Chapter 8. Proofs involving sets:

In this chapter, we are going to see how we can show that an object is an element of a set or how to prove that a set is a subset of another or how to show two sets are equal. This is going to be important since most of the properties that certain mathematical objects share can be given in set form, within set builder notation.

E.g. \( E = \{ n \in \mathbb{N} : n \text{ is even} \} \) or \( E_2 = \{ n \in \mathbb{N} : n^2 \text{ is even} \} \).

We saw that for \( n \in \mathbb{N} \), \( n \) is even \( \iff n^2 \) is even.

So, the immediate question is, how can this proposition translate to a proposition about sets \( E \), \( a, E_2 \)?

Before starting proving things, let’s recall some definitions: If \( A \) and \( B \) are sets, then

\[
A \times B = \{ (x, y) : x \in A, y \in B \}
\]

\[
A \cup B = \{ x : (x \in A) \lor (x \in B) \}
\]

\[
A \cap B = \{ x : (x \in A) \land (x \in B) \}
\]

\[
A - B = \{ x : (x \in A) \land (x \notin B) \}
\]

\( \bar{A} = U - A \) where \( U \) denotes the universal set.

Moreover \( A \subseteq B \) means that every element of \( A \) is an element of \( B \).

8.1: How to prove \( a \in A \).

Recall that we can express most of the sets in set builder notation, say \( A = \{ x : P(x) \} \). Recall that this reads as “\( A \) is the set of all \( x \)’s for which the open statement \( P(x) \) holds. For example,
Another way of writing a set is: \( A = \{ x \in S : P(x) \} \), which says that we are not looking at the set of all \( x \)'s for which \( P(x) \) holds, we are looking at all \( x \)'s which are in the set \( S \) for which \( P(x) \) holds. For example:

\[
\begin{align*}
\{ x \in \mathbb{R} : x^2-2=0 \} &= \{-\sqrt{2}, \sqrt{2} \} \quad \text{whereas} \\
\{ x \in \mathbb{N} : x^2-2=6 \} &= \emptyset, \quad \text{since there are no natural numbers for which } x^2-2=0.
\end{align*}
\]

Ex: \( \cdot \{ x \in \mathbb{N} : 6 \mid x \} = \{ 6, 12, 18, 24, \ldots \} \)
\( \cdot \{ (a, b) \in \mathbb{Z} \times \mathbb{Z} : b = a+5 \} = \{ \ldots, (-2,3), (-1,4), (0,5), (1,6), \ldots \} \)
\( \cdot \{ x \in \mathbb{P}(\mathbb{Z}) : |x|=1 \} = \{ \ldots, -1, 1 \} \}

Now, we can see that, to show \( x \in \mathbb{P}(\mathbb{N}) \), we need to show that \( P(a) \) holds, e.g. \( 9 \notin A_p \), since \( 9 \) is not prime.

Similarly, to show \( a \in \{ x \in S : P(x) \} \), we first need to make sure that \( a \notin S \) and then we need to show \( P(a) \) is true.

Ex: Is \( 2 \in \{ x \in \mathbb{N} : 6 \mid x \} ? \)

We see that \( 2 \in \mathbb{N} \), so that is good, but we also see that \( 6 \nmid 2 \) i.e. \( 2 \notin \{ x \in \mathbb{N} : 6 \mid x \} \) since at least one of the conditions is not satisfied.

\( \cdot \) Is \( \sqrt{2} \in \{ x \in \mathbb{N} : 6 \mid x \} ? \)

We know that \( \sqrt{2} \notin \mathbb{N} \), thus \( \sqrt{2} \notin \{ x \in \mathbb{N} : 6 \mid x \} \).

\( \cdot \) Is \( \{ 1, 3 \} \in \{ x \in \mathbb{P}(\mathbb{Z}) : |x|=1 \} ? \)

We see that \( \{ 1, 3 \} = 1 \) but \( \frac{1}{2} \notin \mathbb{Z} \) and thus \( \{ 1, 3 \} \notin \mathbb{P}(\mathbb{Z}) \). Therefore \( \{ 1, 3 \} \notin \{ x \in \mathbb{P}(\mathbb{Z}) : |x|=1 \} \).

