EXERCISES 7.23. Explain how you know that each of the following deductions is not valid.

1) $\exists x, (x \in A),\ \exists x, (x \in B),\ \therefore\ \exists x, ((x \in A)\ \&\ (x \in B))$

2) $\forall a \in A, \exists b \in B, (a \neq b),\ A \neq \emptyset,\ \therefore\ \forall b \in B, \exists a \in A, (a \neq b).$ False

3) $A \neq B,\ \therefore\ A \cup B \neq A.$

4) $\forall x \in A, (x \notin B),\ \forall x \in B, (x \notin A),\ \therefore\ A \neq B.$

1) $\exists x, (x \in A) = T$, $\exists x, (x \in B) = T$ but $\exists x\ ((x \in A)\ \&\ (x \in B)) = F$

For instance take $A = \{\square\}$ and $B = \{\text{apple}\}$, form a counter example.

2) ($A = \{1,2\}$ $B = \{3\}$ X)

$A = \{1\}$ $B = \{1,2\}$

form a counter example

$(\forall a \in A)\ [\exists b \in B]\ (a \neq b)$ True

$A \neq b$ True

$(\forall b \in B)(\exists a \in A)\ (a \neq b)$

↳ false $b = 1$

$A = \{1\}$

$B = \{1,2\}$

3) $\dfrac{A \neq B \text{ True}}{A \cup B \neq A \text{ False}}$ $B = \{1\}$, $A = \{1,2\}$

4) ($A = \{1\}$, $B = \{2\}$ $A \cap B = \phi$ $A \neq B$

$B = \{7,8\}$)

$A = \phi$, $B = \phi$ form a counter example

$\forall x \in A,\ x \notin B$ True

$\forall x \in B,\ x \notin A$ True

$A \neq B$ False

$(\forall x \in \phi)\ P(x) = \text{true}$

$\forall x\ (x \in \phi \rightarrow P(x))$

False

Fact: Let A, B, C be sets. Then

(1) $\phi \subseteq A$, $A \subseteq A$,
$A \subseteq A \cup B$, $A \cap B \subseteq A$

(2) If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$

(3) ($\cup$ and $\cap$ are commutative)
$A \cup B = B \cup A$, $A \cap B = B \cap A$

(4) ($\cup$ and $\cap$ are associative)
$(A \cup B) \cup C = A \cup (B \cup C)$
$A \cap (B \cap C) = A \cap (B \cap C)$

(5) ($\cup / \cap$ distributes over $\cap / \cup$)
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(6) (Idempotent laws)
$A \cup A = A$, $A \cap A = A$

---

(7) (Identity Laws)
$A \cup \phi = A$, $A \cap \mathcal{U} = A$
($\mathcal{U}$: universal set)

(8) (Absorption Laws)
$A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$
Indeed more generally
$X \subseteq A \Rightarrow A \cup X = A$
$A \subseteq Y \Rightarrow A \cap Y = A$

(9) (Domination Laws)
$A \cup \mathcal{U} = \mathcal{U}$, $A \cap \phi = \phi$
($\mathcal{U}$: universal set)

(10) (Inverse Laws)
$A \cup A^c = \mathcal{U}$, $A \cap A^c = \phi$
($\mathcal{U}$: universal set)

(11) (Double complement)
$(A^c)^c = A$

(12) (De Morgan's Rules) ***
$(A \cup B)^c = A^c \cap B^c$
$(A \cap B)^c = A^c \cup B^c$
$C - (A \cup B) = (C - A) \cap (C - B)$
$C - (A \cap B) = (C - A) \cup (C - B)$

Proof: (Exercise) For illustration we prove here

(2) (As we want to prove $A \subseteq C$, we should take an arbitrary element a from A and we must justify that a is in C). Take any $a \in A$. As $A \subseteq B$, $a \in B$. As $B \subseteq C$ and $a \in B$, it follows (from the definition of subset) that $a \in C$. Hence $A \subseteq C$

(5) We prove here that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. (As we want to prove that two sets (LHS & RHS) are equal, it sufficies to prove that $LHS \subseteq RHS$ and $RHS \subseteq LHS$).

Let $x \in A \cup (B \cap C)$. From the definition of the union, $x \in A$ or $x \in B \cap C$. So we have two cases to consider.

Case 1: Assume $x \in A$. It follows from the definition of the union that $x \in A \cup B$ and $x \in A \cup C$. Since x is in the both sets $(A \cup B)$ and $(A \cup C)$, x is in their intersection $(A \cup B) \cap (A \cup C)$. So $x \in (A \cup B) \cap (A \cup C)$.

Case 2: Assume that $x \in B \cap C$. From the definition of the intersection, we see that $x \in B$ and $x \in C$. It then follows from the definition of the union that $x \in A \cup B$ (because $x \in B$) and $x \in A \cup C$ (because $x \in C$). As $x \in A \cup B$ and $x \in A \cup C$, we conclude that $x \in (A \cup B) \cap (A \cup C)$.

