Notes for Chapter 1

1. In this class, we adopt an informal approach to set theory. A set is a collection of things called elements. We use the notation \( x \in A \) to denote that \( x \) is an element of the set \( A \). We use the notation \( x \notin A \) to denote that \( x \) is not an element of the set \( A \). Two sets are equal if and only if they contain exactly the same elements. A set \( S \) may be either finite or infinite. If \( S \) is a finite set, the cardinality of \( S \) denoted \(|S|\) is the number of elements in \(|S|\).

2. The unique set with cardinality zero is called the empty set and denoted \( \emptyset \).

3. We let \( \mathbb{R} \) denote the set of real numbers, \( \mathbb{Q} \) the set of rational numbers, \( \mathbb{Z} \) the set of integers, \( \mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \} \), and \( \mathbb{N} \) the set of positive integers, \( \mathbb{N} = \{1, 2, 3, \ldots \} \).

4. We often use set builder notation to define a set. For example, the set of rational numbers is given by
   \[
   \mathbb{Q} = \{x \in \mathbb{R} : x = \frac{p}{q} \text{ for some } p, q \in \mathbb{Z} \text{ with } q \neq 0\}.
   \]

5. Suppose that \( A \) and \( B \) are sets. We let \( A \times B \) denote the set of ordered pairs \( (a, b) \) such that \( a \in A \) and \( b \in B \). Two ordered pairs \( (c, d) \) and \( (v, w) \) are equal if and only if \( c = v \) and \( d = w \).

6. More generally, if \( n \) is a positive integer and \( A_1, A_2, \ldots A_n \) are sets, we define the Cartesian product of these sets by
   \[
   A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n \}.
   \]
   The expression \( (x_1, x_2, \ldots, x_n) \) is called an ordered \( n \)-tuple. Two ordered \( n \)-tuples \( (x_1, x_2, \ldots, x_n) \) and \( (y_1, y_2, \ldots, y_n) \) are equal if and only if \( x_i = y_i \) for each \( i = 1, 2, \ldots, n \). Note the meaning of \( \ldots \) (dots).
7. If $A$ is a set and $n$ is a positive integer we define the Cartesian power $A^n$ by

$$A^n = A_1 \times A_2 \times \cdots \times A_n,$$

where $A_i = A$ for each $i = 1, 2, \ldots, n$.

8. Suppose that $A$ and $B$ are sets. We say that $A$ is a subset of $B$, denoted $A \subseteq B$, if and only if every element of $A$ is also an element of $B$. We note that two sets $A$ and $B$ are equal if and only if $A \subseteq B$ and $B \subseteq A$.

9. Note that for any set $A$, we have $\emptyset \subseteq A$.

10. Suppose that $A$ and $B$ are sets. We assume that there exist sets $A \cap B$, $A \cup B$, and $A - B$ given by

- $x \in A \cap B$ if and only if $x \in A$ and $x \in B$,
- $x \in A \cup B$ if and only if $x \in A$ or $x \in B$,
- $x \in A - B$ if and only if $x \in A$ and $x \notin B$.

These sets are called the intersection, union, and difference of the sets $A$ and $B$. The notation $A \setminus B$ is often used instead of $A - B$.

11. If $A$ is a set, we assume that there exists a unique set $S$ such that $x \in S$ if and only if $x \subseteq A$. This set is called the power set of $A$ and is denoted by $\mathcal{P}(A)$. So $x \in \mathcal{P}(A)$ if and only if $x \subseteq A$. Note that if a finite set $A$ has $n$ elements, then $\mathcal{P}(A)$ is a finite set which has $2^n$ elements.

12. Suppose that $S$ is a set, and for each $s \in S$, a set $A_s$ is defined. We assume that there are sets denoted by $\bigcup_{s \in S} A_s$ and $\bigcap_{s \in S} A_s$ such that $x \in \bigcup_{s \in S} A_s$ if and only if there exists $s \in S$ with $x \in A_s$, and $x \in \bigcap_{s \in S} A_s$ if and only if for every $s \in S$ we have $x \in A_s$.

The set $S$ is called an index set, the family of sets $A_s$ is called an indexed family of sets, the set $\bigcup_{s \in S} A_s$ is called the union of the indexed family of sets, and the set $\bigcap_{s \in S} A_s$ is called the intersection of the indexed family of sets.

If $S = \{1, 2, \ldots, n\}$, instead of $\bigcup_{s \in S} A_s$ we often write $\bigcup_{i=1}^n A_i$ or $A_1 \cup A_2 \cup \cdots \cup A_n$. 
If \( S = \mathbb{N} \), instead of \( \bigcup_{s \in S} A_s \) we often use the notation \( \bigcup_{i=1}^{\infty} A_i \) or \( A_1 \cup A_2 \cup \ldots \).
The same is true for \( \bigcap_{s \in S} A_s \).

