Selected Solutions to Exercise Problems

Section 2: Propositional Calculus.

S02E09. Let P xor Q mean "P exclusive or Q." In other words, P xor Q should be true just when exactly one of P and Q is true.

(a) Write out the truth table for P xor Q.

Proof. According to the description given above, the truth table for P xor Q is completed as

P	Q	P xor Q
T	T	F
T	F	T
F	T	T
F	F	F

$\square$

(b) Show by a truth table that P xor Q is logically equivalent to $(P \wedge \neg Q) \vee (Q \wedge \neg P)$.

Proof. Below is the truth table for $(P \wedge \neg Q) \vee (Q \wedge \neg P)$

P	Q	$P \wedge \neg Q$	$Q \wedge \neg P$	$(P \wedge \neg Q) \vee (Q \wedge \neg P)$
T	T	F	F	F
T	F	T	F	T
F	T	F	T	T
F	F	F	F	F

Note that the last column of this truth table headed by $(P \wedge \neg Q) \vee (Q \wedge \neg P)$ is identical to the last column of the previous truth table headed by P xor Q. Hence, P xor Q is logically equivalent to $(P \wedge \neg Q) \vee (Q \wedge \neg P)$. $\square$

(c) Show by truth tables that the following four sentences are logically equivalent:

$$P \text{ xor } Q,\ \neg(P \Leftrightarrow Q),\ (\neg P) \Leftrightarrow Q,\ P \Leftrightarrow (\neg Q).$$

Proof. Below is the truth table for $\neg(P \Leftrightarrow Q), (\neg P) \Leftrightarrow Q, P \Leftrightarrow (\neg Q)$. Intermediate columns are omitted.

P	Q	$\neg(P \Leftrightarrow Q)$	$(\neg P) \Leftrightarrow Q$	$P \Leftrightarrow (\neg Q)$
T	T	F	F	F
T	F	T	T	T
F	T	T	T	T
F	F	F	F	F

Each of the last three columns is identical to the last column of the truth table from part (a). Thus the four sentences in the headers of these columns are logically equivalent. □

(d) Show by a truth table that $(\neg P) \Leftrightarrow (\neg Q)$ is logically equivalent to $P \Leftrightarrow Q$.

S02E15. Use the method of conditional proof to explain in words why the sentence

$$\{(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow S)]\} \Rightarrow (R \vee S)$$

is a tautology. Be explicit about discharging assumptions.

Proof.

A1: Suppose $(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow S)]$ is true.
(We wish to show that $R \vee S$ is true.)
Then both of $P \vee Q$ and $(P \Rightarrow R) \wedge (Q \Rightarrow S)$ are true.
Since $P \vee Q$ is true, at least one of P and Q is true.

Case 1. Suppose P is true.
Since $(P \Rightarrow R) \wedge (Q \Rightarrow S)$ is true, $P \Rightarrow R$ is true.
Thus $P \Rightarrow R$ is true and P is true.
Hence, by modus ponens, R is true.

Case 2. Suppose Q is true.
Since $(P \Rightarrow R) \wedge (Q \Rightarrow S)$ is true, $Q \Rightarrow S$ is true.
Thus $Q \Rightarrow S$ is true and Q is true.
Hence, by modus ponens, S is true.

Thus in either case, R is true or S is true.
We have shown that $R \vee S$ is true under the assumption A1 that $(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow S)]$ is true.

Discharging A1, we see that $\{(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow S)]\} \Rightarrow (R \vee S)$ is true under no assumptions, so it is a tautology. □

S02E17. Use the method of conditional proof to explain in words why the sentence

$$(P \Rightarrow Q) \Rightarrow \{[P \Rightarrow (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)\}$$

is a tautology. Be explicit about discharging assumptions.

Proof.

A1: Suppose $A_1 : P \Rightarrow Q$ is true. (We wish to show that $C_1 : [P \Rightarrow (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ is true.)

A2: Suppose $A_2 : P \Rightarrow (Q \Rightarrow R)$ is true. (We wish to show that $C_2 : P \Rightarrow R$ is true.)

A3: Suppose $A_3 : P$ is true. (We wish to show that $C_3 : R$ is true.)
From A1 and A3, we see that Q is true, by modus ponens.
From A2 and A3, we see that $Q \Rightarrow R$ is true, by modus ponens.
From this and the fact that Q is true, we see that R is true, by modus ponens.
We have shown that C_3 is true under A1, A2, and A3.

Discharging A3, we see that $C_2 : A_3 \Rightarrow C_3$ is true under A1 and A2.

Discharging A2, we see that $C_1 : A_2 \Rightarrow C_2$ is true under A1 alone.

Finally, discharging A1, we see that $A_1 \Rightarrow C_1$ is true under no assumptions, so it is a tautology. □

Section 3: Quantifiers.

S03E07. Let P be the sentence

$$(\exists x \in \mathbb{R})(x \geqslant 0 \text{ and } \sqrt{x+2} < \sqrt{x} + \sqrt{2}).$$

(a) Use one of the generalized De Morgan's laws to show that $\neg P$ is logically equivalent to

$$(\forall x \in \mathbb{R})(x < 0 \text{ or } \sqrt{x+2} \geqslant \sqrt{x} + \sqrt{2}).$$

Proof.

$$\begin{aligned}
&\neg(\exists x \in \mathbb{R})(x \geqslant 0 \text{ and } \sqrt{x+2} < \sqrt{x} + \sqrt{2}) && \\
\text{iff} \quad &(\forall x \in \mathbb{R})\neg(x \geqslant 0 \text{ and } \sqrt{x+2} < \sqrt{x} + \sqrt{2}) && \text{(by a generalized De Morgan's law)} \\
\text{iff} \quad &(\forall x \in \mathbb{R})(x < 0 \text{ or } \sqrt{x+2} \geqslant \sqrt{x} + \sqrt{2}) && \text{(by a De Morgan's law)}
\end{aligned}$$

□

(b) The sentence $P : (\exists x \in \mathbb{R})(x \geqslant 0 \text{ and } \sqrt{x+2} < \sqrt{x} + \sqrt{2})$ is true because $2 \geqslant 0$ and $\sqrt{2+2} = \sqrt{4} = 2 < \sqrt{2} + \sqrt{2}$. □

S03E10. For each of the following sentences, write out what it means in words, state whether it is true or false, and prove your statement.

(a) $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(x + y = x)$ means "There exists a real number y such that for each real number x, $x + y = x$." We claim that this sentence is true.

Proof. It suffices to exhibit a value of y such that the universal sentence $(\forall x \in \mathbb{R})(x + y = x)$ is true. We claim that 0 is such a value of y. To see this, let x_0 be any real number. Then $\mathrm{x}_0 + 0 = \mathrm{x}_0$. Now x_0 is an arbitrary element of $\mathbb{R}$. Hence $(\forall x \in \mathbb{R})(x + y = x)$ is true. This proves the claim. Therefore $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(x + y = x)$ is true. □

(b) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = x)$ means "For each real number x, there exists a real number y such that, $x + y = x$." We claim that this sentence is true.

Proof. Let x_0 be any real number. Then $x_0 + 0 = x_0$. Hence $(\exists y \in \mathbb{R})(x_0 + y = x_0)$ is true, because 0 is such a value of y. Now x_0 is an arbitrary element of $\mathbb{R}$. Therefore $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = x)$ is true. □

(e) $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(xy = 1)$ means "There exists a real number y such that for each real number x, $xy = 1$." We claim that this sentence is false.

Proof. Suppose it is true. Then we can pick $y_0 \in \mathbb{R}$ such that $(\forall x \in \mathbb{R})(xy_0 = 1)$. But then in particular, $0 \cdot y_0 = 1$, so $0 = 1$. But $0 \neq 1$. This is a contradiction. Hence $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(xy = 1)$ must be false. □

(f) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 1)$ means "For each real number x, there exists a real number y such that $xy = 1$." We claim that this sentence is false.

