Discrete Structures

September 28, 2023

Contents

Chapter 1

Sentential Logic

1.1 Deductive Reasoning and Logical Connectives

Convention 1.1. Here are our first three *connective symbols* and the words they stand for:

Symbol	Meaning
$\vee$	or
$\wedge$	and
$\neg$	not

Thus, if P and Q standard for two statements, then we'll write

Logical forms	Meaning 1	Meaning 2
$P \vee Q$	P or Q	disjunction of P and Q
$P \wedge Q$	P and Q	conjunction of P and Q
$\neg P$	not P	negation of P

Example 1.2. For the following 3 examples, assume the premises are true, then the conclusion is true as well.

(a) *premises:*

It will either rain (P) or snow tomorrow (Q). In other words, $P \vee Q$
It's too warm for snow (not Q). In other words, $\neg Q$

conclusion:

Therefore, it will rain (P).

(b) *premises:*

If today is Sunday, then I don't have to go to work today.
Today is Sunday.

conclusion:

Therefore, I don't have to go to work today.

(c) *premises:*

I will go to work either tomorrow (P) or today (Q). In other words, $P \vee Q$
I am going to stay home today (H). (H implies $\neg Q$, but notices that $H \neq \neg Q$.)

conclusion:

Therefore, I will go to work tomorrow (P).

Remark. In Example (c), If one of the premises "I will go to work either tomorrow or today" is false, i.e., I won't go to work both tomorrow and today. The conclusion becomes false as well.

Example 1.3. Here is an example of an invalid deductive argument.

Either the butler is guilty or the maid is guilty.

Either the maid is guilty or the cook is guilty.

Therefore, either the butler is guilty or the cook is guilty?

The argument has this form:

(a) B or M,

(b) M or C.

(c) Therefore, B or C? No. it could be M.

Example 1.4. Analyze the logical forms of the following statements:

(a) Either John went to the store, or we're out of eggs.

Let P stand for the statement "John went to the store" and Q stand for "We are out of eggs", then this statement could be represented symbolically as $P \vee Q$.

(b) Joe is going to leave home and not come back.

Method 1: Let P stand for the statement "Joe is going to leave home" and Q stand for the statement "Joe is not going to come back", then we could represent this statement symbolically as $P \wedge Q$.

Method 2: Let P stand for the statement "Joe is going to leave home" and R stand for the statement "Joe is going to come back", then we could represent this statement symbolically as $P \wedge \neg R$.

(c) Either Bill is at work and Jane isn't, or Jane is at work and Bill isn't.

Let B stand for the statement "Bill is at work" and J stand J for "Jane is work", then we could represent this statement symbolically as $(B \wedge \neg J) \vee (J \wedge \neg B)$. Note that the priority: $\neg > \wedge > \vee$, that's why we add parentheses when we form the disjunction of $B \wedge \neg J$ and $J \wedge \neg B$, and why we don't need to add parentheses for $\neg J$ and $\neg B$.

Example 1.5. What English sentences are represented by the following expressions?

(a) $(\neg S \wedge L) \vee S$, where S stands for "John is stupid" and L stands for "John is lazy".

Either John isn't stupid and he is lazy, or he's stupid.

(b) $\neg S \wedge (L \vee S)$, where S and L have the same meaning as before.

John isn't stupid, and either he's lazy or he's stupid.

(c) $\neg(S \wedge L) \vee S$, with S and L still as before.

Either John isn't **both** stupid and lazy, or John is stupid.

1.2 True Tables

Assume that P, Q, and R stand for statements that are either true or false.

Proposition 1.6. (a) The *true table* for the formula P and Q.

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

Figure 1

Thus, $P \wedge Q$ is true if and only if both P and Q are true.

(b) The *true table* for the formula $\neg P$.

P	$\neg P$
F	T
T	F

Figure 2

Thus, $\neg P$ is true if and only if P is false.

(c) The *true table* for the formula $P \vee Q$.

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

Figure 3

Thus, $P \vee Q$ is true if and only if either P or Q is true.

Example 1.7. Make a true table for the formula $\neg(P \vee \neg Q)$.

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

Example 1.8. Make a true table for the formula $\neg(P \wedge \neg Q) \vee \neg R$.

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

Remark. If a formula contain n different letter, its true table will have 2^n lines.

Definition 1.9. We say an argument is *valid* if the premises are all true, then the conclusion must be also true.

Example 1.10. Determine whether the following argument is valid.

premises:

It will either rain (P) or snow tomorrow (Q). In other words, $P \vee Q$
It's too warm for snow (not Q). In other words, $\neg Q$

conclusion:

Therefore, it will rain (P).

The argument is represented symbolically as follows:

$$\begin{array}{ll} P \vee Q & \\ \neg Q & \\ \hline \therefore P & \text{(The symbol } \therefore \text{ means } \textit{therefore}.) \end{array}$$

Looking at Figure 4 we see that only row of the table in which both premises come out true is row three, and in this row the conclusion is also true. Thus, the true table confirms that if the premises are all true, the conclusion must also be true, so the argument is valid.

		Premises		Conclusion
P	Q	$P \vee Q$	$\neg Q$	P
F	F	F	T	F
F	T	T	F	F
T	F	T	T	T
T	T	T	F	T

Figure 4

Example 1.11. Determine whether the following arguments are valid.

(a) *premises:*

Either John isn't stupid and he is lazy, or he's stupid.
John is stupid.

conclusion:

Therefore, John isn't lazy.

Let S stand for the statement "John is stupid" and L stand for "John is lazy". Then the argument has the form:

$$\begin{array}{l} (\neg S \wedge L) \vee S \\ S \\ \hline \therefore \neg L \end{array}$$

Here is the truth table for the premises and conclusion:

		Premises		Conclusion
S	L	$(\neg S \wedge L) \vee S$	S	$\neg L$
F	F	F	F	T
F	T	T	F	F
T	F	T	T	T
T	T	T	T	F

Figure 5

Both premises are true in lines three and four of this table. The conclusion is also true in line three, but it is false in line four. Thus, it is possible for both premises to be true and the conclusion false, so the argument is invalid.

(b) *premises:*

The butler and the cook are not both innocent.
Either the butler is lying or the cook is innocent.

conclusion:

Therefore, the butler is either lying or guilty.

Let B stand for the statement "The butler is innocent", C for the statement "The cook is innocent", and L for the statement "The butler is lying". Then the argument has the form:

$$\begin{array}{l} \neg(B \wedge C) \\ L \vee C \\ \hline \therefore L \vee \neg B \end{array}$$

Here is the truth table for the premises and conclusion:

			Premises		Conclusion
B	C	L	$\neg(B \wedge C)$	$L \vee C$	$L \vee \neg B$
F	F	F	T	F	T
F	F	T	T	T	T
F	T	F	T	T	T
F	T	T	T	T	T
T	F	F	T	F	F
T	F	T	T	T	T
T	T	F	F	T	F
T	T	T	F	T	T

Figure 6

The premises are both true only in lines two, three, four, and six, and in each of these cases the conclusion is true as well. Therefore, the argument is valid.

We use "$\longleftrightarrow$" to denote the equivalence.

DeMorgan's laws

$$\neg(P \wedge Q) \longleftrightarrow \neg P \vee \neg Q$$
$$\neg(P \vee Q) \longleftrightarrow \neg P \wedge \neg Q$$

Commutative laws

$$P \wedge Q \longleftrightarrow Q \wedge P$$
$$P \vee Q \longleftrightarrow Q \vee P$$

Associative laws

$$P \wedge (Q \wedge R) \longleftrightarrow (P \wedge Q) \wedge R$$
$$P \vee (Q \vee R) \longleftrightarrow (P \vee Q) \vee R$$

Idempotent's laws

$$P \wedge P \longleftrightarrow P$$
$$P \vee P \longleftrightarrow P$$

Distributive laws

$$P \wedge (Q \vee R) \longleftrightarrow (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) \longleftrightarrow (P \vee Q) \wedge (P \vee R)$$

Absorption laws

$$P \vee (P \wedge Q) \longleftrightarrow P$$
$$P \wedge (P \vee Q) \longleftrightarrow P$$

Double Negation law

$$\neg\neg P \longleftrightarrow P$$

Remark. If you have interest, you may use the truth table to prove these laws. For example,

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

The third and fourth column in this table are identical, so $\neg(P \wedge Q) = \neg P \vee \neg Q$.

Example 1.12. Find simpler formulas equivalent to these formulas:

(a)

$$\begin{aligned} \neg(P \vee \neg Q) &\longleftrightarrow \neg P \wedge \neg\neg Q && \text{(DeMorgan's law)} \\ &\longleftrightarrow \neg P \wedge Q && \text{(Double negation law)} \end{aligned}$$

(b)

$$\begin{aligned} \neg(Q \wedge \neg P) \vee P &\longleftrightarrow (\neg Q \vee \neg\neg P) \vee P && \text{(DeMorgan's law)} \\ &\longleftrightarrow (\neg Q \vee P) \vee P && \text{(double negation law)} \\ &\longleftrightarrow \neg Q \vee (P \vee P) && \text{(associative law)} \\ &\longleftrightarrow \neg Q \vee P && \text{(idempotent law)} \end{aligned}$$

Fact 1.13. Use the truth table to check that

$$\neg P \vee P \longleftrightarrow \mathrm{T},$$

$$\neg P \wedge P \longleftrightarrow \mathrm{F}.$$

Formulas that are always true are called *tautologies*. Formulas that are always false are called *contradictions*. We use T to denote a tautology and F denote a contradiction.

Tautology laws

$$P \wedge \mathrm{T} \longleftrightarrow P,$$

$$P \vee \mathrm{T} \longleftrightarrow \mathrm{T},$$

$$\neg \mathrm{T} \longleftrightarrow \mathrm{F}.$$

Contradiction laws

$$P \vee \mathrm{F} \longleftrightarrow P,$$

$$P \wedge \mathrm{F} \longleftrightarrow \mathrm{F},$$

$$\neg \mathrm{F} \longleftrightarrow \mathrm{T}.$$

These laws can be deduced from Proposition 1.6.

Example 1.14. (a)

$$\begin{aligned} P \vee (Q \vee \neg P) &\longleftrightarrow P \vee (\neg P \vee Q) && \text{(commutative law)} \\ &\longleftrightarrow (P \vee \neg P) \vee Q && \text{(associative law)} \\ &\longleftrightarrow \mathrm{T} \vee Q && \text{(tautology law)} \\ &\longleftrightarrow \mathrm{T}. \end{aligned}$$

So it is a tautologie.

(b)

$$\begin{aligned} P \wedge \neg(Q \vee \neg Q) &\longleftrightarrow P \wedge \neg \mathrm{T} \\ &\longleftrightarrow P \wedge \mathrm{F} && \text{(tautology law)} \\ &\longleftrightarrow \mathrm{F}. \end{aligned}$$

So it is a contradiction.

(c)

$$\begin{aligned} P \vee \neg(Q \vee \neg Q) &\longleftrightarrow P \vee \neg \mathrm{T} \\ &\longleftrightarrow P \vee \mathrm{F} && \text{(tautology law)} \\ &\longleftrightarrow P. && \text{(contradiction law)} \end{aligned}$$

Example 1.15. Find simpler formulas equivalent to these formulas:

(a)

$$\begin{aligned} P \vee (Q \wedge \neg P) &\longleftrightarrow (P \vee Q) \wedge (P \vee \neg P) \\ &\longleftrightarrow (P \vee Q) \wedge \mathrm{T} \\ &\longleftrightarrow P \vee Q. \end{aligned}$$

(b)

$$\begin{aligned} \neg(P \vee (Q \wedge \neg R)) \wedge Q &\longleftrightarrow (\neg P \wedge \neg(Q \wedge \neg R)) \wedge Q \\ &\longleftrightarrow (\neg P \wedge (\neg Q \vee \neg\neg R)) \wedge Q \\ &\longleftrightarrow (\neg P \wedge (\neg Q \vee R)) \wedge Q \\ &\longleftrightarrow \neg P \wedge ((\neg Q \vee R) \wedge Q) \\ &\longleftrightarrow \neg P \wedge (Q \wedge (\neg Q \vee R)) \\ &\longleftrightarrow \neg P \wedge ((Q \wedge \neg Q) \vee (Q \wedge R)) \\ &\longleftrightarrow \neg P \wedge (\mathrm{T} \vee (Q \wedge R)) \\ &\longleftrightarrow \neg P \wedge (Q \wedge R) \\ &\longleftrightarrow \neg P \wedge Q \wedge R. \end{aligned}$$

1.3 Variables and Sets

Definition 1.16. Objects that are represented by letters are called *variables.*

Notation 1.17. (a) If a statment P contains one variable x, we use $P(x)$ to stand for that statement P.

(b) If a statement D contains two variables p, q, we use $D(p, q)$ stand for that statement D.

Example 1.18. (a) For example, we could let $P(x)$ stand for the statement "x is a prime number". Then $P(7)$ would represent the statement "7 is a prime number".

(b) We might represent the statement "p is divisible by q" by $D(p, q)$. In this case, $D(12, 4)$ would mean "12 is divisible by 4".

Example 1.19. Analyze the logical form of the following statements:

(a) x is a prime number, and either y or z is divisible by x.

Let $P(x)$ stand for "x is a prime number" and $D(y, x)$ for "y is divisible by x". Then $D(z, x)$ would mean "z is divisible by x", and so the entire statement would be $P(x) \wedge (D(y, x) \vee D(z, x))$.

(b) x is a man and y is a woman and x likes y, but y doesn't like x.

Let $M(x)$ stand for "x is a man", $W(y)$ for "y is a woman", and $L(x, y)$ for "x likes y". Then $L(y, x)$ would mean "y likes x". The entire statement would then be $M(x) \wedge W(y) \wedge L(x, y) \wedge \neg L(y, x)$.

Recall 1.20. A *set* is a collection of objects. The objects in the collection are called the *elements* of the fspa. We usually list elements of a set between braces. For example, $\{3, 7, 14\}$ is the set whose elements are the threes numbers $3, 7, 14$. We use the symbol $\in$ to mean *is an element of.* For example, if $A = \{3, 7, 14\}$, then we could write $7 \in A$ to say that 7 is an element of A. To say that 11 is not an element of A, we write $11 \notin A$.

Note 1.21. The elements in a set have no order, for example, $\{3, 7, 14\} = \{14, 3, 7\} = \{3, 7, 14, 7\}$.

Example 1.22. If a set is large, we can list a few elements then add an ellipsis ($\dots$) after them, if it is clear how the list should be continued. For example, if we write $B = \{2, 3, 5, 7, 11, 13, 17, \dots\}$, you know that the B represents all the prime numbers, and the number after 17 is 23.

Actually, it is better to define such a set by spelling out the pattern that determines the elements of the set. In this case we could be explicit by defining B as follows:

$$B = \{x \mid x \text{ is a prime number}\}.$$

This is read "$B =$ the set of all x such that x is a prime number".

Example 1.23. (a)

$$E = \{2, 4, 6, 8, \dots\} = \{n \mid n \text{ is a positive even integer}\}.$$

(b)

$$\begin{aligned} P &= \{\text{George Washington, John Adams, Thomas Jefferson, James Madison}, \dots\} \\ &= \{z \mid z \text{ was a president of the United States}\}. \end{aligned}$$

Definition 1.24. The *truth set* of a statement $P(x)$ is the set of all values of x that make the statement $P(x)$ true. In other words,

$$\text{True set of } P(x) = \{x \mid P(x)\}.$$

Example 1.25. What are the truth sets of the following statement?

(a) Shakespeare wrote x.

$$\{x \mid \text{Shakespeare wrote } x\} = \{\text{Hamlet,Macbeth,Twelfth Night}, \dots\}.$$

(b) n is an even prime number.

$$\{n \mid n \text{ is an even prime number}\} = \{2\}.$$

Note that $2 \neq \{2\}$.

Note 1.26. If A is the true set of $P(x)$, namely, $A = \{x \mid P(x)\}$, then $y \in A$ means that $P(y)$, and $y \notin \{x \mid P(x)\}$ means that $\neg P(y)$.

Example 1.27. (a) $y \in \{x \mid x \text{ is divisible by } w\}$ means that y is divisible by w.

(b) $a + b \notin \{x \mid x \text{ is an even number}\}$ means that $a + b$ is not an even number.

(c) $2 \in \{w \mid 6 \notin \{x \mid x \text{ is divisible by } w\}\}$ means that $6 \notin \{x \mid x \text{ is disible by } 2\}$, namely, 6 is not divisible by 2, which is a false statement.

Definition 1.28. In the statement $y \in \{x \mid P(x)\}$, y is a *free variable*, whereas x is *bound* variable (or *dummy* variable).

Example 1.29.

$$5 \notin \{x \mid x^2 < 9\}.$$
$$1.1 \in \{y \mid y^2 < 9\}.$$

Notation 1.30.

$$\begin{aligned}
\mathbb{R} &= \{x \mid x \text{ is a real number}\}.\\
\mathbb{Q} &= \{x \mid x \text{ is a rational number}\}.\\
\mathbb{Z} &= \{x \mid x \text{ is an integer}\}.\\
\mathbb{N} &= \{x \mid x \text{ is a natural number}\} = \{0, 1, 2, 3, \dots\}.
\end{aligned}$$

Notation 1.31.

$$\begin{aligned}
\mathbb{R}^+ &= \{x \mid x \text{ is a positive real number}\}.\\
\mathbb{Q}^+ &= \{x \mid x \text{ is a positive rational number}\}.\\
\mathbb{Z}^+ &= \{x \mid x \text{ is a positive integer}\}.\\
\mathbb{R}^- &= \{x \mid x \text{ is a negative real number}\}.\\
\mathbb{Q}^- &= \{x \mid x \text{ is a negative rational number}\}.\\
\mathbb{Z}^- &= \{x \mid x \text{ is a negative integer}\}.
\end{aligned}$$

Definition 1.32. We read $\{x \in U \mid P(x)\}$ to mean that "the set of all x in U such that $P(x)$".

Example 1.33.

$$\begin{aligned}\{x \in \mathbb{Z} \mid x^2 < 9\} &= \{-2, -1, 0, 1, 2\}.\\ \{x \in \mathbb{N} \mid x^2 < 9\} &= \{0, 1, 2\}.\end{aligned}$$

Remark. In general, $y \in \{x \in A \mid P(x)\}$ means the same thing as $y \in A \wedge P(y)$.

Example 1.34.

$$\begin{aligned}\{x \in \mathbb{R} \mid x^2 \geqslant 0\} &= \mathbb{R}.\\ \{x \in \mathbb{Z} \mid x \neq x\} &= \emptyset = \{\}.\end{aligned}$$

Remark.

$$\{\emptyset\} \neq \emptyset,$$

where the first is a set with one element, whereas the second is a set with no elements.

1.4 Operations on Sets

Definition 1.35. The *intersection* of two sets A and B is the set $A \cap B$ defined as follows:

$$\begin{aligned}A \cap B &= \{x \mid x \in A \text{ and } x \in B\}\\ &\longleftrightarrow \{x \mid x \in A \wedge x \in B\}.\end{aligned}$$

The *union* of A and B is the set $A \cup B$ defined as follows:

$$\begin{aligned}A \cup B &= \{x \mid x \in A \text{ or } x \in B\}\\ &\longleftrightarrow \{x \mid x \in A \vee x \in B\}.\end{aligned}$$

The *difference* of A and B is the set $A \smallsetminus B$ defined as follows:

$$\begin{aligned}A \smallsetminus B &= \{x \mid x \in A \text{ and } x \notin B\}\\ &\longleftrightarrow \{x \mid x \in A \wedge x \notin B\}\\ &\longleftrightarrow \{x \mid x \in A \wedge \neg(x \in B)\}.\end{aligned}$$

Example 1.36. Suppose $A = \{1, 2, 3, 4, 5\}$ and $B = \{2, 4, 6, 8, 10\}$. List the elements of the following set:

(a)

$$A \cap B = \{2, 4\}.$$

(b)

$$A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}.$$

(c)

$$A \smallsetminus B = \{1, 3, 5\}.$$

(d)

$$(A \cup B) \setminus (A \cap B) = \{1, 3, 5, 6, 8, 10\}.$$

(e) Since $B \setminus A = \{6, 8, 10\}$,

$$(A \setminus B) \cup (B \setminus A) = \{1, 3, 5, 6, 8, 10\}.$$

Example 1.37. Suppose $A = \{x \mid x \text{ is a man}\}$ and $B = \{x \mid x \text{ has brown hair}\}$. What are $A \cap B$, $A \cup B$ and $A \setminus B$?

$$\begin{aligned} A \cap B &= \{x \mid x \in A \text{ and } x \in B\} \\ &= \{x \mid x \text{ is a man and } x \text{ has brown hair}\}. \end{aligned}$$

$$\begin{aligned} A \cup B &= \{x \mid x \in A \text{ or } x \in B\} \\ &= \{x \mid x \text{ is a man or } x \text{ has brown hair}\}. \end{aligned}$$

$$\begin{aligned} A \setminus B &= \{x \mid x \in A \text{ and } x \in B\} \\ &= \{x \mid x \text{ is a man or } x \text{ does not have brown hair}\}. \end{aligned}$$

Sometimes, it is helpful when working with operations on sets to draw pictures of the results of these operations. One way to do this is with diagrams like that in Figure 1. This is called a *Venn diagram.*

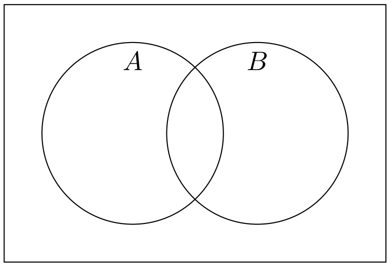
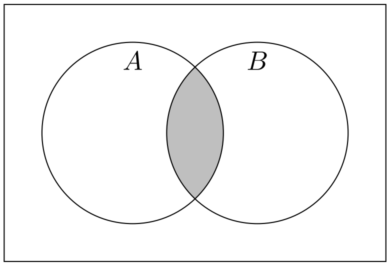
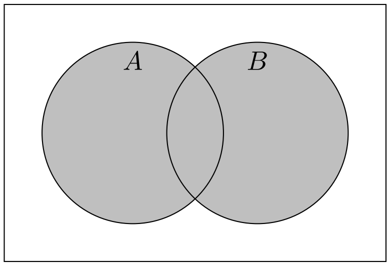


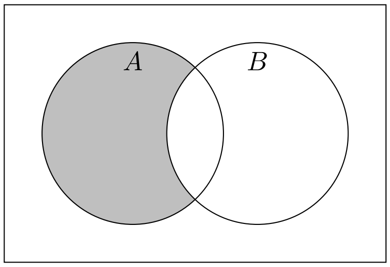
Figure 1



$A \cap B$
Figure 2



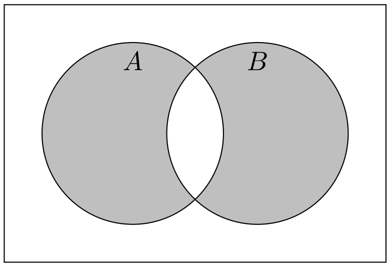
$A \cup B$
Figure 3



$A \smallsetminus B$
Figure 4

From Venn diagram, you can see that

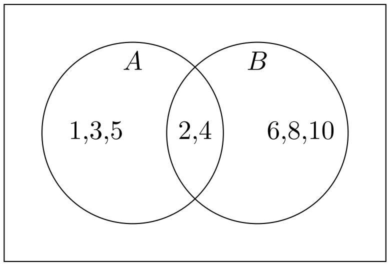
$$(A \cup B) \smallsetminus (A \cap B) = (A \smallsetminus B) \cup (B \smallsetminus A).$$



Definition 1.38. Define the *symmetric difference* $A \triangle B$ of A and B by

$$A \triangle B = (A \cup B) \smallsetminus (A \cap B) = (A \smallsetminus B) \cup (B \smallsetminus A).$$

Example 1.39. In Example 1.36, $A = \{1, 2, 3, 4, 5\}$ and $B = \{2, 4, 6, 8, 10\}$.



Then

$$A \triangle B = \{1, 3, 5, 6, 8, 10\}.$$

Remark. The set theory operations are $\cap$, $\cup$, and $\smallsetminus$. The logical connectives are $\wedge$, $\vee$ and $\neg$.

Notation 1.40. (a) $x \in A \cap B$ means that $x \in A \wedge x \in B$.

(b) $x \in A \cup B$ means that $x \in A \vee x \in B$.

(c) $x \in A \smallsetminus B$ means that $x \in A \wedge x \notin B$, or in other words, $x \in A \wedge \neg(x \in B)$.

Example 1.41. (a)

$$\begin{aligned} x \in A \cap (B \cup C) &\longleftrightarrow x \in A \wedge x \in (B \cup C) \\ &\longleftrightarrow x \in A \wedge (x \in B \vee x \in C). \end{aligned}$$

(b)

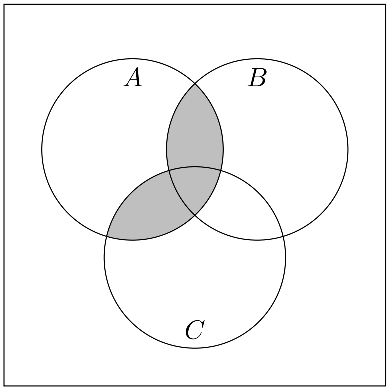
$$\begin{aligned} x \in A \smallsetminus (B \cap C) &\longleftrightarrow x \in A \wedge \neg(x \in B \cap C) \\ &\longleftrightarrow x \in A \wedge \neg(x \in B \wedge x \in C). \end{aligned}$$

(c)

$$\begin{aligned} x \in (A \cap B) \cup (A \cap C) &\longleftrightarrow (x \in A \cap B) \vee (x \in A \cap C) \\ &\longleftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C). \end{aligned}$$

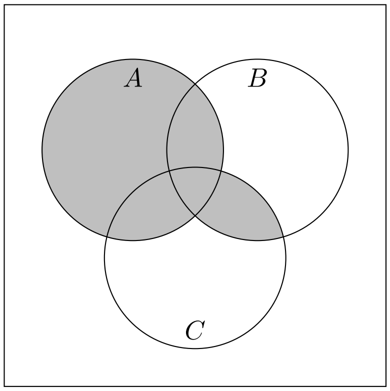
Remark. From the Venn diagram, you can see the distributive laws for **sets** holds:

(a)



$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

(b)



$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Note 1.42. We rarely create Venn diagrams for more than three sets.

Proposition 1.43. For any sets A, B and C,

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

Proof.

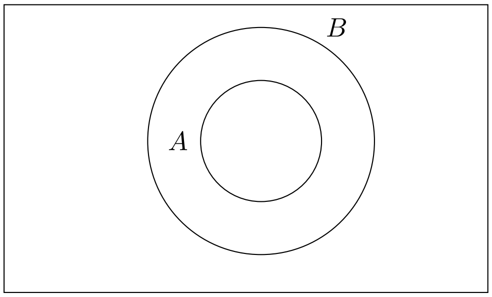
$$\begin{aligned} x \in A \setminus (B \cap C) &\longleftrightarrow x \in A \land \neg(x \in B \land x \in C) \\ &\longleftrightarrow x \in A \land (x \notin B \lor x \notin C) \\ &\longleftrightarrow (x \in A \land x \notin B) \lor (x \in A \land x \notin C) \\ &\longleftrightarrow (x \in A \setminus B) \lor (x \in A \setminus C) \\ &\longleftrightarrow x \in (A \setminus B) \cup (A \setminus C). \end{aligned}$$

□

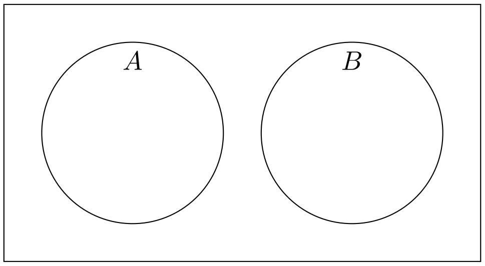
Definition 1.44. Suppose A and B are sets. We will say that A is a *subset* of B if every element of A is also an element of B. We write $A \subseteq B$ to mean that A is a subset of B. A and B are said to be *disjoint* if they have no elements in common, or in other words $A \cap B = \emptyset$.

