PEARSON NEW INTERNATIONAL EDITION

Mathematical Proofs: A Transition to Advanced Mathematics

Chartrand Polimeni Zhang

Third Edition

PEARSON®

Pearson New International Edition

Mathematical Proofs:
A Transition to Advanced Mathematics
Chartrand Polimeni Zhang
Third Edition

PEARSON®

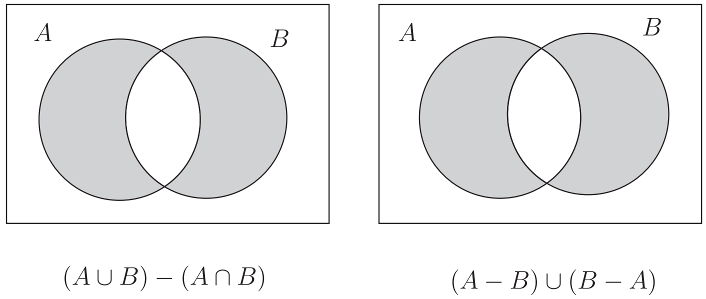

Figure 2 Venn diagrams for $(A \cup B) - (A \cap B)$ and $(A - B) \cup (B - A)$

Next, let's consider the Venn diagrams for $(A \cup B) - (A \cap B)$ and $(A - B) \cup (B - A)$, which are shown in Figure 2. From these two diagrams, we might conclude (correctly) that the two sets $(A \cup B) - (A \cap B)$ and $(A - B) \cup (B - A)$ are equal. Indeed, all that is lacking is a *proof* that these two sets are equal. That is, Venn diagrams can be useful in suggesting certain results concerning sets, but they are only drawings and do not constitute a proof.

Result 20 *For every two sets A and B,*

$$(A \cup B) - (A \cap B) = (A - B) \cup (B - A).$$

Proof First we show that $(A \cup B) - (A \cap B) \subseteq (A - B) \cup (B - A)$. Let $x \in (A \cup B) - (A \cap B)$. Then $x \in A \cup B$ and $x \notin A \cap B$. Since $x \in A \cup B$, it follows that $x \in A$ or $x \in B$. Without loss of generality, we can assume $x \in A$. Since $x \notin A \cap B$, the element $x \notin B$. Therefore, $x \in A - B$ and so $x \in (A - B) \cup (B - A)$. Hence

$$(A \cup B) - (A \cap B) \subseteq (A - B) \cup (B - A).$$

Next we show that $(A - B) \cup (B - A) \subseteq (A \cup B) - (A \cap B)$. Let $x \in (A - B) \cup (B - A)$. Then $x \in A - B$ or $x \in B - A$, say the former. So $x \in A$ and $x \notin B$. Thus $x \in A \cup B$ and $x \notin A \cap B$. Consequently, $x \in (A \cup B) - (A \cap B)$. Therefore,

$$(A - B) \cup (B - A) \subseteq (A \cup B) - (A \cap B),$$

as desired. ■

PROOF ANALYSIS In the proof of Result 20, when we were verifying the set inclusion

$$(A \cup B) - (A \cap B) \subseteq (A - B) \cup (B - A),$$

we concluded that $x \in A$ or $x \in B$. At that point, we could have divided the proof into two cases (*Case* 1. $x \in A$ and *Case* 2. $x \in B$); however, the proofs of the two cases would be identical, except that A and B would be interchanged. Therefore, we decided to consider only one of these. Since it really didn't matter which case we handled, we simply chose the case where $x \in A$. This was accomplished by writing:

Without loss of generality, assume that $x \in A$.

In the proof of the reverse set containment, we found ourselves in a similar situation, namely, $x \in A - B$ or $x \in B - A$. Again, these two situations were basically identical and we simply chose to work with the first (former) situation. (Had we decided to assume that $x \in B - A$, we would have considered the *latter* case.) ♦

We now look at an example of a biconditional concerning sets.

