CHAPTER 8

Proofs Involving Sets

Students in their first advanced mathematics classes are often surprised by the extensive role that sets play and by the fact that most of the proofs they encounter are proofs about sets. Perhaps you've already seen such proofs in your linear algebra course, where a **vector space** was defined to be a *set* of objects (called vectors) that obey certain properties. Your text proved many things about vector spaces, such as the fact that the intersection of two vector spaces is also a vector space, and the proofs used ideas from set theory. As you go deeper into mathematics, you will encounter more and more ideas, theorems and proofs that involve sets. The purpose of this chapter is to give you a foundation that will prepare you for this new outlook.

We will discuss how to show that an object is an element of a set, how to prove one set is a subset of another and how to prove two sets are equal. As you read this chapter, you may need to occasionally refer back to Chapter 1 to refresh your memory. For your convenience, the main definitions from Chapter 1 are summarized below. If A and B are sets, then:

$$\begin{aligned} A \times B &= \{(x,y) : x \in A,\ y \in B\}, \\ A \cup B &= \{x : (x \in A) \vee (x \in B)\}, \\ A \cap B &= \{x : (x \in A) \wedge (x \in B)\}, \\ A - B &= \{x : (x \in A) \wedge (x \notin B)\}, \\ \overline{A} &= U - A. \end{aligned}$$

Recall that $A \subseteq B$ means that every element of A is also an element of B.

8.1 How to Prove $a \in A$

We will begin with a review of set-builder notation, and then review how to show that a given object a is an element of some set A.

Generally, a set A will be expressed in set-builder notation $A = \{x : P(x)\}$, where $P(x)$ is some statement (or open sentence) about x. The set A is understood to have as elements all those things x for which $P(x)$ is true. For example,

$$\{x : x \text{ is an odd integer}\} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}.$$

A common variation of this notation is to express a set as $A = \{x \in S : P(x)\}$. Here it is understood that A consists of all elements x of the (predetermined) set S for which $P(x)$ is true. Keep in mind that, depending on context, x could be any kind of object (integer, ordered pair, set, function, etc.). There is also nothing special about the particular variable x; any reasonable symbol x, y, k, etc., would do. Some examples follow.

$$\begin{aligned}
\{n \in \mathbb{Z} : n \text{ is odd}\} &= \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\} \\
\{x \in \mathbb{N} : 6 \mid x\} &= \{6, 12, 18, 24, 30, \ldots\} \\
\{(a,b) \in \mathbb{Z} \times \mathbb{Z} : b = a + 5\} &= \{\ldots, (-2,3), (-1,4), (0,5), (1,6), \ldots\} \\
\{X \in \mathscr{P}(\mathbb{Z}) : |X| = 1\} &= \{\ldots, \{-1\}, \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \ldots\}
\end{aligned}$$

Now it should be clear how to prove that an object a belongs to a set $\{x : P(x)\}$. Since $\{x : P(x)\}$ consists of all things x for which $P(x)$ is true, to show that $a \in \{x : P(x)\}$ we just need to show that $P(a)$ is true. Likewise, to show $a \in \{x \in S : P(x)\}$, we need to confirm that $a \in S$ *and* that $P(a)$ is true. These ideas are summarized below. However, you should **not** memorize these methods, you should **understand** them. With contemplation and practice, using them becomes natural and intuitive.

How to show $\mathbf{a \in \{x : P(x)\}}$

Show that $P(a)$ is true.

How to show $\mathbf{a \in \{x \in S : P(x)\}}$

1. Verify that $a \in S$.
2. Show that $P(a)$ is true.

Example 8.1 Let's investigate elements of $A = \{x : x \in \mathbb{N} \text{ and } 7 \mid x\}$. This set has form $A = \{x : P(x)\}$ where $P(x)$ is the open sentence $(x \in \mathbb{N}) \wedge (7 \mid x)$. Thus $21 \in A$ because $P(21)$ is true. Similarly, $7, 14, 28, 35$, etc., are all elements of A. But $8 \notin A$ (for example) because $P(8)$ is false. Likewise $-14 \notin A$ because $P(-14)$ is false.

Example 8.2 Consider the set $A = \{X \in \mathscr{P}(\mathbb{N}) : |X| = 3\}$. We know that $\{4, 13, 45\} \in A$ because $\{4, 13, 45\} \in \mathscr{P}(\mathbb{N})$ and $|\{4, 13, 45\}| = 3$. Also $\{1, 2, 3\} \in A$, $\{10, 854, 3\} \in A$, etc. However $\{1, 2, 3, 4\} \notin A$ because $|\{1, 2, 3, 4\}| \neq 3$. Further, $\{-1, 2, 3\} \notin A$ because $\{-1, 2, 3\} \notin \mathscr{P}(\mathbb{N})$.

