DISCRETE MATHEMATICS, PROOFS

FARID ALINIAEIFARD

Contents

1. Fundamentals

1.1. **Sets.**

Definition. *A* **set** *is a collection of things. The things in the collection are called* **elements** *of the set.*

Example 1.1. $\{2,4,6,8\}$ *is a set and the elements of this set are* $2,4,6$ *and* 8*. Some sets have infinitely many elements, for example the set of all integers*

$$\mathbb{Z} = \{\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots\}$$

has infinitely many elements.

Definition. *A set is called an* **infinite set** *if it has infinitely many elements, otherwise it is called* **finite set.** *For example* $\{10, 11, 18\}$ *is finite and the set of integers* $\mathbb{Z}$ *is infinite.*

Definition. *Two sets are* **equal** *if they contain exactly the same elements. For example* $\{2,4,6,8\} = \{4,2,8,6\}$ *but* $\{2,4,6,8\} \neq \{2,4,6,7\}$*.*

Definition. *Let* $A = \{2,4,6,8\}$*. Then* 2 *is an element of* A *and we write* $2 \in A$*, and we say "*2 *is an element of* A*" or* 2 *in* A*. We also have* $4 \in A$*,* $6 \in A$*, and* $8 \in A$*, but* $5 \notin A$*, we read this last expression as "*5 *is not an element of* A*" or "*5 *not in* A*".*

Notation. The set of **natural numbers** is denoted by $\mathbb{N}$ and is

$$\mathbb{N} = \{1, 2, 3, 4, \cdots\}.$$

The set of **integers** is denoted by $\mathbb{Z}$ and is

$$\mathbb{Z} = \{\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots\}.$$

An also the set of real number is denoted by $\mathbb{R}$.

Remark. *Sets do not need have just numbers as elements. For example,*

(1) $B = \{F, T\}$.
(2) $C = \{a, e, i, o, u\}$*, the set of vowels.*
(3) $D = \{(0,0), (1,0), (0,1), (1,1)\}$*. Note that* $(0,0) \in D$ *and* $(1,0) \in D$*, but* $(1,2) \notin D$*.*
(4) $E = \{1, \{2,3\}, \{2,4\}\}$ *has there elements: the number* 1*, the set* $\{2,3\}$*, and the set* $\{2,4\}$*. But* $2 \notin E$ *and* $3 \notin E$*.*
(5)

$$M = \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\}.$$

Note that $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M$ *but* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \notin M$*.*

Definition. *If* X *is a set, its* **cardinality** *or* **size** *is the number of elements it has, and the cardinality of the set* X *is denoted by* $|X|$*. In the previous example we have* $|B| = 2$*,* $|C| = 5$*,* $|D| = 4$*,* $|E| = 3$*, and* $|M| = 3$*.*

Definition. *The* **empty set** *is the set* $\{\}$ *that has no elements. We denote it as* $\emptyset$*, so* $\emptyset = \{\}$*.* **Warning:** *Do not write* $\{\emptyset\}$ *when you mean* $\emptyset$*.*

We did an example by using some plastic bags in the classroom.

Example 1.2. *$F = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$. Then $|F| = 3$.*

Definition. *A special notation called* **set-builder notation** *is used to describe sets that are too big or complex to list between braces.*

Example 1.3. *$E = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$ in set-builder notation is written as*

$$E = \{2n : n \in \mathbb{Z}\}.$$

Remark. *In general, a set X written with set-builder notation has the syntax*

$$X = \{expression : rule\}.$$

Also, in set-builder notation we can express a set in some different ways, for example

$$E = \{2n : n \in \mathbb{Z}\} = \{n \in \mathbb{Z} : n \text{ is even}\}.$$

(read "E is the set of all $n \in \mathbb{Z}$ such that n is even").

1. $\{n : n \text{ is a prime number}\} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$
2. $\{n \in \mathbb{N} : n \text{ is prime}\} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$
3. $\{n^2 : n \in \mathbb{Z}\} = \{0, 1, 4, 9, 16, 25, \ldots\}$
4. $\{x \in \mathbb{R} : x^2 - 2 = 0\} = \{\sqrt{2}, -\sqrt{2}\}$
5. $\{x \in \mathbb{Z} : x^2 - 2 = 0\} = \emptyset$
6. $\{x \in \mathbb{Z} : |x| < 4\} = \{-3, -2, -1, 0, 1, 2, 3\}$
7. $\{2x : x \in \mathbb{Z}, |x| < 4\} = \{-6, -4, -2, 0, 2, 4, 6\}$
8. $\{x \in \mathbb{Z} : |2x| < 4\} = \{-1, 0, 1\}$

Definition. *The set of Rational numbers is denoted by $\mathbb{Q}$ and is*

$$\mathbb{Q} = \{x : x = m/n, \text{ where } m, n \in \mathbb{Z} \text{ and } n \neq 0\}.$$

For example, $-2/3, 4/6, 8/-10 \in \mathbb{Q}$.

Homeworks for Section 1.1:4,12,15,24, 27, 30, 31, 35, 36, 40, 43.

1.2. **The Cartesian Product.**

Definition. *An* **ordered pair** *is a list* (x, y) *of two things* x *and* y*, enclosed in parentheses and separated by a comma. For example,* $(4, 2)$ *is an ordered pair, as is* $(2, 4)$*. Note that* $(2, 4) \neq (4, 2)$*. We can have a ordered pair of letters,* (l, m)*. Also,* $(\{1, 2, 3\}, a)$ *is an ordered pair.*

Definition. *The* **Cartesian product** *of two sets* A *and* B *is another set, denoted by* $A \times B$ *and defined as* $A \times B = \{(a, b) : a \in A, b \in B\}$.

Example 1.4. (1) *Let* $A = \{k, l, m\}$ *and* $B = \{q, r\}$*, then*

$$A \times B = \{(k, q), (k, r), (l, q), (l, r), (m, q), (m, r)\}.$$

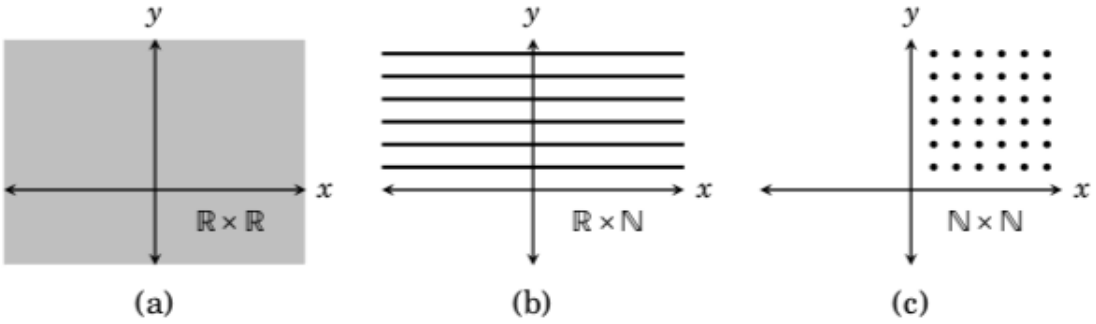
(2) *Let* $C = \{0, 1\}$ *and* $D = \{2, 1\}$*. Then*

$$C \times D = \{(0, 2), (0, 1), (1, 2), (1, 1)\}.$$

(Sketch it)

Example 1.5. *Sketch* $[0, 1] \times [-1, 1]$.

Fact. If A and B are finite sets, then $|A \times B| = |A|.|B|$. In the above example, $|A \times B| = |A||B| = 3.2 = 6$, and $|C \times D| = |C||D| = 2.2 = 4$.



Definition. *An* **Ordered triple** *is a list* (x, y, z)*. Also,*

$$A \times B \times C = \{(a, b, c) : a \in A, b \in B, c \in C\}.$$

In general,

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \cdots, x_n) : x_i \in A_i \text{ for each } i = 1, 2, \cdots, n\}.$$

Definition. *We can take* **Cartesian Powers** *of sets. For any set* A *and positive integer* n*, the power* A^n *is the Cartesian power of* A *with itself* n *times:*

$$A^n = A \times A \times \cdots \times A = \{(x_1, x_2, \cdots, x_n) : x_i \in A \text{ for each } i = 1, 2, \cdots, n\}.$$

Example 1.6.

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

Homework for Section 1.2: 1(a), 1(b), 1(e), 3, 4, 7, 10, 12,16.

1.3. **Subsets.**

Example 1.7. *Consider the following sets*

$$A = \{0, 2, 4\}\ B = \{0, 1, 2, 4\}.$$

Note that each element of A is an element of B. In this situation we say A is a subset of B

Definition. *Suppose A and B are sets. If every element of A is also an element of B, then we say A is a* **subset** *of B, and we denote this as $A \subseteq B$. We write $A \nsubseteq B$ is A is not a subset of B, and that is when there is at least one element in A that is not an element of B.*

Example 1.2 Be sure you understand why each of the following is true.

1. $\{2,3,7\} \subseteq \{2,3,4,5,6,7\}$
2. $\{2,3,7\} \nsubseteq \{2,4,5,6,7\}$
3. $\{2,3,7\} \subseteq \{2,3,7\}$
4. $\{2n : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$
5. $\{(x, \sin(x)) : x \in \mathbb{R}\} \subseteq \mathbb{R}^2$
6. $\{2,3,5,7,11,13,17,\ldots\} \subseteq \mathbb{N}$
7. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
8. $\mathbb{R} \times \mathbb{N} \subseteq \mathbb{R} \times \mathbb{R}$

In class, We used the plastic bags to show the following fact.
Fact The empty set is a subset of every set, that is, $\emptyset \subseteq B$ for any set B.

Example 1.8. *Write all of the subsets of $A = \{a, b, c\}$.*

Solution. All subsets of A are

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

Fact. If a finite set has n elements, then it has 2^n subsets.

Example 1.9. *All subsets of $B = \{1, 2, \{1, 3\}\}$ are*

$$\{\}, \{1\}, \{2\}, \{\{1, 3\}\}, \{1, 2\}, \{1, \{1, 3\}\}, \{2, \{1, 3\}\}, \{1, 2, \{1, 3\}\}.$$

Question.

(1) *Is $\{1, 3\}$ a subset of B ($\{1, 3\} \subseteq B$)? No, because $3 \in \{1, 3\}$ but $3 \notin B$.*
(2) *Is $\{1, 3\}$ in B ($\{1, 3\} \in B$)? Yes.*
(3) *Is $\{\{1, 3\}\}$ a subset of B ($\{\{1, 3\}\} \subseteq B$)? Yes.*

Example 1.3 Be sure you understand why the following statements are true. Each illustrates an aspect of set theory that you've learned so far.

1. $1 \in \{1,\{1\}\}$ ..... 1 is the first element listed in $\{1,\{1\}\}$
2. $1 \notin \{1,\{1\}\}$ ..... because 1 is not a set
3. $\{1\} \in \{1,\{1\}\}$ ..... $\{1\}$ is the second element listed in $\{1,\{1\}\}$
4. $\{1\} \subseteq \{1,\{1\}\}$ ..... make subset $\{1\}$ by selecting 1 from $\{1,\{1\}\}$
5. $\{\{1\}\} \notin \{1,\{1\}\}$ ..... because $\{1,\{1\}\}$ contains only 1 and $\{1\}$, and not $\{\{1\}\}$
6. $\{\{1\}\} \subseteq \{1,\{1\}\}$ ..... make subset $\{\{1\}\}$ by selecting $\{1\}$ from $\{1,\{1\}\}$
7. $\mathbb{N} \notin \mathbb{N}$ ..... because $\mathbb{N}$ is a set (not a number) and $\mathbb{N}$ contains only numbers
8. $\mathbb{N} \subseteq \mathbb{N}$ ..... because $X \subseteq X$ for every set X
9. $\emptyset \notin \mathbb{N}$ ..... because the set $\mathbb{N}$ contains only numbers and no sets
10. $\emptyset \subseteq \mathbb{N}$ ..... because $\emptyset$ is a subset of every set
11. $\mathbb{N} \in \{\mathbb{N}\}$ ..... because $\{\mathbb{N}\}$ has just one element, the set $\mathbb{N}$
12. $\mathbb{N} \not\subseteq \{\mathbb{N}\}$ ..... because, for instance, $1 \in \mathbb{N}$ but $1 \notin \{\mathbb{N}\}$
13. $\emptyset \notin \{\mathbb{N}\}$ ..... note that the only element of $\{\mathbb{N}\}$ is $\mathbb{N}$, and $\mathbb{N} \neq \emptyset$
14. $\emptyset \subseteq \{\mathbb{N}\}$ ..... because $\emptyset$ is a subset of every set
15. $\emptyset \in \{\emptyset,\mathbb{N}\}$ ..... $\emptyset$ is the first element listed in $\{\emptyset,\mathbb{N}\}$
16. $\emptyset \subseteq \{\emptyset,\mathbb{N}\}$ ..... because $\emptyset$ is a subset of every set
17. $\{\mathbb{N}\} \subseteq \{\emptyset,\mathbb{N}\}$ ..... make subset $\{\mathbb{N}\}$ by selecting $\mathbb{N}$ from $\{\emptyset,\mathbb{N}\}$
18. $\{\mathbb{N}\} \not\subseteq \{\emptyset,\{\mathbb{N}\}\}$ ..... because $\mathbb{N} \notin \{\emptyset,\{\mathbb{N}\}\}$
19. $\{\mathbb{N}\} \in \{\emptyset,\{\mathbb{N}\}\}$ ..... $\{\mathbb{N}\}$ is the second element listed in $\{\emptyset,\{\mathbb{N}\}\}$
20. $\{(1,2),(2,2),(7,1)\} \subseteq \mathbb{N} \times \mathbb{N}$ ..... each of (1,2), (2,2), (7,1) is in $\mathbb{N} \times \mathbb{N}$

Homework for Section 1.3: 2,4,5,8,9,10,15,16.

1.4. **Power Sets.**

Definition. *If A is a set, the* **power set** *of A is another set, denoted as $\mathcal{P}(A)$ and defined to be the set of all subsets of A.*

Example 1.10. *If $A = \{1, 2, 3\}$. Then*

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Fact. If A is a finite set, then $|\mathcal{P}| = 2^{|A|}$.

Example 1.4 You should examine the following statements and make sure you understand how the answers were obtained. In particular, notice that in each instance the equation $|\mathscr{P}(A)| = 2^{|A|}$ is true.

1. $\mathscr{P}(\{0,1,3\}) = \{\emptyset, \{0\}, \{1\}, \{3\}, \{0,1\}, \{0,3\}, \{1,3\}, \{0,1,3\}\}$
2. $\mathscr{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
3. $\mathscr{P}(\{1\}) = \{\emptyset, \{1\}\}$
4. $\mathscr{P}(\emptyset) = \{\emptyset\}$
5. $\mathscr{P}(\{a\}) = \{\emptyset, \{a\}\}$
6. $\mathscr{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
7. $\mathscr{P}(\{a\}) \times \mathscr{P}(\{\emptyset\}) = \{(\emptyset,\emptyset), (\emptyset,\{\emptyset\}), (\{a\},\emptyset), (\{a\},\{\emptyset\})\}$
8. $\mathscr{P}(\mathscr{P}(\{\emptyset\})) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset,\{\emptyset\}\}\}$
9. $\mathscr{P}(\{1,\{1,2\}\}) = \{\emptyset, \{1\}, \{\{1,2\}\}, \{1,\{1,2\}\}\}$
10. $\mathscr{P}(\{\mathbb{Z},\mathbb{N}\}) = \{\emptyset, \{\mathbb{Z}\}, \{\mathbb{N}\}, \{\mathbb{Z},\mathbb{N}\}\}$

Next are some that are **wrong**. See if you can determine why they are wrong and make sure you understand the explanation on the right.

11. $\mathscr{P}(1) = \{\emptyset, \{1\}\}$ ..... meaningless because 1 is not a set
12. $\mathscr{P}(\{1,\{1,2\}\}) = \{\emptyset,\{1\},\{1,2\},\{1,\{1,2\}\}\}$ ..... wrong because $\{1,2\} \not\subseteq \{1,\{1,2\}\}$
13. $\mathscr{P}(\{1,\{1,2\}\}) = \{\emptyset,\{\{1\}\},\{\{1,2\}\},\{\emptyset,\{1,2\}\}\}$ ..... wrong because $\{\{1\}\} \not\subseteq \{1,\{1,2\}\}$

Homework for Section 1.4: 1, 6, 8, 11, 12, 14, 16, 17, 19.

1.5. **Union, Intersection, and Difference.**

Definition. *Suppose A and B are sets.*

(1) *The* **union** *of A and B is the set*
$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$
(2) *The* **intersection** *of A and B is the set*
$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$
(3) *The* **difference** *of A and B is the set*
$$A - B = \{x : x \in A, x \notin B\}.$$

Example 1.5 Suppose $A = \{a,b,c,d,e\}$, $B = \{d,e,f\}$ and $C = \{1,2,3\}$.

1. $A \cup B = \{a,b,c,d,e,f\}$
2. $A \cap B = \{d,e\}$
3. $A - B = \{a,b,c\}$
4. $B - A = \{f\}$
5. $(A-B) \cup (B-A) = \{a,b,c,f\}$
6. $A \cup C = \{a,b,c,d,e,1,2,3\}$
7. $A \cap C = \emptyset$
8. $A - C = \{a,b,c,d,e\}$
9. $(A \cap C) \cup (A - C) = \{a,b,c,d,e\}$
10. $(A \cap B) \times B = \{(d,d),(d,e),(d,f),(e,d),(e,e),(e,f)\}$
11. $(A \times C) \cap (B \times C) = \{(d,1),(d,2),(d,3),(e,1),(e,2),(e,3)\}$

Remark. *Let X and Y be two sets. Then we have $X \cup Y = Y \cup X$, $X \cap Y = Y \cap X$, and $X - Y = Y - X$.*

12. $[2,5] \cup [3,6] = [2,6]$
13. $[2,5] \cap [3,6] = [3,5]$
14. $[2,5] - [3,6] = [2,3)$
15. $[0,3] - [1,2] = [0,1) \cup (2,3]$

Homework for Section 1.5: 1(e), 1(c), 2(a), 2(b), 3(c), 3(e), 3(f), 3(h), 4 (a), 4(b), 16.

