MATH 16110 (Honors Calculus I IBL) Notes

Steven Labalme

October 16, 2020

Contents

List of Figures

Notes on Proofs

Responses

9/27: **Lemma 4.** *Let x, y be positive integers. Then xy is odd if and only if x and y are both odd.*

Proof. We wish to prove that if x and y are not both odd, then xy is not odd. In other words, we wish to prove that if at least one of x or y is even, then xy is even. Let's begin. WLOG, let x be even. Then $x = 2k$ for some $k \in \mathbb{N}$. Thus, $xy = 2(ky)$, proving that xy is even since $ky \in \mathbb{N}$. The proof is symmetric for y. $\square$

Corollary 5. *Let x, y be positive integers. Then xy is even if and only if at least one of x and y is even.*

Proof. We wish to prove that xy is even if and only if at least one of x and y is even. Consequently, we must prove the dual implications "if xy is even, then at least one of x and y is even" and "if at least one of x and y is even, then xy is even." Let's begin. For the first statement, let xy be even and suppose for the sake of contradiction that and both x and y are not even, i.e., are odd. But by Lemma 4, it follows from the assumption that x and y are both odd that xy is odd, which contradicts the fact that xy is even. Therefore, at least one of x or y must be even. As to the second statement, suppose that at least one of x or y is even. In this case, x and y are not both odd. Thus, by Lemma 4, xy is not odd, or, equivalently, xy is even. $\square$

Exercise 8.

a) Are there positive integers m, n such that m and n have no common factors (other than 1) and $m^2 = 3n^2$? Either give an example or prove that no example is possible.

Proof. Let m, n be relatively prime positive integers and suppose for the sake of contradiction that $m^2 = 3n^2$. We divide into two cases (the case where n is even, and the case where n is odd); we seek contradictions in both cases. First off, if n is even, then $n = 2k$ for some $k \in \mathbb{N}$. Thus, $3n^2 = 3(2k)^2 = 12k^2 = 2(6k^2) = m^2$, proving that m^2 is even since $6k^2 \in \mathbb{N}$. By Corollary 5, this implies that m is even. Therefore, since m and n are both even, they have a common factor, a contradiction. On the other hand, if n is odd, then $n = 2k+1$ for some $k \in \mathbb{N}$. Thus, $3n^2 = 3(2k+1)^2 = 12k^2+12k+3 = 2(6k^2+6k+1)+1 = m^2$, proving that m^2 is odd since $6k^2+6k+1 \in \mathbb{N}$. Thus, by Lemma 4, m is odd. Consequently, $m = 2l+1$ for some $l \in \mathbb{N}$, so $m^2 = (2l+1)^2 = 4l^2+4l+1 = 12k^2+12k+3$, the last equality holding because we also have $m^2 = 3n^2 = 12k^2 + 12k + 3$. This implies the following.

$$\begin{aligned}
4l^2 + 4l + 1 &= 12k^2 + 12k + 3 \\
4l^2 + 4l &= 12k^2 + 12k + 2 \\
2l^2 + 2l &= 6k^2 + 6k + 1 \\
2(l^2 + l) &= 2(3k^2 + 3k) + 1
\end{aligned}$$

Since $l^2 + l$ and $3k^2 + 3k$ are both natural numbers, the above asserts that an odd number equals an even number, a contradiction. Hence, in both cases, we must have that $m^2 \neq 3n^2$. $\square$

b) Are there positive integers m, n such that m and n have no common factors (other than 1) and $m^2 = 6n^2$? Either give an example or prove that no example is possible.

Proof. Let $m, n \in \mathbb{N}$ have no common factors (other than 1), and suppose for the sake of contradiction that $m^2 = 6n^2$. Since $m^2 = 6n^2 = 2(3n^2)$, m^2 is even. It follows by Corollary 5 that m is even, implying that $m = 2k$ for some $k \in \mathbb{N}$. Thus, $6n^2 = m^2 = (2k)^2 = 4k^2$, so $3n^2 = 2k^2$. Since $k^2 \in \mathbb{N}$, $3n^2$ is even. Consequently, we have that n^2 is even by Corollary 5 (since at least one of 3 or n^2 is even and $3 = 2(1) + 1$ is odd). By Corollary 5 again, n is even. Thus, m and n are both even, contradicting the assumption that they have no common factors other than 1. □

c) Are there positive integers m, n such that m and n have no common factors (other than 1) and $m^2 = 4n^2$? Either give an example or prove that no example is possible.

Proof. Let $m = 2$ and $n = 1$. Then $m^2 = 2^2 = 4 = 4 \cdot 1^2 = 4n^2$. □

Discussion

9/29:

- Dr. Cartee.
- Sam Craig (super reader) is an advanced undergraduate who has taken this class before.
- Honors Calculus uses Spivak — we do not have a textbook, just scripts.
  - Few lectures in the traditional sense.
  - Majority of material is presented and developed by the students.
  - Several scripts will be covered throughout the quarter.
    - In scripts: It is our job to complete the exercises, prove the theorems/lemmas/propositions, etc.
  - Be on the look-out for "no proof required" theorems.
  - 3 chances to learn/review scripts material:
    1. Before class, you prepare your own proof.
    2. During class, we discuss.
    3. After class and before the journal is due, we type up our own record of the proof in LaTeX.
- Before each class, he will tell us which theorems/exercises we need to work through.
- Your proofs do not have to be perfect in the beginning! Sam and Dr. Cartee will help us. Expect to present every other week.
  - For the first two scripts, you have the ability to rewrite your journal after Sam reviews it to recover up to half of the lost credit.
  - You only recover credit if your new solution is perfect.
  - Return your changes one week after Sam grades it.
    - Mark what parts/problems you have rewritten, and turn in the original as well.
- Later this afternoon, Dr. Cartee will share which Script 0 problems we should do before Thursday. Sign up for problems on a Google Doc when each script is released. You also get a "buddy," who discusses your proof with you before you present.
- Class participation: When and how often and the quality of our presentations, and also how good are our questions that help presenters fill in the gaps.
- We can use Overleaf for collaborative LaTeX projects.
- We can check in with Dr. Cartee on our progress whenever throughout the quarter.
- Sam's office hours: We get to talk to him one-on-one with questions.

  - 7:00-8:00 PM on Thursdays

- You have one chance to ask for a 24-hour extension on HW (like if you're sick).
- In the case of a switch to virtual class:
  - We can present by turning our phone into a document camera or using a white board behind us or typing up in LaTeX (in real time?).
- Get good at writing — you cannot type up your solutions during exams!
- We submit HW assignments through Canvas if we type it up in LaTeX, or in class by hand. It's nice if we can type it up.

Script 0

The Natural Numbers and Mathematical Induction

0.1 Responses

10/1: **Exercise 0.2** (PMI Exercise 2)**.** Prove that if $x > -1$, then $(1+x)^n \geq 1 + nx$ for any natural number n. (Note that although this script is focused on the natural numbers, your argument should hold for any real number $x > -1$.)

Proof. We induct on n. For the base case $k = 1$, we have $(1+x)^1 = 1 + x \geq 1 + (1)x$, where the greater than or equal to relation could be strengthened to equality but will be left as such for the sake of the argument. Now suppose inductively that we have proven the claim for some natural number k, i.e., we know that $(1+x)^k \geq 1 + kx$ if $x > -1$. We now seek to prove it for $k+1$. To begin, we have

$$(1+x)^{k+1} = (1+x)^k(1+x)$$

by the laws of exponents. By the inductive hypothesis and the fact that $ac \geq bc$ if and only if a, b, c are positive numbers and $a \geq b$ (note that $x > -1$ implies $1 + x > 0$ along with $(1+x)^k > 0$), we have that the above is

$$\geq (1+kx)(1+x)$$

Now expand and simplify.

$$\begin{aligned} &= 1 + kx + x + kx^2 \\ &= 1 + (k+1)x + kx^2 \end{aligned}$$

Since x^2 must be positive or zero and $k \in \mathbb{N}$ is clearly positive, we have that $kx^2 \geq 0$ so that the above is

$$\geq 1 + (k+1)x$$

thus closing the induction. □

Additional Exercises

10/8: 7. Let n be a natural number and $k \leq n$ also be a natural number. Define

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

where $k! = 1 \times 2 \times \cdots \times k$. Show that

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

for all $n \in \mathbb{N}$.

Proof. We begin with a lemma proving some basic properties of combinations.

Lemma. *Let n be a natural number and $k \leq n$ also be a natural number. Define*

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

where $k! = 1 \times 2 \times \cdots \times k$. Then

a) $\binom{n}{0} = 1$ *for all* $n \in \mathbb{N}$*;*

b) $\binom{n}{n} = 1$ *for all* $n \in \mathbb{N}$*;*

c) $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ *for all natural numbers n and $1 \leq k \leq n$.*

Proof of Lemma 1. We will address each of the three parts of the lemma in turn.

For part (a), we know by the definition of $\binom{n}{k}$ that $\binom{n}{0} = \frac{n!}{0!(n-0)!}$ and by the definition of a factorial that $\frac{n!}{0!(n-0)!} = \frac{1 \cdot n!}{n!} = 1$. Thus, $\binom{n}{0} = 1$, as desired.

For part (b), we proceed in a similar manner to the above: $\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n! \cdot 1} = 1$.

For part (c), we repeatedly apply the definition of $\binom{n}{k}$ and of a factorial in the following algebra. Note that we proceed from the right side of the equality we seek to prove since it makes the algebra flow more logically (via simplification rather than expansion).

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

□

Now we begin to address the question in earnest by inducting on n. For the base case $n = 1$, begin with the left side of the equality we wish to verify and employ the definition of exponents.

$$(x+y)^1 = x + y$$

Now use a couple of "clever forms of 1," which we can, of course, multiply to the terms in the above equation and still preserve equality.

$$= \frac{1!}{0!(1-0)!}x^1y^0 + \frac{1!}{1!(1-1)!}x^0y^1$$

Now just employ the definition of $\binom{n}{k}$ and use summation notation to simplify the expression.

$$\begin{aligned}
&= \binom{1}{0}x^{1-0}y^0 + \binom{1}{1}x^{1-1}y^1 \\
&= \sum_{k=0}^{1}\binom{1}{k}x^{1-k}y^k
\end{aligned}$$

This proves the base case. Now suppose inductively that we have proven the claim for some natural number n, i.e., we know given the definitions in the question that $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$. We wish to prove the claim for $n+1$, which can be done as follows. Once again, begin with the left side of the equality we wish to prove and employ a rule of exponents.

$$(x+y)^{n+1} = (x+y)^1(x+y)^n$$

Now substitute using the induction hypothesis.

