \{[a] : a \in A\}.$$

We stress that $A/\sim$ is a set of sets. There is, as with many other things, an important function $A \to A/\sim$:

Definition 15.6. Let A be a set, and let $\sim$ be an equivalence relation on A. The *quotient map* is the function $\pi : A \to A/\sim$ given by $\pi(a) = [a]$.

In other texts, the map π is sometimes called the *projection map* or the *canonical surjection.*[10] We also note that $\pi(a) = \pi(b)$ if and only if $a \sim b$.

Example 15.7. Consider the equivalence relation $\equiv$ on $\mathbb{Z}$ given by congruence modulo k. We have seen that we have k equivalence classes, namely $[0], [1], \ldots, [k-1]$. Hence

$$(\mathbb{Z}/\equiv) = \{[0], [1], \ldots, [k-1]\}.$$

However, it is often more useful to think of $\mathbb{Z}/\equiv$ as simply the integers from 0 to $k-1$, so we will often drop the square brackets when discussing this set. In abstract algebra, this quotient set is known as the *ring of integers modulo k* and is denoted $\mathbb{Z}_k$ or $\mathbb{Z}/k\mathbb{Z}$.

Example 15.8. Let $X := \mathbb{Z} \times \mathbb{Z}^\times$. [Here, $\mathbb{Z}^\times$ denotes the non-zero integers.] Define the relation $\sim$ on X such that $(m, n) \sim (m', n')$ whenever $nm' = mn'$. For example, $(1, 2) = (2, 4)$, as $2 \cdot 2 = 1 \cdot 4$. Consider the set $X/\sim$, which is a set of equivalence classes $[(m, n)]$. For example, we see

$$[(2, 3)] = \{(2, 3), (4, 6), (6, 9), (8, 12), \ldots\}.$$

This pattern looks familiar to us, as we know that

$$\frac{2}{3} = \frac{4}{6} = \frac{6}{9} = \frac{8}{12} = \cdots.$$

Hence, this gives us a rigorous definition of the *rational numbers* $\mathbb{Q}$, as we can simply set $\mathbb{Q} := X/\sim$, and denote m/n in place of $[(m, n)]$. Addition and multiplication on $\mathbb{Q}$ are defined in the expected way:

$$[(m, n)] \cdot [(m', n')] := [(mm', nn')],$$

$$[(m, n)] + [(m', n')] := [(mn' + nm', nn')].$$

The reader should verify that these definitions are exactly what happens when we write m/n and m'/n' in place of the equivalence relation notation.

Example 15.9. Let $X := [0, 1]$, the unit real interval. Define the equivalence relation $\sim$ on X by

$$\sim := \{(t, t) : t \in X\} \cup \{(1, 0), (0, 1)\}.$$

That is, we have $0 \sim 1$ and $t \sim t$ for all $t \in X$. The reader should verify that this is indeed an equivalence relation, and the quotient set $X/\sim$ is given by $\{[t] : t \in [0, 1)\}$, where we of course have $[0] = [1]$. The sets $[t]$, for $t \in (0, 1)$ are singleton sets, and $[0] = \{0, 1\}$. Geometrically, we have taken the unit real interval and connected the endpoints, to form a closed loop.

Exercise 54. Draw a picture corresponding to the geometric interpretation above.

[10] Why is it obvious that this function is surjective?

Example 15.10. Let $X := [0,1]^2$, the unit square. Define the equivalence relation $\sim$ on X by precisely setting $(0,t) \sim (1,t)$ and $(t,0) \sim (t,1)$ for all $t \in [0,1]$. The quotient set $X/\sim$ thus describes a torus, as outlined in the next exercise.

Exercise 55. Take a square sheet of paper (large enough) to represent X as above, and consider the condition $(t,0) \sim (t,1)$ for all $t \in [0,1]$. This corresponds to considering the top edge and the bottom edge of the sheet to be "the same," so roll up the piece of paper so the bottoms and tops match. Next, consider the condition $(0,t) \sim (1,t)$, so that the left and right edges, now the ends of some open cylinder, are considered "the same," so connect the two ends. You have now constructed a torus.

Well-Definition

Often, defining functions on quotient sets are why we think of quotient sets in the first place; however, this involves defining expressions of the form $f([a])$, so a concern we need to often consider is whether the definition of $f([a])$ is overly sensitive on the choice of the representative a. That is, if $[a] = [b]$, does $f([a]) = f([b])$; i.e., is the function even well-defined? That is all the concept of well-definedness even is — check if the function is actually a function. We give one example.

Example 15.11. Consider the quotient set $\mathbb{Z}_n$, the ring of integers modulo n. Define the operations[11] $+$ and $\cdot$ on $\mathbb{Z}_n$ by setting $[m] + [n] := [m+n]$ and $[m] \cdot [n] := [mn]$. These operations are well-defined, and we show this for the addition operation we defined.