13. Sometimes, we restrict attention to subsets of some understood larger set, which we call a universal set or universe. If a universal set \( U \) is understood, we may define the complement of a set \( B \). (If it is not clear what the universe is we say the complement of \( B \) in \( U \).) In our text, the complement of \( B \) is denoted by \( \overline{B} \) and given by \( \overline{B} = U - B \).

14. Before we begin to prove some results, we will accept some things as facts. We will accept the basic properties of real numbers (see the link on the course website). Also,

\[ \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}. \]

In addition, we will accept the following as facts.

15. **Fact** Any nonempty subset of \( \mathbb{N} \) has a smallest element.

16. **Fact** Any finite nonempty subset of \( \mathbb{R} \) has a largest element and a smallest element.

17. **Fact and Notation.** If \( x \in \mathbb{R} \) and \( x \geq 0 \), then there is a unique \( y \in \mathbb{R} \) such that \( y \geq 0 \) and \( y^2 = x \). This number \( y \) is denoted by \( \sqrt{x} \).

18. **Fact.** If \( a, b \in \mathbb{Z} \), then \( a + b \in \mathbb{Z} \), \( -a \in \mathbb{Z} \), \( ab \in \mathbb{Z} \), and \( a - b \in \mathbb{Z} \).

19. **Fact (The Division Algorithm).** If \( a, b \in \mathbb{Z} \) and \( b > 0 \), then there exist unique integers \( q \) and \( r \) such that \( a = qb + r \) and \( 0 \leq r < b \).
Notes for Chapter 2

20. A **statement** is a sentence that is either definitely true or definitely false. An **open sentence** is a sentence whose truth depends on the value of one or more variables. If $P$ and $Q$ are statements or open sentences, we can form three new expressions:

$P \land Q$ (and)

$P \lor Q$ (or)

$\sim P$ (negation)

See the truth tables for these expressions on page 15 of the text.

21. We can also form more complicated logical expressions such as

$$(P \land Q) \lor (\sim P \land \sim Q)$$

and construct truth tables.

22. We say that two logical expressions $P$ and $Q$ are logically equivalent if and only if $P$ is true whenever $Q$ is true, and $P$ is false whenever $Q$ is false. See the laws on page 52 of the text.

23. A logical expressions which is always true is called a tautology. A logical expressions which is always false is called a contradiction.

24. If $P$ and $Q$ are statements, we can also form the two new statements:

$P \implies Q$ (implies) (conditional statement)

$P \iff Q$ (is equivalent to) (biconditional statement).

See the truth tables for these statements on pages 43 and 47 of the text.

25. Note that $P \implies Q$ is equivalent to $\sim P \lor Q$, and $\sim (P \implies Q)$ is equivalent to $P \land \sim Q$.

26. Also, $P \lor Q$ is equivalent to $\sim P \implies Q$. This equivalence is often used to prove a statement of the form $P \lor Q$.

27. **Contrapositive Law.**

$P \implies Q$ is equivalent to $\sim Q \implies \sim P$. 
28. If $C$ is a contradiction, then $(P \land \sim Q) \Rightarrow C$ is equivalent to $P \Rightarrow Q$. This fact, is the basis for proof by contradiction, which we will discuss later.

29. Here are some ways to express the statement $P \Rightarrow Q$:
   - If $P$ then $Q$.
   - $P$ implies $Q$.
   - $P$ is a sufficient condition for $Q$.
   - $Q$ is a necessary condition for $P$.
   - $P$ only if $Q$.

30. Here are some ways to express the statement $P \Leftrightarrow Q$:
   - $P$ if and only if $Q$.
   - $Q$ is a necessary and sufficient condition for $P$.

31. The converse of a statement $P \Rightarrow Q$ is the statement $Q \Rightarrow P$. The converse of a true statement need not be true.

32. We introduce the universal quantifier $\forall$ and the existential quantifier $\exists$. A statement of the form $\forall x, P(x)$ means that for all $x$ in the universe $P(x)$ is true. A statement of the form $\forall x \in B, P(x)$ means that for all $x$ in the set $B$, $P(x)$ is true. A statement of the form $\exists x, P(x)$ means that there exists $x$ in the universe such that $P(x)$ is true. A statement of the form $\exists x \in B, (P(x))$ means that there exists $x$ in the set $B$ with $P(x)$ true. In mathematics the words ”for some $x$” mean ”there exists $x$”.

