Proof Template 6 Proving one set is a subset of another.

To show $A \subseteq B$:
Let $x \in A$. ... Therefore $x \in B$. Therefore $A \subseteq B$. ■

We illustrate the use of Proof Template 6 using the following concept.

Definition 10.4 **(Pythagorean Triple)** A list of three integers (a, b, c) is called a *Pythagorean triple* provided $a^2 + b^2 = c^2$.

Please note that $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is not a Pythagorean triple because the numbers in the list are not integers; the term *Pythagorean triple* only applies to lists of integers.

For example, $(3, 4, 5)$ is a Pythagorean triple because $3^2 + 4^2 = 5^2$. Pythagorean triples are so named because they are the lengths of the sides of a right triangle.

Proposition 10.5 Let P be the set of Pythagorean triples; that is,

$$P = \{(a, b, c) : a, b, c \in \mathbb{Z} \text{ and } a^2 + b^2 = c^2\}$$

and let T be the set

$$T = \{(p, q, r) : p = x^2 - y^2,\ q = 2xy,\ \text{and } r = x^2 + y^2 \text{ where } x, y \in \mathbb{Z}\}.$$

Then $T \subseteq P$.

For example, if we let $x = 3$ and $y = 2$ and we calculate

$$p = x^2 - y^2 = 9 - 4 = 5, \qquad q = 2xy = 12, \qquad r = x^2 + y^2 = 9 + 4 = 13$$

we find that $(5, 12, 13) \in T$. Proposition 10.5 asserts that $T \subseteq P$, which implies $(5, 12, 13) \in P$. Indeed, this is correct since

$$5^2 + 12^2 = 25 + 144 = 169 = 13^2.$$

We now develop the proof of Proposition 10.5 by utilizing Proof Template 6.

Let P and T be as in the statement of Proposition 10.5.
Let $(p, q, r) \in T$. ... Therefore $(p, q, r) \in P$. ■

Unravel the meaning of $(p, q, r) \in T$.

Let P and T be as in the statement of Proposition 10.5.
Let $(p, q, r) \in T$. Therefore there are integers x and y such that $p = x^2 - y^2$, $q = 2xy$, and $r = x^2 + y^2$. ... Therefore $(p, q, r) \in P$. ■

To verify that $(p, q, r) \in P$, we simply have to check that all three are integers (which is clear) and that $p^2 + q^2 = r^2$. We can write p, q, and r in terms of x and y, so the problem reduces to an algebraic computation. We finish the proof.

Let P and T be as in the statement of Proposition 10.5.

Let $(p, q, r) \in T$. Therefore there are integers x and y such that $p = x^2 - y^2$, $q = 2xy$, and $r = x^2 + y^2$. Note that p, q, and r are integers because x and y are integers. We calculate

$$\begin{aligned} p^2 + q^2 &= (x^2 - y^2)^2 + (2xy)^2 \\ &= (x^4 - 2x^2y^2 + y^4) + 4x^2y^2 \\ &= x^4 + 2x^2y^2 + y^4 \\ &= (x^2 + y^2)^2 = r^2. \end{aligned}$$

Therefore (p, q, r) is a Pythagorean triple and so $(p, q, r) \in P$. ■

The symbols $\in$ and $\subseteq$ may be written backward: $\ni$ and $\supseteq$. The notation $A \ni x$ means exactly the same thing as $x \in A$. The symbol $\ni$ can be read, "contains the element." The notation $B \supseteq A$ means exactly the same thing as $A \subseteq B$. We say that B is a *superset* of A.

(We also say that B contains A and A is contained in B, but the word *contains* can be a bit ambiguous. If we say "B contains A," we generally mean that $B \supseteq A$, but it might mean $B \ni A$. We avoid this term unless the meaning is utterly clear from context.)

Counting Subsets

How many subsets does a set have? Let us consider an example.