Proof that $+$ is Well-defined. Take $m, m', n, n' \in \mathbb{Z}$ such that $[m] = [m']$ and $[n] = [n']$. Then we see $[m]+[n] = [m+n]$ and $[m']+[n'] = [m'+n']$, so we must show that $[m+n] = [m'+n']$. Because the equivalence classes in $\mathbb{Z}_n$ determine a partition on the integers $\mathbb{Z}$, it suffices to show that $[m+n] \cap [m'+n'] \neq \varnothing$, and we do this by showing $m'+n' \in [m+n]$. To see this, note that $[m] = [m']$ and $[n] = [n']$ imply that $k \mid (m-m')$ and $k \mid (n-n')$, so that

$$(m+n) - (m'-n') = (m-m') + (n-n')$$

is a multiple of k, so we are done. □

Of course, the following are exercises to try.

Exercise 56. Let $f : A \to B$ be a function, and define the equivalence relation $\sim$ on A by $x \sim y$ if and only if $f(x) = f(y)$.

(a) Let $\pi : A \to A/\sim$ be given by $a \mapsto [a]$, where $[a]$ is the *equivalence class* of a, for all $a \in A$. Show that there is a unique function $g : (A/\sim) \to B$ such that $f = g \circ \pi$.

(b) Fixing the above notation, show that f is surjective if and only if g is bijective.

This exercise demonstrates the First Isomorphism Theorem on the level of sets. This is worth revisiting in Math 120A.

Exercise 57. Determine if the following functions are well-defined.

(a) $f_1 : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_{nm}$ by $([x],[y]) \mapsto [mx+ny]$.

[11] The operations in this case are actually functions $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$.

(b) $f_2 : \mathbb{Z}_{10} \to \mathbb{Z}_5$ by $[x] \mapsto [x]$.

(c) $f_3 : \mathbb{Z}_5 \to \mathbb{Z}_{10}$ by $[x] \mapsto [x]$.

(d) $f_4 : \mathbb{Z}_5 \times \mathbb{Z}_2 \to \mathbb{Z}_{10}$ by $([x], [y]) \mapsto [x^y]$.

(e) $f_5 : \mathbb{Z}/\sim \to \{\pm 1\}$ by $[x] \mapsto (-1)^x$, where $a \sim b$ if and only if $2 \mid (a + b)$.

Exercise 58. Let $\mathsf{GL}_n(\mathbb{R})$ be the set of all invertible $n \times n$ matrices with real number entries. Define a relation $\sim$ on $\mathsf{GL}_n(\mathbb{R})$ by $A \sim B$ if $A \sim P^{-1}BP$ for some $P \in \mathsf{GL}_n(\mathbb{R})$.

(a) Show that $\sim$ is an equivalence relation.

(b) Show that $f : (\mathsf{GL}_n(\mathbb{R})/\sim) \to \mathbb{R}$ defined by $f([A]) = \det A$ is well-defined.

If we let $\mathsf{SL}_n(\mathbb{R})$ denote the set of $n \times n$ real matrices with determinant 1, the above exercise shows in group-theoretic terms that $\mathsf{SL}_n(\mathbb{R}) \trianglelefteq \mathsf{GL}_n(\mathbb{R})$ and that the *quotient group* is *isomorphic* to $\mathbb{R} \setminus \{0\}$ under multiplication.

16 Cardinalities of Infinite Sets

This last section is perhaps the most neglected of the Math 13 curriculum, as most professors stop short of even Section 15 and focus on the material prior to that. However, the material here is definitely the most interesting among the topics in Math 13. Recall that two *finite* sets A and B have the same cardinality if and only if there exists a bijection $f : A \to B$. This was a *theorem* for finite sets, as cardinality was a finite number we can count; however, we must take this for definition for infinite sets — how can we compare two *infinite* sets to see which one has more elements?

Definition 16.1. Let A and B be arbitrary sets (finite or infinite). We define the *cardinality* of sets A and B to be the "size" of A and B, subject to the following comparison rules:

- We say $|A| \leq |B|$ if there exists a injection $f : A \to B$.
- We say $|A| = |B|$ if there exists a bijection $g : A \to B$.
- We say $|A| \geq |B|$ if there exists a surjection $h : A \to B$.

Of course, we note that by function composition, the relation $\sim$ on the collection of sets given by $A \sim B \iff |A| = |B|$ is an equivalence relation. Hence, we define $|A| := [A]$, the equivalence class of A under the relation $\sim$. Of course, for finite sets, we see that if $|A| = n$ under the usual sense, then

$$|A| = |\{1, 2, \ldots, n\}|$$

by the obvious bijection of labeling the elements of A. Hence, this definition matches what we have been doing for finite sets. These definitions seem fair enough, but we quickly run into unintuitive truths.

