Chapter 1

Introduction to Proofs

1.1 Preview of Proof

This section previews many of the key ideas of proof and cites [in brackets] the sections where they are discussed thoroughly. All of these ideas are discussed at much greater length throughout the text.

Definition 1. *A **proof** of a theorem is a sequence of statements which demonstrates that the theorem is a logical consequence of prior results [Sections 3.1 and 3.3]. Prior results are results already known to be true prior to the theorem. A proof arranges selected prior results so that the theorem follows logically from them.*

This first example illustrates how prior results and logic combine to make a proof.

Example 1: Suppose we have as prior results these two rules of algebra:
Uniqueness of Addition Rule: $a = b$ if and only if $a + c = b + c$.
The Zero Product Rule: $ab = 0$ if and only if $a = 0$ or $b = 0$.

Theorem: $(x - a)(x - b) = 0$ iff $x = a$ or $x = b$. [*iff* abbreviates *if and only if*]

Proof:

$(x - a)(x - b) = 0$ iff $x - a = 0$ or $x - b = 0$	by the Zero Product Rule.
$x - a = 0$ or $x - b = 0$ iff $x = a$ or $x = b$	by Uniqueness of Addition, twice.

Therefore, $(x - a)(x - b) = 0$ iff $x = a$ or $x = b$. □

This is a proof because the component statements are prior results and the desired conclusion follows logically [Section 1.6].

This proof has the logical form

A iff B	[a prior result] and
B iff C	[another prior result]
implies A iff C	[by logic]

The first two steps are prior results and the third step follows logically from them because the form [Section 1.3] is the tautology [Section 1.6] known as transitivity of the logical connective iff : $[(A \text{ iff } B) \text{ and } (B \text{ iff } C)] \Rightarrow (A \text{ iff } C)$. ◇

Placeholders. The prior results used in Example 1 are stated with placeholders which permit switching letters [Section 2.1]. The letters used in the steps are not the same as the letters used in the cited rule. For example, in the place where Step 1 has

$$(x - a)(x - b) = 0$$

the rule has $ab = 0$.

Nevertheless, the rule applies because ab represents any product, and in the theorem $(x - a)(x - b)$ is a product. In the rule the letters a and b are placeholders.

Definition 2. *A variable (usually a letter) is a* ***placeholder*** *(also known as a* ***dummy variable****) when it is used to hold the place of any expression of its kind (for example, any number or numerical expression), as opposed to representing a particular number. (Definition 15 of quantifiers is relevant.)*

Translation. It is common for theorems to be stated using terms that have been recently defined. Then the terms are translated, using their definitions, and the work is done with the translated version [Figure 2.3.4 and Sections 1.2 and 4.1].

For example, the next theorem could be in a section on set theory shortly after the terms subset and complement were defined [Sections 1.2, 4.1]. In the proof, sentences with those terms are replaced, that is, translated, using their definitions, by equivalent sentences given in terms that are more primitive.

Definition 3. *Two sentences with the same variable are* ***equivalent*** *if and only if they are true for the same values of the variable and false for the same values of the variable. That is, they are true or false together.*

Equivalence can be expressed with the connective if and only if (abbreviated iff) or symbolized by a double arrow, $\Leftrightarrow$, or just written out "is equivalent to".

Example 2: $2x = 10$ is equivalent to $x = 5$. Both are true when $x = 5$. Both are false when $x \neq 5$.

$ab = 0$ is equivalent to $a = 0$ or $b = 0$. ◇

Example 3: Suppose we are studying sets and we have the definitions of *subset* and *complement* as prior results:
Notation for *member*: $x \in S$ is a notation for "x is a member of S."
Definition of *subset*: S is a *subset* of T if and only if (if $x \in S$, then $x \in T$).
Notation for *subset*: $S \subset T$ is a notation for "S is a subset of T ."
Definition of *complement*: $x \in S^c$ if and only if $x \notin S$ (and $x \in U$, the universal set).