Having proved $x \in (A \cup B) \cap (A \cup C)$ in both cases, we have justified that

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C).$$

Let now $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$ by the definition of the intersection. So, $x \in A$ or $x \in B$, and $x \in A$ or $x \in C$ by the definition of the union. We need to consider 3 cases where $x \in A$, $x \in B$, or $x \in C$. Instead we may consider the 2 cases in which $x \in A$ or $x \notin A$ (Note that when $x \notin A$ it follows that $x \in B$ and $x \in C$).

Case 1: Assume $x \in A$. The definition of the union implies that $x \in A \cup (B \cap C)$

Case 2: Assume $x \notin A$. Since $x \in A \cup B$ and $x \in A \cup C$, we see from the definition of the union that $x \in B$ and $x \in C$. From $x \in B$ and $x \in C$, we get $x \in B \cap C$. As $x \in B \cap C$, the definition of the union implies that $x \in A \cup (B \cap C)$.

Having proved $x \in A \cup (B \cap C)$, we have justified that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

(11) Recall the definition of the complement M^c of a set M, $M^c = \{x \mid x \notin M\}$. Therefore, "$x \notin M^c$ iff $x \in M$". Using this here ↓

$$x \in (A^c)^c \text{ iff } x \notin A^c \text{ iff } x \in A$$

$$\| \quad \{x \mid x \notin A^c\}$$

— ∘ —

Ex: Prove or disprove: $A \cap C = B \cap C \not\Rightarrow A = B$

Sol: This is not true. For instance, $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{1\}$ is a counter example

---

Ex: Prove that: $A \cap C = B \cap C$ and $A \cup C = B \cup C \not\Rightarrow A = B$

Proof: First Proof: (We may work with elements to show that $A \subseteq B$ and $B \subseteq A$).

Let $a \in A$. Then $a \in A \cup C$ and so $a \in B \cup C$, because it is given that $A \cup C = B \cup C$. So $a \in B$ or $a \in C$. If $a \in B$ then we are done. So assume now that $a \in C$. From $a \in A$ and $a \in C$, we get $a \in A \cap C$, and so $a \in B \cap C$ (because $A \cap C = B \cap C$), implying that $a \in B$. Consequently, $A \subseteq B$.

The proof of the other containment $B \subseteq A$ is similar and it is left as an exercise. Or you may just say that "by the symmetry" $A \subseteq B$, because we may interchange A with B in the statement of the result. (Indeed, for instance, instead of $A \cap C = B \cap C$, we may write $B \cap C = A \cap C$).

Second Proof: (Instead of working with elements we may use known identites/results).

$$
\begin{aligned}
A &= A \cup (A \cap C) && \text{, absorption } (\text{or better you may just write because } A \cap C \subseteq A) \\
&= A \cup (B \cap C) && \text{, } A \cap C = B \cap C \text{ is given} \\
&= (A \cup B) \cap (A \cup C) && \text{, distribution} \\
&= (A \cup B) \cap (B \cup C) && \text{, } A \cup C = B \cup C \text{ is given} \\
&= (A \cup B) \cap (C \cup B) && \text{, commutativity} \\
&= (A \cap C) \cup B && \text{, distribution} \\
&= (B \cap C) \cup B && \text{, } A \cap C = B \cap C \text{ is given} \\
&= B && \text{, absorption } (\text{or better you may just write because } B \cap C \subseteq B)
\end{aligned}
$$

Ex: Give an example of a nonempty set A such that $a \subseteq A$ for every $a \in A$
(i.e., such that every element is a subset)

Sol: (For instance A cannot be $\{1,2\}$, because $1 \in \{1,2\}$ but $1 \notin \{1,2\}$. As every element is a subset (in particular a set), each element of such a set must itself be a set. Furthermore, if $a = \{?\} \in A$ then from $\{?\} \subseteq A$ we see that $? \in A$. So A must be of the form $A = \{?, \{?\}, \dots\}$. We want also that $?$ is a subset of A. As the empty set is a subset of every set, we may let $?$ be the empty set ϕ).

Any of the following sets is an example satisfying the required condition:

$$A = \{\phi\}, \text{ or } \{\phi, \{\phi\}\} \text{ or } \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\} \dots\dots$$

Ex: Let A be a set. Prove that $\{P(X) \mid X \subseteq A\} \subseteq P(P(A))$

Sol: (We take an arbitrary element from the set $\{P(X) \mid X \subseteq A\}$ and try to show that this element is in $P(P(A))$).

