Proofs (with the notations of Logic), Two-Column Proofs

Recall that any valid deduction is called a theorem. Establishing validity of a given theorem or providing a completely convincing explanation that a given deduction is valid is called a proof of the theorem. Giving a proof of a theorem may be tedious. To ease the process, in a proof we may use (relatively short) valid deductions (i.e., theorems), whose are already known. We list below theorems that will be used frequently in proofs.

Remark (Rules of Propositional Logic, see Exercise 3.31 in textbook)

Each of the following is a valid deduction (i.e., a theorem).

1) (repeat) $P, \therefore P$

2) ($\wedge$-introduction) $P, Q, \therefore P \wedge Q$

3) ($\wedge$-elimination) $P \wedge Q, \therefore P$ $\quad P \wedge Q, \therefore Q$

4) ($\vee$-introduction) $P, \therefore P \vee Q$ $\quad Q, \therefore P \vee Q$

5) ($\vee$-elimination) $P \vee Q, \neg P, \therefore Q$ $\quad P \vee Q, \neg Q \therefore P$

6) ($\Rightarrow$-elimination) $P \to Q, P, \therefore Q$

7) ($\Leftrightarrow$-introduction) $P \to Q, Q \to P, \therefore P \leftrightarrow Q$

8) ($\Leftrightarrow$-elimination) $P \leftrightarrow Q, \therefore P \to Q$ $\quad P \leftrightarrow Q, \therefore Q \to P$

9) (proof by cases) $P \vee Q, P \to R, Q \to R, \therefore P \vee Q \to R$

10) ($\Rightarrow$-introduction) $P, \therefore Q \to P$

11) ($\forall$-elimination, or Universal instantiation) $\forall x\, P(x), \therefore P(a)$ where a is an arbitrary element of the universe

12) ($\forall$-introduction, or Universal generalization) $P(a), \therefore \forall x\, P(x)$ where a is an arbitrary element of the universe

13) ($\exists$-elimination, or Existential instantiation) $\exists x\, P(x), \therefore P(a)$ where a is some element of the universe

14) ($\exists$-introduction, or Existential generalization) $P(a), \therefore \exists x\, P(x)$ where a is some element of the universe

(Other notations and terminology in other books)

2) (Conjunction) $\dfrac{P \quad Q}{P \wedge Q}$

3) (Conjunctive simplication) $\dfrac{P \wedge Q}{P}$

4) (Disjunctive amplification) $\dfrac{P}{P \vee Q}$

5) (Disjunctive Syllogism) $\dfrac{P \vee Q \quad \neg P}{Q}$

6) (Modus Ponens) $\dfrac{P \to Q \quad P}{Q}$

15) $\dfrac{P \to Q \quad Q \to R}{P \to R}$ (Syllogism)

16) $\dfrac{P \to Q \quad \neg Q}{\neg P}$ (Modus tollens)

Proof : Exercise

The above remark is called "Rules of Inferences" or "Basic Logical Implication" in some books.

When writing a proof of a theorem with the notations of Logic we usually use the technique of two-column proofs. Although examples will explain it well, let us explain its format briefly: To prove a theorem $A_1, A_2, \ldots, A_n, \therefore B$ we first write each hypotheses in different lines, and draw a horizontal line below the hypotheses. Below the horizontal line, in each line we use the assertions appearing above the present line and use some known theorems (i.e., theorems in the above remark) to obtain new assertions. Of course, at the end we want to obtain the conclusion B. Each line is numbered in the left margin for easy reference. Each assertions lies on the left of the line, and on the right we write justification of the assertion on the left (i.e., how is it obtained?)

1) A_1 , hypothesis
2) A_2 , hypothesis
⋮
n) A_n , hypothesis

⋮

m) B , k) and l) by the theorem ...

left column — right column (So we have two columns, motivating the name of "two-column proof")

Ex: Establish the validity of the following deductions (Write proofs for the following theorems)

(a) $P,\ P \to Q,\ S \vee R,\ R \to \neg Q,\ \therefore S \vee T$

(b) $U \to Q,\ P \vee S,\ P \to (Q \to R),\ \neg S,\ \therefore \neg R \to \neg U$

(c) $\forall x\,(A(x) \to B(x)),\ \exists x\,(A(x) \wedge \neg C(x)),\ \forall x\,[(A(x) \wedge B(x)) \to C(x)],\ \therefore \exists x\,(\neg D(x))$

Sol: (a) 1) P , hypothesis
2) $P \to Q$, hypothesis
3) $S \vee R$, hypothesis
4) $R \to \neg Q$, hypothesis