Example 8.3 Consider the set $B = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 5\}$. Notice $(8,23) \in B$ because $(8,23) \in \mathbb{Z} \times \mathbb{Z}$ and $8 \equiv 23 \pmod 5$. Likewise, $(100,75) \in B$, $(102,77) \in B$, etc., but $(6,10) \notin B$.

Now suppose $n \in \mathbb{Z}$ and consider the ordered pair $(4n+3, 9n-2)$. Does this ordered pair belong to B? To answer this, we first observe that $(4n+3, 9n-2) \in \mathbb{Z} \times \mathbb{Z}$. Next, we observe that $(4n+3)-(9n-2) = -5n+5 = 5(1-n)$, so $5 \mid \big((4n+3)-(9n-2)\big)$, which means $(4n+3) \equiv (9n-2) \pmod 5$. Therefore we have established that $(4n+3, 9n-2)$ meets the requirements for belonging to B, so $(4n+3, 9n-2) \in B$ for every $n \in \mathbb{Z}$.

Example 8.4 This illustrates another common way of defining a set. Consider the set $C = \{3x^3 + 2 : x \in \mathbb{Z}\}$. Elements of this set consist of all the values $3x^3 + 2$ where x is an integer. Thus $-22 \in C$ because $-22 = 3(-2)^3 + 2$. You can confirm $-1 \in C$ and $5 \in C$, etc. Also $0 \notin C$ and $\frac{1}{2} \notin C$, etc.

8.2 How to Prove $A \subseteq B$

In this course (and more importantly, beyond it) you will encounter many circumstances where it is necessary to prove that one set is a subset of another. This section explains how to do this. The methods we discuss should improve your skills in both writing your own proofs and in comprehending the proofs that you read.

Recall (Definition 1.3) that if A and B are sets, then $A \subseteq B$ means that every element of A is also an element of B. In other words, it means *if* $a \in A$, *then* $a \in B$. Therefore to prove that $A \subseteq B$, we just need to prove that the conditional statement

"If $a \in A$, then $a \in B$"

is true. This can be proved directly, by assuming $a \in A$ and deducing $a \in B$. The contrapositive approach is another option: Assume $a \notin B$ and deduce $a \notin A$. Each of these two approaches is outlined below.

How to Prove $A \subseteq B$
(Direct approach)

Proof. Suppose $a \in A$.
⋮
Therefore $a \in B$.
Thus $a \in A$ implies $a \in B$,
so it follows that $A \subseteq B$. ■

How to Prove $A \subseteq B$
(Contrapositive approach)

Proof. Suppose $a \notin B$.
⋮
Therefore $a \notin A$.
Thus $a \notin B$ implies $a \notin A$,
so it follows that $A \subseteq B$. ■

In practice, the direct approach usually results in the most straightforward and easy proof, though occasionally the contrapositive is the most expedient. (You can even prove $A \subseteq B$ by contradiction: Assume $(a \in A) \wedge (a \notin B)$, and deduce a contradiction.) The remainder of this section consists of examples with occasional commentary. Unless stated otherwise, we will use the direct approach in all proofs; pay special attention to how the above outline for the direct approach is used.

Example 8.5 Prove that $\{x \in \mathbb{Z} : 18 | x\} \subseteq \{x \in \mathbb{Z} : 6 | x\}$.

Proof. Suppose $a \in \{x \in \mathbb{Z} : 18 | x\}$.
This means that $a \in \mathbb{Z}$ and $18 | a$.
By definition of divisibility, there is an integer c for which $a = 18c$.
Consequently $a = 6(3c)$, and from this we deduce that $6 | a$.
Therefore a is one of the integers that 6 divides, so $a \in \{x \in \mathbb{Z} : 6 | x\}$.

We've shown $a \in \{x \in \mathbb{Z} : 18 | x\}$ implies $a \in \{n \in \mathbb{Z} : 6 | x\}$, so it follows that $\{x \in \mathbb{Z} : 18 | x\} \subseteq \{x \in \mathbb{Z} : 6 | x\}$. ■

Example 8.6 Prove that $\{x \in \mathbb{Z} : 2 | x\} \cap \{x \in \mathbb{Z} : 9 | x\} \subseteq \{x \in \mathbb{Z} : 6 | x\}$.

Proof. Suppose $a \in \{x \in \mathbb{Z} : 2 | x\} \cap \{x \in \mathbb{Z} : 9 | x\}$.
By definition of intersection, this means $a \in \{x \in \mathbb{Z} : 2 | x\}$ and $a \in \{x \in \mathbb{Z} : 9 | x\}$.
Since $a \in \{x \in \mathbb{Z} : 2 | x\}$ we know $2 | a$, so $a = 2c$ for some $c \in \mathbb{Z}$. Thus a is even.
Since $a \in \{x \in \mathbb{Z} : 9 | x\}$ we know $9 | a$, so $a = 9d$ for some $d \in \mathbb{Z}$.
As a is even, $a = 9d$ implies d is even. (Otherwise $a = 9d$ would be odd.)
Then $d = 2e$ for some integer e, and we have $a = 9d = 9(2e) = 6(3e)$.
From $a = 6(3e)$, we conclude $6 | a$, and this means $a \in \{x \in \mathbb{Z} : 6 | x\}$.