Example 16.2 (Galileo's Paradox)**.** The set of all *perfect squares* S is somewhat "sparse" in $\mathbb{Z}^+$, in that $S \subsetneq \mathbb{Z}^+$, and intuitively, "most" positive integers are not perfect squares. However, $f : \mathbb{Z}^+ \to S$ by $n \mapsto n^2$ is a bijection. Hence, we are forced to concede that $|\mathbb{Z}^+| = |S|$; i.e., the sets have the same size when considering cardinality, though if we consider "size" using subset inclusion, we have a disagreement. However, we will think of size using *cardinality* in this text, as this allows us to consider and compare any two arbitrary sets.

There is one infinite cardinality that will drive the rest of this section forward: the cardinality of the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Definition 16.3. A set A is *countable* if it is either finite or has the same cardinality as $\mathbb{N}$. In the case that $|A| = |\mathbb{N}|$, we say that A is *countably infinite*, and we denote $|\mathbb{N}| =: \aleph_0$ (read "aleph-null").

Equivalently stated, if A is countably infinite, there is a bijection $f : X \to \mathbb{N}$. Now, we continue with more intuition-defying facts.

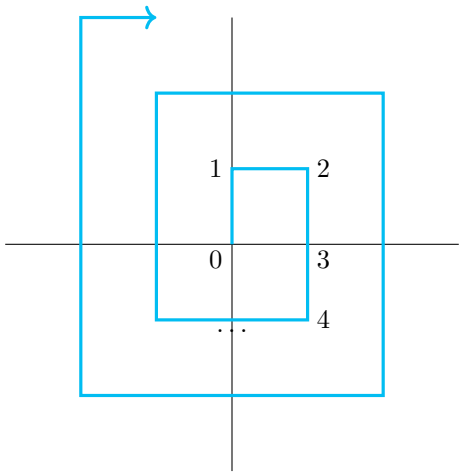
Proposition 16.4. *$\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are both countable sets.*

Proof. For $\mathbb{Z}$, we specify a bijection $f : \mathbb{N} \to \mathbb{Z}$ by listing out the elements in the following way:

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	$\cdots$
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	$\cdots$

By construction, this determines a bijection.

For $\mathbb{Z} \times \mathbb{Z}$, we have to be more tricky. Follow the following spiral path, leaving a unique natural number at each lattice point stop:



By construction, this determines a bijection. □

Exercise 59. Determine an explicit piecewise formula for the bijection $f : \mathbb{N} \to \mathbb{Z}$ in the proof above.

In general, we note that $\mathbb{Z}^n$ is countable by considering spirals in higher dimensions. However, the reader may already expect this to be true — there is enough space between lattice points in order to have $|\mathbb{Z}^n| = \aleph_0$. However, $\mathbb{Q}$ is dense, in that in between any two rational numbers, there exists a third rational number. Hence, it is reasonable to expect $\mathbb{Q}$ to have a larger cardinality, but we will show something certainly upsetting, at least to mathematicians in the early 20th century.

Theorem 16.5. *$\mathbb{Q}$ is countable.*

Proof of a Special Case. We just discuss the rational interval $I := [0,1] \cap \mathbb{Q}$. We enumerate this set by first considering the and denominator:

$$I = \left\{ \frac{0}{1}, \frac{1}{1}, \frac{0}{2}, \frac{1}{2}, \frac{2}{2}, \frac{0}{3}, \frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \frac{0}{4}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \dots \right\}.$$

We simply delete the duplicates off the list to get an enumeration of I:

$$I = \left\{ 0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \dots \right\}.$$

□

Using a careful enough "spiral," we can show that $\mathbb{Q}$ is countable. However, we will state the following principle, which shows that deleting the duplicates was not actually necessary.

Proposition 16.6. *Let X be a set. If there exists a surjection $f : \mathbb{N} \to X$, then X is countable.*

Exercise 60. In the case that X is infinite, provide a proof of the statement above by finding a bijection $g : \mathbb{N} \to X$ using the surjection $f : \mathbb{N} \to X$ given.

One may ask, are there sets too large to be countable? The answer is *yes* — there are in fact sets larger than $\mathbb{Q}$ that cannot be put into bijection with the natural numbers.

Definition 16.7. A set A is *uncountable* if it is not countable.

Of course, this set must be infinite in size. We are already familiar with one such uncountable set: the real numbers.