Proof. Suppose it is true. Then in particular, since 0 is a real number, $(\exists y \in \mathbb{R})(0 \cdot y = 1)$ is true, so we can pick $y_0 \in \mathbb{R}$ such that $0 \cdot y_0 = 1$, so $0 = 1$. But $0 \neq 1$. This is a contradiction. Hence $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 1)$ is false. □

S03E11. Let S be a subset of $\mathbb{R}$.

(a) Let S be the set of all real numbers. We claim that this S is not bounded above. By Example 3.15, S *is not bounded above* if and only if $(\forall b \in \mathbb{R})(\exists x \in S)(x > b)$, which we use in the proof below.

Proof. Let $b_0 \in \mathbb{R}$ be arbitrary. Since $b_0 + 1 \in \mathbb{R}$ and $b_0 + 1 > b_0$, it is an example value of x for which $(\exists x \in S)(x > b)$. Since b_0 is arbitrary, it follows that $(\forall b \in \mathbb{R})(\exists x \in S)(x > b)$. Therefore S is not bounded above. □

(b) Let S be the set of all numbers x such that some person on earth has x hairs on his or her head. We claim that this S is bounded above. Recall that S *is bounded above* if and only if $(\exists b \in \mathbb{R})(\forall x \in S)(x \leqslant b)$, which we use in the proof below.

Proof. S is a finite set because there are finitely many people on earth. So S has a maximal element; call it m. Then, for any $x_0 \in S$, $x_0 \leqslant m$. Thus $(\forall x \in S)(x \leqslant m)$ because x_0 is arbitrary. Hence $(\exists b \in \mathbb{R})(\forall x \in S)(x \leqslant b)$ because m is an example value of b. Therefore S is bounded above. □

S03E14. For each of the following sentences, write out what it means in words, state whether it is true or false, and prove your statement.

(c) $(\exists! x \in \mathbb{Z})(x^2 - 4x + 3 < 0)$ means "There exists a unique integer x such that $x^2 - 4x + 3$ is less than 0." We claim that this sentence is true.

Proof. 2 is an integer and $2^2 - 4 \cdot 2 + 3 = -1 < 0$. Now suppose x is another integer such that $x^2 - 4x + 3 < 0$. (We wish to show that $x = 2$.) By completing the square, $x^2 - 4x + 3 = (x - 2)^2 - 1 \geqslant -1$. Thus $-1 \leqslant (x - 2)^2 - 1 < 0$. Since x is an integer, $(x - 2)^2 - 1$ is an integer, thus it must be the case that $(x - 2)^2 - 1 = -1$. It follows that $(x - 2)^2 = 0$, so $x - 2 = 0$, so $x = 2$. □

(e) $(\exists! x \in \mathbb{R})(x^2 - 4x + 5 = 0)$ means "There exists a unique real number x such that $x^2 - 4x + 5$ is 0." We claim that this sentence is false.

Proof. To disprove $(\exists! x \in \mathbb{R})(x^2 - 4x + 5 = 0)$, we will show that $(\exists x \in \mathbb{R})(x^2 - 4x + 5 = 0)$ is false. Assume $(\exists x \in \mathbb{R})(x^2 - 4x + 5 = 0)$ is true. Then in particular, we can pick a real number x_0 such that $x_0^2 - 4x_0 + 5 = 0$. But $x_0^2 - 4x_0 + 5 = (x_0 - 2)^2 + 1 \geqslant 1$. So $x_0^2 - 4x_0 + 5 \neq 0$. This is a contradiction. So $(\exists x \in \mathbb{R})(x^2 - 4x + 5 = 0)$ is false, and it follows that $(\exists! x \in \mathbb{R})(x^2 - 4x + 5 = 0)$ is false. □

(i) $(\forall x \in \mathbb{R})(\exists! y \in \mathbb{R})(xy = 0)$ means "For each real number x, there exists a unique real number y such that xy is 0." We claim that this sentence is false.

Proof. Suppose $(\forall x \in \mathbb{R})(\exists! y \in \mathbb{R})(xy = 0)$ is true. Then in particular, since 0 is a real number, $(\exists! y \in \mathbb{R})(0 \cdot y = 0)$ is true. But 1 and -1 are two different real values of y for which $0 \cdot y = 0$. So $(\exists! y \in \mathbb{R})(0 \cdot y = 0)$ is false. This is a contradiction. Therefore $(\forall x \in \mathbb{R})(\exists! y \in \mathbb{R})(xy = 0)$ is false. □

(j) $(\forall x \in \mathbb{R})[\text{ if } x \neq 0, \text{ then } (\exists! y \in \mathbb{R})(xy = 0)]$ means "For each real number x, if x is nonzero, then there exists a unique real number y such that xy is 0." We claim that this sentence is true.

Proof. Let $x \in \mathbb{R}$ be arbitrary. Assume that $x \neq 0$. (Here we are proceeding by way of conditional proof. We wish to show that $(\exists! y \in \mathbb{R})(xy = 0)$ is true.) Note that 0 is a real number, $x \cdot 0 = 0$, and if y is another real number such that $xy = 0$, then $y = 0$ because $x \neq 0$. This shows that $(\exists! y \in \mathbb{R})(xy = 0)$ is true. Since x is arbitrary, we conclude that $(\forall x \in \mathbb{R})[\text{ if } x \neq 0, \text{ then } (\exists! y \in \mathbb{R})(xy = 0)]$ is true. □

Section 4: First Examples of Mathematical Proofs.

S04E03. Let x be an integer. Prove that $x(x+1)$ is even.

Proof. Since x is an integer, x is even or x is odd.

Case 1. Suppose x is even. Then we can pick an integer k such that $x = 2k$. Then $x(x+1) = 2k(2k+1) = 2[k(2k+1)]$. Since $k(2k+1)$ is an integer, it follows that $x(x+1)$ is even.

Case 2. Suppose x is odd. Then we can pick an integer k such that $x = 2k$. Then $x(x+1) = (2k+1)((2k+1)+1) = (2k+1)(2k+2) = 2[(2k+1)(k+1)]$. Since $(2k+1)(k+1)$ is an integer, it follows that $x(x+1)$ is even.

Thus in either case, $x(x+1)$ is even. □

S04E04.

(a) The sentence "For each real number x, if x is an even number, then x is not an odd number." is true.

Proof. Let $x \in \mathbb{R}$ be arbitrary. Suppose that x is even. We wish to show that x is not odd. Suppose x is odd. Then x is both even and odd. But, by (a) of Remark 4.12, x is not both even and odd. Thus we have reached a contradiction. Thus it must be that x is not odd. Since x is arbitrary, it follows that for each $x \in \mathbb{R}$, if x is even, then x is not odd. □

(b) The sentence "For each real number x, if x is not an odd number, then x is an even number." is false.

Proof. Suppose it is true. Then in particular, $1/2$ is a real number and $1/2$ is not odd, so $1/2$ is even. Then we can find $k \in \mathbb{Z}$ such that $1/2 = 2k$, so $1 = 2(2k)$. Thus 1 is even. But $1 = 2 \cdot 0 + 1$, so 1 is odd. So 1 is both even and odd. But since 1 is an integer, by (a) of Remark 4.12, 1 is not both even and odd. This is a contradiction. Therefore, the sentence must be false. □

In the proof above, we used the number $1/2$ is not odd without proving it. Though obvious, let's prove it here.

Claim 1. *The number* $1/2$ *is not an odd number.*

Proof. Suppose $1/2$ is odd. Then we can pick $k \in \mathbb{Z}$ such that $1/2 = 2k+1$, so $1 = 2(2k+1)$. Thus 1 is even. But $1 = 2 \cdot 0 + 1$, so 1 is odd. Since 1 is an integer, by part (c) of Remark 4.12, 1 is not even. This is a contradiction. So $1/2$ is not even. □

S04E08. Let u, v, and w be rational numbers.

