WON SERIES IN DISCRETE MATHEMATICS AND MODERN ALGEBRA VOLUME 0

SET THEORY

AMIN WITNO

www.witno.com

Logic & Set Theory

Revision Notes and Problems

Amin Witno <www.witno.com>

Preface

These notes are for students of Math 251 as a revision workbook and are not meant to substitute the in-class notes. No student is expected to really benefit from these notes unless they have regularly attended the lectures.

References

1. Smith, Eggen, and St. Andre, A Transition to Advanced Mathematics, 6th edition 2006, Brooks Cole.
2. Keith Devlin, Sets, Functions, and Logic: An Introduction to Abstract Mathematics, 3rd edition 2004, CRC Press.
3. Michael L. O'Leary, The Structure of Proof with Logic and Set Theory, 2002, Prentice Hall.
4. David L. Johnson, Elements of Logic via Numbers and Sets, 1998, Springer Verlag.

Copyrights

Chapter 0
Preliminaries

In mathematics very often we study sets whose elements are the real numbers. Some special number sets which are frequently encountered are defined as follow.

- The set of natural numbers $\mathbb{N}$ contains the elements 1, 2, 3, ...
- The set of integers $\mathbb{Z}$ contains all the natural numbers together with their negatives and zero: ... , –3, –2, –1, 0, 1, 2, 3, ...
- The set of rational numbers $\mathbb{Q}$ consists of numbers of the form a/b where a and b are integers with $b \neq 0$, for examples 1/2, 5 = 5/1, –22/7, 0/19, etc. Hence all integers are rational numbers, but some rational numbers are not integers.
- The set of all real numbers is denoted by $\mathbb{R}$.
- The set of irrational numbers $\Im$ consists of all real numbers which are not rational, such as $\sqrt{2}$, π, etc.
- The set of even numbers $\mathcal{E}$ contains the elements 0, ±2, ±4, ±6, ... which are those of the form $2n$ for some integer n.
- The set of odd numbers $\mho$ is the set of integers which are not even. Hence odd numbers are ±1, ±3, ±5, ... which can be written as $2n + 1$ for some integer n.

0.1 Prove that the number $\sqrt{2}$ is not rational.

A set of real numbers x in the range $a < x < b$ can also be written using the **interval notation** (a, b). The round bracket at either end can be replaced by a square bracket to indicate inclusion. For example $(a, b]$ means the set $a < x \leq b$. Moreover we use the infinity symbol to indicate unboundedness, such as $[a, \infty)$ for the set $x \geq a$.

0.2 Write the interval notation for each set.

a) $a \leq x < b$
b) $a \leq x \leq b$
c) $x < b$
d) $x \leq b$

For real numbers x we define the **absolute value** of x to be $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$. For example $|-2| = 2$, $|\sqrt{2}| = \sqrt{2}$, and $|0| = 0$. A useful fact is that $\sqrt{(x^2)} = |x|$.

0.3 Find all real number solutions of these equations.

a) $|x| = 3$
b) $|x + 1| = 3$
c) $|x + 1| > 3$
d) $|2x + 1| > 3$

For real numbers x, the **greatest integer function** $[x]$ gives the greatest integer not greater than x. For example $[3.14] = 3$.

0.4 Evaluate $[x]$ for these values of x.

a) 5
b) 1.999
c) 234/5

d) -2.3
e) $\sqrt{10}$

For two integers m and $n > 0$ define the **modulo operation** $m \bmod n = m - [m/n]\, n$. For example $217/5 = 43.4$ hence $217 \bmod 5 = 217 - (43 \times 5) = 2$. Equivalently $217 = (43) \times 5 + (2)$ hence $217 \bmod 5 = 2$, which is the remainder when 217 is divided by 5.

0.5 Evaluate the following.
a) 123 mod 3
b) 2000 mod 7
c) 25 mod 5
d) 25 mod 11
e) 11 mod 25

Note that $m \bmod n$ is the remainder when m is divided by n. In particular $m \bmod n = 0$ when m is a **multiple** of n, or we say that n **divides** m. For example $12 \bmod 3 = 0$ because $12 = 3 \times 4$, so we say 3 divides 12. Also $m \bmod 2 = 0$ whenever m is an even number, so all even numbers are multiples of 2.

A **sequence** is a function $f(n)$ defined over the natural numbers, hence it can be ordered as $f(1), f(2), f(3), \ldots$

Examples: 1) $f(n) = n^2$ is the sequence 1, 4, 9, 16, 25, 36, 49, ...
2) $f(n) = 2n - 1$ is the sequence 1, 3, 5, 7, 9, 11, 13, ...

0.6 Write out the following sequences.
a) $f(n) = 2n + 1$
b) $n(n + 1)$
c) $n \bmod 5$
d) $[n/2]$

0.7 Find a formula $f(n)$ for each sequence.
a) 1, 2, 4, 8, 16, 32, 64, ...
b) 3, 6, 9, 12, 15, 18, 21, ...
c) 7, 11, 15, 19, 23, 27, 31, ...
d) 1, 2, 3, 1, 2, 3, 1, 2, 3, ...

Summations over some or all terms in a sequence can be represented using **sigma notation**. For example $\sum_{n=1}^{5} n^2 = 1+4+9+16+25$.

0.8 Write the following summations using sigma notations.
a) 16 + 32 + 64 + 128
b) 2 + 4 + 6 + 8 + 10 + ...
c) 3 + 6 + 9 + 12 + ... + 300
d) 11 + 13 + 15 + 17 + 19 + ...

Chapter 1
Logic

A **proposition** is a statement which has a truth value either true or false. For examples, “2 is even”, “2 + 2 = 4”, “2 + 2 = 5”.

The **negation** of a proposition p is also called **not** p, and is denoted by $\neg p$.

Example: 1) If p: “2 is even” then $\neg p$: “2 is not even”.
1) If p: “2 + 2 = 5” then $\neg p$: “$2 + 2 \neq 5$”.

If p and q are two propositions then their **conjunction** is the proposition whose value is true only when both are true. A conjunction can also be written $p \wedge q$ which is read p **and** q.

1.1 Let p: “2 is even” and q: “2 + 2 = 5”. State these propositions and find their value.

a) $p \wedge q$
b) $p \wedge \neg q$
c) $\neg p \wedge q$
d) $\neg p \wedge \neg q$

Similarly the **disjunction** of p and q has value false only when both are false. It is denoted by $p \vee q$ and read p **or** q.