Each definition gives a pair of equivalent sentences. By definition of *subset*, "S is a subset of T" is equivalent to "if $x \in S$, then $x \in T$," and both are equivalent to "$S \subset T$" by definition of the notation.

With these prior results we can prove:
Theorem: $S \subset T$ if and only if $T^c \subset S^c$.

Proof:
[Step 1] $S \subset T$ iff $x \in S \Rightarrow x \in T$ by definition of *subset*
[Step 2] iff $x \notin T \Rightarrow x \notin S$ by contrapositive [logic, Theorem 1.4.2]
[Step 3] iff $x \in T^c \Rightarrow x \in S^c$ by definition of *complement*, twice
[Step 4] iff $T^c \subset S^c$ by definition of *subset*. □

The reader is expected to realize that, by transitivity of the logical connective iff, the first sentence is equivalent to the last, so the proof is complete.

This proof used

definitions:	in Steps 1, 3 and 4 [Section 2.3]
notations:	(notations such as $\subset$ and $\notin$ are defined as abbreviations)
logic:	the contrapositive, in Step 2, and the overall logic [Sections 1.3-1.6]
letter-switching:	in Step 3, where the complement of T is used even though the definition uses S, and in Step 4, where the definition of subset is used with T^c in place of S.) [Section 2.1]

◇

Prior Results on the List. A proof is a sequence of sentences (steps). To prove any given result, the steps must be results prior to it.

Definition 4. *We imagine mathematical results to be in sequence on a list, one after another [Section 3.3]. For the proof of any given assertion,* ***prior results*** *consist of*

1) axioms (These are rare. We mention one below as Axiom 12.)

2) definitions (Definitions include notations. Definitions are abbreviations), or

3) proven results that are on the list prior to the given assertion.

The proof in Example 3 is a proof because the logic is correct [Sections 1.3-1.6] and each step is a result prior to the theorem.

Logic. Logic concerns truth and falsehood. The truth of a compound sentence depends upon the truth of its component sentences and the arrangement of its logical connectives [Sections 1.3-1.6].

Definition 5. *There are five basic* ***logical connectives****:*

1) not	*(sometimes symbolized by $\sim$ or $\neg$. We spell out* not.*)*
2) and	*(sometimes symbolized by $\wedge$)*
3) or	*(sometimes symbolized by $\vee$. We spell out* or.*)*
4) if . . . , then . . .	*($\Rightarrow$)*
5) if and only if	*($\Leftrightarrow$)*

Definition 6. *Sentences with the connective* ***if*** *...,* ***then*** *... are called* ***conditional sentences****.*

Example 4: Here is an assertion: "If $x > 5$, then $x^2 > 25$." The assertion uses the connective *if ..., then ...* to make a compound sentence from the two component sentences "$x > 5$" and "$x^2 > 25$." It is a conditional sentence. The assertion is true. For all $x > 5$, $x^2 > 25$. ◇

Sentences with the connective *if ..., then ...* and a variable are interpreted as generalizations.

Definition 7. *A* ***generalization*** *is a declarative sentence that asserts, explicitly or implicitly, that something is always true [Section 2.1].*

Example 4: [continued] The sentence "If $x > 5$, then $x^2 > 25$" is a generalization. It is true for all x. The "for all" wording is suppressed, but understood. It is equivalent to "For all $x > 5$, $x^2 > 25$." It is also equivalent to "For all x, if $x > 5$, then $x^2 > 25$." ◇

Example 5: $x^2 \geq 0$. This is true for all x and is interpreted that way even if the phrase "for all x" is omitted. ◇

Example 6: The sentence "For all $x, 2(x + 1) = 2x + 2$," is a generalization. It is true. It is often abbreviated by leaving off the "For all x" part: "$2(x + 1) = 2x + 2$." The reader is supposed to recognize that the equation is true for each x. ◇

Definition 8. *An equation with a variable which is true for all values of the variable is called an* ***identity****. (An identity may be regarded as an abbreviated generalization, merely lacking an explicit "for all ... ".)*

Example 6: [continued] The equation"$2(x + 1) = 2x + 2$" is an identity. When we attach "for all x" to it (explicitly or implicitly) it becomes a generalization. ◇

An identity is an *equation* with a variable such that the equation is always true (that is, for all values of the variable). A generalization is an *assertion* that something is always true. The assertion could be wrong and the generalization false.