(a) $-v$ is a rational number.

Proof. Since v is a rational number, we can pick $a, b \in \mathbb{Z}$ such that $b \neq 0$ and $v = a/b$. Then $-v = -(a/b) = (-a)/b$. Since $-a$ is an integer and b is an integer that is not zero, $-v$ is a rational number. □

(b) $u - v$ is a rational number.

Proof. (Using definition) Since u and v are rational numbers, we can pick $a, b, c, d \in \mathbb{Z}$ such that $b, d \neq 0$ and $u = a/b$ and $v = c/d$. Then

$$u - v = \frac{a}{b} - \frac{c}{d} = \frac{ad}{bd} - \frac{bc}{bd} = \frac{ad - bc}{bd}.$$

Since $ad - bc$ is an integer and bd is an integer that is not zero as a product of two nonzero integers, $u - v$ is a rational number. □

Proof. (Using other results) By part (a), since v is a rational number, $-v$ is a rational number. By Example 4.21, since u and $-v$ are both rational numbers, $u + (-v) = u - v$ is a rational number. □

(d) If $w \neq 0$, then $1/w$ is a rational number.

Proof. Let $w \neq 0$ be a rational number. Then we can pick $a, b \in \mathbb{Z}$ such that $a, b \neq 0$ and $w = a/b$. (Note that $a \neq 0$ because $w \neq 0$.) Then $1/w = 1/(a/b) = b/a$. Since $a, b \in \mathbb{Z}$ and $a \neq 0$, it follows that $1/w$ is a rational number. □

S04E10. Let x be a rational number and let y be an irrational number.

(a) $-y$ is irrational.

Proof. Since y is irrational, y is real and y is not rational. Since y is real, $-y$ is also real. It remains to show that $-y$ is not rational. Suppoe that $-y$ is rational. Then by Exercise 8(a), $-(-y) = y$ is rational. So y is not rational and y is rational. This is a contradiction. Thus $-y$ is not rational. Hence $-y$ is irrational. □

(b) $x - y$ is irrational.

Proof. Since x is rational and y is irrational, both x and y are real, so $x - y$ is real. It remains to show that $x - y$ is not rational. Suppose that $x - y$ is rational. Then $x - (x - y) = y$ is rational, because the difference of two rational numbers is rational; see Exercise 8(b). But y is not rational because y is irrational. This is a contradiction. Thus $x - y$ is not rational. Therefore $x - y$ is irrational. □

(d) If $x \neq 0$, then xy is irrational.

Proof. Assume that $x \neq 0$. (We wish to show that xy is irrational.) Since x is rational and y is irrational, both x and y are real, so xy is real. It remains to show that xy is not rational. Suppose xy is rational. Then by Exercise 8(e), $(xy)/x = y$ is rational. (Note that Exercise 8(b) is applicable since both x and xy are rational and $x \neq 0$.) But y is not rational because y is irrational. This is a contradiction. Thus xy is not rational. Therefore xy is irrational. □

S04E12. For each $x \in \mathbb{R}$, $\pi + x$ is irrational or $\pi - x$ is irrational.

Proof. Let $x \in \mathbb{R}$. Then both of $\pi + x$ and $\pi - x$ are real. It remains to show that $\pi + x$ is not rational or $\pi - x$ is not rational. Assume, by way of contradiction, that $\pi + x$ is rational and $\pi - x$ is rational. Since the sum of two rational numbers is a rational number, $(\pi + x) + (\pi - x) = 2\pi$ is a rational number. Since the quotient of rational numbers (with nonzero denominator) is a rational number, $(2\pi)/2 = \pi$ is a rational number. But since π is an irrational number, π is not a rational number. This is a contradiction. Hence $\pi + x$ is not rational or $\pi - x$ is not rational. □

S04E14. Let $a, b, c \in \mathbb{Z}$.

(b) If a divides b and b divides a, then $b = a$ or $b = -a$.

Proof. Since a divides b, we can pick $k \in \mathbb{Z}$ such that $b = ka$. Since b divides a, we can pick $\ell \in \mathbb{Z}$ such that $a = \ell b$. On substitution, $b = k(\ell b) = (k\ell)b$, so $b - (k\ell)b = b(1 - k\ell) = 0$, so $b = 0$ or $k\ell = 1$.

Case 1. Suppose $b = 0$. Then $a = \ell b = \ell \cdot 0 = 0$, so $b = a$.

Case 2. Suppose $k\ell = 1$. Then $k = \ell = 1$ or $k = \ell = -1$, because $k, \ell \in \mathbb{Z}$. In particular, $k = 1$ or $k = -1$. Since $b = ka$, it follows that $b = a$ or $b = -a$.

Thus in either case, $b = a$ or $b = -a$. □

(c) If a divides b and b divides c, then a divides c.

Proof. Since a divides b and b divides c, we can pick $k, \ell \in \mathbb{Z}$ such that $b = ka$ and $c = \ell b$. But then $c = \ell b = \ell(ka) = (\ell k)a$. Since $\ell k \in \mathbb{Z}$, it follows that a divides c. □

S04E16. Let $n \in \mathbb{N}$. Prove that there exists a prime number q such that $n < q \leqslant 1 + n!$.

Proof. Let $x = 1 + n!$. We claim that none of $2, 3, \ldots, n$ divides x. By way of contradiction, assume that one of $2, 3, \ldots, n$ divides x; call it k. But then k divides $x - 1 = n!$ because $n!$ is the product of $1, 2, \ldots, n$, one of which is k. Thus k divides x and k divides $x - 1$, so k divides $x - (x - 1) = 1$. This is a contradiction because $k \geqslant 2$ because k is one of $2, 3, \ldots, n$ and $k \leqslant 1$ because k divides 1. Hence none of $2, 3, \ldots, n$ divides x. Now $x \in \mathbb{N}$ and $x \neq 1$, so there must exists a prime number q such that q divides x. But since none of $2, 3, \ldots n$ divides x, q is not one of them, and so $q > n$. Since q divides x and q is a prime number, it must be the case that $q \leqslant x$. Therefore $n < q \leqslant x = 1 + n!$. □

S04E17.

(a) Let x be a rational number such that $x^3 = c$, where c is an integer. Prove that x is an integer.

Proof. Since x is rational, we can pick $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that $x = a/b$ and the fraction a/b is in lowest terms. Since $x^3 = c$ and $x = a/b$, we have $(a/b)^3 = c$, so $a^3/b^3 = c$, so $a^3 = cb^3$, so $a^3 = (cb^2)b$. Since cb^2 is an integer, it follows that b divides $a^3 = a \cdot a \cdot a$. Hence by Remark 4.50, we can pick $b_1, b_2, b_3 \in \mathbb{N}$ such that $b_1 \mid a$, $b_2 \mid a$, $b_3 \mid a$, and $b = b_1 b_2 b_3$. Then b_1 divides both a and b. But since a/b is in lowest terms, it must be the case that $b_1 = 1$. Similarly, $b_2 = b_3 = 1$. Hence $b = b_1 b_2 b_3 = 1 \cdot 1 \cdot 1 = 1$. But then $x = a/b = a/1 = a$, so x is an integer, because a is an integer. □

(b) Let c be an integer which is not a perfect cube. Prove that $\sqrt[3]{c}$ is irrational.

Proof. Since c is an integer, $\sqrt[3]{c}$ is real. So it remains to show that $\sqrt[3]{c}$ is not rational. Suppose $\sqrt[3]{c}$ is rational. Let $x = \sqrt[3]{c}$. Then $x^3 = c$. But by part (a), since x is rational and c is an integer, x is an integer. But since c is not a perfect cube, there is no integer whose cube is c. In particular, $x^3 \neq c$. We have reached a contradiction. Therefore $\sqrt[3]{c}$ is not rational. □

S04E18. Let $x \in \mathbb{R}$ such that $x^3 = rx^2 + sx + t$, where $r, s, t \in \mathbb{Z}$.