Example 1.45. Suppose $A = \{\text{red}, \text{green}\}$, $B = \{\text{red,yellow,green,purple}\}$, and $C = \{\text{blue, purple}\}$. Then two elements of A, red and green, are both also in B, and theorefore $A \subseteq B$. Also, $A \cap C = \emptyset$, aos A and C are disjoint.

Remark. We draw a Venn diagram for subsets and disjoint sets.



$A \subseteq B$



$A \cap B = \emptyset$

The following fact and theorem can be easily seen from the Venn diagram.

Fact 1.46.

$$(A \cap B) \cap (A \smallsetminus B) = \emptyset.$$

Theorem 1.47. *For any sets A and B,*

$$(A \cup B) \smallsetminus B \subseteq A.$$

Proof. Let $x \in (A \cup B) \smallsetminus B$. It is enough to show that $x \in A$. Note that

$$\begin{aligned} x \in (A \cup B) \smallsetminus B &\longrightarrow (x \in A \cup B) \wedge (x \notin B) \\ &\longrightarrow (x \in A \vee x \in B) \wedge x \notin B \\ &\longrightarrow x \in A. \end{aligned}$$ □

1.5 The Conditional and Biconditional Connectives

Notation 1.48. We write $P \to Q$ to represent the statement "If P then Q". This statement is sometimes called a *conditional* statement, with P as its *antecedent* and Q as its *consequent.*

Example 1.49. We analyze the logical form of the following statement:

premises:

If today is Sunday, then I don't have to go to work today.
Today is Sunday.

conclusion:

Therefore, I don't have to go to work today.

Let P stand for the statement "Today is Sunday" and Q for the statement "I don't have to go to work today", then the logical form of the argument would be

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

Out analysis of the new connective → should lead to the conclusion that this argument is valid.

Example 1.50. Analyze the logical form of the following statements:

(a) If it's raining and I don't have my umbrella, then I'll get wet.

Let R stand for the statement "It is raining", U for "I have my umbrella", and W for "I'll get wet". Then it would be represented by the formula $(R \wedge \neg U) \to W$.

(b) If Mary did her homework, then the teacher won't collect it, and if she didn't, then he'll ask her to do it on the board.

Let H stand for "Mary did her homework", C for "The teacher will collect it", and B for "The teacher will ask Mary to do the homework on the board". Then it means $(H \to \neg C) \wedge (\neg H \to B)$.

Example 1.51. The truth table for the formula $P \to Q$.

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

Figure 1

Because $P \to Q$ has the same true table as $\neg P \vee Q$,

$$P \to Q \longleftrightarrow \neg P \vee Q.$$

This implies that (Substituting P for $\neg P$)

$$\neg P \to Q \longleftrightarrow P \vee Q.$$

Conditional laws

$$P \to Q \longleftrightarrow \neg P \vee Q \longleftrightarrow \neg(P \wedge \neg Q).$$

Definition 1.52. The formula $Q \to P$ is called the *converse* of $P \to Q$.

Remark.

$$P \to Q \not\longleftrightarrow Q \to P.$$

Contrapositive laws

$$P \to Q \longleftrightarrow \neg Q \to \neg P.$$

Example 1.53. Which of the following statement are equivalent?

(a) If it's either raining or snowing, then the game has been canceled.

(b) If the game hasn't been canceled, then it's not raining and it's not snowing.

(c) If the same has been canceled, then it's either raining or snowing.

(d) If it's raining then the game has been canceled, and if it's snowing then the game has been canceled.

(e) If it's neither raining nor snowing, then the game hasn't been canceled.

Let R stand for the statement "It's raining", S for "It's snowing", and C for "The game has been canceled". Then we translate all of the statements into the notation of logic:

(a) $(R \vee S) \to C$.

(b) $\neg C \to (\neg R \wedge \neg S)$.

(c) $C \to (R \vee S)$.

(d) $(R \to C) \wedge (S \to C)$.

(e) $\neg(R \vee S) \to \neg C$.

Thus, (a) = (b) because by the contrapositive law

$$\begin{aligned}(R \vee S) \to C &\longleftrightarrow \neg C \to \neg(R \vee S)\\ &\longleftrightarrow \neg C \to (\neg R \wedge \neg S).\end{aligned}$$

(a) $\longleftrightarrow$ (d) because

$$\begin{aligned}(R \to C) \wedge (S \to C) &\longleftrightarrow (\neg R \vee C) \wedge (\neg S \vee C)\\ &\longleftrightarrow (\neg R \wedge \neg S) \vee C\\ &\longleftrightarrow \neg(R \vee S) \vee C\\ &\longleftrightarrow (R \vee S) \to C.\end{aligned}$$

(c) $\not\longleftrightarrow$ (a) because (c) is converse of (a). (c) $\longleftrightarrow$ (e) by the contrapositive law. Therefore,

$$\text{(a)} \longleftrightarrow \text{(b)} \longleftrightarrow \text{(d)} \not\longleftrightarrow \text{(c)} \longleftrightarrow \text{(e)}.$$

Remark. The ways to express $P \to Q$:

P implies Q.

Q, if P.

P only if Q. (This is eqivalent to $\neg Q \to \neg P$, which is equivalent $P \to Q$).

P is a sufficient condition for Q. (The truth of P suffices to guarantee the truth of Q.)

Q is a necessary condition for P. (In order for P to be true, it is necessary for Q to be true also.)

Example 1.54. Analyze the logical forms of the following statements:

(a) If at least ten people are there, then the lecture will be given.

(b) The lecture will be given only if at least ten people are there.

(c) The lecture will be given if at least ten people are there.

(d) Having at least ten people there is a sufficient condition for the lecture being given.

(e) Having at least ten people there is a necessary condition for the lecture being given.

Let T stand for the statement "At least ten people are there" and L for "The lecture will be given".

(a) $T \to L$.

(b) $L \to T$.

(c) $T \to L$.

(d) $T \to L$.

(e) $L \to T$.

Definition 1.55. Define $P \longleftrightarrow Q$ to be

$$(P \to Q) \wedge (Q \to P).$$

Example 1.56. Using the definition of $P \longleftrightarrow Q$, we get the truth table for it:

P	Q	$P \longleftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Figure 2

Remark. Because $Q \to P$ can be written "P if Q" and $P \to Q$ can be written "P only if Q", $P \longleftrightarrow Q$ means "P if Q and P only if Q", and this is often written "P if and only if Q".

We use the abbreviation *iff* for the phrase *if and only if.* Thus, $P \longleftrightarrow Q$ is usually written "P iff Q". Another statement that means $P \longleftrightarrow Q$ is "P is a necessary and sufficient condition for Q".

Example 1.57. Analyze the logical forms of the following statements:

(a) The game will be canceled iff it's either raining or snowing.

Let C stand for "The game will be canceled", R for "It's raining', and S for "It's snowing". Then the statement would be represented by $C \longleftrightarrow (R \vee S)$.

(b) Having at least ten people there is a necessary and sufficient condition for the lecture being given.

Let T stand for "There are at least ten people there" and L for "The lecture will be given". Then the statement means $T \longleftrightarrow L$.

(c) If John went to the store then we have some eggs, and if he didn't then we don't.

Let S stand for "John went to the store" and E for "We have some eggs". Then the statement means $(S \to E) \wedge (\neg S \to \neg E)$, which is equivalent to $(S \to E) \wedge (E \to \neg S)$ by the contrapositive law, which is equivalent to $S \longleftrightarrow E$ by definition.

Chapter 2

Quantificational Logic

2.1 Quantifiers

Notation 2.1. To say that $P(x)$ is true for every value of x in the universe of discourse U, we will write $\forall x\, P(x)$. This is read "For all x, $P(x)$". The symbol $\forall$ is called the *universal quantifier.*

You could also think of the statement $\forall x P(x)$ as saying

$$\{x \mid P(x)\} = U,$$

where U is the whole universe.

Notation 2.2. To say that there is at least one value of x in the universe for which $P(x)$ is true, we will write $\exists x\, P(x)$. This is read "There exists an x such that $P(x)$". The symbol $\exists$ is called the *existential quantifier.*

Example 2.3. What do the following formulas mean? Are they true or false?

(a) $\forall x\,(x^2 \geqslant 0)$, where the universe of discourse is $\mathbb{R}$.

This means that for every real number x, $x^2 \geqslant 0$. This is true.

(b) $\exists x\,(x^2 - 2x + 3 = 0)$, with universe $\mathbb{R}$.

This means that there is at least one real number x that makes the equation $x^2 - 2x + 3 = 0$ come out true. In other words, the equation has at least one real solution. This is false because $(-2)^2 < 4(3) = 12$.

(c) $\exists x\,(M(x) \wedge B(x))$, where the universe of discourse is the set of all people, $M(x)$ stands for the statement "x is a man", and $B(x)$ means "x has brown hair".

There is at least one people x such that x is a man and x has brown hair. In other words, there is at least one man who has brown hair. This is true.

(d) $\forall x\,(M(x) \to B(x))$, with the same universe and the same meaning for $M(x)$ and $B(x)$.

For every person x, if x is a man, then x has brown hair. In other words, all men have brown hair. This is false.

(e) $\forall x\, L(x, y)$, where the universe is the set of all people, and $L(x, y)$ means "x likes y".

For every person x, x likes y. In other words, everyone likes y. It is either true or false, because it depends on whom y is. In this statement y is a free variable.

Remark. x is a dummy variable in the statement $\forall x\, P(x)$ and $\exists x\, P(x)$. This means $\forall x\, P(x)$ is equivalent to $\forall w\, P(w)$, and $\exists x\, P(x)$ is equivalent to $\exists z\, P(z)$. Also, $\forall x\, L(x, y)$ is equivalent to $\forall w\, L(w, y)$, both of them mean the same thing as "Everyone likes y".

Words such as *everyone*, *someone*, *everything*, or *something* are often used to express the meanings of statements containing quantifiers.

Convention 2.4. As with the symbol $\neg$, we follow the convention that the expressions $\forall x$ and $\exists x$ apply only to the statements that come immediately after them. For example, $\forall x\, P(x) \to Q(x)$ means $(\forall x\, P(x)) \to Q(x)$.

Example 2.5. Analyze the logical forms of the following statements.

(a) Someone didn't do the homework.

Let $H(x)$ stand for the statement "x did the homework". We write this as $\exists x \neg H(x)$.

(b) Everything in that store is either overpriced or poorly made.

Let $S(x)$ stand for "x is in that store", $O(x)$ for "x is overpriced", and $P(x)$ for "x is poorly made".

The answer is $\forall x\, [S(x) \to (O(x) \vee P(x))]$.

(c) Nobody's perfect.

Method 1. This means $\neg$(somebody is perfect), or in other words, $\neg\exists x\, P(x)$, where $P(x)$ stands for "x is perfect".

Method 2. $\forall x \neg P(x)$, where $P(x)$ stands for "x is perfect".

(d) Susan likes everyone who dislike Joe.

It means "If a person dislikes Joe then Susan likes that person". Then we can start by rewriting the given statement as $\forall x$ (if x dislikes Joe then Susan likes x). Let $L(x, y)$ stand for "x likes y", j for Joe and s for Susan. Then the answer is $\forall x\, (\neg L(x, j) \to L(s, x))$.

(e) $A \subseteq B$.

It could be written as $\forall x\, (x \in A \to x \in B)$.

(f) $A \cap B \subseteq B \smallsetminus C$.

It could be written as $\forall x\, (x \in A \cap B \to x \in B \smallsetminus C)$. We can expand this further to get $\forall x\, [(x \in A \wedge x \in B) \to (x \in B \wedge x \notin C)]$.

Example 2.6. Let's look at some examples containing more than one quantifier.

(a) Some students are married.

To be married means to be married to *someone*.

$$\exists x\, (S(x) \wedge \exists y\, M(x, y)),$$

where $S(x)$ stand for "x is a student" and $M(x, y)$ for "x is married to y".

(b) All parents are married.

$$\forall x\,(\exists y\,P(x,y) \to \exists z M(x,z)),$$

where $P(x,y)$ means "x is a parent of y" and $M(x,z)$ means "x is married to z",

Example 2.7. Analyze the logical forms of the following statements.

(a) Everybody in the dorm has a roommate he doesn't like.

This means that $\forall x$ (if x lives in the dorm then x has a roommate he doesn't like).

$$\forall x\,[D(x) \to \exists y\,(R(x,y) \wedge \neg L(x,y))],$$

where $R(x,y)$ stand for x and y are roommate and $L(x,y)$ for x likes y.

(b) Nobody likes a sore loser.

Method 1. This means that $\forall x$ (if x is a sore loser then nobody likes x).

$$\forall x\,(S(x) \to \neg\exists y\,L(y,x)).$$

Method 2. This means that $\forall x$ (if x is a sore loser then everybody dislikes x).

$$\forall x[S(x) \to \forall y \neg L(y,x)].$$

Method 3. This means that $\neg$(Somebody likes a sore loser) $=$ $\neg$(A sore loser is liked by someone).

$$\neg[\exists y(S(y) \wedge \exists x\,L(x,y))].$$

(c) Anyone who has a friend who has the measles will have to be quarantined.

$$\forall x\,(\exists y\,(F(x,y) \wedge M(y)) \to Q(x)),$$

where $F(x,y)$ stand for y is a friend of x, $M(y)$ for "y has the measles", and $Q(x)$ for "x will have to be quarantined".

(d) If anyone in the dorm has a friend who has the measles, then everyone in the dorm will have to be quarantined.

$$\forall x\,[D(x) \wedge \exists y\,(F(x,y) \wedge M(y))] \to \forall z\,(D(z) \to Q(z)).$$

(e) If $A \subseteq B$, then A and $C \setminus B$ are disjoint.

$$(\forall x\,(x \in A \to x \in B)) \to \neg\exists x(x \in A \wedge x \in C \wedge x \notin B).$$

Example 2.8. What do the following statements mean? Are they true or false? The universe of discourse in each case is $\mathbb{N}$, the set of all natural numbers.

(a) $\forall x \exists y\,(x < y)$. T

(b) $\exists y \forall x(x < y)$. F

(c) $\exists x \forall y (x < y)$. F

(d) $\forall y \exists x (x < y)$. F (T if the universe of discourse U is $\mathbb{Z}$ or $\mathbb{R}$)

(e) $\exists x \exists y (x < y)$. T

(f) $\forall x \forall y (x < y)$. F

Example 2.9. What do the following statements mean? Are they true or false? The universe of discourse in each case is $\mathbb{N}$, the set of all natural numbers.

(a) $\forall x \exists y (x \leqslant y)$. T

(b) $\exists y \forall x (x \leqslant y)$. F (Because $\mathbb{N}$ has no maximum)

(c) $\exists x \forall y (x \leqslant y)$. T (Take $x = 0$, 0 is the minimum of $\mathbb{N}$)

(d) $\forall y \exists x (x \leqslant y)$. T (Take $x = y$)

(e) $\exists x \exists y (x \leqslant y)$. T

(f) $\forall x \forall y (x \leqslant y)$. F

2.2 Equivalences Involving Quantifiers

Quantifier Negation laws

$$\neg \exists x\, P(x) \longleftrightarrow \forall x \neg P(x).$$
$$\neg \forall x\, P(x) \longleftrightarrow \exists x \neg P(x).$$

Example 2.10. Negate these statements and then reexpress the results as equivalent positive statements.

(a) $A \subseteq B$. $A \subseteq B$ means $\forall x\, (x \in A \to x \in B)$. To reexpress the negation of this statement as an equivalent positive statement, we reason as follows:

$$\begin{aligned} \neg \forall x\, (x \in A \to x \in B) &\longleftrightarrow \exists x \neg (x \in A \to x \in B) \\ &\longleftrightarrow \exists x \neg (x \notin A \vee x \in B) \\ &\longleftrightarrow \exists x\, (x \in A \wedge x \notin B). \end{aligned}$$

(b) Everyone has a relative he doesn't like.

This statement would be written $\forall x \exists y (R(x,y) \wedge \neg L(x,y))$. Now we negate this and try to find a simpler, equivalent positive statement:

$$\begin{aligned} \neg \forall x \exists y\, (R(x,y) \wedge \neg L(x,y)) &\longleftrightarrow \exists x \neg \exists y\, (R(x,y) \wedge \neg L(x,y)) \\ &\longleftrightarrow \exists x \forall y \neg (R(x,y) \wedge \neg L(x,y)) \\ &\longleftrightarrow \exists x \forall y\, (\neg R(x,y) \vee L(x,y)) \\ &\longleftrightarrow \exists x \forall y\, (R(x,y) \to L(x,y)), \end{aligned}$$

where the first equality follows from the second quantifier negation law with the dummy variable x and the second equality follows from the first quantifier negation law with the dummy variable y.

Remark. Reversing the order of two quantifiers can sometimes change the meaning of a formula. However, if the quantifiers are the same type (both $\forall$ or both $\exists$), then the order can always be switched.

Example 2.11. Consider the formula $\forall x \forall y\, (L(x,y) \to A(x,y))$, where $L(x,y)$ means "x likes y" and $A(x,y)$ means "x admires y". Then this formula saying "For all people x and y", if x likes y, then x admires y.

Remark. The above formula also means that people who like themselves also admire themselves.

Example 2.12. There exists a bigamist. The logical form is

$$\exists x\, (\exists y \exists z\, (M(x,y) \wedge M(x,z) \wedge y \neq z)),$$

where $M(x,y)$ means "x is married to y".

Example 2.13. Analyze the logical forms of the following statements.

(a) All married couples have fights.

$$\forall x \forall y\, (M(x,y) \to F(x,y)),$$

where $M(x,y)$ means "x and y are married to each other" and $F(x,y)$ means "x and y fight with each other".

(b) Everyone likes at least two people.

$$\forall x \exists y \exists z\, (L(x,y) \wedge L(x,z) \wedge y \neq z),$$

where $L(x,y)$ stands for "x likes y".

(c) John likes exactly one person.

$$\exists x\, (L(j,x) \wedge \forall y (y \neq x \to \neg L(j,y))).$$

Notation 2.14. (a) We write $\forall x \in U\, P(x)$ to mean "For all x in U, $P(x)$ is true".

(b) We write $\exists x \in U\, P(x)$ to mean "There exists an x in the universe U such that $P(x)$ is true.".

Example 2.15. We have the following examples.

(a) $\forall x \in \mathbb{R}\, (x \geqslant 0)$. F

(b) $\forall x \in \mathbb{N}\, (x \geqslant 0)$. T

Notation 2.16. We have two kinds of *bounded quantifiers*:

(a) We write $\forall x \in A\, P(x)$ to mean "For all x in A, $P(x)$ is true".

(b) We write $\exists x \in A\, P(x)$ to mean "There exists an x in A such that $P(x)$ is true.".

Example 2.17. We have the following examples.

(a) To say that every positive real number has a square root, we would say

$$\forall x \in \mathbb{R}^+ \exists y \, (y^2 = x).$$

(b) To say that every positive real number has a negative square root, we would say

$$\forall x \in \mathbb{R}^+ \exists y \in \mathbb{R}^- \, (y^2 = x).$$

We could also write it as

$$\forall x > 0 \, \exists y < 0 \, (y^2 = x).$$

Remark.

$$\forall x \in A \, P(x) \text{ is equivalent to } \forall x \, (x \in A \to P(x)).$$

Example 2.18. The logical form $\forall x \, (x \in A \to x \in B)$ of $A \subseteq B$ could also be written as

$$\forall x \in A \, (x \in B).$$

Bounded Quantifier Negation laws

$$\neg \exists x \in A \, P(x) \longleftrightarrow \forall x \in A \neg P(x).$$

$$\neg \forall x \in A \, P(x) \longleftrightarrow \exists x \in A \neg P(x).$$

Let's prove the second bounded quantifier negation law:

Proof.

$$\begin{aligned} \neg \forall x \in A \, P(x) &\longleftrightarrow \neg \forall x \, (x \in A \to P(x)) \\ &\longleftrightarrow \exists x \neg (x \in A \to P(x)) \\ &\longleftrightarrow \exists x \neg (x \notin A \vee P(x)) \\ &\longleftrightarrow \exists x (x \in A \wedge \neg P(x)) \\ &\longleftrightarrow \exists x \in A \neg P(x). \end{aligned}$$

□

Remark. (a) If $A = \emptyset$, then $\exists x \in A \, P(x)$ is false.

(b) If $A = \emptyset$, then $\forall x \in A \, P(x)$ is true because

$$\forall x \in A \, P(x) \longleftrightarrow \neg\neg \forall x \in A \, P(x) \longleftrightarrow \neg \exists x \in A \neg P(x),$$

and $\exists x \in A \neg P(x)$ is false.

Theorem 2.19. *The empty set is a subset of every set.*

Proof. Rewrite the statement $A \subseteq B$ in the equivalent form $\forall x \in A \, (x \in B)$. Now if $A = \emptyset$, then $\forall x \in A \, (x \in B)$ is true. □

Theorem 2.20. *The universal quantifier distributes over conjunction:*

$$\forall x \, (P(x) \wedge Q(x)) \longleftrightarrow \forall x \, P(x) \wedge \forall x \, Q(x).$$

Example 2.21. Analyze the logical forms of the following statements.

(a) Let the universe of discourse be $\mathbb{N}$.

(1) x is a perfect square.

$$\exists y\,(x = y^2).$$

(2) x is multiple of y.

$$\exists z\,(x = yz).$$

(3) x is prime.

$$x > 1 \wedge \neg\exists y \exists z\,(x = yz \wedge y < x \wedge z < x).$$

(4) x is the smallest number that is a multiple of both y and z.

$$\exists a\,(x = ya) \wedge \exists b\,(x = zb) \wedge \neg\exists w(w < x \wedge \exists c\,(w = yc) \wedge \exists d\,(w = zd)).$$

(b) Let the universe of discourse be $\mathbb{R}$.

(1) The identity element for addition is 0.

$$\forall x\,(x + 0 = x).$$

(2) Every real number has an additive inverse.

$$\forall x \exists y\,(x + y = 0).$$

(3) Negative numbers don't have square roots.

$$\forall x(x < 0 \to \neg\exists y\,(y^2 = x)).$$

(4) Every positive number has exactly two square roots.

$$\forall x\,(x > 0 \to \exists y \exists z\,((y^2 = x) \wedge (z^2 = x) \wedge (y \neq z) \wedge \neg\exists w\,((w^2 = x) \wedge (w \neq y) \wedge (w \neq z)))).$$

2.3 More operation on Sets

Notation 2.22. Let S be the set of all perfect squares. Then

$$S = \{x \mid \exists n\,(x = n^2)\}.$$

We can also write S as

$$S = \{n^2 \mid n \in \mathbb{N}\}.$$

Therefore,

$$x \in \{n^2 \mid n \in \mathbb{N}\} \text{ means the same thing as } \exists n \in \mathbb{N}\,(x = n^2).$$

Notation 2.23. Let P be the of the first 100 prime numbers. We might start by numbering the prime numbers, calling them $p_1, p_2, p_3, \ldots$. In other words, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so on. Then

$$P = \{p_1, p_2, p_3, \ldots, p_{100}\}.$$

Another way of describing P would be to say that it consists of all numbers p_i, for i an element of the set

$$I = \{1, 2, 3, \ldots, 100\} = \{i \in \mathbb{N} \mid 1 \leqslant i \leqslant 100\}.$$

This could be written

$$P = \{p_i \mid i \in I\}.$$

Each element p_i in this set is identified by a number $i \in I$, called the *index* of the element. A set defined in this way is sometimes called an *indexed family*, and I is called the *index set*.

Example 2.24. Let M be the set of all mothers of students in your school and S be the set of all students in your school. We might let m_s stand for the mother of s for any student s in your school. Then

$$M = \{m_s \mid s \in S\}.$$

For example, if $S = \{\text{Tom,Lily,Jack}\}$, Tom and Lily have the same mother Ann, and the mother of Jack is Mary, then

$$M = \{\text{Ann,Mary}\}.$$

Example 2.25. Analyze the logical forms of the following statements by writing out the definitions of the set theory notation used.

(a) $y \in \{\sqrt[3]{x} \mid x \in \mathbb{Q}\}$

$\exists x \in \mathbb{Q}\, (y = \sqrt[3]{x})$.

(b) $\{x_i \mid i \in I\} \subseteq A$.

$\forall i \in I\, (x_i \in A)$.

(c) $\{n^2 \mid n \in \mathbb{N}\}$ and $\{n^3 \mid n \in \mathbb{N}\}$ are not disjoint.

$\exists m \in \mathbb{N} \exists n \in \mathbb{N}\, (m^2 = n^3)$.

Example 2.26 (Family of sets)**.** Let $A = \{1, 2, 3\}$, $B = \{4\}$ and $C = \emptyset$. Let

$$\mathcal{F} = \{A, B, C\} = \{\{1, 2, 3\}, \{4\}, \emptyset\}.$$

Note that $1 \in A$, $A \in \mathcal{F}$, but $1 \notin \mathcal{F}$. Sets such as $\mathcal{F}$, whose elements are all sets are sometimes called *families* of sets.

Example 2.27 (Family of sets)**.** Let S stand for the set of all students in your school, and for each student s we let C_s be the set of courses that s has taken. Let

$$\mathcal{F} = \{C_s \mid s \in S\}.$$

The elements of this family are *sets* of courses. If we let t stand for some particular student Tina, and $C_t = \{\text{Calculus, English, Composition, American History}\}$, then $C_t \in \mathcal{F}$ but Calculus $\notin \mathcal{F}$.

An important example of a family of sets is given by the power set of a set.

Definition 2.28. Suppose A is a set. The *power set* of A, denoted $\mathscr{P}(A)$, is the set whose elements are all subsets of A, in other words,

$$\mathscr{P}(A) = \{x \mid x \subseteq A\}.$$

Example 2.29. (a) Let $A = \{7, 12\}$. Then

$$\mathscr{P}(A) = \{\emptyset, \{7\}, \{12\}, \{7, 12\}\}.$$

(b)

$$\mathscr{P}(\emptyset) = \{\emptyset\}.$$

Example 2.30. In Example 2.27, let C be the set of all courses offered at your school, then $C_s \subseteq C$ for each student s. Then $C_s \in \mathscr{P}(C)$, and so $\mathcal{F} \subseteq \mathscr{P}(C)$.

Example 2.31. Analyze the logical forms of the following statements.

(a) $x \in \mathscr{P}(A)$.

$$x \subseteq A \longleftrightarrow \forall y \in x (y \in A).$$

(b) $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

$$\begin{aligned} \forall x\, (x \in \mathscr{P}(A) \to x \in \mathscr{P}(B)) &\longleftrightarrow \forall x (x \subseteq A \to x \subseteq B) \\ &\longleftrightarrow \forall x\, (\forall y \in x\, (y \in A) \to \forall z \in x\, (z \in B)) \end{aligned}$$

(c) $B \in \{\mathscr{P}(A) \mid A \in \mathcal{F}\}$, where $\mathcal{F}$ is a family of sets.

Note that

$$B \in \{\mathscr{P}(A) \mid A \in \mathcal{F}\} \longleftrightarrow \exists A \in \mathcal{F}\, (B = \mathscr{P}(A)),$$

where

$$\begin{aligned} B = \mathscr{P}(A) &\longleftrightarrow \forall x\, (x \in B \leftrightarrow x \in \mathscr{P}(A)) \\ &\longleftrightarrow \forall x\, (x \in B \leftrightarrow x \subseteq A) \\ &\longleftrightarrow \forall x\, (x \in B \leftrightarrow \forall y \in x\, (y \in A)) \end{aligned}$$

Then

$$\exists A \in \mathcal{F}\, (B = \mathscr{P}(A)) \longleftrightarrow \exists A \in \mathcal{F} \forall x\, (x \in B \leftrightarrow \forall y \in x\, (y \in A))$$

(d) $x \in \mathscr{P}(A \cap B)$.

$$x \subseteq A \cap B \longleftrightarrow \forall y \in x\, (y \in A \cap B) \longleftrightarrow \forall y \in x\, (y \in A \wedge y \in B).$$

(e) $x \in \mathscr{P}(A) \cap \mathscr{P}(B)$.

$$(x \in \mathscr{P}(A)) \wedge (x \in \mathscr{P}(B)) \longleftrightarrow (\forall y \in x\, (y \in A)) \wedge (\forall y \in x\, (y \in B)).$$

Remark. One can show that

$$\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B).$$

If we change $\cap$ to $\cup$, this is not true in general.