Result 21 *Let A and B be sets. Then $A \cup B = A$ if and only if $B \subseteq A$.*

Proof First we prove that if $A \cup B = A$, then $B \subseteq A$. We use a proof by contrapositive. Assume that B is not a subset of A. Then there must be some element $x \in B$ such that $x \notin A$. Since $x \in B$, it follows that $x \in A \cup B$. However, since $x \notin A$, we have $A \cup B \neq A$.

Next we verify the converse, namely, if $B \subseteq A$, then $A \cup B = A$. We use a direct proof here. Assume that $B \subseteq A$. To verify that $A \cup B = A$, we show that $A \subseteq A \cup B$ and $A \cup B \subseteq A$. The set inclusion $A \subseteq A \cup B$ is immediate (if $x \in A$, then $x \in A \cup B$). It remains only to show then that $A \cup B \subseteq A$. Let $y \in A \cup B$. Thus $y \in A$ or $y \in B$. If $y \in A$, then we already have the desired result. If $y \in B$, then since $B \subseteq A$, it follows that $y \in A$. Thus $A \cup B \subseteq A$. ■

PROOF ANALYSIS In the first paragraph of the proof of Result 21 we indicated that we were using a proof by contrapositive, while in the second paragraph we mentioned that we were using a direct proof. This really wasn't necessary as the assumptions we made would inform the reader what technique we were applying. Also, in the proof of Result 21, we used a proof by contrapositive for one implication and a direct proof for its converse. This wasn't necessary either. Indeed, it is quite possible to interchange the techniques we used (see Exercise 41). ♦

5 Fundamental Properties of Set Operations

Many results concerning sets follow from some very fundamental properties of sets, which, in turn, follow from corresponding results about logical statements. For example, we know that if P and Q are two statements, then $P \vee Q$ and $Q \vee P$ are logically equivalent. Similarly, if A and B are two sets, then $A \cup B = B \cup A$. We list some of the fundamental properties of set operations in the following theorem.

Theorem 22 *For sets A, B and C,*

(1) *Commutative Laws*

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

(2) *Associative Laws*

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

(3) *Distributive Laws*

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

(4) *De Morgan's Laws*

(*a*) $\overline{A \cup B} = \overline{A} \cap \overline{B}$
(*b*) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

We present proofs of only three parts of Theorem 22, beginning with the commutative law of the union of two sets.

Proof of Theorem 22(1a) We show that $A \cup B \subseteq B \cup A$. Assume that $x \in A \cup B$. Then $x \in A$ or $x \in B$. Applying the commutative law for disjunction of statements, we conclude that $x \in B$ or $x \in A$; so $x \in B \cup A$. Thus, $A \cup B \subseteq B \cup A$. The proof of the reverse set inclusion $B \cup A \subseteq A \cup B$ is similar and is therefore omitted. ■

Next we verify one of the distributive laws.

Proof of Theorem 22(3a) First we show that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Let $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$. Thus $x \in (A \cup B) \cap (A \cup C)$, as desired. On the other hand, if $x \in B \cap C$, then $x \in B$ and $x \in C$; and again, $x \in A \cup B$ and $x \in A \cup C$. So $x \in (A \cup B) \cap (A \cup C)$. Therefore, $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

To verify the reverse set inclusion, let $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. If $x \in A$, then $x \in A \cup (B \cap C)$. So we may assume that $x \notin A$. Then the fact that $x \in A \cup B$ and $x \notin A$ implies that $x \in B$. By the same reasoning, $x \in C$. Thus $x \in B \cap C$ and so $x \in A \cup (B \cap C)$. Therefore, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. ■

As a final example, we prove one of De Morgan's laws.

Proof of Theorem 22(4a) First, we show that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$. Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$. Hence $x \notin A$ and $x \notin B$. Therefore, $x \in \overline{A}$ and $x \in \overline{B}$, so $x \in \overline{A} \cap \overline{B}$; Consequently, $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Next we show that $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. Let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A}$ and $x \in \overline{B}$. Thus, $x \notin A$ and $x \notin B$; so $x \notin A \cup B$. Therefore, $x \in \overline{A \cup B}$. Hence $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. ■