We have shown that $a \in \{x \in \mathbb{Z} : 2 | x\} \cap \{x \in \mathbb{Z} : 9 | x\}$ implies $a \in \{x \in \mathbb{Z} : 6 | x\}$, so it follows that $\{x \in \mathbb{Z} : 2 | x\} \cap \{x \in \mathbb{Z} : 9 | x\} \subseteq \{x \in \mathbb{Z} : 6 | x\}$. ■

Example 8.7 Show $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 6\} \subseteq \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 3\}$.

Proof. Suppose $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 6\}$.
This means $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ and $a \equiv b \pmod 6$.
Consequently $6 | (a - b)$, so $a - b = 6c$ for some integer c.
It follows that $a - b = 3(2c)$, and this means $3 | (a - b)$, so $a \equiv b \pmod 3$.
Thus $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 3\}$.

We've now seen that $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 6\}$ implies $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 3\}$, so it follows that $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 6\} \subseteq \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod 3\}$. ■

Some statements involving subsets are transparent enough that we often accept (and use) them without proof. For example, if A and B are any sets, then it's very easy to confirm $A \cap B \subseteq A$. (Reason: Suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$ by definition of intersection, so in particular $x \in A$. Thus $x \in A \cap B$ implies $x \in A$, so $A \cap B \subseteq A$.) Other statements of this nature include $A \subseteq A \cup B$ and $A - B \subseteq A$, as well as conditional statements such as $\big((A \subseteq B) \wedge (B \subseteq C)\big) \Rightarrow (A \subseteq C)$ and $(X \subseteq A) \Rightarrow (X \subseteq A \cup B)$. Our point of view in this text is that we do not need to prove such obvious statements unless we are explicitly asked to do so in an exercise. (Still, you should do some quick mental proofs to convince yourself that the above statements are true. If you don't see that $A \cap B \subseteq A$ is true but that $A \subseteq A \cap B$ is not necessarily true, then you need to spend more time on this topic.)

The next example will show that if A and B are sets, then $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$. Before beginning our proof, let's look at an example to see if this statement really makes sense. Suppose $A = \{1,2\}$ and $B = \{2,3\}$. Then

$$\begin{aligned} \mathscr{P}(A) \cup \mathscr{P}(B) &= \{\emptyset, \{1\}, \{2\}, \{1,2\}\} \cup \{\emptyset, \{2\}, \{3\}, \{2,3\}\} \\ &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}\}. \end{aligned}$$

Also $\mathscr{P}(A \cup B) = \mathscr{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$. Thus, even though $\mathscr{P}(A) \cup \mathscr{P}(B) \neq \mathscr{P}(A \cup B)$, it is true that $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$ for this particular A and B. Now let's prove $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$ no matter what sets A and B are.

Example 8.8 Prove that if A and B are sets, then $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$.

Proof. Suppose $X \in \mathscr{P}(A) \cup \mathscr{P}(B)$.
By definition of union, this means $X \in \mathscr{P}(A)$ or $X \in \mathscr{P}(B)$.
Therefore $X \subseteq A$ or $X \subseteq B$ (by definition of power sets). We consider cases.
Case 1. Suppose $X \subseteq A$. Then $X \subseteq A \cup B$, and this means $X \in \mathscr{P}(A \cup B)$.
Case 2. Suppose $X \subseteq B$. Then $X \subseteq A \cup B$, and this means $X \in \mathscr{P}(A \cup B)$.
(We do not need to consider the case where $X \subseteq A$ *and* $X \subseteq B$ because that is taken care of by either of cases 1 or 2.) The above cases show that $X \in \mathscr{P}(A \cup B)$.

Thus we've shown that $X \in \mathscr{P}(A) \cup \mathscr{P}(B)$ implies $X \in \mathscr{P}(A \cup B)$, and this completes the proof that $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$. ■

In our next example, we prove a conditional statement. Direct proof is used, and in the process we use our new technique for showing $A \subseteq B$.

Example 8.9 Suppose A and B are sets. If $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, then $A \subseteq B$.