Example 2.32. Let $\mathcal{F} = \{\{1,2,3,4\},\{2,3,4,5\},\{3,4,5,6\}\}$. Then

$$\begin{aligned}\cap\mathscr{F} &= \{1,2,3,4\} \cap \{2,3,4,5\} \cap \{3,4,5,6\} = \{3.,4\}.\\ \cup\mathcal{F} &= \{1,2,3,4\} \cup \{2,3,4,5\} \cup \{3,4,5,6\} = \{1,2,3,4,5,6\}.\end{aligned}$$

Definition 2.33. Suppose $\mathscr{F}$ is a family of sets. Then the *intersection* and union of $\mathcal{F}$ are the sets $\cap\mathcal{F}$ and $\cup\mathcal{F}$ defined as follows:

$$\begin{aligned}\cap\mathcal{F} &= \{x \mid \forall A \in \mathcal{F}\,(x \in A)\}.\\ \cup\mathcal{F} &= \{x \mid \exists A \in \mathcal{F}\,(x \in A)\}.\end{aligned}$$

Remark. We will use the notation $\cap\mathcal{F}$ only when $\mathcal{F} \neq \emptyset$.

Remark. If $\mathcal{F} = \{A, B\}$, then

$$\cap\mathcal{F} = A \cap B.$$

$$\cup\mathcal{F} = A \cup B.$$

Example 2.34. Analyze the logical forms of the following statements.

(a) $x \in \cap\mathcal{F}$.

$$\forall A \in \mathcal{F}\,(x \in A).$$

(b) $\cap\mathcal{F} \not\subseteq \cup\mathcal{G}$.

$$\begin{aligned}\cap\mathcal{F} \not\subseteq \cup\mathcal{G} &\longleftrightarrow \exists x\,(x \in \cap\mathcal{F} \wedge x \notin \cup\mathcal{G})\\ &\longleftrightarrow \exists x\,[\forall A \in \mathcal{F}(x \in A) \wedge \neg\exists A \in \mathcal{G}\,(x \in A)]\\ &\longleftrightarrow \exists x\,[\forall A \in \mathcal{F}(x \in A) \wedge \forall A \in \mathcal{G}\,(x \notin A)].\end{aligned}$$

(c) $x \in \mathscr{P}(\cup\mathcal{F})$.

$$\begin{aligned}x \in \mathscr{P}(\cup P) &\longleftrightarrow x \subseteq \cup\mathcal{F}\\ &\longleftrightarrow \forall y \in x\,(y \in \cup\mathcal{F})\\ &\longleftrightarrow \forall y \in x\,(\exists A \in \mathcal{F}\,(y \in A)).\end{aligned}$$

(d) $x \in \cup\{\mathscr{P}(A) \mid A \in \mathcal{F}\}$. Let $\mathcal{G} = \{\mathscr{P}(A) \mid A \in \mathcal{F}\}$. Then $\mathcal{G}$ is a family of power sets, and so

$$\begin{aligned}x \in \cup\{\mathscr{P}(A) \mid A \in \mathcal{F}\} &\longleftrightarrow x \in \cup\mathcal{G}\\ &\longleftrightarrow x \in \cup_{A\in\mathcal{F}}\mathscr{P}(A)\\ &\longleftrightarrow \exists A \in \mathcal{F}\,(x \in \mathscr{P}(A))\\ &\longleftrightarrow \exists A \in \mathcal{F}(x \subseteq A)\\ &\longleftrightarrow \exists A \in \mathcal{F}(\forall y \in x\,(y \in A)).\end{aligned}$$

Notation 2.35. Suppose $\mathcal{F} = \{A_i \mid i \in I\}$. Then

$$\begin{aligned} \cap\mathcal{F} &= \cap_{i\in I} A_i = \{x \mid \forall i \in I\,(x \in A_i)\} \\ \cup\mathcal{F} &= \cup_{i\in I} A_i = \{x \mid \exists i \in I\,(x \in A_i)\}. \end{aligned}$$

Example 2.36. Let $I = \{1, 2, 3\}$, and for each $i \in I$ let $A_i = \{i, i+1, i+2, i+3\}$. Find $\cap_{i\in I} A_i$ and $\cup_{i\in I} A_i$.

Note that

$$\begin{aligned} A_1 &= \{1, 2, 3, 4\} \\ A_2 &= \{2, 3, 4, 5\} \\ A_3 &= \{3, 4, 5, 6\}. \end{aligned}$$

Then

$$\begin{aligned} \cap_{i\in I} A_i &= A_1 \cap A_2 \cap A_3 = \{1, 2, 3, 4\} \cap \{2, 3, 4, 5\} \cap \{3, 4, 5, 6\} = \{3, 4\}. \\ \cup_{i\in I} A_i &= A_1 \cup A_2 \cup A_3 = \{1, 2, 3, 4\} \cup \{2, 3, 4, 5\} \cup \{3, 4, 5, 6\} = \{1, 2, 3, 4, 5, 6\}. \end{aligned}$$

In fact, we can now see that the question asked in this example is exactly the same as the one in Example 2.32, but with different notation.

Chapter 3

Proofs

3.1 Proof Strategies

Theorem. Suppose $x > 3$ and $y < 2$. Then $x^2 - 2y > 5$.

Proof. Exercise. □

Incorrect Theorem. Suppose $x > 3$. The $x^2 - 2y > 5$. The counterexample is $x = 4$ and $y = 6$, where x, y are free variables, and $(4, 6)$ is an instance for (x, y).

Remark. If you find a counterexample for a theorem, then you can be sure that the theorem is incorrect, but the only way to know for sure that is a theorem is correct is to prove it.

Our first proof strategy:
To prove a conclusion of the form $P \to Q$:
Assume P is true and then prove Q.

Assuming P is true amounts to the same thing as adding P to your list of hypotheses, then the conclusion is changed from $P \to Q$ to Q.

Definition 3.1. We will refer to the statements that are known or assumed to be true at some point in the course of figuring out a proof as *givens*, and the statement that remains to be proven at that as the *goal*.

Scratch work

Before using strategy:

Givens	Goal
—	$P \to Q$
—	

After using strategy:

Givens	Goal
—	Q
—	
P	

Form of final proof:

Suppose P.
  [Proof of Q goes here.]
Therefore $P \to Q$.

Example 3.2. Suppose a and b are real numbers. Prove that if $0 < a < b$ then $a^2 < b^2$.

Proof. We are given as a hypothesis that a and b are real numbers. Our conclusion has the form $P \to Q$, where P is the statement $0 < a < b$ and Q is the statement $a^2 < b^2$. Thus we start with these statements as given and goal:

Givens	Goal
a and b are real numbers	$(a < a < b) \to (a^2 < b^2)$

We transform the problem by adding $0 < a < b$ to the list of givens and making $a^2 < b^2$ our goal:

Givens	Goal
a and b are real numbers	$a^2 < b^2$
$0 < a < b$	

Since $a, b \in \mathbb{R}^+$, multiplying $a < b$ by a gives us $a^2 < ab$; multiplying $a < b$ by b gives us $ab < b^2$. Thus, $a^2 < ab < b^2$, and so $a^2 < b^2$. □

Theorem 3.3. *Suppose a and b are real numbers. If $0 < a < b$ then $a^2 < b^2$.*

Proof. Suppose that $0 < a < b$. Then $a, b \in \mathbb{R}^+$. Multiplying $a < b$ by a gives us $a^2 < ab$ and multiplying $a < b$ by b gives us $ab < b^2$. Thus, $a^2 < ab < b^2$, and so $a^2 < b^2$. Thus, if $0 < a < b$ then $a^2 < b^2$. □

Our second proof strategy:
To prove a goal of the form $P \to Q$:
Assume Q is false and prove that P is false:

Scratch work

Before using strategy:

Givens	Goal
—	$P \to Q$
—	

This is equivalent to

Givens	Goal
—	$\neg Q \to \neg P$
—	

After using strategy:

Givens	Goal
—	$\neg P$
—	
$\neg Q$	

Form of final proof:

Suppose $\neg Q$ (or Q is false).
[Proof of $\neg P$ goes here.]
Therefore $P \to Q$.

Example 3.4. Suppose a, b, and c are real numbers and $a > b$. Prove that if $ac \leqslant bc$ then $c \leqslant 0$.

Scratch work

Givens	Goal
a, b, and c are real numbers	$(ac \leqslant bc) \to (c \leqslant 0)$
$a > b$	

This is equivalent to

Givens	Goal
a, b, and c are real numbers	$c > 0 \to ac > bc$
$a > b$	

The contrapositive of the goal is $\neg(c \leqslant 0) \to \neg(ac \leqslant bc)$, or in other words $(c > 0) \to (ac > bc)$, so we can prove it by adding $c > 0$ to the list of gives and make $ac > bc$ our new goal:

Givens	Goal
a, b, and c are real numbers	$ac > bc$
$a > b$	
$c > 0$	

Form of final proof:

Suppose $c > 0$.
[Proof of $ac > bc$ goes here.]
Therefore if $ac \leqslant bc$ then $c \leqslant 0$.

Theorem 3.5. *Suppose a, b, and c are real numbers and $a > b$. If $ac \leqslant bc$ then $c \leqslant 0$.*

Proof. We will prove the contrapositive. Suppose that $c > 0$. Then we can multiply both sides of the given inequality $a > b$ by c and conclude that $ac > bc$. Therefore, if $ac \leqslant bc$ then $c \leqslant 0$. □

3.2 Proof Involving Negations and Conditions

Out first strategy for proving negated statements is :

To prove a goal of the form $\neg P$:

If possible, reexpress the goal in some other form and then use one of the proof strategies for this other goal form.

Example 3.6. Suppose $A \cap C \subseteq B$ and $a \in C$. Prove that $a \notin A \setminus B$.

Scratch work

Givens	Goal
$A \cap C \subset B$	$a \notin A \smallsetminus B$
$a \in C$	

Because the goal is a negated statement, we try to reexpress it:

$$\begin{aligned} a \notin A \smallsetminus B &= \neg(a \in A \wedge a \notin B) \\ &= a \notin A \vee a \in B \\ &= a \in A \rightarrow a \in B. \end{aligned}$$

Rewrite the goal in this way gives us:

Givens	Goal
$A \cap C \subset B$	$a \in A \rightarrow a \in B$
$a \in C$	

We now prove the goal in this new form, using the first strategy from Section 3.1. (Note that in other situations we might choose the second strategy from Section 3.1.) Thus, we add $a \in A$ to our list of givens and make $a \in B$ our goal:

Givens	Goal
$A \cap C \subset B$	$a \in B$
$a \in C$	
$a \in A$	

The proof is now easy: From the givens $a \in A$ and $a \in C$ we can conclude that $a \in A \cap C$, and then, since $A \cap C \subseteq B$, it follows that $a \in B$.

Theorem 3.7. *Suppose $A \cap C \subseteq B$ and $a \in C$. Then $a \notin A \smallsetminus B$.*

Proof.

$$\begin{aligned} a \notin A \smallsetminus B &\text{ is equivalent to } \neg(a \in A \wedge a \notin B) \\ &\text{which is equivalent to } a \notin A \vee a \in B \\ &\text{which is equivalent to } a \in A \rightarrow a \in B. \end{aligned}$$

Suppose $a \in A$. Then since $a \in C$, $a \in A \cap C$. But then since $A \cap C \subseteq B$ it follows that $a \in B$. Therefore, if $A \cap C \subseteq B$ and $a \in C$, then $a \notin A \smallsetminus B$. □

Out second strategy for proving negated statements is :

To prove a goal of the form $\neg P$:

Assume P is true and try to reach a contradiction. Once you have reached a contradiction, you can conclude that P must be false.

Scratch work

Before using strategy:

Givens	Goal
—	$\neg P$
—	

After using strategy:

Givens	Goal
—	Contradiction
—	
$\neg P$	

Form of final proof:

Suppose P.
  [Proof of contradiction goes here.]
Therefore P is false.

Example 3.8 (Using the second strategy)**.** Suppose $A \cap C \subseteq B$ and $a \in C$. Then $a \notin A \smallsetminus B$.

Proof. Suppose $\neg(a \notin A \smallsetminus B)$. Then $a \in A \smallsetminus B$, and so $a \in A$ and $a \notin B$. Since $a \in C$, $a \in A \cap C$. But then since $A \cap C \subseteq B$ it follows that $a \in B$, contradicting $a \notin B$. Therefore, if $A \cap C \subseteq B$ and $a \in C$, then $a \notin A \smallsetminus B$. □

Example 3.9. Prove that if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Scratch work

Givens	Goal
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

We try proof by contradiction and transform the problem as follows:

Givens	Goal
$x^2 + y = 13$	Contradiction
$y \neq 4$	
$x = 3$	

Theorem 3.10. *If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.*

Proof. Suppose $x^2 + y = 13$ and $y \neq 4$. Suppose $x = 3$. Substituting this into the equation $x^2 + y = 13$, we get $9 + y = 13$, so $y = 4$, contradicting $y \neq 4$. Therefore, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$. □

This is our first strategy based on the logical form of a *given.*

To use a given of the form $\neg P$:

If you're doing a proof by contradiction, try making P your goal. If you can prove P, then the proof will be complete, because P contradicts the given $\neg P$.

Scratch work

Before using strategy:

Givens	Goal
$\neg P$	Contradiction
—	
—	

After using strategy:

Givens	Goal
$\neg P$	P
—	
—	

Form of final proof:

[Proof of contradiction goes here.]
Since we already know $\neg P$, this is a contradiction.

Example 3.11. Suppose A, B, and C are sets, $A \smallsetminus B \subseteq C$. Prove that if $x \in A \smallsetminus C$ then $x \in B$.

Scratch work

Before using strategy:

Givens	Goal
$A \smallsetminus B \subseteq C$	$x \in B$
$x \in A \smallsetminus C$	

The goal $x \in B$ contains no logical connectives, so none of the techniques we have studied so far apply, and it is not obvious why the goal follows from the givens. Let's try proof by contradiction.

Givens	Goal
$A \smallsetminus B \subseteq C$	Contradiction
$x \in A \smallsetminus C$	
$x \notin B$	

Note that $x \in A \smallsetminus C$ means $x \in A$ and $x \notin C$. Replacing this given by its definition gives us:

Givens	Goal
$A \smallsetminus B \subseteq C$	Contradiction
$x \in A$	
$x \notin C$	
$x \notin B$	

Now the third given also has the form $\neg P$, where P is the statement $x \in C$, so we can apply the strategy for using givens of the form $\neg P$ and make $x \in C$ our goal.
After using strategy:

Givens	Goal
$A \smallsetminus B \subseteq C$	$x \in C$
$x \in A$	
$x \notin C$	
$x \notin B$	

Theorem 3.12. *Suppose A, B, and C are sets, $A \smallsetminus B \subseteq C$. If $x \in A \smallsetminus C$ then $x \in B$.*

Proof. Suppose $x \in A \smallsetminus C$. Then $x \in A$ and $x \notin C$. Suppose $x \notin B$. Then $x \in A \smallsetminus B$. Since $A \smallsetminus B \subseteq C$, $x \in C$, contradicting $x \notin C$. Thus, if $x \in A \smallsetminus C$ then $x \in B$. □

Remark. Prove by contradiction directly. Suppose $x \notin B$. Since $x \in A \smallsetminus C$, $x \in A$ and $x \notin C$. Hence $x \in A \smallsetminus B$, contradicting $A \smallsetminus B \subseteq C$. Thus, if $x \in A \smallsetminus C$ then $x \in B$.

To use a given of the form $\neg P$:

If possible, reexpress this given in some other form.

To use a given of the form $P \to Q$:

If you are also given P, or if you can prove that P is true, then you can use this given to conclude that Q is true (*modus ponens*). Since it is equivalent to $\neg Q \to \neg P$, if you can prove that Q is false, you can use this given to conclude that P is false (*modus tollens*).

(a) modus ponens: $(P \to Q) \wedge P \longrightarrow Q$.

(b) modus tollens: $(P \to Q) \wedge \neg Q \longrightarrow \neg P$.

Example 3.13. Suppose $P \to (Q \to R)$. Prove that $\neg R \to (P \to \neg Q)$.

Scratch work

Before using strategy:

Givens	Goal
$P \to (Q \to R)$	$\neg R \to (P \to \neg Q)$

The goal is a conditional statement, so

Givens	Goal
$P \to (Q \to R)$	$P \to \neg Q$
$\neg R$	

Similarly,

Givens	Goal
$P \to (Q \to R)$	$\neg Q$
$\neg R$	
P	

By modus ponens,

Givens	Goal
$P \to (Q \to R)$	$\neg Q$
$\neg R$	
P	
$Q \to R$	

Theorem 3.14. *Suppose $P \to (Q \to R)$. Then $\neg R \to (P \to \neg Q)$.*

Proof. Suppose $\neg R$. Suppose P. Since P and $P \to (Q \to R)$, it follows that $Q \to R$. But then, since $\neg R$, we can conclude $\neg Q$. Thus, $P \to \neg Q$. Therefore $\neg R \to (P \to \neg Q)$. □

Example 3.15. Suppose that $A \subseteq B$, $a \in A$, and $a \notin B \smallsetminus C$. Prove that $a \in C$.

Scratch work

Before using strategy:

Givens	Goal
$A \subseteq B$	$a \in C$
$a \in A$	
$a \notin B \smallsetminus C$	

Note that

$$\begin{aligned} a \notin B \smallsetminus C &= \neg(a \in B \land a \notin C) \\ &= a \notin B \lor a \in C \\ &= a \in B \to a \in C. \end{aligned}$$

Now

Givens	Goal
$A \subseteq B$	$a \in C$
$a \in A$	
$a \in B \to a \in C$	

If we could prove that $a \in B$, then we could use modus ponens to reach our goal.

Givens	Goal
$A \subseteq B$	$a \in B$
$a \in A$	
$a \in B \to a \in C$	

Theorem 3.16. *Suppose that $A \subseteq B$, $a \in A$, and $a \notin B \smallsetminus C$. Prove that $a \in C$.*

Proof. Since $a \in A$ and $A \subseteq B$, we can conclude that $a \in B$. But $a \notin B \smallsetminus C$, so it follows that $a \in C$. □

3.3 Proofs Involving Quantifiers

> **To prove a goal of the form $\forall x\, P(x)$:**
> Let x stand for an arbitrary object and prove $P(x)$.

Scratch work

Before using strategy:

Givens	Goal
—	$\forall x\, P(x)$
—	

After using strategy:

Givens	Goal
—	$P(x)$
—	

Form of final proof:

Let x be arbitrary.
  [Proof of $P(x)$ goes here.]
Since x was arbitrary, we can conclude that $\forall x\, P(x)$.

Example 3.17. Suppose A, B, and C are sets, and $A \smallsetminus B \subseteq C$. Prove that $A \smallsetminus C \subseteq B$.

Scratch work

Before using strategy:

Givens	Goal
$A \smallsetminus B \subseteq C$	$A \smallsetminus C \subseteq B$

After writting out the definition of $\subseteq$:

Givens	Goal
$A \smallsetminus B \subseteq C$	$\forall x\, (x \in A \smallsetminus C \to x \in B)$

We introduce a new variable x into the proof to stand for an arbitrary object. Then change our goal:

Givens	Goal
$A \smallsetminus B \subseteq C$	$x \in A \smallsetminus C \to x \in B$

This is equivalent to

Givens	Goal
$A \smallsetminus B \subseteq C$	$x \in B$
$x \in A \smallsetminus C$	

This is equivalent to

Givens	Goal
$A \smallsetminus B \subseteq C$	$x \in B$
$x \in A$	
$x \notin C$	

This is equivalent to

Givens	Goal
$A \smallsetminus B \subseteq C$	contradiction
$x \in A$	
$x \notin C$	
$x \notin B$	

This is equivalent to

Givens	Goal
$A \smallsetminus B \subseteq C$	contradiction
$x \in A \smallsetminus B$	
$x \notin C$	

Theorem 3.18. *Suppose A, B, and C are sets, and $A \smallsetminus B \subseteq C$. Prove that $A \smallsetminus C \subseteq B$.*

Proof. Let x be arbitrary. Suppose $x \in A \smallsetminus C$. Then $x \in A$ and $x \notin C$. Suppose $x \notin B$. Then $x \in A \smallsetminus B$. Since $A \smallsetminus B \subseteq C$, $x \in C$, contradicting $x \notin C$. Thus, if $x \in A \smallsetminus C$ then $x \in B$. Since x was arbitrary, we can concludee that $\forall x\,(x \in A \smallsetminus C \to x \in B)$, so $A \smallsetminus C \subseteq B$. □

Remark. The problem is exactly the same as in Example 3.12.

Example 3.19. Suppose A and B are sets, Prove that if $A \cap B = A$ then $A \subseteq B$.

Scratch work

Before using strategy:

Givens	Goal
$A \cap B = A$	$\forall x\,(x \in A \to x \in B)$

Let x be arbitrary, assume $x \in A$, and prove $x \in B$:

Givens	Goal
$A \cap B = A$	$x \in B$
$x \in A$	

Theorem 3.20. *Suppose A and B are sets, If $A \cap B = A$ then $A \subseteq B$.*

Proof. Suppose $A \cap B = A$, and suppose $x \in A$. Then since $A \cap B = A$, $x \in A \cap B$, so $x \in B$. Since x was an arbitrary element of A, we can conclude that $A \subseteq B$. □

To prove a goal of the form $\exists x\, P(x)$:
Try to find a value x for which you think $P(x)$ will be true. Then start your proof with "Let $x =$ (the value you decided on)" and proceed to prove $P(x)$ for this value of x.

Scratch work

Before using strategy:

Givens	Goal
—	$\exists x\, P(x)$
—	

After using strategy:

Givens	Goal
—	$P(x)$
—	

$x =$ (the value you decided on).

Form of final proof:

Let $x =$ (the value you decided on).
[Proof of $P(x)$ goes here.]
Since x was arbitrary, we can conclude that $\forall x\, P(x)$.

Example 3.21. Prove that for every $x \in \mathbb{R}$, if $x > 0$ then there is a $y \in \mathbb{R}$ such that $y(y+1) = x$.

Scratch work

In symbols, our goal is $\forall x\,(x > 0 \to \exists y\,[y(y+1) = x)]$, where the variables x and y are understood to range over $\mathbb{R}$. We therefore start by letting x be an arbitrary real number, and we then assume that $x > 0$ and try to prove that $\exists y\,[y(y+1) = x]$. Thus, we now have the following given and goal:

Givens	Goal
$x > 0$	$\exists y\,[y(y+1) = x]$

We try to solving the equation $y(y+1) = x$ for y.

$$y(y+1) = x \qquad \Longrightarrow \qquad y^2 + y - x = 0 \qquad \Longrightarrow \qquad y = \tfrac{-1+\sqrt{1+4x}}{2}$$

Since $x > 0$, Either of two solutions is a real number and could be used in the proof. Now

Givens	Goal
$x > 0$	$y(y+1) = x$
$y = \tfrac{-1+\sqrt{1+4x}}{2}$	

Theorem 3.22. *For every real number x, if $x > 0$, then there is a real number y such that $y(y+1) = x$.*

Proof. Let $x \in \mathbb{R}$ be arbitrary and suppose $x > 0$. Let

$$y = \frac{-1+\sqrt{1+4x}}{2} \in \mathbb{R}.$$

Then

$$\begin{aligned} y(y+1) &= \frac{-1+\sqrt{1+4x}}{2} \cdot \left(\frac{-1+\sqrt{1+4x}}{2} + 1\right) \\ &= \frac{\sqrt{1+4x}-1}{2} \cdot \frac{\sqrt{1+4x}+1}{2} \\ &= \frac{1+4x-1}{4} \\ &= x \end{aligned}$$

□

To use a given of the form $\exists x\, P(x)$:

Introduce a new variable x_0 into the proof to stand for an object for which $P(x_0)$ is true. This means that you can now assume that $P(x_0)$ is true. Logicians call this rule of inference *existential instantiation.*

To use a given of the form $\forall x\, P(x)$:

You can plug in any value, say a, for x and use this given to conclude that $P(a)$ is true. The rule is called *universal instantiation.*

Example 3.23. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Prove that $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.

Scratch work

Givens	Goal
$\mathcal{F} \cap \mathcal{G} \neq \emptyset$	$\forall x\,(x \in \cap\mathcal{F} \to x \in \cup\mathcal{G})$

Let x be arbitrary, assume $x \in \cap\mathcal{F}$, and prove $x \in \cup\mathcal{G}$.

Givens	Goal
$\mathcal{F} \cap \mathcal{G} \neq \emptyset$	$x \in \cup\mathcal{G}$
$x \in \cap\mathcal{F}$	

Then

Givens	Goal
$\exists A\,(A \in \mathcal{F} \cap \mathcal{G})$	$\exists A \in \mathcal{G}\,(x \in A)$
$\forall A \in \mathcal{F}\,(x \in A)$	

Then

Givens	Goal
$A_0 \in \mathcal{F}$	$\exists A \in \mathcal{G}\,(x \in A)$
$A_0 \in \mathcal{G}$	
$\forall A \in \mathcal{F}\,(x \in A)$	

Theorem 3.24. *Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Then $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.*

Proof. Suppose $x \in \cap\mathcal{F}$. Since $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, we can let $A_0 \in \mathcal{F} \cap \mathcal{G}$. Then $A_0 \in \mathcal{F}$ and $A_0 \in \mathcal{G}$. Since $x \in \cap\mathcal{F}$ and $A_0 \in \mathcal{F}$, it follows that $x \in A_0$. But we also know that $A_0 \in \mathcal{G}$, so we can conclude that $x \in \cup\mathcal{G}$. □

Example 3.25. Suppose B is a set and $\mathcal{F}$ is a family of sets. Prove that if $\cup\mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathscr{P}(B)$.

Scratch work

Let x be an arbitrary set.

Givens	Goal
$\cup\mathcal{F} \subseteq B$	$A \in \mathscr{P}(B)$
$A \in \mathcal{F}$	

Now

Givens	Goal
$\cup\mathcal{F} \subseteq B$	$A \subseteq B$
$A \in \mathcal{F}$	

Let y be arbitrary. Then

Givens	Goal
$\cup\mathcal{F} \subseteq B$	$y \in B$
$A \in \mathcal{F}$	
$y \in A$	

If we knew that $y \in \cup\mathcal{F}$, then the proof will be done.

Givens	Goal
$\cup\mathcal{F} \subseteq B$	$y \in \cup\mathcal{F}$
$A \in \mathcal{F}$	
$y \in A$	

Theorem 3.26. *Suppose B is a set and $\mathcal{F}$ is a family of sets. If $\cup\mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathscr{P}(B)$.*

Proof. Suppose $\cup\mathcal{F} \subseteq B$. Let $A \in \mathcal{F}$ be arbitrary, we need to prove $A \in \mathscr{P}(B)$, i.e., $A \subseteq B$. Let $y \in A$ be arbitrary. Then $y \in \cup\mathcal{F}$. Since $\cup\mathcal{F} \subseteq B$, $y \in B$. Hence $A \subseteq B$, so $A \in \mathscr{P}(B)$. □

Remark. In the proof, we didn't do any expansion for $\cup\mathcal{F} \subseteq B$.

Definition 3.27. For any $x, y \in \mathbb{Z}$, we say x *divides* y (or y is *divisible* by x) if $\exists k \in \mathbb{Z}(kx = y)$. We use the notation $x \mid y$ to mean "x divides y". For example, $4 \mid 20$, since $5(4) = 20$.

Theorem 3.28. *For all integers a, b, and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. Let $a, b, c \in \mathbb{Z}$ be arbitrary. Suppose $a \mid b$ and $b \mid c$. Then $ma = b$ and $nb = c$ for some $m, n \in \mathbb{Z}$. Therefore $c = bn = nma$, so $a \mid c$ since $nm \in \mathbb{Z}$. □

3.4 Proofs Involving Conjunctions and Biconditionals

To prove a goal of the form $P \wedge Q$:
Prove P and Q separately.
To use a given of the form $P \wedge Q$:
Treat this given as two separate givens: P and Q.

Example 3.29. Suppose $A \subseteq B$ and $A \cap C = \emptyset$. Prove that $A \subseteq B \smallsetminus C$.