PROOF ANALYSIS In the proof of the De Morgan law that we just presented, we arrived at the step $x \notin A \cup B$ at one point and then next wrote $x \notin A$ *and* $x \notin B$. Since $x \in A \cup B$ implies that $x \in A$ *or* $x \in B$, you might have expected us to write that $x \notin A$ *or* $x \notin B$ after writing $x \notin A \cup B$, but this would not be the correct conclusion. When we say that $x \notin A \cup B$, this is equivalent to writing $\sim (x \in A \cup B)$, which is logically equivalent to $\sim ((x \in A)$ or $(x \in B))$. By the De Morgan law for the negation of the disjunction of two statements (or two open sentences), we have that $\sim ((x \in A)$ or $(x \in B))$ is logically equivalent to $\sim (x \in A)$ and $\sim (x \in B)$; that is, $x \notin A$ *and* $x \notin B$. ♦

Proofs of some other parts of Theorem 22 are left as exercises.

6 Proofs Involving Cartesian Products of Sets

Recall that the **Cartesian product** (or simply the **product**) $A \times B$ of two sets A and B is defined as

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

If $A = \emptyset$ or $B = \emptyset$, then $A \times B = \emptyset$.

Before looking at several examples of proofs concerning Cartesian products of sets, it is important to keep in mind that an arbitrary element of the Cartesian product $A \times B$ of two sets A and B is of the form (a, b), where $a \in A$ and $b \in B$.

Result 23 *Let A, B, C and D be sets. If $A \subseteq C$ and $B \subseteq D$, then $A \times B \subseteq C \times D$.*

Proof Let $(x, y) \in A \times B$. Then $x \in A$ and $y \in B$. Since $A \subseteq C$ and $B \subseteq D$, it follows that $x \in C$ and $y \in D$. Hence $(x, y) \in C \times D$. ■

Result 24 *For sets A, B and C,*

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

Proof We first show that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$. Let $(x, y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in B \cup C$. Thus $y \in B$ or $y \in C$, say the former. Then $(x, y) \in A \times B$ and so $(x, y) \in (A \times B) \cup (A \times C)$. Consequently, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Next we show that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. Let $(x, y) \in (A \times B) \cup (A \times C)$. Then $(x, y) \in A \times B$ or $(x, y) \in A \times C$, say the former. Then $x \in A$ and $y \in B \subseteq B \cup C$. Hence $(x, y) \in A \times (B \cup C)$, implying that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. ■

We give one additional example of a proof involving the Cartesian products of sets.

Result 25 *For sets A, B and C,*

$$A \times (B - C) = (A \times B) - (A \times C).$$

Proof First we show that $A \times (B - C) \subseteq (A \times B) - (A \times C)$. Let $(x, y) \in A \times (B - C)$. Then $x \in A$ and $y \in B - C$. Since $y \in B - C$, it follows that $y \in B$ and $y \notin C$. Because $x \in A$ and $y \in B$, we have $(x, y) \in A \times B$. Since $y \notin C$, however, $(x, y) \notin A \times C$. Therefore, $(x, y) \in (A \times B) - (A \times C)$. Hence $A \times (B - C) \subseteq (A \times B) - (A \times C)$.

We now show that $(A \times B) - (A \times C) \subseteq A \times (B - C)$. Let $(x, y) \in (A \times B) - (A \times C)$. Then $(x, y) \in A \times B$ and $(x, y) \notin A \times C$. Since $(x, y) \in A \times B$, it follows that $x \in A$ and $y \in B$. Also, since $x \in A$ and $(x, y) \notin A \times C$, it follows that $y \notin C$. So $y \in B - C$. Thus $(x, y) \in A \times (B - C)$ and $(A \times B) - (A \times C) \subseteq A \times (B - C)$. ■

PROOF ANALYSIS We add one comment concerning the preceding proof. During the proof of $(A \times B) - (A \times C) \subseteq A \times (B - C)$, we needed to show that $y \notin C$. We learned that $(x, y) \notin A \times C$. However, this information alone did not allow us to conclude that $y \notin C$. Indeed, if

$(x, y) \notin A \times C$, then $x \notin A$ *or* $y \notin C$. Since we knew, however, that $x \in A$ *and* $(x, y) \notin A \times C$, we were able to conclude that $y \notin C$. ♦