Let $z \in \{P(X) \mid X \subseteq A\}$. Then $z = P(X)$ for some $X \subseteq A$. We want to show that $z \in P(P(A))$. By the definition of the power set $P(B) = \{Y \mid Y \subseteq B\}$ of a set B, we see that "$z \in P(P(A))$ iff $z \subseteq P(A)$" So it is enough to prove that $z \subseteq P(A)$, that is $P(X) \subseteq P(A)$: Indeed, if $S \in P(X)$, then $S \subseteq X$ and so $S \subseteq A$ (because $X \subseteq A$), implying that $S \in P(A)$. Thus $P(X) \subseteq P(A)$, as desired.

Ex: Let A and B be sets. Prove that the following conditions are equivalent:

① $A \subseteq B$

② $A \cup B = B$

③ $A \cap B^c = \emptyset$

④ $B^c \subseteq A^c$

Proof: (We are required to prove that ① $\equiv$ ② $\equiv$ ③ $\equiv$ ④. We may prove that each $\Rightarrow$ in ① $\Rightarrow$ ② $\Rightarrow$ ③ $\Rightarrow$ ④ $\Rightarrow$ ① is a valid deduction (i.e. a tautology)).

① $\Rightarrow$ ②: (Assume ① and prove ②) We want to prove that $A \cup B \subseteq B$ and $B \subseteq A \cup B$. The second containment $B \subseteq A \cup B$ is obvious. Consider the first. Take any $x \in A \cup B$. We want to show that $x \in B$. As $x \in A \cup B$, $x \in A$ or $x \in B$. If $x \in B$ then we are done. If $x \in A$, then it follows from "① $A \subseteq B$" that $x \in B$. Thus $A \cup B \subseteq B$

② $\Rightarrow$ ③: (Assume ② and prove ③). The proof is by contradiction. Assume for a moment that $A \cap B^c \neq \emptyset$. Then there is an x such that $x \in A$ and $x \in B^c$. As $x \in B^c$, $x \notin B$. Now, $x \notin B$ but $x \in A \cup B$ (because $x \in A$), implying that $A \cup B \neq B$. This contradicts with the assumption ②.

③ $\Rightarrow$ ④: Exercise

④ $\Rightarrow$ ①: Exercise

Ex: Let A, B, C be sets. Prove that if $A - (B - C) \subseteq (A - B) - C$, then A and C are disjoint.

Proof: We want to show that $A \cap C = \emptyset$. The proof is by contradiction. Assume for a contradiction that $A \cap C \neq \emptyset$. Then $A \cap C$ contains at least one

element x. From $x \in A \cap C$, we see that $x \in A$ and $x \in C$.

As $x \in C$, $x \notin B - C$. From $x \in A$ and $x \notin B - C$, $x \in A - (B - C)$.

On the other hand, as $x \in C$, we see that $x \notin (A - B) - C$.

Having proved that $x \in A - (B - C)$ and $x \notin (A - B) - C$, we conclude that $A - (B - C) \not\subseteq (A - B) - C$. This is a contradiction to the hypothesis.

(i.e., the condition "$A - (B - C) \subseteq (A - B) - C$")

Fact: $A - B = A \cap B^c$ for any sets A and B.

Proof: $x \in A - B$ iff $x \in A$ but $x \notin B$ iff $x \in A$ and $x \in B^c$ iff $x \in A \cap B^c$

(recall that $A - B = \{x \mid x \in A \text{ and } x \notin B\}$) (recall that $B^c = \{x \mid x \notin B\}$)

Cartesian products (or Cross products):

Let A and B be sets. We define their cartesian product (or cross product) $A \times B$ to be the set $A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}$ of ordered pairs (a,b). For any ordered pairs $(a_1, b_1), (a_2, b_2) \in A \times B$,

$(a_1, b_1) = (a_2, b_2)$ iff $a_1 = a_2$ and $b_1 = b_2$ (Indeed, this is because the formal definition of an ordered pair in set theory is "$(a,b) = \{\{a\}, \{a,b\}\}$").

Note for (finite) sets A and B we have $|A \times B| = |A|\,|B|$. (Indeed, if $A = \{a_1, a_2, \dots, a_m\}$ and $B = \{b_1, b_2, \dots, b_n\}$, then $A \times B = \{(a_i, b_j) \mid i = 1, 2, \dots, m,\ j = 1, 2, \dots, n\}$ has mn elements)

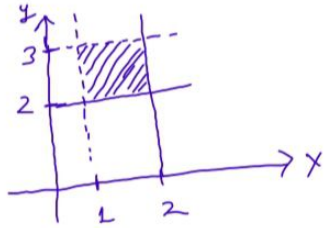
Ex: Let $A = \{1, 2\}$ and $B = \{\Delta, \square, \circ\}$. Then

$A \times B = \{(1,\Delta), (1,\square), (1,\circ), (2,\Delta), (2,\square), (2,\circ)\}$