Scratch work

Givens	Goal
$A \subseteq B$	$A \subseteq B \smallsetminus C$
$A \cap C = \emptyset$	

Let x be arbitrary.

Givens	Goal
$A \subseteq B$	$x \in B \smallsetminus C$
$A \cap C = \emptyset$	
$x \in A$	

Then

Givens	Goal
$A \subseteq B$	$x \in B$
$A \cap C = \emptyset$	$x \notin C$
$x \in A$	

Theorem 3.30. *Suppose $A \subseteq B$ and $A \cap C = \emptyset$. Then $A \subseteq B \smallsetminus C$.*

Proof. Suppose $x \in A$. Since $A \subseteq B$, $x \in B$. Since $A \cap C = \emptyset$, we must have $x \notin C$. Thus, $x \in B \smallsetminus C$. Since $x \in A$ is arbitrary, we can conclude that $A \subseteq B \smallsetminus C$. □

> **To prove a goal of the form $P \leftrightarrow Q$:**
> Prove $P \to Q$ and $Q \to P$ separately.
> **To use a given of the form $P \wedge Q$:**
> Treat this given as two separate givens: $P \to Q$ and $Q \to P$.

Definition 3.31. $x \in \mathbb{Z}$ is *even* if $\exists k \in \mathbb{Z}(x = 2k)$, and x is *odd* if $\exists k \in \mathbb{Z}(x = 2k+1)$.

Fact 3.32. Every $x \in \mathbb{Z}$ is either even or odd, but not both.

Example 3.33. Suppose $x \in \mathbb{Z}$. Prove that x is even iff x^2 is even.

Scratch work

($\longrightarrow$)

Givens	Goal
$x \in \mathbb{Z}$	x^2 is even
x is even	

Then

Givens	Goal
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j)$
$\exists k \in \mathbb{Z}(x = 2k)$	

Then

Givens	Goal
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j)$
$k \in \mathbb{Z}$	
$x = 2k$	

To prove ($\longleftarrow$): (x^2 is even) → (x is even), we will prove the contrapositive (x is odd) → (x^2 is odd) instead.

Givens	Goal
$x \in \mathbb{Z}$	x^2 is odd
x is odd	

Then

Givens	Goal
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j+1)$
$\exists k \in \mathbb{Z}(x = 2k+1)$	

Then

Givens	Goal
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j+1)$
$k \in \mathbb{Z}$	
$x = 2k+1$	

Theorem 3.34. *Suppose $x \in \mathbb{Z}$. Then x is even iff x^2 is even.*

Proof. ($\longrightarrow$) Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Therefore, $x^2 = 4k^2 = 2(2k^2)$, so x^2 is even since $2k^2 \in \mathbb{Z}$.

($\longleftarrow$) Suppose x is odd. Then $x = 2k+1$ for some $k \in \mathbb{Z}$. Therefore, $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so x^2 is odd since $2k^2 + 2k \in \mathbb{Z}$. □

Example 3.35. Prove that $\forall x \neg P(x) \longleftrightarrow \neg \exists x\, P(x)$.

Scratch work

($\longrightarrow$)

Givens	Goal
$\forall x \neg P(x)$	$\neg \exists y\, P(y)$

We use proof by contradiction.

Givens	Goal
$\forall x \neg P(x)$	Contradiction
$\exists y\, P(y)$	

($\longleftarrow$)

Givens	Goal
$\neg \exists x\, P(x)$	$\forall y \neg P(y)$

Let y be arbitrary.

Givens	Goal
$\neg \exists x\, P(x)$	$\neg P(y)$

We use proof by contradiction.

Givens	Goal
$\neg \exists x\, P(x)$	Contradiction
$P(y)$	

Our first given is a negated statement, and this suggests that we could get the contradiction we need by proving $\exists x\, P(x)$.

Givens	Goal
$\neg \exists x\, P(x)$	$\exists x\, P(x)$
$P(y)$	

Theorem 3.36. $\forall x \neg P(x) \longleftrightarrow \neg \exists x\, P(x)$.

Proof. (→) Suppose $\forall x \neg P(x)$. Suppose $\exists y\, P(y)$. Then we can choose some y_0 such that $P(y_0)$ is true. But since $\forall x\, \neg P(x)$, we have that $\neg P(y_0)$, contradicting $P(y_0)$ is true.

(←) Suppose $\neg\exists x\, P(x)$. Let y be arbitrary. Suppose $P(y)$ is true. Then $\exists y\, P(y)$, contradicting $\neg\exists x\, P(x)$. □

Remark. For the backward implication, we use proof by contradiction in the middle of the proof.

Notation 3.37. (a) We use $P \to R \to Q$ to denote $(P \to R) \wedge (R \to Q)$.

(b) We use $P \leftrightarrow R \leftrightarrow Q$ to denote $(P \leftrightarrow R) \wedge (R \leftrightarrow Q)$.

(c) We use P iff R iff Q to denote (P iff Q) and (R iff Q).

Example 3.38. Suppose A, B, and C are sets. Prove that $A \cap (B \smallsetminus C) = (A \cap B) \smallsetminus C$.

Scratch work

The equation $A \cap (B \smallsetminus C) = (A \cap B) \smallsetminus C$ means $\forall x\, (x \in A \cap (B \smallsetminus C) \leftrightarrow x \in (A \cap B) \smallsetminus C)$. Note that for any x,

$$\begin{aligned} x \in A \cap (B \setminus C) &\longleftrightarrow x \in A \wedge x \in B \smallsetminus C \longleftrightarrow x \in A \wedge x \in B \wedge x \notin C \\ x \in (A \cap B) \setminus C &\longleftrightarrow x \in A \cap B \wedge x \notin C \longleftrightarrow x \in A \wedge x \in B \wedge x \notin C. \end{aligned}$$

Theorem 3.39. *Suppose A, B, and C are sets. Then $A \cap (B \smallsetminus C) = (A \cap B) \smallsetminus C$.*

Proof. Let x be arbitrary. Then

$$\begin{aligned} x \in A \cap (B \smallsetminus C) &\longleftrightarrow x \in A \wedge x \in B \smallsetminus C \\ &\longleftrightarrow x \in A \wedge x \in B \wedge x \notin C \\ &\longleftrightarrow x \in (A \cap B) \wedge x \notin C \\ &\longleftrightarrow x \in (A \cap B) \smallsetminus C. \end{aligned}$$

Thus,

$$\forall x\, (x \in A \cap (B \smallsetminus C)) \longleftrightarrow x \in (A \cap B) \smallsetminus C,$$

so $A \cap (B \smallsetminus C) = (A \cap B) \smallsetminus C$. □

Example 3.40. Prove that for any $a, b \in \mathbb{R}$,

$$(a+b)^2 - 4(a-b)^2 = (3b-a)(3a-b).$$

Multiplying out both sides gives us:

$$\begin{aligned} (a+b)^2 - 4(a-b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2) \\ &= -3a^2 + 10ab - 3b^2 \\ (3b-a)(3a-b) &= 9ab - 3a^2 - 3b^2 + ab \\ &= -3a^2 + 10ab - 3b^2. \end{aligned}$$

Theorem 3.41. *For any $a, b \in \mathbb{R}$,*

$$(a+b)^2 - 4(a-b)^2 = (3b-a)(3a-b).$$

Proof. Let $a, b \in \mathbb{R}$ be arbitrary.

$$\begin{aligned}(a+b)^2 - 4(a-b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2)\\ &= -3a^2 + 10ab - 3b^2\\ &= 9ab - 3a^2 - 3b^2 + ab\\ &= (3b-a)(3a-b).\end{aligned}$$ □

Theorem 3.42. *Fro every $n \in \mathbb{Z}$, $6 \mid n$ iff $2 \mid n$ and $3 \mid n$.*

Proof. Let $n \in \mathbb{Z}$ be arbitrary.

($\rightarrow$) Suppose $6 \mid n$. Then $\exists k \in \mathbb{Z}(6k = n)$. Therefore $n = 6k = (3k)(2) = (2k)3$. Since $2k, 3k \in \mathbb{Z}$, $2 \mid n$ and $3 \mid n$.

($\leftarrow$) Suppose $2 \mid n$ and $3 \mid n$. Then $\exists j \in \mathbb{Z}(n = 2j)$ and $\exists k \in \mathbb{Z}(n = 3k)$. Therefore, $6(j-k) = 6j - 6k = 3(2j) - 2(3k) = 3n - 2n = n$, so $6 \mid n$. □

3.5 Proofs Involving Disjunctions

To use a given of the form $P \vee Q$:

Break your proof into cases: For case 1, assume that P is true and use this assumption to prove the goal. For case 2, assume Q is true and give another proof of the goal.

Scratch work

Before using strategy:

Givens	Goal
$P \vee Q$	—

After using strategy:

Case 1: Givens	Goal
P	—
—	

Case 2: Givens	Goal
Q	—
—	

Form of final proof:

Case 1. P is true.
[Proof of goal goes here.]
Case 2. Q is true.
[Proof of goal goes here.]
Since we know $P \vee Q$, these cases cover all the possibilities. Therefore the goal must be true.

Example 3.43. Suppose that A, B, and C are sets. Prove that if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Scratch work

We assume $A \subseteq C$ and $B \subseteq C$ and prove $A \cup B \subseteq C$. Writing out the goal using logical symbols gives us the following givens and goal:

Givens	Goal
$A \subseteq C$	$\forall x\,(x \in A \cup B \to x \in C)$
$B \subseteq C$	

Let x be arbitrary, assume $x \in A \cup B$, and try to prove $x \in C$.

Givens	Goal
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A \vee x \in B$	

For the first case we assume $x \in A$.

Givens	Goal
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A$	

For the second case we assume $x \in B$.

Givens	Goal
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in B$	

Theorem 3.44. *Suppose that A, B, and C are sets. If $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.*

Proof. Suppose $A \subseteq C$ and $B \subseteq C$, and $x \in A \cup B$ be arbitrary. Then either $x \in A$ or $x \in B$.

Case 1. $x \in A$. Then since $A \subseteq C$, $x \in C$.

Case 1. $x \in B$. Then since $B \subseteq C$, $x \in C$.

These cases cover all the possibilities, so we can conclude that $x \in C$, so we can conclude that $x \in C$. Since $x \in A \cup B$ is arbitrary, $A \cup B \subseteq C$. □

Remark. The cases must be exhaustive, but they need not be exclusive.

To prove a goal of the form $P \vee Q$:
Break your proof into cases: In each case, either prove P or prove Q.

Example 3.45. Suppose that A, B, and C are sets. Prove that $A \smallsetminus (B \smallsetminus C) \subseteq (A \smallsetminus B) \cup C$.

Scratch work

Let x be arbitrary, assume $x \in A \smallsetminus (B \smallsetminus C)$, and try to prove $x \in (A \smallsetminus B) \cup C$.

Givens	Goal
$x \in A \wedge \neg(x \in B \wedge x \notin C)$	$(x \in A \wedge x \notin B) \vee x \in C$

After using one of DeMorgan's laws:

Givens	Goal
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \notin B \vee x \in C$	

For the first case we assume $x \notin B$.

Givens	Goal
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \notin B$	

For the first case we assume $x \in C$.

Givens	Goal
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \in C$	

Theorem 3.46. *Suppose that A, B, and C are sets. Then $A \smallsetminus (B \smallsetminus C) \subseteq (A \smallsetminus B) \cup C$.*

Proof. Suppose $x \in A \smallsetminus (B \smallsetminus C)$. Then $x \in A$ and $x \notin B \smallsetminus C$. Note that

$$\begin{aligned} x \notin B \smallsetminus C &= \neg(x \in B \smallsetminus C) \\ &= \neg(x \in B \wedge x \notin C) \\ &= x \notin B \vee x \in C. \end{aligned}$$

Hence either $x \notin B$ or $x \in C$.

Case 1. $x \notin B$. Then since $x \in A$, $x \in A \smallsetminus B$, so $x \in (A \smallsetminus B) \cup C$.

Case 2. $x \in C$. Then clearly $x \in (A \smallsetminus B) \cup C$.

Since $x \in A \smallsetminus (B \smallsetminus C)$ was arbitrary, we can conlude that $A \smallsetminus (B \smallsetminus C) \subseteq (A \smallsetminus B) \cup C$. □

Remark. Sometimes you may find it useful to break a proof into cases even if the cases are not suggested by a given of the form $P \vee Q$.

Example 3.47. Prove that for every $x \in \mathbb{Z}$, the remainder when x^2 is divided by 4 is either 0 or 1.

Scratch work

Givens	Goal
$x \in \mathbb{Z}$	$(x^2 \div 4 \text{ has remainder } 0) \vee (x^2 \div 4 \text{ has remainder } 1)$

Trying out a few values for x:

x	x^2	quotient of $x^2 \div 4$	remainder of $x^2 \div 4$
1	1	0	1
2	4	1	0
3	9	2	1
4	16	4	0
5	25	6	1
6	36	9	0

Case 1:

Givens	Goal
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 0
$\exists k \in \mathbb{Z}(x = 2k)$	

Case 2:

Givens	Goal
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 1
$\exists k \in \mathbb{Z}(x = 2k + 1)$	

Theorem 3.48. *For every $x \in \mathbb{Z}$, the remainder when x^2 is divided by 4 is either 0 or 1.*

Proof. Suppose x is an integer.

Case 1. x is even. Then $\exists k \in \mathbb{Z}(x = 2k)$, so $x^2 = 4k^2$. Clearly the remainder when x^2 is divided by 4 is 0.

Case 2. x is odd. Then $\exists k \in \mathbb{Z}(x = 2k + 1)$, so $x^2 = 4k^2 + 4k + 1$. Clearly in this case the remainder when x^2 is divided by 4 is 1. □

To prove a goal of the form $P \vee Q$:

If P is true, then clearly the goal $P \vee Q$ is true, so you only need to worry about the case in which P is false. You can complete the proof in this case by proving that Q is true.

Scratch work

Before using strategy:

Givens	Goal
—	$P \vee Q$
—	

After using strategy:

Givens	Goal
—	Q
—	
$\neg P$	

Form of final proof:

If P is true, then of course $P \vee Q$ is true. Now suppose P is false.
[Proof of Q goes here.]
Therefore $P \vee Q$ is false.

Example 3.49. Prove that for every $x \in \mathbb{R}$, if $x^2 \geqslant x$ then either $x \leqslant 0$ or $x \geqslant 1$.

Scratch work

Givens	Goal
$x^2 \geqslant x$	$x \leqslant 0 \vee x \geqslant 1$

Assume $x > 0$.

Givens	Goal
$x^2 \geqslant x$	$x \geqslant 1$
$x > 0$	

Theorem 3.50. *For every $x \in \mathbb{R}$, if $x^2 \geqslant x$ then either $x \leqslant 0$ or $x \geqslant 1$.*

Proof. Suppose $x^2 \geqslant x$. If $x \leqslant 0$, then of course $x \leqslant 0$ or $x \geqslant 1$. Now suppose $x > 0$. Then we can divide both sides of the inequality $x^2 \geqslant x$ by x to conclude that $x \geqslant 1$. Thus, either $x \leqslant 0$ or $x \geqslant 1$. □

To use a given of the form $P \vee Q$:
If you are given $\neg P$, then Q. If you are given $\neg Q$, then P.

We end this section with a proof for you to read without the benefit of a preliminary Scratch work analysis.

Theorem 3.51. *Suppose $m, n \in \mathbb{Z}$. If mn is even, then either m is even or n is even.*

Proof. Suppose mn is even. Then $\exists k \in \mathbb{Z}\,(mn = 2k)$. If m is even then there is nothing more to prove, so suppose m is odd. Then $\exists j \in \mathbb{Z}\,(m = 2j + 1)$. Substituting this into the equation $mn = 2k$, we get $(2j + 1)n = 2k$, so $2jn + n = 2k$, and therefore $n = 2k - 2jn = 2(k - jn)$. Since $k - jn \in \mathbb{Z}$, it follows that n is even. □

3.6 Existence and Uniqueness Proofs

In this section we consider proofs in which the goal has the form $\exists! x\, P(x)$, which is equivalent to

$$\exists x\,(P(x) \wedge \neg\exists y\,(P(y) \wedge y \neq x)).$$

Note that

$$\begin{aligned} \neg\exists y\,(P(y) \wedge y \neq x) &\longleftrightarrow \forall y \neg(P(y) \wedge y \neq x) \\ &\longleftrightarrow \forall y\,(\neg P(y) \vee y = x) \\ &\longleftrightarrow \forall y\,(P(y) \to y = x). \end{aligned}$$

Thus,

$$\exists! x\, P(x) \longleftrightarrow \exists x\,(P(x) \wedge \forall y\,(P(y) \to y = x)).$$

As the next example shows, several other formulas are also equivalent to $\exists! x\, P(x)$.

Example 3.52. Prove that the following formulas are equivalent.

(a) $\exists x\,(P(x) \wedge \forall y\,(P(y) \to y = x))$.

(b) $\exists x \forall y\,(P(y) \leftrightarrow y = x)$.

(c) $\exists x\, P(x) \wedge \forall y \forall z\,((P(y) \wedge P(z)) \to y = z)$.

Scratch work

(a) $\longrightarrow$ (b)

Givens	Goal
$P(x_0)$	$\exists x \forall y\,(P(y) \leftrightarrow y = x)$
$\forall y\,(P(y) \to y = x_0)$	

(b) $\longrightarrow$ (c)

Givens	Goal
$\forall y\,(P(y) \leftrightarrow y = x_0)$	$\exists x P(x)$
	$\forall y \forall z\,((P(y) \wedge P(z)) \to y = z)$

For the first goal, consider x_0 and let $y = x_0$ in the given, then $P(x_0) \leftrightarrow x_0 = x_0$. Of course, $x_0 = x_0$ is true, so by the $\leftarrow$ direction of the biconditional, we get $P(x_0)$.

For the second goal, we let y and z be arbitrary, assume $P(y)$ and $P(z)$, and try to prove $y = z$.

Givens	Goal
$\forall y\,(P(y) \leftrightarrow y = x_0)$	$y = z$
$P(y)$	
$P(z)$	

By the first and the second given, we get $y = x_0$. By the first and the third given, we get $z = x_0$. Thus, $y = z$.

(c) $\longrightarrow$ (a).

Givens	Goal
$P(x_0)$	$P(x_0) \wedge \forall y\,(P(y) \to y = x_0)$
$\forall y \forall z\,((P(y) \wedge P(z)) \to y = z)$	

We already know the first half of the goal, so we only need to prove the second. Let y be arbitrary, assume $P(y)$, and make $y = x_0$ our goal.

Givens	Goal
$P(x_0)$	$y = x_0$
$\forall y \forall z\,((P(y) \wedge P(z)) \to y = z)$	
$P(y)$	

Theorem 3.53. *The following formulas are equivalent.*

(a) $\exists x\,(P(x) \wedge \forall y\,(P(y) \to y = x))$.

(b) $\exists x \forall y\,(P(y) \leftrightarrow y = x)$.

(c) $\exists x\, P(x) \wedge \forall y \forall z\, ((P(y) \wedge P(z)) \to y = z)$.

Proof. (a) $\longrightarrow$ (b) By statement (a), we can let x_0 be some object such that $P(x_0)$ and $\forall y\, (P(y) \to y = x_0)$. To prove statement (b) we will show that $\forall y\, (P(y) \leftrightarrow y = x_0)$. We already know the $\longrightarrow$ direction. For the $\longleftarrow$ direction, suppose $y = x_0$. Then since we know $P(x_0)$, we can conclude $P(y)$.

(b) $\longrightarrow$ (c) By statement (b), choose x_0 such that $\forall y\, (P(y) \leftrightarrow y = x_0)$. Then, in particular, $P(x_0) \longleftrightarrow x_0 = x_0$, and since clearly $x_0 = x_0$, it follows that $P(x_0)$ is true. Thus, $\exists x\, P(x)$. To prove the second half of statement (c), let y and z be arbitrary and suppose $P(y)$ and $P(z)$. Then by our choice of x_0, it follows that $y = x_0$ and $z = x_0$, so $y = z$.

(c) $\longrightarrow$ (a) By the first half of statement (c), let x_0 be some object such that $P(x_0)$. Statement (a) will follow if we can show that $\forall y\, (P(y) \to y = x_0)$, so suppose $P(y)$. Since we now have both $P(x_0)$ and $P(y)$, by the second half of statement (c) we can conclude that $y = x_0$, as required. □

To prove a goal of the form $\exists! x\, P(x)$:
Prove $\exists x\, P(x)$ and $\forall y \forall z\, ((P(y) \wedge P(z)) \to y = z)$.

Form of final proof:

Existence: [Proof of $\exists x P(x)$ goes here.]
Uniqueness: [Proof of $\forall y \forall z\, ((P(y) \wedge P(z)) \to y = z)$ goes here.]

Example 3.54. Prove that there is a unique set A such that for every set B, $A \cup B = B$.

Scratch work

Our goal is

$$\exists! A \forall B\, (A \cup B = B).$$

For the existence of the proof, let $A = \emptyset$, then the goal becomes

$$\forall B\, (\emptyset \cup B = B).$$

For the uniqueness, we prove

$$\forall C \forall D\, (P(C) \wedge P(D) \to C = D),$$

where

$$P(C) = \forall B (C \cup B = B),$$
$$P(D) = \forall B (D \cup B = B),$$

Let C, D be arbitrary. Then

Givens	Goal
$\forall B(C \cup B = B)$	$C = D$
$\forall B(D \cup B = B)$	

Let $B = D$ in the first given, then we get $C \cup D = D$. Let $B = C$ in the first given, then we get $D \cup C = C$. But clearly $C \cup D = D \cup C$. The goal $C = D$ follows immediately.

Theorem 3.55. *There is a unique set A such that for every set B, $A \cup B = B$.*

Proof. Existence: Clearly $\forall B(\emptyset \cup B = B)$, so $\emptyset$ has the required property.

Uniqueness: Let C, D be arbitrary sets. Suppose $\forall B(C \cup B = B)$ and $\forall B(D \cup B = B)$. Applying the first of these assumptions to D we see that $C \cup D = D$, and applying the second to C we get $D \cup C = D$. But clearly $C \cup = D \cup C$, so $C = D$. □

To prove a goal of the form $\exists x\, P(x)$:
Prove $\exists x\,(P(x) \wedge \forall y\,(P(y) \to y = x))$.

Example 3.56. Prove that for every $x \in \mathbb{R}$, if $x \neq 2$ then there is a unique $y \in \mathbb{R}$ such that $2y/(y+1) = x$.

Scratch work

Let $x \in \mathbb{R}$ be arbitrary.

Givens	Goal
$x \neq 2$	$\exists! y\,(2y/(y+1) = x)$

The goal is of the form $\exists! y\, P(y)$, where $P(y) =$ "$(2y/(y+1) = x)$". The goal is equivalent to

$$\exists y\,(P(y) \wedge \forall z\,(P(z) \to z = y)),$$

i.e.,

$$\exists y\,(2y/(y+1) = x \wedge \forall z\,(2z/(z+1) = x \to z = y)).$$

Then

Givens	Goal
$x \neq 2$	$\exists y\,(2y/(y+1) = x \wedge \forall z\,(2z/(z+1) = x \to z = y))$

We solve the equation $2y/(y+1) = x$ for y:

$$\tfrac{2y}{y+1} = x \quad\Longrightarrow\quad 2y = x(y+1) \quad\Longrightarrow\quad y(2-x) = x \quad\Longrightarrow\quad y = \tfrac{x}{2-x}$$

Now

Givens	Goal
$x \neq 2$	$\frac{2y}{y+1} = x$
$y = \frac{x}{2-x}$	$\forall z\left(\frac{2z}{z+1} = x \to z = y\right)$

The first goal is easy to verify by simply plugging in $x/(2-x)$ for y. For the second, we let z be arbitrary, assume $2z(z+1) = x$, and prove $z = y$:

Givens	Goal
$x \neq 2$	$z = y$
$y = \frac{x}{2-x}$	
$\frac{2z}{z+1} = x$	

We can shoe that $z = y$ now by solving for z in the third given:

$$\tfrac{2z}{z+1} = x \quad\Longrightarrow\quad 2z = x(z+1) \quad\Longrightarrow\quad z(2-x) = x \quad\Longrightarrow\quad z = \tfrac{x}{2-x} = y$$

Theorem 3.57. *For every $x \in \mathbb{R}$, if $x \neq 2$ then there is a unique $y \in \mathbb{R}$ such that $2y/(y+1) = x$.*

Proof. Let $x \in \mathbb{R} \smallsetminus \{2\}$ be arbitrary. Let $y = x/(2-x)$, which is defined since $x \neq 2$. Then

$$\frac{2y}{y+1} = \frac{\frac{2x}{2-x}}{\frac{x}{2-x}+1} = \frac{\frac{2x}{2-x}}{\frac{2}{2-x}} = \frac{2x}{2} = x.$$

To see that this solution is unique, suppose $2z/(z+1) = x$. Then $2x = x(z+1)$, so $z(2-x) = x$. Since $x \neq 2$ we can divide both side by $2-x$ to get $z = x/(2-x) = y$. □

To use a given of the form $\exists! x\, P(x)$:
Treat this as two given statements, $\exists x\, P(x)$ and $\forall y \forall z\, ((P(y) \wedge P(z)) \rightarrow y = z)$.

Example 3.58. Suppose A, B, and C are sets, $A \cap B = \emptyset$, $A \cap C \neq \emptyset$, and A has exactly one element. Prove that $B \cap C \neq \emptyset$.

Scratch work

Givens	Goal
$A \cap B \neq \emptyset$	$B \cap C \neq \emptyset$
$A \cap C \neq \emptyset$	
$\exists! x\, (x \in A)$	

We treat the last given as two separate givens, and write out the meanings of the other givens and the goal.

Givens	Goal
$\exists x\, (x \in A \wedge x \in B)$	$\exists x\, (x \in B \wedge x \in C)$
$\exists x\, (x \in A \wedge x \in C)$	
$\exists x\, (x \in A)$	
$\forall y \forall z\, ((y \in A \wedge z \in A) \rightarrow y = z)$	

The first given tells us that we can choose b such that $b \in A$ and $b \in B$. The second given tells us that we can choose c such that $c \in A$ and $c \in C$. Then $b \in A$ and $c \in A$. The last given says that $b = c$. Since $b \in B$ and $b = c \in C$, we prove the goal.

Theorem 3.59. *Suppose A, B, and C are sets, $A \cap B \neq \emptyset$, $A \cap C \neq \emptyset$, and A has exactly one element. Prove that $B \cap C \neq \emptyset$.*

Proof. Since $A \cap B \neq \emptyset$, we can let b be such that $b \in A$ and $b \in B$. Since $A \cap C \neq \emptyset$, there is a c such that $c \in A$ and $c \in C$. Since A only has one element, we must have $b = c$. Thus $b = c \in B \cap C$ and therefore $B \cap C \neq \emptyset$. □

Chapter 4

Relations

4.1 Ordered Pairs and Cartesian Products

Definition 4.1. Suppose A and B are sets. Then the *Cartesian product* of A and B, denoted $A \times B$, is defined by

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

Example 4.2. (a) If $A = \{\text{red}, \text{green}\}$ and $B = \{2, 3, 5\}$, then

$$A \times B = \{(\text{red}, 2), (\text{red}, 3), (\text{red}, 5), (\text{gree}, 2), (\text{gree}, 3), (\text{gree}, 5)\}.$$

(b) If P is the set of all people, then

$$P \times \mathbb{N} = \{(p, n) \mid p \text{ is a person and } n \text{ is a natural number}\}.$$

(c)

$$\mathbb{R}^2 := \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \text{ and } y \text{ are real numbers}\}.$$

These are the coordinates of all the points in the plane.

Theorem 4.3. *Suppose A, B, C and D are sets.*

(a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(c) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap B)$.

(d) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

(e) $A \times \emptyset = \emptyset \times A = \emptyset$.

Proof. (a) $\subseteq$ Let $p := (x, y) \in A \times (B \cap C)$ be arbitrary. Then $x \in A$ and $y \in B \cap C$, and so $y \in B$ and $y \in C$. Hence $(x, y) \in A \times B$ and $(x, y) \in A \times C$. Thus, $(x, y) \in (A \times B) \cap (A \times C)$. Since $p \in A \times (B \cap C)$ was arbitrary, $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

$\supseteq$ Let $p := (x, y) \in (A \times B) \cap (A \times C)$ be arbitrary. Then $(x, y) \in A \times B$ and $(x, y) \in A \times C$, so $x \in A$, $y \in B$ and $y \in C$, and hence $y \in B \cap C$. Thus, $p = (x, y) \in A \times (B \cap C)$. Since $p \in (A \times B) \cap (A \times C)$ be arbitrary, $(B \cap C) \supseteq (A \times B) \cap (A \times C)$.