Proof. We use direct proof. Assume $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.
Based on this assumption, we must now show that $A \subseteq B$.
To show $A \subseteq B$, suppose that $a \in A$.
Then the one-element set $\{a\}$ is a subset of A, so $\{a\} \in \mathscr{P}(A)$.
But then, since $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, it follows that $\{a\} \in \mathscr{P}(B)$.
This means that $\{a\} \subseteq B$, hence $a \in B$.
We've shown that $a \in A$ implies $a \in B$, so therefore $A \subseteq B$. ■

8.3 How to Prove A = B

In proofs it is often necessary to show that two sets are equal. There is a standard way of doing this. Suppose we want to show $A = B$. If we show $A \subseteq B$, then every element of A is also in B, but there is still a possibility that B could have some elements that are not in A, so we can't conclude $A = B$. But if *in addition* we also show $B \subseteq A$, then B can't contain anything that is not in A, so $A = B$. This is the standard procedure for proving $A = B$: Prove both $A \subseteq B$ and $B \subseteq A$.

How to Prove A = B

Proof.
[Prove that $A \subseteq B$.]
[Prove that $B \subseteq A$.]

Therefore, since $A \subseteq B$ and $B \subseteq A$,
it follows that $A = B$. ■

Example 8.10 Prove that $\{n \in \mathbb{Z} : 35 | n\} = \{n \in \mathbb{Z} : 5 | n\} \cap \{n \in \mathbb{Z} : 7 | n\}$.

Proof. First we show $\{n \in \mathbb{Z} : 35 | n\} \subseteq \{n \in \mathbb{Z} : 5 | n\} \cap \{n \in \mathbb{Z} : 7 | n\}$. Suppose $a \in \{n \in \mathbb{Z} : 35 | n\}$. This means $35 | a$, so $a = 35c$ for some $c \in \mathbb{Z}$. Thus $a = 5(7c)$ and $a = 7(5c)$. From $a = 5(7c)$ it follows that $5 | a$, so $a \in \{n \in \mathbb{Z} : 5 | n\}$. From $a = 7(5c)$ it follows that $7 | a$, which means $a \in \{n \in \mathbb{Z} : 7 | n\}$. As a belongs to both $\{n \in \mathbb{Z} : 5 | n\}$ and $\{n \in \mathbb{Z} : 7 | n\}$, we get $a \in \{n \in \mathbb{Z} : 5 | n\} \cap \{n \in \mathbb{Z} : 7 | n\}$. Thus we've shown that $\{n \in \mathbb{Z} : 35 | n\} \subseteq \{n \in \mathbb{Z} : 5 | n\} \cap \{n \in \mathbb{Z} : 7 | n\}$.

Next we show $\{n \in \mathbb{Z} : 5 | n\} \cap \{n \in \mathbb{Z} : 7 | n\} \subseteq \{n \in \mathbb{Z} : 35 | n\}$. Suppose that $a \in \{n \in \mathbb{Z} : 5 | n\} \cap \{n \in \mathbb{Z} : 7 | n\}$. By definition of intersection, this means that $a \in \{n \in \mathbb{Z} : 5 | n\}$ and $a \in \{n \in \mathbb{Z} : 7 | n\}$. Therefore it follows that $5 | a$ and $7 | a$. By definition of divisibility, there are integers c and d with $a = 5c$ and $a = 7d$. Then a has both 5 and 7 as prime factors, so the prime factorization of a

must include factors of 5 and 7. Hence $5 \cdot 7 = 35$ divides a, so $a \in \{n \in \mathbb{Z} : 35 \mid n\}$. We've now shown that $\{n \in \mathbb{Z} : 5 \mid n\} \cap \{n \in \mathbb{Z} : 7 \mid n\} \subseteq \{n \in \mathbb{Z} : 35 \mid n\}$.

At this point we've shown that $\{n \in \mathbb{Z} : 35 \mid n\} \subseteq \{n \in \mathbb{Z} : 5 \mid n\} \cap \{n \in \mathbb{Z} : 7 \mid n\}$ and $\{n \in \mathbb{Z} : 5 \mid n\} \cap \{n \in \mathbb{Z} : 7 \mid n\} \subseteq \{n \in \mathbb{Z} : 35 \mid n\}$, so we've proved $\{n \in \mathbb{Z} : 35 \mid n\} = \{n \in \mathbb{Z} : 5 \mid n\} \cap \{n \in \mathbb{Z} : 7 \mid n\}$. ■

You know from algebra that if $c \neq 0$ and $ac = bc$, then $a = b$. The next example shows that an analogous statement holds for sets A, B and C. The example asks us to prove a conditional statement. We will prove it with direct proof. In carrying out the process of direct proof, we will have to use the new techniques from this section.

Example 8.11 Suppose A, B, and C are sets, and $C \neq \emptyset$. Prove that if $A \times C = B \times C$, then $A = B$.

Proof. Suppose $A \times C = B \times C$. We must now show $A = B$.

First we will show $A \subseteq B$. Suppose $a \in A$. Since $C \neq \emptyset$, there exists an element $c \in C$. Thus, since $a \in A$ and $c \in C$, we have $(a, c) \in A \times C$, by definition of the Cartesian product. But then, since $A \times C = B \times C$, it follows that $(a, c) \in B \times C$. Again by definition of the Cartesian product, it follows that $a \in B$. We have shown $a \in A$ implies $a \in B$, so $A \subseteq B$.