---

5) Q , $\to$-elimination (lines 1) and 2))
6) $\neg R \vee \neg Q$, the equivalence "$M \to N \equiv \neg M \vee N$" (line 4))
7) $\neg\neg Q$, double negation (line 5))
8) $\neg R$, $\vee$-elimination (lines 6) and 7))
9) S , $\vee$-elimination (lines 3) and 8))
10) $S \vee T$, $\vee$- introduction (line 9))

(b) 1) $U \to Q$, hypothesis
2) $P \vee S$, hypothesis
3) $P \to (Q \to R)$, hypothesis
4) $\neg S$, hypothesis

---

5) P , $\vee$-elimination, lines 2) and 4)
6) $Q \to R$, $\to$-elimination, lines 3) and 5)
7) $U \to R$, "$A \to B, B \to C, \therefore A \to C$" , lines 1) and 6)
8) $\neg R \to \neg U$, "every implication is equivalent to its contrapositive", line 7)

(c) 1) $\forall x (A(x) \wedge B(x))$, hypothesis
2) $\exists x (A(x) \wedge \neg C(x))$, hypothesis
3) $\forall x [(A(x) \wedge D(x)) \to C(x)]$, hypothesis

---

4) $A(a) \wedge \neg C(a)$, $\exists$- elimination, line 2), (for some a!)
5) $A(a) \wedge B(a)$, $\forall$-elimination, line 1)
6) $(A(a) \wedge D(a)) \to C(a)$, $\forall$-elimination, line 3)
7) $\neg C(a)$, $\wedge$-elimination, line 4)
8) $\neg (A(a) \wedge D(a))$, "$M \to N, \neg N, \therefore \neg M$", line 6)
9) $\neg A(a) \vee \neg D(a)$, DeMorgan's Laws, line 8)
10) $A(a)$, $\wedge$-elimination, line 4)

11) $\neg\Delta(a)$, V-elimination, lines 9) and 10)

12) $\exists x \neg\Delta(x)$, $\exists$-introduction, line 11)

Subproofs, assumptions:

Suppose we are trying to prove a given theorem $A_1, A_2, \ldots, A_n \therefore B$. We should accept that each hypothesis A_i is true. We may wonder which conclusions, possibly other than B, can be derived from the hypotheses A_i if we add another hypothesis M to hypotheses A_i. Suppose we manage to derive the conclusion N from the hypotheses $A_1, A_2, \ldots, A_n, M$. Therefore $M \to N$ must be true under the acceptance that hypotheses $A_1, A_2, \ldots, A_n$ are all true, and so we may use $M \to N$ in the proof the given theorem. Here, M is called assumption. The derivation of N is called a subproof. In the two column proof we indent all the lines between the assumption M and the conclusion N. That is, we indent the subproof. We cannot use a line from a subproof in the proof the given theorem, we can only use $M \to N$. The proof of the given theorem will be of the form:

1) A_1 , hypothesis
2) A_2 , hypothesis

n) A_n , hypothesis

)

⋮

)

k) M, assumption (want N)

⋮

ℓ) N, ...

) $M \to N$, $\Rightarrow$-introduction, lines k) and ℓ)

subproof

⋮

) B

Direct proofs: If the conclusion of a theorem is an implication $M \to N$, then it is reasonable to make assumption M and obtain N in a subproof. Since we obtain $M \to N$ by deriving N under the assumption M and the hypotheses of the theorem (i.e., in a direct way), this proof may be called a direct proof. Why it works follow from the following logical equivalence

Remark: $A \to (B \to C) \equiv (A \wedge B) \to C$

In particular, the following two deductions

$P_1, P_2, \ldots, P_n, \therefore B \to C$ and $P_1, P_2, \ldots, P_n, B, \therefore C$

are both valid or both invalid.

Proof: Exercise

Ex: Write a proof for the theorem $U \to Q, P \vee S, P \to (Q \to R), \neg S, \therefore \neg R \to \neg Q$

Sol:

1)	$U \to Q$	, hypothesis
2)	$P \vee S$	, hypothesis
3)	$P \to (Q \to R)$	, hypothesis
4)	$\neg S$	, hypothesis
5)	$\neg R$	, assumption (want $\neg Q$)
6)	P	, $\vee$-elimination, lines 2) and 4)
7)	$Q \to R$	, $\Rightarrow$-elimination, lines 3) and 6)
8)	$\neg Q \vee R$	, "$A \to B \equiv \neg A \vee B$", line 7)
9)	$\neg Q$	, $\vee$-elimination, lines 5) and 8)
10)	$\neg R \to \neg Q$	, $\Rightarrow$-introduction, lines 5) and 6)

subproof ↓

1)	$U \to Q$	,
2)	$P \vee S$	,
3)	$P \to (Q \to R)$	,
4)	$\neg S$	
5)	P	,
6)	$Q \to R$	,
7)	$\neg R$	, assumption
8)	$\neg Q \vee R$	,
9)	$\neg Q$	
10)	$\neg R \to \neg Q$	,