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

Distribute the summation to each term in $x+y$, and then "distribute" x and y into the general term of the summation.

$$\begin{aligned}
&= x\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k + y\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{(n+1)-k}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1}
\end{aligned}$$

Reindex the second summation (instead of iterating from 0 to n, iterate from 1 to $n+1$ [the same number of terms] and subtract 1 from each instance of the index variable k). Note that this does not change the sum at all; it just changes how the sum is written. After the reindexing, algebraically manipulate the exponents into an equivalent form that matches the exponents in the other summation.

$$\begin{aligned}
&= \sum_{k=0}^{n}\binom{n}{k}x^{(n+1)-k}y^k + \sum_{k=1}^{n+1}\binom{n}{k-1}x^{n-(k-1)}y^{(k-1)+1} \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{(n+1)-k}y^k + \sum_{k=1}^{n+1}\binom{n}{k-1}x^{(n+1)-k}y^k
\end{aligned}$$

Separate the first term of the left summation and the last term of the right summation from the summation notation.

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

Now that the sums are once again indexed alike, combine them and do some algebraic manipulations to set up a substitution.

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

In the first term, use Lemma 1a to make the substitution $\binom{n}{0} = 1 = \binom{n+1}{0}$. In the last term, use Lemma 1b to make the substitution $\binom{n}{n} = 1 = \binom{n+1}{n+1}$. In the summation, use Lemma 1c to make the substitution $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ (notice how k varies between 1 and n in the summation, just like it is allowed to in the statement of Lemma 1c).

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

Expand the limits of the summation to encompass the first and last terms.

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

This closes the induction. □

9. From Peano's Postulates (below), prove the following claims.

Axioms (Peano's Postulates)**.** *The natural numbers are defined as a set* $\mathbb{N}$ *together with a unary "successor" function* $S : \mathbb{N} \to \mathbb{N}$ *and a special element* $1 \in \mathbb{N}$ *satisfying the following postulates.*

I. $1 \in \mathbb{N}$.

II. *If* $n \in \mathbb{N}$, *then* $S(n) \in \mathbb{N}$.

III. *There is no* $n \in \mathbb{N}$ *such that* $S(n) = 1$.

IV. *If* $n, m \in \mathbb{N}$ *and* $S(n) = S(m)$, *then* $n = m$.

V. *If* $A \subset \mathbb{N}$ *is a subset satisfying the two properties:*

- $1 \in A$;
- *if* $n \in A$, *then* $S(n) \in A$;

then $A = \mathbb{N}$.

(a) **Bonus exercise**. Show that

$$\mathbb{N} = \{1, S(1), S(S(1)), S(S(S(1))), \cdots\}$$

Proof. We wish to eventually use Axiom V to show that the set on the right side of the above equality (which we shall call A) is equal to $\mathbb{N}$. Thus, we begin by demonstrating that A is a subset of $\mathbb{N}$. To do so, we must verify that every element of A is an element of $\mathbb{N}$. Now A consists of 1 and elements in the codomain of S, so since $1 \in \mathbb{N}$ (Axiom I) and any element of the codomain of S is clearly an element of $\mathbb{N}$ (because the codomain of S *is* $\mathbb{N}$), $A \subset \mathbb{N}$. Moving on, as previously referenced, $1 \in A$, so the first property of Axiom V holds. Additionally, the pattern defining A clearly indicates that for any $a \in A$, $S(a) \in A$, so the second property of Axiom V holds. Therefore, by Axiom V, $A = \mathbb{N}$. □

(b) Prove that the Principle of Mathematical Induction follows from Peano's Postulates.

Proof. We wish to prove, using only Axioms I-V above and set theoretic results, that if $P(n)$ is a proposition pertaining to each natural number n, $P(1)$ is true, and the truth of $P(k)$ implies that $P(S(n))$[1] is also true, then $P(n)$ is true for all natural numbers n. We will do this by defining a set A such that "$P(n)$ is true" is logically equivalent to $n \in A$. Then if we can show that $n \in A$ for all $n \in \mathbb{N}$ (i.e., that $A = \mathbb{N}$), we will have verified that $P(n)$ is true for all $n \in \mathbb{N}$ as desired. Lastly, note that we will show that $A = \mathbb{N}$ by demonstrating that A satisfies the stipulations of Axiom V. Let's begin.

[1] Addition has not yet been defined. Although we do not yet "know" that $n + 1 = S(n)$ we must assume it for the sake of this proof.

Let $A = \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$. Since every element of A is an element of $\mathbb{N}$ by the definition of A, $A \subset \mathbb{N}$. Additionally, since $P(1)$ is true by hypothesis and $1 \in \mathbb{N}$ by Axiom I, we know by the definition of A that $1 \in A$. Now suppose $n \in A$. It follows that $n \in \mathbb{N}$ and $P(n)$ is true. But by hypothesis, the truth of $P(n)$ implies that $P(S(n))$ is true. This, combined with the fact that $S(n) \in \mathbb{N}$ by Axiom II, shows that $S(n) \in A$. Having now proven that $A \subset \mathbb{N}$, $1 \in A$, and $n \in A$ implies $S(n) \in A$, Axiom V tells us that $A = \mathbb{N}$, as desired. □

(c) Define a special element $0 \notin \mathbb{N}$ and define $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Let $s : \mathbb{N}_0 \to \mathbb{N}$ be defined by

$$\begin{aligned} s(0) &= 1 \\ s(n) &= S(n), \text{ for } n \in \mathbb{N} \end{aligned}$$

where S is the successor function defined in Peano's Postulates.

Definition. We define addition $x + y$ for $x, y \in \mathbb{N}_0$ inductively on y by

$$\begin{aligned} x + 0 &= x \\ x + s(y) &= s(x + y) \end{aligned}$$

Theorem. *The following facts all hold.*

i. *If $x, y \in \mathbb{N}_0$, then $x + y \in \mathbb{N}_0$.*
ii. *$0 + x = x$, for all $x \in \mathbb{N}_0$.*
iii. *(Commutative Law) $x + y = y + x$ for all $x, y \in \mathbb{N}_0$.*
iv. *(Associative Law) $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{N}_0$.*
v. *Given $x, y, z \in \mathbb{N}_0$, if $x + y = x + z$, then $y = z$.*

Prove that $x+1 = s(x)$ for all $x \in \mathbb{N}_0$ and then prove items (i), (ii), and (iv) in the above theorem.

Proof of first claim. Since $1 = s(0)$ by definition, we know by repeated applications of the various parts of the definition of addition that $x + 1 = x + s(0) = s(x + 0) = s(x)$, as desired. □

Proof of i. We keep x fixed and induct on y. For the base case $y = 0$, we have by the definition of addition that $x + 0 = x$. Since $x \in \mathbb{N}_0$ by assumption, it clearly follows that $x + 0 \in \mathbb{N}_0$, thus proving the base case. Now suppose inductively that we have proven that $x + y \in \mathbb{N}_0$ for some $y \in \mathbb{N}_0$; we now seek to prove that $x + (y + 1) \in \mathbb{N}_0$. By the above argument, $y + 1 = s(y)$, so

$$x + (y + 1) = x + s(y)$$

It follows by the definition of addition that the above

$$= s(x + y)$$

Since $s : \mathbb{N}_0 \to \mathbb{N}$ and $x+y \in \mathbb{N}_0$ by hypothesis, $s(x+y) \in \mathbb{N}$. Thus, $x+(y+1) \in \mathbb{N}$. Consequently, $x + (y + 1) \in \mathbb{N} \cup \{0\}$, implying by the definition of $\mathbb{N}_0$ that $x + (y + 1) \in \mathbb{N}_0$. This closes the induction. □

Proof of ii. We induct on x. For the base case $x = 0$, we have by the definition of addition that $0+0 = 0$, thus proving the base case. Now suppose inductively that we have proven that $0+x = x$ for some $x \in \mathbb{N}_0$; we now seek to prove that $0 + (x + 1) = x + 1$. As before, we can write that

$$\begin{aligned} 0 + (x + 1) &= 0 + s(x) \\ &= s(0 + x) \end{aligned}$$

But by the inductive hypothesis and the first claim proven herein, it follows that the above

$$\begin{aligned} &= s(x) \\ &= x + 1 \end{aligned}$$

This closes the induction. □

Proof of iv. We induct on x (keeping y, z fixed). For the base case $x = 0$, we must consider $0 + (y + z)$. By part (i), $y + z \in \mathbb{N}_0$. Thus, part (ii) applies, and implies that

$$0 + (y + z) = y + z$$

Since $y \in \mathbb{N}_0$ by assumption, we can apply part (ii) again in reverse to demonstrate that $y = 0 + y$. Thus, the above is

$$= (0 + y) + z$$

This proves the base case. Now suppose inductively that we have proven that $x + (y + z) = (x + y) + z$ for some $x \in \mathbb{N}_0$; we now seek to prove that $(x + 1) + (y + z) = ((x + 1) + y) + z$. As before,

$$(x + 1) + (y + z) = s(x) + (y + z)$$

By part (iii) (which implies that $s(y) + x = s(y + x)$ is also true), the fact that $y + z \in \mathbb{N}_0$ by part (i), and the definition of addition, we thus have that the above

$$= s(x + (y + z))$$

We now apply the inductive hypothesis.

$$= s((x + y) + z)$$

By the fact that $x + y \in \mathbb{N}_0$ (part i) and consecutive applications of the definition of addition, we find that the above

$$\begin{aligned} &= s(x + y) + z \\ &= (s(x) + y) + z \end{aligned}$$

To finish it off, we once again use the first claim proved herein:

$$= ((x + 1) + y) + z$$

This closes the induction. □

(d) **Definition.** We define multiplication $x \cdot y$ for $x, y \in \mathbb{N}_0$ inductively on $\mathbb{N}_0$ by

$$\begin{aligned} x \cdot 0 &= 0 \\ x \cdot s(y) &= x \cdot y + x \end{aligned}$$

Prove that $x \cdot 1 = x$ for all $x \in \mathbb{N}_0$.