Next we show $B \subseteq A$. We use the same argument as above, with the roles of A and B reversed. Suppose $a \in B$. Since $C \neq \emptyset$, there exists an element $c \in C$. Thus, since $a \in B$ and $c \in C$, we have $(a, c) \in B \times C$. But then, since $B \times C = A \times C$, we have $(a, c) \in A \times C$. It follows that $a \in A$. We have shown $a \in B$ implies $a \in A$, so $B \subseteq A$.

The previous two paragraphs have shown $A \subseteq B$ and $B \subseteq A$, so $A = B$. In summary, we have shown that if $A \times C = B \times C$, then $A = B$. This completes the proof. ■

Now we'll look at another way that set operations are similar to operations on numbers. From algebra you are familiar with the distributive property $a \cdot (b + c) = a \cdot b + a \cdot c$. Replace the numbers a, b, c with sets A, B, C, and replace $\cdot$ with $\times$ and $+$ with $\cap$. We get $A \times (B \cap C) = (A \times B) \cap (A \times C)$. This statement turns out to be true, as we now prove.

Example 8.12 Given sets A, B, and C, prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proof. First we will show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.
Suppose $(a, b) \in A \times (B \cap C)$.
By definition of the Cartesian product, this means $a \in A$ and $b \in B \cap C$.
By definition of intersection, it follows that $b \in B$ and $b \in C$.

Thus, since $a \in A$ and $b \in B$, it follows that $(a,b) \in A \times B$ (by definition of $\times$).
Also, since $a \in A$ and $b \in C$, it follows that $(a,b) \in A \times C$ (by definition of $\times$).
Now we have $(a,b) \in A \times B$ and $(a,b) \in A \times C$, so $(a,b) \in (A \times B) \cap (A \times C)$.
We've shown that $(a,b) \in A \times (B \cap C)$ implies $(a,b) \in (A \times B) \cap (A \times C)$ so we have $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

Next we will show that $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.
Suppose $(a,b) \in (A \times B) \cap (A \times C)$.
By definition of intersection, this means $(a,b) \in A \times B$ and $(a,b) \in A \times C$.
By definition of the Cartesian product, $(a,b) \in A \times B$ means $a \in A$ and $b \in B$.
By definition of the Cartesian product, $(a,b) \in A \times C$ means $a \in A$ and $b \in C$.
We now have $b \in B$ and $b \in C$, so $b \in B \cap C$, by definition of intersection.
Thus we've deduced that $a \in A$ and $b \in B \cap C$, so $(a,b) \in A \times (B \cap C)$.
In summary, we've shown that $(a,b) \in (A \times B) \cap (A \times C)$ implies $(a,b) \in A \times (B \cap C)$ so we have $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

The previous two paragraphs show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$ and $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$, so it follows that $(A \times B) \cap (A \times C) = A \times (B \cap C)$. ■

Occasionally you can prove two sets are equal by working out a series of equalities leading from one set to the other. This is analogous to showing two algebraic expressions are equal by manipulating one until you obtain the other. We illustrate this in the following example, which gives an alternate solution to the previous example. You are cautioned that this approach is sometimes difficult to apply, but when it works it can shorten a proof dramatically.

Before beginning the example, a note is in order. Notice that any statement P is logically equivalent to $P \wedge P$. (Write out a truth table if you are in doubt.) At one point in the following example we will replace the expression $x \in A$ with the logically equivalent statement $(x \in A) \wedge (x \in A)$.

Example 8.13 Given sets A, B, and C, prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proof. Just observe the following sequence of equalities.

$$\begin{aligned}
A \times (B \cap C) &= \{(x,y) : (x \in A) \wedge (y \in B \cap C)\} && \text{(def. of } \times) \\
&= \{(x,y) : (x \in A) \wedge (y \in B) \wedge (y \in C)\} && \text{(def. of } \cap) \\
&= \{(x,y) : (x \in A) \wedge (x \in A) \wedge (y \in B) \wedge (y \in C)\} && (P = P \wedge P) \\
&= \{(x,y) : ((x \in A) \wedge (y \in B)) \wedge ((x \in A) \wedge (y \in C))\} && \text{(rearrange)} \\
&= \{(x,y) : (x \in A) \wedge (y \in B)\} \cap \{(x,y) : (x \in A) \wedge (y \in C)\} && \text{(def. of } \cap) \\
&= (A \times B) \cap (A \times C) && \text{(def. of } \times)
\end{aligned}$$

The proof is complete. ■

The equation $A \times (B \cap C) = (A \times B) \cap (A \times C)$ just obtained is a fundamental law that you may actually use fairly often as you continue with mathematics. Some similar equations are listed below. Each of these can be proved with this section's techniques, and the exercises will ask that you do so.