(a) Prove that if x is rational, then x is an integer.

Proof. Since x is rational, we can pick $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that $x = a/b$ and the fraction a/b is in lowest terms. Since $x^3 = rx^2 + sx + t$ and $x = a/b$, we have

$$
\begin{aligned}
&\left(\frac{a}{b}\right)^3 = r\left(\frac{a}{b}\right)^2 + s\frac{a}{b} + t \\
\text{iff}\quad &\frac{a^3}{b^3} = r\frac{a^2}{b^2} + s\frac{a}{b} + t \\
\text{iff}\quad &\frac{a^3}{b^3} = r\frac{a^2b}{b^3} + s\frac{ab^2}{b^3} + t\frac{b^3}{b^3} \\
\text{iff}\quad &\frac{a^3}{b^3} = \frac{ra^2b + sab^2 + tb^3}{b^3} \\
\text{iff}\quad &a^3 = ra^2b + sab^2 + tb^3 \qquad \text{(since } b^3 \neq 0) \\
\text{iff}\quad &a^3 = (ra^2 + sab + tb^2)b.
\end{aligned}
$$

Since $ra^2 + sab + tb^2$ is an integer, it follows that b divides $a^3 = a \cdot a \cdot a$. Hence by Remark 4.50, we can pick $b_1, b_2, b_3 \in \mathbb{N}$ such that $b_1 \mid a$, $b_2 \mid a$, $b_3 \mid a$, and $b = b_1b_2b_3$. Then b_1 divides both a and b. But since a/b is in lowest terms, it must be the case that $b_1 = 1$. Similarly, $b_2 = b_3 = 1$. Hence $b = b_1b_2b_3 = 1 \cdot 1 \cdot 1 = 1$. But then $x = a/b = a/1 = a$, so x is an integer, because a is an integer. ☐

(b) Prove that if x is not an integer, then x is irrational.

Proof. Suppose that x is not an integer. Since x is a real number, it remains to show that x is not rational. Assume by way of contradiction that x is rational. But then by part (a), x is an integer. This is a contradiction. Therefore, x is not rational. ☐

Note. This is the contrapositive of the previous part.

S04E25. Let $m \in \mathbb{Z}$. Show that:

(a) For each $a \in \mathbb{Z}$, we have $a \equiv a \mod m$. (*Reflexivity.*)

Proof. Omitted as was done in class. ☐

(b) For all $a, b \in \mathbb{Z}$, if $a \equiv b \mod m$, then $b \equiv a \mod m$. (*Symmetry.*)

Proof. Let $a, b \in \mathbb{Z}$ such that $a \equiv b \mod m$. Then m divides $b - a$, so we can pick $k \in \mathbb{Z}$ such that $b - a = km$. But then $a - b = -(b - a) = -km = (-k)m$. Since $-k$ is also an integer, it follows that m divides $a - b$. Hence, $b \equiv a \mod m$. ☐

(c) For all $a, b, c \in \mathbb{Z}$, if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$. (*Transitivity.*)

Proof. Let $a, b, c \in \mathbb{Z}$ such that $a \equiv b \mod m$ and $b \equiv c \mod m$. Then m divides $b - a$ and m divides $c - a$, so we can pick $k, \ell \in \mathbb{Z}$ such that $b - a = km$ and $c - b = \ell m$. But then

$$c - a = (c - b) - (b - a) = \ell m - km = (\ell - k)m.$$

Since $\ell - k$ is also an integer, it follows that m divides $c - a$. Hence, $a \equiv c \mod m$. ☐

S04E26. Let $m, a_1, b_1, a_2, b_2 \in \mathbb{Z}$. Suppose that $a_1 \equiv b_1 \mod m$ and $a_2 \equiv b_2 \mod m$. Prove that:

(a) $a_1 + a_2 \equiv b_1 + b_2 \mod m$.

Proof. Omitted as was done in class. □

(b) $a_1 a_2 \equiv b_1 b_2 \mod m$.

Proof. Since $a_1 \equiv b_1 \mod m$ and $a_2 \equiv b_2 \mod m$, m divides $b_1 - a_1$ and m divides $b_2 - a_2$, so we can pick $k, \ell \in \mathbb{Z}$ such that $b_1 - a_1 = km$ and $b_2 - a_2 = \ell m$, so

$$b_1 = a_1 + km \quad \text{and} \quad b_2 = a_2 + \ell m.$$

But then

$$b_1 b_2 = (a_1 + km)(a_2 + \ell m) = a_1 a_2 + a_1 \ell m + a_2 km + k\ell m^2 = a_1 a_2 + (a_1 \ell + a_2 k + k\ell m)m,$$

so

$$b_1 b_2 - a_1 a_2 = (a_1 \ell + a_2 k + k\ell m)m.$$

Since $a_1 \ell + a_2 k + k\ell m \in \mathbb{Z}$, it follows that m divides $b_1 b_2 - a_1 a_2$. Therefore, $a_1 a_2 \equiv b_1 b_2 \mod m$. □

Section 5: Induction.

Example 1. Prove by induction that for each $n \in \mathbb{N}$,

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

Proof. Let $P(n)$ be the sentence

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

BASE CASE: Note that $P(1)$ is true, because if $n = 1$, then $1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/[n \cdot (n+1)]$ is really just $1/[1 \cdot (1+1)] = 1/2$, and $n/(n+1) = 1/(1+1) = 1/2$.

INDUCTIVE STEP: Let $n \in \mathbb{N}$ such that $P(n)$ is true. Then

$$\begin{aligned}
\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)} + \frac{1}{(n+1)(n+2)} & \\
&= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} && \text{(by the inductive hypothesis)} \\
&= \frac{n(n+2)}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n(n+2)+1}{(n+1)(n+2)} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{n+1}{n+2} = \frac{n+1}{(n+1)+1}.
\end{aligned}$$

Thus $P(n+1)$ is true.

CONCLUSION: Therefore, by induction, for each $n \in \mathbb{N}$, $P(n)$ is true. In other words, for each $n \in \mathbb{N}$, $1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/[n \cdot (n+1)] = n/(n+1)$. ☐

Example 2. Prove by induction that for each $n \in \mathbb{N}$, 5 divides $8^n - 3^n$.

Proof. Let $P(n)$ be the sentence

$$5 \text{ divides } 8^n - 3^n.$$

BASE CASE: Note that $P(1)$ is true, because $8^1 - 3^1 = 7 - 2 = 5$ and 5 clearly divides 5.

INDUCTIVE STEP: Now let $n \in \mathbb{N}$ such that $P(n)$ is true. Notice that $8^{n+1} - 3^{n+1} = (8)(8^n) - (3)(3^n) = (5+3)(8^n) - (3)(3^n) = (5)(8^n) + (3)(8^n - 3^n)$. Now obviously 5 divides $(5)(8^n)$ and by the inductive hypothesis, 5 divides $3(8^n - 3^n)$. Hence 5 divides $(5)(8^n) + (3)(8^n - 3^n)$, that is, 5 divides $8^{n+1} - 3^{n+1}$. Thus $P(n+1)$ is true as well.

CONCLUSION: Therefore, by induction, for each $n \in \mathbb{N}$, $P(n)$ is true. In other words, for each $n \in \mathbb{N}$, 5 divides $8^n - 3^n$. ☐

Example 3. Prove that for each $x \in \mathbb{Z}$, 6 divides $x^3 + 5x$.

Proof. Let $P(x)$ be the sentence

$$6 \text{ divides } x^3 + 5x.$$

Consider any $x \in \mathbb{Z}$. Then $x \geqslant 0$ or $x \leqslant -1$, so we shall prove that $(\forall x \in \mathbb{Z})P(x)$ is true in two parts.

PART 1. We shall prove by induction that for each $x \in \boldsymbol{\omega}$, $P(x)$ is true.