Theorem 16.8. *$\mathbb{R}$ is uncountable.*

Proof. Obviously $(0,1) \subseteq \mathbb{R}$. We first show that $(0,1)$ is uncountable. Assume for contradiction that $(0,1)$ is countable. Hence write

$$(0,1) = \{x_1, x_2, x_3, x_4, \dots\},$$

which is an enumeration of the set $(0,1)$. Write each x_i in its infinite decimal expansion[12] and arrange them as such. By assumption, this list consists of all elements of $(0,1)$:

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13}a_{14}a_{15}\dots \\ x_2 &= 0.a_{21}a_{22}a_{23}a_{24}a_{25}\dots \\ x_3 &= 0.a_{31}a_{32}a_{33}a_{34}a_{35}\dots \\ x_4 &= 0.a_{41}a_{42}a_{43}a_{44}a_{45}\dots \\ &\vdots \end{aligned}$$

For our contradiction, we produce an element x that does not lie on the list. Define the digit b_i to be given by $b_i = 4$ if $a_{ii} \neq 4$ and $b_i = 5$ if $a_{ii} = 4$, and set $x = 0.b_1b_2b_3b_4b_5\dots$. We see that x disagrees with each x_i at the ith decimal place; hence, it cannot be on the list. Yet $b_i \in (0,1)$, a contradiction. Hence, $(0,1)$ is be uncountable. Now, consider the chain of functions

$$(0,1) \xrightarrow{f} \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \xrightarrow{g} \mathbb{R}$$

where $f(x) := -\frac{\pi}{2} + \pi x$ and $g(x) := \tan x$. The reader can show that both f and g are bijections, so that $g \circ f$ is also a bijection. Hence $|(0,1)| = |\mathbb{R}|$, so $\mathbb{R}$ is uncountable. □

[12] That is, if $x_i = 1/4$, then write $x_i = 0.24\overline{9}$ instead of $x_i = 0.25$.

The argument we used to prove that $(0,1)$ was uncountable is known as a *diagonal argument*, due to how we only considered the digits a_{ii}, which appear on the diagonal of our hypothetical list we made above.

Exercise 61. Using a similar diagonal argument, prove that $\mathcal{P}(\mathbb{N})$ is uncountable. However, show that the set of all *finite* subsets of $\mathbb{N}$ is in fact *countable*.

Recall that our definition of cardinality requires that we find a bijection between two sets. However, in the uncountable case, this is often difficult, but we have the following theorem. We will not prove the theorem, and we recommend the reader read the various proofs online.

Theorem 16.9 (Cantor-Schröder-Bernstein Theorem)**.** *Let A, B be sets. If there exist injections $f : A \to B$ and $g : B \to A$, then there exists a bijection $h : A \to B$.*

In short, the theorem states that if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. This statement is surely true for numbers and for finite cardinalities, though it is not a triviality for infinite sets. We view some examples.

Example 16.10. We show that $(0,1)$ and $(0,1)^2$ have the same cardinality. For one, notice that $f : (0,1) \to (0,1)^2$ by $x \mapsto (x, 1/2)$ is an injection by construction. Now, we find an injection $g : (0,1)^2 \to (0,1)$. Notice that every element $x \in (0,1)$ has a unique decimal expansion, as long as we always choose the non-terminating expansion when necessary. Now, define $g : (0,1)^2 \to (0,1)$ such that if $x = 0.d_1d_2d_3\ldots$ and $y = 0.e_1e_2e_3\ldots$, we have

$$g(x,y) = 0.d_1e_1d_2e_2d_3e_3\ldots.$$

Again, g is injective by construction. Hence $|(0,1)| = \left|(0,1)^2\right|$.

Exercise 62. Prove that the set of all *infinite binary sequences* (i.e., sequences of 0's and 1's) is uncountable without a diagonalization argument.

Now, we turn to a third way of determining countability: by using a set's subsets. We have already done this to some extent when we showed that $\mathbb{R}$ contained an uncountable subset, but we did so by constructing an explicit bijection between that subset and $\mathbb{R}$. The next few theorems show us that we can skip this step, but we first introduce some notation.

Definition 16.11. Let I be a set, and to each $i \in I$ assign a set A_i. That is, the sets A_i are *indexed* by the set I. We define the *indexed union* by

$$\bigcup_{i\in I} A_i := \Big\{x : (\exists i \in I)\, x \in A_i\Big\}$$

and the *indexed intersection* by

$$\bigcap_{i\in I} A_i := \Big\{x : (\forall i \in I)\, x \in A_i\Big\}.$$

We note that in the case that $I = \mathbb{Z}^+$, we often write $\bigcup_{i=1}^{\infty} A_i$ (and similarly for intersections) in place of the notation presented here. However, when we are proving something about a union or intersection indexed by $\mathbb{Z}^+$, **you <u>may not</u> write**

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots$$

and attempt to manipulate the expression on the right-hand side, no matter how true it seems — that is **not** the definition of the indexed union, though it is a useful shorthand, even if the notation is technically abusive. We demonstrate this principle in the proof of the theorem below.