$$\left.\begin{aligned} \overline{A \cap B} &= \overline{A} \cup \overline{B} \\ \overline{A \cup B} &= \overline{A} \cap \overline{B} \end{aligned}\right\} \quad \text{DeMorgan's laws for sets}$$

$$\left.\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \end{aligned}\right\} \quad \text{Distributive laws for sets}$$

$$\left.\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C) \\ A \times (B \cap C) &= (A \times B) \cap (A \times C) \end{aligned}\right\} \quad \text{Distributive laws for sets}$$

It is very good practice to prove these equations. Depending on your learning style, it is probably not necessary to commit them to memory. But don't forget them entirely. They may well be useful later in your mathematical education. If so, you can look them up or re-derive them on the spot. If you go on to study mathematics deeply, you will at some point realize that you've internalized them without even being cognizant of it.

8.4 Examples: Perfect Numbers

Sometimes it takes a good bit of work and creativity to show that one set is a subset of another or that they are equal. We illustrate this now with examples from number theory involving what are called perfect numbers. Even though this topic is quite old, dating back more than 2000 years, it leads to some questions that are unanswered even today.

The problem involves adding up the positive divisors of a natural number. To begin the discussion, consider the number 12. If we add up the positive divisors of 12 that are less than 12, we obtain $1+2+3+4+6=16$, which is greater than 12. Doing the same thing for 15, we get $1+3+5=9$ which is less than 15. For the most part, given a natural number p, the sum of its positive divisors less than itself will either be greater than p or less than p. But occasionally the divisors add up to exactly p. If this happens, then p is said to be a *perfect number*.

Definition 8.1 A number $p \in \mathbb{N}$ is **perfect** if it equals the sum of its positive divisors less than itself. Some examples follow.

- The number 6 is perfect since $6 = 1+2+3$.
- The number 28 is perfect since $28 = 1+2+4+7+14$.
- The number 496 is perfect since $496 = 1+2+4+8+16+31+62+124+248$.

Though it would take a while to find it by trial-and-error, the next perfect number after 496 is 8128. You can check that 8128 is perfect. Its divisors are 1, 2, 4, 8, 16, 32, 64, 127, 254, 508, 1016, 2032, 4064 and indeed

$$8128 = 1+2+4+8+16+32+64+127+254+508+1016+2032+4064.$$

Are there other perfect numbers? How can they be found? Do they obey any patterns? These questions fascinated the ancient Greek mathematicians. In what follows we will develop an idea—recorded by Euclid—that partially answers these questions. Although Euclid did not use sets,[1] we will nonetheless phrase his idea using the language of sets.

Since our goal is to understand what numbers are perfect, let's define the following set:

$$P = \{p \in \mathbb{N} : \ p \text{ is perfect}\}.$$

Therefore $P = \{6, 28, 496, 8128, \ldots\}$, but it is unclear what numbers are in P other than the ones listed. Our goal is to gain a better understanding of just which numbers the set P includes. To do this, we will examine the following set A. It looks more complicated than P, but it will be very helpful for understanding P, as we will soon see.

$$A = \{2^{n-1}(2^n - 1) : n \in \mathbb{N}, \text{ and } 2^n - 1 \text{ is prime}\}$$

In words, A consists of every natural number of form $2^{n-1}(2^n-1)$, where $2^n - 1$ is prime. To get a feel for what numbers belong to A, look at the following table. For each natural number n, it tallies the corresponding numbers 2^{n-1} and $2^n - 1$. If $2^n - 1$ happens to be prime, then the product $2^{n-1}(2^n-1)$ is given; otherwise that entry is labeled with an $*$.

n	2^{n-1}	$2^n - 1$	$2^{n-1}(2^n-1)$
1	1	1	$*$
2	2	3	6
3	4	7	28
4	8	15	$*$
5	16	31	496
6	32	63	$*$
7	64	127	8128
8	128	255	$*$
9	256	511	$*$
10	512	1023	$*$
11	1024	2047	$*$
12	2048	4095	$*$
13	4096	8191	33,550,336

[1] Set theory was invented over 2000 years after Euclid died.

Notice that the first four entries of A are the perfect numbers 6, 28, 496 and 8128. At this point you may want to jump to the conclusion that $A = P$. But it is a shocking fact that in over 2000 years no one has ever been able to determine whether or not $A = P$. But it is known that $A \subseteq P$, and we will now prove it. In other words, we are going to show that every element of A is perfect. (But by itself, that leaves open the possibility that there may be some perfect numbers in P that are not in A.)