BASE CASE: Note that $P(0)$ is true, because 6 divides $0^3 + 5 \cdot 0 = 0$.

INDUCTIVE STEP: Let $x \in \boldsymbol{\omega}$ such that $P(x)$ is true. Then

$$\begin{aligned}(x+1)^3 + 5(x+1) &= (x^3 + 3x^2 + 3x + 1) + (5x + 5) \\ &= (x^3 + 5x) + (3x^2 + 3x) + 6 \\ &= (x^3 + 5x) + 3x(x+1) + 6.\end{aligned}$$

By the inductive hypothesis, 6 divides $x^3 + 5x$. Since $x(x+1)$ is an even (see S04E03), we can pick $k \in \mathbb{Z}$ such that $x(x+1) = 2k$, so $3x(x+1) = 3(2k) = 6k$, so 6 divides $3x(x+1)$. Lastly, 6 divides 6. It follows that 6 divides $(x^3 + 5x) + 3x(x+1) + 6$. Thus $P(x+1)$ is true as well.

CONCLUSION: Therefore, by induction, for each $x \in \boldsymbol{\omega}$, $P(x)$ is true.

PART 2. We shall prove that for each integer $x \leqslant -1$, $P(x)$ is true.

Suppose $x \leqslant -1$ be an integer. Then $-x \in \boldsymbol{\omega}$, so $P(-x)$ is true by part 1. In other words, 6 divides $(-x)^3 + 5(-x)$. Now $(-x)^3 + 5(-x) = -x^3 - 5x = -(x^3 + 5x)$, so we can pick $k \in \mathbb{Z}$ such that $-(x^3 + 5x) = 6k$, so $x^3 + 5x = -6k = 6(-k)$, so 6 divides $x^3 + 5x$ because $-k$ is also an integer. Thus $P(x)$ is true for any integer $x \leqslant -1$.

CONCLUSION. Therefore, by parts 1 and 2, for each $x \in \mathbb{Z}$, 6 divides $x^3 + 5x$. $\square$

S05E05. Prove by induction that for each $n \in \mathbb{N}$, 5 divides $7^n - 2^n$.

Proof. Let $P(n)$ be the sentence

$$5 \text{ divides } 7^n - 2^n.$$

BASE CASE: Note that $P(1)$ is true, because $7^1 - 2^1 = 7 - 2 = 5$ and 5 clearly divides 5.

INDUCTIVE STEP: Now let $n \in \mathbb{N}$ such that $P(n)$ is true. Notice that $7^{n+1} - 4^{n+1} = (7)(7^n) - (2)(2^n) = (5+2)(7^n) - (2)(2^n) = (5)(7^n) + (2)(7^n - 2^n)$. Now obviously 5 divides $(5)(7^n)$ and by the inductive hypothesis, 5 divides $2(7^n - 2^n)$. Hence 5 divides $(5)(7^n) + (2)(7^n - 2^n)$, that is, 5 divides $7^{n+1} - 2^{n+1}$. Thus $P(n+1)$ is true as well.

CONCLUSION: Therefore, by induction, for each $n \in \mathbb{N}$, $P(n)$ is true. In other words, for each $n \in \mathbb{N}$, 5 divides $7^n - 2^n$. $\square$

S05E11. (*The binomial theorem.*) Let $a, b \in \mathbb{R}$. Prove by induction that for each $n \in \boldsymbol{\omega}$,

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

Proof. Let $P(n)$ be the sentence

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

<u>BASE CASE</u>: Note that $P(0)$ is true. This is so because if $n = 0$, then $(a+b)^n = (a+b)^0 = 1$, and $\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ is really just $\binom{0}{0} a^{0-0} b^0$, which is equal to 1.

<u>INDUCTIVE STEP</u>: Now let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. Then

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b) = (a+b)^n a + (a+b)^n b \\
&= \left[\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k\right] a + \left[\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k\right] b \qquad \text{(by induction hypothesis)} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} \\
&= \binom{n}{0} a^{n+1} b^0 + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} b^k \\
&\qquad + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} + \binom{n}{n} a^0 b^{n+1} \\
&= \binom{n}{0} a^{n+1} b^0 + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} b^k \\
&\qquad + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1} b^k + \binom{n}{n} a^0 b^{n+1} && (1) \\
&= \binom{n+1}{0} a^{n+1} b^0 + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1}\right] a^{(n+1)-k} b^k + \binom{n+1}{n+1} a^0 b^{n+1} && (2) \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{(n+1)-k} b^k, && (3)
\end{aligned}$$

where (1) is by changing indices of the second sum, (2) is by $\binom{n}{0} = 1 = \binom{n+1}{0}$ and $\binom{n}{n} = 1 = \binom{n+1}{n+1}$, and (3) is by the recurrence relation. Thus $P(n+1)$ is true as well.

<u>CONCLUSION</u>: Therefore, by induction, for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. $\square$

Section 6: Insight versus Induction.

S06E02. Use a suitable telescoping sum to give a proof without explicit induction that for each $n \in \mathbb{N}$,

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

Solution. Let $n \in \mathbb{N}$ and let $T(n) = \sum_{k=1}^{n} [k^4 - (k-1)^4]$. On the one hand, note that $T(n)$ is a telescoping sum such that

$$T(n) = [1^4 - 0^4] + [2^4 - 1^4] + [3^4 - 2^4] + \cdots + [(n-1)^4 - (n-2)^4] + [n^4 - (n-1)^4] = n^4.$$

On the other hand, since

$$k^4 - (k-1)^4 = k^4 - (k^4 - 4k^3 + 6k^2 - 4k + 1) = 4k^3 - 6k^2 + 4k - 1,$$

we see that

$$\begin{aligned} T(n) &= \sum_{k=1}^{n} (4k^3 - 6k^2 + 4k - 1) \\ &= 4\sum_{k=1}^{n} k^3 - 6\sum_{k=1}^{n} k^2 + 4\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 \\ &= 4S_3(n) - 6S_2(n) + 4S_1(n) - S_0(n). \end{aligned}$$

Hence $n^4 = 4S_3(n) - 6S_2(n) + 4S_1(n) - S_0(n)$, so

$$S_3(n) = \frac{1}{4}\left(n^4 + 6S_2(n) - 4S_1(n) + S_0(n)\right).$$

Since we know that $S_0(n) = n$, $S_1(n) = [n(n+1)]/2$, and $S_2(n) = [n(n+1)(2n+1)]/6$, we obtain

$$\begin{aligned} S_3(n) &= \frac{1}{4}\left(n^4 + 6\frac{n(n+1)(2n+1)}{6} - 4\frac{n(n+1)}{2} + n\right) \\ &= \frac{1}{4}\left(n^4 + n(n+1)(2n+1) - 2n(n+1) + n\right) \\ &= \frac{n^4 + n[(n+1)(2n+1) - 2(n+1) + 1]}{4} \\ &= \frac{n^4 + n(2n^2 + 3n + 1 - 2n - 2 + 1)}{4} \\ &= \frac{n^4 + n(2n^2 + n)}{4} \\ &= \frac{n^4 + 2n^3 + n^2}{4} \\ &= \frac{n^2(n^2 + 2n + 1)}{4} = \frac{n^2(n+1)^2}{4}. \end{aligned}$$

Section 7: Complete Induction.

Question. Prove that PCMI implies PMI.

Proof. Assume that PCMI is true. Consider any sentence $P(n)$. Suppose we have proved that

(1) $P(1)$ is true.

(2) For each $n \in \mathbb{N}$, if $P(n)$ is true, then $P(n+1)$ is true.

We wish to show that for each $n \in \mathbb{N}$, $P(n)$ is true; we shall do so by complete induction.
BASE CASE: $P(1)$ is true by assumption (1).