1.2 Repeat Problem 1.1 with $\wedge$ replaced by $\vee$.

The **implication** of p and q has value false only when p is true and q is false. It is denoted by $p \rightarrow q$ and read **if** p **then** q. A statement in the form $p \rightarrow q$ is also called a **conditional statement,** in which p is a **sufficient** condition for q and q is a **necessary** condition for p.

1.3 Repeat Problem 1.1 with $\wedge$ replaced by $\rightarrow$.

The **equivalence statement** $p \leftrightarrow q$ is true only when p and q have the same value. It is read p **if and only if** q and is also called a **biconditional statement**, in which p is a necessary and sufficient condition for q, and vice versa.

1.4 Repeat Problem 1.1 with $\wedge$ replaced by $\leftrightarrow$.

1.5 Let p: “Today is cold”, q: “Today is hot”, and r: “Today is windy”. Write the following propositions using p, q, r.

a) Today is hot if and only if not windy.
b) Either today is cold or not cold.
c) If today is not windy then it is not hot.
d) Today is neither cold nor windy.
e) If today is windy then either it is hot or cold.

Logic operators can be presented in their **truth tables**:

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
T	**T**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**
F	**T**	**F**	**T**	**T**	**F**
F	**F**	**F**	**F**	**T**	**T**

1.6 Draw the truth table for each of the following propositions.

a) $\neg p \vee \neg q$
b) $\neg(p \wedge q) \rightarrow p$
c) $(p \wedge \neg q) \leftrightarrow (\neg p \vee q)$
d) $(p \rightarrow q) \rightarrow r$
e) $[(p \wedge q) \rightarrow r] \leftrightarrow [\neg p \vee (q \leftrightarrow \neg r)]$

Two propositions are **equivalent** if their truth tables are identical. We write $p \equiv q$ when the two are equivalent. For example we can show that $\neg p \vee \neg q \equiv \neg(p \wedge q)$.

1.7 Prove the following equivalences by drawing the truth tables.

a) $\neg p \wedge \neg q \equiv \neg(p \vee q)$
b) $p \rightarrow q \equiv \neg p \vee q$
c) $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
d) $p \rightarrow (q \rightarrow r) \equiv q \rightarrow (p \rightarrow r)$

The **contrapositive** of $p \rightarrow q$ is the proposition $\neg q \rightarrow \neg p$. It can be shown that these two are equivalent: $p \rightarrow q \equiv \neg q \rightarrow \neg p$.

1.8 Write an equivalent statement using contrapositive.

a) If I study hard then I get good mark.
b) If it rains then it is not hot.
c) If today is not Sunday then tomorrow is not Monday.
d) If I am not lazy then I come to the lecture.

The **converse** of $p \rightarrow q$ is the proposition $q \rightarrow p$.

1.9 Write the converse of the propositions in Problem 1.8. Is $p \rightarrow q \equiv q \rightarrow p$?

Theorem: The following is a list of some common logical equivalence rules:

1) $p \wedge q \equiv q \wedge p$
   $p \vee q \equiv q \vee p$
2) $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
   $p \vee (q \vee r) \equiv (p \vee q) \vee r$
3) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
   $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4) $\neg(\neg p) \equiv p$
   $\neg(p \wedge q) \equiv \neg p \vee \neg q$
   $\neg(p \vee q) \equiv \neg p \wedge \neg q$
5) $p \rightarrow q \equiv \neg p \vee q$
   $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

1.10 Prove by applying the above rules.

a) $\neg(p \to q) \equiv p \wedge \neg q$
b) $p \to q \equiv \neg q \to \neg p$
c) $p \to (q \to r) \equiv q \to (p \to r)$
d) $p \to (q \wedge r) \equiv (p \to q) \wedge (p \to r)$
e) $(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$

1.11 True or False. Prove by any method you like.

a) $p \to (q \to r) \equiv (p \to q) \to r$
b) $p \to (q \vee r) \equiv (p \to q) \vee (p \to r)$
c) $p \wedge (q \to r) \equiv (p \wedge q) \to (p \wedge r)$
d) $p \vee (q \to r) \equiv (p \vee q) \to (p \vee r)$

A **predicate** is a propositional function such as $P(x)$: $x + 2 = 5$. The statement "$x + 2 = 5$" by itself is not a proposition because it does not have a truth value. But for each value of x, $P(x)$ becomes a proposition, for instance, $P(3)$: $3 + 2 = 5$ is true and $P(2)$: $2 + 2 = 5$ is false.

1.12 Let $P(x)$: $x^2 < x$.

a) What is the value of $P(1)$?
b) What is the value of $P(2)$?
c) For which x is the value of $P(x)$ true?

1.13 Let $P(x,y)$: $x^2 + y^2 = (x + y)^2$. Find the values of the following propositions.

a) $P(0,1)$
b) $P(0,0)$
c) $P(1,1)$
d) For which (x,y) is the value of $P(x,y)$ true?

A predicate can also be made a proposition by adding a **quantifier**. There are three quantifiers:

1) $\forall$: for all / for any / for each / for every
2) $\exists$: for some / there is / there exists / there is at least one
3) $\exists!$: there is a unique / there is exactly one / there exists only one

Example: Let $P(x)$: $x + 2 = 5$.

1) $\forall x\, P(x)$: "for all real numbers x, $x + 2 = 5$", which is false.
2) $\exists x\, P(x)$: "there is a real number x such that $x + 2 = 5$", which is true.
3) $\exists! x\, P(x)$: "there is a unique real number x such that $x + 2 = 5$", which is true.

1.14 Let $P(x)$: $x < 2x$.

a) What is the value of $\forall x\, P(x)$?
b) What is the value of $\exists x\, P(x)$?
c) What is the value of $\exists! x\, P(x)$?

1.15 Let P(x, y): $x^2 + y^2 = (x + y)^2$. Find the values of the following propositions.

a) $\exists x \exists y P(x, y)$
b) $\exists x \forall y P(x, y)$
c) $\forall x \exists y P(x, y)$
d) $\exists y \forall x P(x, y)$
e) $\forall y \exists x P(x, y)$

1.16 Repeat Problem 1.15, employing $\exists!$ instead of $\exists$.

1.17 Repeat Problem 1.15 using the following predicates.

a) $P(x, y): x^2 + y^2 > 0$
b) $P(x, y): x^2 + y^2 \geq 1$
c) $P(x, y): x^2 - y^2 \geq 0$
d) $P(x, y): x^2 - y > 0$

Note that $\neg\exists x\, P(x) \equiv \forall y\, \neg P(x)$ and similarly $\neg\forall x\, P(x) \equiv \exists y\, \neg P(x)$.