The main ingredient for the proof will be the formula for the sum of a geometric series with common ratio r. You probably saw this most recently in Calculus II. The formula is

$$\sum_{k=0}^{n} r^k = \frac{r^{n+1}-1}{r-1}.$$

We will need this for the case $r = 2$, which is

$$\sum_{k=0}^{n} 2^k = 2^{n+1} - 1. \tag{8.1}$$

(See the solution for Exercise 19 in Section 7.4 for a proof of this formula.) Now we are ready to prove our result. Let's draw attention to its significance by calling it a theorem rather than a proposition.

Theorem 8.1 If $A = \{2^{n-1}(2^n - 1) : n \in \mathbb{N}, \text{ and } 2^n - 1 \text{ is prime}\}$ and $P = \{p \in \mathbb{N} : \ p \text{ is perfect}\}$, then $A \subseteq P$.

Proof. Assume A and P are as stated. To show $A \subseteq P$, we must show that $p \in A$ implies $p \in P$. Thus suppose $p \in A$. By definition of A, this means

$$p = 2^{n-1}(2^n - 1) \tag{8.2}$$

for some $n \in \mathbb{N}$ for which $2^n - 1$ is prime. We want to show that $p \in P$, that is, we want to show p is perfect. Thus, we need to show that the sum of the positive divisors of p that are less than p add up to p. Notice that since $2^n - 1$ is prime, any divisor of $p = 2^{n-1}(2^n - 1)$ must have the form 2^k or $2^k(2^n - 1)$ for $0 \le k \le n - 1$. Thus the positive divisors of p are as follows:

$$\begin{array}{lllll} 2^0, & 2^1, & 2^2, & \dots\ 2^{n-2}, & 2^{n-1}, \\ 2^0(2^n-1), & 2^1(2^n-1), & 2^2(2^n-1), & \dots\ 2^{n-2}(2^n-1), & 2^{n-1}(2^n-1). \end{array}$$

Notice that this list starts with $2^0 = 1$ and ends with $2^{n-1}(2^n - 1) = p$.

If we add up all these divisors except for the last one (which equals p) we get the following:

$$\begin{aligned}
\sum_{k=0}^{n-1} 2^k + \sum_{k=0}^{n-2} 2^k(2^n-1) &= \sum_{k=0}^{n-1} 2^k + (2^n-1)\sum_{k=0}^{n-2} 2^k \\
&= (2^n-1)+(2^n-1)(2^{n-1}-1) \quad \text{(by Equation (8.1))} \\
&= [1+(2^{n-1}-1)](2^n-1) \\
&= 2^{n-1}(2^n-1) \\
&= p \qquad \text{(by Equation (8.2)).}
\end{aligned}$$

This shows that the positive divisors of p that are less than p add up to p. Therefore p is perfect, by definition of a perfect number. Thus $p \in P$, by definition of P.

We have shown that $p \in A$ implies $p \in P$, which means $A \subseteq P$. ■

Combined with the chart on the previous page, this theorem gives us a new perfect number! The element $p = 2^{13-1}(2^{13}-1) = 33,550,336$ in A is perfect.

Observe also that every element of A is a multiple of a power of 2, and therefore even. But this does not necessarily mean every perfect number is even, because we've only shown $A \subseteq P$, not $A = P$. For all we know there may be odd perfect numbers in $P - A$ that are not in A.

Are there any odd perfect numbers? No one knows.

In over 2000 years, no one has ever found an odd perfect number, nor has anyone been able to prove that there are none. But it *is* known that the set A does contain every *even* perfect number. This fact was first proved by Euler, and we duplicate his reasoning in the next theorem, which proves that $A = E$, where E is the set of all *even* perfect numbers. It is a good example of how to prove two sets are equal.

For convenience, we are going to use a slightly different definition of a perfect number. A number $p \in \mathbb{N}$ is **perfect** if its positive divisors add up to $2p$. For example, the number 6 is perfect since the sum of its divisors is $1+2+3+6 = 2 \cdot 6$. This definition is simpler than the first one because we do not have to stipulate that we are adding up the divisors that are *less than* p. Instead we add in the last divisor p, and that has the effect of adding an additional p, thereby doubling the answer.

Theorem 8.2 If $A = \{2^{n-1}(2^n-1) : n \in \mathbb{N}, \text{ and } 2^n-1 \text{ is prime}\}$ and $E = \{p \in \mathbb{N} : p \text{ is perfect and even}\}$, then $A = E$.

Proof. To show that $A = E$, we need to show $A \subseteq E$ and $E \subseteq A$.

First we will show that $A \subseteq E$. Suppose $p \in A$. This means p is even, because the definition of A shows that every element of A is a multiple of a power of 2. Also, p is a perfect number because Theorem 8.1 states that every element of A is also an element of P, hence perfect. Thus p is an even perfect number, so $p \in E$. Therefore $A \subseteq E$.