(d) $\subseteq$ Let $(x, y) \in (A \times B) \cup (C \times D)$ be arbitrary. Then either $(x, y) \in A \times B$ or $(x, y) \in C \times D$.

Case 1. $(x, y) \in A \times B$. Then $x \in A$ and $y \in B$, so clearly $x \in A \cup C$ and $y \in B \cup D$. Therefore $(x, y) \in (A \cup C) \times (B \cup D)$.

Case 2. $(x, y) \in C \times D$. Then $x \in C$ and $y \in D$, so clearly $x \in A \cup C$ and $y \in B \cup D$. Therefore $(x, y) \in (A \cup C) \times (B \cup D)$.

Since $(x, y) \in (A \times B) \cup (C \times D)$ was arbitrary, $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

(e) Suppose that $A \times \emptyset \neq \emptyset$. There exists $(x, y) \in A \times \emptyset$, so $x \in A$ and $y \in \emptyset$, contradicting $\emptyset$ has no elements. □

Theorem 4.4. *Suppose A and B are sets. Then $A \times B = B \times A$ if and only if either $A = \emptyset$, $B = \emptyset$, or $A = B$.*

Proof. ($\rightarrow$) Suppose $A \times B = B \times A$. If either $A = \emptyset$ or $B = \emptyset$, then there is nothing to prove, so suppose $A \neq \emptyset$ and $B \neq \emptyset$. We will show that $A = B$.

$\subseteq$ Let $x \in A$ be arbitrary. Since $B \neq \emptyset$, we can choose some $y \in B$. Then $(x, y) \in A \times B = B \times A$, so $x \in B$. Thus, $A \subseteq B$.

$\supseteq$ Let $x \in B$ be arbitrary. Since $A \neq \emptyset$, we can choose some $z \in A$. Then $(x, z) \in B \times A = A \times B$, so $x \in A$. Thus, $A \supseteq B$.

($\leftarrow$) Suppose either $A = \emptyset$, $B = \emptyset$, or $A = B$.

Case 1. $A = \emptyset$. Then $A \times B = \emptyset \times B = \emptyset = B \times \emptyset = B \times A$.

Case 2. $B = \emptyset$. Then $A \times B = A \times \emptyset = \emptyset = \emptyset \times A = B \times A$.

Case 3. $A = B$. Then $A \times B = A \times A = B \times A$. □

Definition 4.5. Suppose $P(x, y)$ is a statement with two free variables in which x ranges over a set A and y ranges over another set B. Then $A \times B$ is the set of all assignments to x and y that make sense in the statement $P(x, y)$. Also,

$$\text{truth set of } P(x, y) = \{(a, b) \in A \times B \mid P(a, b)\}.$$

Example 4.6. What are the truth sets of the following statements?

(a) "x has y children", where x ranges over the set P of all people and y ranges over $\mathbb{N}$.

$$\{(p, n) \in P \times \mathbb{N} \mid \text{the person } p \text{ has } n \text{ children}\}.$$

Note that the size of the true set is equal to the size of P, because for a given person, he or she can only have the fixed number of children.

(b) "x is located in y", where x ranges over the set C of all cities and y ranges over the set N of all countries.

$$\{(x, y) \in C \times N \mid \text{the city } c \text{ is located in the country } n\}.$$

(c) "$y = 2x - 3$", where x and y range over $\mathbb{R}$.

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x - 3\}.$$

4.2 Relations

Definition 4.7. Suppose A and B are sets. Then a set $R \subseteq A \times B$ is called a *relation from A to B*.

Example 4.8. If a free variable x ranges over A and a free variable y ranges over B, then the truth set of any statement $P(x, y)$ will be a relation from A to B.

Example 4.9. Here are some examples of relations from one set to another.

(a) Let $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$, and $R = \{(1, 3), (1, 5), (3, 3)\}$. Then $R \subseteq A \times B$, so R is a relation from A to B.

(b) Let $G = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x > y\}$. Then G is relation from $\mathbb{R}$ to $\mathbb{R}$.

(c) Let $A = \{1, 2\}$ and $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Let $E = \{(x, y) \in A \times B \mid x \in y\}$. Then E is a relation from A to B. In this case, $E = \{(1, \{1\}), (1, \{1, 2\}), (2, \{2\}), (2, \{1, 2\})\}$.

For the next three examples, let S be the set of all students at your school, R the set of all dorm rooms, P the set of all professors, and C the set of all course.

(d) Let $L = \{(s, r) \in S \times R \mid \text{the student } s \text{ lives in the dorm room } r\}$. Then L is a relation from S to R.

(e) Let $E = \{(s, c) \in S \times C \mid \text{the student } s \text{ is enrolled in the course } c\}$. Then E is a relation from S to C.

(f) Let $T = \{(c, p) \in C \times P \mid \text{the course } c \text{ is taught by the professor } p\}$. Then T is a relation from C to P.

Definition 4.10. Suppose R is a relation from A to B. Then the domain of R is the set

$$\mathrm{Dom}(R) = \{a \in A \mid \exists b \in B((a, b) \in R)\}.$$

The range of R is the set

$$\mathrm{Ran}(R) = \{b \in B \mid \exists a \in A((a, b) \in R)\}.$$

The inverse of R is the relation R^{-1} from B to A defined as follows:

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

Finally, suppose R is a relation from A to B and S is a relation from B to C. Then the *composition* of S and R is the relation $S \circ R$ from A to C defined as follows:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B((a, b) \in R \text{ and } (b, c) \in S)\}.$$

Note that we have assumed that the second coordinates of pairs in R and the first coordinates of pairs in S both come from the same set.

Example 4.11. Let S, R, C, and P be the sets of students, dorm rooms, course, and professors at your school. Let L, E, and T be the relations defined in parts (d)-(f) of Example 4.9. Describe the following relations.

(a)

$$\begin{aligned} E^{-1} &= \{(c,s) \in C \times S \mid (s,c) \in E\} \\ &= \{(c,s) \in C \times S \mid \text{ the student } s \text{ is enrolled in the course } c\}. \end{aligned}$$

(b) Because L^{-1} is a relation from R to S and E is a relation from S to C, $E \circ L^{-1}$ will be a relation from R to C defined as follows.

$$\begin{aligned} E \circ L^{-1} &= \{(r,c) \in R \times C \mid \exists s \in S((r,s) \in L^{-1} \text{ and } (s,c) \in E)\} \\ &= \{(r,c) \in R \times C \mid \exists s \in S((s,r) \in L \text{ and } (s,c) \in E)\} \\ &= \{(r,c) \in R \times C \mid \exists s \in S(\text{the student } s \text{ lives in the dorm} \\ &\qquad \text{room } r \text{ and is enrolled in the course } c)\}. \end{aligned}$$

(c) Because E is a relation from S to C and E^{-1} is a relation from C to S, $E^{-1} \circ E$ is the relation from S to S defined as follows.

$$\begin{aligned} E^{-1} \circ E &= \{(s,t) \in S \times S \mid \exists c \in C((s,c) \in E \text{ and } (c,t) \in E^{-1})\} \\ &= \{(s,t) \in S \times S \mid \exists s \in S((s,c) \in E \text{ and } (t,c) \in E)\} \\ &= \{(s,t) \in S \times S \mid \exists s \in S(\text{the student } s \text{ is enrolled in the} \\ &\qquad \text{course } c\text{, and so is the student } t)\} \\ &= \{(s,t) \in S \times S \mid \text{there is some course that the student } s \\ &\qquad \text{and } t \text{ are both enrolled in}\}. \end{aligned}$$

(d) Because E^{-1} is a relation from C to S and E is a relation from S to C, $E \circ E^{-1}$ is the relation from C to C defined as follows.

$$\begin{aligned} E \circ E^{-1} &= \{(c,d) \in C \times C \mid \exists s \in S((c,s) \in E^{-1} \text{ and } (s,d) \in E)\} \\ &= \{(c,d) \in C \times C \mid \exists s \in S((s,c) \in E \text{ and } (s,d) \in E)\} \\ &= \{(c,d) \in C \times C \mid \exists s \in S(\text{the student } s \text{ is enrolled in the} \\ &\qquad \text{course } c\text{, and he is also enrolled in the course } d)\} \\ &= \{(c,d) \in C \times C \mid \text{there is some student who is enrolled in} \\ &\qquad \text{both of the courses } c \text{ and } d\}. \end{aligned}$$

(e) We saw in part (b) that $E \circ L^{-1}$ is a relation from R to C, and T is a relation from C to P, so $T \circ (E \circ L^{-1})$ is the relation from R to P defined as follows.

$$\begin{aligned} T \circ (E \circ L^{-1}) &= \{(r,p) \in R \times P \mid \exists c \in ((r,c) \in E \circ L^{-1} \text{ and } (c,p) \in T)\} \\ &= \{(r,p) \in R \times P \mid \exists c \in C(\text{some student who lives in the room } r \text{ is enrolled in the} \\ &\qquad \text{course } c\text{, and } c \text{ is taught by the professor } p)\} \\ &= \{(r,p) \in R \times P \mid \text{some student who lives in the room } r \text{ is enrolled in some course} \\ &\qquad \text{taught by the professor } p\}. \end{aligned}$$

(f) Note that L^{-1} is a relation from R to S, and $T \circ E$ is a relation from S to P, so $(T \circ E) \circ L^{-1}$ is the relation from R to P defined as follows.

$$\begin{aligned}(T \circ E) \circ L^{-1} &= \{(r,p) \in R \times P \mid \exists s \in S((r,s) \in L^{-1} \text{ and } (s,p) \in T \circ E)\} \\ &= \{(r,p) \in R \times P \mid \exists s \in S((s,r) \in L \text{ and } (s,p) \in T \circ E)\} \\ &= \{(r,p) \in R \times P \mid \exists s \in S(\text{the student } s \text{ lives in the room } r\text{, and is enrolled} \\ &\qquad \text{in some course taught by the professor } p)\} \\ &= \{(r,p) \in R \times P \mid \text{some student who lives in the room } r \text{ is enrolled in some} \\ &\qquad \text{course taught by the professor } p\}.\end{aligned}$$

Theorem 4.12. *Suppose R is a relation from A to B, S is a relation from B to C, and T is a relation from C to D. Then*

(a) $(R^{-1})^{-1} = R$.

(b) $\mathrm{Dom}(R^{-1}) = \mathrm{Ran}(R)$.

(c) $\mathrm{Ran}(R^{-1}) = \mathrm{Dom}(R)$.

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

(e) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Proof. (a) Note that R^{-1} is a relation from B to A, so $(R^{-1})^{-1}$ is a relation from A to B, just like R. To see that $(R^{-1})^{-1} = R$, let $(a,b) \in A \times B$ be arbitrary. Then

$$(a,b) \in (R^{-1})^{-1} \text{ iff } (b,a) \in R^{-1} \text{ iff } (a,b) \in R.$$

(b) Note that $\mathrm{Dom}(R^{-1}) \subseteq B$ and $\mathrm{Ran}(R) \subseteq B$. Let $b \in B$ be arbitrary. Then

$$b \in \mathrm{Dom}(R^{-1}) \text{ iff } \exists a \in A((b,a) \in R^{-1}) \text{ iff } \exists a \in A((a,b) \in R) \text{ iff } b \in \mathrm{Ran}(R).$$

(d) Clearly $T \circ (S \circ R)$ and $(T \circ S) \circ R$ are both relations from A to D. Let $(a,d) \in A \times D$ be arbitrary. We will prove that $T \circ (S \circ R) = (T \circ S) \circ R$.

$\subseteq$ Suppose that $(a,d) \in T \circ (S \circ R)$. Then there exists some $c \in C$ such that $(a,c) \in S \circ R$ and $(c,d) \in T$. Since $(a,c) \in S \circ R$, there exists some $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$. Now since $(b,c) \in S$ and $(c,d) \in T$, $(b,d) \in T \circ S$. Since $(a,b) \in R$ and $(b,d) \in T \circ S$, $(a,d) \in (T \circ S) \circ R$.

$\supseteq$ Suppose that $(a,d) \in (T \circ S) \circ R$. A similar argument shows that $(a,d) \in T \circ (S \circ R)$.

Thus, $T \circ (S \circ R) = (T \circ S) \circ R$. □

4.3 More About Relations

Notation 4.13. If R is a relation from A to B, $x \in A$ and $y \in B$, we use xRy to mean $(x,y) \in R$.

Example 4.14. $x < y$, $x \in Y$, and $x \subseteq y$, where $<$, $\in$, and $\subseteq$ are relations.

Example 4.15. As in the Example 4.9(d), for any student s and dorm room r, sLr means $(s,r) \in L$, or in other words, the student lives in the dorm room r.

Definition 4.16. Suppose R is a relation from A to B and S is a relation from B to C. Then the *composition* of S and R is the relation $S \circ R$ from A to C defined as follows:

$$\begin{aligned} S \circ R &= \{(a,c) \in A \times C \mid \exists b \in B((a,b) \in R \text{ and } (b,c) \in S)\} \\ &= \{(a,c) \in A \times C \mid \exists b \in B\,(aRb \text{ and } bSc)\}. \end{aligned}$$

Notation 4.17. Let $A = \{1,2,3\}$, $B = \{3,4,5\}$, and $R = \{(1,3),(1,5),(3,3)\}$. We use a figure to shows the relation R from A to B.

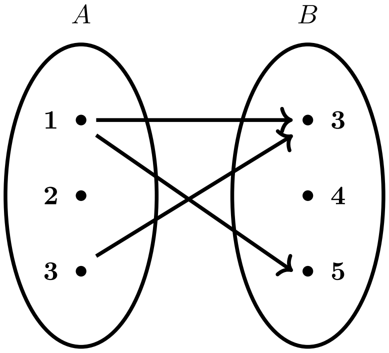


Figure 4.1

In the figure, each of these sets is represented by an oval, with the elements of the set represented by dots inside the oval. Each ordered pair $(a,b) \in R$ is represented by an arrow from the dot representing a to the dot representing b. The dots representing the elements of A and B in such a picture are called *vertices*, and the arrows representing the ordered pairs in R are called *edges*.

You could find the domain of R by locating those vertices in A that have edges pointing away from them. The range of R would consist of those elements of B whose vertices have edges pointing toward them. For the relation R shown in Figure 1, we have $\mathrm{Dom}(R) = \{1,3\}$ and $\mathrm{Ran}(R) = \{3,5\}$. A picture of R^{-1} would look just like a picture of R but with directions of all the arrows reversed.

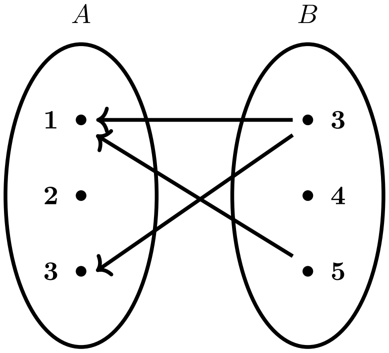


Figure 4.2

Consider again the relations E and T from Example 4.9(e) and (f), Figure 4.3 shows what part of both relations might look like.

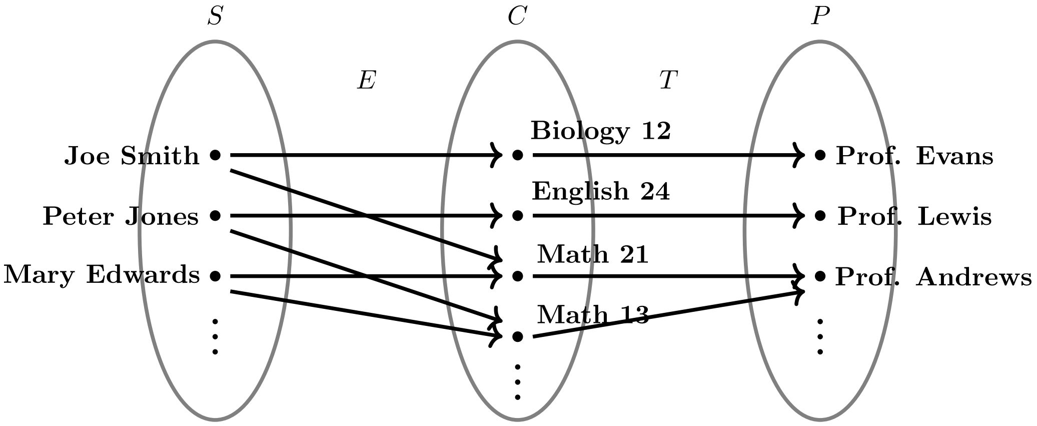


Figure 4.3

According to the definition of composition,

$$\begin{aligned} T \circ E &= \{(s,p) \in S \times P \mid \exists c \in C\,(sEc \text{ and } cTp)\} \\ &= \{(s,p) \in S \times P \mid \exists c \in C\,(\text{in Figure 4.3, there is an arrow} \\ &\quad \text{from } s \text{ to } c \text{ and an arrow from } c \text{ to } p)\} \\ &= \{(s,p) \in S \times P \mid \text{in Figure 4.3, you can get from } s \text{ to } p \text{ in} \\ &\quad \text{two steps by following the arrows}\}. \end{aligned}$$

For example, starting at the vertex labeled Mary Edwards, we can get to Prof. Andrews in two steps (going by way of either Math 21 or Math 13), so (Mary Edwards, Prof. Andrews) $\in T \circ E$.

Definition 4.18. Let A be a set. If $R \subseteq A \times A$, then R is a (*binary*) *relation* on A.

Example 4.19. (a) The relation G in Example 4.9(b) is a reltion on $\mathbb{R}$.

(b) The relation $E^{-1} \circ E$ from Example 4.11(c) is a relation on S, and the relation $E \circ E^{-1}$ from Example 4.11(d) is a relation on C.

Example 4.20. We have the following examples.

(a) Let $A = \{1,2\}$ and $B = \mathcal{P}(A)$. Then $S = \{(x,y) \in B \times B \mid x \subseteq y\}$ is a relation on B.

(b) Let A be a set. Then $i_A = \{(x,y) \in A \times A \mid x = y\} = \{(x,x) \mid x \in A\}$ is a relation on A. It is sometimes called the *identity relation on A*. For example, if $A = \{1,2,3\}$, then $i_A = \{(1,1),(2,2),(3,3)\}$.

(c) For $r \in \mathbb{R}^+$, $D_r = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid |x-y| < r\}$ is a relation on $\mathbb{R}$.

Notation 4.21. Suppose R is a relation on a set A. To draw a picture of R, we draw just one copy of A and then connect the vertices representing the elements of A with edges to represent the ordered pairs in R. For example, Figure 4.4 shows a picture of the relation S from Example 4.20(a).

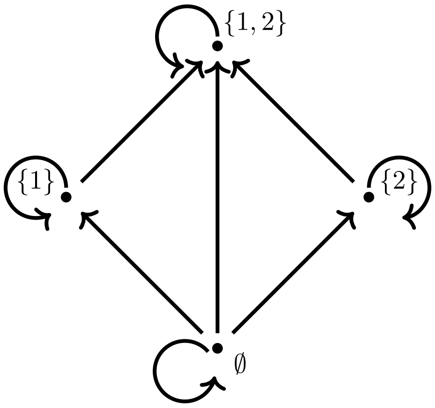


Figure 4.4

Picture like the one in Figure 4.4 are called *directed graphs.* Edges that go from a vertex to itself are called *loops.* In fact, in Figure 4.4, there is a loop at every vertex.

Definition 4.22. Suppose R is a relation on A.

(a) R is said to be *reflexive* on A if $\forall x \in A\,(xRx)$.

(b) R is *symmetric* if $\forall x \in A \forall y \in A(xRy \to yRx)$.

(c) R is transitive if $\forall x \in A \forall y \in A \forall z \in A\,((xRy \wedge yRz) \to xRz)$.

Remark. If R is reflexive on A, then the directed graph representing R will have loops at all vertices. If R is symmetric, then whenever there is an edge from x to y, there will also be an edge from y to x. If R is transitive, then whenever there is edge from x to y and y to z, there is also an edge from x to z.

Example 4.23. (a) Is the relation G from Example 4.9(b) reflexive? Is it symmetric? Transitive?

There is a x such that $x \not> x$, so G is not reflexive. There is $x \in \mathbb{R}$ and $y \in \mathbb{R}$ such that $x > y$ and $y \not> x$, so G is not symmetric. It is transitive because $\forall x \in \mathbb{R} \forall y \in \mathbb{R} \forall z \in \mathbb{R}\,((x > y \wedge y > z) \to x > z)$.

(b) Are the relations in Example 4.20 reflexive, symmetric, or transitive?

In Example 4.20(a), S is reflexive, not symmetric, and transitive.

In Example 4.20(b), S is reflexive, symmetric, and transitive.

In Example 4.20(c), S is reflexive and symmetric. It is not transitive, because for $x = a$, $y = a + 2r/3$, and $z = a + 4r/3$, we have that $|x - y| = 2r/3 < r$, $|y - z| = 2r/3 < r$, but $|x - z| = 4r/3 > r$.

Theorem 4.24. *Suppose R is a relation on a set A.*

(a) R is reflexive iff $i_A \subseteq R$, where i_A is the identity relation on A.

(b) R is symmetric iff $R = R^{-1}$.

(c) R is transitive iff $R \circ R = R$.

Proof. (b) ($\rightarrow$) Suppose R is symmetric. Let $(x, y) \in R$ be arbitrary. Then xRy, so yRx since R is symmetric, and hence $(y, x) \in R$. Hence $(x, y) \in R^{-1}$ by the definition of R^{-1}. Since (x, y) was arbitrary, $R \subseteq R^{-1}$. On the other hand, let $(x, y) \in R^{-1}$ be arbitrary. Then $(y, x) \in R$, and so $(x, y) \in R$ since R is symmetric. Since (x, y) was arbitrary, $R^{-1} \subseteq R$. Thus, $R = R^{-1}$.

($\leftarrow$) Suppose that $R = R^{-1}$. Let $x, y \in A$ be arbitrary. Suppose xRy. Then $(x, y) \in R = R^{-1}$, so $(y, x) \in R$, and hence yRx. Thus, $\forall x \in A \forall y \in A(xRy \rightarrow yRx)$. □

4.4 Ordering Relations

Definition 4.25. Suppose R is a relation on a set A. Then R is said to be *antisymmetric* if $\forall x \in A \forall y \in A ((xRy \wedge yRx) \rightarrow x = y)$.

Example 4.26. We have the following examples.

(a) Let $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leqslant y\}$. Then L is antisymmetric because for any $x, y \in A$, if $x \leqslant y$ and $y \leqslant x$, we must have $x = y$.

(b) The relation $S = \{(x, y) \in B \times B \mid x \subseteq y\}$ from Example 4.20(a) is antisymmetric.

Definition 4.27. Suppose R is a relation on a set A. Then R is called a *partial order on A* if it is reflexive, transitive, and antisymmetric. It is called a *total order on A* if it is a partial order, and in addition it has the following property:

$$\forall x \in A \forall y \in A (xRy \vee yRx).$$

Example 4.28. The relations L and S from Example 4.26 are both partial orders. L is total order because for any $x, y \in \mathbb{R}$, either $x \leqslant y$ or $y \leqslant x$. S is not a total order because we have that $\{1\} \not\subseteq \{2\}$ and $\{2\} \not\subseteq \{1\}$.

Example 4.29. Which of the following relations are partial orders? Which are total orders?

(a) Let A be any set, $B = \mathcal{P}(A)$, and $S = \{(x, y) \in B \times B \mid x \subseteq y\}$.

From 4.23(b), S is reflexive and transitive. From Example 4.26, S is antisymmetric. Hence S is a partial order. Similar to Example 4.28, S is not a total order.

(b) Let $A = \{1, 2\}$ and $B = \mathcal{P}(A)$. Let

$$\begin{aligned} R &= \{(x, y) \in B \times B \mid y \text{ has at least as many elements as } x\} \\ &= \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{2\}), (\{1\}, \{1, 2\}), \\ &\quad (\{2\}, \{1\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}. \end{aligned}$$

Note that $(\{1\}, \{2\}) \in R$ and $(\{2\}, \{1\}) \in R$, but $\{1\} \neq \{2\}$. Thus, R is not antisymmetric, so it is not a partial order.

(c) $D = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x \text{ divides } y\}$.

Note that D is reflexive, transitive, and antisymmetric, so D is a partial order. D is not a total order because $(3, 5) \notin D$ and $(5, 3) \notin D$.

(d) $G = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geqslant y\}$.

Note that D is reflexive, transitive, and antisymmetric, so D is a partial order. D is total order because for any $x, y \in \mathbb{R}$, either $x \geqslant y$ or $y \geqslant x$.

Definition 4.30. Suppose R is a partial order on a set A, $B \subseteq A$, and $b \in B$. Then b is called an *R-smallest element of B* if $\forall x \in B\,(bRx)$. It is called an *R-minimal element of B* if $\neg\exists x \in B\,(xRb \wedge x \neq b)$.

Example 4.31. (a) Let $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leqslant y\}$. Let $B = \{x \in \mathbb{R} \mid x \geqslant 7\}$. What are the L-minimal elements and L-smallest elements of B. What about the set $C = \{x \in \mathbb{R} \mid x > 7\}$.

Clearly, $7 \leqslant x$ for every $x \in B$, so $\forall x \in B\,(7Lx)$, thus 7 is an L-smallest element of B. 7 is also an L-minimal element because $\neg\exists x \in B\,(x \leqslant 7 \wedge x \neq 7)$. There are no other smallest or minimal elements.

C has no L-smallest or L-minimal elements.

(b) Let $D = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x \text{ divides } y\}$. Let $B = \{3, 4, 5, 6, 7, 8, 9\}$. Does B have any D-smallest or D-minimal elements?

Since $\exists 3 \in B\,((3 \mid 6) \wedge 3 \neq 6)$ and $\exists 3 \in B\,((3 \mid 9) \wedge 3 \neq 9)$, 6 and 9 are not minimal. Since $\exists 4 \in B\,((4 \mid 8) \wedge 4 \neq 8)$, 8 is not minimal. Since $\neg\exists x \in B\,((x \mid 5) \wedge x \neq 5)$, 5 is minimal. Similarly, 3 and 7 are minimal.

Since there is no $b \in B$ such that $b \mid x$ for any $x \in B$, i.e., there is no $b \in B$ such that $\forall x \in B\,(bDx)$, B has no smallest element.

Theorem 4.32. *Suppose R is a partial order on a set A, and $B \subseteq A$.*

(a) If B has a smallest element, then this smallest element is unique.

(b) Suppose b is the smallest element of B. Then b is also a minimal element of B, and it is the only minimal element.

(c) If R is a total order and b is a minimal element of B, then b is the smallest element of B.

Proof. (a) Suppose b and c are smallest elements of B. Then $\forall x \in B\,(bRx)$ and $\forall y \in B\,(cRy)$. Hence in particular, bRc and cRb. Since R is a partial order, it is antisymmetric, so $b = c$.

(b) To show b is minimal, we need to show that $\neg\exists x \in B\,(xRb \wedge x \neq b)$. By quantifier negation law, it is equivalent to show that $\forall x \in B\,(\neg xRb \vee x = b)$, which is equivalent to $\forall x \in B\,(xRb \rightarrow x = b)$. Let $x \in B$ be arbitrary. Suppose that xRb. Since b is the smallest element of B, bRx. Now by antisymmetry it follows that $x = b$. Thus, b is a minimal element.

Suppose c is also a minimal element. Since b is the smallest element of B, bRc. Suppose that $b \neq c$, then $\exists b \in B\,(bRc \wedge b \neq c)$, contradicting the minimality of c. Thus, $b = c$.

(c) We need to show that $\forall x \in B\,(bRx)$. If Let $x \in B$ be arbitrary. If $x = b$, then since R is reflexive, bRx, and we are done. Now suppose $x \neq b$. Since R is a total order, we have that either xRb or bRx. Suppose xRb, then $\exists x \in B\,(xRb \wedge x \neq b)$, contradicting the minimality of b. Thus, bRx. □

Example 4.33. (a) Find the smallest set of real numbers X such that $5 \in X$ and for all real numbers x and y, if $x \in X$ and $x < y$ then $y \in X$.