Subproofs may begin at any line

Proof by contradiction: A usual way to prove that an assertion A is true is to show that A cannot be false (equivalently, its negation $\neg A$ cannot be true). We do this by considering what would happen if $\neg A$ were true. If we can show that the assumption $\neg A$ is true leads to a contradiction (i.e., $P \wedge \neg P$), then we can

conclude that the assumption $\neg A$ is true was wrong, and so A must be true. This method of proof is called **proof by contradiction**. Suppose we are required to write a proof for a given theorem by using this method. We first assume that what we are trying to prove (i.e., the conclusion of the theorem) is false, and then use this assumption and the hypotheses of the theorem in order to get a contradiction (i.e., $P \wedge \neg P$). Why it works follows from the following logical equivalence.

Remark: $A \to B \equiv (A \wedge \neg B) \to F_0$, where $F_0 = P \wedge \neg P$ is a contradiction.

In particular, the following deductions

$P_1, P_2, \ldots, P_n \therefore Q$ and $P_1, P_2, \ldots, P_n, \neg Q \therefore F_0$

are both valid or both invalid.

Proof: Exercise

Ex: Prove the following theorem by proof by contradiction

$\neg P \to Q, Q \to R, \neg R \therefore P$

Sol:

1)	$\neg P \to Q$	hypothesis
2)	$Q \to R$	hypothesis
3)	$\neg R$	hypothesis
4)	$\neg P$	assumption (for a contradiction)
5)	Q	$\Rightarrow$-elimination, lines 1) and 4)
6)	R	$\Rightarrow$-elimination, lines 2) and 5)
7)	$R \wedge \neg R$	$\wedge$-introduction, lines 3) and 6), (a contradiction!)
8)	P	$\neg$-introduction, lines 4) and 7)

From lines 4) and 7) $\Rightarrow$-introduction gives

$\neg P \to (R \wedge \neg R)$ (false)

So $\neg P$ must be false

So P must be true

Ex Write a proof by contradiction to the following theorem

$\forall x \left(P(x) \vee Q(x)\right)$, $\forall x \left[(\neg P(x) \wedge Q(x)) \rightarrow R(x)\right]$, $\therefore \forall x \left(\neg R(x) \rightarrow P(x)\right)$

Sol:

1) $\forall x \left(P(x) \vee Q(x)\right)$, hypothesis

2) $\forall x \left[(\neg P(x) \wedge Q(x)) \rightarrow R(x)\right]$, hypothesis

---

3) $\neg \left[\forall x \left(\neg R(x) \rightarrow P(x)\right)\right]$, assumption (for a contradiction)

4) $\neg \left[\forall x \left(R(x) \vee P(x)\right)\right]$, "$M \rightarrow N \equiv \neg M \vee N$", line 3)

5) $\exists x \left(\neg R(x) \wedge \neg P(x)\right)$, Negation, line 4)

6) $\neg R(a) \wedge \neg P(a)$, $\exists$-elimination, line 5), (for some a!)

7) $P(a) \vee Q(a)$, $\forall$-elimination, line 1)

8) $(\neg P(a) \wedge Q(a)) \rightarrow R(a)$, $\forall$-elimination, line 2)

9) $\neg R(a)$, $\S$-elimination, line 6)

10) $\neg (\neg P(a) \wedge Q(a))$, "$M \rightarrow N, \neg N, \therefore \neg M$", lines 8) and 9)

11) $P(a) \vee \neg Q(a)$, De Morgan's Laws, line 10)

12) $\neg P(a)$, $\S$-elimination, line 6)

13) $\neg Q(a)$, $\vee$-elimination, lines 11) and 12)

14) $Q(a)$, $\vee$-elimination, lines 7) and 12)

15) $Q(a) \wedge \neg Q(a)$, $\S$-introduction, lines 13) and 14), (a contradiction)

---

16) $\forall x \left(\neg R(x) \rightarrow P(x)\right)$, $\neg$-introduction, lines 3) and 15)

— o —

Proof strategies (from textbook)

(I) In notations of Logic

There is no simple recipe for doing proofs, and there is no substitute for practice. Here, though, are some rules of thumb and strategies to keep in mind.