Theorem 16.12. *A union of countably many countable sets is countable. That is, if* $A_1, A_2, A_3, \ldots$ *is a sequence of countable sets, then* $\bigcup_{i=1}^{\infty} A_i$ *is countable.*

Proof. Let $A := \bigcup_{i=1}^{\infty} A_i$. We construct a surjection $f : \mathbb{N} \to A$, so by Proposition 16.6, we are done. We note that $A_i \subseteq A$ for every $i \in \mathbb{Z}^+$,[13] so it follows that we can just list the elements of A, grouped by the A_i:

$$A_1 = \{a_{11}, a_{12}, a_{13}, \ldots\}$$
$$A_2 = \{a_{21}, a_{22}, a_{23}, \ldots\}$$
$$A_3 = \{a_{31}, a_{32}, a_{33}, \ldots\}$$

Now, count the elements by going diagonally across from right to left: send $1 \mapsto a_{11}, 2 \mapsto a_{12}, 3 \mapsto a_{21}, 4 \mapsto a_{13}, 5 \mapsto a_{22}, 6 \mapsto a_{31}$, and so on and so forth. This gives a surjection $f : \mathbb{N} \to A$, so we are done. □

Example 16.13. Let S be the set of natural-number sequences with finitely many nonzero terms. We show that S is countable.

Proof. Define $S_n := \left\{(x_0, x_1, x_2, \ldots) \in S : \sum_{i=0}^{\infty} x_i = n\right\}$. Of course, because only finitely many terms in each sequence is nonzero, the sum converges, so our definition is valid. Then, we see that

$$S = \bigcup_{n \in \mathbb{N}} S_n,$$

as no sum of the sequences in S can possibly diverge. We claim that each of the S_n's are countable. To each $n \in \mathbb{N}$, fix some $m \in \mathbb{N}$ with $m \leq n$, and consider the set $S_n(m)$ given by

$$S_n(m) := \{x \in S_n : x \text{ has exactly } m \text{ nonzero terms}\}.$$

We leave it for the reader to verify that each $S_n(m)$ is indeed countable, and that

$$S_n = \bigcup_{m=1}^{n} S_n(m),$$[14]

hence S_n is countable. By the preceding theorem, we are done. □

Our next theorem allows us to quickly establish uncountability.

Theorem 16.14. *If A is uncountable and B is countable, then $A \setminus B$ is uncountable.*

Proof. Notice that $A = (A \setminus B) \cup (A \cap B)$. Clearly, $A \cap B$ is countable. Now, assume for contradiction that $A \setminus B$ is countable. Then the restriction Theorem 16.12 to finite unions would imply A is countable, a contradiction. Hence $A \setminus B$ is uncountable. □

[13] Prove this statement carefully.

[14] This is an honest finite union $S_n(1) \cup S_n(2) \cup \cdots \cup S_n(n)$.

Example 16.15. The irrational numbers $\mathbb{R} \setminus \mathbb{Q}$ are uncountable, as $\mathbb{Q}$ is countable while $\mathbb{R}$ is not.

In fact, we can say something slightly stronger than the previous theorem.

Theorem 16.16. *If A is infinite and B is countable, and $A \setminus B$ is infinite, then $|A \setminus B| = |A|$.*

Proof. Since A is infinite, A must contain a countably infinite subset.[15] Since B is countable, so is $A \cap B$, so we enumerate

$$A \cap B = \{b_0, b_1, b_2, b_3, \ldots\}.$$

Now, define $S := \{a_0, a_1, a_2, \ldots\} \subseteq A \setminus B$. We consider two cases.

Case I: If $A \cap B$ is finite, there is basically no work to be done.

Case II: If $A \cap B$ is infinite, define the function $f : A \to A \setminus B$ by

$$f(x) = \begin{cases} x & x \notin (A \cap B) \cup S \\ a_{2n+1} & x = b_n \text{ for some } n \in \mathbb{N} \\ a_{2n} & x = a_n \text{ for some } n \in \mathbb{N}. \end{cases}$$

We leave it for the reader to show that f is indeed injective. Now, the embedding $g : A \setminus B \to A$ by $g(x) = x$ is obviously injective, so by Cantor-Schröder-Bernstein, we are done. □

Similarly, the following holds as well.

Proposition 16.17. *If A is infinite and B is countable, then $|A \cup B| = |A|$.*

Exercise 63. Prove the above proposition, using a similar argument as to Theorem 16.16.

Infinite Infinities

Thus far, we have only seen two types of infinities: countable infinity $\aleph_0$ and the size of the real numbers $\mathbb{R}$, sometimes known as the *continuum* (denoted $\mathfrak{c}$). However, we can continue building larger and larger infinities, using the power set operation. Recall that the power set gives as a notion of exponentiation (with base 2), which gives us larger sets. This is even true for *infinite* sets, as we shall see in the theorem and proof below.