Proof. Since $s(0) = 1$,

$$x \cdot 1 = x \cdot s(0)$$

By the definition of multiplication, the above is

$$= x \cdot 0 + x$$

From the above, we can use the definition of multiplication to substitute $x \cdot 0 = 0$.

$$= 0 + x$$

Now just apply part (ii) of the Theorem in part (c).

$$= x$$

□

(e) **Definition.** We define $<$ on $\mathbb{N}_0$ by

$$x < y \text{ if and only if } y = x + u \text{ for some } u \in \mathbb{N}.$$

i. Prove that $1 < n$ for all $n \in (\mathbb{N} \setminus \{1\})$.
ii. Prove that if $a, x, y \in \mathbb{N}$ with $x < y$, then $a \cdot x < a \cdot y$.

Proof of i. We induct on n. For the base case $n = 2$, we have $2 = s(1+0) = 1 + s(0) = 1 + 1$, so $1 < 2$. Now suppose inductively that $1 < n$ for some $n \in \mathbb{N}$; we wish to prove that $1 < n+1$. By the induction hypothesis and the definition of $<$, $n = 1 + u$. Thus, $n + 1 = 1 + u + 1$ by the inverse of the cancellation law for addition. Since $u + 1 \in \mathbb{N}$ by part (c) Theorem part (i), we have that $n + 1 = 1 + (u + 1)$, implying that $1 < n + 1$. This closes the induction. □

Proof of ii. We induct on a (keeping x, y fixed). For the base case $a = 1$, we have by part (d) that $x < y$ is equivalent to $1 \cdot x < 1 \cdot y$ since $x = 1 \cdot x$ for all $x \in \mathbb{N}$. Now suppose inductively that we have proven that $a \cdot x < a \cdot y$; we wish to prove that $(a+1) \cdot x < (a+1) \cdot y$. Let's start with

$$a \cdot x < a \cdot y$$

By the definition of $<$, we know that this implies

$$a \cdot y = a \cdot x + u$$

By the inverse of the cancellation law for addition, we can add a quantity to both sides, say y.

$$a \cdot y + y = a \cdot x + y + u$$

Since $x < y$ by assumption, $y = x + u'$ for some $u' \in \mathbb{N}$.

$$a \cdot y + y = a \cdot x + x + u' + u$$

Use the definition of multiplication and addition.

$$s(a) \cdot y = s(a) \cdot x + u' + u$$
$$(a+1) \cdot y = (a+1) \cdot x + u' + u$$

If we treat $u' + u$ as a single natural number, which we can do because of part (c) Theorem part i, we can employ the definition of $<$ one more time.

$$(a+1) \cdot x < (a+1) \cdot y$$

□

0.2 Discussion

- How much of the proof of Additional Exercise 7 proof could be left out as unnecessary verbage?

Script 1

Sets, Functions, and Cardinality

1.1 Journal

10/1: **Definition 1.2.** Two sets A and B are **equal** if they contain precisely the same elements, that is, $x \in A$ if and only if $x \in B$. When A and B are equal, we denote this by $A = B$.

Definition 1.3. A set A is a **subset** of a set B if every element of A is also an element of B, that is, if $x \in A$, then $x \in B$. When A is a subset of B, we denote this by $A \subset B$. If $A \subset B$ but $A \neq B$, we say that A is a **proper subset** of B, and we denote this by $A \subsetneq B$.

10/6: **Exercise 1.4.** Let $A = \{1, \{2\}\}$. Is $1 \in A$? Is $2 \in A$? Is $\{1\} \subset A$? Is $\{2\} \subset A$? Is $1 \subset A$? Is $\{1\} \in A$? Is $\{2\} \in A$? Is $\{\{2\}\} \subset A$? Explain.

Proof. We list affirmative or negative answers and short explanations.

Yes, $1 \in A$.
No, $2 \notin A$, but $\{2\} \in A$.
Yes, $\{1\} \subset A$ since 1 is the only element of $\{1\}$ and $1 \in A$ (as previously established).
No, $\{2\} \not\subset A$ since $2 \in \{2\}$ but $2 \notin A$ (as previously established).
No, $1 \not\subset A$ since 1 is not a set.
No, $\{1\} \notin A$, but $1 \in A$ and $\{1\} \subset A$ as previously established.
Yes, $\{2\} \in A$.
Yes, $\{\{2\}\} \subset A$ since $\{2\}$ is the only element of $\{\{2\}\}$ and $\{2\} \in A$ (as previously established). $\square$

10/1: **Definition 1.5.** Let A and B be two sets. The **union** of A and B is the set

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

Definition 1.6. Let A and B be two sets. The **intersection** of A and B is the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

Definition 1.8. The **empty set** is the set with no elements, and it is denoted $\emptyset$. That is, no matter what x is, we have $x \in \emptyset$.

Definition 1.9. Two sets A and B are **disjoint** if $A \cap B = \emptyset$.

10/6: **Exercise 1.10.** Show that if A is any set, then $\emptyset \subset A$.

Proof. Suppose for the sake of contradiction that there exists a set A such that $\emptyset \not\subset A$. Then by Definition 1.3, not every element of $\emptyset$ is also an element of A, i.e., there exists an element $x \in \emptyset$ such that $x \notin A$. But by Definition 1.8, x (like all other objects) cannot be an element of $\emptyset$, a contradiction. Therefore, $\emptyset \subset A$ for all sets A. $\square$

10/1: **Definition 1.11.** Let A and B be two sets. The **difference** of B from A is the set

$$A \setminus B = \{x \in A \mid x \notin B\}$$

The set $A \setminus B$ is also called the **complement** of B relative to A. When the set A is clear from the context, this set is sometimes denoted B^c, but we will try to avoid this imprecise formulation and use it only with warning.

Theorem 1.12. *Let X be a set, and let $A, B \subset X$. Then*

a) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$

b) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

Proof of a. To prove that $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$, Definition 1.2 tells us that it will suffice to prove that $x \in X \setminus (A \cup B)$ if and only if $x \in (X \setminus A) \cap (X \setminus B)$, i.e., that if $x \in X \setminus (A \cup B)$, then $x \in (X \setminus A) \cap (X \setminus B)$ and if $x \in (X \setminus A) \cap (X \setminus B)$, then $x \in X \setminus (A \cup B)$. To begin, let $x \in X \setminus (A \cup B)$. By Definition 1.11, $x \in X$ and $x \notin A \cup B$. By Definition 1.5, it follows that $x \notin A$ and $x \notin B$. Since we know that $x \in X$ and $x \notin A$, Definition 1.11 tells us that $x \in X \setminus A$. Similarly, $x \in X \setminus B$. Since $x \in X \setminus A$ and $x \in X \setminus B$, we have by Definition 1.6 that $x \in (X \setminus A) \cap (X \setminus B)$, as desired. The proof of the other implication is the preceding proof "in reverse." For clarity, let $x \in (X \setminus A) \cap (X \setminus B)$. By Definition 1.6, $x \in X \setminus A$ and $x \in X \setminus B$. By consecutive applications of Definition 1.11, $x \in X$, $x \notin A$, and $x \notin B$. Since $x \notin A$ and $x \notin B$, Definition 1.5 reveals that $x \notin A \cup B$. But as previously established, $x \in X$, so Definition 1.11 tells us that $x \in X \setminus (A \cup B)$. ☐

Proof of b. To prove that $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$, Definition 1.2 tells us that it will suffice to prove that $x \in X \setminus (A \cap B)$ if and only if $x \in (X \setminus A) \cup (X \setminus B)$. To begin, let $x \in X \setminus (A \cap B)$. By Definition 1.11, $x \in X$ and $x \notin A \cap B$. By Definition 1.6, it follows that $x \notin A$ or $x \notin B$. We divide into two cases. If $x \notin A$, then since we know that $x \in X$, Definition 1.11 tells us that $x \in X \setminus A$. It naturally follows that $x \in (X \setminus A) \cup (X \setminus B)$, since x need only be an element of one of the two unionized sets (see Definition 1.5). The proof is symmetric if $x \notin B$. Now let $x \in (X \setminus A) \cup (X \setminus B)$. By Definition 1.5, $x \in X \setminus A$ or $x \in X \setminus B$. Once again, we divide into two cases. If $x \in X \setminus A$, then $x \in X$ and $x \notin A$ by Definition 1.11. Consequently, by Definition 1.6, $x \notin A \cap B$. Therefore, $x \in X \setminus (A \cap B)$ by Defintion 1.11. The proof is symmetric if $x \in X \setminus B$. ☐

Definition 1.15. Let A and B be two nonempty sets. The **Cartesian product** of A and B is the set of ordered pairs

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

If $(a, b), (a', b') \in A \times B$, we say that (a, b) and (a', b') are **equal** if and only if $a = a'$ and $b = b'$. In this case, we write $(a, b) = (a', b')$.

Definition 1.16. Let A and B be two nonempty sets. A **function** f from A to B is a subset $f \subset A \times B$ such that for all $a \in A$, there exists a unique $b \in B$ satisfying $(a, b) \in f$. To express the idea that $(a, b) \in f$, we most often write $f(a) = b$. To express that f is a function from A to B in symbols, we write $f : A \to B$.

Definition 1.18. Let $f : A \to B$ be a function. The **domain** of f is A and the **codomain** of f is B. If $X \subset A$, then the **image** of X under f is the set

$$f(X) = \{f(x) \in B \mid x \in X\}$$

If $Y \subset B$, then the **preimage** of Y under f is the set

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$$

Exercise 1.19. Must $f(f^{-1}(Y)) = Y$ and $f^{-1}(f(X)) = X$? For each, either prove that it always holds or give a counterexample.

Proof. We will address each statement in turn.