Example: Let $P(x)$: $x + 2 = 5$.

1) $\exists x\, P(x)$: "there is a real number x such that $x + 2 = 5$".
   $\neg\exists x\, P(x)$: "there is no real number x such that $x + 2 = 5$" which is equivalent to $\forall y\, \neg P(x)$: "for all real numbers x, $x + 2 \neq 5$".
2) $\forall x\, P(x)$: "for all real numbers x, $x + 2 = 5$".
   $\neg\forall x\, P(x)$: "not all real numbers x satisfies $x + 2 = 5$" which is equivalent to $\exists y\, \neg P(x)$: "there is a real number x such that $x + 2 \neq 5$".

1.18 Write the negations by interchanging $\exists$ and $\forall$.

a) There is a real number x such that $x^2 < 0$.
b) Every integer is even.
c) All triangles have angle sum equal 180 degrees.
d) There is an integer x such that $x^2 + 2x + 3 = 0$.

1.19 What is the negation of $\exists! x\, P(x)$? Use your answer to write the negation of the statement "There is a unique real number x such that $Ax^2 + Bx + C = 0$".

Chapter 2
Proofs

Proving Conditional Statements:

To prove a proposition in the form $p \to q$, we begin by assuming that p is true and then show that q must be true.

Example: Prove that if x is an odd integer then x^2 is also odd.

Solution: Let p: x is odd, and q: x^2 is odd. We want to prove $p \to q$.
Start: p: x is odd
$\to x = 2n + 1$ for some integer n
$\to x^2 = (2n + 1)^2$
$\to x^2 = 4n^2 + 4n + 1$
$\to x^2 = 2(2n^2 + 2n) + 1$
$\to x^2 = 2m + 1$, where $m = (2n^2 + 2n)$ is an integer
$\to x^2$ is odd
$\to q$

2.1 Prove the following propositions.

a) If x is an even number then x^3 is also even.
b) If x is odd then $x^2 - 3x$ is even.
c) If x and y are odd then $x + y$ is even.
d) If x and y are even then 4 divides xy.
e) If x is odd then $x^2 - 1$ is a multiple of 8.

Proof by Contrapositive:

To prove a proposition in the form $p \to q$ we may instead prove its contrapositive: $\neg q \to \neg p$. This works because $p \to q \equiv \neg q \to \neg p$.

Example: Prove that if x^2 is odd then x must be odd.

Solution: Let p: x^2 is odd, and q: x is odd. We prove $p \to q$ by proving $\neg q \to \neg p$.
Start: $\neg q$: x is even
$\to x = 2n$ for some integer n
$\to x^2 = (2n)^2$
$\to x^2 = 4n^2$
$\to x^2 = 2(2n^2)$
$\to x^2 = 2m$, where $m = 2n^2$ is an integer
$\to x^2$ is even
$\to \neg p$

2.2 Prove the following propositions.

a) If x^2 is even then x must be even.
b) If x^3 is even then x must be even.

c) If $x^2 - 2x$ is even then x is even.

d) If $x^3 - 4x + 2$ is odd then x is odd.

Proof by Contradiction:

To prove that a proposition p is true we may assume that $\neg p$ is true and then show that it would lead to a contradiction or a false statement.

Example: Prove that $\sqrt{2}$ is irrational.

Solution: Let p: $\sqrt{2}$ is irrational. Now assume $\neg p$ is true, that is, $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ which has been reduced, that is for some integers a and b with no common factors. Hence $a^2 = 2b^2$ which means that a^2 is even and so is a, say $a = 2c$ with integer c. Substituting yields $4c^2 = 2b^2$ or $2c^2 = b^2$ hence b is also even. This means that a and b have a common factor 2 which is a contradiction, and so $\neg p$ must be false and p is true.

2.3 Prove the following propositions.

a) The number $\sqrt[3]{2}$ is irrational.

b) The number $\sqrt{2} + \sqrt{2}$ is irrational.

c) The number $3 + \sqrt{2}$ is irrational.

d) There is no largest natural number.

Proving Equivalent Statements:

To prove a proposition in the form $p \leftrightarrow q$ we must prove both $p \rightarrow q$ and its converse $q \rightarrow p$. This is so because $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$.

Example: Prove that x is odd if and only if x^2 is odd.

Solution: Let p: x is odd, and q: x^2 is odd. We must prove $p \rightarrow q$ as well as $q \rightarrow p$. Both of these have been shown in the previous two examples.

2.4 Prove the following propositions.

a) x is even if and only if x^2 is even.

b) x^3 is even if and only if x is even.

c) xy is odd if and only if both x and y are odd.

d) $x^3 + x^2 + x + 1$ is even if and only if x is odd.

2.5 Prove that $a \bmod n = b \bmod n$ if and only if n divides $(a - b)$.

Proof by Cases:

To prove a proposition in the form $p \rightarrow q$ where $p \equiv a \vee b$ we may instead prove both $a \rightarrow q$ and $b \rightarrow q$.

Example: Prove that if x is an integer then $x^2 + x$ is even.

Solution: Let p: x is integer, and q: $x^2 + x$ is even. We must prove $p \rightarrow q$.
Let a: x is even, and b: x is odd. Then $p \equiv a \vee b$ because any integer is either even or odd. We will now prove the two cases $a \rightarrow q$ and $b \rightarrow q$...

2.6 Prove the following propositions.

a) If x is an integer then $x^2 - x$ is even.
b) If x or y is even then xy is even.
c) If x is an integer then $x^2 + 2$ is not a multiple of 4.
d) If x is a real number then $-|x| \le x \le |x|$.

2.7 Prove the equivalence $(a \vee b) \to q \equiv (a \to q) \wedge (b \to q)$.

Proof by cases can be generalized to three (or more) steps. Suppose we want to prove $p \to q$ where $p \equiv a \vee b \vee c$. Then we must prove the three cases $a \to q$ and $b \to q$ and $c \to q$.

2.8 Prove that if x is an integer then $x^3 - x$ is a multiple of 3.

2.9 Prove that if x and y are real numbers then $|x\, y| = |x|\ |y|$.

Proving Existence Statements:

To prove a proposition in the form $\exists x\, P(x)$, it suffices, when possible, to find one value of x for which $P(x)$ is true.

Example: Prove that there exists an irrational number.
Solution: Let $P(x)$: x is irrational. We will prove $\exists x\, P(x)$ by showing that $P(\sqrt{2})$ is true. This was done is Problem 1.1.