1.6. **Complement.**

Definition. (1) *We say U is a* **universal set** *or a* **universe** *for a set A if $A \subseteq U$.*

(2) *Let A be a set with a universal set U. The* **complement** *of A, denoted $\overline{A}$, is the set $\overline{A} = U - A$.*

Example 1.11. (1) *Let $A = \{a, c, d\}$ and $U = \{a, b, c, \dots, h\}$ be a universal set for A. Then*

$$\overline{A} = \{b, e, f, g, h\}.$$

(2) *Let P be the set of all prime numbers, and $\mathbb{N}$ be a universal set for P. Then*

$$\overline{P} = \mathbb{N} - P = \{1, 4, 6, 8, 9, \cdots\}.$$

Homework for Section 1.6: 1(a), 1(b), 1(c), 1(d), 1(e), 2(f), 2(g), 2(h), 2 (i), 3.

1.7. **Venn Diagrams.**

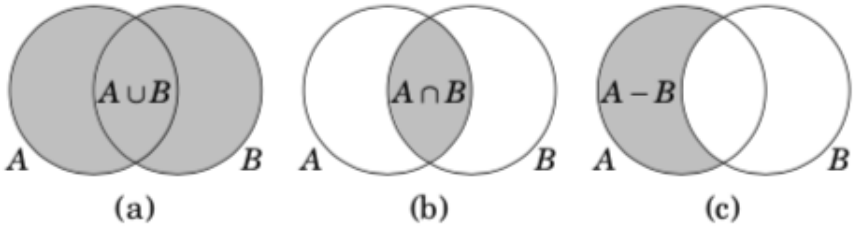


Figure 1.7. Venn diagrams for two sets

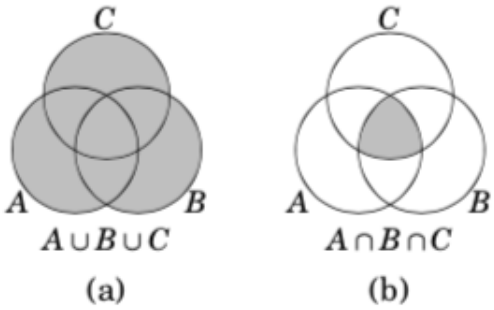


Figure 1.8. Venn diagrams for three sets

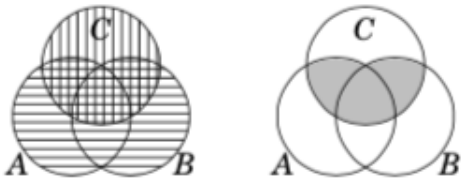


Figure 1.9. How to make a Venn diagram for $(A \cup B) \cap C$

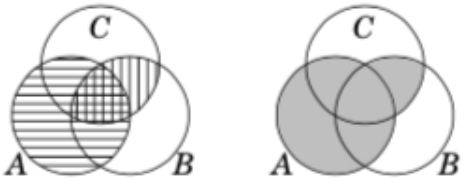


Figure 1.10. How to make a Venn diagram for $A \cup (B \cap C)$

Remark. *Comparing Figures 1.9 and 1.10, we see that the parentheses are* **essential**.

Homework for Section 1.7: 2, 5, 6, 9, 10, 12, 13, 14.

1.8. **Indexed Sets.** We usually use indexed sets when a problem involved lots of sets.

Example 1.12. *Suppose* $A_1 = \{0, 2, 5\}$, $A_2 = \{1, 2, 5\}$, *and* $A_3 = \{2, 5, 7\}$. *Then*

$$\bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3 = \{0, 1, 2, 5, 7\} \text{ and } \bigcap_{i=1}^{3} A_i = A_1 \cap A_2 \cap A_3 = \{2, 5\}.$$

Definition. *Suppose* $A_1, A_2, \dots, A_n$ *are sets. Then*

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n = \{x : x \in A_i \text{ for at least one set } A_i, \text{ for } 1 \le i \le n\},$$

and

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n = \{x : x \in A_i \text{ for every set } A_i, \text{ for } 1 \le i \le n\}.$$

We even can use this notation we have infinitely many sets.

Example 1.13. *This example involves the following infinite list of sets.*

$$A_1 = \{-1, 0, 1\}, A_2 = \{-2, 0, 2\}, A_3 = \{-3, 0, 3\}, \cdots, A_i = \{-i, 0, i\}, \cdots$$

Observe that

$$\bigcup_{i=1}^{\infty} = A_1 \cup A_2 \cup A_3 \cdots = \mathbb{Z} \text{ and } \bigcap_{i=1}^{\infty} = A_1 \cap A_2 \cap A_3 \cap \cdots = \{0\}.$$

Remark. *Here is a useful notation.*

$$\bigcup_{i=1}^{3} A_i = \bigcup_{i \in \{1,2,3\}} A_i \text{ and } \bigcap_{i=1}^{3} A_i = \bigcap_{i \in \{1,2,3\}} A_i$$

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i \in \mathbb{N}} A_i \quad \text{and} \quad \bigcap_{i=1}^{\infty} A_i = \bigcap_{i \in \mathbb{N}} A_i.$$

Definition. *If we have a set* A_i *for every* i *in some set index set* I, *then*

$$\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ for at least one set } A_i \text{ with } i \in I\}$$

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for every set } A_i \text{ with } i \in I\}$$

Example 1.14. *Let* $A_i = \{i\}$ *and* $B_i = [0, 1] \times \{i\}$. *Then*

$$\bigcup_{i \in [1,2]} = [1, 2] \text{ and } \bigcap_{i \in [0,2]} B_i = [0, 1] \times [0, 2].$$

Homework for Section 1.8: 2, 4, 8, 9, 12, 14.

1.9. **Sets that are number systems.**

Example 1.15. *Consider all following subset of* $\mathbb{N}$.

$$A = \{x \in \mathbb{N} : x \geq 4\}, B = \{5, 10, 15, ...\}, C = \{x \in \mathbb{N} : x^2 \geq 3\}$$

The smallest element of each of these sets exits and for A *is 4, for* B *is 5, for* C *is* 2.

Fact: Well-ordering principal: Every non-empty subset of natural numbers $\mathbb{N}$ has a smallest element.

Fact. Given integers a and b with $b > 0$, there exist integers q and r for which $a = qb + r$ and $0 \leq r < b$. For example, if $a = 17$ and $b = 5$, then $17 = 5 \times 3 + 2$, and if $a = -19$ and $b = 6$, then $-19 = (6 \times -4) + 5$.

1.10. **Russell's Paradox.** Russell's Paradox involves the following set.

$$A = \{X : X \text{ is a set and } X \notin X\}.$$

There are many sets that are in A, for example, $\mathbb{Z} \notin \mathbb{Z}$, therefore $\mathbb{Z} \in A$, also, $\{1, 2, 3\} \notin \{1, 2, 3\}$, and so $\{1, 2, 3\} \in A$. Now there are two important questions:

(a) Is there a set that is not in A?
(b) Is A an element of A? (Rossell's paradox arises from this question)

To answer part (a) consider $B = \{\{\{\{...\}\}\}\}$, then B has only one element which is itself. So $B \in B$ and we can conclude that $B \notin A$.
Part (b): if $A \in A$ is true, then by the definition of A, we must have $A \notin A$ is true, so at the same time we have $A \in A$ and $A \notin A$. Therefore, this is a mathematical statement that is both true and false.

The Russel's Paradox caused that mathematicians review the concept of set theory and come up with an evaluation of what can and cannot be regarded as a set.
Zermelo-Fraenkel axioms:
(1) Well-ordering axiom
(2) The axiom of **foundation**: no nonempty set X is allowed to have the property that $X \cap x \neq \emptyset$ for all its elements x (i.e., there is at least one element $x \in X$ such that $X \cap x = \emptyset$).

By Zermelo-Fraenkel axioms as described above, B is not a set. By axiom of function, not set is a element of itself. Assume on the contrary that A is an element of itself. Then $A = \{A\}$, but this is a contradiction to axiom of foundation. Therefore, if A in Russel's paradox is a set, we must explicitly say that $A \in A$ is false, which we can not, therefore, A is not a set.

2. Logic

2.1. **Statements.**

Definition. *A* **statement** *is a sentence or a mathematical expression that is either definitely true or definitely false. We usually denote the statement by capital letters.*
Example 2.1.

P : *There is a snake in this class.*
Q : 2 *is not an even number.*
T : *A positive integer is odd or even.*
P_1: *If* x *is a multiple of* 6*, then* x *is not even.*
P_2: 3 *is odd and* 2 *is even.*
P_3: $\mathbb{N} \subseteq \mathbb{Z}$

More famous examples:
Fermat's last theorem: For all numbers $a, b, c, n \in \mathbb{N}$ with $n > 2$, it is the case that $a^n + b^n \neq c^n$.
Goldbach conjecture: Every even integer greater than 2 is a sum of two prime numbers.

2.2. **And, or, not.** Some times we can make some new statement by using other statements. For example,
P: 2 is an even number
Q : 3 is an even number
R : There is a snake in our classroom.
S: We have at least one desk in the classroom.
are two statement, we can construct new statements:
$P \wedge Q$: 2 is an even number **and** 3 is an even number.
$P \vee Q$: 2 is an even number **or** 3 is an even number.
$\sim P$: 2 is **not** an even number.
$\sim Q$: 3 is **not** an even number.
$Q \wedge R$: 3 is an even number **and** there is a snake in our classroom.
$S \vee R$: We have at least one desk in our classroom **or** there is a snake in our classroom.
$P \wedge \sim Q$: 2 is an even number **and** 3 is an odd number.
$\sim Q \wedge \sim R$: 3 is **not** an even number **and** there is not a snake in our classroom.

And ($\wedge$):

We now want to find out if we have statements P and Q, then when $P \wedge Q$ (P and Q) is true and when it is false.

Example 2.2. *Consider the following two statements*
P : 2 *is an even integer.*
Q : 3 *is an odd integer.*
Then P is true, Q is true, and also
$P \wedge Q$: 2 *is an even integer* **and** 3 *is an odd integer is true.*

P : *There is a snack in our classroom.*
Q : *There is at least one desk in our classroom.*
Then P is not true, Q is true, and
$P \wedge Q$: *There is a snack in our classroom* **and** *there is at least one desk in our classroom*
is false.

P : 5 *is an even integer.*
Q : *there is at least one desk in our classroom.*
Then P is false, Q is true, and also
$P \wedge Q$: 5 *is an even integer* **and** *there is an at least one desk in the classroom*
is false.

P : 5 *is an even integer.*
Q : *there is a snake in our classroom.*
Then P is false, Q is false, and also
$P \wedge Q$: 5 *is an even integer* **and** *there is a snake in the classroom*
is false.

We can see that $P \wedge Q$ is true if both P and Q are true.

Truth Table:

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

Or ($\vee$):

We now want to find out if we have statements P and Q, then when $P \vee Q$ (P **or** Q) is true and when it is false.

Example 2.3. *Consider the following two statements*
P : 2 *is an even integer.*
Q : 3 *is an odd integer.*
Then P is true, Q is true, and also
$P \vee Q$: 2 *is an even integer* **or** 3 *is an odd integer is true.*

P : *There is a snack in our classroom.*
Q : *There is at least one desk in our classroom.*
Then P is not true, Q is true, and
$P \vee Q$: *There is a snack in our classroom* **or** *there is at least one desk in our classroom*
is true.

P : 5 *is an even integer.*
Q : *there is at least one desk in our classroom.*
Then P is false, Q is true, and also
$P \vee Q$: 5 *is an even integer* **and** *there is an at least one desk in the classroom*
is true.

P : 5 *is an even integer.*
Q : *there is a snake in our classroom.*
Then P is false, Q is false, and also
$P \vee Q$: 5 *is an even integer* **or** *there is a snake in the classroom*
is false.

We can see that $P \wedge Q$ is true if both P and Q are true.

Truth Table:

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

Remark. *The* $\vee$ *(***or***) in mathematics is slightly different from the* **or** *in English. We have that* $P \vee Q$ *is true means that at least one of* P *and* Q *is true, or even it is fine if both are true. But consider the following statement in English:*
"$(P:)$ *You pay your tuition* **or** $(Q:)$ *you are not allowed to take any courses." It is not possible that both* P *and* Q *happen at the same time.*

Negation:

Negation of an statement P ($\sim P$) is the statement "It is not true that P". For example,
P : It is raining.
$\sim P$: It is not raining.

Now if P is true (it is raining), then $\sim P$ (it is not raining) is false. If P is false (it is not raining), then $\sim P$ is true (it is not raining).

Truth Table:

P	$\sim P$
T	F
F	T

Homeworks for Section 2.2: 1, 2, 3, 4, 5, 6, 7, 8.

2.3. **Conditional Statements.**

Example 2.4. *Assume that we have the following statements.*
P : *The integer a is a multiple of* 6.
Q : *the integer a is divisible by* 2.
There is yet another way to construct a new statement by using "if...., then....".
R : *If a is a multiple of* 6, *then a is divisible by* 2.

Definition. *In general, given any two statements P and Q, we can form the new statement "If P, then Q." This is written symbolically as $P \Rightarrow Q$ which we read as "If P, then Q" or "P implies Q". A statement of the form $P \Rightarrow Q$ is called a* **conditional** *statement because it means Q will be true under the condition that P is true.*

Now we are planning to construct the truth table of $P \Rightarrow Q$.

Example 2.5. *Suppose your professor makes the following promise:*
If *you pass the final exam,* **then** *you will pass the course.*
So the professor makes the following promise:
(You pass the final) $\Rightarrow$ (You pass the course).
We now want to check that under which situation the professor lies (not me that professor :)).

You pass the final	*You pass the course*	$(Youpassthefinal) \Rightarrow$ *(You pass the course)*
T	T	T
T	F	F
F	T	T
F	F	T

The truth table for $P \Rightarrow Q$ is the same as the above example:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Remark. *There are other grammatical constructions that also mean $P \Rightarrow Q$. Here is a summary of the main ones:*

If P, then Q.	$P \Rightarrow Q$
Q if P.	
Q whenever P.	
Q, provided that P.	
Whenever P, then also Q.	
P is a sufficient condition for Q.	
For Q, it is sufficient that P.	
Q is a necessary condition for P.	
For P, it is necessary that Q.	
P only if Q.	

Homeworks for Section 2.3: *1, 2, 5, 6, 8, 9, 10.*

2.4. **Biconditional Statements.**

Example 2.6. *Consider*
P : *a is a multiple of* 6
Q : *a is divisible by* 2

$$(P \Rightarrow Q)\ (a \text{ is a multiple of } 6) \Rightarrow (a \text{ is divisible by } 2)$$
$$(Q \Rightarrow P)\ (a \text{ is divisible by } 2) \Rightarrow (a \text{ is a multiple of } 6)$$

Note that the first statement $(P \Rightarrow Q)$ is true but the second statement $(Q \Rightarrow P)$ is not true. So, we can not say if $(P \Rightarrow Q)$ is true, then $(Q \Rightarrow P)$ is also true.

Definition. *The conditional statement $Q \Rightarrow P$ is called the* **converse** *of $P \Rightarrow Q$, so a conditional statement and its inverse express different things.*

Remark. *It happen sometimes that $P \Rightarrow Q$ and also $Q \Rightarrow P$ are both true. For example, consider*

$$(a \text{ is even}) \Rightarrow (a \text{ is divisible by } 2),$$
$$(a \text{ is divisible by } 2) \Rightarrow (a \text{ is even}).$$

Notation. We introduce a new symbol $\Leftrightarrow$ to express the meaning of the statement $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. The expression $P \Leftrightarrow Q$ is understood to have exactly the same meaning as $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. We read $P \Leftrightarrow Q$ as "P if and only if Q."

The following is the truth table for $P \Leftrightarrow Q$.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

The following constructions all mean $P \Leftrightarrow Q$:

P if and only if Q.
P is a necessary and sufficient condition for Q.
For P it is necessary and sufficient that Q.
If P, then Q, and conversely.

} $P \Leftrightarrow Q$

Section 2.4: 1, 2, 3, 4, 5.

2.5. **Truth Tables for Statements.** We know the truth table for $\wedge, \vee, \sim, \Rightarrow, \Leftrightarrow$. We now combine them to make some new statements and will build their truth tables.

Truth table of $(P \vee Q) \wedge \sim (P \wedge Q)$.

P	Q	$(P \vee Q)$	$(P \wedge Q)$	$\sim (P \wedge Q)$	$(P \vee Q) \wedge \sim (P \wedge Q)$
T	T	T	T	F	**F**
T	F	T	F	T	**T**
F	T	T	F	T	**T**
F	F	F	F	T	**F**

Truth table of $P \Leftrightarrow (Q \vee R)$.

P	Q	R	$Q \vee R$	$P \Leftrightarrow (Q \vee R)$
T	T	T	T	**T**
T	T	F	T	**T**
T	F	T	T	**T**
T	F	F	F	**F**
F	T	T	T	**F**
F	T	F	T	**F**
F	F	T	T	**F**
F	F	F	F	**T**

Remark. $\sim P \vee Q$ *means* $(\sim P) \vee Q$.

Section 2.5: 2, 8, 6, 11.