- *Work backwards from what you want.* The ultimate goal is to derive the conclusion. Look at the conclusion and ask what the introduction rule is for its main logical operator. This gives you an idea of where you want to be *just before* the last line of the proof. Then you can treat this line as if it were your goal. Ask what you could do to derive this new goal.

  For example: If your conclusion is a conditional $\mathcal{A} \Rightarrow \mathcal{B}$, plan to use the $\Rightarrow$-intro rule. This requires starting a subproof (a separate paragraph) in which you assume $\mathcal{A}$. In the subproof, you want to derive $\mathcal{B}$.

- *Work forwards from what you have.* Look at the hypotheses (and any other assertions that you have derived so far). Think about the elimination rules for the main operators in these assertions. These will tell you what your options are. For example:

  - If you have $\mathcal{A} \vee \mathcal{B}$, you should think about using a proof by cases.
  - If you have $\mathcal{A} \Rightarrow \mathcal{B}$, you should think about whether you can obtain $\mathcal{A}$ somehow, so that you can apply $\Rightarrow$-elimination.

- *Change what you are looking at.* Replacement rules can often make your life easier; if a proof seems impossible, try out some different substitutions. For example, it is often difficult to prove a disjunction $\mathcal{A} \vee \mathcal{B}$ by using the basic rules; it is often easier to show $\neg\mathcal{A} \Rightarrow \mathcal{B}$, which is a logically equivalent assertion.

  And De Morgan's Laws should become second nature; they can often transform an assertion into a more useful form.

- *Try breaking the proof down into cases.* If it looks like you need an additional hypothesis (P) to prove what you want, try considering two cases: since $P \vee \neg P$ is a tautology ("law of the excluded middle"), it suffices to prove that P and $\neg P$ each yield the desired conclusion.

- *Do not forget proof by contradiction.* If you cannot find a way to show something directly, try assuming its negation, and then look for a contradiction.

- *Repeat as necessary.* After you have made some progress, by either deriving some new assertions or deciding on a new goal that would represent substantial progress, see what the above strategies suggest in your new situation.

- *Persist.* Try different things. If one approach fails, try something else.

(II) In plain English

The goal of a mathematical proof is to provide a completely convincing explanation that a deduction is valid. It needs to be so carefully written that it would hold up in court forever, even against your worst enemy, in any country of the world, and without any further explanation required. Fortunately, the rules of logic are accepted worldwide, so, if applied properly, they create an irrefutable case.

In the previous sections of this chapter, we wrote our proofs in two-column format. We will now start the transition to writing our proofs in English prose: our ideas will be expressed in sentences and paragraphs, using correct grammar, combining words with appropriate mathematical notation. A proof written in prose needs to convey the same information as would be found in a two-column proof, so essentially the same rules and strategies will still apply, but writing in ordinary English provides more freedom, and often leads to shorter proofs that are more reader-friendly.

Remark 4.19. The big advantage of a two-column proof is that the rules are very clear, so it is a good method for beginners who may have difficulty deciding what they are allowed to do. The disadvantage is that

> *"... its confining and verbose format render it of very limited utility to any but the most simple of theorems."*

Just as when using the two-column format, our proofs will be a sequence of assertions that lead from the hypotheses to the desired conclusion. Each assertion must have a logical justification based on assertions that were stated earlier in the proof. Any subproof will form a paragraph of its own within the proof.

Before the proof begins, we always provide a statement of the theorem that will be proved.

- The statement is preceded by the label "Theorem" (or a suitable substitute).
- The statement of the result begins with a list all of the hypotheses. To make it clear that they are assumptions, not conclusions, this list of assertions is introduced by an appropriate word or phrase such as "Assume...," or "Suppose that ...," or "If ...," or "Let ...."
- The statement of the result ends with a statement of the desired conclusion, introduced by an appropriate word or phrase such as "Then ...," or "Therefore, ..."

Following the statement of the result, we begin our proof in a new paragraph.

- The proof is labelled with the single word: "Proof."
- We then proceed to give a series of assertions that logically leads from our hypotheses to the desired conclusion.
- A small square is drawn at the right margin at the end of the proof to signify that the proof is complete.

For example, here is how the chapter's first deduction could be treated:

THEOREM. *Assume:*

a) if the Pope is here, then the Queen and the Russian are both here, and

b) the Pope is here.

Then the Russian is here.