Let $\mathcal{B} = \mathcal{P}(\mathbb{R})$ and $R = \{(x, y) \in \mathcal{B} \times \mathcal{B} \mid x \subseteq y\}$. Then R is a partial order on $\mathcal{B}$. Let

$$\mathcal{F} = \{X \subseteq \mathbb{R} \mid 5 \in X \wedge \forall x \in \mathbb{R} \forall y \in \mathbb{R}\,(x \in X \wedge x < y \to y \in X)\}.$$

Then $\mathcal{F} \subseteq \mathcal{B}$. Let $A = \{y \in \mathbb{R} \mid y \geqslant 5\}$. Let $X \in \mathcal{F}$ be arbitrary. We will show that $A \subseteq X$.

Let $y \in A$, then $y \geqslant 5$. If $y = 5$, then $y = 5 \in X$. Assume now that $y > 5$. Since $5 \in X$ and $5 < y$, we have that $y \in X$ by the property of X. Hence $A \subseteq X$. Thus, $\forall X \in \mathcal{F}\,(A \subseteq X)$, so A is the R-smallest element of $\mathcal{F}$.

(b) Find the smallest set of real numbers X such that $X \neq \emptyset$ and for all real numbers x and y, if $x \in X$ and $x < y$ then $y \in X$.

Let $\mathcal{B} = \mathcal{P}(\mathbb{R})$ and $R = \{(x, y) \in \mathcal{B} \times \mathcal{B} \mid x \subseteq y\}$. Then R is a partial order on $\mathcal{B}$. Let

$$\mathcal{F} = \{X \subseteq \mathbb{R} \mid X \neq \emptyset \text{ and } \forall x \in \mathbb{R} \forall y \in \mathbb{R}\,(x \in X \wedge x < y \to y \in X)\}.$$

Then $\mathcal{F} \subseteq \mathcal{B}$. Then $\{1\} \in F$ since $\neg\exists x \in \mathcal{F}\,(x \subseteq \{1\} \wedge x \neq \{1\})$. Hence $\{1\}$ is a minimal element of $\mathcal{F}$. Similarly, $\{2\}$ is a minimal element of $\mathcal{F}$. Hence $\mathcal{F}$ have no smallest elements by Theorem 4.32(b).

Definition 4.34. Suppose R is a partial order on A, $B \subseteq A$, and $a \in A$. Then a is called a *lower bound* for B if $\forall x \in B(aRx)$. Similarly, it is an *upper bound* for B if $\forall x \in B(xRa)$.

Definition 4.35. Suppose R is a partial order on A, and $B \subseteq A$. Let U be the set of all upper bounds for B, and L the set of all lower bounds. If U has a smallest element, then this smallest element is called the *least upper bound* (*l.u.b*) of B. If L has a largest element, then this largest element is called the *greatest lower bound* (*g.l.b*) of B.

Example 4.36. Let $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leqslant y\}$, a total order on $\mathbb{R}$. Let $B = \{1/n \mid n \in \mathbb{Z}^+\} = \{1, 1/2, 1/3, 1/4, 1/5, \dots\} \subseteq \mathbb{R}$.

Clearly, $\{x \in \mathbb{R} \mid x \geqslant 1\}$ is the set of upper bounds for B. The smallest element of this set is 1, so 1 is the l.u.b of B.

Clearly, $\{x \in \mathbb{R} \mid x \leqslant 0\}$ is the set of lower bounds for B. The largest element of this set is 0, so 0 is the g.l.b of B.

Theorem 4.37. *Suppose A is a set, $\mathcal{F} \subseteq \mathcal{P}(A)$, and $\mathcal{F} \neq \emptyset$. Then the l.u.b of $\mathcal{F}$ is $\cup\mathcal{F}$ and the g.l.b of $\mathcal{F}$ is $\cap\mathcal{F}$.*

4.5 *Closures

Definition 4.38. Suppose R is a relation on a set A. Then the *reflexive closure* of R is the smallest set $S \subseteq A \times A$ such that $R \subseteq S$ and R is reflexive, if there is such a smallest set. In other words, a relation $S \subseteq A \times A$ is the *reflexive closure* of R if it has the following three properties:

(a) $R \subseteq S$.

(b) S is reflexive.

(c) For every relation $T \subseteq A \times A$, if $R \subseteq T$ and T is reflexive, then $S \subseteq T$.

Remark. According to Theorem 4.32, if a set has a smallest element, then it can have only one smallest element. Thus, if a relation R has a reflexive closure, then this reflexive closure must be unique.

Theorem 4.39. *Suppose R is a relation on A. Then R has a reflexive closure.*

Proof. Let $S := R \cup i_A$, where i_A is the identity relation on A. We will show that S is the reflexive closure of A.

(a) $R \subseteq R \cup i_A = S$.

(b) Since $i_A \subseteq R \cup i_A = S$, S is reflexive by Theorem 4.24(a).

(c) Suppose T is a relation on A, $R \subseteq T$, and T is reflexive. Then $i_A \subseteq T$ by Theorem 4.24(a). Hence $S = R \cup i_A \subseteq T$. □

Example 4.40. Let $M = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$. By Theorem 4.39, the reflexive closure of M would be the relation

$$\begin{aligned} M \cup i_{\mathbb{R}} &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (x, y) \in M \vee (x, y) \in i_{\mathbb{R}}\} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y \vee x = y\} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leqslant y\}. \end{aligned}$$

Example 4.41. Let $P = \{(x, y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid x \subsetneq y\}$. By Theorem 4.39, the reflexive closure of P would be the relation

$$\begin{aligned} P \cup i_{\mathcal{P}(A)} &= \{(x, y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid (x, y) \in P \vee (x, y) \in i_{\mathcal{P}(A)}\} \\ &= \{(x, y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid x \subsetneq y \vee x = y\} \\ &= \{(x, y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid x \subseteq y\}. \end{aligned}$$

Definition 4.42. Suppose R is a relation on A. Then R is said to be *irreflexive* if $\forall x \in A\,((x, x) \notin R)$. R is called a *strict partial order* if it is irreflexive and transitive. It is called a *strict total order* if it is a strict partial order, and in addition it satisfies the following requirement, called *trichotomy*:

$$\forall x \in A \forall y \in A\,(xRy \vee yRx \vee x = y).$$

Definition 4.43. Suppose R is a relation on a set A. Then the *symmetric closure* of R is the smallest set $S \subseteq A \times A$ such that $R \subseteq S$ and R is symmetric, if there is such a smallest set. In other words, a relation $S \subseteq A \times A$ is the *symmetric closure* of R if it has the following three properties:

(a) $R \subseteq S$.

(b) S is symmetric.

(c) For every relation $T \subseteq A \times A$, if $R \subseteq T$ and T is symmetric, then $S \subseteq T$.

Definition 4.44. Suppose R is a relation on a set A. Then the *transitive closure* of R is the smallest set $S \subseteq A \times A$ such that $R \subseteq S$ and R is transitive, if there is such a smallest set. In other words, a relation $S \subseteq A \times A$ is the *transitive closure* of R if it has the following three properties:

(a) $R \subseteq S$.

(b) S is transitive.

(c) For every relation $T \subseteq A \times A$, if $R \subseteq T$ and T is transitive, then $S \subseteq T$.

Theorem 4.45. *Suppose R is a relation on a set A. Then R has a symmetric closure.*

Proof. Let $S := R \cup R^{-1}$. We will show that S is the symmetric closure of A.

(a) $R \subseteq R \cup R^{-1} = S$.

(b) Let $(x, y) \in S$ be arbitrary. Since $S = R \cup R^{-1}$, we have that $(x, y) \in R$ or $(x, y) \in R^{-1}$. If $(x, y) \in R$, then $(y, x) \in R^{-1} \subseteq S$. If $(x, y) \in R^{-1}$, then $(y, x) \in R \subseteq S$. Thus, S is symmetric.

(c) Suppose T is a relation on A, $R \subseteq T$, and T is symmetric. Let $(x, y) \in S$ be arbitrary. Then $(x, y) \in R$ or $(x, y) \in R^{-1}$. If $(x, y) \in R$, then since $R \subseteq T$, $(x, y) \in T$. If $(x, y) \in R^{-1}$, then $(y, x) \in R$, so $(y, x) \in T$ since $R \subseteq T$. But T is symmetric, so it follows that $(x, y) \in T$. Thus, $S \subseteq T$. □

Theorem 4.46. *Suppose R is relation on a set A. Then R has a transitive closure.*

Proof. Let $\mathcal{F} = \{T \subseteq A \times A \mid R \subseteq T \text{ and } T \text{ is transitive}\}$. It is straightforward to see that $A \times A \subseteq \mathcal{F}$. Then $\mathcal{F} \neq \emptyset$. Let $S := \cap\mathcal{F}$. We will show that S is the transitive closure of A.

(a) Let $(x, y) \in R$ be arbitrary. Let $T \in \mathcal{F}$ be arbitrary. Then $R \subseteq T$, so $(x, y) \in T$. Hence $\forall T \in \mathcal{F}\,((x, y) \in T)$, so $(x, y) \in \cap\mathcal{F} = S$. Thus, $R \subseteq S$.

(b) Let $(x, y) \in S$ and $(y, z) \in S$ be arbitrary. Let $T \in \mathcal{F}$ be arbitrary. Since $(x, y) \in S = \cap\mathcal{F}$, $(x, y) \in T$. Similarly, $(y, z) \in T$. Since $T \in \mathcal{F}$, T is transitive. Hence $(x, z) \in T$. Thus, $\forall T \in \mathcal{F}\,((x, z) \in T)$, so $(x, z) \in \cap\mathcal{F} = S$. Therefore, S is transitive.

(c) Suppose T is a relation on A, $R \subseteq T$, and T is transitive. Then $T \in \mathcal{F}$. Then $S = \cap\mathcal{F} \subseteq T$ by exercise 9 of Section 3.3. □

4.6 Equivalence Relations

Definition 4.47. Suppose R is a relation on a set A. Then R is called an *equivalence relation* on A if it is reflexive, symmetric, and transitive.

Example 4.48. We have the following examples.

(a) Let A be a set, then the identity relation i_A is an equivalence relation on A.

(b) Let T be the set of all triangles. Let

$$C = \{(s, t) \in T \times T \mid \text{the triangle } s \text{ is congruent to the triangle } t\}.$$

Then C is an equivalence relation on T.

Definition 4.49. Suppose A is a set and $\mathcal{F} \subseteq \mathcal{P}(A)$. We will say that $\mathcal{F}$ is *pairwise disjoint* if every pair of distinct elements of $\mathcal{F}$ are disjoint, or in other words,

$$\forall X \in \mathcal{F} \forall Y \in \mathcal{F}(X \neq Y \to X \cap Y = \emptyset),$$

which is equivalent to

$$\forall X \in \mathcal{F} \forall Y \in \mathcal{F}(X \cap Y \neq \emptyset \to X = Y).$$

$\mathcal{F}$ is called a *partition* of A if it has the following properties:

(a) $\cup\mathcal{F} = A$.

(b) $\mathcal{F}$ is pairwise disjoint.

(c) $\forall X \in \mathcal{F}(X \neq \emptyset)$.

Example 4.50. Let $A = \{1, 2, 3, 4\}$ and $\mathcal{F} = \{\{2\}, \{1, 3\}, \{4\}\}$. Then $\mathcal{F} \subseteq \mathcal{P}(A)$.

(a) $\cup\mathcal{F} = \{2\} \cup \{1, 3\} \cup \{4\} = \{1, 2, 3, 4\} = A$.

(b) $\mathcal{F}$ is pairwise disjoint, since $\{2\} \cap \{1, 3\} = \emptyset$, $\{2\} \cap \{4\} = \emptyset$, and $\{1, 3\} \cap \{4\} = \emptyset$.

(c) All the sets in $\mathcal{F}$ are nonempty.

Thus, $\mathcal{F}$ is a partition of A.

Definition 4.51. Suppose R is an equivalence relation on a set A, and $x \in A$. Then the *equivalence class of x with respect to R* is the set

$$[x]_R = \{y \in A \mid yRx\}.$$

If R is clear from context, then we just write $[x]$ instead of $[x]_R$. The set of all equivalence classes of elements of A is called *A modulo R*, and is denoted A/R. Thus,

$$A/R = \{[x]_R \mid x \in A\} = \{X \subseteq A \mid \exists x \in A(X = [x]_R)\}.$$

Example 4.52. Let S be the relation on $\mathbb{R}$ defined as follows:

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{Z}\}.$$

We will show that S is an equivalence relation.

(a) For any $x \in \mathbb{R}$, $(x, x) \in S$ since $(x, x) \in \mathbb{R} \times \mathbb{R}$ and $x - x = 0 \in \mathbb{Z}$. Hence S is reflexive.

(b) Let $(x, y) \in S$ be arbitrary. Then $(x, y) \in \mathbb{R} \times \mathbb{R}$ and $x - y \in \mathbb{Z}$. Clearly, $(y, x) \in \mathbb{R} \times \mathbb{R}$ and $y - x = -(x - y) \in \mathbb{Z}$. Hence $(y, x) \in S$. Thus, S is symmetric.

(c) Let $(x, y) \in S$ and $(y, z) \in S$ be arbitrary. Then $(x, y) \in \mathbb{R}$ and $(y, z) \in \mathbb{R}$, so $x \in \mathbb{R}$ and $z \in \mathbb{R}$, and hence $(x, z) \in \mathbb{R}$. Also, we have that $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$, so $x - z = (x - y) + (y - z) \in \mathbb{Z}$. Thus, $(x, z) \in S$, so S is transitive.

Therefore, S is an equivalence relation on $\mathbb{R}$. For example,

$$\begin{aligned}[2.73] &= \{y \in \mathbb{R} \mid (y, x) \in \mathbb{R}\} \\ &= \{y \in \mathbb{R} \mid y - x \in \mathbb{Z}\} \\ &= \{\dots, -1.27, -0.27, 0.73, 1.73, 2.73, 3.73, 4.73, 5.73, \dots\}.\end{aligned}$$

In general, for any $x \in \mathbb{R}$,

$$[x] = \{\dots, x-3, x-2, x-1, x, x+1, x+2, x+3, \dots\}.$$

By the following lemma, We have that $[2.73] = [0.73]$. In general, for any $x \in \mathbb{R}$, there is always a $y \in [0, 1)$ such that $y - x \in \mathbb{Z}$, so $[x] = [y]$.

Lemma 4.53. Suppose R is an equivalence relation on A. Then

(a) For every $x \in A$, $x \in [x]$.

(b) For every $x \in A$ and $y \in A$, $y \in [x]$ if and only if $[y] = [x]$.

Proof. (a) Let $x \in A$ be arbitrary. Since R is reflexive, xRx. Then by the definition of equivalence class, $x \in [x]$.

(b) $(\rightarrow)$ Suppose $y \in [x]$. Then yRx. We will prove that $[y] = [x]$.

$\subseteq$ Let $z \in [y]$ be arbitrary. Then zRy. Since R is transitive, zRx. Hence $z \in [x]$, and so $[y] \subseteq [x]$.

$\supseteq$ Let $z \in [x]$ be arbitrary. Then zRx. Since R is symmetric and yRx, xRy. Since R is transitive, zRy. Hence $z \in [y]$, and so $[x] \subseteq [y]$. Thus, $[x] = [y]$.

$(\leftarrow)$ Suppose $[y] = [x]$. By (a), $y \in [y] = [x]$. □

Theorem 4.54. *Suppose R is an equivalence relation on A. Then A/R is a partition of A.*

Proof. (a) We need to show that $\cup(A/R) = A$, or in other words that $\cup_{x \in A}[x] = A$.

$\subseteq$ Since $[x] \subseteq A$ for each $x \in A$, we have that $\cup_{x \in A}[x] \subseteq A$.

$\supseteq$ Let $x \in A$ be arbitrary. Then $x \in [x]$ by Lemma 4.53(a). Hence $x \in \cup_{x \in A}[x]$. Thus, $A \subseteq \cup_{x \in A}[x]$.

(b) Let $[x], [y] \in A/R$ be arbitrary, where $x, y \in A$. Suppose that $[x] \cap [y] \neq \emptyset$. Then there exists $z \in [x]$ and $z \in [y]$. By Lemma 4.53(b), $[x] = [z] = [y]$.

(c) Let $[x] \in A/R$ be arbitrary, where $x \in A$. Then $x \in [x]$ by Lemma 4.53(a). Thus, $[x] \neq \emptyset$. □

The remaining of this section is not required to study.

Lemma 4.55. Suppose A is a set and $\mathcal{F}$ is a partition of A. Let $R = \cup_{X \in \mathcal{F}}(X \times X)$. Then R is an equivalence relation on A. We will call R the equivalence relation determined by $\mathcal{F}$.

Proof. (a) Let $x \in A$ be arbitrary. Since $\mathcal{F}$ is a partition of A, $\cup\mathcal{F} = A$, so $x \in \cup\mathcal{F}$. Then there exists $X \in \mathcal{F}$ such that $x \in A$. But then $(x, x) \in X \times X$, so $(x, x) \in X \times X \in \cup_{X \in \mathcal{F}}(X \times X) = R$. Thus, R is reflexive.

(b) (Symmetry) Exercise.

(c) (Transitivity) Exercise. □

Lemma 4.56. Suppose A is a set and $\mathcal{F}$ is a partition of A. Let R be the equivalence relation determined by $\mathcal{F}$. Suppose $X \in \mathcal{F}$ and $x \in X$. Then $[x]_R = X$.

Proof. $\subseteq$ Let $y \in [x]_R$ be arbitrary. Then $(y, x) \in R$. Since R is the equivalence relation determined by $\mathcal{F}$, $R = \cup_{X \in \mathcal{F}}(X \times X)$. Hence there exists $Y \in \mathcal{F}$ such that $(y, x) \in Y \times Y$, and so $y \in Y$ and $x \in Y$. Since $x \in X$ by assumption, we have that $X \cap Y \neq \emptyset$. But $\mathcal{F}$ is pairwise disjoint, $X = Y$. Hence $y \in Y = X$. Thus, $[x]_R \subseteq X$.

$\supseteq$ Let $y \in X$ be arbitrary. Since $x \in X$, we have that $(y, x) \in X \times X$, so $(y, x) \in R$. Hence $y \in [x]_R$, and so $X \subseteq [x]_R$. □

Theorem 4.57. *Suppose A is a set and $\mathcal{F}$ is a partition of A. Then there is an equivalence relation R on A such that $A/R = \mathcal{F}$.*

Proof. Let $R = \cup_{X \in \mathcal{F}}(X \times X)$. Then R is an equivalence relation by Lemma 4.55. We will show that $A/R = \mathcal{F}$.

$\subseteq$ Let $[x] \in A/R$ be arbitrary, where $x \in A$. Since $\mathcal{F}$ is a partition of A, $x \in A = \cup\mathcal{F}$. Then there exists $Y \in \mathcal{F}$ such that $x \in Y$. Then $[x] = Y \in \mathcal{F}$ by Lemma 4.56. Thus, $A/R \subseteq \mathcal{F}$.

$\supseteq$ Let $X \in \mathcal{F}$ be arbitrary. Since $\mathcal{F}$ is a partition, $X \neq \emptyset$. Hence we can choose some $x \in X$. Then by Lemma 4.56, $X = [x] \in A/R$. Thus, $\mathcal{F} \subseteq A/R$. □

Definition 4.58. Suppose $m \in \mathbb{Z}^+$. For any $x, y \in \mathbb{Z}$, we will say that x is *congruent* to y *modulo* m if $\exists k \in \mathbb{Z}(x - y = km)$. In other words, x is congruent to y modulo m iff $m \mid (x - y)$. We will use the notation $x \equiv y \pmod{m}$ to mean that x is congruent to y modulo m.

Example 4.59. We have that $12 \equiv 27 \pmod{5}$ since $23 - 27 = -15 = (-3)5$.

Fact 4.60. Let $C_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod{m}\}$. Then C_m is an equivalence relation on $\mathbb{Z}$. There are only m different equivalence classes, which are

$$[0], [1], \ldots, [m - 1].$$

Chapter 5

Functions

5.1 Functions

Definition 5.1. Suppose F is a relation from A to B. Then F is called a *function from A to B* if for every $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in F$. In other words, to say that F is a function from A to B means:

$$\forall a \in A \exists! b \in B \, ((a, b) \in F).$$

To indicate that F is a function from A to B, we will write $F : A \to B$.

Example 5.2. (a) Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, and $F = \{(1, 5), (2, 4), (3, 5)\}$.

F is a function from A to B because 1 is paired only with 5, 2 is paired only with 4, and 3 is only paired with 5.

(b) Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, and $G = \{(1, 5), (2, 4), (1, 6)\}$.

G is not a function from A to B because 3 isn't paired with any element of B in the relation G, or because 1 is paired with two different elements of B, 5 and 6.

(c) Let A be any set, the identity relation i_A on A is a function on A.

Existence: For any $a \in A$, there exists $a \in A$ such that $(a, a) \in i_A$.

Uniqueness: For any $a \in A$, if $a' \in A \setminus \{a\}$, then $(a, a') \notin i_A$.

(d) Let $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$.

f is function from $\mathbb{R}$ to $\mathbb{R}$ because for any real number x, there is a unique real number which equals the square of x. In other words, for any $x \in \mathbb{R}$, x is paired only with $x^2 \in \mathbb{R}$.

Notation 5.3. Suppose $f : A \to B$. If $a \in A$, then the unique $b \in B$ such that $(a, b) \in f$ is called "the value of f at a", or "the image of a under f", and it is written $f(a)$. In other words,

$$\forall a \in A \forall b \in B \, (b = f(a) \leftrightarrow (a, b) \in f).$$

Example 5.4. Consider the Example 5.12.

(a) $F(1) = 5$, $F(2) = 4$, $F(3) = 5$.

(c) $i_A(a) = a$ for each $a \in A$.

(d) $f(x) = x^2$ for each $x \in \mathbb{R}$.

It is often useful to think of a function f from A to B as representing a rule that associates, with each $a \in a$, some corresponding object $b = f(a) \in B$. However, you need to be careful when doing this. For example, the following relations g and h are different because $(0.5, 4) \in h$, but $(0.5, 4) \notin g$.

$$g = \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = 2x + 3\}$$
$$h = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x + 3\}$$

Convention 5.5. We often denote a relation like $\{(x, f(x)) \in \mathbb{R} \times \mathbb{R} \mid f(x) = x^2 + 7\}$ by "let f be a function from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x) = x^2 + 7$".

Theorem 5.6. *Suppose f and g are functions from A to B. If $\forall a \in A\,(f(a) = g(a))$, then $f = g$.*

Proof. Suppose that for any $a \in A$, $f(a) = g(a)$. Let $(a, b) \in f$ be arbitrary. Then by Notation 5.3 $b = f(a) = g(a)$, and so $(a, b) \in g$. Hence $f \subseteq g$. A similar argument shows that $g \subseteq f$. Thus, $f = g$. □

Remark. In the future, to prove $f = g$ we will usually prove $\forall a \in A\,(f(a) = g(a))$.

Proposition 5.7. Let $f : A \to B$. The domain of f is the set

$$\mathrm{Dom}(f) = \{a \in A \mid \exists b \in B\,((a, b) \in f)\} = A.$$

The range of f is the set

$$\mathrm{Ran}(f) = \{b \in B \mid \exists a \in A\,((a, b) \in f)\} = \{f(a) \mid a \in A\}.$$

Example 5.8. Consider the Example 5.12 and 5.4.

(a) $\mathrm{Dom}(F) = A$ and $\mathrm{Ran}(F) = \{4, 5\}$.

(c) $\mathrm{Dom}(i_A) = A$ and

$$\mathrm{Ran}(i_A) = \{i_A(a) \mid a \in A\} = \{a \mid a \in A\} = A.$$

(d) $\mathrm{Dom}(f) = \mathbb{R}$ and

$$\mathrm{Ran}(f) = \{f(x) \mid x \in F\} = \{x^2 \mid x \in \mathbb{R}\} = \mathbb{R}^+,$$

where we prove the last equality:

$\subseteq$ follow from $x^2 \in \mathbb{R}^+$ for any $x \in \mathbb{R}$.

$\supseteq$ Let $y \in \mathbb{R}^+$. Then $x := \sqrt{y} \in \mathbb{R}$ and $x^2 = (\sqrt{y})^2 = y$. Hence $y \in \{x^2 \mid x \in \mathbb{R}\}$.

Theorem 5.9. *Suppose $f : A \to B$ and $g : B \to C$. Then $g \circ f : A \to C$, and for any $a \in A$, the value of $g \circ f$ at a is given by the formula $(g \circ f)(a) = g(f(a))$.*

Proof. Let $a \in A$ be arbitrary. We must show that there is a unique $c \in C$ such that $(a, c) \in g \circ f$.

Existence: Let $b := f(a) \in B$ since $f : A \to B$. Let $c := g(b) \in C$ since $g : B \to C$. Then $(a, b) \in f$ and $(b, c) \in g$ by Notation 5.3. Hence by definition of composition of relations, $(a, c) \in g \circ f$.

Uniqueness: Suppose that $(a, c_1), (a, c_2) \in g \circ f$. We will prove that $c_1 = c_2$. Since

$$(a, c_1) \in g \circ f = \{(a, c) \mid \exists b \in B\,((a, b) \in f \wedge (b, c) \in g)\}.$$

there exists $b_1 \in B$ such that $(a, b_1) \in f$ and $(b_1, c_1) \in g$. Since $(a, c_2) \in g \circ f$, simiarly, there exists $b_2 \in B$ such that $(a, b_2) \in f$ and $(b_2, c_2) \in g$. Since $(a, b_1), (a, b_2) \in f$ and f is a function, we have that $b_1 = b_2$. Since $(b_1, c_1), (b_2, c_2) \in g$ and g is a function, $c_1 = c_2$.

Thus, $g \circ f$ is a function from A to C.

For any $a \in A$, in the proof of the existence we showed that $(g \circ f)(a) = c$, where $c = g(b)$ and $b = f(a)$. Thus,

$$(g \circ f)(a) = c = g(b) = g(f(a)). \qquad \square$$

Example 5.10. Let $g : \mathbb{Z} \to \mathbb{R}$ be the function defined by $g(x) = 2x + 3$. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = n^2 - 3n + 1$. Then $g \circ f : \mathbb{Z} \to \mathbb{R}$. For example,

$$(g \circ f)(2) = g(f(2)) = g(2^2 - 3(2) + 1) = g(-1) = 1.$$

In general, for every $n \in \mathbb{Z}$,

$$(g \circ f)(n) = g(f(n)) = g(n^2 - 3n + 1) = 2(n^2 - 3n + 1) + 3 = 2n^2 - 6n + 5.$$

5.2 One-to-One and Onto

Definition 5.11. Suppose $f : A \to B$. We will say that f is *one-to-one* if

$$\neg \exists a_1 \in A \, \exists a_2 \in A\,(f(a_1) = f(a_2) \wedge a_1 \neq a_2).$$

We say that f is *onto* if

$$\forall b \in B \, \exists a \in A\,(f(a) = b).$$

One-to-one function are sometimes also called *injections*, and onto function are sometimes called *surjections*.

Remark. Diagrammatically, we have the following cases.