Theorem 16.18 (Cantor's Theorem)**.** *Let X be any set. then $|X| < |\mathcal{P}(X)|$.*

Proof. We have already proved the finite case, so suppose X is infinite. First, we know $|X| \leq |\mathcal{P}(X)|$, as we have the embedding $f : X \to \mathcal{P}(X)$ by $x \mapsto \{x\}$. Now, assume for contradiction that $|\mathcal{P}(X)| = |X|$; i.e., there is a bijection between elements of X and subsets of X. If g is such a bijection, we denote $g(x) = A_x$. Define

$$R := \{x \in X : x \notin A_x\} \subseteq X,$$

that is, R contains all elements of X that are not contained in their image A_x. Since $R \subseteq X$, we have $R = A_y$ for some $y \in X$. Now, the question is, does R contain y?

If $y \in R$, then $y \notin A_y$ by definition of R. But $A_y = R$, a contradiction. Similarly, if $y \notin R$, then $y \notin A_y$, but by definition of R, $y \in R$, a contradiction. Hence, the existence of the bijection causes a contradiction, so we must have $|X| < |\mathcal{P}(X)|$. □

[15] That is, $\aleph_0$ is the "smallest" infinity. See the exercises at the end of this section.

This allows us to build a chain of increasing infinities.

Corollary 16.19. *There exists an infinite sequence of infinite sets $A_1, A_2, A_3, \ldots$ such that*

$$|A_1| < |A_2| < |A_3| < \cdots .$$

Proof. Take $A_1 = \mathbb{N}$, $A_2 = \mathcal{P}(\mathbb{N})$, and inductively take $A_n = \mathcal{P}(A_{n-1})$ for $n \geq 2$. By Cantor's Theorem, we have $|A_n| < |A_{n+1}|$ for all $n \geq 1$, so we are done. □

Conclusion: Transcendental Numbers

We finish these notes with a discussion of polynomials and their relation to cardinality. Let us start with the following definitions.

Definition 16.20. A complex number α is *algebraic* if it is a root of a polynomial with integer coefficients.

For the sake of notation, we denote the set of all polynomials with integer coefficients by $\mathbb{Z}[x]$. Hence, α is algebraic if there exists some $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Definition 16.21. Let $\alpha \in \mathbb{C}$ be algebraic. The *degree* of α is the minimal degree of a polynomial $f \in \mathbb{Z}[x]$ such that α is a root of f.

Example 16.22. Suppose α has (algebraic) degree 1. Hence α is the root of some $ax + b \in \mathbb{Z}[x]$, $a \neq 0$, i.e., $\alpha = -b/a \in \mathbb{Q}$. In fact, this shows that $\alpha \in \mathbb{Q}$ is equivalent to α being algebraic of degree 1. Similarly, if β is algebraic of degree 2, then it is the root of some $ax^2 + bx + c \in \mathbb{Z}[x]$, $a \neq 0$, so that by the quadratic formula

$$\beta = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

taking either plus or minus as necessary.

Definition 16.23. We say $\alpha \in \mathbb{C}$ is *transcendental* if it is not algebraic.

In abstract algebra, "not algebraic" is sometimes formulated as "if $f(x) \in \mathbb{Z}[x]$ satisfies $f(\alpha) = 0$, then $f = 0$." [The reader may show that this is equivalent.] Transcendental numbers are notoriously hard to find, and it is always a hefty task to show that a number is not algebraic, as there are infinitely many polynomials $\mathbb{Z}[x]$ of arbitrarily high degree. To give a little bit of history:

- Johann Heinrich Lambert *conjectured* in 1761 that π was transcendental.
- Joseph Liouville showed that transcendental numbers actually existed in 1844, and he found the example $L := \displaystyle\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$.
- Charles Hermite showed that e, the base of the natural logarithm, was transcendental in 1873.
- Ferdinand von Lindemann, over a century after it was conjectured, finally proved that π was transcendental in 1882. He first showed that e^α was transcendental when α was algebraic.[16] Since $e^{\pi i} = -1$, it follows that πi is transcendental, hence π is transcendental.

[16] This statement is today known as the Lindemann-Weierstrass Theorem, with Karl Weierstrass proving a more general case.

Additionally, to this day (2024) we only know that at least one of $e+\pi$ and $e\pi$ is transcendental, yet we find ourselves unable to conclusively say which one(s) is/are transcendental. For certain other types of numbers, we have even worse luck than this.

Definition 16.24. Let $s \in \mathbb{C}$. We define the *Riemann zeta function* to be the sum

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots,$$

where the domain of ζ is any place in the complex plane where the infinite sum converges.