EXERCISES

Section 1: Proofs Involving Divisibility of Integers

1. Let a and b be integers, where $a \neq 0$. Prove that if $a \mid b$, then $a^2 \mid b^2$.
2. Let $a, b \in \mathbf{Z}$, where $a \neq 0$ and $b \neq 0$. Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
3. Let $m \in \mathbf{Z}$.
   (a) Give a direct proof of the following: If $3 \mid m$, then $3 \mid m^2$.
   (b) State the contrapositive of the implication in (a).
   (c) Give a direct proof of the following: If $3 \nmid m$, then $3 \nmid m^2$.
   (d) State the contrapositive of the implication in (c).
   (e) State the conjunction of the implications in (a) and (c) using "if and only if."
4. Let $x, y \in \mathbf{Z}$. Prove that if $3 \nmid x$ and $3 \nmid y$, then $3 \mid (x^2 - y^2)$.
5. Let $a, b, c \in \mathbf{Z}$, where $a \neq 0$. Prove that if $a \nmid bc$, then $a \nmid b$ and $a \nmid c$.
6. Let $a \in \mathbf{Z}$. Prove that if $3 \mid 2a$, then $3 \mid a$.
7. Let $n \in \mathbf{Z}$. Prove that $3 \mid (2n^2 + 1)$ if and only if $3 \nmid n$.
8. In Result 4, it was proved for an integer x that if $2 \mid (x^2 - 1)$, then $4 \mid (x^2 - 1)$. Prove that if $2 \mid (x^2 - 1)$, then $8 \mid (x^2 - 1)$.
9. (a) Let $x \in \mathbf{Z}$. Prove that if $2 \mid (x^2 - 5)$, then $4 \mid (x^2 - 5)$.
   (b) Give an example of an integer x such that $2 \mid (x^2 - 5)$ but $8 \nmid (x^2 - 5)$.
10. Let $n \in \mathbf{Z}$. Prove that $2 \mid (n^4 - 3)$ if and only if $4 \mid (n^2 + 3)$.
11. Prove that for every integer $n \geq 8$, there exist nonnegative integers a and b such that $n = 3a + 5b$.
12. In Result 7, it was proved for integers x and y that $4 \mid (x^2 - y^2)$ if and only if x and y are of the same parity. In particular, this says that if x and y are both even, then $4 \mid (x^2 - y^2)$; while if x and y are both odd, then $4 \mid (x^2 - y^2)$. Prove that if x and y are both odd, then $8 \mid (x^2 - y^2)$.
13. Prove that if $a, b, c \in \mathbf{Z}$ and $a^2 + b^2 = c^2$, then $3 \mid ab$.

Section 2: Proofs Involving Congruence of Integers

14. Let $a, b, n \in \mathbf{Z}$, where $n \geq 2$. Prove that if $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.
15. Let $a, b, c, n \in \mathbf{Z}$, where $n \geq 2$. Prove that if $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{n}$.
16. Let $a, b \in \mathbf{Z}$. Prove that if $a^2 + 2b^2 \equiv 0 \pmod{3}$, then either a and b are both congruent to 0 modulo 3 or neither is congruent to 0 modulo 3.
17. (a) Prove that if a is an integer such that $a \equiv 1 \pmod{5}$, then $a^2 \equiv 1 \pmod{5}$.
    (b) Given that b is an integer such that $b \equiv 1 \pmod{5}$, what can we conclude from (a)?
18. Let $m, n \in \mathbf{N}$ such that $m \geq 2$ and $m \mid n$. Prove that if a and b are integers such that $a \equiv b \pmod{n}$, then $a \equiv b \pmod{m}$.
19. Let $a, b \in \mathbf{Z}$. Show that if $a \equiv 5 \pmod{6}$ and $b \equiv 3 \pmod{4}$, then $4a + 6b \equiv 6 \pmod{8}$.

20. (a) Result 12 states: Let $n \in \mathbf{Z}$. If $n^2 \not\equiv n \pmod 3$, then $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$. State and prove the converse of this result.
    (b) State the conjunction of Result 12 and its converse using "if and only if."
21. Let $a \in \mathbf{Z}$. Prove that $a^3 \equiv a \pmod 3$.
22. Let $n \in \mathbf{Z}$. Prove each of the statements (a)–(f).