PROOF. From Assumption (b), we know that the Pope is here. Therefore, Assumption (a) tells us that the Queen and the Russian are both here. In particular, the Russian is here. □

Remark 4.20. Note that some of the rules of the two-column format are relaxed for proofs written in prose:

1) We will no longer list all of the hypotheses at the start of our proof. Instead, we refer to the list that is in the statement of the theorem.
2) We will no longer make a practice of numbering all of the assertions in our proofs. However, if there is a particular assertion that will be used repeatedly, we may label it with a number for easy reference.
3) We will usually not cite the basic rules of Propositional Logic by name every time they are used. However, we should be able to justify any assertion with a rule, if called upon to do so.

(III) For quantified assertions:

The proof of an assertion that begins
"there exists $x \in X$, such that..."
will usually be based on the statement "Let $x =$ $\square$,"
where the box is filled with an appropriate element of X.

The proof of an assertion that begins "for all $x \in X$,"
will usually begin with "Let x be an arbitrary element of X"
or, for short, "Given $x \in X$,").

- If you have $\exists x, \mathcal{A}(x)$, you will probably use $\exists$-elimination: assume $\mathcal{A}(c)$ for some letter c that is not already in use, and then derive a conclusion that does not contain c.
- If the desired conclusion is $\forall x \in X, \mathcal{A}(x)$, then your proof will almost certainly be based on $\forall$-introduction, so the first words of your proof will usually be "Given $x \in X$, ...".
- If you have $\forall x, \mathcal{A}(x)$, and it might be helpful to know $\mathcal{A}(c)$ (for some constant c), then you could use $\forall$-elimination.

8C. Theorems, Propositions, Corollaries, and Lemmas

Mathematicians use a number of different names for assertions that can be proved. Sometimes they are called theorems, but other names are also used. In addition to "theorem," the names most commonly used are "lemma," "proposition," and "corollary." There are no hard-and-fast rules for which name to use when, but here are some guidelines.

- A **theorem** is generally a result that the author believes to be important. A theorem may be given a special name, for ease of reference. Often, important theorems are named after the mathematician who first proved them, for example "Hall's Theorem." Sometimes theorems are given names that relate to their content or importance, for example "the Fundamental Theorem of Calculus."
- A **proposition** is a minor theorem. In text books, mathematicians employ the term "proposition" to refer to some result that they do not think is sufficiently important to be called a theorem.
- A **corollary** is a result that can be proved very easily from some other result.
- A **lemma** is generally a minor result that is being used as a stepping stone for proving a more significant result (a theorem, usually). Mathematicians will separate a lemma from the main proof of a theorem either because the proof is long and complicated and needs to be broken down into smaller steps, or because it is a step that needs to be performed repeatedly. It is much easier and clearer to refer to a lemma multiple times,

than to either include the reasoning repeatedly, or refer back to an earlier portion of a single long proof.

Like "theorem," "lemma" is a word that was originally Greek, although it was also adopted into Latin. Although the English plural "lemmas" is quite acceptable, some mathematicians prefer the original plural form of the word, "lemmata."

- A fact is any true assertion, mostly a minor proposition.
- An axiom is a statement that is taken to be true, which cannot be proved or disproved by all the other true assertions. (They are usually intuitively true, and they serve as starting point for developing further theorems)
- A definition is usually of the form " ..... is called ... if ..... ". Here, "if" is equal to "iff".

To sum up, a Theorem / Proposition / Corollary / Lemma / Fact ... is usually stated as

Theorem. Let / Suppose / Assume ..... (hypotheses)

Then ..... (conclusion)

A theorem says that if one assumes that each of its hypothes is True then its conclusion is True. In other words, a theorem says that the implication "its hypotheses $\Rightarrow$ its conclusion" (i.e., "$P_1 \wedge P_2 \wedge \cdots \wedge P_n \to C$" where P_i are hypotheses and C is the conclusion) is True (tautology)

We may also state a theorem as follows

Theorem. Hypotheses $\Rightarrow$ Conclusion

Here theorem says that the implication "Hypotheses $\Rightarrow$ Conclusion" is True (tautology).

A proof of a theorem is a justification of why the Theorem (i.e., "hypothesis $\Rightarrow$ conclusion") is True. In proof written in plain English we don't write each hypothesis because they are already written in the Theorem, but we may refer them whenever necessary. We also don't mention the trivial / obvious / basic rules of inference (such as $\vee$-elimination, $\wedge$-introduction, $\to$-introduction)

A proof of a Theorem is usually written in the following format.

Proof. .....

.....

..... So / Thus / Therefore, the conclusion of the Theorem. □

The box at the end means that the proof is completed. Some books may prefer to write Q.E.D instead of □ to mean that the proof is finished. Q.E.D is the abbreviation for the Latin phrase "Quad erat demonstrandum" (= "what was to be shown").