2.10 Prove the following propositions.

a) There is a positive integer n such that $n^2 - 2n - 8 = 0$.
b) There is a real number x such that $x^2 - x = 5$.
c) There is an integer n such that $\sqrt{n}$ is also an integer.
d) There are two real numbers x and y such that $x^2 + y^2 = (x + y)^2$.
e) There is an integer n such that $n \bmod 5 = 2$ and $n \bmod 6 = 4$.

2.11 Prove that there are irrational numbers a and b such that a^b is rational.

Proving Uniqueness:

To prove a proposition in the form $\exists! x\, P(x)$ we first prove $\exists x\, P(x)$ and then prove the proposition $P(x_1) \wedge P(x_2) \to x_1 = x_2$.

Example: Prove that there is a unique integer x such that $2x + 9 = 3$.
Solution: Let $P(x)$: $2x + 9 = 3$. First $P(-3)$ is true (Check!) so we proved $\exists x\, P(x)$. Next suppose $P(x_1)$ and $P(x_2)$ are both true. Then $2x_1 + 9 = 3 = 2x_2 + 9 \to 2x_1 + 9 = 2x_2 + 9 \to 2x_1 = 2x_2 \to x_1 = x_2$. Hence we proved $\exists! x\, P(x)$.

2.12 Prove the following propositions.

a) There is a unique real number x such that $a + x = a$ for any number a.
b) There is a unique real number x such that $ax = a$ for all real numbers a.
c) Let a be any integer. There is a unique integer x such that $a + x = 0$.

d) Let a be any non-zero rational number. There is a unique rational number x such that $ax = 1$.

Proving False Statements:

To prove that p is false it suffices, when possible, to show that $\neg p$ is true.

2.13 Prove that the proposition is false.

a) For all real numbers, $x - x^2 \leq 0$.

b) For all real numbers, $(x + y)^2 = x^2 + y^2$.

c) For all real numbers, $|x + y| = |x| + |y|$.

d) For all natural numbers, $2^n > n!$

e) For all natural numbers, $3^n > n!$

2.14 Prove that the following proposition is false: There is a unique real number x such that $2x^2 - 3x = 2$.

Proof by Mathematical Induction:

To prove a proposition in the form $\forall n\ P(n)$ where n is a natural number, it suffices to prove $P(1)$ and $P(n) \rightarrow P(n+1)$.

Example: Prove the following formula for all natural numbers n.

$1 + 3 + 5 + 7 + 9 + ... + (2n - 1) = n^2$

Solution: Let $P(n)$: $1 + 3 + 5 + 7 + 9 + ... + (2n - 1) = n^2$

We shall prove $\forall n\ P(n)$ in two steps:

1) $P(1)$: $1 = 1^2$ so this proposition is true.

2) $P(n)$: $1 + 3 + 5 + 7 + 9 + ... + (2n - 1) = n^2$

$\rightarrow 1 + 3 + 5 + 7 + 9 + ... + (2n - 1) + (2n + 1) = n^2 + (2n + 1)$

$\rightarrow 1 + 3 + 5 + 7 + 9 + ... + (2n - 1) + (2n + 1) = (n + 1)^2$

$\rightarrow P(n+1)$

2.15 Prove the following formulas for all natural numbers n.

a) $1 + 2 + 3 + 4 + 5 + ... + n = ½\, n\, (n + 1)$

b) $2 + 4 + 6 + 8 + 10 + ... + 2n = n^2 + n$

c) $1 + 2 + 4 + 8 + 16 + ... + 2^{n-1} = 2^n - 1$

d) $1 + 3 + 9 + 27 + 81 + ... + 3^{n-1} = ½\, (3^n - 1)$

e) $1 + 4 + 9 + 16 + 25 + ... + n^2 = n(n + 1)(2n + 1) / 6$

2.16 Prove by induction for all natural numbers n.

a) $(2^{2n} - 1) \bmod 3 = 0$

b) 7 divides $(2^{3n} - 1)$

c) $(n^3 + 2n) \bmod 3 = 0$

d) $(n^5 - n)$ is a multiple of 5.

e) 7 divides $(2^{n+1} + 3^{2n-1})$

The **Principle of Mathematical Induction** used in the last method of proof can be stated by the proposition $P(1) \wedge \{P(n) \rightarrow P(n+1)\} \rightarrow \forall n \geq 1\ P(n)$. Other variations of this principle can sometimes be applied. The following are some of them.

1) **Induction with base** k:
   $P(k) \wedge \{P(n) \rightarrow P(n+1)\} \rightarrow \forall n \geq k\ P(n)$
2) **Cumulative Induction**:
   $P(1) \wedge \{P(1) \wedge P(2) \wedge \ldots \wedge P(n) \rightarrow P(n+1)\} \rightarrow \forall n \geq 1\ P(n)$
3) **Double Induction**:
   $\forall m \geq 1\ P(m,1) \wedge \{P(m, n) \rightarrow P(m, n+1)\} \rightarrow \forall m \geq 1\ \forall n \geq 1\ P(m, n)$

2.17 Prove by induction for the given base.

a) $n < 2^n$ for all $n \geq 1$
b) $2^n < n!$ for all $n \geq 4$
c) $3^n < n!$ for all $n \geq 7$
d) $2^n > n^2$ for all $n \geq 5$
e) $n! < n^n$ for all $n \geq 2$

Chapter 3
Sets

A **set** is a collection of objects called the **elements** of the set. The ordering of the elements is not important and repetition of elements is ignored, for example $\{1, 3, 1, 2, 2, 1\} = \{1, 2, 3\}$. A set may also be empty and it is denoted by φ or $\{\ \}$. If x is an element of the set A then we write $x \in A$, while the negation is written $x \notin A$.

Set notations can be very convenient. For examples we may redefine the number sets given in Chapter 0 as follow. Here the notation $A = \{x \mid P(x)\}$ means that the set A consists of the elements x for which $P(x)$ is true.

- $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, ...\}$
- $\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}$
- $\mathcal{E} = \{2n \mid n \in \mathbb{Z}\}$
- $\mho = \{x \in \mathbb{Z} \mid x \notin \mathcal{E}\}$
- $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z} \wedge b \in \mathbb{N}\}$
- $\Im = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$

For any two sets A and B, define the following set operations.