Consider the sets $\{1\}$ and $\{3,4\}$, and let $f : \{1\} \to \{3,4\}$ be a function defined by $f(1) = 3$. Let $Y = \{4\}$ (we clearly have $Y \subset \{3,4\}$ since 4 is the only element of Y and $4 \in \{3,4\}$ [see Definition 1.3]). Then $f^{-1}(Y) = \{a \in \{1\} \mid f(a) \in \{4\}\} = \emptyset$ and $f(f^{-1}(Y)) = \{f(x) \in \{3,4\} \mid x \in \emptyset\} = \emptyset$ by consecutive applications of Definition 1.18. Therefore, $f(f^{-1}(Y)) \neq Y$ since $4 \in Y$ but $4 \notin f(f^{-1}(Y))$ (see Definition 1.2)[1].

Similarly, consider the sets $\{1,2\}$ and $\{3\}$, and let $f : \{1,2\} \to \{3\}$ be a function defined by $f(1) = 3$ and $f(2) = 3$. Let $X = \{1\}$ (we clearly have $X \subset \{1,2\}$ since 1 is the only element of X and $1 \in \{1,2\}$ [see Definition 1.3]). Then $f(X) = \{f(x) \in \{3\} \mid x \in \{1\}\} = \{f(1)\} = \{3\}$ and $f^{-1}(f(X)) = \{a \in \{1,2\} \mid f(a) \in \{3\}\} = \{1,2\}$ by consecutive applications of Definition 1.18. Therefore, $f^{-1}(f(X)) \neq X$ since $2 \in f^{-1}(f(X))$ but $2 \notin X$ (see Definition 1.2)[2]. $\square$

Definition 1.20. A function $f : A \to B$ is **surjective** (*also known as* **onto**) if for every $b \in B$, there is some $a \in A$ such that $f(a) = b$. The function f is **injective** (*also known as* **one-to-one**) if for all $a, a' \in A$, if $f(a) = f(a')$, then $a = a'$. The function f is **bijective** (*also known as* a **bijection**, a **one-to-one correspondence**) if it is surjective and injective.

10/6: **Exercise 1.21.** Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$. Is f injective? Is f surjective?

Proof. f is injective: Let $f(n) = f(n')$. Then $n^2 = (n')^2$, implying that $n = n'$ (note that this last step is not permissible in all number systems, but it is within the naturals).

f is not surjective: For example, $2 \in \mathbb{N}$ but there exists no natural number n such that $f(n) = n^2 = 2$ (suppose for the sake of contradiction that there exists a natural number n such that $n^2 = 2$. Since $n^2 = 2 > 1$, we know that $n < 2$ (a number is less than its square if its square is greater than 1). But the only natural number less than 2 is 1, and $1^2 = 1 \neq 2$, a contradiction). $\square$

Exercise 1.22. Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n + 2$. Is f injective? Is f surjective?

Proof. f is injective: Let $f(n) = f(n')$. Then $n + 2 = n' + 2$, implying by the cancellation law for addition that $n = n'$.

f is not surjective: For example, $1 \in \mathbb{N}$ but there exists no natural number n such that $n+2 = 1$ (suppose for the sake of contradiction that there exists a natural number n such that $n + 2 = 1$. Because $1 = n + 2$, we know that $1 > n$. But we also know that $1 \leq n$ for all $n \in \mathbb{N}$ (as can be proven by induction), which contradicts the trichotomy). $\square$

Exercise 1.23. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^2$. Is f injective? Is f surjective?

Proof. f is not injective: For example, $f(2) = 4 = f(-2)$, but $2 \neq -2$.

f is not surjective: For example, $2 \in \mathbb{Z}$ but there exists no integer x such that $f(x) = x^2 = 2$ (suppose for the sake of contradiction that there exists an integer x such that $x^2 = 2$. Since $x^2 = 2$, $|x| < 2$ for similar reasons to those discussed in Exercise 1.21. Thus, $x = -1$, $x = 0$, or $x = 1$. But $(-1)^2 = 1 \neq 2$, $0^2 = 0 \neq 2$, and $1^2 = 1 \neq 2$, a contradiction). $\square$

10/1: **Definition 1.25.** Let $f : A \to B$ and $g : B \to C$. Then the **composition** $g \circ f : A \to C$ is defined by $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

Proposition 1.26. *Let A, B, and C be sets and suppose that $f : A \to B$ and $g : B \to C$. Then $g \circ f : A \to C$ and*

a) if f and g are both injections, so is $g \circ f$.

b) if f and g are both surjections, so is $g \circ f$.

c) if f and g are both bijections, so is $g \circ f$.

[1] Note that the reason $f(f^{-1}(Y)) \neq Y$ in this case is because f is not surjective.
[2] Note that the reason $f^{-1}(f(X)) \neq X$ in this case is because f is not injective.

Proof of a. Suppose that $(g \circ f)(a) = (g \circ f)(a')$. By Definition 1.25, this implies that $g(f(a)) = g(f(a'))$. Since g is injective, Definition 1.20 tells us that $f(a) = f(a')$. Similarly, the fact that f is injective tells us that $a = a'$. Since we have shown that $(g \circ f)(a) = (g \circ f)(a')$ implies that $a = a'$ under the given conditions, we know by Definition 1.20 that $g \circ f$ is injective. □

Proof of b. Let c be an arbitrary element of C. We wish to prove that there exists some $a \in A$ such that $(g \circ f)(a) = c$ (Definition 1.20). By Definition 1.25, it will suffice to show that there exists some $a \in A$ such that $g(f(a)) = c$. Let's begin. By the surjectivity of g, there exists some $b \in B$ such that $g(b) = c$ (see Definition 1.20). If we now consider this b, we have by the surjectivity of f that there exists some $a \in A$ such that $f(a) = b$ (see Definition 1.20). But this a is an element of A such that $g(f(a)) = g(b) = c$, as desired. □

Proof of c. Suppose that f and g are two bijective functions. By Definition 1.20, this implies that f and g are both injections and are both surjections. Thus, by part (a), $g \circ f$ is an injection, and by part (b), $g \circ f$ is a surjection. Therefore, by Definition 1.20, $g \circ f$ is a bijection. □

10/6: **Proposition 1.27.** *Suppose that $f : A \to B$ is bijective. Then there exists a bijection $g : B \to A$ that satisfies $(g \circ f)(a) = a$ for all $a \in A$, and $(f \circ g)(b) = b$ for all $b \in B$.*

Proof. Let $g : B \to A$ be defined by the rule, "$g(b) = a$ if and only if $f(a) = b$." For g to be a function as defined, Definition 1.16 tells us that we must show that for every $b \in B$, there exists a unique $a \in A$ such that $g(b) = a$. By the surjectivity of f, we know that for all $b \in B$, there exists *an* $a \in A$ such that $f(a) = b$. On the uniqueness of this a, let $a \neq a'$ and suppose for the sake of contradiction that $g(b) = a$ and $g(b) = a'$. By the definition of g, we have that $f(a) = b$ and $f(a') = b$, so $f(a) = f(a')$. But by the injectivity of f, this means that $a = a'$, a contradiction. Therefore, g indeed maps every $b \in B$ to a unique $a \in A$. To demonstrate that g satisfies the remainder of the necessary constraints, we will work through them one by one.

To prove that g is injective, Definition 1.20 tells us that we must verify that if $g(b) = g(b')$, then $b = b'$. Let $g(b) = g(b')$. Since g is a function, $g(b) = g(b') = a$, where $a \in A$. This implies by the definition of g that $f(a) = b$ and $f(a) = b'$. But this means that $b = f(a) = b'$, as desired. To prove that g is surjective, Definition 1.20 tells us that we must verify that for all $a \in A$, there exists a $b \in B$ such that $g(b) = a$. Let a be an arbitrary element of A. By Definition 1.16 and the status of f as a function, there exists an element $b \in B$ such that $f(a) = b$. But by the definition of g, $f(a) = b$ implies that $g(b) = a$, meaning that this b satisfies the desired constraint. On the basis of this and the previous argument, Definition 1.20 allows us to conclude that g is bijective.

We now prove that $(g \circ f)(a) = a$ for all $a \in A$. Let a be an arbitrary element of A. Then by Definition 1.16 and the status of f as a function, $f(a) = b$ where $b \in B$. Thus, by the definition of g, $g(b) = a$, implying that $g(b) = g(f(a)) = a$. But by Definition 1.25, $g(f(a)) = (g \circ f)(a) = a$, as desired.

A symmetric argument can demonstrate that $(f \circ g)(b) = b$ for all $b \in B$. □

Definition 1.28. We say that two sets A and B are in **bijective correspondence** when there exists a bijection from A to B or, equivalently, from B to A.

Definition 1.29. Let $n \in \mathbb{N}$ be a natural number. We define $[n]$ to be the set $\{1, 2, \dots, n\}$. Additionally, we define $[0] = \emptyset$.

Definition 1.30. A set A is **finite** if $A = \emptyset$ or if there exists a natural number n and a bijective correspondence between A and the set $[n]$. If A is not finite, we say that A is **infinite**.

Theorem 1.31. *Let $n, m \in \mathbb{N}$ with $n < m$. Then there does not exist an injective function $f : [m] \to [n]$.*

Theorem 1.32. *Let A be a finite set. Suppose that A is in bijective correspondence both with $[m]$ and with $[n]$. Then $m = n$.*

Proof. If A is in bijective correspondence with both $[m]$ and with $[n]$, then Definition 1.28 tells us that there exist bijections $f : [m] \to A$ and $g : A \to [n]$. Thus, by Proposition 1.26, $g \circ f : [m] \to [n]$ is bijective. Now suppose for the sake of contradiction that $m \neq n$. Then by the trichotomy, either $m > n$ or $m < n$. We divide into two cases. If $m > n$, then Theorem 1.31 tells us that no injective function $h : [m] \to [n]$ exists.

But $f : [m] \to [n]$ is bijective, hence injective by Definition 1.20, a contradiction. On the other hand, if $m < n$, then Theorem 1.31 tells us that no injective function $h : [n] \to [m]$ exists. But by Proposition 1.27, the existence of the bijection $f : [m] \to [n]$ implies the existence of a bijection $f^{-1} : [n] \to [m]$. As before, the bijectivity of f^{-1} implies that it is also injective by Definition 1.20, a contradiction. Therefore, we must have $m = n$ based on the given conditions. ☐

10/8: **Definition 1.33** (Cardinality of a finite set)**.** If A is a finite set that is in bijective correspondence with $[n]$, then we say that the **cardinality** of A is n, and we write $|A| = n$. (By Theorem 1.32, there is exactly one such natural number n.) We also say that A contains n elements. We define the cardinality of the empty set to be 0.