Example 7: Resolve the conjecture: $x^2 \geq x$, for all x. (This might be written, "$x^2 \geq x$," without the "for all x" part.) This conjecture is a generalization.

Definition 9. *In this text the word* ***conjecture*** *is a synonym for* ***statement****, but without any connotation of truth or falsehood. To* ***resolve*** *a conjecture means to decide if it is true or false, and to prove it if it is true or disprove it if it is false.*

The conjecture in Example 7 is false because there is a counterexample, $x = \frac{1}{2}$ The statement "$(\frac{1}{2})^2 \geq \frac{1}{2}$" is false, so the generalization is false. ◇

Definition 10. *A **counterexample** to a generalization is an example that demonstrates that the generalization is false by showing that the component assertion is not always true.*

Any *one* counterexample *proves* that a generalization is false (i.e., disproves the generalization) [Section 2.2].

To prove a generalization false, we prove its negation true. The negation of a generalization is an existence statement [Section 2.2]. This is an axiom.

Definition 11. *An **axiom** is a statement that is accepted without proof.*

Usually axioms are accepted because they are "obvious" or so primitive that there are no relevant results prior to them.

Axiom 12. *Let $P(x)$ be an assertion with truth value that may depend upon x. The negation of the generalization, "For all x, $P(x)$," is the existence statement, "There exists an x such that (not $P(x)$)."*

Therefore the generalization, "For all $x, P(x)$," is false if and only if the existence statement, "There exists an x such that (not $P(x)$)," is true.

Example 7: [continued] "For all $x, x^2 \geq x$," is a false generalization because "There exists x such that $x^2 < x$," is a true existence statement. $x = \frac{1}{2}$ is an example that proves this. This example is a counterexample to the conjecture in Example 7. It proves that "$x^2 \geq x$" is false. ◇

Definition 13. *A statement that (explicitly or implicitly) asserts that something exists is an **existence statement** [Section 2.2].*

Theorem 14. [1] *A **counterexample** to a generalization of the form "If H, then C," is an example such that the hypothesis, H, is true and the conclusion, C, is false.*

Example 8: Resolve the conjecture: If $x^2 > 25$, then $x > 5$.

The conjecture is false; there is a counterexample: $x = -10$.

When $x = -10$, $x^2 = 100$ and the hypothesis is true. However, -10 is not greater than 5, so the conclusion is false.

Actually, there are many different possible counterexamples. $x = -6$ is another. But it is good style to just pick one counterexample, as simple as possible. One counterexample is enough to prove that a generalization is false. ◇

[1] The theorems and definitions that you need to know are numbered in bold print in a single sequence. So, "Theorem 14" does not mean it is the fourteenth theorem, rather it is the fourteenth major result of the section. This should make important results easy to locate. When a theorem is cited in a later section, it will be prefixed with the section number, so "1.1.14" refers to the fourteenth major result in bold in Section 1.1. Examples are numbered in their own, separate, underlined sequence.

Definition 15. *There are two quantifiers,* ***for all*** *and* ***there exists****, used to quantify variables in generalizations and existence statements. Frequently the quantifier is not given in exactly those words, rather it is understood, or expressed by a synonym. The phrase* ***for each*** *is a good synonym for* ***for all*** *[Section 2.1]. Quantified variables are* ***placeholders****.*

Example 9: "For all $x > 5, x^2 > 25$" is a true generalization. It has the same meaning as "For all $c > 5, c^2 > 25$." The letters are placeholders. The symbols "x" and "c" are used to hold places where anything of their kind could go. However, we would not put S in those places because that symbol usually represents a set and not a number.