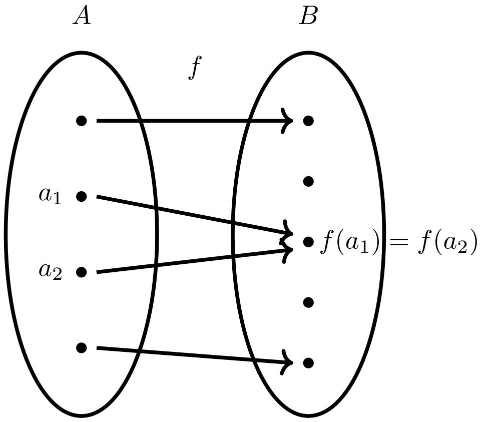


Figure 5.1: f is neither ono-to-one nor onto

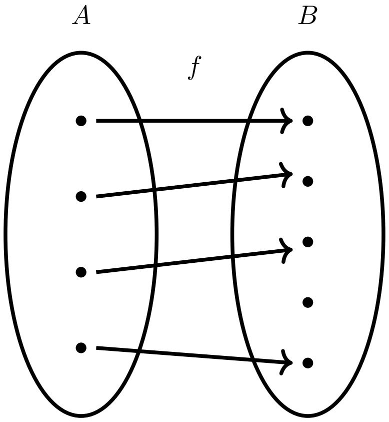


Figure 5.2: f is one-to-one but not onto

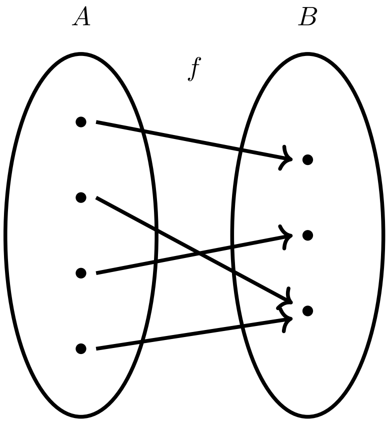


Figure 5.3: f is onto but not one-to one

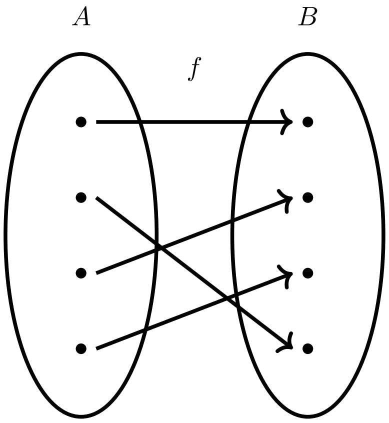


Figure 5.4: f is both one-to-one and onto

Remark. Let A, B be finite sets and $f \subseteq A \times B$ be represented diagrammatically.

If for each $a \in A$ there is a unique arrow pointing away from a, then f is a function.

If for each $a \in A$ there is a unique arrow pointing away from a, and for each $b \in B$ there is **at most** one arrow pointing toward b, then f is an one-to-one function.

If for each $a \in A$ there is a unique arrow pointing away from a, and for each $b \in B$ there is **at least** one arrow pointing toward b, then f is an onto function.

If for each $a \in A$ there is a unique arrow pointing away from a, and for each $b \in B$ there is a **unique** arrow pointing toward b, then f is an one-to-one and onto function.

Example 5.12. (a) Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$. Then the function $F = \{(1, 5), (2, 4), (3, 5)\}$ is one-to-one but not onto.

It is not one-to-one because $F(1) = 5 = F(3)$. It is not onto because $6 \in B$, but there is no $a \in A$ such that $F(a) = 6$.

(b) Let A be any set, the identity function i_A is 1-1.

Prove by contradiction. Suppose there exist $a, a' \in A$ such that $i_A(a) = i_A(a')$ and $a \neq a'$. But $i_A(a) = i_A(a')$ implies that $a = a'$, contradicting $a \neq a'$. Thus, i_A is one-to-one.

(c) Let $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$.

f is not 1-1 because

$$f(2) = 2^2 = 4 = (-2)^2 = f(-2),$$

f is not onto because $-1 \in B$, but there is no $a \in \mathbb{R}$ such that $a^2 = -1$, and so there is no $a \in \mathbb{R}$ such that $f(a) = -1$

(d) Let

$$\begin{aligned} g &= \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = 2x + 3\} \\ h &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x + 3\}. \end{aligned}$$

Similar to previous examples, we have that both g and h is 1-1. Also, g is not onto, h is onto.

Theorem 5.13. *Suppose $f : A \to B$.*

(a) f is one-to-one iff $\forall a_1 \in A \forall a_2 \in A(f(a_1) = f(a_2) \to a_1 = a_2)$.

(b) f is onto iff $\mathrm{Ran}(f) = B$.

Proof. (a)

$$\begin{aligned} f \text{ is one-to-one} &\longleftrightarrow \neg\exists a_1 \in A \exists a_2 \in A(f(a_1) = f(a_2) \wedge a_1 \neq a_2) \\ &\longleftrightarrow \forall a_1 \in A \neg(\exists a_2 \in A(f(a_1) = f(a_2) \wedge a_1 \neq a_2)) \\ &\longleftrightarrow \forall a_1 \in A \forall a_2 \in A \neg(f(a_1) = f(a_2) \wedge a_1 \neq a_2) \\ &\longleftrightarrow \forall a_1 \in A \forall a_2 \in A(f(a_1) \neq f(a_2) \vee a_1 = a_2) \\ &\longleftrightarrow \forall a_1 \in A \forall a_2 \in A(f(a_1) = f(a_2) \to a_1 = a_2). \end{aligned}$$

(b)

$$\begin{aligned} f \text{ is onto} &\longleftrightarrow \forall b \in B \exists a \in A(f(a) = b) \\ &\longleftrightarrow \forall b \in B \exists a \in A((a, b) \in f) \\ &\longleftrightarrow \forall b \in B(b \in \mathrm{Ran}(f)) \\ &\longleftrightarrow B \subseteq \mathrm{Ran}(f) \\ &\longleftrightarrow \mathrm{Ran}(f) = B, \end{aligned}$$

where the equivalence follows from the fact that $\mathrm{Ran}(f) \subseteq B$. □

Example 5.14. Let $A = \mathbb{R} \setminus \{-1\}$, and define $f : A \to \mathbb{R}$ by the formula

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

Prove that f is one-to-one but not onto.

Proof. Let $a_1, a_2 \in A$ be arbitrary. Then $a_1 \neq -1 \neq a_2$. Assume that $f(a_1) = f(a_2)$. Then

$$\begin{aligned} f(a_1) = f(a_2) &\longleftrightarrow \frac{2a_1}{a_1+1} = \frac{2a_2}{a_2+1} \\ &\longleftrightarrow \frac{a_1}{a_1+1} = \frac{a_2}{a_2+1} \\ &\longleftrightarrow a_1(a_2+1) = a_2(a_1+1) \\ &\longleftrightarrow a_1a_2 + a_1 = a_1a_2 + a_2 \\ &\longleftrightarrow a_1 = a_2, \end{aligned}$$

where the third equivalence follows from that $a_1 \neq -1 \neq a_2$. (Note that we only need the forward implications.)

To show f is not onto, it suffices to show that $2 \notin \mathrm{Ran}(f)$, since $2 \in \mathbb{R}$. Suppose $2 \in \mathrm{Ran}(f)$. Then there exists $a \in A$ such that $f(a) = 2$, i.e., $\frac{2a}{a+1} = 2$, then $2a = 2a + 2$, which is impossible. Thus, $2 \notin \mathrm{Ran}(f)$. □

Theorem 5.15. *Suppose $f : A \to B$ and $g : B \to C$. Then*

(a) If f and g are both one-to-one, then so is $g \circ f$.

(b) If f and g are both onto, then so is $g \circ f$.

Proof. By Theorem 5.9, $g \circ f : A \to C$.

(a) Let $a_1, a_2 \in A$ be arbitrary. Suppose that $g \circ f(a_1) = (g \circ f)(a_2)$. By Theorem 5.9 this means that $g(f(a_1)) = g(f(a_2))$. Since g is one-to-one, it follows that $f(a_1) = f(a_2)$. Since f is 1-1, we can conclude that $a_1 = a_2$.

(b) Let $c \in C$ be arbitrary. Since g is onto, we can find some $b \in B$ such that $g(b) = c$. Since f is onto, there is some $a \in A$ such that $f(a) = b$. Then $(g \circ f)(a) = g(f(a)) = g(b) = c$. Thus, $g \circ f$ is onto. □

5.3 Inverses of Functions

Example 5.16. Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, and $F = \{(1, 5), (2, 4), (3, 5)\}$. Then $F : A \to B$. We have the relation $F^{-1} = \{(5, 1), (4, 2), (5, 3)\}$, so F^{-1} is not a function from B to A.

Theorem 5.17. *Suppose $f : A \to B$. If f is one-to-one and onto, then $f^{-1} : B \to A$.*

Proof. Let $b \in B$. We need to show that $\exists! a \in A((b, a) \in f^{-1})$.

Existence: Since f is onto, there is some $a \in A$ such that $f(a) = b$. Then $(a, b) \in f$, and so $(b, a) \in f^{-1}$.

Uniquenss: Suppose that $(b, a_1) \in f^{-1}$ and $(b, a_2) \in f^{-1}$ for some $a_1, a_2 \in A$. Then $(a_1, b) \in f$ and $(a_2, b) \in f$. Hence $f(a_1) = b = f(a_2)$. Since f is 1-1, it follows that $a_1 = a_2$. □

Remark. Let $f : A \to B$. If $f^{-1} : B \to A$, then for $b \in B$

$$\begin{aligned} f^{-1}(b) &= \text{the unique } a \in A \text{ such that } (b, a) \in f^{-1} \\ &= \text{the unique } a \in A \text{ such that } (a, b) \in f \\ &= \text{the unique } a \in A \text{ such that } f(a) = b. \end{aligned}$$

Theorem 5.18. *Suppose $f : A \to B$ and $f^{-1} : B \to A$. Then $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.*

Proof. We prove the first half.

Note that $f^{-1} \circ f : A \to A$ and $i_A : A \to A$. Let $a \in A$ be arbitrary. Let $b := f(a) \in B$. Then $(a, b) \in f$, so $(b, a) \in f^{-1}$ and therefore $f^{-1}(b) = a$. Thus,

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = i_A(a).$$

Hence $f^{-1} \circ f = i_A$. □

Example 5.19. (a) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x$. Then f is one-to-one and onto. Hence $f^{-1} : \mathbb{R} \to \mathbb{R}$. For $x \in \mathbb{R}$,

$$\begin{aligned} f^{-1}(x) &= \text{“the unique } y \text{ such that } f(y) = x\text{”} \\ &= \text{“the unique } y \text{ such that } 2y = x\text{”} \\ &= x/2. \end{aligned}$$

Hence $f^{-1} \circ f : \mathbb{R} \to \mathbb{R}$ and $(f \circ f^{-1}) : \mathbb{R} \to \mathbb{R}$. For $x \in \mathbb{R}$,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(2x) = (2x)/2 = x.$$

For $x \in \mathbb{R}$,

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(x/2) = 2(x/2) = x.$$

(b) Let $f : \mathbb{R} \to \mathbb{R}^+$ be defined by $f(x) = e^x$. Then f is one-to-one and onto. Hence $f^{-1} : \mathbb{R}^+ \to \mathbb{R}$. For $x \in \mathbb{R}$,

$$\begin{aligned} f^{-1}(x) &= \text{“the unique } y \text{ such that } f(y) = x\text{”} \\ &= \text{“the unique } y \text{ such that } e^y = x\text{”} \\ &= \ln x. \end{aligned}$$

Hence $f^{-1} \circ f : \mathbb{R} \to \mathbb{R}$ and $(f \circ f^{-1}) : \mathbb{R}^+ \to \mathbb{R}^+$. For $x \in \mathbb{R}$,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(e^x) = \ln(e^x) = x.$$

For $x \in \mathbb{R}^+$,

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(\ln x) = e^{\ln x} = x.$$

Theorem 5.20. *Suppose that $f : A \to B$.*

(a) If there is a $g : B \to A$ such that $g \circ f = i_A$, then f is one-to-one.

(b) If there is a $g : B \to A$ such that $f \circ g$ then f is onto.

Proof. We prove part (a).

(a) Let $a_1, a_2 \in A$ be arbitrary. Suppose that $f(a_1) = f(a_2)$. Applying g to both sides of this equation we get $g(f(a_1)) = g(f(a_2))$. But

$$g(f(a_1)) = (g \circ f)(a_1) = i_A(a_1) = a_1,$$
$$g(f(a_1)) = (g \circ f)(a_2) = i_A(a_2) = a_2.$$

Hence $a_1 = a_2$. □

Theorem 5.21. *Suppose $f : A \to B$. Then the following statements are equivalent.*

(a) f is one-to-one and onto.

(b) $f^{-1} : B \to A$.

(c) There is a $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$.

Proof. (a) → (b) follows from Theorem 5.17.

(b) → (c) follows from Theorem 5.18 by letting $g = f^{-1}$.

(c) → (a) follows from Theorem 5.20. □

Remark. The easiest way to prove that several statements are equivalent is to prove a circle of implication. In this case we have proven the circle (a) → (b) → (c) → (a).

$$\begin{tikzcd}
& (a) \arrow[dr] & \\
(c) \arrow[ur] & & (b) \arrow[ll]
\end{tikzcd}$$

Theorem 5.22. *Suppose $f : A \to B$, $g : B \to A$, $g \circ f = i_A$, and $f \circ g = i_B$. Then $g = f^{-1}$.*

Proof. By Theorem 5.21, $f^{-1} : B \to A$. Then $f^{-1} \circ f = i_A$ by Theorem 5.18. Then

$$g = i_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ i_B = f^{-1},$$

where the first equality and last equality follows from exercise 9 of Section 4.3. □

Example 5.23. In each part, determine whether f is one-to-one and onto. If it is, find f^{-1}.

(a) Let $\mathbb{A} = \mathbb{R} \smallsetminus \{0\}$ and $B = \mathbb{R} \smallsetminus \{2\}$, and define $f : A \to B$ by the formula

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

Note that for all $x \in A$, $f(x) = \frac{1}{x} + 2 \in \mathbb{R} \smallsetminus \{2\} = B$. Hence $f^{-1} : B \to A$. For $x \in A$,

$$\begin{aligned} f^{-1}(x) &= \text{“the unique } y \text{ such that } f(y) = x\text{”} \\ &= \text{“the unique } y \text{ such that } \frac{1}{y} + 2 = x\text{”} \\ &= \frac{1}{x-2}. \end{aligned}$$

Thus, $f^{-1} : B \to A$ is defined by $f^{-1}(x) = \frac{1}{x-2}$.

One can also let $g : B \to A$ be defined by $g(x) = \frac{1}{x-2}$, and then check that $g \circ f = i_A$ and $f \circ g = i_B$, implying that f is 1-1 and onto by Theorem 5.21.

(b) Let $A = \mathbb{R}$ and $B = \{x \in \mathbb{R} \mid x \geqslant 0\}$, and define $f : A \to B$ by the formula

$$f(x) = x^2.$$

It is not one-to-one because

$$f(2) = 2^2 = 4 = (-2)^2 = f(-2).$$

It is onto. Let $g : B \to A$ be defined by $g(x) = \sqrt{x}$. This definition makes sense (or is well-defined) because any element in B is nonnegative and we can take its square root. Then $f \circ g : B \to B$. For $x \in B$,

$$(f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x.$$

Hence $f \circ g = i_B$. Thus, g is onto by Theorem 5.20(b)

5.4 Images and Inverse Images: A Research Project

Definition 5.24. Suppose $f : A \to B$ and $X \subseteq A$. Then the *image* of X under f is the set $f(X)$ defined as follows:

$$\begin{aligned} f(X) &= \{f(x) \mid x \in X\} \\ &= \{b \in B \mid \exists x \in X\, (f(x) = b)\}. \end{aligned}$$

In particular, $f(\emptyset) = \emptyset$ and

$$f(A) = \{f(x) \mid x \in A\} = \mathrm{Ran}(f).$$

Definition 5.25. Suppose $f : A \to B$ and $Y \subseteq B$. Then the *inverse image* of Y under f is the set $f^{-1}(Y)$ defined as follows:

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

In particular, $f^{-1}(\emptyset) = \emptyset$ and

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

Remark. If f is not one-to-one or onto, then f^{-1} is not a function, then the notation "$f^{-1}(y)$" is meaningless. However, $f^{-1}(\{y\})$ makes sense since it is the inverse image of the subset $\{y\}$ of B.

Example 5.26. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by the formula $f(x) = x^2$, and $X = \{x \in \mathbb{R} \mid 0 \leqslant x < 2\}$. Then

$$\begin{aligned} f(X) &= \{f(x) \mid x \in X\} \\ &= \{x^2 \mid x \in \mathbb{R} \text{ and } 0 \leqslant x < 2\} \\ &= \{x \in \mathbb{R} \mid 0 \leqslant x < 4\}. \end{aligned}$$

Let $Y = \{x \in \mathbb{R} \mid 0 \leqslant x < 4\}$. Then

$$\begin{aligned} f^{-1}(Y) &= \{x \in \mathbb{R} \mid f(x) \in Y\} \\ &= \{x \in \mathbb{R} \mid 0 \leqslant f(x) < 4\} \\ &= \{x \in \mathbb{R} \mid 0 \leqslant x^2 < 4\} \\ &= \{x \in \mathbb{R} \mid -2 < x < 2\}. \end{aligned}$$

Observe that in this example, we have that

$$X \subsetneq f^{-1}(f(X)).$$

Question 5.27. Suppose $f : A \to B$, and $W, X \subseteq A$. Question: Is $f(W \cap X) = f(W) \cap f(X)$ true?

Proof. $\subseteq$ Since $W \cap X \subseteq W, X$ we have that $f(W \cap X) \subseteq f(W), f(X)$. Hence $f(W \cap X) \subseteq f(W) \cap f(X)$.

$\supseteq$ Let $y \in f(W) \cap f(X)$ be arbitrary. Then $y \in f(W)$ and $y \in f(X)$. Then there exists $w \in W$ and $x \in X$ such that $f(w) = y = f(x)$. If only we knew that $w = x$, then we could conclude that $w = x \in W \cap X$, and so $y = f(x) \in f(W \cap X)$. This should remind you that of the definition of one-to-one. If we knew f is one-to-one, we could conclude from the fact that $f(w) = f(x)$ that $w = x$, and the proof would be done. □

Summary 5.28. Suppose $f : A \to B$, and $W, X \subseteq A$. Then $f(W \cap X) \subseteq f(W) \cap f(X)$. If f is one-to-one, then $f(W \cap X) = f(W) \cap f(X)$.

Question 5.29. Suppose $f : A \to B$, and $W, X \subseteq A$. Question: Is $f(W \cap X) = f(W) \cap f(X)$ true?

We try to find a counterexample in which f is not one-to-one. Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, and $f = \{(1, 4), (2, 5), (3, 5)\}$. Then $f : A \to B$. The attempted proof ran into trouble when W contains w and W contains x such that $w \neq x$ but $f(w) \neq f(x)$. Hence we choose $W = \{2\}$ and $X = \{3\}$. With these choices we get $f(W) = \{f(2)\} = \{5\}$ and $f(X) = \{f(3)\} = \{5\}$. But $f(W \cap X) = f(\emptyset) = \emptyset$, so $f(W \cap X) \neq f(W) \cap f(X)$.

Chapter 6

Mathematical Induction

6.1 Proof by Mathematical Induction

Recall that the set all natural numbers is $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

The key idea behind mathematical induction is that to list all the natural numbers all you have to do is start with 0 and repeatedly add 1. Thus, you can show that every natural number has the property P by showing that 0 has property P, and whenever you add 1 to a number that has property P, the resulting number also has property P.

To prove a goal of the form $\forall n \in \mathbb{N}\, P(n)$:

First prove $P(0)$, and then prove $\forall n \in \mathbb{N}\,(P(n) \to P(n+1))$. The first of these proofs is sometimes called the *base case* and the second the *induction step*. $P(n)$ is called the *inductive hypothesis*.

Form of final proof:

Base case: [Proof of $P(0)$ goes here.]

Induction step: [Proof of $\forall n \in \mathbb{N}\,(P(n) \to P(n+1))$ goes here]

Theorem 6.1. *For every $n \in \mathbb{N}$, $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$, i.e., $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.*

Proof. We use mathematical induction.

Base case: Setting $n = 0$, we get $2^0 = 1 = 2^1 - 1$ as required.

Induction step: Let $n \in \mathbb{N}$ be arbitrary. Suppose that

$$P(n): \qquad 2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1.$$

We need to prove that

$$P(n+1): \qquad 2^0 + 2^1 + \cdots + 2^{n+1} = 2^{(n+1)+1} - 1 = 2^{n+2} - 1.$$

Note that

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^{n+1} &= (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} \\ &= (2^{n+1} - 1) + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \\ &= 2^{n+2} - 1. \end{aligned}$$

□

Theorem 6.2. *For every $n \in \mathbb{N}$, $3 \mid (n^3 - n)$.*

Proof. We use mathematical induction.

Base case: If $n = 0$, then $n^3 - n = 0 = 3 \cdot 0$, so $3 \mid (n^3 - n)$.

Induction step: Let $n \in \mathbb{N}$ be arbitrary. Suppose that

$$P(n): \qquad 3 \mid (n^3 - n).$$

We need to prove that

$$P(n+1): \qquad 3 \mid ((n+1)^3 - (n+1)).$$

Since $3 \mid (n^3 - n)$, there exists $k \in \mathbb{Z}$ such that $3k = n^3 - n$. Then

$$\begin{aligned} (n+1)^3 - (n+1) &= (n+1)((n+1)^2 - 1) \\ &= (n+1)(n^2 + 2n) \\ &= n^3 + 3n^2 + 2n \\ &= (n^3 - n) + 3n^2 + 3n \\ &= 3k + 3n^2 + 3n \\ &= 3(k + n^2 + n). \end{aligned}$$

Thus, $3 \mid ((n+1)^3 - (n+1))$. □

Theorem 6.3. *For every $n \in \mathbb{N}$ such that $n \geqslant 5$, $2^n > n^2$.*

Proof. We use mathematical induction.

Base case: When $n = 5$, then $2^n = 32 > 25 = 5^2 = n^2$.

Induction step: Let $n \in \mathbb{N}$ be arbitrary. Suppose that

$$P(n): \qquad 2^n > n^2.$$

We need to prove that

$$P(n+1): \qquad 2^{n+1} > (n+1)^2.$$

Note that

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2n^2 && \text{by inductive hypothesis} \\ &= n^2 + n \cdot n \\ &\geqslant n^2 + 5 \cdot n && (\text{since } n \geqslant 5) \\ &= n^2 + 2n + 3n \\ &> n^2 + 2n + 1 \\ &= (n+1)^2. \end{aligned}$$

□

6.2 Recursion

We can define a function with domain $\mathbb{N}$ recursively.

Definition 6.4. We might use the following equation to define a function f with domain $\mathbb{N}$:

$$\begin{aligned}&f(0) = 1;\\ &\forall n \in \mathbb{N},\, f(n+1) = (n+1)f(n).\end{aligned}$$

For example,

$$\begin{aligned}f(4) &= 4f(3)\\ &= 4(3)f(2)\\ &= 4(3)f(2)\\ &= 4(3)(2)f(1)\\ &= 4(3)(2)(1)f(0)\\ &= 4(3)(2)(1)(1)\\ &= 24.\end{aligned}$$

Let $n \in \mathbb{N}$ be such that $n \geqslant 1$. Then

$$\begin{aligned}f(n) &= nf(n-1)\\ &= n(n-1)f(n-2)\\ &= n(n-1)(n-2)f(n-3)\\ &= \cdots\\ &= n(n-1)(n-2)\cdots(1)f(0)\\ &= n(n-1)(n-2)\cdots(1)\\ &=: n!,\end{aligned}$$

which is called n *factorial*.

Definition 6.5. For $n \in \mathbb{N}$, we define n *factorial* $n!$ as follows:

$$\begin{aligned}&0! = 1;\\ &\forall n \in \mathbb{N},\, (n+1)! = (n+1)\cdot n!.\end{aligned}$$

Example 6.6. For $n \in \mathbb{N}$, let

$$f(n) = 2^0 + 2^1 + 2^2 + \cdots + 2^n.$$

Then

$$\begin{aligned}f(n+1) &= 2^0 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1}\\ &= f(n) + 2^{n+1}.\end{aligned}$$

Thus, we could define f recursively as follows:

$$\begin{aligned}&f(0) = 2^0 = 1;\\ &\forall n \in \mathbb{N},\, f(n+1) = f(n) + 2^{n+1}.\end{aligned}$$

Definition 6.7. For $a \in \mathbb{R} \smallsetminus \{0\}$, we define a^n with the following recursive definition:

$$\begin{aligned} &a^0 = 1; \\ &\forall n \in \mathbb{N},\, a^{n+1} = a^n \cdot a \; (= a \cdot a^n). \end{aligned}$$

For example,

$$\begin{aligned} a^4 &= a^3 \cdot a \\ &= a^2 \cdot a \cdot a \\ &= a^1 \cdot a \cdot a \cdot a \\ &= a^0 \cdot a \cdot a \cdot a \cdot a \\ &= a \cdot a \cdot a \cdot a. \end{aligned}$$

Definition 6.8. If $a_0, a_1, \ldots, a_n$ is a list of numbers, then the *sum* of these is written

$$\sum_{i=0}^{n} a_i.$$

This is read "the sum as i goes from 0 to n of a_i."

Example 6.9.

$$\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + 2^2 + \cdots + 2^n.$$

Definition 6.10. If $a_0, a_1, \ldots, a_n$ is a list of numbers, if $n \geqslant m$, then

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + a_{m+2} + \cdots + a_n.$$

Example 6.11.

$$\sum_{i=3}^{6} i^2 = 3^2 + 4^2 + 5^2 + 6^2 = 9 + 16 + 25 + 36 = 86.$$

Remark. The letter i in these formulas is a bound variable and therefore can be replaced by a new variable without changing the meaning of the formula.

Theorem 6.12. *For every $n \in \mathbb{N}$ with $n \geqslant 4$, $n! > 2^n$.*

Proof. By mathematical induction.

Base case: When $n = 4$ we have that $n! = 24 > 16 = 2^n$.

Induction step: Let $n \geqslant 4$ be an arbitrary integer. Suppose that $n! > 2^n$. Then

$$\begin{aligned} (n+1)! &= (n+1)(n!) \\ &> (n+1)(2^n) \\ &> 2 \cdot 2^n \\ &= 2^{n+1}. \end{aligned}$$

□

Theorem 6.13. *For any $a \in \mathbb{R} \smallsetminus \{0\}$ and $m, n \in \mathbb{N}$, $a^{m+n} = a^m \cdot a^n$.*

Proof. Let $a \in \mathbb{R} \smallsetminus \{0\}$ and $m \in \mathbb{N}$ be arbitrary. We now proceed by induction on n.

Base case: When $n = 0$, we have that

$$a^{m+n} = a^{m+0} = a^m = a^m \cdot 1 = a^m \cdot a^0 = a^m \cdot a^n.$$

Induction step: Let $n \in \mathbb{N}$ be arbitrary. Suppose that $a^{m+n} = a^m \cdot a^n$. Then

$$\begin{aligned} a^{m+(n+1)} &= a^{(m+n)+1} \\ &= a^{m+n} \cdot a && \text{(by definition of exponentiation)} \\ &= a^m \cdot a^n \cdot a && \text{(by inductive hypothesis)} \\ &= a^m \cdot a^{n+1} && \text{(by definition of exponentiation).} \end{aligned}$$ □

Theorem 6.14. *A sequence of numbers $a_0, a_1, a_2, \ldots$ is defined recursively as follows:*

$$\begin{aligned} &a_0 = 0; \\ &\forall n \in \mathbb{N},\ a_{n+1} = 2a_n + 1. \end{aligned}$$

Then for each $n \in \mathbb{N}$, $a_n = 2^n - 1$.

Proof. By induction.

Base case: $a_0 = 0 = 1 - 1 = 2^0 - 1$.

Induction step: Let $n \in \mathbb{N}$ be arbitrary. Suppose that $a_n = 2^n - 1$. Then

$$\begin{aligned} a_{n+1} &= 2a_n + 1 \\ &= 2(2^n - 1) + 1 \\ &= 2^{n+1} - 2 + 1 \\ &= 2^{n+1} - 1. \end{aligned}$$ □

Theorem 6.15. *For every $x > -1$ and every $n \in \mathbb{N}$, $(1+x)^n > nx$.*

Proof. Let $x > -1$ be arbitrary. We will prove by induction on n.