Exercise 1.34. Let A and B be finite sets.

a) If $A \subset B$, then $|A| \leq |B|$.

Proof. Let $|A| = m$ and $|B| = n$. Using these variables, Definitions 1.33 and 1.28 tell us that there exist bijections $f : [m] \to A$ and $g : B \to [n]$. Now let $h : A \to B$ be defined by $h(a) = a$ for each $a \in A$. By Definition 1.16, to verify that h is a function, we must show that for every $a \in A$, there exists a unique $b \in B$ such that $h(a) = b$. Let a be an arbitrary element of A. Since $A \subset B$, Definition 1.3 implies that $a \in B$. Thus, since $h(a) = a$, $h(a) \in B$. Now suppose for the sake of contradiction that $h(a) = b$ and $h(a) = b'$ for two elements $b, b' \in B$ such that $b \neq b'$. By the definition of h, $h(a) = a$, so $a = b$ and $a = b'$, implying by transitivity that $b = b'$, a contradiction. Thus, h is a well-defined function.

We now demonstrate that h is injective. By Definition 1.20, it will suffice to show that $h(a) = h(a')$ implies that $a = a'$ (where $a, a' \in A$). So suppose that $h(a) = h(a')$. By the definition of h, $h(a) = a$ and $h(a') = a'$, so by assumption, $a = h(a) = h(a') = a'$, as desired. Therefore, h is injective.

To recap, at this point we have injective functions $f : [m] \to A$, $h : A \to B$, and $g : B \to [n]$, where the injectivity of f and g follows from their bijectivity (see Definition 1.20). It follows by consecutive applications of Proposition 1.26 that $h \circ f$ is injective, and that $g \circ (h \circ f)$ is injective. Thus, there exists an injective function $g \circ (h \circ f) : [m] \to [n]$, so the contrapositive of Theorem 1.31 implies that it is false that $n < m$. Equivalently, it is true that $n \geq m$, or, to return substitutions, that $|A| \leq |B|$. ☐

b) Let $A \cap B = \emptyset$. Then $|A \cup B| = |A| + |B|$.

Proof. Let $|A| = m$ and $|B| = n$. Thus, $|A| + |B| = m + n$, so to prove that $|A \cup B| = |A| + |B|$, Definition 1.33 and 1.28 tell us that that we must find a bijection $f : A \cup B \to [m + n]$. Let's begin.

Since $|A| = m$ and $|B| = n$, by Definition 1.33 and 1.28, there exist bijections $g_1 : A \to [m]$ and $g_2 : B \to [n]$. As such, let $f : A \cup B \to [m + n]$ be defined as follows:

$$f(x) = \begin{cases} g_1(x) & x \in A \\ g_2(x) + m & x \in B \end{cases}$$

Since the two cases defining f are both functions, the only possible barrier to f itself being a function is if there exists some $x \in A \cup B$ such that $x \in A$ and $x \in B$. To address this, suppose for the sake of contradiction that this is the case. Fortunately, such a hypothesis implies by Definition 1.6 that $x \in A \cap B$, contradicting the fact that $A \cap B = \emptyset$.

To prove that f is injective, the contrapositive of Definition 1.20 tells us that we must verify that if $x \neq x'$, then $f(x) \neq f(x')$. We divide into three cases ($x, x' \in A$, $x, x' \in B$, and WLOG $x \in A$ and $x' \in B$[3]). First, suppose that $x, x' \in A$. Then $f(x) = g_1(x)$ and $f(x') = g_1(x')$. By the injectivity of g_1 (which follows from its bijectivity by Definition 1.20), we have that $g_1(x) \neq g_1(x')$, which means that $f(x) = g_1(x) \neq g_1(x') = f(x')$, as desired. Second, suppose that $x, x' \in B$. Then

[3]Note that we do not have to treat the case that $x \in B$ and $x' \in A$ since in this case, we just call the object represented by x, "x'," and vice versa — this reversal of names is what is implied by "Without the Loss Of Generality," or WLOG.

$f(x) = g_2(x) + m$ and $f(x') = g_2(x') + m$. By the injectivity of g_2, we have that $g_2(x) \neq g_2(x')$, which implies by the inverse of the cancellation law for addition that $g_2(x) + m \neq g_2(x') + m$. Thus, $f(x) = g_2(x) + m \neq g_2(x') + m = f(x')$, as desired. Third, suppose that $x \in A$ and $x' \in B$. Then $f(x) = g_1(x)$ is an element of $[n]$ while $f(x') = g_2(x')$ is an element of $[m+1 : m+n]$, two sets that are clearly disjoint (see Axioms III and IV of the Peano Postulates). Thus, we cannot have $f(x) = f(x')$, as desired.

To prove that f is surjective, Definition 1.20 tells us that we must verify that for every $i \in [m+n]$, there exists an $x \in A \cup B$ such that $f(x) = i$. We divide into two cases ($i \leq m$ and $i \geq m+1$). If $i \leq m$, then $i \in [m]$. It follows by the surjectivity of g_1 (which follows from its bijectivity by Definition 1.20) that there exists an $x \in A$ such that $g_1(x) = i$. Now by Definition 1.5, this x is also an element of $A \cup B$, so $g_1(x) = f(x) = i$, as desired. On the other hand, if $i \geq m+1$, then $i = m + u$ for some $u \in [n]$. It follows by the surjectivity of g_2 that there exists an $x \in B$ such that $g_2(x) = u$. Thus, $i = m + u = m + g_2(x) = f(x)$, as desired.

At this point, Definition 1.20 implies that f is bijective, meaning by Definition 1.28 and 1.33 that $|A \cup B| = m + n = |A| + |B|$, as desired. ☐

c) $|A \cup B| + |A \cap B| = |A| + |B|$.

Proof. We begin with a lemma.

Lemma. *Let A and B be sets. Then*

a) $A \cup B = (B \setminus A) \cup A$;
b) $(B \setminus A) \cap A = \emptyset$.
c) $B = (B \setminus A) \cup (A \cap B)$.
d) $(B \setminus A) \cap (A \cap B) = \emptyset$.

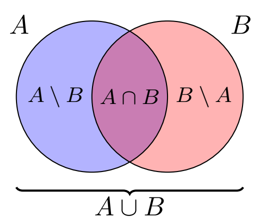


Figure 1.1: Set union Venn diagram.

Proof. All of these claims can be read directly from the above diagram — for the sake of space and because proving these claims is not the main point of this exercise, a rigorous proof of this lemma will be omitted. ☐

Back to the main claim, we want to show that $|A \cup B| + |A \cap B| = |A| + |B|$, which we can do by using the above lemma to justify various manipulations inspired by part (b). To begin, use Lemma (a) as follows.

$$|A \cup B| + |A \cap B| = |(B \setminus A) \cup A| + |A \cap B|$$

Since $(B \setminus A) \cup A$ is a union of two disjoint sets (see Lemma (b)), it follows by part (b) that the above

$$\begin{aligned} &= |B \setminus A| + |A| + |A \cap B| \\ &= |A| + |B \setminus A| + |A \cap B| \end{aligned}$$

Since $B \setminus A$ and $A \cap B$ are disjoint (see Lemma (d)), we know that the above

$$= |A| + |(B \setminus A) \cup (A \cap B)|$$

Lastly, apply Lemma (c):

$$= |A| + |B|$$

□

10/13: d) $|A \times B| = |A| \cdot |B|$.

Proof. Let $|A| = n$ and $|B| = m$. Then since A and B are finite, Definition 1.30 and 1.28 tell us that there exist bijections $f : A \to [n]$ and $g : B \to [m]$. By Definition 1.33 and 1.28, to prove the claim, it will suffice to find a bijection $h : A \times B \to [m \cdot n]$.

Let $h : A \times B \to [m \cdot n]$ be defined by

$$h(a, b) = f(a) + n \cdot (g(b) - 1)$$

Clearly, the above rule assigns a unique value to every (a, b), and since f and g map all $a \in A$ and $b \in B$, respectively, the above function is not undefined for any $(a, b) \in A \times B$. Thus, h is a function as defined in Definition 1.16.

We must now prove that h is bijective. By Definition 1.20, it will suffice to prove that h is injective and surjective, which we may do as follows. We shall start with injectivity.

Let

$$h(a, b) = h(a', b')$$

Then by the definition of h,

$$\begin{aligned} f(a) + n \cdot (g(b) - 1) &= f(a') + n \cdot (g(b') - 1) \\ f(a) - f(a') &= n \cdot (g(b') - 1) - n \cdot (g(b) - 1) \\ f(a) - f(a') &= n \cdot (g(b') - g(b)) \end{aligned}$$

Since $f(a)$ and $f(a')$ are both elements of $[n]$, we have $|f(a) - f(a')| < n$ (since $\max([n]) - \min([n]) = n - 1 < n$). Substituting, we have that $|n \cdot (g(b') - g(b))| < n$, i.e., $|g(b') - g(b)| < 1$. But since $g(b), g(b') \in [m]$, the only way that $|g(b') - g(b) < 1$ is if $|g(b') - g(b)| = 0$. Consequently, $g(b') - g(b) = 0$, so additionally, $f(a) - f(a') = n \cdot (g(b') - g(b)) = 0$. Having ascertained that $g(b') - g(b) = 0$ and $f(a) - f(a') = 0$, it is a simple matter to find that $g(b) = g(b')$ and $f(a) = f(a')$, meaning by the bijectivity (more specifically, the injectivity) of f and g that $b = b'$ and $a = a'$. But by Definition 1.15, this implies that $(a, b) = (a', b')$, as desired.