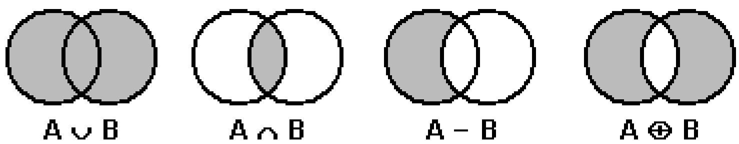
1) The **union** $A \cup B = \{x \mid x \in A \vee x \in B\}$
2) The **intersection** $A \cap B = \{x \mid x \in A \wedge x \in B\}$
3) The **difference** $A - B = \{x \mid x \in A \wedge x \notin B\}$
4) The **symmetric difference** $A \oplus B = \{x \mid x \in A \leftrightarrow x \notin B\}$

For examples if $A = \{1, 2, 3, 4, 5\}$ and $B = \{0, 2, 4, 6\}$ then $A \cup B = \{0, 1, 2, 3, 4, 5, 6\}$, $A \cap B = \{2, 4\}$, $A - B = \{1, 3, 5\}$, $B - A = \{0, 6\}$, and $A \oplus B = \{0, 1, 3, 5, 6\}$. Also we can see that $\mathcal{E} \cup \mho = \mathbb{Z}$, $\mathbb{Q} \cup \Im = \mathbb{R}$, $\mathbb{Q} \cap \Im = \varphi$, $\mathbb{Z} - \mathcal{E} = \mho$, etc.

3.1 Let $A = \{1, 2, 3, 4, 5\}$, $B = \{0, 2, 4, 6\}$ and $C = \{1, 3, 5\}$. Find the following sets.

a) $(A \cup C) \oplus (A \cap C)$
b) $A \oplus (B \cup C)$
c) $(A \oplus B) - (A \oplus C)$
d) $(A - B) \oplus (A - C)$

These set operations can be illustrated using **Venn diagrams**,



or truth tables, in which the value is true if x is an element of the set and false if not.

A	B	$A \cap B$	$A \cup B$	$A - B$	$A \oplus B$
T	**T**	**T**	**T**	**F**	**F**
T	**F**	**F**	**T**	**T**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**F**	**F**	**F**	**F**	**F**

3.2 True or False? Use Venn diagrams or truth tables to verify.

a) $(A \cup B) - (A \cap B) = A \oplus B$
b) $(A - B) \cup (B - A) = A \oplus B$
c) $(A \oplus B) - B = A$
d) $(A \oplus B) \oplus B = A$
e) $A \oplus A = A - A$

Define the **complement** of a set A to be $-A = \{x \mid x \notin A\}$. For example $-\Im = \mathbb{Q}$.

Theorem: The following set identities are the analog of logical equivalences.

1) $A \cup B = B \cup A$
   $A \cap B = B \cap A$
2) $A \cup (B \cup C) = (A \cup B) \cup C$
   $A \cap (B \cap C) = (A \cap B) \cap C$
3) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4) $-(-A) = A$
   $-(A \cup B) = -A \cap -B$
   $-(A \cap B) = -A \cup -B$
5) $A - B = A \cap -B$
   $A \oplus B = (A - B) \cup (B - A)$

Two sets are **disjoint** if their intersection is empty: $A \cap B = \varphi$. For example $\mathcal{E}$ and $\mho$ are disjoint, and so are $\mathbb{Q}$ and $\Im$.

3.3 Prove that if A and B are disjoint then $A - B = A$ and $A \oplus B = A \cup B$.

A set S is a **subset** of a set A if $x \in S \to x \in A$. This relation can be written $S \subseteq A$ or sometimes $A \supseteq S$. For example $\{1, 3\} \subseteq \{1, 2, 3, 4\}$, $\mathcal{E} \subseteq \mathbb{Z}$, $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, etc.

3.4 Prove the following statements.

a) $\varphi \subseteq A$
b) $A \subseteq A$
c) $A \cap B \subseteq A$
d) $A \subseteq A \cup B$
e) $A \subseteq B \wedge B \subseteq C \to A \subseteq C$

3.5 Prove that if $A \subseteq B$ then

a) $A \cup B = B$
b) $A \cap B = A$
c) $A - B = \varphi$
d) $A \oplus B = B - A$

Theorem: $A = B \leftrightarrow A \subseteq B \wedge B \subseteq A$

3.6 Use the above theorem to prove the following identities.

a) $-(A \cup B) = -A \cap -B$
b) $A - B = A \cap -B$

The **power set** of a set A is defined by $P(A) = \{S \mid S \subseteq A\}$. Hence $P(A)$ is the set consisting of all the subsets of A.

Example: Find $P(A)$ for $A = \{1, 2\}$.
Solution: A has a total of four subsets namely $\{1\}$, $\{2\}$, φ, and A itself.
Hence $P(A) = \{\varphi, \{1\}, \{2\}, A\}$.

3.7 Find $P(A)$ for each set A.

a) $A = \{1, 2, 3\}$
b) $A= \{1, 2, 3, 4\}$
c) $A = \varphi$
d) $A = P(\varphi)$
e) $A = P(P(\varphi))$

3.8 Prove the following statements.

a) $P(A \cap B) = P(A) \cap P(B)$
b) $P(A \cup B) \supseteq P(A) \cup P(B)$
c) $A \subseteq B \leftrightarrow P(A) \subseteq P(B)$

The **cardinality** of a set A is the number of elements in A, denoted by $|A|$. For example $|\{1, 3, 5, 7\}| = 4$, $|\varphi| = 0$, and $|\mathbb{Z}| = \infty$.

Theorem: If $|A| = n$ then $|P(A)| = 2^n$ (Every set with n elements has 2^n subsets.)

3.9 Prove the above theorem by cumulative induction.

The **cross product** of A and B is the set $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.

Example: If $A = \{1, 2, 3\}$ and $B = \{x, y\}$ then
$A \times B = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}$
$B \times A = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$

Theorem: If $|A| = m$ and $|B| = n$ then $|A \times B| = mn$.

3.10 Prove the following statements.

a) $A \times B = B \times A \leftrightarrow A = B$
b) $A \times (B \times C) \neq (A \times B) \times C$
c) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
d) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

Let S be any set of sets. The **generalized union** and **generalized intersection** over S are defined as follow.

1) $\bigcup_{A \in S} A = \{x \mid \exists A \in S, x \in A\}$
2) $\bigcap_{A \in S} A = \{x \mid \forall A \in S, x \in A\}$

For example let A_n be the interval $[0, 1/n]$ and $S = \{A_n \mid n \in \mathbb{N}\}$. Then the generalized union and intersection over S are $\cup A_n = [0, 1]$ and $\cap A_n = \{0\}$.