33. Quantifier Negation laws:
   - $\sim (\exists x \in A, P(x))$ is equivalent to $\forall x \in A, \sim P(x)$.
   - $\sim (\forall x \in A, P(x))$ is equivalent to $\exists x \in A, \sim P(x)$.

34. Many mathematical statements are in the form
   \[ \forall x \in A (P(x) \Rightarrow Q(x)). \]
   Sometimes, this will be shortened to $(P(x) \Rightarrow Q(x))$. When this is done, the $\forall x \in A$ is understood.
To prove a statement of this form, we begin the proof with "Suppose $x \in A$ and $P(x)$." Then we prove $Q(x)$. Sometimes the "$x \in A$" is understood but not explicitly stated.

35. Here are three rules of inference that we sometimes use.

(modus ponens) If $P$ and $P \Rightarrow Q$ are both true, we can conclude that $Q$ is true.

(modus tollens) If $Q$ is false and $P \Rightarrow Q$ is true, we can conclude that $P$ is false.

(elimination) If $P \lor Q$ is true and $P$ is false, then $Q$ is true.

Notes for Chapter 4

36. Here are some important term that are use in mathematics.

A **theorem** is a mathematical statement that has been verified to be true.

A **proof** of a theorem is a written verification that shows that the theorem is unequivocally true.

Sometimes in mathematical material the word **proposition** is used in place of the word theorem. The most significant results are called theorems, and the other results are called proposition.

A **lemma** is a theorem whose main purpose is to prove another theorem.

A **corollary** is a result which follows easily from another theorem.

37. To prove a statement of the form $P \Rightarrow Q$ with a direct proof:

Begin the proof with "Suppose $P$"

End the proof with "Therefore $Q$."

38. **Definition.** An integer $n$ is **even** if and only if $n=2a$ for some $a \in \mathbb{Z}$.

39. **Remark.** It is a common convention in mathematics to use "if" instead "if and only if" in definitions. With this convention it is understood that the word "if" means "if and only if". This convention
is used in the text, but not in these notes. On the other hand in mathematical theorems, this convention is never used. In theorems, ”if” always has a different meaning than ”if and only if”.

40. **Definition.** An integer $n$ is **odd** if and only if $n=2a+1$ for some $a \in \mathbb{Z}$.

41. **Proposition.** An integer $n$ is either even or odd, but not both even and odd.

42. **Definition.** Two integers have the same parity if and only if they are both even or both odd. Two integers have the opposite parity if and only if they do not have the same parity.

43. **Definition.** Suppose $a$ and $b$ are integers. We say that $a$ divides $b$, written $a|b$ if and only 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 $a$.

44. **Proposition.** Suppose that $n$ and $k$ are positive integers and $k|n$. Then $k \in \{1, 2, \ldots, n\}$.

45. **Definition.** Suppose that $n$ is an integer with $n \geq 2$. We say that $n$ is **composite** if and only if there exists a divisor $b$ of $n$ with $1 < b < n$. We say that $n$ is **prime** if and only if $n$ is not composite.

46. **Remark.** Suppose that $n$ is an integer with $n \geq 2$. Then $n$ is prime if and only if $n$ has exactly two positive divisors, 1 and $n$.

47. **Definition.** Suppose that $a$ and $b$ are integers, not both zero. The greatest common divisor of $a$ and $b$, denoted $gcd(a, b)$, is the largest integer that divides both $a$ and $b$.

48. **Definition.** Suppose that $a$ and $b$ are non-zero integers. The least common multiple of $a$ and $b$, denoted $lcm(a, b)$, is the smallest positive integer that is a multiple of both $a$ and $b$.

49. **Proposition.** If $a, b, c \in \mathbb{N}$, then $lcm(ca, cb) = c \cdot lcm(a, b)$.
Notes for Chapter 5

To prove a statement of the form $P \Rightarrow Q$ by contrapositive, begin the proof with: ”Suppose $\sim Q.”$ End the proof with: ”Therefore $\sim P.$

50. Definition. Let $m \geq 1$ be an integer, and let $x$ and $y$ be integers. We say that $x$ is congruent to $y$ modulo $m$ if and only if $m$ divides $x - y.$ We use the notation,

$$x \equiv y \pmod{m}.$$

Notes for Chapter 6

51. To prove a statement of the form $P \Rightarrow Q$ with a proof by contradiction: Begin the proof with ”Suppose $P.”$

Next say: ”Proceeding by contradiction, suppose $\sim Q.$

End the proof by proving a contradiction (a statement of the form $R \land \sim R$).

Sometimes either $R$ or $\sim R$ is something known by a previous result.