Next we show that $E \subseteq A$. Suppose $p \in E$. This means p is an even perfect number. Write the prime factorization of p as $p = 2^k 3^{n_1} 5^{n_2} 7^{n_2} \ldots$, where some of the powers n_1, n_2, $n_3 \ldots$ may be zero. But, as p is even, the power k must be greater than zero. It follows $p = 2^k q$ for some positive integer k and an odd integer q. Now, our aim is to show that $p \in A$, which means we must show p has form $p = 2^{n-1}(2^n-1)$. To get our current $p = 2^k q$ closer to this form, let $n = k+1$, so we now have

$$p = 2^{n-1} q. \tag{8.3}$$

List the positive divisors of q as $d_1, d_2, d_3, \ldots, d_m$. (Where $d_1 = 1$ and $d_m = q$.) Then the divisors of p are:

$$\begin{array}{ccccc} 2^0 d_1 & 2^0 d_2 & 2^0 d_3 & \ldots & 2^0 d_m \\ 2^1 d_1 & 2^1 d_2 & 2^1 d_3 & \ldots & 2^1 d_m \\ 2^2 d_1 & 2^2 d_2 & 2^2 d_3 & \ldots & 2^2 d_m \\ 2^3 d_1 & 2^3 d_2 & 2^3 d_3 & \ldots & 2^3 d_m \\ \vdots & \vdots & \vdots & & \vdots \\ 2^{n-1} d_1 & 2^{n-1} d_2 & 2^{n-1} d_3 & \ldots & 2^{n-1} d_m \end{array}$$

Since p is perfect, these divisors add up to $2p$. By Equation (8.3), their sum is $2p = 2(2^{n-1}q) = 2^n q$. Adding the divisors column-by-column, we get

$$\sum_{k=0}^{n-1} 2^k d_1 + \sum_{k=0}^{n-1} 2^k d_2 + \sum_{k=0}^{n-1} 2^k d_3 + \cdots + \sum_{k=0}^{n-1} 2^k d_m \quad = \quad 2^n q.$$

Applying Equation (8.1), this becomes

$$\begin{aligned} (2^n-1)d_1 + (2^n-1)d_2 + (2^n-1)d_3 + \cdots + (2^n-1)d_m &= 2^n q \\ (2^n-1)(d_1 + d_2 + d_3 + \cdots + d_m) &= 2^n q \\ d_1 + d_2 + d_3 + \cdots + d_m &= \frac{2^n q}{2^n - 1}, \end{aligned}$$

so that

$$d_1 + d_2 + d_3 + \cdots + d_m = \frac{(2^n - 1 + 1)q}{2^n - 1} = \frac{(2^n - 1)q + q}{2^n - 1} = q + \frac{q}{2^n - 1}.$$

From this we see that $\frac{q}{2^n-1}$ is an integer. It follows that both q and $\frac{q}{2^n-1}$ are positive divisors of q. Since their sum equals the sum of *all* positive divisors of q, it follows that q has only two positive divisors, q and $\frac{q}{2^n-1}$. Since one of its divisors must be 1, it must be that $\frac{q}{2^n-1} = 1$, which means $q = 2^n - 1$. Now a number with just two positive divisors is prime, so $q = 2^n - 1$ is prime. Plugging this into Equation (8.3) gives $p = 2^{n-1}(2^n - 1)$, where $2^n - 1$ is prime. This means $p \in A$, by definition of A. We have now shown that $p \in E$ implies $p \in A$, so $E \subseteq A$.

Since $A \subseteq E$ and $E \subseteq A$, it follows that $A = E$. ■

Do not be alarmed if you feel that you wouldn't have thought of this proof. It took the genius of Euler to discover this approach.

We'll conclude this chapter with some facts about perfect numbers.

- The sixth perfect number is $p = 2^{17-1}(2^{17} - 1) = 8589869056$.
- The seventh perfect number is $p = 2^{19-1}(2^{19} - 1) = 137438691328$.
- The eighth perfect number is $p = 2^{31-1}(2^{31} - 1) = 2305843008139952128$.
- The twentieth perfect number is $p = 2^{4423-1}(2^{4423} - 1)$. It has 2663 digits.
- The twenty-third perfect number is $p = 2^{11213-1}(2^{11213} - 1)$. It has 6957 digits.

As mentioned earlier, no one knows whether or not there are any odd perfect numbers. It is not even known whether there are finitely many or infinitely many perfect numbers. It **is** known that the last digit of every even perfect number is either a 6 or an 8. Perhaps this is something you'd enjoy proving.

We've seen that perfect numbers are closely related to prime numbers that have the form $2^n - 1$. Such prime numbers are called **Mersenne primes**, after the French scholar Marin Mersenne (1588–1648), who popularized them. The first several Mersenne primes are $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ and $2^{13} - 1 = 8191$. To date, only 48 Mersenne primes are known, the largest of which is $2^{57,885,161} - 1$. There is a substantial cash prize for anyone who finds a 49th. (See http://www.mersenne.org/prime.htm.) You will probably have better luck with the exercises.