As to surjectivity, let c be an arbitrary element of $[n \cdot m]$. As a natural number, c can be written in the form $c = \beta \cdot n + \alpha$ where $1 \leq \alpha \leq n$ and $\beta \in \mathbb{N}$. We know that $\min([n \cdot m]) = 1 = 0 \cdot n + 1$ and $\max([n \cdot m]) = m \cdot n = (m - 1) \cdot n + n$; thus, if we restrict the possible values of β to $0 \leq \beta \leq m - 1$, we still know that $c = \beta \cdot n + \alpha$ for some $1 \leq \alpha \leq n$ and $0 \leq \beta \leq m - 1$. Now by the surjectivity of f, there exists an $a \in A$ such that $f(a) = \alpha$ for any $1 \leq \alpha \leq n$. Similarly, the surjectivity of g implies that there exists a $b \in B$ such that $g(b) = \beta + 1$ for any $1 \leq \beta + 1 \leq m$, i.e., there exists a $b \in B$ such that $g(b) - 1 = \beta$ for any $0 \leq \beta \leq m - 1$. Therefore, c can be written in the form $c = f(a) + n \cdot (g(b) - 1)$ for some $a \in A$ and $b \in B$, which by the definition of h means that $c = h(a, b)$ for some $(a, b) \in A \times B$, as desired. □

10/8: **Definition 1.35.** An infinite set A is said to be **countable** if it is in bijective correspondence with $\mathbb{N}$. An infinite set that is not countable is called **uncountable**.

Exercise 1.36. Prove that $\mathbb{Z}$ is a countable set.

Proof. To prove that $\mathbb{Z}$ is countable, Definition 1.35 and, subsequently, Definition 1.28 tell us that we must find a bijection $f : \mathbb{Z} \to \mathbb{N}$. To do so, we will define a matching and then prove that the guiding rule generates a (1) function that is (2) injective and (3) surjective (demonstrating injectivity and surjectivity verifies bijectivity by Definition 1.20).

Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as follows:

$$f(z) = \begin{cases} -2z+1 & z \in -\mathbb{N} \\ 1 & z \in \{0\} \\ 2z & z \in \mathbb{N} \end{cases}$$

Since $\mathbb{Z} = (-\mathbb{N}) \cup \{0\} \cup (\mathbb{N})$, it is clear that the above mapping sends every element of $\mathbb{Z}$ to *an* element of $\mathbb{N}$. Additionally, since $-\mathbb{N}$, $\{0\}$, and $\mathbb{N}$ are all disjoint from one another, it follows that each element of $\mathbb{Z}$ is only mapped once. Thus, by Definition 1.16, f is a function as defined.

Let $f(z) = f(z')$. Since the outputs of the first case in the definition of f are the odd natural numbers except 1, the one of the second case is 1, and those of the third case are the even natural numbers, the outputs form three disjoint sets, so $f(z)$ and $f(z')$ as equal quantities are elements of only one category. We now divide into three cases by category. First, suppose $f(z) = f(z')$ is an odd natural number not equal to 1. Then we have by the definition of f that $-2z+1 = -2z'+1$, implying by the cancellation laws of addition and multiplication, respectively, that $z = z'$. Second, suppose that $f(z) = f(z') = 1$. Then $z = z' = 0$ by the definition of f. Lastly, suppose $f(z) = f(z')$ is an even natural number. Then we have by the definition of f that $2z = 2z'$, implying by the cancellation law of multiplication that $z = z'$. Therefore, in any case, $f(z) = f(z')$ implies that $z = z'$, meaning by Definition 1.20 that f is injective.

Let n be an arbitrary element of $\mathbb{N}$. As noted in "What is a mathematical proof?", n must be either odd or even. Now if n is odd, n is either equal to 1 or not equal to 1. Thus, we can break the natural numbers $\mathbb{N}$ into three disjoint sets: $\mathbb{N} = (\{n \in \mathbb{N} : n \text{ is odd}\} \setminus \{1\}) \cup \{1\} \cup \{n \in \mathbb{N} : n \text{ is even}\}$. We now divide into three cases, each pertaining to one of the disjoint subsets of $\mathbb{N}$ defined above. First, suppose n is odd and not equal to 1. Then $n = 2z + 1$ for some $z \in \mathbb{N}$ (see "What is a mathematical proof?"), or $-2z + 1$ for some $z \in -\mathbb{N}$ (the negative signs cancel). By the definition of f, this $z \in -\mathbb{N}$ is the element of $\mathbb{Z}$ that f sends to n. Second, suppose that $n = 1$. Then since $f(0) = 1$ by the definition of f, 0 is the element of $\mathbb{Z}$ from which f generates 1. Lastly, suppose that n is even. Then $n = 2z$ for some $z \in \mathbb{N}$ (see "What is a mathematical proof?"). By the definition of f, this z is the element of $\mathbb{Z}$ that f sends to n. Therefore, for every element $n \in \mathbb{N}$, there exists a $z \in \mathbb{Z}$ satisfying $f(z) = n$, meaning by Definition 1.20 that f is surjective. As mentioned at the top, the last two results (injectivity and surjectivity) together imply that f is bijective by Definition 1.20. ☐

10/13: **Exercise 1.37.** Prove that every infinite subset of a countable set is also countable.

Lemma. *Every infinite subset of the natural numbers is countable.*

Proof. Let $A \subset \mathbb{N}$ be infinite. To prove that A is countable, Definition 1.35 tells us that it will suffice to show that there exists a bijection $g : \mathbb{N} \to A$. Let's begin.

We define g recursively with strong induction, as follows. Note that $A = A \setminus \{\}$ where $\{\} = \emptyset$. By the well-ordering principle (see Script 0), there exists a minimum element $\min(A \setminus \{\}) \in A \setminus \{\}$; we define $g(1) = \min(A \setminus \{\})$. Now suppose inductively that we have defined $g(1), g(2), \dots, g(n)$. Then we can define $g(n+1)$ by defining $g(n+1) = \min(A \setminus \{g(1), g(2), \dots, g(n)\})$[4]. By the principle of strong mathematical induction, it follows that g is defined for all $n \in \mathbb{N}$, and it is obvious that g is not multiply defined for any $n \in \mathbb{N}$. Thus, g is a function as defined in Definition 1.16.

To prove that g is bijective, Definition 1.20 tells us that it will suffice to show that g is injective and surjective. We will prove each of these qualities in turn. To prove that g is injective, Definition 1.20 tells us that we must verify that $n \neq n'$ implies $g(n) \neq g(n')$. Suppose that $n \neq n'$. Then by the trichotomy,

[4]Basically, what this definition is doing is mapping 1 to the least element of A, 2 to the second-least element of A, 3 to the third-least element of A, and so on and so forth. Notice how the least element of A is denoted by $g(1)$, and $g(2)$ (for example) is equal to $\min(A \setminus \{g(1)\})$, i.e., the minimum value in A if A's least element did not exist, i.e., the second-least element in A. Additionally, $g(3) = \min(A \setminus \{g(1), g(2)\})$, so we can see how $g(3)$ is the third-least element in A by the same logic used in discussing $g(2)$. Obviously, the pattern continues for all $n \in \mathbb{N}$.

either $n > n'$ or $n < n'$. If $n > n'$, then $g(n) = \min(A \setminus \{g(1), \dots, g(n'), \dots, g(n-1)\})$, meaning that $g(n)$ cannot equal $g(n')$ since $g(n)$ is an element of a set (namely, $A \setminus \{g(1), \dots, g(n'), \dots, g(n-1)\}$) of which $g(n')$ is explicitly not a member. The proof is symmetric if $n < n'$. To prove that g is surjective, Definition 1.20 tells us that we must verify that for all $a \in A$, there exists an $n \in \mathbb{N}$ such that $g(n) = a$. Suppose for the sake of contradiction that there exists some $a \in A$ such that $g(n) \neq a$ for any $n \in \mathbb{N}$. This implies that $a \neq \min(A \setminus \{g(1), \dots, g(n)\})$ for any $n \in \mathbb{N}$, which must mean that $a \notin A$, a contradiction. □

Proof. Let A be a countable set and let $B \subset A$ be an infinite set. By Definition 1.35 and 1.28, there exists a bijection $f : A \to \mathbb{N}$. Now consider the set $f(B)$. Clearly $\tilde{f} : B \to f(B)$ defined by $\tilde{f}(b) = f(b)$ is a function and a bijection. Since $f(B) \subset \mathbb{N}$ is infinite, there exists a bijection $g : f(B) \to \mathbb{N}$ by the lemma and Definition 1.35. It follows by Proposition 1.26 that $g \circ \tilde{f} : B \to \mathbb{N}$ is a bijection, proving that B is countable by Definition 1.35, as desired. □

Exercise 1.38. Prove that if there is an injection $f : A \to B$ where B is countable and A is infinite, then A is countable.

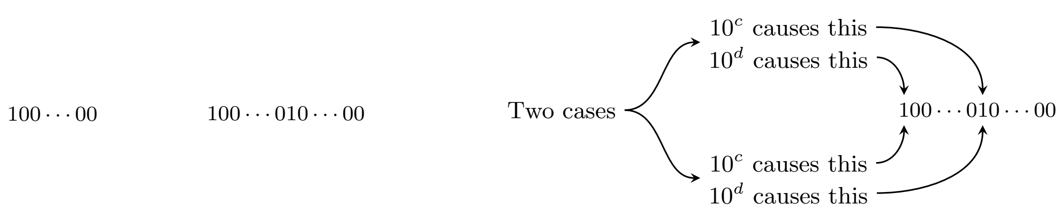
Proof. Let $\tilde{f} : A \to f(A)$ be defined by $\tilde{f}(a) = f(a)$. To prove that $\tilde{f}$ is a function, Definition 1.16 tells us that it will suffice to show that for all $a \in A$, there exists a unique $b \in f(A)$ such that $\tilde{f}(a) = b$. Let a be an arbitrary element of A. It follows by Definition 1.18 that $f(a) \in f(A)$, hence $\tilde{f}(a) \in A$ by the definition of $\tilde{f}$. Furthermore, since $f(a)$ is a unique object, $\tilde{f}(a)$ is also a unique object.