Euler proved in 1735 that $\zeta(2) = \pi^2/6$ in the famous Basel problem, yet it was by Lindemann's result that $\zeta(2)$ was shown to be transcendental. In 1978, Roger Apéry showed that $\zeta(3)$, now known as *Apéry's constant* in his honor, is *irrational* — it is still open whether it is algebraic or transcendental. Similarly, we are unsure whether the very important numbers

$$G := \sum_{i=0}^{n} \frac{(-1)^n}{(2n+1)^2} = \frac{1}{1^2} - \frac{1}{3^2} + \frac{1}{5^2} - \frac{1}{7^2} + \cdots \text{ (Catalan's Constant) and}$$

$$\gamma := \lim_{n\to\infty} \left(-\ln n + \sum_{k=1}^{n} \frac{1}{k} \right) \text{ (Euler-Mascheroni Constant)}$$

are even irrational, let alone transcendental. Hence, we may jump to the conclusion that transcendental numbers are very rare among the complex numbers, and that most numbers are at the very least algebraic. However, our final theorem in these notes show that this is in fact not the case — most complex numbers *are* transcendental! This is somewhat of a scary thought: most of the numbers we even think about form a tiny subset of $\mathbb{R}$, let alone $\mathbb{C}$ — the "average" number is virtually indescribable with our vocabulary.

Theorem 16.25. *There are uncountably many transcendental numbers, while there are only countably many algebraic numbers.*

Proof. Let $\mathbb{A}$ denote the set of algebraic numbers, and let $\mathbb{A}_d$ denote the set of algebraic numbers with degree d. Then

$$\mathbb{A} = \bigcup_{d=1}^{\infty} \mathbb{A}_d.$$

It thus suffices to show that each $\mathbb{A}_d$ is countable. Fixing $d \in \mathbb{Z}^+$, every polynomial in $\mathbb{Z}[x]$ with degree d has at most d unique roots, so it is enough to show that there are only countably infinitely many polynomials with degree d. Now, each polynomial $c_d x^d + c_{d-1}x^{d-1} + c_1 x + c_0 \in \mathbb{Z}[x]$ is uniquely determined by the sequence of coefficients $(c_d, c_{d-1}, \ldots, c_1, c_0) \in \mathbb{Z}^{d+1}$; i.e., we have found a bijection between the set of all polynomials in $\mathbb{Z}[x]$ with degree *at most* d and $\mathbb{Z}^{d+1}$. We know that $\mathbb{Z}^{d+1}$ is countably infinite, so that the set of all polynomials with degree at most d is countably infinite, and thus the number of polynomials wth degree exactly d is countable, hence $\mathbb{A}_d$ is countable. This implies $\mathbb{A}$ is countable, so that $\mathbb{C} \setminus \mathbb{A}$, the set of transcendental numbers, is uncountable as $\mathbb{C}$ is uncountable. □

We end with David Hilbert's quote on Cantor's results which we explored in this section: "From the paradise, that Cantor created for us, no one shall be able to expel us."

Exercises

Exercise 64. Show that a set is infinite if and only if there exists a subset of size n for every $n \geq 1$.

Exercise 65. Let A be a set. Show that the following statements are equivalent:

1. A is infinite.
2. A has a countably infinite subset.
3. A has a *proper* subset B satisfying $|B| = |A|$.

This exercise shows that *all* infinite sets have the unintuitive property that they contain a strictly "smaller" set with the same size, and this property is *necessary and sufficient* for a set to be infinite. [We have used this many times in the proofs of the theorems in the main text.]

Exercise 66. We define $\mathbb{Q}(\sqrt{2}, \sqrt{3}) := \left\{\sqrt{2}r + \sqrt{3}s : r, s \in \mathbb{Q}\right\}$. Show that there exist infinitely many $c \in \mathbb{R}$ such that $3^x \ln y + 5^y \cos x = c$ has no solution $x, y \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Exercise 67. Let $f : (0, 1] \to (0, 1)$ be given by

$$f(x) := \begin{cases} 1/(n+1) & t = 1/n \text{ for some } n \in \mathbb{N} \\ t & \text{otherwise.} \end{cases}$$

Show that f is a bijection. [This gives an explicit bijection between $(0, 1]$ and $(0, 1)$.]

Exercise 68. Construct an explicit bijection $f : (0, 1) \to [0, 1]$.

Exercise 69. Are each of these following sets finite, countably infinite, or uncountably infinite?

(a) $\mathbb{Q}(x) = \{p(x)/q(x) : p, q \in \mathbb{Q}[x]\}$, where $\mathbb{Q}[x]$ is the set of polynomials with rational coefficients.

(b) $\mathbb{R}[x]$, the set of polynomials with real coefficients.

(c) The set of finite subsets of $\mathbb{R}$.