2.6. **Logical Equivalence.** The following truth table includes the truth table of the following two statements.

$$(P \wedge Q) \vee (\sim P \wedge \sim Q) \text{ and } P \Leftrightarrow Q$$

P	Q	$\sim P$	$\sim Q$	$(P \wedge Q)$	$(\sim P \wedge \sim Q)$	$(P \wedge Q) \vee (\sim P \wedge \sim Q)$	$P \Leftrightarrow Q$
T	T	F	F	T	F	**T**	**T**
T	F	F	T	F	F	**F**	**F**
F	T	T	F	F	F	**F**	**F**
F	F	T	T	F	T	**T**	**T**

Consider that the two statements

$$(P \wedge Q) \vee (\sim P \wedge \sim Q) \text{ and } P \Leftrightarrow Q$$

have the same truth tables, and we usually write

$$(P \wedge Q) \vee (\sim P \wedge \sim Q) = P \Leftrightarrow Q.$$

Definition. *In general, two statements are* **logically equivalent** *if their truth values match up line-for-line in a truth table.*

Example 2.7. *(***Contrapositive Law***)*

$$P \Rightarrow Q = (\sim Q) \Rightarrow (\sim P)$$

P	Q	$\sim P$	$\sim Q$	$(\sim Q) \Rightarrow (\sim P)$	$P \Rightarrow Q$
T	T	F	F	**T**	**T**
T	F	F	T	**F**	**F**
F	T	T	F	**T**	**T**
F	F	T	T	**T**	**T**

Theorem 2.8. *(***DeMorgan's Laws***)*

(1) $\sim (P \wedge Q) = (\sim P) \vee (\sim Q)$.
(2) $\sim (P \vee Q) = (\sim P) \wedge (\sim Q)$.

Proof. The following table shows that (1) is true and similarly we can show the second one.

P	Q	$\sim P$	$\sim Q$	$P \wedge Q$	$\sim (P \wedge Q)$	$(\sim P) \vee (\sim Q)$
T	T	F	F	T	**F**	**F**
T	F	F	T	F	**T**	**T**
F	T	T	F	F	**T**	**T**
F	F	T	T	F	**T**	**T**

□

Example 2.9. *It can also be verified that all the following laws are true.*

$$P \Rightarrow Q \;=\; (\sim Q) \Rightarrow (\sim P) \qquad \text{Contrapositive law} \qquad (2.1)$$

$$\left.\begin{aligned} \sim(P \wedge Q) &= \sim P \vee \sim Q \\ \sim(P \vee Q) &= \sim P \wedge \sim Q \end{aligned}\right\} \qquad \text{DeMorgan's laws} \qquad (2.2)$$

$$\left.\begin{aligned} P \wedge Q &= Q \wedge P \\ P \vee Q &= Q \vee P \end{aligned}\right\} \qquad \text{Commutative laws} \qquad (2.3)$$

$$\left.\begin{aligned} P \wedge (Q \vee R) &= (P \wedge Q) \vee (P \wedge R) \\ P \vee (Q \wedge R) &= (P \vee Q) \wedge (P \vee R) \end{aligned}\right\} \qquad \text{Distributive laws} \qquad (2.4)$$

$$\left.\begin{aligned} P \wedge (Q \wedge R) &= (P \wedge Q) \wedge R \\ P \vee (Q \vee R) &= (P \vee Q) \vee R \end{aligned}\right\} \qquad \text{Associative laws} \qquad (2.5)$$

Remark. *Indeed,* $P \vee (Q \wedge R) and (P \vee Q) \wedge R$ *are not logically equivalent.*

Section 2.6: 6, 7, 8, 10, 13.

2.7. **Quantifiers.** Using symbols $\vee, \wedge, \sim, \Rightarrow$, and $\Leftrightarrow$ we can translate some English sentence into symbolic form. We now introduce two new symbols: "$\forall$" which stands for the phrase "For all" or "For every" and the symbol "$\exists$" which stands for the phrase "There exists a" or "There is a". They symbols $\forall$ and $\exists$ are called **quantifiers**. The symbol $\forall$ is called **universal quantifier** and the symbol $\exists$ is called **existential quantifier**.

Example 2.10. *The following English statements are paired with their translations into symbolic forms.*

(1) *For every $n \in \mathbb{Z}$, $2n$ is even.*
$\forall n \in \mathbb{Z}$, $2n$ *is even.*
(2) *There exists a subset X of $\mathbb{N}$ for which $|X| = 5$.*
$\exists X \subseteq \mathbb{N}, |X| = 5$.
(3) *Every integer that is not odd is even.*
$\forall n \in \mathbb{Z}, \sim (n \text{ is odd}) \Rightarrow n$ *is even.*
(4) *For every real number x, there is a real number y for which $y^3 = x$.*
$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x$.

Example 2.11. *We also can translate false statements into symbolic forms.*

(1) *There is an integer n for which $n^2 = 2$.*
$\exists n \in \mathbb{Z}, n^2 = 2$.
(2) *For every real number x, there is a real number y for which $y^2 = x$.*
$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^2 = x$.

Warning. When there are more than one quantifier in a statement, we should be very alert to their order, for reversing the order can change the meaning. for example,

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x$$

is a true statement since we can always choose $y = \sqrt[3]{x}$. However, if we we change the order of quantifiers we have

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y^3 = x$$

which is a false statement.
Section 2.7. 2, 4, 5, 8, 10.

2.8. **More on Conditional Statements.** Statements can contain variables. Here is an example.

$$P : \text{If an integer x is a multiple of 6, then x is even.}$$

This is a sentence that is true. (All multiples of 6 are even, so no matter which multiple of 6 the integer x happens to be, it is even.) Since the sentence P is definitely true, it is a statement.

When a sentence or statement P contains a variable such as x, we sometimes denote it as $P(x)$ to indicate that it is saying something about x. Thus the above statement can be denoted as

$$P(x) : \text{If an integer } x \text{ is a multiple of 6, then } x \text{ is even.}$$

A statement or sentence involving two variables might be denoted $P(x, y)$, and so on. It is quite possible for a sentence containing variables to not be a statement. Consider the following example.

$$Q(x) : \text{The integer } x \text{ is even.}$$

Is this a statement? Whether it is true or false depends on just which integer x is. It is true if $x = 4$ and false if $x = 7$, etc. But without any stipulations on the value of x it is impossible to say whether $Q(x)$ is true or false. Since it is neither definitely true nor definitely false, $Q(x)$ cannot be a statement. A sentence such as this, whose truth depends on the value of one or more variables, is called an **open sentence.**

Now we want to see how to symbolically express the conditional statements.

Example 2.12. (1) *If x is a multiple of* 6*, then x is even.*
$\forall x(x \text{ is a multiple of } 6) \Rightarrow (x \text{ is even})$.
(2) *If $P(x)$, then $Q(x)$.*
$\forall x \in S, P(x) \Rightarrow Q(x)$.

The only time that $P(x) \Rightarrow Q(x)$ is a false statement is when $P(x)$ is true and $Q(x)$ is false. So to check that $P(x) \Rightarrow Q(x)$ is false we need to find one x such that $P(x)$ is true and $Q(x)$ is false.

Example 2.13. *The following are true statements:*

(1) *If $x \in \mathbb{R}$, then $x^2 + 1 > 0$.*
(2) *If a function f is differentiable on $\mathbb{R}$, then f is continuous on $\mathbb{R}$.*

Likewise, the following are false statements:

(1) *If p is a prime number, then p is odd. (2 is prime.)*
(2) *If x is an positive integer, then $\sqrt{x}$ is rational. ($\sqrt{2}$ is not rational.)*

2.9. **Translating English to Symbolic Logic.**

Example 2.14. (1) *If f is continuous on the interval $[a, b]$ and differentiable on (a, b), then there is a number $c \in (a, b)$ for which $f'(c) = \frac{f(b)-f(a)}{b-a}$. Here is a translation to symbolic form:*
((f continuous on $[a, b]$) $\wedge$ (f differentiable on (a, b))) $\Rightarrow$ ($\exists c \in (a, b)$, $f'(c) = \frac{f(b)-f(a)}{b-a}$).

(2) *Every even integer greater than 2 is the sum of two primes. Let P be the set of primes.*
$\forall x \in \{2, 4, 6, ...\}$, $\exists n, m \in P$, $x = m + n$

(3) *At least one of the integers x and y is even.*
(x is even)$\vee$ (y is even)

(4) *The integer x is even, but the integer y is odd.*
(x is even)$\wedge$ (y is odd)

Section 2.9: 2, 4, 6, 8, 10.

2.10. **Negating Statements.**

Definition. *Given a statement R, the statement $\sim R$ is called the negation of R.*

Remember the DeMorgan's laws,

(1) $\sim (P \wedge Q) = (\sim P) \vee (\sim Q)$.
(2) $\sim (P \vee Q) = (\sim P) \wedge (\sim Q)$.

Example 2.15. *Consider the following statement*
R : You can go to school by bus or Ober.
(You can go to school by bus) or (You go to school by Ober)
By DeMorgan's law,
$\sim$ (You can go to school by bus) $\vee$ (You go to school by Ober) = ($\sim$ (You can go to school by bus))$\wedge$ ($\sim$(You go to school by Ober)).
Which means, You cannot go to school by bus and you can not go to school by Ober.

R: The numbers x and y are both odd.
R : (x is odd) and (y is odd)
R : (x is odd) $\wedge$ (y is odd)
$\sim R$: (x is even) $\vee$ (y is even)
which means at least one of x and y is even.

Let look at the following example which is slightly different form previous ones.

Example 2.16. *Look at the following statement $\sim (\forall x \in \mathbb{N}, P(x))$, Reading this in words,*
$P(x)$ is true for all natural numbers x.
The negation of this statement is "this is not true that $P(x)$ is true for all natural numbers", or we can say, "there is $x \in \mathbb{N}$ such that $P(x)$ is not true", in symbols,
$\sim (\forall x \in \mathbb{N}, P(x)) = \exists x \in \mathbb{N}, \sim P(x)$.
In general we have,

(1) $\sim (\forall x \in S, P(x)) = \exists x \in S, \sim P(x)$
(2) $\sim (\exists x \in S, P(x)) = \forall x \in S, \sim P(x)$

Example 2.17. *Consider the following statement.*
R: The square of every real number is non-negative.
$\sim R$: There exists a real number whose square is negative.
In symbols, $R : \forall x \in \mathbb{R}, x^2 \geq 0$
$\sim R : \exists x \in \mathbb{R}, \sim (x^2 \geq 0) = \exists x \in \mathbb{R}, x^2 < 0$.

Example 2.18. *Consider the following statement.*
S : For every real number x there is a real number y for which $y^3 = x$.
$S : \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x$.
$\sim S :\sim (\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x) =$
$\exists x \in \mathbb{R}, \sim (\exists y \in \mathbb{R}, y^3 = x) =$
$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \sim (y^3 = x) = \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, (y^3 \neq x)$.
In words, $\sim S$: There exists a real number x that for all real number y, $y^3 \neq x$. Also, we can say,
$\sim S$: There is a real number x for which $y^3 \neq x$ for all real numbers y.

In writing proofs you will sometimes have to negate a conditional statement $P \Rightarrow Q$, which means we should find a situation that $P \Rightarrow Q$ is false, and we already seen that this happens only when P is true and Q is false.

Theorem 2.19. $\sim (P \Rightarrow Q) = P \wedge \sim Q$.

Proof. It is a straightforward practice to show the above equivalence by using truth table. □

Example 2.20. *Consider the following statement, "If a is odd, then* a^2 *is odd." The negation of this statement, by what we showed above, is "a is odd and* a^2 *is even." In symbols,*
$R : \forall x \in \mathbb{Z}, (x \text{ is odd}) \Rightarrow (x \text{ is odd})$
$\sim R : \exists x \in \mathbb{Z}, (x \text{ is odd}) \wedge \sim (x \text{ is odd})$
$\sim R : \exists x \in \mathbb{Z}, (x \text{ is odd}) \wedge (x \text{ is even})$.

Section 2.10: 2, 4, 6, 8, 10.

2.11. **Logical Inference.** Suppose that we know $P \Rightarrow Q$ is true. Can we say that P is true? No, because we have a situation like P false and Q False, but $P \Rightarrow Q$ is true. So, logically we can not say that P is true or false if $P \Rightarrow Q$ is true. Now assume that we know that $P \Rightarrow Q$ is true and also P is true, can we say that Q is true? Yes, we must have Q is true. You can check this by looking at truth table of $P \Rightarrow Q$. This is called logical inference.

Definition. Logical Inference*: Given two true statements we can infer that a third statement is true.*

$$\frac{P \Rightarrow Q \quad P}{Q} \qquad \frac{P \Rightarrow Q \quad \sim Q}{\sim P} \qquad \frac{P \vee Q \quad \sim P}{Q}$$

We can have other situations, for example,

$$\frac{P \quad Q}{P \wedge Q} \qquad \frac{P \wedge Q}{P} \qquad \frac{P}{P \vee Q}$$

3. Counting

3.1. Counting Lists.

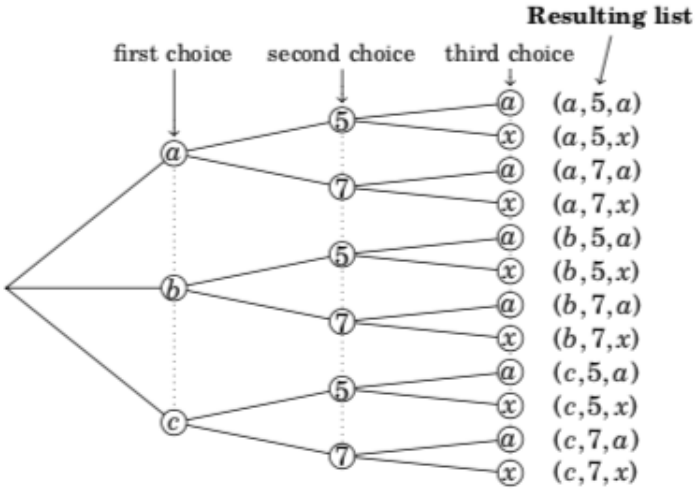
Definition. *A list is an ordered sequence of objects. For example,* (a, b, c, d, e) *is a list and* **entries** *of this list are* a, b, c, d *and* e.

Remark.
(1) *If the entries are rearranged we get a different list, for example* $(a, b, c, d, e) \neq (b, a, c, d, e)$.
(2) *Unlike sets, lists are allowed to have repeated entries. For example* $(5, 3, 5, 4, 3, 3)$ *is a perfectly acceptable list, as is* (S, O, S).
(3) *The number of entries in a list is called its* **length**. *Thus* $(5, 3, 5, 4, 3, 3)$ *has length six, and* (S, O, S) *has length three.*

Example 3.1. $(0, (0, 1, 1))$ *is a list of length two whose second entry is a list of length three. The list* $(\mathbb{N}, \mathbb{Z}, \mathbb{R})$ *has length three.*

Definition. *There is one very special list which has no entries at all. It is called the* **empty list**, *and is denoted* $()$. *It is the only list whose length is zero.*

Example 3.2. *We want to construct a list that its first element is in the set* $\{a, b, c\}$ *and the second entry must be in* $\{5, 7\}$ *and the last entry must be in* $\{a, x\}$.



We summarize the type of reasoning used above in an important fact called the multiplication principle.

Fact (Multiplication Principle) Suppose in making a list of length n there are a_1 possible choices for the first entry, a_2 possible choices for the second entry, a_3 possible choices for the third entry and so on. Then the total number of different lists that can be made this way is the product $a_1 \cdot a_2 \cdot a_3 \ldots a_n$.

Remark. *Sometimes we can look at words, or numbers as a list. For example, we can consider the number* 54837 *as the list* $(5, 4, 8, 3, 7)$ *and "Jimmy" as* (j, i, m, m, y).

Example 3.3. *A standard license plate consists of three letters followed by four numbers. For example, JRB-4412 and MMX-8901 are two standard license plates. (Vanity plates such as LV2COUNT are not included among the standard plates.) How many different standard license plates are possible?*

Solution. We have 26 letters in English and 10 digits $0, 1, 2, \dots, 9$. So if we look at a plate as a list for each of the first three entry we have 26 choices and for the each last four we have 10 choices. Therefore, the number of possible plates are

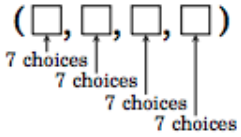
$$26.26.26.10.10.10.10 = 175,760,000.$$

Q.E.D

We say that repetition is allowed in the first type of list and repetition is not allowed in the second kind of list. (Often we call a list in which repetition is not allowed a **non-repetitive list**.)

Example 3.4. *Consider making lists from symbols A, B, C, D, E, F, G.*
(a) How many length-4 lists are possible if repetition is allowed?
(b) How many length-4 lists are possible if repetition is **not** *allowed?*
(c) How many length-4 lists are possible if repetition is **not** *allowed and the list must contain an E?*
(d) How many length-4 lists are possible if repetition is allowed and the list must contain an E?

Solution. (a) We have



So the number of possible list of length 4 is equal to 7^4.

(b) As we can

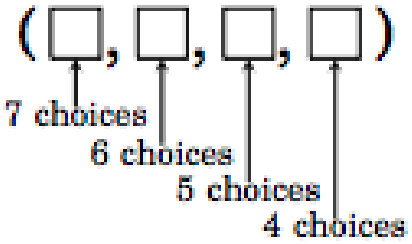


FIGURE 1.

the number of lists are $7.6.5.4 = 840$.

(c) By the following picture

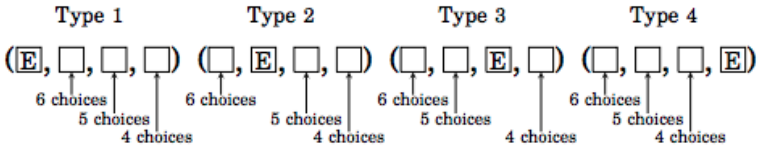


FIGURE 2.

the number of possible lists are $4.(6.5.4) = 480$.

(d) We can count the number of all list that repetition is allowed minus the number of list that does not contain any E and repetition is allowed, which this number is equal to $7^4 - 6^4 = 2401 - 1296 = 1105$.

Is the same idea as we used in part (c) working here? If we use the same idea, we have

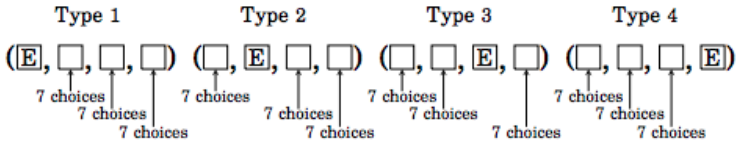


FIGURE 3.

therefore, the number of possible choices are $4.7^3 = 1372$, which is larger than what expected. The reason for this is that there are some lists that we count them twice or more, for example The list (E, E, A, B) is of type 1 and type 2, so it got counted twice.