The inequality "$x^2 > 25$" is not a generalization and in it x is not a placeholder. The inequality is not asserted to be true "for all x." [Variables that are not quantified are called "free variables." See Section 2.1.]

The equation "$x^2 = 5x - 6$" is not a generalization and in it x is not a placeholder. Equations which you are supposed to solve do not use x as a placeholder; they are not expected to be true "for all x."

The sentence, "The equation $x^2 = 5x - 6$ has a solution," is an existence statement. It asserts that **there exists** a solution. The letter x is quantified; it is a placeholder.

Not all existence statements use the exact phrase *there exists.* The existence statement is true; $x = 2$ is an example which proves it. The existence statement could be proved with a different example, $x = 3$, but one example is enough for an existence proof.

The sentence "There is a solution for c to the equation "$c^2 = 5c - 6$" has exactly the same meaning. In the original sentence, "x" is a placeholder which can be replaced by any other letter of the same kind.

$\diamond$

Logical Form. Many proofs use logic to reorganize the original statement into an equivalent statement that is more convenient. Often proofs combine translation [Section 2.4] and logical reorganization [Sections 1.4 and 1.5].

Example 10: Suppose you are studying sets and you have, as prior results, the definitions of $\subset$ (subset), $\cap$ (intersection), and $=$ (equals). (Yes, even "=" has a definition!) [Sections 1.2 and 2.3.]
Definition of *subset* (from Example 2): $S \subset T$ if and only if (if $x \in S$, then $x \in T$).
Definition of *set intersection* ($\cap$): $x \in S \cap T$ if and only if $x \in S$ and $x \in T$.
Definition of *set equality* ($=$): $S = T$ if and only if ($x \in S$ if and only if $x \in T$).

The term *subset* is defined above by giving a sentence equivalent to "$S \subset T$." That definition also applies to "$R \subset P$"; the letters in the definition are placeholders and may be switched, as long as they are switched to letters appropriate for sets in every place where they appear.

Theorems use letters as placeholders. In the following theorem S and T are placeholders. The same theorem could be stated with other letters appropriate for sets.

Theorem If $S \cap T = S$, then $S \subset T$.

Pictures, such as Venn diagrams, may be very useful and convincing, but they are not the same as formal proofs [Sections 1.2 and 2.3].

Proof:
[Step 1] Let $x \in S$.
[Step 2] Then $x \in S \cap T$ by the hypothesis that $S \cap T = S$ [and the definition of *set equality*].
[Step 3] Then $x \in T$ by the definition of *set intersection*. □

The first sentence in this proof is "Let $x \in S$." Why?
The answer involves translation of the term subset and then logical reorganization [Sections 1.2, 1.4, and 1.5].

To organize a proof, first inspect the conclusion.

The conclusion of "If $S \cap T = S$, then $S \subset T$" is "$S \subset T$." The conclusion may not look like a conditional sentence, but when translated [Section 2.3] into terms that are more primitive, it is a conditional sentence. By definition the conclusion, "$S \subset T$," is equivalent to "If $x \in S$, then $x \in T$." So the theorem could be restated:

Theorem again, translated: If $S \cap T = S$, then (if $x \in S$, then $x \in T$).

Many theorems have this form. ◇

Definition 16. *The **form** of a compound sentence is a symbolic representation of it in which the logical connectives are exhibited and the places of the component sentences are held by letters [Section 1.3]. (Many logic books use p and q. We use capital letters such as H and C. We use lower-case letters to represent numbers, not sentences.) A sentence with the connective **if ..., then** ... in the form "If H, then C," is called a **conditional sentence** [Section 1.3]. The component sentence in the place of H is called the **hypothesis** and the sentence in the place of C is called the **conclusion**. The conditional sentence "If H, then C," is often abbreviated to "H ⇒ C," which may be read "H implies C."*

To prove a conditional sentence true, the hypothesis may be regarded as true and treated as if it were a prior result in order to deduce the conclusion [Section 3.3].