(d) The set of continuous functions on $\mathbb{R}$.

Exercise 70. Let $S \subseteq \mathbb{R}^2$ be the set of all points (x, y) such that $x^2 + y^2 = a^2$ and $y = bx$ for some $a, b \in \mathbb{Q}$. Is S countable?

Exercise 71. Are the following sets finite, countably infinite, or uncountably infinite?

(a) The set of all lines in $\mathbb{R}^2$ having rational slope and rational y-intercept.

(b) The set of circles in $\mathbb{R}^2$ having rational radii and centers with rational coordinates.

Exercise 72. Let $f : \mathbb{R} \to \mathbb{Q}$. Show that there exists an uncountable subset $S \subseteq \mathbb{R}$ such that $f(x) = f(y)$ for every $x, y \in S$.

Exercise 73. This exercise provides an alternate proof that the algebraic numbers are countable. Again, use $\mathbb{A}$ to denote the algebraic numbers.

(a) Let $M \in \mathbb{Z}^+$. Show that there are finitely many choices of $d \in \mathbb{Z}^+$ and $a_0, \ldots, a_d \in \mathbb{Z}$ with $M = d + \sum_{k=0}^{d} |a_k|$.

(b) Let $P_M := \{a_d x^d + \cdots + a_1 x + a_0 : M = d + |a_0| + |a_1| + \cdots + |a_d|\}$. Why is P_M *finite*?

(c) We know that every polynomial of degree d has at most d distinct roots in $\mathbb{C}$. Show that $R_M := \{x \in \mathbb{R} : p(x) = 0 \text{ for some } p \in P_M\}$ is finite.

(d) Prove that $\mathbb{A} = \bigcup_{M=1}^{\infty} R_M$, which completes the proof.

Exercise 74. In this exercise we show that if $|A| < \aleph_0$, then A is finite. Suppose for contradiction that A is an infinite set satisfying $|A| < \aleph_0$, so there exists an injection $f : A \to \mathbb{Z}^+$. Enumerate the elements in the range of f in increasing order: $\operatorname{im} f = \{n_1, n_2, n_3, \ldots\}$, where $n_i < n_j$ if $i < j$.

(a) Prove that $\operatorname{im} f$ is infinite.

(b) Show that for all $k \in \mathbb{Z}^+$, there exists a unique $a_k \in A$ with $f(a_k) = n_k$.

(c) Define $g : \mathbb{Z}^+ \to A$ by $g(k) = a_k$. Prove that g is a bijection, and hence deduce a contradiction.

Exercise 75. Let X be a nonempty set and $\mathcal{A} \subseteq \mathcal{P}(X)$. We say that $\mathcal{A}$ is a *σ-algebra* if it satisfies the following 3 conditions:

1. $\varnothing, X \in \mathcal{A}$.
2. If $S \in \mathcal{A}$, then $S^c \in \mathcal{A}$. (We treat X as the universal set.)
3. If $S_1, S_2, \ldots \in \mathcal{A}$, then their union is in $\mathcal{A}$.

This exercise shows that countably infinite σ-algebras cannot exist. We proceed by contradiction: suppose $\mathcal{A} = \{S_1, S_2, S_3, \ldots\}$ is countably infinite, and assume the sets S_i are all distinct.

(a) Show that the universal set X is infinite.

(b) For each $x \in X$, define $B_x := \bigcap_{\{n \in \mathbb{N} : x \in S_n\}} S_n$. Show that $B_x \in \mathcal{A}$ for any $x \in X$.

(c) Show that if $E \in \mathcal{A}$ and $x \in E$, then $B_x \subseteq E$. That is, show that B_x is the smallest set in $\mathcal{A}$ containing x.

(d) Let $x, y \in X$. Suppose $B_x \cap B_y \neq \varnothing$ and let $z \in B_x \cap B_y$. Show $x, y \in B_z$, so that $B_x = B_y = B_z$. That is, show that two sets B_x, B_y are either disjoint or equal.

(e) Show that there exists a sequence $x_1, x_2, x_3, \ldots$ in X such that $x_i \neq x_j$ if $i \neq j$.

(f) Deduce a contradiction by constructing an injection from the set of binary sequences into $\mathcal{A}$.

Exercise 76. Give an example of an uncountable set I and $\{A_t : t \in I\}$ such that each each A_t is countably infinite and the following 3 conditions hold: (1) if $s \neq t$, then $A_s \neq A_t$, (2) for all s, t, either $A_s \subseteq A_t$ or $A_s \supseteq A_t$, and (3) $\bigcup_{t \in I} A_t$ is countably infinite.

References

Though these notes are largely independent of the official Math 13 notes, some of the material here can be found there as well: `https://www.math.uci.edu/~ndonalds/math13/notes.pdf`.