Section 3.1. 4, 6, 8, 10, 12.

3.2. **Factorials.** How many list of length n with n symbols is possible if repetition is allowed.

n	Symbols	Non-repetitive lists of length n made from the symbols	$n!$
0	$\{\}$	$()$	1
1	$\{A\}$	(A)	1
2	$\{A,B\}$	$(A,B),(B,A)$	2
3	$\{A,B,C\}$	$(A,B,C),(A,C,B),(B,C,A),(B,A,C),(C,A,B),(C,B,A)$	6
4	$\{A,B,C,D\}$	$(A,B,C,D),(A,B,D,C),(A,C,B,D),(A,C,D,B),(A,D,B,C),(A,D,C,B)$ $(B,A,C,D),(B,A,D,C),(B,C,A,D),(B,C,D,A),(B,D,A,C),(B,D,C,A)$ $(C,A,B,D),(C,A,D,B),(C,B,A,D),(C,B,D,A),(C,D,A,B),(C,D,B,A)$ $(D,A,B,C),(D,A,C,B),(D,B,A,C),(D,B,C,A),(D,C,A,B),(D,C,B,A)$	24
⋮	⋮	⋮	⋮

FIGURE 4.

Definition. *If n is a non-negative integer, then the factorial of n, denoted $n!$, is the number of non-repetitive lists of length n that can be made from n symbols. Thus $0! = 1$ and $1! = 1$. If $n > 1$, then*

$$n! = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1.$$

Note that $n! = n(n-1)!$.

Example 3.5. *This problem involves making lists of length seven from the symbols $0, 1, 2, 3, 4, 5$ and 6.*
(a) How many such lists are there if repetition is **not** *allowed?*
(b) How many such lists are there if repetition is **not** *allowed and the first three entries must be odd?*
(c) How many such lists are there in which repetition is allowed, and the list must contain at least one repeated number?

Solution. (a) $7!$
(b) $3.2.1.4.3.2.1 = 4!3! = 144$.
(c) It is the same to count the number of all list minus the number of lists with no repetition, which is

$$7^7 - 7! = 818,503.$$

Fact 3.2. The number of non-repetitive lists of length k whose entries are chosen from a set of n possible entries is

$$\frac{n!}{(n-k)!}.$$

Proof. Consider that the number of such a list is

$$n(n-1)\ldots(n-k+1) = \frac{n!}{(n-k)!}.$$

□

Section 3.2: 2, 4, 6, 8.

k	k-element subsets of $\{a,b,c,d\}$	$\binom{4}{k}$
-1		$\binom{4}{-1}=0$
0	$\emptyset$	$\binom{4}{0}=1$
1	$\{a\},\{b\},\{c\},\{d\}$	$\binom{4}{1}=4$
2	$\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\},\{c,d\}$	$\binom{4}{2}=6$
3	$\{a,b,c\},\{a,b,d\},\{a,c,d\},\{b,c,d\}$	$\binom{4}{3}=4$
4	$\{a,b,c,d\}$	$\binom{4}{4}=1$
5		$\binom{4}{5}=0$
6		$\binom{4}{6}=0$

FIGURE 5.

3.3. **Counting Subsets.**

Definition. *If n and k are integers, then $\binom{n}{k}$ denotes the number of subsets that can be made by choosing k elements from a set with n elements. The symbol $\binom{n}{k}$ is read "n choose k." (Some textbooks write $C(n,k)$ instead of $\binom{n}{k}$.*

Fact. If $n,k\in\mathbb{Z}$ and $0\leq k\leq n$, then $\binom{n}{k}=\frac{n!}{n!(n-k)!}$. Otherwise, $\binom{n}{k}=0$.

Example 3.6. *This problem concerns 5-card hands that can be dealt off of a 52-card deck. How many such hands are there in which two of the cards are clubs and three are hearts? (Note that we have four kind of cards, clubs, spades, diamonds, and hearts).*

Example 3.7. *This problem concerns 5-card hands that can be dealt off of a 52-card deck. How many such hands are there in which one of the cards is club and four are hearts?*

Section 3.3: 4, 6, 8, 12, 14.

3.4. **Pascal's Triangle and the Binomial Theorem. Fact.**

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k+1}$$

Consider that $\binom{n+1}{k}$ is the number of possibilities to choose subsets containing k elements from the set $\{0, 1, 2, \dots, n\}$.

The set of subsets of $\{0, 1, 2, \dots, n\}$ with k elements =

(A) The set of subsets of $\{0, 1, 2, \dots, n\}$ with k elements and containing 0

$\bigcup$

(B) The set of subsets of $\{0, 1, 2, \dots, n\}$ with k elements and not containing 0

The set in A has $\binom{n}{k}$ elements and the set in B has $\binom{n}{k+1}$ elements.

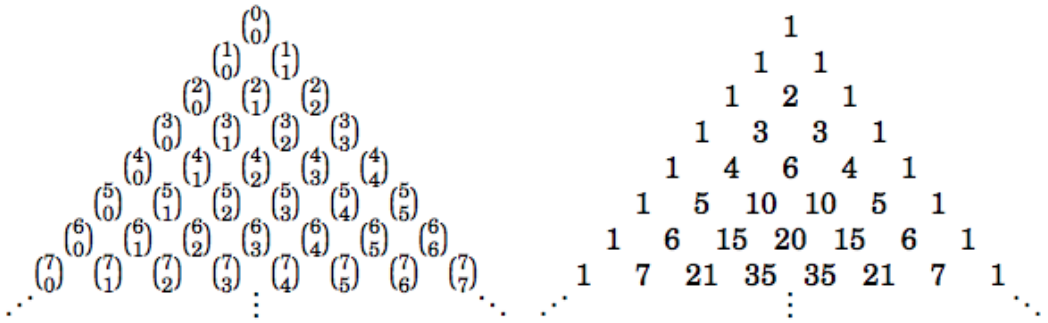


Figure 3.2. Pascal's triangle

FIGURE 6.

Theorem 3.8. (Binomial Theorem) *If n is a non-negative integer, then*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-2}x^2y^{n-2} + \binom{n}{1}xy^{n-1} + \binom{n}{n}y^n.$$

Section 3.4: 2, 4, 6, 8, 10, 12.

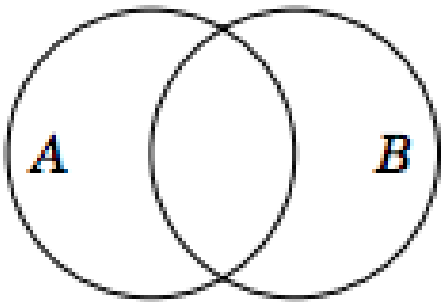


FIGURE 7.

3.5. **Inclusion-Exclusion.** We want to compute $|A \cup B|$, and by the above picture we have

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Example 3.9. *A* 3*-card hand is dealt off of a standard* 52*-card deck. How many different such hands are there for which all* 3 *cards are red or all three cards are face cards?*

Solution. Let A be the set of all choices of 3 cards that are red, and B be the set of all choices of 3 cards that are face cards.

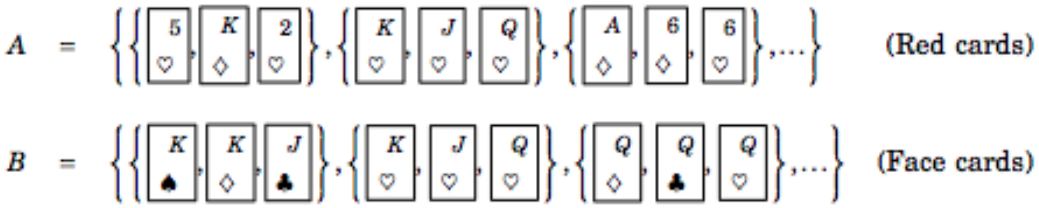


FIGURE 8.

Therefore, $|A| = \binom{26}{3}$ and $|B| = \binom{12}{3}$. Now $A \cap B$ is the set of all 3 cards that are red face cards, so

FIGURE 9.

and $|A \cap B| = \binom{6}{3}$. Therefore,

$$|A \cup B| = |A| + |B| - |A \cap B| = \binom{26}{3} + \binom{12}{3} - \binom{6}{3}.$$

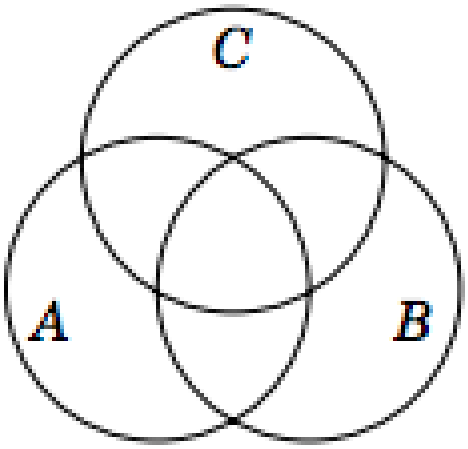


FIGURE 10.

By the above picture we can see that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Fact (**Addition Principal**) If $A_1, A_2, \ldots, A_n$ are sets with $A_i \cap A_j = \emptyset$ whenever $i \neq j$, then

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Section 3.5: 2, 4, 6, 8, 10.

3.6. **Latex Codes.** For different notations and formula check the following web page https://artofproblemsolving.com/wiki/index.php/LaTeX:Symbols

All symbols that we have used:

(1) $\mathbb{Z}$

```
$\mathbb{Z}$
```

(2) $\mathbb{R}$

```
$\mathbb{R}$
```

(3) $\mathbb{N}$

```
$\mathbb{N}$
```

(4)

$$\mathbb{N}=\{1,2,3,\cdots\}$$

```
$$ \mathbb{N}= \{ 1,2,3,\cdots \}$$
```

(5) $\{a,b,c\}$

```
$\{a,b,c \}$
```

(6)

$$\left(\begin{array}{ccc} 1&2&4\\ 6&3&3 \end{array} \right)$$

```
$$\left( \begin{array}{ccc}
1&2&4\\
6&3&3
\end{array} \right)$$
```

(7) $\emptyset$

```
$\emptyset$
```

(8) $2 \in A$

```
$2\in A$
```

(9) $C \times D$

```
$C\times D$
```

(10) $\binom{n}{k}$

```
${n\choose k}$
```

(11) $\binom{7}{4}$

```
${7 \choose 4}$
```

(12) $A \cap B$

```
$A\cap B$
```

(13) $B \cup A$

```
$B\cup A$
```

(14)

$$\bigcup_{i=1}^{n} A_i$$

```
$$\bigcup_{i=1}^nA_i$$
```

(15)

$$\bigcap_{i=1}^{n} A_i$$

```
$$\bigcap_{i=1}^nA_i$$
```

(16) $A \subseteq B$

```
$A\subseteq B$
```

(17) $A \nsubseteq B$

```
$A\not\subseteq B$
```

(18) $2 \notin A$

```
$2\not\in A$
```

(19) $P \Rightarrow Q$

```
$P\Rightarrow Q$
```

(20) $P \Leftrightarrow Q$

```
$P\Leftrightarrow Q$
```

(21)

P	$\sim P$
T	F
F	T

```
$$\begin{array}{c|c}
P&\sim P\\
\hline
\hline
T&F\\
\hline
F&T
\end{array}$$
```

(22) $\forall x \in \mathbb{Z}$

```
$\forall x \in \mathbb{Z}$
```

(23) $\exists x \in \mathbb{R}$

```
$\exists x\in \mathbb{R}$
```

(24) $Y^3 = x$

```
$Y^3=x$
```

(25) $(x^2)^2$

```
${({x^2})}^2$
```

(26) $\sqrt{x}$

```
$\sqrt{x}$
```

(27) $\sqrt[3]{2}$

```
$\sqrt[3]{2}$
```

(28) $\frac{a}{b}$

```
$\frac{a}{b}$
```

(29) $P \wedge Q$

```
$P\wedge Q$
```

(30) $P \vee Q$

```
$P\vee Q$
```

(31) $3 > 2$ and $3 \geq 2$.

```
$3>2$ and $3\geq 2$.
```

For every integer $x \in \mathbb{Z}$, $x^2 \geq 0$.

```
For every integer $x\in \mathbb{Z}$, $x^2\geq 0$.
```

4. Direct Proofs

4.1. **Theorems.**

Definition. (1) *A* **theorem** *is a statement that is true and has been proved to be true.*
(2) *A* **statement** *that is true but not as significant is sometimes called a proposition.*
(3) *A* **lemma** *is a theorem whose main purpose is to help prove another theorem.*
(4) *A* **corollary** *is a result that is an immediate consequence of a theorem or proposition.*

4.2. **Definitions.**

Definition. (1) *An integer n is* **even** *if $n = 2a$ for some integer $a \in \mathbb{Z}$.*
(2) *An integer n is odd if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.*
(3) *Two integers have the* **same parity** *if they are both even or they are both odd. Otherwise they have* **opposite parity**.
(4) *Suppose a and b are integers. We say that a divides b, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a divisor of b, and that b is a multiple of a.*
(5) *A natural number n is* **prime** *if it has exactly two positive divisors, 1 and n. We say a natural number is* **composite** *if it is not prime.*
(6) *The greatest common divisor of integers a and b, denoted $gcd(a, b)$, is the largest integer that divides both a and b. The least common multiple of nonzero integers a and b, denoted $lcm(a, b)$, is smallest positive integer that is a multiple of both a and b.*

Fact.(The Devision Algorithm) Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

4.3. **Direct Proof.** We want to show that the following proposition is true.

Proposition 4.1. *If P, then Q.*

Consider the truth table for $P \Rightarrow Q$,

P	Q	$P \Rightarrow Q$
T	T	T
T	F	$\mathbf{F}$
F	T	T
F	F	T

FIGURE 11.

To show that $P \Rightarrow Q$, we only should check that if P is true, then Q also is true, because in other cases (P is false) always makes the statement true.

Outline for Direct Proof

Proposition If P, then Q.

Proof. Suppose P.

⋮

Therefore Q. ■

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd. Then $x = 2a+1$ for some $a \in \mathbb{Z}$, by definition of an odd number. Thus $x^2 = (2a+1)^2 = 4a^2+4a+1 = 2(2a^2+2a)+1$, so $x^2 = 2b+1$ where $b = 2a^2+2a \in \mathbb{Z}$. Therefore x^2 is odd, by definition of an odd number. ■

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.
By Definition 4.4, we know $a \mid b$ means there is an integer d with $b = ad$.
Likewise, $b \mid c$ means there is an integer e for which $c = be$.
Thus $c = be = (ad)e = a(de)$, *so* $c = ax$ *for the integer* $x = de$.
Therefore $a \mid c$. ■

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.
Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.
So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.
Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.
Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number. ■

Proposition If $a, b, c \in \mathbb{N}$, then $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$.

Proof. Assume $a, b, c \in \mathbb{N}$. Let $m = \text{lcm}(ca, cb)$ and $n = c \cdot \text{lcm}(a, b)$. We will show $m = n$. By definition, $\text{lcm}(a, b)$ is a multiple of both a and b, so $\text{lcm}(a, b) = ax = by$ for some $x, y \in \mathbb{Z}$. From this we see that $n = c \cdot \text{lcm}(a, b) = cax = cby$ is a multiple of both ca and cb. But $m = \text{lcm}(ca, cb)$ is the *smallest* multiple of both ca and cb. Thus $m \leq n$.

On the other hand, as $m = \text{lcm}(ca, cb)$ is a multiple of both ca and cb, we have $m = cax = cby$ for some $x, y \in \mathbb{Z}$. Then $\frac{1}{c}m = ax = by$ is a multiple of both a and b. Therefore $\text{lcm}(a, b) \leq \frac{1}{c}m$, so $c \cdot \text{lcm}(a, b) \leq m$, that is, $n \leq m$.

We've shown $m \leq n$ and $n \leq m$, so $m = n$. The proof is complete. ■

Proposition Let x and y be positive numbers. If $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$.

Proof. Suppose $x \leq y$. Subtracting y from both sides gives $x - y \leq 0$.
This can be written as $\sqrt{x}^2 - \sqrt{y}^2 \leq 0$.
Factor this to get $(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \leq 0$.
Dividing both sides by the positive number $\sqrt{x} + \sqrt{y}$ produces $\sqrt{x} - \sqrt{y} \leq 0$.
Adding $\sqrt{y}$ to both sides gives $\sqrt{x} \leq \sqrt{y}$. ■

Proposition If x and y are positive real numbers, then $2\sqrt{xy} \leq x+y$.

Proof. Suppose x and y are positive real numbers.
Then $0 \leq (x-y)^2$, that is, $0 \leq x^2 - 2xy + y^2$.
Adding $4xy$ to both sides gives $4xy \leq x^2 + 2xy + y^2$.
Factoring yields $4xy \leq (x+y)^2$.
Previously we proved that such an inequality still holds after taking the square root of both sides; doing so produces $2\sqrt{xy} \leq x+y$. ■

4.4. **Using Cases.** We sometimes check all possible cases to show that a statement is true.

Consider the following table

n	$1+(-1)^n(2n-1)$
1	0
2	4
3	−4
4	8
5	−8
6	12

FIGURE 12.

By the above table we can now conjecture that for each $n \in \mathbb{N}$, $1+(-1)^n(2n-1)$ is a multiple of 4.

Proposition If $n \in \mathbb{N}$, then $1+(-1)^n(2n-1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.
Then n is either even or odd. Let's consider these two cases separately.

Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.
Thus $1+(-1)^n(2n-1) = 1+(1)(2\cdot 2k-1) = 4k$, which is a multiple of 4.

Case 2. Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.
Thus $1+(-1)^n(2n-1) = 1-(2(2k+1)-1) = -4k$, which is a multiple of 4.

These cases show that $1+(-1)^n(2n-1)$ is always a multiple of 4. ■

Proposition 4.2. *Every multiple of* 4 *equals* $1 + (-1)^n(2n-1)$ *for some* $n \in \mathbb{N}$.