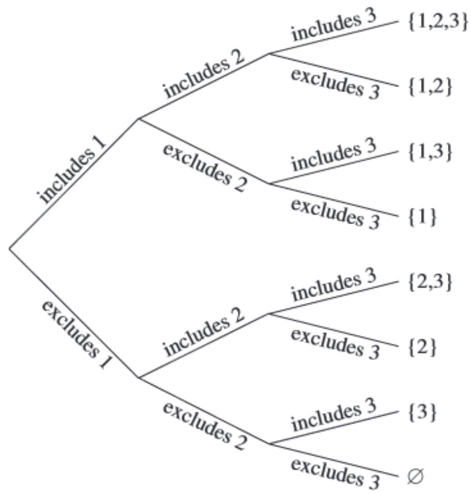
Example 10.6 How many subsets does $A = \{1, 2, 3\}$ have?

The easiest way to do this is to list all the possibilities. Since $|A| = 3$, a subset of A can have anywhere from zero to three elements. Let's write down all the possibilities organized this way.

Number of elements	Subsets	Number
0	$\emptyset$	1
1	$\{1\}, \{2\}, \{3\}$	3
2	$\{1,2\}, \{1,3\}, \{2,3\}$	3
3	$\{1,2,3\}$	1
	Total:	8

Therefore, there are eight subsets of $\{1, 2, 3\}$.

There is another way to analyze this problem. Each element of the set $\{1, 2, 3\}$ either is a member of or is not a member of a subset. Look at the following diagram.



For each element, we have two choices: to include or not to include that element in the subset. We can "ask" each element if it "wants" to be in the subset. The list of answers uniquely determines the subset. So if we ask elements 1, 2, and 3 in turn if they are in the subset and the answers we receive are (yes, yes, no), then the subset is $\{1, 2\}$.

The problem of counting subsets of $\{1, 2, 3\}$ reduces to the problem of counting lists, and we know how to count lists! The number of lists of length three where each entry on the list is either "yes" or "no" is $2 \times 2 \times 2 = 8$.

This list-counting method gives us the solution to the general problem.

Theorem 10.7 Let A be a finite set. The number of subsets of A is $2^{|A|}$.

Proof. Let A be a finite set and let $n = |A|$. Let the n elements of A be named $a_1, a_2, \ldots, a_n$. To each subset B of A we can associate a list of length n; each element of the list is one of the words "yes" or "no." The k^{th} element of the list is "yes" precisely when $a_k \in B$. This establishes a correspondence between length-n yes-no lists and subsets of A. Observe that each subset of A gives a yes-no list, and every yes-no list determines a different subset of A. Therefore the number of subsets of A is exactly the same as the number of length-n yes-no lists. The number of such lists is 2^n, so the number of subsets of A is 2^n where $n = |A|$. ■

This style of proof is called a *bijective* proof. To show that two counting problems have the same answer, we establish a one-to-one correspondence between the two sets we want to count. If we know the answer to one of the counting problems, then we know the answer to the other.

Power Set

A set can be an element of another set. For example, $\{1, 2, \{3, 4\}\}$ is a set with three elements: the number 1, the number 2, and the set $\{3, 4\}$. A special example of this is called the *power set* of a set.

Definition 10.8 (**Power set**) Let A be a set. The *power set* of A is the set of all subsets of A.

For example, the power set of $\{1, 2, 3\}$ is the set

$$\Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\Big\}.$$

The power set of A is denoted 2^A. However, some authors also use the notation $\mathcal{P}(A)$.

Theorem 10.7 tells us that if a set A has n elements, its power set contains 2^n elements (the subsets of A). As a mnemonic, the notation for the power set of A is 2^A. This is a special notation; there is no general meaning for raising a number to an exponent that is a set. The only case in which this makes sense is writing the set as a superscript on the number 2; the meaning of the notation is the power set of A. This notation was created so that we would have

$$\left|2^A\right| = 2^{|A|}$$

for any finite set A. The left side of this equation is the cardinality of the power set of A; the right side is 2 raised to the cardinality of A. On the left, the superscript on 2 is a set, so the notation means power set; on the right, the superscript on 2 is a number, so the notation means ordinary exponentiation.

Recap

In this section, we introduced the concept of a set and the notation $x \in A$. We presented the set-builder notation $\{x \in A : \ldots\}$. We discussed the concepts of empty set ($\emptyset$), subset ($\subseteq$), and superset ($\supseteq$). We distinguished between finite and infinite sets and presented the notation $|A|$ for the cardinality of A. We considered the problem of counting the number of subsets of a finite set and defined the power set of a set, 2^A.