    (a) If $n \equiv 0 \pmod 7$, then $n^2 \equiv 0 \pmod 7$.
    (b) If $n \equiv 1 \pmod 7$, then $n^2 \equiv 1 \pmod 7$.
    (c) If $n \equiv 2 \pmod 7$, then $n^2 \equiv 4 \pmod 7$.
    (d) If $n \equiv 3 \pmod 7$, then $n^2 \equiv 2 \pmod 7$.
    (e) For each integer n, $n^2 \equiv (7-n)^2 \pmod 7$.
    (f) For every integer n, n^2 is congruent to exactly one of 0, 1, 2 or 4 modulo 7.

23. Prove for any set $S = \{a, a+1, \dots, a+5\}$ of six integers where $6 \mid a$ that $24 \mid (x^2 - y^2)$ for distinct odd integers x and y in S if and only if one of x and y is congruent to 1 modulo 6 while the other is congruent to 5 modulo 6.
24. Let x and y be even integers. Prove that $x^2 \equiv y^2 \pmod{16}$ if and only if either (1) $x \equiv 0 \pmod 4$ and $y \equiv 0 \pmod 4$ or (2) $x \equiv 2 \pmod 4$ and $y \equiv 2 \pmod 4$.

Section 3: Proofs Involving Real Numbers

25. Let $x, y \in \mathbf{R}$. Prove that if $x^2 - 4x = y^2 - 4y$ and $x \neq y$, then $x + y = 4$.
26. Let a, b and m be integers. Prove that if $2a + 3b \geq 12m + 1$, then $a \geq 3m + 1$ or $b \geq 2m + 1$.
27. Let $x \in \mathbf{R}$. Prove that if $3x^4 + 1 \leq x^7 + x^3$, then $x > 0$.
28. Prove that if r is a real number such that $0 < r < 1$, then $\frac{1}{r(1-r)} \geq 4$.
29. Prove that if r is a real number such that $|r - 1| < 1$, then $\frac{4}{r(4-r)} \geq 1$.
30. Let $x, y \in \mathbf{R}$. Prove that $|xy| = |x| \cdot |y|$.
31. Prove for every two real numbers x and y that $|x + y| \geq |x| - |y|$.
32. (a) Recall that $\sqrt{r} > 0$ for every positive real number r. Prove that if a and b are positive real numbers, then $0 < \sqrt{ab} \leq \frac{a+b}{2}$. (The number $\sqrt{ab}$ is called the **geometric mean** of a and b, while $(a+b)/2$ is called the **arithmetic mean** or **average** of a and b.)
    (b) Under what conditions does $\sqrt{ab} = (a+b)/2$ for positive real numbers a and b? Justify your answer.
33. The **geometric mean** of three positive real numbers a, b and c is $\sqrt[3]{abc}$ and the **arithmetic mean** is $(a+b+c)/3$. Prove that $\sqrt[3]{abc} \leq (a+b+c)/3$. [Note: The numbers a, b and c can be expressed as $a = r^3$, $b = s^3$ and $c = t^3$ for positive numbers r, s and t.]
34. Prove for every three real numbers x, y and z that $|x - z| \leq |x - y| + |y - z|$.
35. Prove that if x is a real number such that $x(x+1) > 2$, then $x < -2$ or $x > 1$.
36. Prove for every positive real number x that $1 + \frac{1}{x^4} \geq \frac{1}{x} + \frac{1}{x^3}$.
37. Prove for $x, y, z \in \mathbf{R}$ that $x^2 + y^2 + z^2 \geq xy + xz + yz$.
38. Let $a, b, x, y \in \mathbf{R}$ and $r \in \mathbf{R}^+$. Prove that if $|x - a| < r/2$ and $|y - b| < r/2$, then $|(x + y) - (a + b)| < r$.
39. Prove that if $a, b, c, d \in \mathbf{R}$, then $(ab + cd)^2 \leq (a^2 + c^2)(b^2 + d^2)$.