Proof. We can write the statement above as follow: If k is a multiple of 4, then there is $n \in \mathbb{Z}$ such that $1 + (-1)^n(2n-1) = k$. Suppose k is a multiple of 4. Then $k = 4a$ for some $a \in \mathbb{Z}$. We proceed the proof by considering if a is zero, positive, or negative.
Case 1. Suppose $a = 0$. Then we must find an integer n such that $1+(-1)^n(2n-1) = 0$. Consider that when $n = 1$, then $1 + (-1)(2 \times 1 - 1) = 0$.
Case 2. Suppose $a > 0$. Let $n = 2a$. Then $1 + (-1)^{2a}(2(2a) - 1) = 4a = k$.
Case 3. Suppose $a < 0$. Let $n = 1 - 2a$. Then $1 - 2a \in \mathbb{N}$ and $1 + (-1)^{1-2a}(2(1 - 2a) - 1) = 4a = k$. □

Proposition If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers with opposite parity.
We need to show that $m+n$ is odd. This is done in two cases, as follows.
Case 1. Suppose m is even and n is odd. Thus $m = 2a$ and $n = 2b+1$ for some integers a and b. Therefore $m+n = 2a+2b+1 = 2(a+b)+1$, which is odd (by Definition 4.2).
Case 2. Suppose m is odd and n is even. Thus $m = 2a+1$ and $n = 2b$ for some integers a and b. Therefore $m+n = 2a+1+2b = 2(a+b)+1$, which is odd (by Definition 4.2).
In either case, $m+n$ is odd. ■

The phrase "**Without loss of generality...**" (abbreviated as **WLOG**) is a common way of signaling that the proof is treating just one of several nearly identical cases.

Proposition If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers with opposite parity.
We need to show that $m+n$ is odd.
Without loss of generality, suppose m is even and n is odd.
Thus $m=2a$ and $n=2b+1$ for some integers a and b.
Therefore $m+n=2a+2b+1=2(a+b)+1$, which is odd (by Definition 4.2). ■

Chapter 4: 2, 6, 8, 10, 14, 18, 20, 23.

5. Contrapositive Proof

5.1. **Contrapositive Proof.** Remember that $P \Rightarrow Q$ was equivalent to $\sim Q \Rightarrow \sim P$ by the truth table.

P	Q	$\sim Q$	$\sim P$	$P \Rightarrow Q$	$\sim Q \Rightarrow \sim P$
T	T	F	F	**T**	**T**
T	F	T	F	**F**	**F**
F	T	F	T	**T**	**T**
F	F	T	T	**T**	**T**

Figure 13.

So instead of showing that $P \Rightarrow Q$, we show that $\sim Q \Rightarrow \sim P$. The expression $\sim Q \Rightarrow \sim P$ is called the **contrapositive form** of $P \Rightarrow Q$.

Proposition Suppose $x \in \mathbb{Z}$. If $7x+9$ is even, then x is odd.

Proof. (Direct) Suppose $7x+9$ is even.
Thus $7x+9 = 2a$ for some integer a.
Subtracting $6x+9$ from both sides, we get $x = 2a-6x-9$.
Thus $x = 2a-6x-9 = 2a-6x-10+1 = 2(a-3x-5)+1$.
Consequently $x = 2b+1$, where $b = a-3x-5 \in \mathbb{Z}$.
Therefore x is odd. ■

Proposition Suppose $x \in \mathbb{Z}$. If $7x+9$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd.
Thus x is even, so $x = 2a$ for some integer a.
Then $7x+9 = 7(2a)+9 = 14a+8+1 = 2(7a+4)+1$.
Therefore $7x+9 = 2b+1$, where b is the integer $7a+4$.
Consequently $7x+9$ is odd.
Therefore $7x+9$ is not even. ■

Proposition Suppose $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd.
Thus x is even, so $x = 2a$ for some integer a.
So $x^2-6x+5 = (2a)^2-6(2a)+5 = 4a^2-12a+5 = 4a^2-12a+4+1 = 2(2a^2-6a+2)+1$.
Therefore $x^2 - 6x + 5 = 2b + 1$, where b is the integer $2a^2 - 6a + 2$.
Consequently $x^2 - 6x + 5$ is odd.
Therefore $x^2 - 6x + 5$ is not even. ■

Proposition Suppose $x, y \in \mathbb{R}$. If $y^3 + yx^2 \leq x^3 + xy^2$, then $y \leq x$.

Proof. (Contrapositive) Suppose it is not true that $y \leq x$, so $y > x$.
Then $y - x > 0$. Multiply both sides of $y - x > 0$ by the positive value $x^2 + y^2$.

$$\begin{aligned} (y-x)(x^2+y^2) &> 0(x^2+y^2) \\ yx^2+y^3-x^3-xy^2 &> 0 \\ y^3+yx^2 &> x^3+xy^2 \end{aligned}$$

Therefore $y^3 + yx^2 > x^3 + xy^2$, so it is not true that $y^3 + yx^2 \leq x^3 + xy^2$. ■

Proposition Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proof. (Contrapositive) Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$.
By DeMorgan's law, it is not true that $5 \nmid x$ **or** it is not true that $5 \nmid y$.
Therefore $5 \mid x$ or $5 \mid y$. We consider these possibilities separately.
Case 1. Suppose $5 \mid x$. Then $x = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ay)$, and that means $5 \mid xy$.
Case 2. Suppose $5 \mid y$. Then $y = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ax)$, and that means $5 \mid xy$.
The above cases show that $5 \mid xy$, so it is not true that $5 \nmid xy$. ■

5.2. **Congruence of Integers.** We start by a definition.

Definition 5.1 Given integers a and b and an $n \in \mathbb{N}$, we say that a and b are **congruent modulo n** if $n \mid (a-b)$. We express this as $a \equiv b \pmod{n}$. If a and b are not congruent modulo n, we write this as $a \not\equiv b \pmod{n}$.

Example 5.1 Here are some examples:

1. $9 \equiv 1 \pmod 4$ because $4 \mid (9-1)$.
2. $6 \equiv 10 \pmod 4$ because $4 \mid (6-10)$.
3. $14 \not\equiv 8 \pmod 4$ because $4 \nmid (14-8)$.
4. $20 \equiv 4 \pmod 8$ because $8 \mid (20-4)$.
5. $17 \equiv -4 \pmod 3$ because $3 \mid (17-(-4))$.

Fact.(The Devision Algorithm) Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

Proposition 5.1. *Let a and b be integers. If $a \equiv b(mod\ n)$ if and only if a and b have the same remainder when divided by n.*

Proof. We should prove if $a \equiv b(mod\ n)$ then a and b have the same remainder when divided by n and also if a and b have the same remainder when divided by n, then $a \equiv b(mod\ n)$.
($\Leftarrow$) Suppose a and b have the same remainder when divided by n, say r. Then $a = nq + r$ and $b = np + r$ for some $p, q \in \mathbb{Z}$ and $0 \leq r < n$. So,

$$a - b = nq + r - (np + r) = n(q - p)$$

and thus $n|a - b$, and $a \equiv b(mod\ n)$.
($\Rightarrow$) We want to prove that if $a \equiv b(mod\ n)$ then a and b have the same remainder when divided by n. We use contrapositive to prove the above statement. Suppose that a and b do not have the same reminder when divided by n, so assume $a = nq+r$ and $b = np + s$ for some $p, q \in \mathbb{Z}$, $0 \leq r < n$, $0 \leq s < n$, and $s \neq r$. Therefore, $a - b = n(p - q) + (r - s)$, and so $n \not| a - b$. We have that $a \not\equiv b(mod\ n)$. □

Proposition 5.2. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a^2 \not\equiv b^2(modn)$, then $a \not\equiv b(modn)$.*

Proof. (Contrapositive) Suppose $a \equiv b(modn)$. Then $n|a-b$, and so $n|(a-b)(a+b)$, which means $n|a^2 - b^2$. □

Remark. *For any natural number $n > 1$, we have*

$$x^n - 1 = (x - 1)(1 + x + x^2 + \cdots + x^{n-1}).$$

Proposition 5.3. *If $n \in \mathbb{N}$ and $2^n - 1$ is prime, then n is prime.*

Proof. (Contrapositive) Suppose n is not prime, then there is a prime number p such that $p|n$, and so $n = pk$ for some inter k. Then

$$2^n - 1 = 2^{(pk)} - 1 = (2^p)^k - 1 = (2^p - 1)(1 + 2^p + \cdots + (2^p)^{n-1}).$$

Therefore, $2^n - 1$ is not prime. □

5.3 Mathematical Writing

Now that we have begun writing proofs, it is a good time to contemplate the craft of writing. Unlike logic and mathematics, where there is a clear-cut distinction between what is right or wrong, the difference between good and bad writing is sometimes a matter of opinion. But there are some standard guidelines that will make your writing clearer. Some of these are listed below.

1. **Begin each sentence with a word, not a mathematical symbol.** The reason is that sentences begin with capital letters, but mathematical symbols are case sensitive. Because x and X can have entirely different meanings, putting such symbols at the beginning of a sentence can lead to ambiguity. Here are some examples of bad usage (marked with ×) and good usage (marked with ✓).

A is a subset of B.	×
The set A is a subset of B.	✓
x is an integer, so $2x+5$ is an integer.	×
Because x is an integer, $2x+5$ is an integer.	✓
$x^2 - x + 2 = 0$ has two solutions.	×
$X^2 - x + 2 = 0$ has two solutions.	× (and silly too)
The equation $x^2 - x + 2 = 0$ has two solutions.	✓

2. **End each sentence with a period,** even when the sentence ends with a mathematical symbol or expression.

Euler proved that $\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$	×
Euler proved that $\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$.	✓

Mathematical statements (equations, etc.) are like English phrases that happen to contain special symbols, so use normal punctuation.

3. **Separate mathematical symbols and expressions with words.** Not doing this can cause confusion by making distinct expressions appear to merge into one. Compare the clarity of the following examples.

Because $x^2 - 1 = 0$, $x = 1$ or $x = -1$.	×
Because $x^2 - 1 = 0$, it follows that $x = 1$ or $x = -1$.	✓
Unlike $A \cup B$, $A \cap B$ equals $\emptyset$.	×
Unlike $A \cup B$, the set $A \cap B$ equals $\emptyset$.	✓

4. **Avoid misuse of symbols.** Symbols such as $=$, $\leq$, $\subseteq$, $\in$, etc., are not words. While it is appropriate to use them in mathematical expressions, they are out of place in other contexts.

   Since the two sets are $=$, one is a subset of the other. ×
   Since the two sets are equal, one is a subset of the other. ✓

   The empty set is a $\subseteq$ of every set. ×
   The empty set is a subset of every set. ✓

   Since a is odd and x odd $\Rightarrow x^2$ odd, a^2 is odd. ×
   Since a is odd and any odd number squared is odd, then a^2 is odd. ✓

5. **Avoid using unnecessary symbols.** Mathematics is confusing enough without them. Don't muddy the water even more.

   No set X has negative cardinality. ×
   No set has negative cardinality. ✓

6. **Use the first person plural.** In mathematical writing, it is common to use the words "we" and "us" rather than "I," "you" or "me." It is as if the reader and writer are having a conversation, with the writer guiding the reader through the details of the proof.

7. **Use the active voice.** This is just a suggestion, but the active voice makes your writing more lively.

   The value $x = 3$ is obtained through the division of both sides by 5. ×
   Dividing both sides by 5, we get the value $x = 3$. ✓

8. **Explain each new symbol.** In writing a proof, you must explain the meaning of every new symbol you introduce. Failure to do this can lead to ambiguity, misunderstanding and mistakes. For example, consider the following two possibilities for a sentence in a proof, where a and b have been introduced on a previous line.

   Since $a \mid b$, it follows that $b = ac$. ×
   Since $a \mid b$, it follows that $b = ac$ for some integer c. ✓

   If you use the first form, then a reader who has been carefully following your proof may momentarily scan backwards looking for where the c entered into the picture, not realizing at first that it came from the definition of divides.

9. **Watch out for "it."** The pronoun "it" can cause confusion when it is unclear what it refers to. If there is any possibility of confusion, you should avoid the word "it." Here is an example:

Since $X \subseteq Y$, and $0 < |X|$, we see that it is not empty. ×

Is "it" X or Y? Either one would make sense, but which do we mean?

Since $X \subseteq Y$, and $0 < |X|$, we see that Y is not empty. ✓

10. **Since, because, as, for, so.** In proofs, it is common to use these words as conjunctions joining two statements, and meaning that one statement is true and as a consequence the other true. The following statements all mean that P is true (or assumed to be true) and as a consequence Q is true also.

Q since P	Q because P	Q, as P	Q, for P	P, so Q
Since P, Q	Because P, Q	as P, Q		

Notice that the meaning of these constructions is different from that of *"If P, then Q,"* for they are asserting not only that P implies Q, but **also** that P is true. Exercise care in using them. It must be the case that P and Q are both statements **and** that Q really does follow from P.

$x \in \mathbb{N}$, so $\mathbb{Z}$ ×

$x \in \mathbb{N}$, so $x \in \mathbb{Z}$ ✓

11. **Thus, hence, therefore consequently.** These adverbs precede a statement that follows logically from previous sentences or clauses. Be sure that a statement follows them.

Therefore $2k + 1$. ×

Therefore $a = 2k + 1$. ✓

12. **Clarity is the gold standard of mathematical writing.** If you believe breaking a rule makes your writing clearer, then break the rule.

Your mathematical writing will evolve with practice useage. One of the best ways to develop a good mathematical writing style is to read other people's proofs. Adopt what works and avoid what doesn't.

Chapter 5: 2, 6, 8, 12; 14, 16, 18, 22, 27.

6. Proof by Contradiction

The basic idea is to assume that the statement we want to prove is false, and then show that this assumption leads to a nonsense, which is called a contradiction.

Outline for Proof by Contradiction

Proposition. Statement.

Proof. $\sim$ (Statement)

Therefore, a nonsense (a contradiction, some statement of the form $(C \wedge \sim C)$. $\square$

P	C	$\sim P$	$C \wedge \sim C$	$(\sim P) \Rightarrow (C \wedge \sim C)$
T	*T*	*F*	*F*	**T**
T	*F*	*F*	*F*	**T**
F	*T*	*T*	*F*	**F**
F	*F*	*T*	*F*	**F**

Proposition 6.1. *If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.*

Proof. Suppose the above proposition is false, so that is there are $a, b \in \mathbb{Z}$ such that $a^2 - 4b = 2$. We have that $a^2 = 2 + 4b = 2(a + 2b)$, and so a^2 is even. We already had in Homeworks if a^2 is even, then a is even. Let $a = 2c$ for some $c \in \mathbb{Z}$. Then,

$$a^2 - 4b = (2c)^2 - 4b = 4c^2 - 4b = 4(c^2 - b).$$

We can now see that if $a^2 - 4b = 2$, then $2(c^2 - b) = 1$. As a conclusion 1 is even, which is a contradiction. $\square$

Definition. *A real number x is* **rational** *if $x = a/b$ for some $a, b \in \mathbb{Z}$. Also, x is* **irrational** *if it is not rational, that is if $x \neq \frac{a}{b}$ for every $a, b \in \mathbb{Z}$.*

Proposition 6.2. *The number $\sqrt{2}$ is irrational.*

Proof. Suppose for the sake of contradiction $\sqrt{2}$ is rational. Then there are integers a and b such that $\sqrt{2} = a/b$. Let this fraction be fully reduced, i.e., $(a, b) = 1$. Then $2 = a^2/b^2$. Therefore, $2b^2 = a^2$, and so a^2 is even. It follows from Homeworks that a is even. Let $a = 2c$ for some $c \in \mathbb{Z}$. Then $2b^2 = 4c^2$, and so $b^2 = 2c^2$, which means b is even. This is a contradiction because 2 divides both a and b, but $(a, b) = 1$. $\square$

Remark. *In the above proof we can also use "In the contrary," or "Suppose on the contrary that" instead of "Suppose for the sake of contradiction".*

Proposition 6.3. *There are infinitely many primes.*

Proof. Suppose on the contrary that there are finitely many primes $p_1, p_2, \dots, p_n$. Then

$$p_1 p_2 \cdots p_n + 1$$

is not a prime so some p_i must divide $p_1 p_2 \cdots p_n + 1$. Without loss of generality assume that $p_1 | p_1 p_2 \cdots p_n + 1$. So there is an integer k such that $p_1 k = p_1 p_2 \cdots p_n + 1$, and so $p_1 k + p_1 p_2 \cdots p_n = 1$. It follows that

$$p_1(k + p_2 \cdots p_n) = 1.$$

Therefore, p_1 divides 1 which is a contradiction. □

Proposition 6.4. *For every real number $x \in [0, \pi/2]$, $Sinx + Cosx \geq 1$.*

Proof. Suppose on the contrary that there is a real integer $x \in [0, \pi/2]$ such that $Sinx + Cosx < 1$. Since both $Sinx$ and $Cosx$ are nonnegative for $x \in [0, \pi/2]$, we have $(Sinx + Cosx)^2 < 1$, and so

$$Sin^2 x + Cos^2 x + 2SinxCosx < 1.$$

As $Sin^2 x + Cos^2 x = 1$, this becomes $1 + 2SinxCosx < 1$, which means $2SinxCosx < 0$, a contradiction. □

6.1. **Proving Conditional Statements by Contradiction.** To prove a conditional statement $P \Rightarrow Q$ by the method of contradiction, we suppose $\sim (P \Rightarrow Q)$, which the same as $P \wedge \sim Q$. Then we reasoning until we arrive to a nonsense (a contradiction).

Outline for proving a conditional statement with contradiction

Proposition 6.5. *If $P \Rightarrow Q$.*

Proof. Suppose P and $\sim Q$.