Example 11:
The form of "If $x \in S$, then $x \in T$"
is " B ⇒ C."

The form could be expressed with different letters, for example, "$A \Rightarrow B$."

The proof of the theorem has a lot to do with its form. The position of the connectives often dictates how the steps of the proof are arranged.

Theorem, translated: If $S \cap T = S$, then (if $x \in S$, then $x \in T$).
Its form: $H \Rightarrow (B \Rightarrow C)$ $\diamond$

The theorem is a conditional sentence, and inside the theorem its conclusion is also a conditional sentence. It is common to reorganize theorems of this form using this important logical equivalence [Section 1.4].

Theorem 17 (A Hypothesis in the Conclusion)**.** *$H \Rightarrow (B \Rightarrow C)$ is logically equivalent to (B and H) $\Rightarrow C$. B is the hypothesis in the conclusion.*

B is purposely written before H in "(B and H) $\Rightarrow C$" because proofs of such results usually begin with B rather than H.

The proof of Example 10 used the reorganization in Theorem 17

$$\text{If } S \cap T = S, \text{ then } S \subset T$$

is equivalent to

$$\text{If } S \cap T = S, \text{ then (if } x \in S, \text{ then } x \in T)$$

by translation of subset. It has the form $H \Rightarrow (B \Rightarrow C)$, so by logic (A Hypothesis in the Conclusion, Theorem 17), it is equivalent to

$$\text{If } x \in S \text{ and } S \cap T = S, \text{ then } x \in T$$

which has the form B and $H \Rightarrow C$.

The set-theory theorem and its proof are repeated next. Note how the proof uses this logical reorganization perfectly. It begins with B [$x \in S$]. It ends with C [$x \in T$] and uses H [the original hypothesis] in the middle. Logic tells us where to begin and where to end the proof.

Theorem: If $S \cap T = S$, then $S \subset T$.

Proof:		Form
[Step 1] Let $x \in S$		B
[Step 2] then $x \in S \cap T$	by the hypothesis that $S \cap T = S$	
	[and the definition of set equality]	H
[Step 3] Then $x \in T$	by the definition of set intersection.	C

This example shows that it is important to know the common ways in which theorems are translated and logically reorganized. The logic is studied with truth tables [Section 1.3].

Conclusion. A proof of a theorem is a sequence of statements which demonstrate that the theorem is a logical consequence of prior results. In proofs,

logic, prior results, placeholders, translation, form, and logical reorganization play important roles. Each will be discussed thoroughly.

Terms: Proof, prior result, placeholder, equivalent, connective, form, conditional sentence, conjecture, generalization, existence statement, quantifier, counterexample.

Exercises for Section 1.1, **Preview of Proof**:

A1. ☺ True or false?
a) In each section, "**Theorem 5**" in bold refers to the fifth theorem in the section.
b) Generalizations are necessarily true.
c) Identities are necessarily true.
d) Existence statements are necessarily true.

A2. ☺ True or false?
a) In each section, "**Definition 15**" in bold refers to the fifteenth definition in the section.
b) The sentence "The equation $x + 3 = 5$ has a solution" is an existence statement.
c) The equation "$x^2 = 2x$" uses x as a placeholder.
d) The equation "$4x + 5x = 9x$" can be regarded as an abbreviated generalization.

A3. ☺ True or false?
a) Some identities are false. b) Some generalizations are false.
c) Some existence statements are false. d) Some theorems are false.

A4. ☺ True or False?
a) Generalizations are necessarily true.
b) Existence statements are necessarily true.

—— ☺ Equivalence. Are the two sentences equivalent? Yes or no?
A5. $2x = 8,\ x = 4$ A6. $x < 4,\ x^2 < 16$
A7. $x = 3,\ x^2 = 9$ A8. $x > 2,\ x^2 > 4$
A9. $a = b,\ a + c = b + c$ A10. $a = b,\ a - c = b - c$
A11. $a = b,\ ca = cb$ A12. $S \subset T$, S is a subset of T

B1. a) Define *placeholder*. b) Do placeholders permit letter-switching? c) Give an example of letter-switching. [One example requires two sentences, one before switching and one after.]