Chapter 4
Relations

A **relation** on a set A means a subset of $A \times A$. For example if $A = \{1, 2, 3\}$ then the following are some, but not all, possible relations on A.

1) $R = \{(1,1), (1,2), (1,3)\}$
2) $R = \{(2,3)\}$
3) $R = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$
4) $R = \varphi$

4.1 If $|A| = n$ then how many different relations on A are possible?

If R is a relation on A then the **inverse** of R is the relation $R^{-1} = \{(b, a) \mid (a, b) \in R\}$. Furthermore if S is another relation on A then the **composition** of R with S is the relation $S \circ R = \{(a, c) \mid (a, b) \in R \wedge (b, c) \in S\}$. In particular we define $R^2 = R \circ R$, $R^3 = R^2 \circ R$, etc.

Example: Let $A = \{1, 2, 3, 4\}$ and $R = \{(1,2), (2,3), (2,4), (3,3), (4,1)\}$ and $S = \{(1,3), (2,2), (3,1), (3,3)\}$. Then

$R^{-1} = \{(2,1), (3,2), (4,2), (3,3), (1,4)\}$
$S \circ R = \{(1,2), (2,1), (2,3), (3,1), (3,3), (4,3)\}$
$R \circ S = \{(1,3),(2,3), (2,4), (3,2), (3,3)\}$
$R^2 = R \circ R = \{(1,3), (2,3), (2,1), (3,3), (4,2)\}$

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

a) Find R^{-1} and $(R^{-1})^{-1}$
b) Find R^2 and R^3
c) Find $R \circ R^{-1}$ and $R^{-1} \circ R$
d) Find $(R^{-1})^2$ and $(R^2)^{-1}$

4.3 Prove that $R \circ (R \circ R) = (R \circ R) \circ R$. Hence we may write $R^3 = R \circ R \circ R$.

Properties of a relation $R \subseteq A \times A$.

1) **reflexive** if $\forall a \in A\ (a, a) \in R$
2) **symmetric** if $\forall a \in A\ \forall b \in A, (a, b) \in R \rightarrow (b, a) \in R$
3) **anti-symmetric** if $\forall a \in A\ \forall b \in A, (a, b) \in R \wedge (b, a) \in R \rightarrow a = b$
4) **transitive** if $\forall a, b, c \in A, (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R$

Example: Let $A = \{1, 2, 3\}$ and consider three relations on A:

$R = \{(1,1), (1,2), (2,1), (2,2), (3,3)\}$
$S = \{(1,1), (1,3), (2,2), (3,2)\}$
$T = \{(1,2), (1,3), (2,3)\}$
R is reflexive, symmetric, and transitive, but not anti-symmetric.
S is anti-symmetric, but not reflexive, not symmetric, and not transitive.
T is anti-symmetric and transitive, but not reflexive and not symmetric.

4.4 Let $A = \{1, 2, 3, 4\}$. Which properties above are true for each relation R on A?

a) $R = \{(a, b) \in A \times A \mid a \leq b\}$
b) $R = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$
c) $R = \{(1,1), (1,3), (2,1), (2,2), (2,4)\}$
d) $R = \{(a, b) \in A \times A \mid a + b > 5\}$

4.5 Let $A = \{1, 2, 3, 4\}$. Give any example of a relation R on A which is

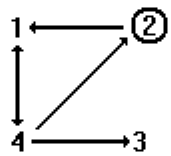
a) reflexive, not anti-symmetric, not transitive.
b) not reflexive, not symmetric, not transitive.
c) symmetric and transitive.
d) neither symmetric nor anti-symmetric.
e) both symmetric and anti-symmetric.

4.6 Let R be a relation on A. Prove the following propositions.

a) R is symmetric if and only if $R^{-1} = R$.
b) R is anti-symmetric if and only if $R \cap R^{-1} \subseteq \{(a, a) \mid a \in A\}$.
c) R is transitive if and only if $R^2 \subseteq R$.

A relation $R \subseteq A \times A$ can be represented by a **digraph** in which each element of A is represented by a **vertex** and each element $(a, b) \in R$ is represented by an **edge** with direction from a to b. In the case $a = b$ the edge is called a **loop**.

Example: $A = \{1, 2, 3, 4\}$ and $R = \{(1, 4), (2, 1), (2, 2), (4, 1), (4, 2), (4, 3)\}$.



4.7 Draw the digraph for each of the relations in Problem 4.4.

4.8 How can you tell from the digraph if R is

a) reflexive
b) **anti-reflexive** [meaning that $\forall a \in A\ (a, a) \notin R$]
c) symmetric
d) anti-symmetric
e) transitive

$R \subseteq A \times A$ is called an **equivalence relation** if it is reflexive, symmetric, and transitive.

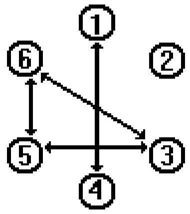
4.9 Prove that the following relations are equivalence relations.

a) $R = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid [a] = [b]\}$
b) $R = \{(a, b) \in A \times A \mid a \bmod 3 = b \bmod 3\}$ where $A = \{0, 1, 2, ..., 9\}$
c) $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \bmod 5 = b \bmod 5\}$
d) $R = \{(a, b) \in A \times A \mid a = b\}$ where $A = \{1, 2, 3, 4\}$
e) $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b \text{ is even}\}$

If R is an equivalence relation on A then A is partitioned into subsets or classes of the forms $Ax = \{a \in A \mid (a, x) \in R\}$ for every $x \in A$. These subsets of A are called the **equivalence classes** of A under R and they satisfy the following properties.

1) $(x, y) \in R \rightarrow Ax = Ay$
2) $(x, y) \notin R \rightarrow Ax \cap Ay = \varphi$
3) $(a, b) \in R \leftrightarrow \exists x \in A, a \in Ax \wedge b \in Ax$

Example: The following digraph shows that R is an equivalence relation. (Why?) There are three equivalence classes namely



$A1 = \{1, 4\} = A4$
$A2 = \{2\}$
$A3 = \{3, 5, 6\} = A5 = A6$

4.10 Find the equivalence classes for each relation in Problem 4.7.

4.11 Define the **congruence** relation on $\mathbb{Z}$ by $a \equiv b$ if and only if a mod $n = b$ mod n. Let $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b\}$. Prove that R is an equivalence relation on $\mathbb{Z}$ and find the equivalence classes.

$R \subseteq A \times A$ is called a **partial order** relation if it is reflexive, anti-symmetric, and transitive.