Therefore, a contradiction ($C \wedge \sim C$). □

Proposition 6.6. *Suppose $a \in \mathbb{Z}$, if a^2 is even, then a is even.*

Proof. Suppose on the contrary that a is odd and a^2 is even. Then $a = 2k$ for some $k \in \mathbb{Z}$. Thus $a^2 = (2k)^2 = 2(2k^2)$ is even, a contradiction since by assumption a^2 is odd. □

Proposition 6.7. *If $a, b \in \mathbb{Z}$ and $a \geq 2$, then $a \nmid b$ or $a \nmid (b + 1)$.*

Proof. Suppose on the contradiction that $a|b$ and $a|(b + 1)$ and $a \geq 2$. Then $ax = b$ and $ay = b + 1$ for some $x, y \in \mathbb{Z}$. Thus $ax = b = ay - 1$. Therefore, $ay - ax = 1$, and so $a(y - x) = 1$, which means $a|1$, a contradiction since $a \geq 2$ and the only divisors of 1 are 1 and -1. □

6.2. **Combining Techniques.** Often, especially in more complex proofs, several proof techniques are combined within a single proof. Consider the following example.

Proposition 6.8. *If r is a nonzero rational number, then r is a product of two irrational numbers. (This statement also can be stated as the following: Every nonzero rational number can be expressed as a product of two irrational numbers).*

Proof. Suppose r is a nonzero rational number. Then we can write

$$r = \sqrt{2}\frac{r}{\sqrt{2}}.$$

As $\sqrt{2}$ is irrational, if we show that $r/\sqrt{2}$ is irrational, then we have shown that r is a product of two irrational number.

To show this, suppose on the contrary that $r/\sqrt{2}$ is rational. Then there are integers a and b with $b \neq 0$ such that $r/\sqrt{2} = a/b$. Thus $\sqrt{2} = r\frac{b}{a}$. Since r is rational, there are integers x, y with $y \neq 0$ such that $r = x/y$. Therefore,

$$\sqrt{2} = \frac{xb}{ya},$$

which means $\sqrt{2}$ is rational, a contradiction. □

Practice Questions:

- For every $n \in \mathbb{Z}$, $4 \nmid (n^2 + 2)$.
- Suppose $a, b \in \mathbb{Z}$. If $4|(a^2 + b^2)$, then a and b are not both odd.

7. If and only if (in the text book, this section is 7.1)

Some propositions have the form

$$P \text{ if and only if } Q.$$

To prove such a statement we must show that both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true.

Outline for If-and-Only-If Proof

Proposition 7.1. *P if and only if Q.*

Prove $P \Rightarrow Q$, you can use any of the methods, direct, contrapositive, or contradiction. (Go to the next line and start your sentence with "Conversely,")

Conversely, [Now prove $Q \Rightarrow P$, you can use any of the methods, direct, contrapositive, or contradiction.] □

Proposition 7.2. *The integer n is odd if and only if n^2 is odd.*

Proof. First we show that if n is odd, then n^2 is odd. Since n is odd, we have $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore $n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$, and it follows that n^2 is odd.

Conversely, suppose n^2 is odd, and we want to show that n is odd. We proceed the proof by contrapositive. Suppose n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. Therefore, $n^2 = (2k)^2 = 2(2k^2)$, and so n^2 is even. □

Proposition 7.3. *Suppose a and b are integers. Then $a \equiv b(mod6)$ if and only if $a \equiv b(mod2)$ and $a \equiv b(mod3)$.*

Proof. First we prove that if $a \equiv b(mod6)$, then $a \equiv b(mod2)$ and $a \equiv b(mod3)$. Since $a \equiv b(mod6)$, we have $6|(a-b)$, and so there is an integer k such that $6k = a - b$. Consider that $6 = 2.3$, and it follows that $2.3.k = (a-b)$. Therefore, both 2 and 3 divide $a-b$. Thus $2|(a-b)$ and $3|(a-b)$ which means $a \equiv b(mod2)$ and $a \equiv b(mod3)$.

Conversely, suppose $a \equiv b(mod2)$ and $a \equiv b(mod3)$. Then $2|(a-b)$ and $3|(a-b)$. Since $2|(a-b)$, there is an integer k such that $a - b = 2k$, and so $a - b$ is even. Also because $3|(a-b)$, there is an integer l such that $a - b = 3l$. Consider that $a - b$ is even, therefore, l must be even. Thus, $l = 2s$ for some $s \in \mathbb{Z}$, and we have $a - b = 3.2.s = 6s$, which implies that $6|(a-b)$. □

8. Disproof (Section 9 in the textbook)

In this section we want to find a process to show some statements are false. The process of carrying out this procedure is called **disproof**.

In mathematics we have three categories of statements:
First Category: The statements that already have been proved and they usually called "theorems", "propositions" and "lemmas".
Second Category: This category contains some statements that are known to be false.
Third Category: It consists of statements whose truth or falsity has not been determined. Examples include things like "Every even integer greater than 2 is the sum of two primes." (The latter statement is called the **Goldbach conjecture**.) Mathematicians have a special name for the statements in this category that they suspect (but haven't yet proved) are true. Such statements are called **conjectures**.

To **disprove** a statement P you must prove $\sim P$.

How to Disprove P : Prove $\sim P$.

8.1. **Disproving Universal Statements: Counterexamples.** To disprove a universally quantified statement such as

$$\forall x \in S, P(x)$$

we must prove its negation. Its negation is

$$\sim (\forall x \in S, P(x)) = \exists x, \sim P(x).$$

How to Disprove $\forall x \in S, P(x)$:

Produce an example of an $x \in S$ that makes $P(x)$ false.

Example 8.1. *For every positive real numbers x and y, $x^2 + y^2 > x + y$.*

Disproof. We can write the above statement in the symbols as follows.

$$\forall x, y > 0, x^2 + y^2 > x + y$$

and so

$$\sim (\forall x, y > 0, x^2 + y^2 > x + y) = \exists x, y > 0, x^2 + y^2 \leq x + y.$$

This is true since for $x = 0.5$ and $y = 0.5$, then $x^2 + y^2 = 0.5$ but $x + y = 1$. □

To disprove a statement $P(x) \Rightarrow Q(x)$, we must prove

$$\sim (P(x) \Rightarrow Q(x) = P(x) \wedge \sim Q(x)$$

so we should find an x such that $P(x)$ is true and $Q(x)$ is false.

How to Disprove $P(x) \Rightarrow Q$:

Produce an example of an x that makes $P(x)$ true and $Q(x)$ is false.

Definition. *There is a special name for an example that disproves a statement: It is called a* **counterexample.**

Example 8.2. *Either prove or disprove the following conjecture.*

Conjecture: *For every $n \in \mathbb{Z}$, the integer $f(n) = n^2 - n + 11$ is prime.*

n	−3	−2	−1	0	1	2	3	4	5	6	7	8	9	10
$f(n)$	23	17	13	11	11	13	17	23	31	41	53	67	83	101

However, consider when $n = 11$, then $f(11) = 11^2$ which is not a prime number.

Disproof. The statement "For every $n \in \mathbb{Z}$, the integer $f(n) = n^2 - n + 11$ is prime," is false. For a counterexample, note that for $n = 11$, the integer $f(11) = 121 = 11 \cdot 11$ is not prime.

Example 8.3. *Either prove or disprove the following conjecture.*

Conjecture: *If A, B and C are sets, then $A - (B \cap C) = (A - B) \cap (A - C)$.*

Disproof. Let $A = \{1, 2, 3\}, B = \{1, 2, 4\}$, and $C = \{3, 4, 5\}$. Then

$A - (B \cap C) = \{1, 2, 3\} - \{4\} \neq (\{1, 2, 3\} - \{1, 2, 4\}) \cap (\{1, 2, 3\} - \{3, 4, 5\}) = \{4\} \cap \{1, 2\} = \emptyset.$

8.2. **Disproving Existence Statements.** To disprove an existence statement such as

$$\exists x \in S, P(x)$$

we must prove its negation. Its negation is

$$\sim (\exists x \in S, P(x)) = \forall x, \sim P(x).$$

How to Disprove $\exists x \in S, P(x)$:
We should show that for all x, the statement $P(x)$ is false.

Example 8.4. *Either prove or disprove the following conjecture.*

Conjecture. *There exists an even integer n such that n^2 is odd.*

Disproof. Let E be the set of even integers and O the set of odd integers. Then the above statement is the same as the following.

$$\exists n \in E, n^2 \in O$$

Example 8.5. *Either prove or disprove the following conjecture.*

Conjecture. *There exist three integers x, y, z, all greater than 1 and no two equal, for which $x^y = y^z$.*

Proof. Note that if $x = 2$, $y = 16$ and $z = 4$, then $2^{16} = (2^4)^4 = (16)^4 = y^z$. □

8.3. **Disproof by Contradiction.** Sometimes to show that a statement P is false, i.e., $\sim P$ is true we use contradiction. To prove by contradiction that $\sim P$ is true, we can assume that $\sim\sim P = P$ is true and we deduce a contradiction.

How to Disprove P **by contradiction:**
Assume P is true, and deduce a contradiction.

Example 8.6. *Either prove or disprove the following conjecture.*

Conjecture: *There is a real number x for which $x^4 < x < x^2$.*

Disproof. Note that the above conjecture can be stated in symbol form as follows,

$$\exists x \in \mathbb{R}, x^4 < x < x^2.$$

The above statement also is same as

$$\exists x \in \mathbb{R}, (x^4 < x) \wedge (x < x^2).$$

We use the contradiction method to show the above is false. So we suppose that there is an integer x such that $(x^4 < x)$ and $(x < x^2)$. Since $x > x^4$ and x^4 is always

nonnegative, we must have x is positive. Then by dividing both side of inequalities by x we can have

$$(x^3 < 1) \text{ and } (1 < x),$$

and it follows

$$x^3 - 1 < 0 \text{ and } x - 1 > 0.$$

Consider that $x^3 - 1 = (x-1)(x^2 + x + 1)$. Therefore, $(x-1)(x^2 + x + 1) < 0$ and $x - 1 > 0$, which implies

$$x^2 + x + 1 < 0$$

which is a contradiction since $x^2 + x + 1$ is always positive as x is positive.

Practice in Class: Write each of the following statement in symbols, and then find their negations, and in the end proof or disproof them.

(1) Suppose $a, b \in \mathbb{Z}$, if $a|b$ and $b|a$, then $a = b$.
(2) There are integers a and b such that $42a + 7b = 1$.

Chapter 9: 2, 6, 10, 18, 24, 30.

9. Mathematical Induction (Chapter 10 of the textbook)

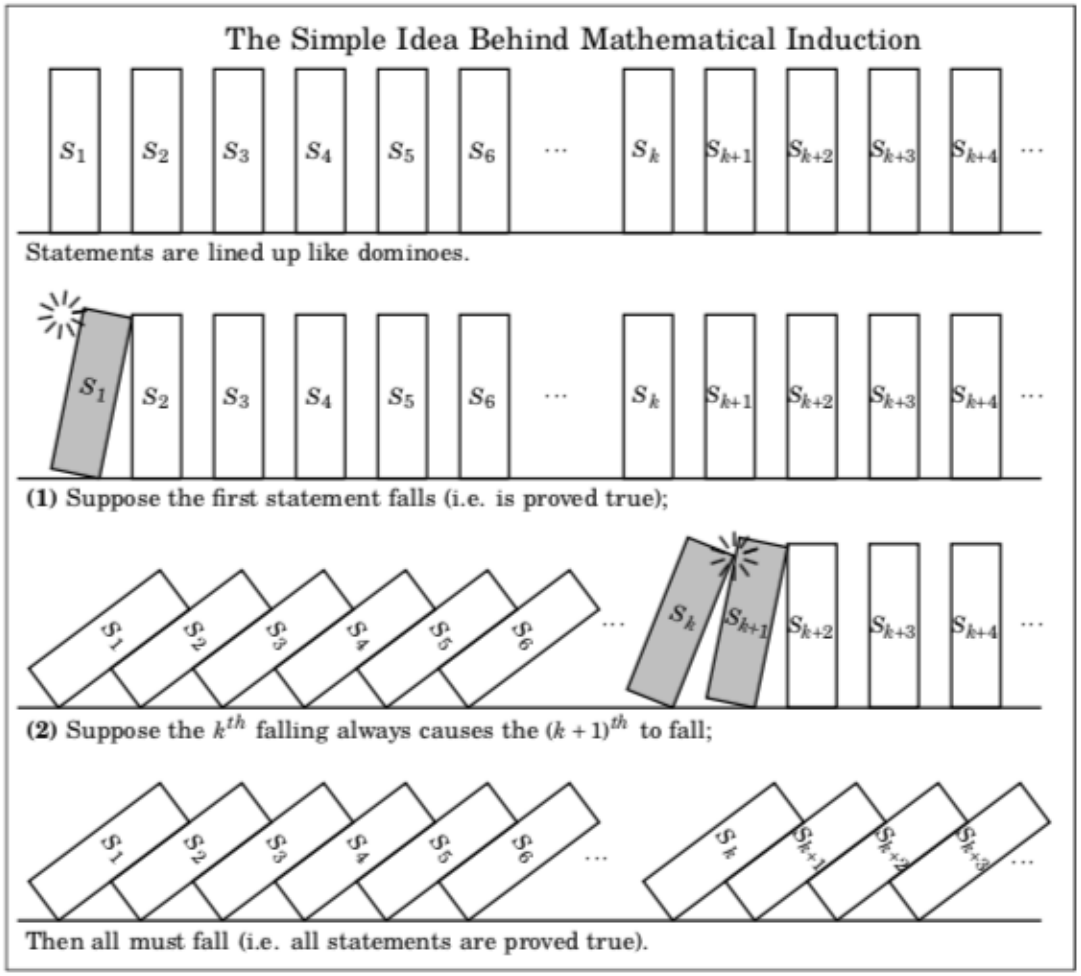
9.1. **Mathematical Induction. Conjecture.** The sum of the first n odd natural numbers equals n^2.

Lets check it for several odd numbers.

n	sum of the first n odd natural numbers	n^2
1	$1 = \ldots\ldots$	1
2	$1+3 = \ldots\ldots$	4
3	$1+3+5 = \ldots\ldots$	9
4	$1+3+5+7 = \ldots\ldots$	16
5	$1+3+5+7+9 = \ldots\ldots$	25
$\vdots$	$\vdots$	$\vdots$
n	$1+3+5+7+9+11+\cdots+(2n-1) = \ldots\ldots$	n^2
$\vdots$	$\vdots$	$\vdots$

Let's rephrase this as follows. For each natural number n (i.e., for each line of the table), we have a statement $S(n)$, as follows:
$S(1) : 1 = 1^2$
$S(2) : 1 + 3 = 4 = 2^2$
$S(3) : 1 + 3 + 5 = 9 = 3^2$
$\vdots$
$S(n) : 1 + 3 + ... + (2n - 1) = n^2$
$\vdots$

Our conjecture actually can be rephrased as the following.
Conjecture. All statements $S(1), S(2), \ldots, S(n), \ldots$ are true.



This picture gives our outline for proof by mathematical induction.

Outline for Proof by Induction

Proposition. The statements $S(1), S(2), S(3), S(4), ...$ are all true.

Proof. (Induction) Firstly, prove that the first statement $S(1)$ is true.
Secondly, given any integer $k \geq 1$, prove that the statement $S(k) \Rightarrow S(k+1)$ is true.
It follows by mathematical induction that every $S(n)$ is true for all $n \geq 1$. □

Definition. *In this setup, the first step (1) is called the* **basis step**.
The second step is called the **inductive step**.
In the inductive step direct proof is most often used to prove $S(k) \Rightarrow S(k+1)$, so this step is usually carried out by assuming $S(k)$ is true and showing this forces $S(k+1)$ to be true. The assumption that $S(k)$ is true is called the **inductive hypothesis**.

Proposition 9.1. *If $n \in \mathbb{N}$, then $1 + 3 + 5 + 7 + ... + (2n-1) = n^2$.*

Proof. We will prove this with mathematical induction.
(1) Observe that if $n = 1$, this statement is $1 = 1^2$, which is obviously true.
(2) We must now prove $S(k) \Rightarrow S(k+1)$ for any $k \geq 1$. That is, we must show that if $1+3+5+7+...+(2k-1) = k^2$, then $1+3+5+7+\cdots+(2(k+1)-1) = (k+1)^2$.

Suppose $1 + 3 + 5 + 7 + ... + (2k - 1) = k^2$. Then

$$1 + 3 + 5 + 7 + \cdots + (2(k + 1) - 1) =$$

$$1 + 3 + 5 + 7 + ... + (2k - 1) + (2(k + 1) - 1) =$$

$$k^2 + (2(k + 1) - 1) = k^2 + 2k + 1 = (k + 1)^2.$$

This proves that $S(k) \Rightarrow S(k + 1)$.

It follows by induction that $1+3+5+7+...+(2n-1) = n^2$ for every $n \in \mathbb{N}$. □

Proposition 9.2. *If n is a non-negative integer, then $5|(n^5 - n)$.*

Proof. We will prove this with mathematical induction.

If $n = 0$, then this statement is $5|(0^5 - 0)$ which is obviously true.

Let $k \geq 0$. We want to show that if $5|(k^5 - k)$, then $5|((k + 1)^5 - (k + 1))$.

Observe that

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

$$(k^5 - k) + 5k^4 + 10k^3 + 10k^2 + 5k$$

By induction hypothesis there is an a such that $k^5 - k = 5a$. Now we can see that

$$((k + 1)^5 - (k + 1)) = 5(a + k^4 + 2k^3 + 2k^2 + k)$$

. Therefore, $5|((k + 1)^5 - (k + 1))$.

Thus we have shown that $5|(k^5 - k)$ implies that $5|((k + 1)^5 - (k + 1))$.

It follows by induction that $5|(n^5 - n)$ for all non-negative integers n. □

Proposition 9.3. *If $n \in \mathbb{Z}$ and $n \geq 0$, then $\sum_{i=0}^{n} i.i! = (n + 1)! - 1$.*

Proof. We will prove this statement by mathematical induction.

When $n = 0$, the above statement is $\sum_{i=0}^{0} i.i! = (0 + 1)! - 1 = 0$, which is a true statement.