One usually try to write the following types of proofs depending on the conclusion of the Theorem.

Theorem. Let / Suppose / Assume ..... (hypotheses)
Then ..... if A then B ..... (conclusion)

Proof. Assume / Let / Suppose A. ..... (Assume A, and show B)
..... So, B. □

Theorem. Let / Suppose / Assume ..... (hypotheses)
Then ..... A or B ..... (conclusion)

Proof. Assume / Suppose / Let A is not true... (Assume $\neg A$, and show B)
..... Hence, B. □

Theorem. Suppose / Assume / Let ..... (hypotheses)
Then ..... A ..... (conclusion)

Proof. (Proof will be by contradiction). Assume / Suppose / Let for (a purpose of) contradiction that A is not true. ..... (Assume $\neg A$, and get a contradiction)
..... This is a contradiction because ... / This is impossible because ..... / This is absurd because ..... / This conradicts ..... / This is a contradiction to / with ..... Hence, A. □

Theorem. ..... (hypotheses)

Then, A if and only if B / $A \iff B$ (conclusion)

Proof. ($\Rightarrow$): (The proof of "$A \Rightarrow B$") .....

($\Leftarrow$): (The proof of "$B \Rightarrow A$") ..... □

(Prove $A \Rightarrow B$ and $B \Rightarrow A$)

Theorem. ..... (hypothesis)

Then, the following conditions are equivalent: (Conclusion)

(1) .....

(2) .....

(3) .....

Proof. (Theorem claims that (1) $\equiv$ (2) $\equiv$ (3). That is, the biconditionals (1) $\iff$ (2), (1) $\iff$ (3), (2) $\iff$ (3) are all true. Instead we may prove that the implications

(1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), (3) $\Rightarrow$ (1)

are true, which is logically equivalent to what the conclusion says).

(1) $\Rightarrow$ (2): .....

(2) $\Rightarrow$ (3): .....

(3) $\Rightarrow$ (1): .....

□

Set Theory

A set is a (well defined) collection of objects; these objects are called the elements (or members) of the set. If A denotes a set and a denotes an element of A, we use the notation $a \in A$ (read as "a is an element of A" or "a is in A") to indicate this. The notation $b \notin A$ is defined to be "$\neg(b \in A)$". So, "$b \notin A$" means that "b is not an element of A". We usually use curly braces $\{\ \}$ to write a set by listing its elements in $\{\ \}$. To illustrate sets visually we sometimes draw closed curves or circles and lists its elements in it, which is called Venn diagrams. For instance,

$A = \{1, \square, 2, \star\}$

Venn Diagram for A

Note that $1 \in A$, $\square \in A$, $\heartsuit \notin A$.

A set is determined by its elements. That is, two sets A and B are equal iff A and B have the same elements (With the notations of Logic, $A = B$ iff $\forall x\,(x \in A \leftrightarrow x \in B)$). However, a set is an unordered collection, and repetion of its elements do not change the set, and we usually list its elements without repetion. For instance,

$\{1, 2, a, b\} = \{a, 2, b, 1\}$ and $\{1, 2, 3\} = \{1, 2, 2, 2, 3, 3\}$

We may also use open statements (i.e., predicates) to define specific sets. If P(x) is an open statement then

$\{x \mid P(x)\}$ or $\{x : P(x)\}$ is the set of all x such that P(x) is true,

$\{x \in A \mid P(x)\}$ or $\{x \in A : P(x)\}$ is the set of all x in A such that P(x) is true.

For instance, if $A = \{0,1,2,3,4,5,6,7,8,9\}$ and $P(x) =$ "x is even", then

$\{x \in A \mid P(x)\} = \{x \in A \mid x \text{ is even}\} = \{0, 2, 4, 6, 8\}$.

Notations: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of integers

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ is the set of natural numbers (Some books may assume that $0 \notin \mathbb{N}$)

$\mathbb{Z}^+ = \mathbb{N}^+ = \{1, 2, 3, \ldots\}$ = the set of positive integers / natural numbers.

$\mathbb{Q}$ = the set of rational numbers, $\mathbb{R}$ = the set of real numbers.

Definitions/Remarks: Let A and B be sets.

1) We say that A is a subset of B, and write $A \subseteq B$ (or $A \subset B$ as in the textbook), if every element of A is an element of B.