To prove that $\tilde{f}$ is bijective, Definition 1.20 tells us that it will suffice to show that $\tilde{f}$ is injective and surjective. We will verify these two characteristics in turn. To prove that $\tilde{f}$ is injective, Definition 1.20 tells us that we must demonstrate that $\tilde{f}(a) = \tilde{f}(a')$ implies $a = a'$. Let $\tilde{f}(a) = \tilde{f}(a')$. By the definition of $\tilde{f}$, $\tilde{f}(a) = f(a)$ and $\tilde{f}(a') = f(a')$. Thus, $f(a) = \tilde{f}(a) = \tilde{f}(a') = f(a')$, i.e., $f(a) = f(a')$. As such, by the injectivity of f, $a = a'$, as desired. To prove that $\tilde{f}$ is surjective, Definition 1.20 tells us that we must demonstrate that for all $b \in f(A)$, there exists an $a \in A$ such that $\tilde{f}(a) = b$. Let b be an arbitrary element of $f(A)$. By Definition 1.18, it follows that $b = f(a)$ for some $a \in A$. But by the definition of $\tilde{f}$, we also have $f(a) = \tilde{f}(a)$, so transitivity implies that $\tilde{f}(a) = b$, as desired.

Since A is infinite, Definition 1.30 tells us that no bijection $h : A \to [n]$ exists for any $n \in \mathbb{N}$. Consequently, since there exists a bijection $\tilde{f} : A \to f(A)$, no bijection $h : f(A) \to [n]$ exists, implying by Definition 1.30 that $f(A)$ is similarly infinite. In addition to being infinite, Definition 1.18 asserts that $f(A) \subset B$. Thus, Exercise 1.37 applies and proves that $f(A)$ is countable. It follows by Definition 1.35 that there exists a bijection $g : f(A) \to \mathbb{N}$. Since $\tilde{f}$ and g are both bijective, Proposition 1.26 implies that $g \circ \tilde{f} : A \to \mathbb{N}$ is bijective. Therefore, A and $\mathbb{N}$ are in bijective correspondence by Definition 1.28, meaning that A is countable by Definition 1.35. □

Exercise 1.39. Prove that $\mathbb{N} \times \mathbb{N}$ is countable by considering the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $f(n, m) = (10^n - 1)10^m$.

Lemma (Informal[5]). *If $10^a + 10^b = 10^c + 10^d$ for $a, b, c, d \in \mathbb{N}$, then either $a = c$ and $b = d$, or $a = d$ and $b = c$.*



(a) 10^a. (b) $10^a + 10^b$. (c) Possible matchings of 10^c and 10^d.

Figure 1.2: Base-10 representations (ignoring the case where $a = b$).

[5]Dr. Cartee approved this.

Proof. Refer to Figure 1.2 throughout the following discussion. Think about the base-10 representation of 10^a — it will be a 1 followed by a bunch of 0s. When we add 10^b to 10^a, either one of the 0s becomes a 1, the 1 becomes a 2, or a further string consisting of a 1 (possibly followed by 0s) is concatenated to the beginning of the existing number. In any of these cases, it is clear that for this number to be written in the form $10^c + 10^d$, one of those two terms (10^c or 10^d) must account for one of the 1s, and the other for the other 1 (or both for the 2, in that case). □

Proof. We wish to prove that f is injective, so that Exercise 1.38 applies. By Definition 1.20, proving that f is injective necessitates showing that $f(a, b) = f(c, d)$ implies that $(a, b) = (c, d)$ for all $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Let $(a, b), (c, d)$ be arbitrary elements $\mathbb{N} \times \mathbb{N}$, and suppose that

$$f(a, b) = f(c, d)$$

Substituting the definition of f and algebraically manipulating, we get

$$\begin{aligned}(10^a - 1)(10^b) &= (10^c - 1)(10^d)\\ 10^{a+b} - 10^b &= 10^{c+d} - 10^d\\ 10^{a+b} + 10^d &= 10^{c+d} + 10^b\end{aligned}$$

By the lemma, either $a + b = b$ and $c + d = d$, or $a + b = c + d$ and $b = d$. In the first case, we must have $a = 0$ and $c = 0$ for the equalities to hold. But since $0 \notin \mathbb{N}$, this implies that $a, c \notin \mathbb{N}$, a contradiction. Thus this case does not hold and it must be that the second case is true. In the second case, $b = d$, so by the cancellation law for addition, $a = c$. Since $a = c$ and $b = d$, Definition 1.15 tells us that $(a, b) = (c, d)$, as desired.

Having proven that there exists an injection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where $\mathbb{N}$ is (clearly) countable and $\mathbb{N} \times \mathbb{N}$ is (clearly) infinite, Exercise 1.38 implies that $\mathbb{N} \times \mathbb{N}$ is countable, as desired. □

Additional Exercises

10/6: 1. In each of the following, write out the elements of the sets.

a) $(\{n \in \mathbb{Z} \mid n \text{ is divisible by } 2\} \cap \mathbb{N}) \cup \{-5\}$

Proof. The elements are -5 as well as 2, 4, 6, and every other even natural number. □

c) $\{[n] \mid n \in \mathbb{N}, 1 \leq n \leq 3\}$

Proof. The elements are the three sets $\{1\}$, $\{1, 2\}$, and $\{1, 2, 3\}$. □

k) $\{\{a\} \cup \{b\} \mid a \in \mathbb{N}, b \in \mathbb{N}, 1 \leq a \leq 4, 3 \leq b \leq 5\}$

Proof. The elements are the 11 sets $\{1, 3\}$, $\{1, 4\}$, $\{1, 5\}$, $\{2, 3\}$, $\{2, 4\}$, $\{2, 5\}$, $\{3\}$, $\{3, 4\}$, $\{3, 5\}$, $\{4\}$, and $\{4, 5\}$. □

1.2 Discussion

10/1:
- Always make sure you use all given assumptions.
- We are allowed to assume that $x \in \{A : Q\}$ tells us that $x \in A$ and Q is true? — yes.
- We can let x be an arbitrary element of a set and deduce stuff like in Tao.
- When we're writing proofs (consider Theorem 1.12), do we do not have to show the definition of $A \cap B$? — we can just say "by Definition 1.6, $y \notin A \cap B$ implies that $y \notin a$ or $y \notin b$."
- What he wrote for the beginning of the proof of Theorem 1.12 (see Figure 1.3) is acceptable on an exam; in our exams, it will be the same as when presenting to class (we do not need complete sentences).

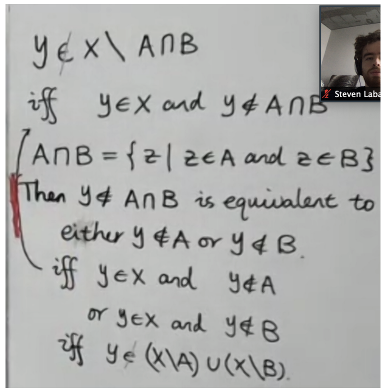


Figure 1.3: Sample exam-ready proof of Theorem 1.12.

- Can we say "A similar argument works in reverse?"

10/6:
- Vacuous truths were introduced.
- If you had to prove your answers to Additional Exercise 1, you would write out the elements of the first set, and rewrite the elements with each additional constraint.
  - For example, $(\{n \in \mathbb{Z} \mid n \text{ is divisible by } 2\} \cap \mathbb{N}) \cup \{-5\} = (\{\cdots, -4, -2, 0, 2, 4, \cdots\} \cap \{1, 2, 3, \cdots\}) \cup \{-5\} = \{2, 4, 6, \cdots\} \cup \{-5\}$.
- In this class, $0 \notin \mathbb{N}$, but $0 \in \mathbb{N}_0$.
- For Exercise 1.21, we can refer to Theorem 7 in "Notes on proofs" to demonstrate that $\sqrt{2} \notin \mathbb{N}$.
- When presenting, write on the board more like I would in a journal.
- Ask about my contradiction proofs for 1.21-1.23!

10/8:
- ! means "unique."
- $\because$ means "since."

10/13:
- What are your office hours? Mondays 4-6 PM.
- Do I need to submit the LaTeX assignment to you? Email it to him!
- Edit this document to reflect switch to section 22!
- Script 2 sign up sheet is on Canvas (sign up within 24 hours)!

Script 2

The Rationals

2.1 Journal

10/15: **Definition 2.1.** Let X be a set. A **relation** R on X is a subset of $X \times X$. The statement $(x, y) \in R$ is read "x is related to y by the relation R" and is often denoted $x \sim y$.

A relation is **reflexive** if $x \sim x$ for all $x \in X$.
A relation is **symmetric** if $y \sim x$ whenever $x \sim y$.
A relation is **transitive** if $x \sim z$ whenever $x \sim y$ and $y \sim z$.
A relation is an **equivalence relation** if it is reflexive, symmetric, and transitive.

Exercise 2.2. Determine which of the following are equivalence relations.

a) Any set X with the relation $=$. So $x \sim y$ if and only if $x = y$.

Proof. To prove that the relation $=$ is reflexive, Definition 2.1 tells us that it will suffice to show that $x \sim x$ for all $x \in X$. Clearly, $x = x$ for all $x \in X$. It follows by the definition of $=$ that $x \sim x$ for all $x \in X$. For symmetry, we must verify that $x \sim y$ implies $y \sim x$ for any $x, y \in X$. Let $x \sim y$ for some $x, y \in X$. Consequently, by the definition of $=$, $x = y$. It follows that $y = x$, and thus that $y \sim x$. For transitivity, we must show that $x \sim y$ and $y \sim z$ imply that $x \sim z$ for any $x, y, z \in X$. Let $x \sim y$ and $y \sim z$ for some $x, y, z \in X$. By the definition of $=$, $x \sim y$ and $y \sim z$ imply that $x = y$ and $y = z$, respectively. Thus, $x = y = z$, so $x = z$, meaning that $x \sim z$ by the definition of the relation $=$. Since the relation $=$ is reflexive, symmetric, and transitive, it is an equivalence relation. $\square$

b) $\mathbb{Z}$ with the relation $<$.