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

Ex: For the intervals $(1,2]$ and $[2,3)$ in $\mathbb{R}$ we have

$$(1,2]\times[2,3) = \{(x,y) \mid 1 < x \leq 2 \text{ and } 2 \leq y < 3\}$$



Fact: For any sets

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \quad \text{and} \quad A \times (B \cap C) = (A \times B) \cap (A \times C)$$

$$(B \cup C) \times A = (B \times A) \cup (C \times A) \quad \text{and} \quad (B \cap C) \times A = (B \times A) \cap (C \times A)$$

(Distribution of $\times$ over $\cup$ & $\cap$)

Proof: Exercise

Generalization: We may define the cartesian product of any number of sets in a similar way, or we may iterate the definition of cartesian product of two sets. For instance, given 3 sets A, B, C we may consider the following two cartesian products

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

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

The two pairs $((a,b),c)$ and $(a,(b,c))$ are virtually the same, and we may just define

$$A \times B \times C = \{(a,b,c) \mid a \in A \text{ and } b \in B \text{ and } c \in C\}$$ where two ordered triples

(a_1, b_1, c_1) and (a_2, b_2, c_2) are equal iff their coordinates are equal

(that is, $a_1 = a_2$ and $b_1 = b_2$ and $c_1 = c_2$)

Given any (finitely many) sets $A_1, A_2, \cdots, A_n$, their cartesian product is defined to be the set $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i \text{ for all } i = 1, 2, \cdots, n\}$

Moreover, for any two elements of the cartesian product

$$(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n) \quad \text{iff} \quad x_i = y_i \text{ for all } i = 1, 2, \cdots, n.$$

For any set A and positive integer n, we may use the notation A^n to denote

$$A^n = \underbrace{A \times A \times \cdots \times A}_{n\text{-times}}$$

Family of sets, the axiom of choice, paradoxes

By a family of sets $\mathcal{F}$ we mean a set all of whose elements are sets. For instance $\{\{1\}, \{1, \square\}\}$ is a family of set. Given a family of sets $\mathcal{F}$ (that is, $\mathcal{F}$ is a set and each element of $\mathcal{F}$ is itself a set) we define

$$\bigcap \mathcal{F} = \bigcap_{A \in \mathcal{F}} A = \text{the intersection of all sets in } \mathcal{F} = \{x \mid x \in A \text{ for all } A \in \mathcal{F}\}$$

$$\bigcup \mathcal{F} = \bigcup_{A \in \mathcal{F}} A = \text{the union of all sets in } \mathcal{F} = \{x \mid x \in A \text{ for some } A \in \mathcal{F}\}$$

If it is possible to give indices to elements of $\mathcal{F}$ so that $\mathcal{F} = \{A_i \mid i \in I\}$ where I is a set, called the index set, we may write

$$\bigcup \mathcal{F} = \bigcup_{i \in I} A_i \quad \text{and} \quad \bigcap \mathcal{F} = \bigcap_{i \in I} A_i$$

Ex: $\bigcap_{i=1}^{\infty} \left(\frac{-1}{i}, \frac{1}{i}\right) = \bigcap \mathcal{F}$ where $\mathcal{F} = \{A_i \mid i \in I\}$ and $A_i = \left(\frac{-1}{i}, \frac{1}{i}\right) = \{x \in \mathbb{R} \mid \frac{-1}{i} < x < \frac{1}{i}\}$ and $I = \mathbb{N}^+$

($\left(\frac{-1}{i}, \frac{1}{i}\right)$: interval in $\mathbb{R}$)

Note that $\bigcap \mathcal{F} = \{0\}$.

Ex: For any set A, $\bigcap_{X \in \mathcal{P}(A)} X = \phi$ where $\mathcal{P}(A)$ is the power set of A.

Fact:

1) $\bigcup_{A \in \phi} A = \phi$ and $\bigcap_{A \in \phi} A =$ the universal set. (Here we consider the empty set as a family of sets)

2) $A_k \subseteq \bigcup_{i \in I} A_i$ for any $k \in I$, $\quad \bigcap_{i \in I} A_i \subseteq A_k$ for any $k \in I$

3) $B \cap \left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} (B \cap A_i)$, $\quad B \cup \left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} (B \cup A_i)$

4) $B - \left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I} (B - A_i)$, $\quad B - \left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I} (B - A_i)$ (De Morgan's Laws)

Proof: Exercise. We only justify here second part of (1). Suppose for a contradiction that $\bigcap_{A\in\phi} A$ is not the universal set. Then there is a z (in the universal set) such that $z \notin \bigcap_{A\in\phi} A$. From the definition of the intersection, there is a $B \in \phi$ such that $z \notin B$. In particular, the empty set ϕ has an element B. This is a contradiction because by the definition the empty set has no elements

———— ∘ ————

The Axiom Of Choice: Given any family $\mathcal{F}$ of nonempty sets (i.e., each element of $\mathcal{F}$ is a nonempty set), we can choose an element simultaneously from each set in $\mathcal{F}$.