INDUCTIVE STEP: Let $n \in \mathbb{N}$ such that $P(1), \ldots, P(n)$ are all true. In particular, $P(n)$ is true, so $P(n+1)$ is true by assumption (2).

CONCLUSION: Therefore, by complete induction, for each $n \in \mathbb{N}$, $P(n)$ is true.
This shows that PMI is true. $\square$

Example 1. (Recursively defined sequenece) Let $a_1 = 2$, $a_2 = 4$, and $a_{n+1} = 7a_n - 10a_{n-1}$ for all $n \geqslant 2$. Conjecture a close formula for a_n and then prove your result.

Example 2. (Recursively defined sequenece) Let $a_1 = 3$, $a_2 = 4$, and $a_{n+1} = (2a_n + a_{n-1})/3$ for all $n \geqslant 2$. Prove that for each $n \in \mathbb{N}$, $3 \leqslant a_n \leqslant 4$.

S07E01. Let $y_1, y_2 \in \mathbb{Z}$.

(a) Without using the theorem on division by a prime, or any of its consequences (such as Remark 4.50) show that if 3 divides y_1y_2, then 3 divides y_1 or 3 divides y_2.

Proof. Suppose 3 divides y_1y_2. We wish to show that 3 divides y_1 or 3 divides y_2. By the division lemma, there exist $q_1, q_2 \in \mathbb{Z}$ and $r_1, r_2 \in \{0, 1, 2\}$ such that $y_1 = 3q_1 + r_1$ and $y_2 = 3q_2 + r_2$. Then $r_1 = y_1 - 3q_1$ and $r_2 = y_2 - 3q_2$, so

$$\begin{aligned} r_1r_2 &= (y_1 - 3q_1)(y_2 - 3q_2) = y_1y_2 - 3y_1q_2 - 3q_1y_2 + 9q_1q_2 \\ &= y_1y_2 - 3(y_1q_2 - q_1y_2 + 3q_1q_2). \end{aligned}$$

By assumption, 3 divides y_1y_2. Since $y_1q_2 - q_1y_2 + 3q_1q_2$ is an integer, 3 also divides $3(y_1q_2 - q_1y_2 + 3q_1q_2)$. Thus 3 divides the difference $y_1y_2 - 3(y_1q_2 - q_1y_2 + 3q_1q_2)$. In other words, 3 divides r_1r_2. But the possible values for each of r_1 and r_2 are 0, 1, and 2, so the possible values for r_1r_2 are

$$\begin{array}{lll} (0)(0) = 0, & (1)(0) = 0, & (2)(0) = 0, \\ (0)(1) = 0, & (1)(1) = 1, & (2)(1) = 2, \\ (0)(2) = 0, & (1)(2) = 2, & (2)(2) = 4. \end{array}$$

Of these possible values for r_1r_2, only 0 is divisible by 3. Thus r_1r_2 must be 0, so at least one of r_1 and r_2 must be 0. If $r_1 = 0$, then $y_1 = 3q_1 + r_1 = 3q_1$, so 3 divides y_1. If $r_2 = 0$, then $y_2 = 3q_2 + r_2 = 3q_2$, so 3 divides y_2. Thus 3 must divides y_1 or 3 divides y_2. This completes the proof. $\square$

S07E02. Let $S = \{3k + 1 : k \in \boldsymbol{\omega}\}$. In other words, let $S = \{1, 4, 7, 10, \ldots\}$.

(a) Show that S is closed under multiplication. In other words, show that for all $x, y \in S$, we have $xy \in S$.

Proof. Let $x, y \in S$. Then we can pick $k, \ell \in \boldsymbol{\omega}$ such that $x = 3k + 1$ and $y = 3\ell + 1$, so

$$xy = (3k + 1)(3\ell + 1) = 9k\ell + 3k + 3\ell + 1 = 3(3k\ell + k + \ell) + 1.$$

Since $3k\ell + k + ell$ is an integer, it follows that $xy \in S$. $\square$

Section 10: Sets.

S10E04(b,c). Which of the following set notations denote the empty set?

(b) We claim that $B = \{a \in \mathbb{R} : a^2 + 2a + 2 = 0\} = \varnothing$.

Proof. Suppose by way of contradiction that B is not empty. Let a be an element of B. Then $a \in \mathbb{R}$ such that $a^2 + 2a + 2 = 0$. But $a^2 + 2a + 2 = (a^2 + 2a + 1) + 1 = (a + 1)^2 + 1 \geqslant 0 + 1 = 1$, so $a^2 + 2a + 2 \neq 0$. This is a contradiction. Thus B is the empty set. $\square$

(c) We claim that $C = \{n \in \mathbb{N} : n^2 + n + 11 \text{ is not prime}\} \neq \varnothing$.

Proof. The natural number 11 is an element of C, because $11^2 + 11 + 11 = 11(11 + 1 + 1) = (11)(13)$ is not prime. Since C has at least one element, namely 11, C is not the empty set. $\square$

S10E05. Let A be a set such that for each set B, we have $A \subseteq B$. Show that $A = \varnothing$.

Proof. By assumption, for each set B, $A \subseteq B$. In particular, $A \subseteq \varnothing$. But since the empty set is a subset of any set (See Proposition 10.5), $\varnothing \subseteq A$. Therefore, $A = \varnothing$. $\square$

S10E06.

(a) Let $A = \{\varnothing\}$ and $B = \varnothing$. We claim that $A \notin B$ and $A \nsubseteq B$.

Proof. Since $B = \varnothing$, for each x, $x \notin B$. In particular, $A \notin B$. Now to see that $A \nsubseteq B$ by way of contradiction, suppose otherwise. Since $\varnothing \in A$ and $A \subseteq B$, we have $\varnothing \in B$. But since $B = \varnothing$, there is no element in B. In particular $\varnothing \notin B$. This is a contradiction. Therefore, $A \nsubseteq B$. $\square$

(b) Let $A = \varnothing$ and $B = \{\varnothing\}$. We claim that $A \in B$ and $A \subseteq B$.

Proof. Since $\varnothing \in B$, $A \in B$. By Proposition 10.5, the empty set is a subset of any set. In particular, $A \subseteq B$. $\square$

S10E07. Let $A = \{1, \{4, 7\}, 9\}$ and $B = \{\{1, 4\}, 7, 9\}$. Then

$$\begin{aligned} A \cup B &= \{1, \{1, 4\}, \{4, 7\}, 7, 9\}, \\ A \cap B &= \{9\}, \\ A \setminus B &= \{1, \{4, 7\}\}, \\ B \setminus A &= \{\{1, 4\}, 7\}. \end{aligned}$$

S10E08. Let A and B be sets. Show that $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

Proof. Let $x \in A \cap B$. Then $x \in A$ and $x \in B$. In particular, $x \in A$. Thus $A \cap B \subseteq A$. Similarly, $A \cap B \subseteq B$. $\square$

S10E09. Let A, B, and C be sets. Suppose $C \subseteq A$ and $C \subseteq B$. Show that $C \subseteq A \cap B$.

Proof. Let $x \in C$. Since $C \subseteq A$ and $C \subseteq B$, $x \in A$ and $x \in B$. Thus $x \in A \cap B$. Hence $C \subseteq A \cap B$. $\square$

S10E10. Let A and B be sets. Show that $A \subseteq B$ iff $A \cap B = A$.

Proof. Suppose $A \subseteq B$. We wish to show that $A \cap B = A$. We know, by S10E08, that $A \cap B \subseteq A$. Next, $A \subseteq A$ by the reflexivity of the set inclusion and $A \subseteq B$ by assumption. Thus, by S10E09, $A \subseteq A \cap B$. Thus $A \cap B \subseteq A$ and $A \subseteq A \cap B$, so $A \cap B = A$.