Proof. The relation $<$ is neither reflexive nor symmetric, although it is transitive. Since demonstrating that $<$ does not satisfy any one of the three properties proves that $<$ is not an equivalence relation, we shall arbitrarily choose to prove that $<$ is not reflexive. Consider $1 \in \mathbb{Z}$, and note that $1 = 1$. Since $1 = 1$, $1 \not< 1$ by the trichotomy. Thus, $1 \nsim 1$ by the relation $<$, proving that $<$ is not reflexive for all $z \in Z$, i.e., $<$ is not an equivalence relation. $\square$

c) Any subset X of $\mathbb{Z}$ with the relation $\leq$. So $x \sim y$ if and only if $x \leq y$.

Proof. Here, we demonstrate a failure of symmetry. Let $X = \{1, 2\}$. Clearly, $X \subset \mathbb{Z}$. Now, $1 \leq 2$, so $1 \sim 2$ by the relation $\leq$, but $2 \nleq 1$ so $2 \nsim 1$. Thus, $x \sim x'$ for $x, x' \in X$ does not necessarily imply that $x' \sim x$. It follows that $\leq$ is not an equivalence relation on *any* subset of $\mathbb{Z}$. $\square$

d) $X = \mathbb{Z}$ with $x \sim y$ if and only if $y - x$ is divisible by 5.

Proof. To prove that the described relation is an equivalence relation, Definition 2.1 tells us that we must verify that it is reflexive, symmetric, and transitive. To prove these properties, it will suffice to show that $x \sim x$ for all $x \in X$, $x \sim y$ implies $y \sim x$ for any $x, y \in X$, and $x \sim y$ and $y \sim z$ implies $x \sim z$ for any $x, y, z \in X$, respectively. Let's begin.

To prove that $x \sim x$ for all $x \in X$, it will suffice to show that $\frac{x-x}{5} \in X$ for an arbitrary element $x \in X$. Let x be such an object. It follows that $\frac{x-x}{5} = \frac{0}{5} = 0$. Since $0 \in X$, $\frac{x-x}{5} \in X$, as desired.

To prove that $x \sim y$ implies that $y \sim x$ for any $x, y \in X$, it will suffice to show that $\frac{x-y}{5} \in X$ given that $\frac{y-x}{5} \in X$. Since $\frac{y-x}{5} \in X$, it follows by the set theoretic definition of $\mathbb{Z}$ that $-\frac{y-x}{5} \in X$. But $-\frac{y-x}{5} = \frac{x-y}{5}$, so $\frac{x-y}{5} \in X$, as desired.

To prove that $x \sim y$ and $y \sim z$ implies that $x \sim y$ for any $x, y, z \in X$, it will suffice to show that $\frac{z-x}{5} \in X$ given that $\frac{y-x}{5} \in X$ and $\frac{z-y}{5} \in X$. Since $\frac{y-x}{5} \in X$ and $\frac{z-y}{5} \in X$, it follows by the closure of integer addition that $\left(\frac{z-y}{5} + \frac{y-x}{5}\right) \in X$. But $\frac{z-y}{5} + \frac{y-x}{5} = \frac{z-y+y-x}{5} = \frac{z-x}{5}$, so $\frac{z-x}{5} \in X$, as desired. ☐

e) $X = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$ with the relation $\sim$ defined by $(a, b) \sim (c, d) \iff ad = bc$.

Proof. Reflexivity: Let (a, b) be an arbitrary element of X. Since $a, b \in \mathbb{Z}$ and integer multiplication is commutative, $ab = ba$. Therefore, by the definition of the relation $\sim$, $(a, b) \sim (a, b)$.

Symmetry: Let $(a, b) \sim (c, d)$ for some $(a, b), (c, d) \in X$. By the definition of the relation $\sim$, $ad = bc$. Thus, $cb = da$ by the symmetry of $=$ (see part (a)) and the commutativity of integer multiplication. Consequently, by the definition of the relation $\sim$, $(c, d) \sim (a, b)$.

Transitivity: Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ for some $(a, b), (c, d), (e, f) \in X$. By consecutive applications of the definition of $\sim$, $ad = bc$ and $cf = de$. Now if we consider $ad = bc$, we can multiply an equal quantity to each side and still preserve the equality. As such, we choose to multiply $cf = de$ to both sides, creating the equation $ad \cdot cf = bc \cdot de$. By the commutativity of multiplication, we have $afcd = becd$. By the cancellation law for multiplication, we have $af = be$ (we cancel out cd from both sides). Therefore, by the definition of the relation $\sim$, $(a, b) \sim (e, f)$. ☐

Remark 2.3. A **partition** of a set is a collection of non-empty disjoint subsets whose union is the original set. Any equivalence relation on a set creates a partition of that set by collecting into subsets all of the elements that are equivalent (related) to each other. When the partition of a set arises from an equivalence relation in this manner, the subsets are referred to as **equivalence classes**.

Remark 2.4. If we think of the set X in Exercise 2.2e as representing the collection of all fractions whose denominators are not zero, then the relation $\sim$ may be thought of as representing the equivalence of two fractions.

Definition 2.5. As a set, the **rational numbers**, denoted $\mathbb{Q}$, are the equivalence classes in the set $X = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$ under the equivalence relation $\sim$ as defined in Exercise 2.2e. If $(a, b) \in X$, we denote the equivalence class of this element as $\left[\frac{a}{b}\right]$. So

$$\left[\frac{a}{b}\right] = \{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a, bb)\} = \{(x_1, x_2) \in X \mid x_1 b = x_2 a\}$$

Then,

$$\mathbb{Q} = \left\{ \left[\frac{a}{b}\right] \middle| (a, b) \in X \right\}$$

Exercise 2.6. $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right] \iff (a, b) \sim (a', b')$

Proof. To prove this claim, we must prove the two implications

$$\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right] \implies (a, b) \sim (a', b') \qquad\qquad (a, b) \sim (a', b') \implies \left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$$

Suppose first that $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$. Then by Definition 2.5,

$$\{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a, b)\} = \{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a', b')\}$$

Since $(a, b) \sim (a, b)$ by Exercise 2.2e and clearly $(a, b) \in X$, it follows that $(a, b) \in \{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a, b)\}$. Consequently, set equality implies that $(a, b) \in \{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a', b')\}$. Thus, $(a, b) \sim (a', b')$, as desired.

Now suppose that $(a, b) \sim (a', b')$. To prove that $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$, Definition 2.5 tells us that it will suffice to show that

$$\{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a, b)\} = \{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a', b')\}$$

Let (x_1, x_2) be an arbitrary element of $\{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a, b)\}$. It follows that $(x_1, x_2) \sim (a, b)$. Thus, since $(a, b) \sim (a', b')$, the transitivity of $\sim$ (see Exercise 2.2e) implies that $(x_1, x_2) \sim (a', b')$. This coupled with the fact that $(x_1, x_2) \in X$ means that $(x_1, x_2) \in \{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a', b')\}$. The proof is symmetric if we first let that (x_1, x_2) be an arbitrary element of $\{(x_1, x_2) \in X \mid (x_1, x_2) \sim (a', b')\}$. ☐

Definition 2.7. We define the binary operations addition and multiplication on $\mathbb{Q}$ as follows. If $\left[\frac{a}{b}\right], \left[\frac{c}{d}\right] \in \mathbb{Q}$, then

$$\left[\frac{a}{b}\right] +_{\mathbb{Q}} \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right]$$
$$\left[\frac{a}{b}\right] \cdot_{\mathbb{Q}} \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right]$$

We use the notation $+_{\mathbb{Q}}$ and $\cdot_{\mathbb{Q}}$ to represent addition and multiplication in $\mathbb{Q}$ so as to distinguish these operations from the usual addition $(+)$ and multiplication $(\cdot)$ in $\mathbb{Z}$.

Theorem 2.8. *Addition in $\mathbb{Q}$ is well-defined. That is, if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then*

$$\left[\frac{a}{b}\right] +_{\mathbb{Q}} \left[\frac{c}{d}\right] = \left[\frac{a'}{b'}\right] +_{\mathbb{Q}} \left[\frac{c'}{d'}\right]$$

Lemma. *If $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $(ad + bc, bd) \sim (a'd' + b'c', b'd')$.*

Proof. By consecutive applications of the definition of $\sim$, we have that

$$ab' = ba' \qquad\qquad cd' = dc'$$

It follows by the multiplicative property of equality that

$$ab'dd' = ba'dd' \qquad\qquad bb'cd' = bb'dc'$$

The above two results can be combined via the additive property of equality, giving the following, which will further be algebraically manipulated.

$$ab'dd' + bb'cd' = ba'dd' + bb'dc'$$
$$adb'd' + bcb'd' = bda'd' + bdb'c'$$
$$(ad + bc)(b'd') = (bd)(a'd' + b'c')$$

The last line above implies by the definition of $\sim$ that $(ad + bc, bd) \sim (a'd' + b'c', b'd')$, as desired. ☐

Proof. Suppose for the sake of contradiction that

$$\left[\frac{a}{b}\right] +_{\mathbb{Q}} \left[\frac{c}{d}\right] \neq \left[\frac{a'}{b'}\right] +_{\mathbb{Q}} \left[\frac{c'}{d'}\right] \text{ for some } \left[\frac{a}{b}\right], \left[\frac{c}{d}\right], \left[\frac{a'}{b'}\right], \left[\frac{c'}{d'}\right] \in \mathbb{Q}$$

Since

$$\left[\frac{a}{b}\right] +_{\mathbb{Q}} \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right] \qquad\qquad \left[\frac{a'}{b'}\right] +_{\mathbb{Q}} \left[\frac{c'}{d'}\right] = \left[\frac{a'd' + b'c'}{b'd'}\right]$$

by Definition 2.7, the supposition implies that

$$\left[\frac{ad+bc}{bd}\right] \neq \left[\frac{a'd'+b'c'}{b'd'}\right]$$

By Exercise 2.6, this means that $(ad+bc, bd) \nsim (a'd'+b'c', b'd')$. But since $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$ by hypothesis, the lemma tells us that $(ad+bc, bd) \sim (a'd'+b'c', b'd')$, a contradiction. Therefore,

$$\left[\frac{a}{b}\right] +_{\mathbb{Q}} \left[\frac{c}{d}\right] = \left[\frac{a'}{b'}\right] +_{\mathbb{Q}} \left[\frac{c'}{d'}\right]$$

under the given conditions, as desired. $\square$