(With notations of logic) $A \subseteq B$ iff $(\forall x \in A)(x \in B)$

$A \subseteq B$ iff $\forall x\,(x \in A \to x \in B)$

To show that $M \subseteq N$ where M and N are sets, we may do: We take an arbitrary $m \in M$ and then we try to justify that $m \in N$.

Instead of $A \subseteq B$, we may also write $B \supseteq A$. Instead of saying "A is a subset of B", we may also say any of "B is a superset of A"
"B contains A"
"A is contained in B".

If A is not a subset of B, we write $A \not\subseteq B$. Thus, $A \not\subseteq B$ iff there is at least one element $a \in A$ such that $a \notin B$.

(With notations of logic) $A \not\subseteq B$ iff $\neg(A \not\subseteq B)$ iff $\neg(\forall x \in A, x \in B)$

iff $\exists x \in A, x \notin B$

2) We say that A is equal to B, and write $A = B$, if $A \subseteq B$ and $B \subseteq A$

(With the notations of logic) $A = B$ iff $A \subseteq B \wedge B \subseteq A$

iff $\forall x\,(x \in A \to x \in B) \wedge \forall x\,(x \in B \to x \in A)$

iff $\forall x\,(x \in A \to x \in B \wedge x \in B \to x \in A)$

iff $\forall x\,(x \in A \leftrightarrow x \in B)$

To show that $M = N$ where M and N are sets, we may do: we first justify $M \subseteq N$ and then we justify $N \subseteq M$.

3) The union $A \cup B$ of A and B is defined to be the set

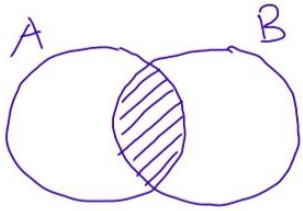
$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

$A \cup B$ is shaded.

To show that $z \in M \cup N$ where M and N sets, we need to justify that either $z \in M$ or $z \in N$; (equivalently we may assume $z \notin M$ and then justify $z \in N$)

4) The intersection $A \cap B$ of A and B is defined to be the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

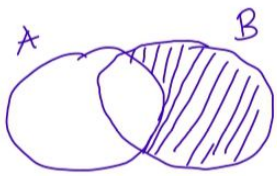


$A \cap B$ is shaded

To show that $z \in M \cap N$ where M and N are sets, we need to justify that both $z \in M$ and $z \in N$.

5) The difference $B - A$ (or $B \setminus A$ as in the textbook) of A in B is defined to be the set

$$B - A = \{x \in B \mid x \notin A\} = \{x \mid x \in B \text{ and } x \notin A\}$$



$B - A$ is shaded

Some books may prefer to say "the (relative) complement of A in B" instead of "the difference of A in B"

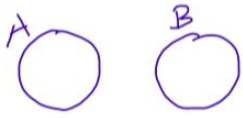
6) We assume that there is a set without any elements. This unique set is called the empty set (or the null set) and denoted by ϕ or $\{\}$. So, it is not the case that there is an element $x \in \phi$; equivalently $\neg(\exists x, x \in \phi)$, which is equivalent to $\forall x, x \in \phi$, so "for all x, we have $x \notin \phi$".

7) We denote by $|A|$ or ($\#A$ as in the textbook) the number of elements of the set. If $|A|$ is finite, then we say that A is a finite set. So A is called a finite set if it has only finitely many elements. If $|A|$ is infinite, then we say that A is an infinite set. Note that the empty set ϕ is finite. For instance, $\mathbb{Z}$ is an infinite set, but $\{1,2,3\}$ is a finite set because $|\{1,2,3\}|=3$ is finite. Note that

$|\{1,2,2,2,3,3\}|=3$ too because repetion of members do not change the set.

In general, $|A|$ is called the cardinality of the set A

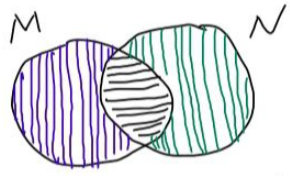
8) We say that A and B are disjoint if $A \cap B = \phi$



The disjoint sets may be important in some counting results in which the cardinality of a union composed of pairwisely disjoint sets. If A_1 and A_2 are disjoint (finite) sets then we easily see that $|A_1 \cup A_2| = |A_1| + |A_2|$. In general, for any two (finite) sets M and N we see that

$$|M \cup N| = |M| + |N| - |M \cap N|$$

$$\left(= \overbrace{|M-N| + |M \cap N|}^{A} \quad \overbrace{|N-M| + |M \cap N|} \right)$$