Conversely, suppose $A \cap B = A$. Now by S10E08, we have $A \cap B \subseteq B$. Since $A \cap B \subseteq B$ and $A \cap B = A$, it follows that $A \subseteq B$. □

S10E12. Let A and B be sets and let x be any object. Show that

$$x \notin A \cap B \text{ iff } x \notin A \text{ or } x \notin B.$$

Proof. We have

$$\begin{aligned}
& x \notin A \cap B \\
\text{iff } & \neg(x \in A \cap B) \\
\text{iff } & \neg(x \in A \wedge x \in B) \\
\text{iff } & \neg(x \in A) \vee \neg(x \in B) && \text{(by a De Morgan's law from propositional calculus)} \\
\text{iff } & x \notin A \vee x \notin B
\end{aligned}$$

This completes the proof. □

S10E13. Let A and B be sets and let x be any object. Show that

$$x \notin A \setminus B \text{ iff } x \notin A \text{ or } x \in B.$$

Proof. We have

$$\begin{aligned}
& x \notin A \setminus B \\
\text{iff } & \neg(x \in A \setminus B) \\
\text{iff } & \neg(x \in A \wedge x \notin B) \\
\text{iff } & \neg(x \in A) \vee \neg(x \notin B) && \text{(by a De Morgan's law from propositional calculus)} \\
\text{iff } & x \notin A \vee x \in B.
\end{aligned}$$

This shows the desired equivalence. □

S10E14. (De Morgan's Laws for Sets.) Let S, A, and B be sets. Show that

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

Proof. For each object x, we have

$$\begin{aligned}
& x \in S \setminus (A \cap B) \\
\text{iff } & x \in S \wedge x \notin A \cap B \\
\text{iff } & x \in S \wedge (x \notin A or x \notin B) && \text{(by Proposition 10.18(b))} \\
\text{iff } & (x \in S \wedge x \notin A) \vee (x \in S \wedge x \notin B) && \text{(by a distrubutive law for propositional calculus)} \\
\text{iff } & x \in S \setminus A \vee x \in S \setminus B \\
\text{iff } & x \in (S \setminus A) \cup (S \setminus B).
\end{aligned}$$

Thus the set $S \setminus (A \cap B)$ has the same elements as the set $(S \setminus A) \cup (S \setminus B)$, so these two sets are equal. □

S10E15. Let S, A, and B be sets.

(a) Prove that $S \setminus (A \setminus B) = (S \setminus A) \cup (S \cap B)$.

Proof. Let x be an arbitrary object. In what follows, we show that $x \in S\setminus(A\setminus B)$ iff $x \in (S\setminus A) \cup (S \cap B)$:

$$\begin{aligned}
& x \in S \setminus (A \setminus B) \\
\text{iff } \ & x \in S \wedge x \notin A \setminus B \\
\text{iff } \ & x \in S \wedge (x \notin A \vee x \in B) && \text{(by S10E13)} \\
\text{iff } \ & (x \in S \wedge x \notin A) \vee (x \in S \wedge x \in B) && \text{(by a distributive law from propositional calculus)} \\
\text{iff } \ & x \in S \setminus A \vee x \in S \cap B \\
\text{iff } \ & x \in (S \setminus A) \cup (S \cap B).
\end{aligned}$$

This completes the proof. □

(b) Deduce that $A \setminus (A \setminus B) = A \cap B$.

Proof. We have

$$\begin{aligned}
A \setminus (A \setminus B) &= (A \setminus A) \cup (A \cap B) && \text{(by (a) with } S \text{ replaced by } A\text{)} \\
&= \varnothing \cup (A \cap B) && \text{(by S10E11)} \\
&= A \cap B. && \text{(by Example 10.17)}
\end{aligned}$$

In the second step, S10E11 was applicable because $A \subseteq A$. In the third step, Example 10.17 was applicable because $\varnothing$ is a subset of any set. □

S10E16. (The Distributive Laws for Unions and Intersections.) Let S, A, and B be sets. Show that

$$S \cup (A \cap B) = (S \cup A) \cap (S \cup B).$$

Proof. Let x be any object. We will be done once we show that $x \in S \cup (A \cap B)$ iff $x \in (S \cup A) \cap (S \cup B)$.

$$\begin{aligned}
& x \in S \cup (A \cap B) \\
\text{iff } \ & x \in S \vee x \in A \cap B \\
\text{iff } \ & x \in S \vee (x \in A \wedge x \in B) \\
\text{iff } \ & (x \in S \vee x \in A) \wedge (x \in S \vee x \in B) && \text{(by a distributive law from propositional calculus)} \\
\text{iff } \ & x \in S \cup A \wedge x \in S \cup B \\
\text{iff } \ & x \in (S \cup A) \cap (x \in S \cup B).
\end{aligned}$$

This completes the proof. □

Section 11: Functions.

S11E08. Let $a, b \in \mathbb{R}$ and suppose $a < b$. Let $C[a, b]$ be the set of all continuous functions from $[a, b]$ to $\mathbb{R}$. For each $f \in C[a, b]$, let

$$I(f) = \int_a^b f(x)\, dx.$$

Then I is a function from $C[a, b]$ to $\mathbb{R}$. What is the range of I? Prove your answer.

Claim. $\text{Rng}(I) = \mathbb{R}$.

Proof. Since $I : C[a, b] \to \mathbb{R}$, $\text{Rng}(I) \subseteq \mathbb{R}$. So it remains to show that $\mathbb{R} \subseteq Rng(I)$. Consider any $y_0 \in \mathbb{R}$. We wish to show that there exists a function $f \in C[a, b]$ such that $I(f) = y_0$. Define $f(x) = y_0/(b - a)$ for all $x \in [a, b]$. (Since $a < b$, $b - a \neq 0$ and so this definition is valid.) This function f is constant on $[a, b]$, so f is continuous on $[a, b]$, *i.e.*, $f \in C[a, b]$. Furthermore, we have

$$I(f) = \int_a^b f(x)\, dx = \int_a^b \frac{y_0}{b - a}\, dx = \frac{y_0}{b - a} x \bigg|_a^b = \frac{y_0}{b - a}(b - a) = y_0.$$

This shows that $I(f) = y_0$. Therefore, $\text{Rng}(I) = \mathbb{R}$. $\square$

S11E09. Let $a, b \in \mathbb{R}$ and suppose $a < b$. Let $C^1[a, b]$ be the set of all continuously differentiable functions from $[a, b]$ to $\mathbb{R}$. For each $f \in C^1[a, b]$, let

$$L(f) = \int_a^b \sqrt{1 + [f'(x)]^2}\, dx.$$

Then L is a function from $C^1[a, b]$ to $\mathbb{R}$. What is the range of L? Prove your answer.

Claim. $\text{Rng}(I) = [b - a, \infty)$.

Proof. See Lecture 33 notes. $\square$

S11E15. Let S and T be sets. Define a function

$$f : \mathcal{P}(S) \times \mathcal{P}(T) \to \mathcal{P}(S \cup T)$$

by $f(A, B) = A \cup B$ for all $A \subseteq S$ and all $B \subseteq T$.

(a) Show that f is a surjection.

Proof. Let $C \in \mathcal{P}(S \cup T)$. Define $A = C \cap S$ and $B = C \cap T$. By S10E08, $A \subseteq S$ and $B \subseteq T$, so $A \in \mathcal{P}(S)$ and $B \in \mathcal{P}(T)$. It follows that $(A, B) \in \mathcal{P}(S) \times \mathcal{P}(T)$ and

$$\begin{aligned} f(A, B) &= A \cup B \\ &= (C \cap S) \cup (C \cap T) \\ &= C \cap (S \cup T) && \text{(by distributive law)} \\ &= C. && \text{(by S10E10)} \end{aligned}$$

We have shown that for the arbitrarily chosen $C \in \mathcal{P}(S \cup T)$, there exists $(A, B) \in \mathcal{P}(S) \times \mathcal{P}(T)$ such that $f(A, B) = A \cup B = C$. This proves that f is a surjection. $\square$

(b) Show that f is an injection iff S and T are disjoint.