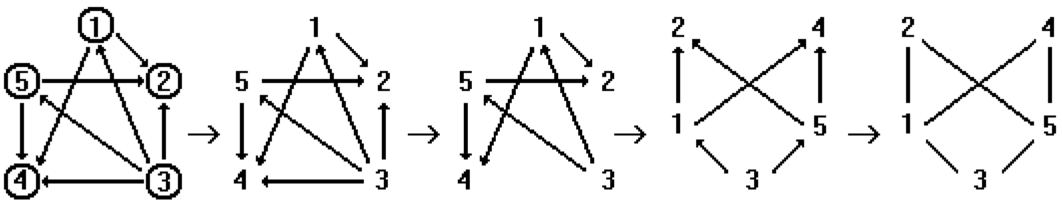
4.12 Prove that the following relations are partial ordering.

a) $A = \{50, 22, 35, 14\}$ and $R = \{(a, b) \in A \times A \mid a \leq b\}$
b) $A = \{1, 2, 6, 12, 24\}$ and $R = \{(a, b) \in A \times A \mid a$ divides $b\}$
c) $A = \{2, 3, 6, 10, 20, 30\}$ and $R = \{(a, b) \in A \times A \mid a$ divides $b\}$
d) $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a$ divides $b\}$

If R is a partial order relation then its digraph can be simplified into a **Hasse diagram** after these four steps:

1) Do not draw loops.
2) Do not draw (a, c) whenever there are (a, b) and (b, c).
3) Redraw the remaining graph so that all edges point upward.
4) Do not draw the directions.

Example: The following digraph shows that R is a partial order relation. (Why?) The four steps above lead to the Hasse diagram of R.



4.13 Draw the Hasse diagram for each partial order relation in Problem 4.12.

A partial order relation R on A is called a **total ordering** if it satisfies one additional proposition: $\forall a \in A\ \forall b \in A, (a, b) \in R \vee (b, a) \in R$.

4.14 Which of the relations given in Problem 4.12 are total ordering? Show that the Hasse diagram of a total ordering can always be drawn as a straight line.

4.15 Prove that the relation $a \leq b$ gives a total ordering on $\mathbb{R}$.

Suppose R is a partial order relation on the set A. An element $l \in A$ is called a **least element** under R if $\forall a \in A$, $(l, a) \in R$. Now R is called a **well ordering** on A if every non-empty subset of A has a least element.

4.16 Which ones of the sets A given in Problem 4.12 have a least element under R? Which relations are well order relations?

4.17 Prove that a well ordering is a total ordering but not conversely.

4.18 Give an example of a total ordering on a set which is not a well ordering.

The **Well Ordering Principle** says that $\mathbb{N}$ is well ordered under the "$\leq$" relation.

Theorem: The Well Ordering Principle is equivalent to the Principle of Mathematical Induction.

If $A = \{1, 2, 3, ..., n\}$ then a relation $R \subseteq A \times A$ can be represented by a **zero-one matrix** M of size $n \times n$ where $(M)_{ij} = 1$ if $(i, j) \in R$ and $(M)_{ij} = 0$ if $(i, j) \notin R$.

Example: Suppose $A = \{1, 2, 3\}$ and $R = \{(1,1), (1,3), (2,1), (3,2), (3,3)\}$. Then the zero-one matrix of R is $M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

4.19 Represent the relations given in Problem 4.4 using zero-one matrices.

4.20 Convert these zero-one matrices to digraphs.

a) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ b) $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ c) $\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ d) $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

The **transitive closure** of $R \subseteq A \times A$ is the smallest transitive relation containing R.

Theorem: The transitive closure of R is given by $R \cup R^2 \cup ... \cup R^n$ where $n = |A|$.

4.21 Let $A = \{1, 2, 3, 4\}$. Use this theorem to find the transitive closure of $R \subseteq A \times A$.

a) $R = \{(1, 2), (2, 1), (2, 3), (3, 4)\}$
b) $R = \{(1, 1), (1, 2), (2, 1), (4, 3)\}$
c) $R = \{(1, 1), (1, 4), (2, 1), (2, 2), (3, 3), (4, 4)\}$
d) $R = \{(1, 4), (2, 1), (2, 4), (3, 2), (3, 4), (4, 3)\}$

4.22 Find the zero-one matrix of the transitive closure for each R in Problem 4.20.

Chapter 5
Functions

A relation from a set A to another set B means a subset of $A \times B$. A **function** f from A to B, denoted by $f : A \to B$, is a relation such that $\forall a \in A\ \exists!(a, b) \in f$.

Example: Let $R \subseteq \{1, 2, 3, 4\} \times \{x, y, z\}$ defined by

1) $R = \{(1,x), (2,y), (3,z), (4,x)\}$
2) $R = \{(1,x), (2,x), (3,x), (4,y)\}$
3) $R = \{(1,z), (2,y), (3,x)\}$
4) $R = \{(1,y), (2,x), (3,y), (3,z), (4,x)\}$

The first two relations are functions but not the last two.

5.1 Suppose $R \subseteq A \times A$. How can we tell from the digraph, or the zero-one matrix, whether or not R is a function from A to A?

5.2 Which ones of the zero-one matrices in Problem 4.20 represent a function?

5.3 Which relations are functions?

a) $R = \{(a, b) \in$ Ɛ × Ʊ $\mid b = a + 1\}$
b) $R = \{(a, b) \in \mathbb{R} \times \mathbb{Z} \mid b = [a]\}$
c) $R = \{(a, b) \in \mathbb{N} \times \mathbb{Z} \mid b^2 = a\}$
d) $R = \{(a, b) \in \mathbb{N} \times \mathfrak{I} \mid b = \sqrt{a}\}$

If $f : A \to B$ is a function then the statement $(a, b) \in f$ can also be written $f(a) = b$. The set A in this relation is called the **domain** of f while B the **codomain** of f. The **range** of f is the subset of B given by $f(A) = \{f(a) \in B \mid a \in A\}$. In Calculus a function is sometimes given in the form $y = f(x)$ whereas its domain and range may be implicit. For example $f(x) = x^2$ is really the function $f = \{(x, x^2) \mid x \in \mathbb{R}\}$ with domain $\mathbb{R}$ and range $[0, \infty)$.