The Axiom of Choice has many logically equivalent formulations some of which will be stated in our future lectures. The axiom of choice has to be assumed to deal with "large sets".

The Cartesian Product over a Family: Let $\mathcal{F}$ be a family of sets. The cartesian product of the sets in $\mathcal{F}$ is defined to be the set

$$\prod_{A\in\mathcal{F}} A = \text{the set of all sequences } (x_A)_A \text{ whose } A^{\text{th}} \text{ term } x_A \text{ is an element of the set } A.$$

If $\mathcal{F} = \{A_i \mid i\in I\}$, then the cartesian product of the sets A_i is

$$\prod_{i\in I} A_i = \{(a_i)_{i\in I} \mid a_i \in I \text{ for all } i\in I\}$$

For instance, letting $I = \mathbb{N}^+ = \{1,2,\dots\}$ and $A_i = \mathbb{R}$ for all $i\in I$, $\prod_{i\in I} A_i$ is

the set of real valued sequences, and for example the sequence $\left(\frac{1}{n}\right)_{n=1}^{\infty}$ is an element of it because for any $i \in I$ the i^{th} term of $\left(\frac{1}{n}\right)_{n=1}^{\infty}$ is $\frac{1}{i}$ and it is an element of $A_i = \mathbb{R}$.

Paradoxes: Recall that we defined a set to be a well-defined collection of objects or recall that we assumed that the sets are subsets of a universal set. We did so because we do not want our sets to be arbitrarily large. Large sets can cause some contradictions and paradoxes. Georg Cantor, the inventor of the set theory, defined a set to be any collection of objects. This definition leads to the following well known paradox.

Russel's Pradox: According to Cantor's definition the collection of all sets is a set and let us denote this set by $\mathcal{A}$. So $\mathcal{A} = \{S \mid S \text{ is a set}\}$. Consider the subset $\mathcal{B} = \{S \in \mathcal{A} \mid S \notin S\}$. Let us try to answer the question:

"Does $\mathcal{B}$ contain itself as an element?", that is, "Is it true that $\mathcal{B} \in \mathcal{B}$?"

This question must have a definite answer (Yes or No). Indeed, if the answer is Yes, then $\mathcal{B} \in \mathcal{B}$ and so the definition of $\mathcal{B}$ implies that $\mathcal{B} \notin \mathcal{B}$. On the other hand, if the answer is No, then $\mathcal{B} \notin \mathcal{B}$ and so the definition of $\mathcal{B}$ implies that $\mathcal{B} \in \mathcal{B}$.

We see from the Russel's Paradox that if we want Set Theory to be consistent (i.e, not leading to any contradiction) then

- The collection of all sets is not a set
- There is no set containing itself as an element

EXERCISES 6.30.

4) Does there exist a set A, such that $\mathcal{P}(A) = \emptyset$?

5) Let

- $V_0 = \emptyset$,
- $V_1 = \mathcal{P}(V_0)$,
- $V_2 = \mathcal{P}(V_1) = \mathcal{P}(\mathcal{P}(V_0))$,
- and so forth.

In general, $V_n = \mathcal{P}(V_{n-1})$ whenever $n > 0$.

(a) What are the cardinalities of V_0, V_1, V_2, V_3, V_4, and V_5?

(b) Describe V_0, V_1, V_2, and V_3 by listing their elements.

(c) (harder) Describe V_4 by listing its elements.

(d) Is it reasonable to ask someone to list the elements of V_5? *Why?*

EXERCISES 8.18. Suppose A, B, and C are sets (and $\mathcal{U}$ is the universal set, as usual).

10) Show that if $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$, then either $A \subset B$ or $B \subset A$.

Proof: Proof is by contradiction. Suppose for a moment that $A \not\subseteq B$ and $B \not\subseteq A$. So there is an $a \in A$ such that $a \notin B$ (because $A \not\subseteq B$), and there is a $b \in B$ such that $b \notin A$ (because $B \not\subseteq A$).

Consider the set $z = \{a, b\}$. Note that $\{a, b\} \subseteq A \cup B$ because $a \in A$ and $b \in B$. Hence $z = \{a, b\} \in \mathcal{P}(A \cup B)$.

As it is given that $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$, $z \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Thus, $z \in \mathcal{P}(A)$ or $z \in \mathcal{P}(B)$.

Case 1 Assume $z \in \mathcal{P}(A)$. Then $z \subseteq A$, $z = \{a, b\} \subseteq A$ which implies that $b \in A$. This is a contradiction

Case 2 Assume $z \in \mathcal{P}(B)$

∴ (exercise)

Since in both cases we get a contradiction, it follows that "$A \not\subseteq B$ and $B \not\subseteq A$" must be false. So $A \subseteq B$ or $B \subseteq A$ □

EXERCISES 8.24.