Proof. ($\Rightarrow$) Suppose f is an injection. Note that $f(S, S \cap T) = S \cup (S \cap T) = S$ because $S \cap T \subseteq S$; see S10E08 and Example 10.17. Note also that $f(S, \varnothing) = S \cup \varnothing = S$. Hence $f(S, S \cap T) = f(S, \varnothing)$. But since f is an injection, $(S, S \cap T) = (S, \varnothing)$. From the fundamental property of order pairs, it follows that $S \cap T = \varnothing$, that is, S and T are disjoint.

($\Leftarrow$) Suppose that S and T are disjoint. Let $(A_1, B_1), (A_2, B_2) \in \mathcal{P}(S) \times \mathcal{P}(T)$ such that $f(A_1, B_1) = f(A_2, B_2)$, that is, $A_1 \cup B_1 = A_2 \cup B_2$. Let $C_1 = A_1 \cup B_1$ and let $C_2 = A_2 \cup B_2$. Note that

$$\begin{aligned}
C_1 \cap A_2 &= (A_1 \cup B_1) \cap A_2 \\
&= (A_1 \cap A_2) \cup (B_1 \cap A_2) && \text{(by distributive law)} \\
&= (A_1 \cap A_2) \cup \varnothing && \text{(by disjointness of } S \text{ and } T\text{)} \\
&= A_1 \cap A_2, && \text{(by Exmaple 10.17)}
\end{aligned}$$

while

$$\begin{aligned}
C_2 \cap A_2 &= (A_2 \cup B_2) \cap A_2 \\
&= (A_2 \cap A_2) \cup (B_2 \cap A_2) && \text{(by distributive law)} \\
&= (A_2 \cap A_2) \cup \varnothing && \text{(by disjointness of } S \text{ and } T\text{)} \\
&= A_2, && \text{(by S10E10)}
\end{aligned}$$

But since $C_1 = C_2$, $C_1 \cap A_2$ must equal $C_2 \cap A_2$, so $A_1 \cap A_2 = A_2$. Then by S10E10 again, $A_2 \subseteq A_1$. Repeating the same argument with $C_1 \cap A_1 = C_2 \cap A_1$, we obtain $A_1 \subseteq A_2$. Hence, $A_1 = A_2$. Similarly, using $C_1 \cap B_1 = C_2 \cap B_1$, one can deduce that $B_1 \subseteq B_2$, and using $C_1 \cap B_2 = C_2 \cap B_2$, one can deduce that $B_2 \subseteq B_1$, hence $B_1 = B_2$. Thus, by the fundamental property of ordered pairs, $(A_1, B_1) = (A_2, B_2)$. This shows that f is an injection. $\square$

S11E20(b). See Lecture 33 for a solution to part (a). Modify it for part (b).

S11E23. Let $\varphi(x) = x/(1 - |x|)$ for all $x \in (-1, 1)$.

(a) Show that φ is a bijection from $(-1, 1)$ to $\mathbb{R}$.

Proof. Let $A = [0, 1)$, $B = (-1, 0)$, $C = [0, \infty)$, and $D = (-\infty, 0)$. Let $X = A \cup B = (-1, 1)$ and $Y = C \cup D = (-1, 1)$. Note that $A \cap B = \varnothing$ and $C \cap D = \varnothing$. Define functions g and h by

$$g(x) = \frac{x}{1 - x} \quad \text{for all } x \in A; \quad h(x) = \frac{x}{1 + x} \quad \text{for all } x \in B.$$

Then, by S11E20, g is a bijection from A to C and h is a bijection from B to D. But observe that

$$\begin{aligned}
\varphi(x) &= \frac{x}{1 - |x|} \quad \text{for all } x \in (-1, 1) \\
&= \begin{cases} x/(1 - x) & \text{if } x \in [0, 1) \\ x/(1 + x) & \text{if } x \in (-1, 0) \end{cases} \\
&= \begin{cases} g(x) & \text{if } x \in A \\ h(x) & \text{if } x \in B \end{cases}.
\end{aligned}$$

Hence, by S11E22(c), φ is a bijection from $X = (-1, 1)$ to $Y = \mathbb{R}$ as desired. $\square$

Section 13: The Fundamental Principles of Counting.

S13E03. (Lemma 13.20) Let A be a set and let s be any object. Then:

(a) For each $n \in \boldsymbol{\omega}$, if A has n elements and $s \notin A$, then $A \cup \{s\}$ has $n+1$ elements.

Proof. Let $n \in \boldsymbol{\omega}$ and suppose that A has n elements and $s \notin A$. Let $B = \{1, \ldots, n\}$. Then, by Definition 13.10, A is equinumerous to B. So it follows from Lemma 13.19 that $A \cup \{s\}$ is equinumerous to $B \cup \{n+1\}$ because $n+1 \notin B$. But $B \cup \{n+1\} = \{1, \ldots, n+1\}$, so A is equinumerous to $\{1, \ldots, n+1\}$. Hence, A has $n+1$ elements. $\square$

(b) If A is finite, then $A \cup \{s\}$ is finite.

Proof. Suppose A is finite. Either $s \in A$ or $s \notin A$.

Case 1. Suppose $s \in A$. Then $A \cup \{s\} = A$, so $A \cup \{s\}$ is finite.

Case 2. Suppose $s \notin A$. Then, by the previous part, $A \cup \{s\}$ has $n+1$ element, so $A \cup \{s\}$ is finite.

In either case, $A \cup \{s\}$ is finite. $\square$

Section 15: Infinite Sets.

S15E01. Show that $A = [1, \infty)$ is equinumerous to $B = (1, \infty)$.

Proof. The function f defined on A by

$$f(x) = \begin{cases} x+1 & \text{if } x \in \mathbb{N}, \\ x & \text{if } x \in A \setminus \mathbb{N}, \end{cases}$$

is a bijection from A to B. (Make sure you can show that this f is indeed a bijection.) $\square$

S15E02. Show that $\mathbb{Z}$ is equinumerous to $\mathbb{N}$.

Proof. Define f on $\mathbb{Z}$ by

$$f(x) = \begin{cases} 2x & \text{if } x \in \mathbb{N}, \\ 2(-x)+1 & \text{if } x \in \mathbb{Z} \setminus \mathbb{N}. \end{cases}$$

Then f is a bijection from $\mathbb{Z}$ to $\mathbb{N}$. (Make sure you can show that this f is indeed a bijection.) $\square$

S15E07.

(a) Show that $(0, 1]$ is equinumerous to $(0, 1)$.

Proof. Let f be defined on $(0, 1]$ as follows:

$$f(x) = \begin{cases} x/2 & \text{if } x \in (0,1] \cap \mathbb{Q}, \\ x & \text{if } x \in (0,1] \setminus \mathbb{Q}. \end{cases}$$

In words, if x is a rational number in $(0, 1]$, then $f(x)$ is half of x; if x is an irrational number between 0 and 1, then $f(x)$ is the same as x. This function f is a bijection from $(0, 1]$ to $(0, 1)$. (Confirm it yourself.) $\square$

(c) Explain that all four intervals $[0, 1]$, $[0, 1)$, $(0, 1]$, and $(0, 1)$ have the same number of elements.

Proof. Let $A = [0, 1]$, $B = [0, 1)$, $C = (0, 1]$, and $D = (0, 1)$. We already know that

1) $A \approx B$ by S15E07(b);
2) $B \approx C$ by S15E06;
3) $C \approx D$ by S15E07(a).

From 1) and 2), it follows that $A \approx C$, by transitivity of equinumerousness.
From this and 3), it follows that $A \approx D$, by transitivity of equinumerousness.
From 2) and 3), it follows that $B \approx D$, by transitivity of equinumerousness.
From 2) and 3), it follows that $B \approx D$, by transitivity of equinumerousness.
Therefore, all four intervals A, B, C, and D have the same number of elements. $\square$