5.4 Find the largest possible domain and range of each function.

a) $f(x) = |x|$
b) $f(x) = \sqrt{x}$
c) $f(x) = 1/x$
d) $f(x) = 1/\sqrt{x}$
e) $f(x) = [x]$

5.5 Let $f : A \to B$ be a function and let S and T be subsets of A. Prove the following.

a) $f(S \cup T) = f(S) \cup f(T)$
b) $f(S \cap T) \subseteq f(S) \cap f(T)$

Properties of a function $f : A \to B$.

1) f is **one-to-one** or an **injection** if $f(a) = f(a') \to a = a'$.
2) f is **onto** or a **surjection** if $f(A) = B$.
3) f is a **bijection** if both one-to-one and onto.

Example: All the following are functions $f : A \to B$.

1) $A = \{1, 2, 3\}$, $B = \{x, y, z, w\}$, $f = \{(1,y), (2,z), (3,w)\}$
2) $A = \{1, 2, 3\}$, $B = \{x, y, z, w\}$, $f = \{(1,y), (2,w), (3,w)\}$
3) $A = \{1, 2, 3\}$, $B = \{x, y, z\}$, $f = \{(1,y), (2,z), (3,x)\}$
4) $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$, $f = \{(1,y), (2,z), (3,y), (4,x)\}$

The first is one-to-one but not onto.
The second is neither one-to-one nor onto.
The third is both one-to-one and onto.
The fourth is onto but not one-to-one.

5.6 Is *f* one-to-one? onto? both?

a) $f = \{(a, b) \in$ Ɛ × Ʊ $\mid b = a + 1\}$
b) $f = \{(a, b) \in \mathbb{R} \times \mathbb{Z} \mid b = [a]\}$
c) $f = \{(a, b) \in \mathbb{N} \times \mathbb{Z} \mid b = -a\}$
d) $f = \{(a, b) \in \mathbb{Z} \times$ Ɛ $\mid b = 2a\}$

The **inverse** of a function $f : A \to B$ is the relation $f^{-1} \subseteq B \times A$ given by $f^{-1}(b) = a \leftrightarrow f(a) = b$. Note that f^{-1} may or may not be a function. Moreover if $S \subseteq B$ then the **inverse image** of S is the subset of A given by $f^{-1}(S) = \{a \in A \mid f(a) \in S\}$.

5.7 Find f^{-1} for each function given in Problem 5.4. Is f^{-1} a function?

5.8 Repeat the question using Problem 5.5.

5.9 Let $f : A \to B$ be a function and let S and T be subsets of B. Prove the following.

a) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$
b) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$

Suppose there are two functions $f : A \to B$ and $g : B \to C$. The **composition** function $g \circ f : A \to C$ is defined by $g \circ f(a) = c \leftrightarrow f(a) = b \wedge g(b) = c$. In particular when $A = B = C$ this definition coincides with that of arbitrary relations on A.

5.10 Find $g \circ f$. Assume you know the appropriate domain and range for each.

a) $f(x) = x$, $g(x) = x^2$
b) $f(x) = x + 1$, $g(x) = x - 1$
c) $f(x) = 2x + 1$, $g(x) = x^2 - 2$
d) $f(x) = 1/x$, $g(x) = 1/x$

5.11 Suppose $f^{-1} : B \to A$ is again a function. Prove that $f^{-1} \circ f(a) = a \; \forall a \in A$ and that $f \circ f^{-1}(b) = b \; \forall b \in B$. Verify these facts using each function given in Problem 5.5 when applicable.

Theorem: The inverse of $f : A \to B$ is again a function if and only if f is a bijection, in which case $f^{-1} : B \to A$ is also a bijection.

Chapter 6
Cardinality

A set is called **finite** or **infinite** depending whether its number of elements is finite or infinite, respectively.

6.1 Suppose both A and B are finite sets. Prove the following statements.

a) $\exists$ injection $f: A \to B \leftrightarrow |A| \leq |B|$
b) $\exists$ surjection $f: A \to B \leftrightarrow |A| \geq |B|$
c) $\exists$ bijection $f: A \to B \leftrightarrow |A| = |B|$
d) If $|A| = |B|$ then any function $f: A \to B$ is one-to-one if and only if onto.

We now generalized the definition of cardinality to infinite sets. For arbitrary set A we associate to it a **cardinal number** $|A|$ satisfying the following properties.

1) $|A| = |B|$ if $\exists$ bijection $f: A \to B$
2) $|A| \leq |B|$ if $\exists$ injection $f: A \to B$
3) $|A| < |B|$ if $|A| \leq |B| \wedge |A| \neq |B|$

Note that the above definitions coincide with the properties of cardinality for finite sets.

Theorem: $|A| \leq |B| \wedge |B| \leq |A| \to |A| = |B|$ (Cantor-Schroeder-Bernstein)

Define $|\mathbb{N}| = \aleph_0$ and call a set A **countable** if $|A| \leq \aleph_0$ or **uncountable** if $|A| > \aleph_0$. For example $\mathbb{N}$ is itself countable under the bijection $f(n) = n \ \forall n \in \mathbb{N}$.

6.2 Prove that the following sets are countable.

a) Ɛ ∩ [1,1000]
b) Ɛ ∩ $\mathbb{N}$
c) Ɛ
d) Ʊ

Theorem: For any set A, exactly one of the following statements must be true:

1) $|A| < \aleph_0$
2) $|A| = \aleph_0$
3) $|A| > \aleph_0$

6.3 Prove that A is finite if and only if $|A| < \aleph_0$.

The above problem says that all finite sets are countable, but not conversely since there exist countable sets which are infinite such as $\mathbb{N}$. In some Mathematics books, an infinite set which is countable is called **denumerable** while in other books the definition of countable sets does not include finite sets.

6.4 Prove the following statements.

a) A subset of a countable set is countable.
b) The union of two countable sets is countable.
c) The cross product of two countable sets is countable.
d) The countable union of countable sets is countable.

6.5 Prove that $\mathbb{Z}$ and $\mathbb{Q}$ are both countable. In particular $|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

Theorem: $\mathbb{R}$ is uncountable. (Cantor)

We define $|\mathbb{R}| = c$, the **cardinality of the continuum**.

6.6 Prove that $|A| < |P(A)|$ for any set A.

Problem 6.6 implies that $\aleph_0 = |\mathbb{N}| < |P(\mathbb{N})|$ and so $P(\mathbb{N})$ is also uncountable. In particular it can be shown that $|P(\mathbb{N})| = c$. **Cantor's Continuum Hypothesis** asserts that there is no cardinal number strictly between $\aleph_0$ and c. There are however cardinal numbers larger than c, for instance $|P(\mathbb{R})|$, $|P(P(\mathbb{R}))|$, etc.