1) Suppose A, B, and C are sets.

(a) Show that if $B \subset C$, then $A \times B \subset A \times C$.

(b) Show that if $A \times B = A \times C$, and $A \neq \emptyset$, then $B = C$.

($M \times N = M \times V \Rightarrow N = V$. Is it true?
Not true because $\emptyset \times \mathbb{N} = \emptyset$)

Exercise

Proof by Induction

To prove theorems involving assertions indexed by natural numbers we usually use the method of "proof by mathematical induction". To explain it suppose we are required to prove that a quantified assertion "$(\forall n \in \mathbb{N}^+)\ P(n)$" is true where $\mathbb{N}^+ = \{1, 2, 3, \ldots, \ldots\}$ is the set of positive natural numbers and $P(n)$ is an open statement. Suppose that we manage to establish (the truthness of) the following (assertions):

(i) $P(1)$ is true

(ii) For any natural number $k \geq 1$, $P(k) \rightarrow P(k+1)$ is true

Then we can conclude that "$P(n)$ is true for all natural numbers $n \in \mathbb{N}^+$" (that is "$(\forall n \in \mathbb{N}^+)\ P(n)$" is true. Indeed, using (ii) successively by putting $k = 1, 2, 3, \ldots$ we see that all of the following assertions are true.

$$P(1) \rightarrow P(2),\ P(2) \rightarrow P(3),\ P(3) \rightarrow P(4),\ \ldots,\ P(k-1) \rightarrow P(k),\ \ldots\ldots$$

As $P(1)$ is true by (i), using the 1^{st}, 2^{nd}, 3^{rd}, ... of the above implications we obtain that $P(2), P(3), P(4), \ldots, P(n), \ldots$ are all true.

Although the above explanation of why "$(\forall n \in \mathbb{N}^+)\ P(n)$" is true is convincing enough, it uses the fact that natural numbers are "well ordered" by the usual less than or equal to relation. This intuitively acceptable result is logically equivalent to the method of proof by induction, and one of them must be taken as an axiom in this introductory lectures. We prefer to take the following as an axiom.

Well Ordering Principle: Any nonempty subset of natural numbers $\mathbb{N}$ has smallest element with respect to the usual $\leq$. (That is, $\mathbb{N}$ is a well ordered set by the usual $\leq$ relation).

Theorem: Let $A \subseteq \mathbb{N}^+$ satisfy the following two conditions:

(i) $1 \in A$

(ii) For any $n \in \mathbb{N}^+$, if $n \in A$ then $n+1 \in A$

Then $A = \mathbb{N}^+$

Proof: The proof will be by contradiction. Suppose for a moment that $A \neq \mathbb{N}^+$. Then $\mathbb{N}^+ - A$ is a nonempty subset of $\mathbb{N}$. By the well ordering principle $\mathbb{N}^+ - A$ has smallest element, say n_0. In particular, $n_0 \in \mathbb{N}^+ - A$, and so $n_0 \notin A$. As $1 \in A$,

we see that $n_0 \neq 1$ and so $n_0 > 1$. Consider now $n_0 - 1$. As $n_0 > 1$, $n_0 - 1 \in \mathbb{N}^+$. Since $n_0 \notin A$, we see from (ii) that $n_0 - 1 \notin A$. Now, having justified that $n_0 - 1 \in \mathbb{N}^+$ and $n_0 - 1 \notin A$, we conclude $n_0 - 1 \in \mathbb{N}^+ - A$. This is a contradiction, because $n_0 - 1$ is smaller than the smallest element n_0 of $\mathbb{N}^+ - A$. □

Corollary:

$$(\forall n \in \mathbb{N}^+)\, P(n) \quad \equiv \quad P(1) \wedge (\forall k \in \mathbb{N}^+)(P(k) \to P(k+1))$$

Proof: If the LHS is true, then $P(m)$ is true for all $m \in \mathbb{N}^+$, and so $P(1)$ and $P(k) \to P(k+1)$ are all true for each k; so the RHS is true. $(T \to T \equiv T)$

Assume now that the RHS is true. We want to justify that the LHS is true. Consider the set $A = \{n \in \mathbb{N}^+ \mid P(n)\}$ which is the set of all $n \in \mathbb{N}^+$ for which $P(n)$ is true. (The LHS is true if and only if $A = \mathbb{N}^+$.) As we assumed that the RHS is true, $P(1)$ and $(\forall k \in \mathbb{N}^+)(P(k) \to P(k+1))$ are both true. So, $1 \in A$ and $(\forall k \in \mathbb{N}^+)(k \in A \to k+1 \in A)$. Thus A satisfies the two conditions of the previous theorem. Hence $A = \mathbb{N}^+$ □

Remark: To prove "$(\forall n \geq n_0) P(n)$ is true" by induction where $n_0 \in \mathbb{N}$, we first justify that $P(n_0)$ is true. This is called base case. We then justify that the implication $P(k) \to P(k+1)$ is true for all $k \geq n_0$. This is called induction step. Recalling the truth value of an implication, we may argue in the induction step as follows: We take an arbitrary natural number k such that $k \geq n_0$ (and fix k throughout the proof). We assume that $P(k)$ is true. This is called the induction hypothesis. We finally justify that $P(k+1)$ is true (by using the induction hypothesis).