Let $k \geq 0$. We now want to show that if $\sum_{i=0}^{k} i.i! = (k+1)! - 1$, then $\sum_{i=0}^{k+1} i.i! = ((k + 1) + 1)! - 1$.

Consider that

$$\sum_{i=0}^{k+1} i.i! = \sum_{i=0}^{k} i.i! + (k + 1).(k + 1)!.$$

By induction hypothesis we have $\sum_{i=0}^{k} i.i! = (k + 1)! - 1$, and by substituting in the above expression we have

$$\sum_{i=0}^{k+1} i.i! = (k + 1)! - 1 + (k + 1).(k + 1)! =$$

$$(k + 1)!((k + 1) + 1) - 1 = (k + 2)! - 1.$$

Therefore, $\sum_{i=0}^{k+1} i.i! = (k + 2)! - 1$.

It follows by induction that $\sum_{i=0}^{n} i.i! = (n+1)! - 1$ for every integer $n \geq 0$.

Practice:

(1) Questions 3,4 in chapter 10, and also questions 19, 22 in the same chapter.

□

Proposition 9.4. *For each $n \in \mathbb{N}$, it follows that $2^n \leq 2^{n+1} - 2^{n-1} - 1$.*

Proof. We proceed this proof by mathematical induction. First consider that when $n = 1$, the above statement is $2^1 \leq 2^{1+1} - 2^{1-1} - 1$, which simplifies to $2 \leq 4 - 1 - 1$ that is true.

Suppose $k \geq 1$. We need to show that if $2^k \leq 2^{k+1} - 2^{k-1} - 1$, then $2^{k+1} \leq 2^{(k+1)+1} - 2^{(k+1)-1} - 1$.

Consider that by induction hypothesis

$$2^k \leq 2^{k+1} - 2^{k-1} - 1$$

and so by multiplying both side by 2 we have

$$2^{k+1} = 2.2^k \leq 2.2^{k+1} - 2.2^{k-1} - 2.1 =$$

$$2^{k+2} - 2^k - 2 \leq (2^{k+2} - 2^k - 2) + 1 = 2^{k+2} - 2^k - 1.$$

Therefore we showed that if $2^k \leq 2^{k+1} - 2^{k-1} - 1$, then $2^{k+1} \leq 2^{(k+1)+1} - 2^{(k+1)-1} - 1$.

It follows by induction that $2^n \leq 2^{n+1} - 2^{n-1} - 1$ for every $n \geq 1$.

□

Proposition 9.5. *If $n \in \mathbb{N}$, then $(1+x)^n \geq 1 + nx$ for all $x \in \mathbb{R}$ with $x > -1$.*

Proof. When $n = 1$, this statement will be $(1+x)^1 \leq 1+x$ which is a true statement.

Let $k \geq 1$ and $x > -1$. We want to show that if $(1+x)^k \geq 1 + kx$, then $(1+x)^{k+1} \geq 1 + (k+1)x$.

By induction hypothesis we have

$$(1+x)^k \geq 1 + kx(\text{ multiplying both side by (1+x)})$$

$$(1+x)^k(1+x) \geq (1+kx)(1+x) = 1 + kx + x + kx^2 = 1 + (k+1)x + kx^2.$$

Since $k \geq 1$ and $x > -1$, we have that $kx^2 > 0$. Therefore, $1 + (k+1)x + kx^2 \geq 1 + (k+1)x$. So we have

$$(1+x)^k(1+x) \geq 1 + (k+1)x + kx^2 \geq 1 + (k+1)x.$$

Therefore we showed that $(1+x)^{k+1} \geq 1 + (k+1)x$.

It follows from mathematical induction for every $n \in \mathbb{N}$, we have $(1+x)^n \geq 1+nx$ for all $x \in \mathbb{R}$ with $x > -1$. □

Practice:

(1) For every $n \in \mathbb{N}$, we have

$$\sum_{i=1}^{n} 1/i^2 \leq 2 - 1/n.$$

(2) For every $n \in \mathbb{N}$, we have

$$\prod_{i=1}^{n}(1-1/2^i) \geq 1/4 + 1/2^{n+1}.$$

Proposition 9.6. *If $a, b \in \mathbb{N}$, then there exist integers k and l for which $gcd(a, b) = ak + bl$.*

Example 9.7. *$gcd(12, 16) = 4 = 16 - 12$.*

Proposition 9.8. *Suppose $a_1, a_2, \dots, a_n$ are n integers, where $n \geq 2$. If p is prime and $p|(a_1 \cdot a_2 \cdot a_3 \dots a_n)$, then $p|a_i$ for at least one of the a_i.*

Proof. First we showed show that if $p|a_1a_2$, then $p|a_1$ or $p|a_2$. Suppose that $p|a_1a_2$, then if $p|a_1$ we are done. So we may assume that $p \nmid a_1$. Then $gcd(p, a_1) = 1$, and by above proposition, there are integers l, k such that $1 = kp + la_1$. By multiplying both sides of the inequality by a_2, we have

$$a_2 = ka_2p + la_1a_2.$$

Note that $p|a_1a_2$, and so there is $s \in \mathbb{Z}$ such that $a_1a_2 = ps$. By substitution in the above expression we have

$$a_2 = pka_2 + ps = p(ka_2 + s),$$

which implies that $p|a_2$.

Therefore, we showed that if $p|a_1a_2$, then $p|a_1$ or $p|a_2$.

Suppose $k \geq 2$ and if $p|(a_1 \cdot a_2 \cdot a_3 \dots a_k)$, then $p|a_i$ for at least one of the a_i. Let $a_1a_2 \dots a_k = b$. Then if $p|(a_1a_2 \dots a_k)a_{k+1}$, it is the same as $p|ba_{k+1}$, then by what we proved in the basis step, we have $p|a_{k+1}$ or $p|b$. If $p|a_{k+1}$ we are done, otherwise $p|b$, it is the same as $p|a_1a_2 \dots a_k$. Therefore by induction hypothesis $p|a_i$ for at least one of the a_i. □

Chapter 10: 2, 6, 8, 12, 16, 20.

9.2. **Proof by Strong Induction.**

Outline for Proof by Strong Induction

Proposition. The statements $S(1), S(2), S(3), S(4), ...$ are all true.

Proof. (Strong Induction) Firstly, prove that the first statement $S(1)$ (or the first several $S(n)$) is true.
Secondly, given any integer $k \geq 1$, prove that the statements $(S(1) \wedge S(2) \wedge ... \wedge S(k)) \Rightarrow S(k+1)$ is true.
It follows by strong induction that every $S(n)$ is true for all $n \geq 1$. □

Proposition 9.9. *Assume that we have a sequence of the following form,* $a_1 = 1$, $a_2 = 3$, *and for every* $n \geq 2$, $a_n = a_{n-2} + 2a_{n-1}$. *Show that for every* n, a_n *is odd.*

Proof. When $n = 1$, $a_1 = 1$ and when $n = 2$, $a_2 = 3$. Therefore, a_1 and a_2 are odd.

We now want to show that if a_k is odd for $1 \leq m \leq k$ and $k \geq 2$ is true, then a_{k+1} is odd. Consider that

$$a_{k+1} = a_{(k+1)-2} + 2a_{(k+1)-1} = a_{k-1} + 2a_k.$$

By induction hypothesis we have a_{k-1} is odd and moreover $2a_k$ is even, therefore, a_{k+1} is a sum of an even number and an odd number which results an odd number. Therefore, a_{k+1} is an odd number. □

Proposition 9.10. *Suppose* $b_1, b_2, b_3, ...$ *is a sequence defined by* $b_1 = 4$, $b_2 = 12$, $b_n = b_{n-2} + b_{n-1}$ *for all integers* $n \geq 3$. *Prove that for every* $n \in \mathbb{N}$, $4|b_n$.

Proof. When $n = 1$, then $4|b_1$ is true, and also when $n = 2$, $4|b_2$ is also true.

Now we want to show that if $4|b_m$ for $1 \leq m \leq k$ and $k \geq 2$, then $4|b_{k+1}$. Consider that

$$b_{k+1} = b_{(k+1)-2} + b_{(k+1)-1} = b_{k-1} + b_k.$$

By induction hypothesis we have $4|b_{k-1}$ and $4|b_k$, therefore, there are integers a and c such that $4a = b_{k-1}$ and $4c = b_k$. Thus,

$$b_{k+1} = b_{k-1} + b_k = 4a + 4b = 4(a + b).$$

So $4|b_{k+1}$.

It follows from strong mathematical induction that $4|b_n$ for every $n \geq 1$. □

Proposition 9.11. *If* $n \in \mathbb{N}$, *then* $12|(n^4 - n^2)$.

Proof. We will prove this statement by strong mathematical induction.
If $n = 1$, then 12 divides $n^4 - n^2 = 1^4 - 1^2 = 0$.
If $n = 2$, then 12 divides $n^4 - n^2 = 2^4 - 2^2 = 12$.
If $n = 3$, then 12 divides $n^4 - n^2 = 3^4 - 3^2 = 72$.
If $n = 4$, then 12 divides $n^4 - n^2 = 4^4 - 4^2 = 240$.
If $n = 5$, then 12 divides $n^4 - n^2 = 5^4 - 5^2 = 600$.
If $n = 6$, then 12 divides $n^4 - n^2 = 6^4 - 6^2 = 1260$.

Let $k \geq 6$ and assume $12|m^4 - m^2$ for $1 \leq m \leq k$. We must show that $12|(k+1)^4 - (k+1)$. Since S_{k-5} is true, we have $12|(k-5)^4 - (k-5)^2$. Let $m = k-5$. Then by induction hypothesis we have $12|m^4 - m^2$, meaning that there is an integer a such that $m^4 - m^2 = 12a$. Consider that

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

$$m^4 + 24m^3 + 216m^2 + 864m + 1296 - (m^2 + 12m + 36) =$$

$$(m^4 - m^2) + 24m^3 + 216m^2 + 864m + 1296 - 12m - 36 =$$

$12a + 24m^3 + 216m^2 + 864m + 1296 - 12m - 36 = 12(a + 2m^3 + 18m^2 + 71m + 105)$.

Therefore, by strong mathematical induction we showed that $12|n^4 - n^2$ for every $n \in \mathbb{N}$.

□

Practice: For every $n \in \mathbb{N}$, $6|n^3 - n$.

Definition. *A* **Graph** *is a set of points called vertices and a set of lines between the vertices called* **edges**.

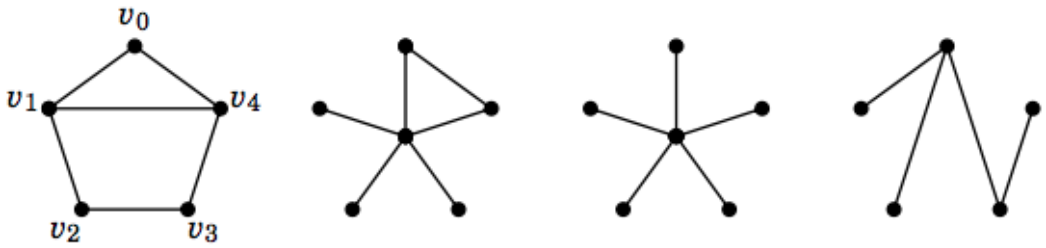


Figure 10.1. Examples of Graphs

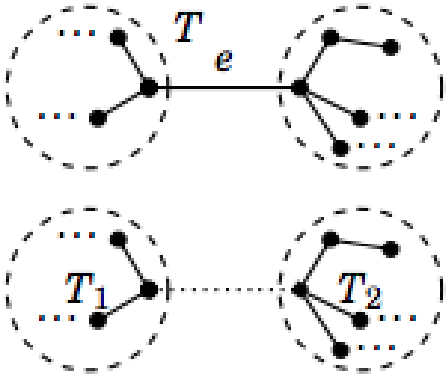
A **cycle** *in a graph is a sequence of distinct edges in the graph that form a route that ends where it began. For example, the graph on the far left of Figure 10.1 has a cycle that starts at vertex v_1, then goes to v_2, then to v_3, then v_4 and finally back to its starting point v_1.*

There is a special name for a graph that has no cycles; it is called a **tree**.

Proposition 9.12. *If a tree has n vertices, then it has $n-1$ edges.*

Proof. We proceed the proof by strong mathematical induction on the number of vertices of the tree. Let n be the number of vertices. If $n = 1$, then the number of edges is $n - 1 = 1 - 1 = 0$ which is true. When $n = 2$, then we have only one edge and so the above statement is true.

Now assume that for ant tree with m vertices $1 \leq m \leq k$, the number of edges is $m - 1$. Now we want to show that if a tree has $k + 1$ vertices it has k edges. Let T be a tree with $k + 1$ vertices. Choose an edge of T and call it e.



Now remove the edge e from T, but leave the two endpoints of e. This leaves two smaller trees T_1 and T_2. Let's say T_1 has x edges and T_2 has y edges. Since the number of vertices of T_1 and T_2 is less than or equal to k, by induction hypothesis the number of edges of T_1 is $x-1$ and the number of edges of T_2 is $y-1$. Consider that the number of vertices of T is $x+y$ and the number of edges of T is equal to the number of edges of T_1 plus the number of edges of T_2 plus it has the additional edge e that belongs to neither T_1 nor T_2. Therefore, the number of edges of T is $x+y-1$ which is the same k.

Therefore, by mathematical induction the number of edges of a graph with n vertices is $n-1$.

□

10. Relation (Chapter 11 of the textbook)

Definition. *A* **relation** *on a set A is a subset $R \subseteq A \times A$. We often abbreviate the statement $(x, y) \in R$ as xRy. The statement $(x, y) \notin R$ is abbreviated as $x \not R y$.*

Example 10.1. *Let $A = \{1, 2, 3, 4\}$, and consider the following set:*

$$R = \{(1,1), (2,1), (2,2), (3,3), (3,2), (3,1), (4,4), (4,3), (4,2), (4,1)\} \subseteq A \times A$$

Consider that $3 \not R 4$ but $4R3$.

Example 10.2. *Let $A = \{1, 2, 3, 4\}$ and consider the following set*

$$S = \{(1,1), (1,3), (3,1), (3,3), (2,2), (2,4), (4,2), (4,4) \subseteq A \times A.$$

Consider that $1 \not S 2$ and $2S4$. More precisely the above relation can be translated as aRb if a and b have the same parity.

Example 10.3. *Let $A = \{1, 2, 3, 4\}$. Define xPy if $x < y$, then*

$$P = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}.$$

Example 10.4. *Consider the set $R = \{(x, y) \in Z \times Z : x - y \in \mathbb{N}\} \subseteq \mathbb{Z} \times \mathbb{Z}$. This is the $>$ relation on the set $A = \mathbb{Z}$. It is infinite because there are infinitely many ways to have $x > y$ where x and y are integers.*

Example 10.5. *Brotherhood is a equivalence relation if we assume every one can be his own brother.*

Definition. *Suppose R is a relation on a set A.*

1. *Relation R is* **reflexive** *if xRx for every $x \in A$. That is, R is reflexive if $\forall x \in A$, xRx.*
2. *Relation R is* **symmetric** *if xRy implies yRx for all $x, y \in A$. That is, R is symmetric if $\forall x, y \in A, xRy \Rightarrow yRx$.*
3. *Relation R is* **transitive** *if whenever xRy and yRz, then also xRz. That is, R is transitive if $\forall x, y, z \in A, (xRy) \wedge (yRz) \Rightarrow xRz$.*

Example 10.6. *Here $A = \{a, b, c, d, e\}$ and R is the following relation on A:*

$$R = \{(b,b), (b,c), (c,b), (c,c), (d,d), (b,d), (d,b), (c,d), (d,c)\}.$$

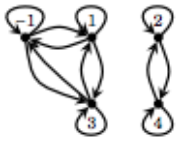
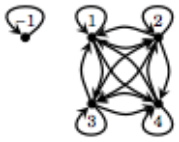
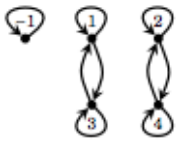
Solution. The above relation is not reflexive but it is symmetric and transitive.

Relations on $\mathbb{Z}$:	$<$	$\leq$	$=$	$\mid$	$\nmid$	$\neq$
Reflexive	no	yes	yes	yes	no	no
Symmetric	no	no	yes	no	no	yes
Transitive	yes	yes	yes	yes	no	no

Definition. *A relation R on a set A is an* **equivalence relation** *if it is reflexive, symmetric and transitive.*

Definition. *Suppose R is an equivalence relation on a set A. Given any element $a \in A$, the* **equivalence class containing** *a is the subset $\{x \in A : xRa\}$ of A consisting of all the elements of A that relate to a. This set is denoted as $[a]$. Thus the equivalence class containing a is the set $[a] = \{x \in A : xRa\}$.*

Example 10.7. *Let $A = \{-1, 1, 2, 3, 4\}$.*

Relation R	Diagram	Equivalence classes (see next page)
"is equal to" (=) $R_1 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4)\}$		$\{-1\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$
"has same parity as" $R_2 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(-1,1),(1,-1),(-1,3),(3,-1),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1,1,3\}$, $\{2,4\}$
"has same sign as" $R_3 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,2),(2,1),(1,3),(3,1),(1,4),(4,1),(3,4),$ $(4,3),(2,3),(3,2),(2,4),(4,2),(1,3),(3,1)\}$		$\{-1\}$, $\{1,2,3,4\}$
"has same parity and sign as" $R_4 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1\}$, $\{1,3\}$, $\{2,4\}$

Theorem 10.8. *Suppose R is an equivalence relation on a set A. Suppose also that $a, b \in A$. Then $[a] = [b]$ if and only if aRb.*

Proof. We first show that if $[a] = [b]$, then aRb. Suppose $[a] = [b]$, then

$$\{x \in A : xRa\} = \{x \in A : xRb\}.$$

Since R is an equivalence relation we have aRa, and so $a \in [a]$ which implies that $a \in [b] = \{x \in A : xRb\}$. Therefore, aRb.