Base case: If $n = 0$, then since $1 + x \neq 0$, we have that

$$(1+x)^n = (1+x)^0 = 1 = 1 + 0 = 1 + 0 \cdot x = 1 + nx.$$

Induction step: Let $n \in \mathbb{N}$ be arbitrary. Suppose that $(1+x)^n > nx$. Then

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &> (1+x)(1+nx) && \text{because } 1 + x > 0 \\ &= 1 + x + nx + nx^2 \\ &\geqslant 1 + x + nx && \text{because } nx^2 \geqslant 0 \\ &= 1 + (n+1)x \\ &> (n+1)x. \end{aligned}$$ □

Using a similar proof, one can prove the following:

Theorem 6.16. *For every $x > -1$ and every $n \in \mathbb{N}$, $(1+x)^n \geqslant 1 + nx$.*

6.3 Strong Induction

In some cases the assumption from the mathematical induction isn't strong enough to make the proof work, and we need to assume that all smaller natural numbers have the property. This is the idea behind a variant of mathematical induction sometimes called *strong induction*:

To prove a goal of the form $\forall n \in \mathbb{N}\, P(n)$:

Prove that $\forall n \in \mathbb{N}\, [(\forall k \in \mathbb{N}_{\leqslant n-1} P(k)) \to P(n)]$, where $\mathbb{N}_{\leqslant n-1}$ denotes all natural numbers no larger than $n-1$.

Remark. Note that no base case is necessary in a proof by strong induction. Indeed, we have that $\forall k \in \mathbb{N}_{\leqslant -1} P(k)$ is always true, if we proved $\forall n \in \mathbb{N}\, [(\forall k \in \mathbb{N}_{\leqslant n-1} P(k)) \to P(n)]$, then in particular, we proved that $(\forall k \in \mathbb{N}_{\leqslant -1} P(k)) \to P(0)$. Hence by modus ponens, we have that $P(0)$ is true.

Theorem 6.17 (Division algorithm)**.** *For all $n \in \mathbb{N}$ and $m \in \mathbb{N}_{\geqslant 1}$, there are $q, r \in \mathbb{N}$ such that $n = mq + r$ and $r < m$. (The numbers q and r are called the* quotient *and* remainder *when n is divided by m.)*

Proof. We let $m \in \mathbb{N}_{\geqslant 1}$ be arbitrary and then proceed by strong induction on n.

Let $n \in \mathbb{N}$ be arbitrary. Suppose that for any $k \in \mathbb{N}_{n-1}$ there exists $q, r \in \mathbb{N}$ such that $k = mq+r$ and $r < m$. We need to prove that there exist $q', r' \in \mathbb{N}$ such that $n = mq' + r'$ and $r' < m$.

Case 1. $n < m$. Let $q' = 0$ and $r' = n$. Then

$$n = r' = m(0) + r' = mq' + r'.$$

Also, $r' = n < m$.

Case 2. $n \geqslant m$. Then $1 \leqslant m \leqslant n$, so $n - m \in \mathbb{N}_{\leqslant n-1}$. Hence by inductive hypothesis there exist $q, r \in \mathbb{N}$ such that $n - m = mq + r$ and $r < m$. Then $n = m(q+1) + r$. Letting $q' = q + 1 \in \mathbb{N}$ and $r' = r \in \mathbb{N}$, we have that $n = mq' + r'$ and $r' = r < m$. □

Definition 6.18. Let $a \in \mathbb{N}_{\geqslant 1}$ and $b, c \in \mathbb{N}$ such that $b \neq 0$ or $c \neq 0$.

(a) If $a \mid b$ and $a \mid c$, we say that a is a *common divisor* of b and c.

(b) The largest common positive divisor of b and c is called the *greatest common divisor* of b and c, denoted by $\gcd(b, c)$,

For $n \in \mathbb{N}$ and $m \in \mathbb{N}_{\geqslant 1}$, the Euclidean Algorithm allows us to express the $\gcd(n, m)$ as an integral sum of n and m.

Theorem 6.19 (Euclidean Algorithm)**.** *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}_{\geqslant 1}$. If $m \mid n$, the* $\gcd(n, m) = m$. *Without loss of generality, assume that $m \nmid n$. Then repeat applying the division algorithm, write*

$$\begin{aligned} n &= mq_1 + r_1, 0 < r_1 < m, \\ m &= r_1 q_2 + r_2, 0 < r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Then $r_n = \gcd(n, m)$. *(As* $r_1 > r_2 > \cdots > r_{n-1} > r_n > 0$*, the algorithm terminates after finite steps.)*

Example 6.20. Write the gcd$(48, 27)$ as an integral sum of 48 and 27. Note that

$$48 = 27(1) + 21,$$

$$27 = 21(1) + 6,$$
$$21 = 6(3) + 3,$$
$$6 = 3(2).$$

Now working backwards:

$$\gcd(48, 27) = 3 = 21 - 6(3) = 21 - (27 - 21)(3) = 4(21) - 3(27) = 4(48 - 27) - 3(27) = 4(48) - 7(27).$$

Chapter 7

Infinite Sets

7.1 Equinumerous Sets

Definition 7.1. Let A and B be sets. We'll say that A is *equinumerous* with B if there is a function $f : A \to B$ that is one-to-one and onto. We'll write $A \sim B$ to indicate that A is equinumerous with B.

Definition 7.2. For each $n \in \mathbb{N}$, let $I_n = \mathbb{N}_{\leqslant n}$. A set A is called *finite* if there is an $n \in \mathbb{N}$ such $I_n \sim A$. Otherwise, A is infinite.

Definition 7.3. If A is a finite set and $A \sim I_n$ for some $n \in \mathbb{N}$, then the *cardinality* of A, denoted $|A|$, is defined to be n. In particular, $|\emptyset| = 0$.

The definition of equinumerous can also be applied to infinite sets. We will see that $\mathbb{Z}^+ \sim \mathbb{Z}$. Consider the function $f : \mathbb{Z}^+ \to \mathbb{Z}$ defined as follows:

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

The table of values for f in the following reveals a pattern that suggests that f might be one-to-one and onto.

n	$f(n)$
1	0
2	1
3	-1
4	2
5	-2
6	3
7	-3
$\vdots$	$\vdots$

Theorem 7.4.

$$\mathbb{Z}^+ \sim \mathbb{Z}.$$

Proof. Consider the function $f : \mathbb{Z}^+ \to \mathbb{Z}$ defined as follows:

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Then it suffices to show that f is one-to-one and onto.

Let $n_1, n_2 \in \mathbb{Z}^+$ be such that $f(n_1) = f(n_2)$.

Case 1: n_1 and n_2 are both even. Then $\frac{n_1}{2} = f(n_1) = f(n_2) = \frac{n_2}{2}$, and so $n_1 = n_2$.

Case 2: n_1 and n_2 are both odd. Then $\frac{1-n_1}{2} = f(n_1) = f(n_2) = \frac{1-n_2}{2}$, and so $n_1 = n_2$.

Case 3: n_1 is even and n_2 is odd. Then $f(n_1) = \frac{n_1}{2} > 0$, but $f(n_2) = \frac{1-n_2}{2} \leqslant 0$, contradicting $f(n_1) = f(n_2)$, This case is impossible.

Case 4: n_1 is odd and n_2 is even. Then similar to the case 3, this case is impossible, too.

Thus, f is one-to-one.

Let $m \in \mathbb{Z}$.

Case 1: If $m \in \mathbb{Z}^+$, then $2m \in \mathbb{Z}^+$ and $2m$ is even such that $f(2m) = \frac{2m}{2} = m$.

Case 2: If $m \in \mathbb{Z} \setminus \mathbb{Z}^+$, then $-m \in \mathbb{N}$, so $2(-m)+1 \in \mathbb{Z}^+$ and $2(-m)+1$ is odd such that $f(2(-m)+1) = \frac{1-(2(-m)+1)}{2} = m$.

Thus, f is onto. □

Theorem 7.5.

$$\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+.$$

Proof. Define a function f by

$$\begin{aligned} f : \mathbb{Z}^+ \times \mathbb{Z}^+ &\longrightarrow \mathbb{Z}^+ \\ (i,j) &\longmapsto \frac{(i+j-2)(i+j-1)}{2} + i. \end{aligned}$$

First, note that the integers $i+j-2$ and $i+j-1$ are neighbors, so one of them must be even, hence $2 \mid (i+j-2)(i+j-1)$. Also note that $(i+j-2)(i+j-1) \geqslant 0$, and so $\frac{(i+j-2)(i+j-1)}{2} + i \in \mathbb{Z}^+$, thus the functions is well-defined. The table of values in the following may help you understand this example.

				j		
	$f(i,j)$	1	2	3	4	5
	1	1	2	4	7	11
	2	3	5	8	12	
i	3	6	9	13		
	4	10	14			$\ddots$
	5	15				

Check that f is one-to-one and onto. □

Theorem 7.6. *Suppose $A \sim B$ and $C \sim D$. Then*

(a) $A \times C \sim B \times D$.

(b) If $A \cap C = \emptyset$ and $B \cap D = \emptyset$, then $A \sqcup C \sim B \sqcup D$.

Proof. Since $A \sim B$ and $C \sim D$, there exist one-to-one and onto functions $f : A \to B$ and $g : C \to D$.

(a) Define a function h by

$$\begin{aligned} h : A \times C &\longrightarrow B \times D \\ (a, c) &\longmapsto (f(a), g(c)). \end{aligned}$$

Check that h is one-to-one and onto.

(b) Define a function $f \sqcup g$ by

$$\begin{aligned} f \sqcup g : A \sqcup C &\longrightarrow B \sqcup D \\ a &\longmapsto f(a), \forall a \in A \\ c &\longmapsto g(c), \forall c \in C. \end{aligned}$$

Check that $f \sqcup g$ is one-to-one and onto. □

Theorem 7.7. *For any sets A, B, and C:*

(a) $A \sim A$.

(b) If $A \sim B$, then $B \sim A$.

(c) If $A \sim B$ and $B \sim C$, then $A \sim C$.

Proof. (a) The identity function $i_A : A \to A$ is one-to-one and onto.

(b) Since $A \sim B$, there exists one-to-one and onto function $f : A \to B$. Then $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$ by Theorem 5.18. Hence $f^{-1} : B \to A$ is onto and one-to-one by Theorem 5.20, so $B \sim A$.

(c) Since $A \sim B$ and $B \sim C$, there exist one-to-one and onto functions $f : A \to B$ and $g : B \to C$. By Theorem 5.15, $g \circ f : A \to C$ is one-to-one and onto, so $A \sim C$. □

Corollary 7.8.

$$\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}.$$

Proof. By Theorem 7.5, $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$. By Theorem 7.4, $\mathbb{Z}^+ \sim \mathbb{Z}$. Thus, $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}$ by Theorem 7.1. □

Definition 7.9. A set A is called *denumerable* if $\mathbb{Z}^+ \sim A$. It is called *countable* if it is either finite or denumerable. Otherwise, it is *uncountable*.

Theorem 7.10. *Let A be a set. The following statements are equivalent:*

(a) A is countable.

(b) Either $A = \emptyset$ or there is a function $f : \mathbb{Z}^+ \to A$ that is onto.

(c) There is a function $f : A \to \mathbb{Z}^+$ that is ono-to-one.

Theorem 7.11. *$\mathbb{Q}$ is denumerable.*

Proof. Define a function f by

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z}^+ &\longrightarrow \mathbb{Q} \\ (p, q) &\longmapsto p/q. \end{aligned}$$

For $(p, q) \in \mathbb{Z} \times \mathbb{Z}^+$, we have that $q \neq 0$, so $p/q \in \mathbb{Q}$, and hence f is well-defined. Clearly, f is onto, since all rational numbers can be written as fractions.

Since $\mathbb{Z}^+ \sim \mathbb{Z}$ and $\mathbb{Z}^+ \sim \mathbb{Z}^+$, we have that $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}^+$ by Theorem 7.6(a), and so $\mathbb{Z} \times \mathbb{Z}^+ \sim \mathbb{Z}^+ \times \mathbb{Z}^+$. By Theorem 7.5, $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$. Hence $\mathbb{Z} \times \mathbb{Z}^+ \sim \mathbb{Z}^+$, and so $\mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}^+$. Thus, there exists a one-to-one and onto function $g : \mathbb{Z}^+ \to \mathbb{Z} \times \mathbb{Z}^+$. Also, since f was onto, $f \circ g : \mathbb{Z}^+ \to \mathbb{Q}$ is onto by Theorem 5.15(b). Therefore, $\mathbb{Q}$ is countable by Theorem 7.10. Clearly $\mathbb{Q}$ is not finite, so it must be denumerable. □

7.2 Counting Basics

Theorem 7.12. *Let A and B be finite sets. Then*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. Case 1: $A = \emptyset$ or $B = \emptyset$. Without loss of generality, we assume that $A = \emptyset$. Then $A \cup B = B$ and $A \cap B = \emptyset$. Hence

$$|A \cup B| = |B| = 0 + |B| - 0 = |\emptyset| + |B| - |\emptyset| = |A| + |B| - |A \cap B|.$$

Case 2: $A \neq \emptyset \neq B$ and $A \cap B = \emptyset$. Assume that $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_\ell\}$, where $k, \ell \in \mathbb{Z}^+$ and $a_i \neq b_j$ for $i = 1, \ldots, k$ and $j = 1, \ldots, \ell$. Then $A \cap B = \emptyset$ and

$$A \cup B = \{a_1, \ldots, a_k, b_1, \ldots, b_\ell\}.$$

Hence

$$|A \cup B| = k + \ell = k + \ell - 0 = |A| + |B| - |A \cap B|.$$

Case 3: $A \cap B \neq \emptyset$. Assume $A = \{a_1, \ldots, a_k, x_1, \ldots, x_r\}$ and $B = \{b_1, \ldots, b_\ell, x_1, \ldots, x_r\}$ with $A \cap B = \{x_1, \ldots, x_r\}$. This implies that $a_i \neq b_j$ for $i = 1, \ldots, k$ and $j = 1, \ldots, \ell$. Hence

$$A \cup B = \{a_1, \ldots, a_k, b_1, \ldots, \ell, x_1, \ldots, x_r\}.$$

Thus,

$$|A \cup B| = k + \ell + r = (k + r) + (\ell + r) - r = |A| + |B| - |A \cap B|.$$ □

Example 7.13. At a certain school there are 120 students who take French and 98 who take German and 23 students who take both French and German, then there are

$$|F \cup G| = |F| + |G| - |F \cap G| = 120 + 98 - 23 = 195$$

students studying French or German at that school.

Corollary 7.14 (Addition Rule)**.** Let A and B be finite sets and $A \cap B = \emptyset$. Then

$$|A \sqcup B| = |A| + |B|.$$

Proof. It is immediately from Theorem 7.12. □

Corollary 7.15. Let A and B be finite sets. Then

$$|A \smallsetminus B| = |A| - |A \cap B|.$$

Proof. Note that $(A \setminus B) \cap (A \cap B) = \emptyset$ and $(A \setminus B) \cup (A \cap B) = A$. Then by Corollary 7.14,

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

Hence $|A \smallsetminus B| = |A| - |A \cap B|$. □

Definition 7.16. Let $a \in \mathbb{R}$. Define the *floor* function of a by

$$\lfloor a \rfloor = \max\{n \in \mathbb{Z} \mid n \leqslant a\}.$$

Example 7.17. $\lfloor 2.8 \rfloor = 2$, $\lfloor 3 \rfloor = 3$, and $\lfloor -2.8 \rfloor = -3$.

Example 7.18. There are $\lfloor \frac{100}{3} \rfloor = 33$ integers divisible by 3 between 1 and 100.
There are $\lfloor \frac{100}{7} \rfloor = 14$ integers divisible by 7 between 1 and 100.
There are $\lfloor \frac{100}{21} \rfloor = 4$ integers divisible by both 3 and 7 between 1 and 100.
Thus, there are $33 + 14 - 4 = 43$ integers between 1 and 100 divisible by either 3 or 7.
There are $33 - 4 = 29$ integers between 1 and 100 which are divisible by 3 but not 7.

Theorem 7.19 (Principal of Inclusion-Exclusion)**.** *Let $A_1, \dots, A_n$ be finite sets. Then*

$$|A_1 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|.$$

Example 7.20. Let A_1, A_2, A_3 be finite sets. Then

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Theorem 7.21 (Multiplication Rule)**.** *Let $A_1, \dots, A_n$ be finite sets. Then*

$$|A_1 \times \cdots \times A_n| = \prod_{i=1}^{n} |A_i|.$$

Example 7.22. For example at a restaurant, one has a choice of 4 salads, 10 entrees and 6 desserts, how many ways can you order a three-course meals if you choose exactly one salad, one entree and one dessert? We use the multiplication rule and see that we have $4(10)(6) = 240$ possible three-course meals.

If at the same restaurant, you will only order two of the three courses, how many ways can you choose a two-course meal. Here we will combine the addition rule and the multiplication rule. You can order either a salad and an entree, a salad and a dessert or an entree and a dessert. Hence there are $4(10) + 4(6) + 10(6) = 124$ ways to order 2 courses.

7.3 Permutation

Suppose 20 runners are participating in a Cross Country race. How many possible ways can the top 5 places be awarded? The first place can be chosen from among all 20 runners, but once the first place runner has been chosen, then there are only 19 competing for 2nd place, 18 for 3rd, 17 for 4th and 16 for 5th place. So there are $20(19)(18)(17)(16) = 1860480$ ways to award the top 5 places.

Suppose you have three sculptures and 10 display cases in your house where you could put the sculptures. If each display case is to hold at most one sculpture, how many ways can you display your three sculptures? There are 10 ways to choose one display case for the first sculpture. Once this case has been chosen there are only 9 left to display the remaining 2 sculptures and once one of these is chosen there will only be 8 remaining cases to display the last sculpture so there are $10(9)(8) = 720$ ways to display the sculptures.

In each of the above scenarios, we had n distinct objects and r distinct slots to place them in. For example with the runners we had 20 unique objects (the runners) and 5 unique slots (the places) that we wanted to place these runners. With the sculpture and the display cases, the objects are now the display cases and the slots are the sculptures. We define a *permutation* to be a set of distinct symbols which are arranged in order. An r-permutation of n symbols is a permutation of r of the n symbols. The number of r-permutations is

$$P(n,r) := n(n-1)\cdots(n-r+1) = \frac{n(n-1)\cdots(n-r+1)(n-r)!}{(n-r)!} = \frac{n!}{(n-r)!}.$$

Example 7.23. A man, a woman, a boy, a girl and a dog are lined up for a picture.

(a) How many ways can they line up for the picture?

Since there are 5 distinct living things lined up in the picture there are $5! = 120$ ways for them to line up.

(b) How many ways can they line up if the dog is in the middle? If the dog is in the middle, then there are four people left to line up so there are $4! = 24$ ways for them to line up with the dog in the middle.

(c) How many ways can they line up if the man always follows the woman in the line up?

If the man always follows the woman, we can treat them as a block taking up two slots in the line. There are 4 ways to place the man and the woman in two adjacent spots where the man follows the woman. After the man and the woman have taken their spots, there are 3 spots left in the line where the boy, girl and the dog can line up so $3!$ ways. Using the multiplication rule we see there are $4(3!) = 4! = 24$ ways for them to line up this way too.

7.4 Combinations and Binomial Coefficients

Suppose now that we have n distinct objects and we want to select r of them without caring about the order. For example, we may have a red, a green, a blue and a yellow marble in a bag and we want to grab 2 of the marbles out of the bag. When we grab the marbles we don't do it in any particular order. Grabbing a blue and a yellow marble is indistinguishable from grabbing a yellow and a blue marble. There are 6 ways to select two marbles. Let R denote red, G denote green, B

denote blue and Y denote yellow. The possibilities are RG, RB, RY, GB, GY and BY. This is an example of the set of 2 combinations of 4 which we will define below.

Definition 7.24. An r-combination of n distinct objects is any collection of r of the objects. The number of r-combinations of n objects is denoted either $\binom{n}{r}$ and is $\frac{n!}{r!(n-r)!}$.

Remark.

$$\binom{n}{r} = \frac{P(n,r)}{r!},$$

where $P(n,r) = \frac{n!}{(n-r)!}$ is the number of r-permuation of n sysmbols.

Example 7.25. Suppose a 5 member committee is to be chosen from a group of 4 women and 6 men.

(a) How many ways can committees be chosen?

Since there are 10 people, there are

$$\binom{10}{5} = \frac{10!}{5!5!} = \frac{10(9)(8)(7)(6)}{5(4)(3)(2)} = 252.$$

(b) How many ways can committees be chosen if the committee has exactly 2 women?

There are 4 women to choose the 2 women from and 6 men to choose the 3 men from. So there are $\binom{4}{2} = 6$ ways to choose the women on the committee and $\binom{6}{3} = 20$ ways to choose the men. Now using the multiplication rule, there will be $6(20) = 120$ ways of choosing a committee with 2 women and 3 men.

(c) How many ways can committees be chosen if there are at most two women?

If at most two women are on the committee, then either there are no women, one woman or two women. These scenario's are mutually exclusive so the sets of committees with no women, one woman and two women will be pairwise disjoint. So using the addition rule we can add the number of committees with no women to the number with one woman to the number with two women to find our answer. There are $\binom{6}{5} = 6$ ways of choosing a committee with no women. There are $\binom{7}{4}\binom{4}{1} = 35(4) = 140$ ways of choosing a committee with one woman. There are 120 ways of choosing a committee with two women as we did in (2) above. So there are $6 + 140 + 120 = 266$ ways of choosing a committee with at most two women.

Example 7.26. Suppose we have 6 ceramic sculptures which could be on display in any of 13 display cases. Assuming that each display case can hold at most one sculpture. How many ways can we display 4 of these sculpture in the display cases?

We first have to choose which of the four sculptures will be on display. There are $\binom{6}{4} = 15$ ways of choosing the 4 sculptures. Now that we have chosen the sculptures, we need to determine the 4 locations for the sculptures. Since there are 13 cases, there are $P(13,4) = 13(12)(11)(10) = 17,160$ ways of displaying the 4 chosen sculptures. So there are $15(17160) = 257,400$ ways of displaying any of the 4 sculptures.

Remark. The r-combinations of n are used heavily in the binomial theorem. Consider

$$(x+y)(x+y)(x+y)(x+y) = (x+y)^4.$$

In expanding this expression as a sum of terms, we need to determine how many copies of x^4, x^3y, x^2y^2, xy^3 and y^4 there are. There will be only one copy of x^4 since from each of the four copies of $x+y$ in the product we will choose the x or 0 copies of y. There will be $4 = \binom{4}{1}$ copies of x^3y since we can choose one y from each of the four copies of $x+y$. Similarly, there will be $6 = \binom{4}{2}$ copies of x^2y^2, $4 = \binom{4}{3}$ copies of xy^3 and $1 = \binom{4}{4}$ copy of y^4. Hence

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.$$

Theorem 7.27 (Binomial Theorem)**.** *For any $n \in \mathbb{N}$,*

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

Before proving the theorem, notice that the binomial coefficients appearing in the sum above correspond to the coefficients in the nth row of Pascal's triangle

$$\begin{array}{l ccccccccccccc}
n=0 & & & & & & & 1 & & & & & & \\
n=1 & & & & & & 1 & & 1 & & & & & \\
n=2 & & & & & 1 & & 2 & & 1 & & & & \\
n=3 & & & & 1 & & 3 & & 3 & & 1 & & & \\
n=4 & & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
n=5 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
n=6 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

This symmetric triangle continues infinitely downward. Notice that every entry is the sum of the two entries directly above it. We can make it a proposition as follows:

Proposition 7.28. For all $n, r \in \mathbb{N}$ with $n \geqslant 2$ and $1 \leqslant r \leqslant n$,

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Proof.

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

□

Now using this proposition we can prove the binomial theorem.

Proof of the binomial theorem: Prove by induction.

Base case:

$$(x+y)^1 = (x+y) = \binom{1}{0}x + \binom{1}{1}y.$$

Induction step: Assume that $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i$ for some $n \geqslant 2$. Multiply both sides by $(x+y)$ to obtain

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

where the third equality follows from the change of index (variable): $j = i+1$ or $i = j-1$.

As a consequence of the theorem, we can see that each row of Pascal's Triangle sums to $2n$ since

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

7.5 Repetitions

Suppose now that we allow some repetition of our objects. For example, suppose we have three identical white marbles and we want to place them among 10 distinct boxes. If at most one marble goes in each box, we know how to count this already. We just need to choose three boxes from the 10 or we have $\binom{10}{3} = 120$ ways of placing the marbles.

Now suppose we can put any number of marbles into a box. We can either put at most one marble in a box, or we could put 2 in one box and one in another box, or we could put all three in one box. There are $2!\binom{10}{2} = 90$ ways of placing 2 marbles in one box and one in another. The reason why we multiplied by 2! is because once we have chosen the two boxes, we can either place 2 in the first box or two in the second box. There are 10 ways of placing all three in the 10 boxes.

Using our addition principle, we find that there are 220 ways of placing the 3 marbles in the 10 boxes.

Notice that $\binom{10+3-1}{3} = \frac{12(11)(10)}{3(2)(1)} = 220$. If we try to put 9 identical marbles into 4 distinct boxes, this is much harder to analyze on a case by case basis but actually there are $\binom{4+9-1}{9} = 220$ ways of placing the 9 marbles in the 4 boxes. We will use the following proposition for counting the placement of identical objects in distinct boxes.

Proposition 7.29. Let $n, r \in \mathbb{Z}^+$. There are $\binom{n+r-1}{r}$ ways of placing r identical objects into n distinct boxes, where we suppose that each box can hold up to r objects.

Example 7.30. Suppose we have 3 identical red marbles and 2 identical blue marbles. How many ways can we place them in 7 distinct boxes? There are $\binom{7+3-1}{3} = 84$ ways to place the red marbles in the boxes and $\binom{7+2-1}{2} = 28$ ways to place the blue marbles. Using the multiplication principle, we have $84(28) = 2352$ ways of placing the marbles.

Example 7.31. Let $n, r \in \mathbb{Z}^+$. How many nonnegative integer solutions are there to

$$x_1 + x_2 + \cdots + x_n = r?$$

We can think of $r = 1 + 1 + \cdots + 1$ and the solutions to this equation will be the placements of 1's into the "box" for each variable. So the number of solutions is $\binom{n+r-1}{r}$.

Example 7.32. We also need to be careful when we have permutations involving some objects which are not distinct. For example, suppose we want to determine the number of anagrams of CHEESE. The E's are not distinct. First pretend the E's are distinct. For example, one is E, the other e and the last is ϵ. There are $6! = 720$ anagrams with different representations for each E. However, since they were all the same after all, we will divide by 3! which is the number of ways that we can order the three "distinct" E's. So there are $\frac{6!}{3!} = 120$ anagrams of CHEESE.

Example 7.33. If we want to place 4 red marbles, 3 blue marbles and 2 green marbles in 9 boxes so that each box has at most one marble, we can use the multiplication principle to find that there are $\binom{9}{4}\binom{5}{3}\binom{2}{2} = \frac{9!}{4!3!2!}$. Notice the similarity to Example 7.32.

7.6 Pigeonhole Principle

Proposition 7.34. (Pigeonhole Principle Version 1) Let $n, m \in \mathbb{Z}^+$. Suppose we have $n > m$ objects that need to be placed in m boxes. Then at least one box has at least two objects in it.

Proof. Let A_n represent the set of the n objects and B_m represent the set of m boxes. Consider a function $f : A_n \to B_m$ which represents the placement of objects into boxes. Since $|A_n| = n > m = |B_m|$, then f cannot be one to one so there exists $i, j \in A_n$ and $k \in B_m$ with $f(i) = k = f(j)$. Thus, the box represented by k has at least two objects placed in it. □

Proposition 7.35. (Pigeonhole Principle Version 2) Let A and B be finite sets and $|A| = n = |B|$, where $n \in \mathbb{Z}^+$. Let $f : A \to B$. Then the following properties are equivalent.

(i) f is one-to-one.

(i) f is onto.

Proof. (i) $\Longrightarrow$ (ii) Assume that f is one-to-one. Suppose that f is not onto. Then there exists some $b_1, \ldots, b_k \in B$ such that $b_1, \ldots, b_k \notin \operatorname{Ran}(f)$. Then we need place n objects in A to $n-k$ boxes. Hence by proposition 7.34, at least one box has at least two objects in it, contradicting the definition of the function f.

(ii) $\Longrightarrow$ (i) Assume that f is onto. Suppose that f is not one-to-one. Then there exists $i, j \in A$ such that $f(i) = f(j)$. Hence $|\operatorname{Ran}(f)| < |A| = |B|$, so $\operatorname{Ran}(f) \subsetneq B$, contradicting f is onto. □