$|M \cap N|$ is counted twice in $|M|+|N|$

We may define the union and intersection of any number of sets similarly. The union and intersection of (finitely many) sets $S_1, S_2, \ldots, S_n$ are defined as follows:

$$S_1 \cup S_2 \cup \cdots \cup S_n = \{x \mid x \in S_i \text{ for some } i\} \quad \text{(i.e., } x \text{ is in some } S_i\text{)}$$

$$S_1 \cap S_2 \cap \cdots \cap S_n = \{x \mid x \in S_i \text{ for all } i\} \quad \text{(i.e., } x \text{ is in all } S_i\text{)}$$

If S_i are pairwisely disjoint (that means $S_k \cap S_\ell = \phi$ for all k, ℓ with $k \neq \ell$) then we easily see that $|S_1 \cup S_2 \cup S_2 \cup \cdots \cup S_n| = \sum_{i=1}^{n} |S_i|$

For not necessarily pairwisely disjoint sets the cardinality of their union is given by the formula so called "the inclusion-exclusion principle". (Google it).

9) The power set $\mathcal{P}(A)$ of the set A is defined to be the set of all subsets of A. So $\mathcal{P}(A) = \{X \mid X \subseteq A\}$. Hence, $X \in \mathcal{P}(A)$ iff $X \subseteq A$.

We may easily see for a (finite set) A, $|\mathcal{P}(A)| = 2^{|A|}$ (Indeed, let $A = \{a_1, a_2, \ldots, a_n\}$. For a subset S of A we have 2 possibilities for each element $a_i \in A$; either $a_i \in S$ or $a_i \notin S$. As $|A| = n$, we can only have 2^n distinct subsets of A).

10) We say that A is a proper subset of B if $A \subseteq B$ and $A \neq B$. Recalling the equality of sets "$A = B$ iff $A \subseteq B$ and $B \subseteq A$", we see that

A is a proper subset of B iff $A \subseteq B$ but $B \nsubseteq A$.

(With the notations of Logic) A is a proper subset of B iff $(\forall x \in A)(x \in B) \wedge (\exists x \in B)(x \notin A)$

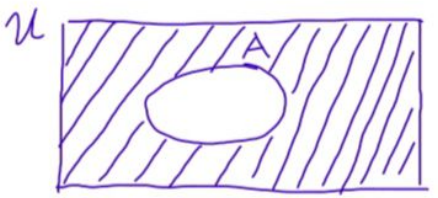
To show that M is a proper subset of N where M and N are sets, we may do: We first take an arbitrary $m \in M$ and then try to justify that $m \in N$ (If it is done, it proves $M \subseteq N$). Finally, we try to find at least one element $n \in N$ such that $n \notin M$ (If it is done, it proves that $N \nsubseteq M$).

Some books may use the notation $A \subsetneq B$ to indicate that A is a proper subset of B.

11) We usually (implicitly) assume that there is a set $\mathcal{U}$, called the universal set (or universe of discourse) such that any set we are considering is a subset of $\mathcal{U}$. This is quite natural in practice. For instance, by the quantified assertion "Everyone is happy", we usually mean everyone in some particular set such as the set of people in our class / family / ..... The assumption of a universal set will

also help us to get rid of some paradoxes, that will be explained later.

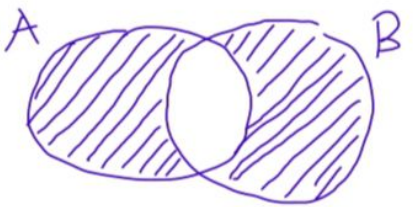
12) The <u>complement</u> A^c is defined to be the set $A^c = \mathcal{U} - A$ where $\mathcal{U}$ is the universal set. We may also use the notation $\overline{A}$ for the complement of A. (Our textbook use this notation $\overline{A}$)



So, $A^c = \{x \mid x \notin A\} = \{x \in \mathcal{U} \mid x \notin A\}$

13) The symmetric difference $A \triangle B$ of A and B is defined to be the set

$$A \triangle B = (A - B) \cup (B - A)$$



<u>Ex:</u> Let $A = \{1,2,3,4,5\}$, $B = \{3,4,5,6,7\}$, $C = \{7,8,9\}$. Then

$A \cap B = \{3,4,5\}$, $A \cap C = \phi$; so A and C are disjoint, but A and B are not disjoint

$A \cup B = \{1,2,3,4,5,6,7\}$, $A - B = \{1,2\}$, $B - A = \{6,7\}$, $C \notin A$,

$\{7\}$ is a proper subset of C, $P(C) = \{\phi, \{7\}, \{8\}, \{9\}, \{7,8\}, \{7,9\}, \{8,9\}, \{7,8,9\}\}$