— ∘ —

The format of a proof by induction is as follows:

Theorem: $P(n)$ for all natural numbers $n \geq n_0$

Proof: (The proof is by induction on n)

Base case: $P(n_0)$ is true.

Induction step: Assume $k \in \mathbb{N}$ with $k \geq n_0$ and $P(k)$ is true. (induction hypothesis)

Then .....

So $P(k+1)$ is true.

Therefore, by the principle of mathematical induction, we conclude that $P(n)$ is true for every $n \in \mathbb{N}$ with $n \geq n_0$. □

Ex: Prove that $4n < n^2 - 7$ for all $n \in \mathbb{N}$ with $n \geq 6$.

Proof: (The proof will be by induction on n) Let "$P(n): 4n < n^2 - 7$".

Base case: For $n = 6$, $4n < n^2 - 7$ becomes $4(6) < 6^2 - 7$, $24 < 29$ which is true. So $P(6)$ is true.

Induction step: Let $k \in \mathbb{N}$ be such that $k \geq 6$. Assume that $P(k)$ is true. That is, assume that $4k < k^2 - 7$. (This is the induction hypothesis)

(We want to show that $P(k+1): 4(k+1) < (k+1)^2 - 7$ is true).

Note that
$$\begin{aligned} 4(k+1) &= 4k + 4 \\ &< (k^2 - 7) + 4 \quad \text{by induction hypothesis} \\ &= k^2 - 3 \\ &= (k+1)^2 - 2k - 4 \\ &= (k+1)^2 - 7 + (3 - 2k) \\ &< (k+1)^2 - 7 \quad \text{because } (3-2k) < 0 \text{ for } k \geq 6 \end{aligned}$$

So $P(k+1)$ is true.

Therefore, by the principle of mathematical induction $4n < n^2 - 7$ for all $n \in \mathbb{N}$ with $n \geq 6$. □

Be careful about notations. The letter k (dummy variable) may be changed with any other letters which are not used previously. Our textbook justifies that the implication "$(\forall k \geq n_0 + 1)\ (P(k-1) \to P(k))$" is true in the induction step, which is of course equivalent to the implication "$(\forall k \geq n_0)\ (P(k) \to P(k+1))$". So, in our textbook, it is assumed that k is any natural number with $k \geq n_0 + 1$ and that $P(k-1)$ is true. (The induction hypothesis), and then $P(k)$ is justified.

Ex: For any $n \in \mathbb{N}^+$ we define $H_n = \sum_{i=1}^{n} \frac{1}{i} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$

Prove that $\sum_{i=1}^{n} H_i = (n+1) H_n - n$ for all $n \in \mathbb{N}^+$.

Proof: The proof is by induction on n. Let "$P(n): \sum_{i=1}^{n} H_i = (n+1) H_n - n$"

Base case: For $n=1$, $P(1)$ becomes $H_1 = 2H_1 - 1$ which is true because $H_1 = 1$.

Induction step: Assume $k \in \mathbb{N}^+$ and assume $P(k)$ is true. That is we assume that $\sum_{i=1}^{k} H_i = (k+1) H_k - k$ (This is the induction hypothesis)

(We want to show that $P(k+1)$ is true. That is we want to show that $\sum_{i=1}^{k+1} H_i = (k+2) H_{k+1} - (k+1)$)

Now, $\sum_{i=1}^{k+1} H_i = \left(\sum_{i=1}^{k} H_i\right) + H_{k+1} = (k+1) H_k - k + H_{k+1}$ (I)

↑ by induction hypothesis

We want to obtain only H_{k+1} on the rhs of (I). For this note that

$$H_{k+1} = \sum_{i=1}^{k+1} \frac{1}{i} = \left(\sum_{i=1}^{k} \frac{1}{i}\right) + \frac{1}{k+1} = H_k + \frac{1}{k+1}$$

Substituting $H_k = H_{k+1} - \frac{1}{k+1}$ into (I) we get

$$\sum_{i=1}^{k+1} H_i = (k+1)\left(H_{k+1} - \frac{1}{k+1}\right) - k + H_{k+1} = (k+2)H_{k+1} - (k+1)$$

as desired. So $P(k+1)$ is true. Hence, the result follows by induction □

Ex: Prove that $(1+m)^{n+1} > 1+(n+1)m$ for all $m, n \in \mathbb{N}^+$.