Conversely, let $x \in [a] = \{x \in A : xRa\}$. Therefore, xRa and aRb, as R is a transitive relation, we must have xRb and so $x \in [b]$. Therefore, $[a] \subseteq [b]$. Similarly, we can show that $[b] \subseteq [a]$, and thus $[a] = [b]$. □

Definition. *A* **partition** *of a set A is a set of non-empty subsets of A, such that the union of all the subsets equals A, and the intersection of any two different subsets is $\emptyset$.*

Example 10.9. *Let* $A = \{a, b, c, d, e\}$. *Then*

$$\{\{a, b\}, \{c, d\}, \{e\}\}$$

and also

$$\{\{a, b, c\}, \{d, e\}\}$$

are partitions of A.

Theorem 10.10. *Suppose* R *is an equivalence relation on a set* A. *Then the set* $\{[a] : a \in A\}$ *of equivalence classes of* R *forms a partition of* A.

Proof. To show that $\{[a] : a \in A\}$ is a partition of A, we must that

$$A = \bigcup_{a \in A} [a]$$

and also $[a] \cap [b] = \emptyset$ if $[a] \neq [b]$. It is clear that $A = \bigcup_{a \in A} [a]$. We now want to proof that either $[a] \cap [b] = \emptyset$ or $[a] = [b]$ If $[a] \cap [b] = \emptyset$, we are done, otherwise there is x in both $[a]$ and $[b]$. Therefore, xRa and xRb. As R is an equivalence relation, it is symmetric, so we can say aRx too. Therefore, $aRx \wedge xRb$, which implies that aRb. Thus by previous theorem we have $[a] = [b]$. □

Practice: Let $n \in \mathbb{N}$. The relation $\equiv (mod\ n)$ on the set $\mathbb{Z}$ is reflexive, symmetric and transitive.

11. Functions

Definition. *A* **relation** *from set A to B is a subset of $A \times B$.*

Example 11.1. *Let's start on familiar ground. Consider the function $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$. Its graph is the set of points*

$$R = \{(x, x^2) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}.$$

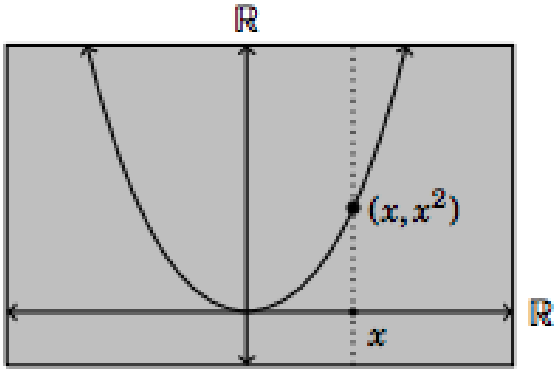


Figure 12.1. A familiar function

Example 11.2. *We also can write the function $f : \mathbb{Z} \to \mathbb{N}$, defined by $f(n) = |n| + 2$, as a relation*

$$\{(n, |n| + 2), n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{N}.$$

Definition. *Suppose A and B are sets. A* **function** *f from A to B (denoted as $f : A \to B$) is a relation $f \subseteq A \times B$ from A to B, satisfying the property that for each $a \in A$ the relation f contains exactly one ordered pair of form (a, b). The statement $(a, b) \in f$ is abbreviated $f(a) = b$.*

Definition. *For a function $f : A \to B$, the set A is called the* **domain** *of f . (Think of the domain as the set of possible "input values" for f .) The set B is called the* **codomain** *of f . The* **range** *of f is the set $\{f(a) : a \in A\} = \{b : (a, b) \in f\}$. (Think of the range as the set of all possible "output values" for f . Think of the codomain as a sort of "target" for the outputs.)*

Example 11.3. *Let $A = \{p, q, r, s\}$ and $B = \{0, 1, 2\}$, and*

$$f = \{(p, 0), (q, 1), (r, 2), (s, 2)\} \subseteq A \times B.$$

This is a function $f : A \to B$ because each element of A occurs exactly once as a first coordinate of an ordered pair in f . We have $f(p) = 0$, $f(q) = 1$, $f(r) = 2$ and $f(s) = 2$. The domain of f is $\{p, q, r, s\}$, and the codomain and range are both $\{0, 1, 2\}$.

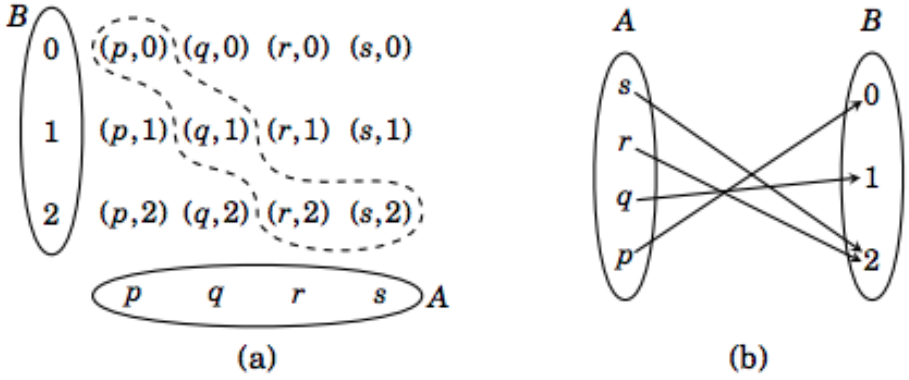


Figure 12.3. Two ways of drawing the function $f = \{(p,0),(q,1),(r,2),(s,2)\}$

Example 11.4. *Say a function $\phi : \mathbb{Z}^2 \to \mathbb{Z}$ is defined as $\phi(m,n) = 6m - 9n$. Note that as a set, this function is*

$$\phi = \{((m,n), 6m - 9n) : (m,n) \in \mathbb{Z}^2 \times \mathbb{Z}\}.$$

What is the range of ϕ?

Solution. We will show the range of ϕ is the set of all multiples of 3,

$$\{3k : k \in \mathbb{Z}\}.$$

Consider that the range of ϕ is the set

$$\{6m - 9n : n, m \in \mathbb{Z}\}.$$

Any element of the form $6m - 9n$ is of the form $3(2m - 3n)$ so it is a multiple of 3, and so

$$\{6m - 9n : n, m \in \mathbb{Z}\} \subseteq \{3k : k \in \mathbb{Z}\}.$$

Moreover, we have

$$3k = 3.1.k = 3(2 \times -1 - 3 \times -1)k = 3(2(-k) - 3(-k)) = 6(-k) - (9(-k)).$$

Therefore, if we choose $m = -k$ and $n = -k$, then $6m - 9n = 3k$. Thus,

$$\{3k : k \in \mathbb{Z}\} \subseteq \{6m - 9n : n, m \in \mathbb{Z}\}.$$

And so the sets are equal which means the range is the same as $\{3k : k \in \mathbb{Z}\}$.

Definition. *Two functions $f : A \to B$ and $g : A \to D$ are equal if $f(x) = g(x)$ for every $x \in A$.*

Notation. Some times a function $f : A \to B$ denotes by

$$\begin{array}{rccc} f: & A & \to & B \\ & a & \mapsto & f(a). \end{array}$$

Example 11.5. *Define*

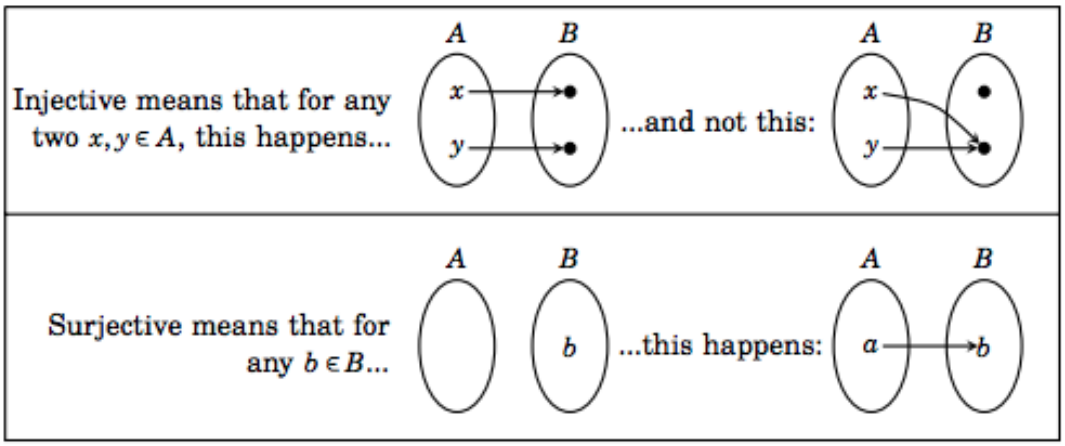
$$\begin{array}{rccc} f: & \{-1,0,1\} & \to & \mathbb{Z} \\ & x & \mapsto & x^2. \end{array} \quad \textit{and} \quad \begin{array}{rccc} g: & \{-1,0,1\} & \to & \mathbb{R} \\ & -1 & \mapsto & 1 \\ & 0 & \mapsto & 0 \\ & 1 & \mapsto & 1 \end{array}$$

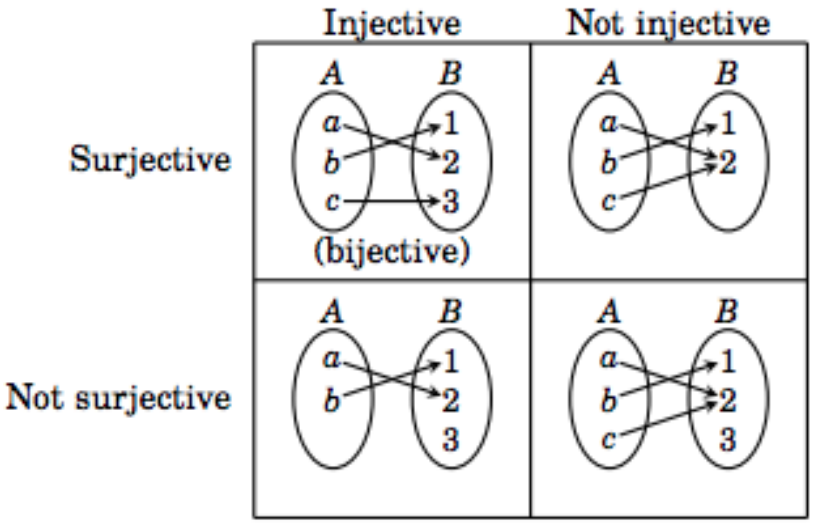
Then $f = g$.

11.1. **Injective and Surjective Functions.**

Definition. *A function $f : A \to B$ is:*

(1) **injective (or one-to-one)** *if for every $x, y \in A$, $x \neq y$ implies $f(x) \neq f(y)$;*
(2) **surjective (or onto)** *if for every $b \in B$ there is an $a \in A$ with $f(a) = b$;*
(3) **bijective** *if f is both injective and surjective.*





How to show a function $f : A \to B$ is injective:

Direct approach:	**Contrapositive approach:**
Suppose $x, y \in A$ and $x \neq y$.	Suppose $x, y \in A$ and $f(x) = f(y)$.
$\vdots$	$\vdots$
Therefore $f(x) \neq f(y)$.	Therefore $x = y$.

How to show a function $f : A \to B$ is surjective:

Suppose $b \in B$.
[Prove there exists $a \in A$ for which $f(a) = b$.]

Example 11.6. *Show that the function $f : \mathbb{R} - \{0\} \to \mathbb{R}$ defined as $f(x) = 1/x + 1$ is injective but not surjective.*

Solution. We will use the contrapositive approach to show that f is injective. Suppose $f(x) = f(y)$, then $1/x + 1 = 1/y + 1$, and so $1/x = 1/y$. Therefore, $x = y$.

Also the function f is not surjective because $1 \in \mathbb{R}$, but we show there is not any element in $\mathbb{R} - \{0\}$ such that $1/x + 1 = 1$. Suppose on the contrary there is $\mathbb{R} - \{0\}$ such that $1/x + 1 = 1$. Then $1/x = 0$ which is a contradiction.

Practice:

(1) Show that the function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by the formula

$$g(m, n) = (m + n, m + 2n),$$

is both injective and surjective.

(2) Consider function $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$ defined as $h(m, n) = \frac{m}{|n|+1}$.

Solution. We first use the method of contradiction to show that g is injective. Let

$$g(m_1, n_1) = g(m_2, n_2).$$

Then

$$(m_1 + n_1, m_1 + 2n_1) = (m_2 + n_2, m_2 + 2n_2),$$

it follows that $\begin{cases} m_1 + n_1 = m_2 + n_2 \\ m_1 + 2n_1 = m_2 + 2n_2 \end{cases}$ and so $\begin{cases} (m_1 - m_2) + (n_1 - n_2) = 0 \\ (m_1 - m_2) + 2(n_1 - n_2) = 0 \end{cases}$

by subtracting the below expression to top one, we have $n_1 = n_2$. Also, we can show that $m_1 = m_2$. Therefore, g is injective.

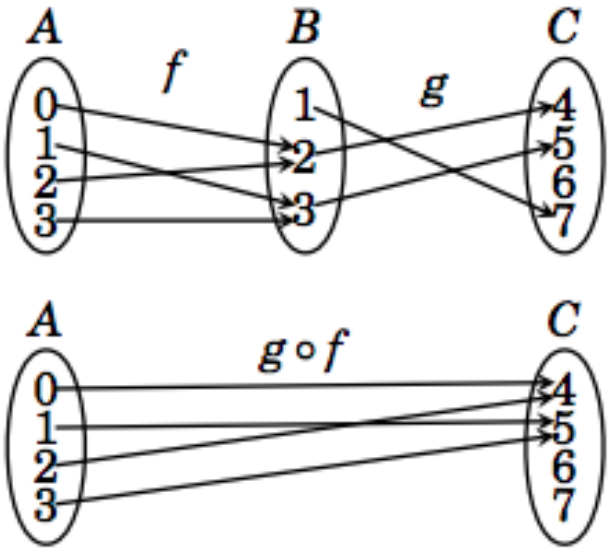
Now show g is surjective.

(2) Note that h is not injective, because $(1, 1) \neq (2, 3)$, but $h(1, 1) = 1/2 = h(2, 3)$. However, this function is surjective. Let x/y be an element in $\mathbb{Q}$. Then if both x and

y are positive $h(x, y-1) = x/y$. And moreover, if x/y is negative, then without loss o generality we may assume that x is negative, and again $h(x, y-1) = x/y$.

11.2. **Composition.**

Definition. *Suppose $f : A \to B$ and $g : B \to C$ are functions with the property that the codomain of f equals the domain of g. The* **composition** *of f with g is another function, denoted as $g \circ f$ and defined as follows: If $x \in A$, then $g \circ f(x) = g(f(x))$. Therefore $g \circ f$ sends elements of A to elements of C, so $g \circ f : A \to C$.*



Example 11.7. *Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = x^2 + x$, and $g : \mathbb{R} \to \mathbb{R}$ be defined as $g(x) = x^3 + 1$. Then $g \circ f : \mathbb{R} \to \mathbb{R}$ is the function defined by the formula $g \circ f(x) = g(f(x)) = g(x^2 + x) = (x2 + x)^3 + 1$.*

Theorem 11.8. *Composition of functions is associative. That is if $f : A \to B$, $g : B \to C$ and $h : C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$.*

Theorem 11.9. *Suppose $f : A \to B$ and $g : B \to C$. If both f and g are injective, then $g \circ f$ is injective. If both f and g are surjective, then $g \circ f$ is surjective.*

Proof. Suppose both f and g are injective. We show by method of contrapositive that $f \circ g$ is injective. Let $f \circ g(x) = f \circ g(y)$. Then $f(g(x)) = f(g(y))$. Because f is injective we have $g(x) = g(y)$, and since g is injective, thus $x = y$.

Now we show that if both f and g are surjective, then $f \circ g$ also is surjective. Let $y \in \mathbb{R}$. Since f is surjective, there is $a \in \mathbb{R}$ such that $f(a) = y$. Consider that g is surjective so there is $x \in \mathbb{R}$ such that $g(x) = a$, therefore,

$$f \circ g(x) = f(g(x)) = f(a) = y.$$

Therefore, $f \circ g$ is surjective when both f and g are surjective. □

11.3. **Inverse Functions.**

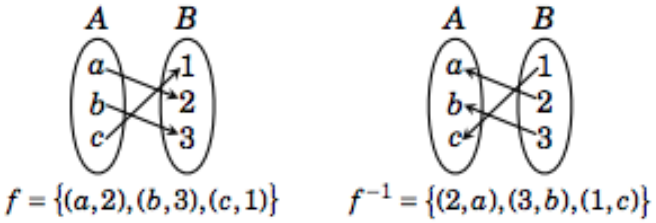
Example 11.10. *Let* $f(x) = x^3$ *and* $g(x) = \sqrt[3]{x}$. *Then*

$$f \circ g(x) = f(\sqrt[3]{x}) = \sqrt[3]{x}^3 = x.$$

Definition. *Given a set* A, *the identity function on* A *is the function* $i_A : A \to A$ *defined as* $i_A(x) = x$ *for every* $x \in A$.

Example 11.11. *If* $A = \{1, 2, 3\}$, *then* $i_A = \{(1, 1), (2, 2), (3, 3)\}$. *Also* $i_{\mathbb{Z}} = \{(n, n) : n \in \mathbb{Z}\}$. *The identity function on a set is the function that sends any element of the set to itself.*

Definition. *Given a relation* R *from* A *to* B, *the inverse relation of* R *is the relation from* B *to* A *defined as* $R^{-1} = \{(y, x) : (x, y) \in R\}$. *In other words, the inverse of* R *is the relation* R^{-1} *obtained by interchanging the elements in every ordered pair in* R.



Definition. *If* $f : A \to B$ *is bijective then its inverse is the function* $f^{-1} : B \to A$. *Functions* f *and* f^{-1} *obey the equations* $f^{-1} \circ f = i_A$ *and* $f \circ f^{-1} = i_B$.

References

[1] Richard Hammack, BOOK OF PROOF (Second Edition)