B2. The Zero Product Rule stated in Example 1 could be stated with other letters. Do it.
B3. In the definition of *subset* in Example 3 the variables are placeholders. Restate it using R and S.
B4. In the definition of *complement* in Example 3 the letter S is a placeholder. State the definition using letter T.

—— ☺ When a variable in a sentence is a placeholder, it may be replaced by some other letter of the same kind without changing the meaning of the sentence. Which of these use x as a placeholder?

B5. For all $x, 2x + 3x = 5x$.
B6. $2x + 3x = 5$.
B7. $x < 5$ iff $2x < 10$.
B8. If $x > 3$, then $x^2 > 9$.
B9. $x^2 = x + 7$.
B10. $x + 5 = 7$ iff $x = 2$.
B11. $(x + 1)^2 = x^2 + 2x + 1$.
B12. $(x + 1)^2 = 16$.
B13. $2(x + 5) = 30$.
B14. $2(x + 5) = 2x + 10$.

B15. a) Define *generalization*. b) Are generalizations always true? c) Define *identity*. d) What is the difference between a generalization and an identity?
B16. Define *counterexample*.

—— ☺ Here are some generalizations. Restate each making the *for all* (or *for each*) explicit.

B17. If $b > 5$, then $|b| > 5$.
B18. If $x > 5$, then $5x > 25$.
B19. $ab = 0$ iff $a = 0$ or b =0.
B20. $a = b$ iff $a + c = b + c$.

—— ☺ Here are some generalizations. Are they true? If they are true, just say so. If not, give a counterexample.

B21. If $x < 5$, then $x^2 < 25$.
B22. If $x > 5$, then $x^2 > 25$.
B23. If $x^2 > 25$, then $x > 5$.
B24. If $x^2 < 25$, then $x < 5$.
B25. If $b > 4$, then $|b| > 4$.
B26. If $b < 4$, then $|b| < 4$.
B27. If $|b| < 4$, then $b < 4$.
B28. If $|b| > 4$, then $b > 4$.
B29. $2x \geq x$.
B30. $x + c > x$.
B31. If $c > 0$ and $x > 0$, then $cx \geq x$.
B32. $x/2 \leq x$.

—— ☺ Here are some existence statements. Are they true?

B33. There exists x such that $x^2 < x$.
B34. There exists x such that $x^2 = (x + 1)^2$.
B35. There exists x such that $|x| < x$.
B36. There exists x such that $|x| > x$.
B37. $x^2 = 2$ has a real-valued solution.
B38. $x^2 = -2$ has a real-valued solution.
B39. $x^2 = 2$ has a rational-number solution.
B40. $x^2 = 16$ has a rational-number solution.

B41. ☺ Here is a theorem: $x^3 + bx^2 + cx + d = 0$ has a solution.
a) Is it an existence statement? If so, what exists?
b) Is it a generalization? If so, what is the quantifier *for all* attached to?
B42. ☺ Identify the form of "If $x < 5$, then $x^2 < 25$."
B43. Define *proof*. Proofs have two major components. What are they?

C1. "$x^2 = 25$ is equivalent to $x = 5$ or $x = -5$." The sentence is true.
a) Does it say that $x^2 = 25$?
b) Is the sentence in quotations marks true if $x = 3$?
c) How can it be true if $x = 3$?

C2. The Zero Product Rule may be stated: $ab = 0$ iff $a = 0$ or $b = 0$.
a) The quantifier *for all* is suppressed. What would be mentioned there if the *for all* were explicit? b) Is it true if $a = 2$ and $b = 3$?
c) How can it be true if $a = 2$ and $b = 3$? Then $ab = 6$ and not 0!