Proof: Let $m \in \mathbb{N}^+$ be arbitrary. The proof will be by induction on n.

Let "$P(n)$: $(1+m)^{n+1} > 1+(n+1)m$".

For $n=1$, $P(1)$ becomes $(1+m)^2 > 1+2m$ which is true because $(1+m)^2 = 1+2m+m^2 > 1+2m$ because $m > 0$.

Take an arbitrary $k \in \mathbb{N}^+$ and assume that $P(k)$ is true. So we assume that $(1+m)^{k+1} > 1+(k+1)m$. (We want to show that $(1+m)^{k+2} > 1+(k+2)m$, that is want to show that $P(k+1)$ is true).

Now, $(1+m)^{k+2} = (1+m)(1+m)^{k+1}$

$> (1+m)[1+(k+1)m]$, by the induction hypothesis

$= 1+(k+1)m+m+(k+1)m^2$

$= 1+(k+2)m+(k+1)m^2$

$> 1+(k+2)m$, because $(k+1)m^2 > 0$

as desired.

So the result follows by induction on n. □

Ex: Prove that $|P(A)| = 2^{|A|}$ for any finite set A.

Proof: We will prove that "for any $n \in \mathbb{N}$, any set with cardinality n has 2^n subsets". The proof will be by induction on n.

For $n=0$, any set with cardinality 0 must be the empty set $\emptyset$ and $P(\emptyset) = \{\emptyset\}$ and so $\emptyset$ has $1 = 2^0$ subsets. So the statement is true for $n=0$.

Let $k \in \mathbb{N}$. Assume that any set with cardinality k has 2^k subsets. Let B be any set with cardinality $k+1$. We want to show that B has 2^{k+1} subsets.

As $k+1 > 0$, $B \neq \emptyset$ and so B has an element $b \in B$. Then, for any subset X of B, either $b \in X$ or $b \notin X$, but not both. So

$$P(B) = \{Y \subseteq B \mid b \in Y\} \cup \{Y \subseteq B \mid b \notin Y\}, \text{ (disjoint union)}$$

Note that the above two sets are disjoint. So

$$|P(B)| = |\{Y \subseteq B \mid b \in Y\}| + |\{Y \subseteq B \mid b \notin Y\}|$$

$$= |\{Z \cup \{b\} \mid Z \subseteq B - \{b\}\}| \qquad = |\{Z \mid Z \subseteq B - \{b\}\}|$$

$$= |P(B - \{b\})| \qquad = |P(B - \{b\})|$$

($B - \{b\}$ has k elements)

$$= 2^k \qquad = 2^k \quad \leftarrow \text{by induction hypothesis}$$

$$= 2^k + 2^k = 2^{k+1}, \text{ as desired.}$$

So the result follows by induction.

□

Sometimes justifying that "P(k+1) is true" by using the induction hypothesis that "P(k) is true" may not be easy, but may be very easy if we assume that some P( ) of previous natural numbers are all true. For instance, we want to show that $F_n < 2^n$ for all $n \in \mathbb{N}^+$ where F_n are the Fibonacci numbers, defined by the recursive formula $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Letting $P(n): F_n < 2^n$, let us try to prove it by induction. In the induction step, we assume $F_k < 2^k$ (i.e., P(k) is true) and want to show that $F_{k+1} < 2^{k+1}$ (i.e., P(k+1) is true). From the recursive formula, we write

$$F_{k+1} = F_k + F_{k-1} \underset{\text{ind. hypot. "P(k) is true"}}{<} 2^k + F_{k-1}$$

It now should be clear that if we further assume that P(k-1) is true then $F_{k-1} < 2^{k-1}$, and the above inequality becomes

$$F_{k+1} < 2^k + F_{k-1} \underset{\text{by the assumption that "P(k-1) is true"}}{<} 2^k + 2^{k-1} \overset{2^{k-1} \leq 2^k}{\leq} 2^k + 2^k < 2^{k+1}$$

as desired. So, in this example, justifying that "$P(k) \to P(k+1)$ is true" is not easy, but justifying that "$P(k-1) \wedge P(k) \to P(k+1)$ is true" is very easy.

The above is a part of an example of a proof by strong induction.

"The principal of induction" and "the principal of strong induction" are logically equivalent, and both can be used to prove theorems involving assertions indexed by natural numbers.

Fact: $(\forall n \in \mathbb{N}^+) P(n) \equiv P(1) \wedge (\forall k \in \mathbb{N}^+)\big(P(1) \wedge P(2) \wedge \cdots \wedge P(k) \to P(k+1)\big)$

Proof: Exercise

—o—