Ex: Consider the set \( B = \{ (x,y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{5} \} \).
For $n \in \mathbb{Z}$, show that the pair $(4n+3, 9n-2) \in B$.

We see that since $n \in \mathbb{Z}$, $4n+3 \in \mathbb{Z}$ and $9n-2 \in \mathbb{Z}$, i.e. the ordered pair $(4n+3, 9n-2) \in \mathbb{Z} \times \mathbb{Z}$. Now the question is $4n+3 \equiv 9n-2 \pmod{5}$? (Recall the defn: $a \equiv b \pmod{m}$ if $m \mid (a-b)$.) We see that $(4n+3)-(9n-2)=5-5n+5(4-n)$ i.e. $5 \mid (4n+3)-(9n-2)$ which means $4n+3 \equiv 9n-2 \pmod{5}$. Therefore $(4n+3, 9n-2) \in B$.

Recall that we can express the sets of the form $A = \{ n : n = f(k) \text{ for } k \in S \}$ also as $A = \{ f(k) : k \in S \}$. This means that $A$ is the set of all objects of the form $f(k)$ where $k \in S$.

Ex: $A = \{ f(k+1) : n \in \mathbb{Z} \}$ is the set of all numbers of the form $2n+1$ for some $n \in \mathbb{Z}$. We know this set, this is the set of odd numbers. Now, let's see how we can show that an object is an element of such a set.

Ex: Let $C = \{ x^2+2x : x \in \mathbb{R} \}$. Is $8 \in C$?

To check that, we need to see whether $8$ can be written in the form $x^2+2x$ for some $x \in \mathbb{R}$, i.e. is there an $x \in \mathbb{R}$ s.t. $x^2+2x=8$?

We see that $x^2+2x=8 \Rightarrow x^2+2x-8=0$ i.e. $x=2$ or $x=-4$ satisfy $x^2+2x=8$. Thus $8 \in C$.

What about $-2$? Is $-2 \in C$? Let's check:

We want to see whether $-2 = x^2+2x$ for some $x \in \mathbb{R}$. $-2 = x^2+2x \Rightarrow x^2+2x+2=0 \Rightarrow (x^2+2x+1)=0 \Rightarrow (x+1)^2=0$, i.e. $(x+1)^2=0$ which is not satisfied by any real number $x$. Thus $-2 \notin C$. 

How to Prove an Object is in a Set Page 3
8.2 & 8.3: How to Prove $A \subseteq B$ & $A = B$.

In the previous chapter we saw how to prove that an object is in a set. In this section we are going to learn how to show that a set $A$ is a subset of another set $B$ and how to show that those two sets are equal.

To show $A \subseteq B$, we need to remember what this subset relation means. Recall that we say $A$ is a subset of $B$, denoted by $A \subseteq B$ if every element of $A$ is also an element of $B$. In other words, $(A \subseteq B)$ if $(a \in A \Rightarrow a \in B)$.

This means that, to show that $A \subseteq B$, all we need to do is to show that if $a \in A$, then $a \in B$, or if we consider the contrapositive, we can also show if $a \notin B$, then $a \notin A$. 

Let's see this in examples:

**Example 1:** Prove that \( \{x \in \mathbb{Z} : 18 \mid x^3 \} \subseteq \{x \in \mathbb{Z} : 6 \mid x^3 \} \).

**Proof of example 1:** To show this subset relation we need to show that every element of the set \( \{x \in \mathbb{Z} : 18 \mid x^3 \} \) (i.e., the set of multiples of 18) is an element of the set \( \{x \in \mathbb{Z} : 6 \mid x^3 \} \) (i.e., the set of multiples of 6). In other words, we need to show if \( a \in \{x \in \mathbb{Z} : 18 \mid x^3 \} \), then \( a \in \{x \in \mathbb{Z} : 6 \mid x^3 \} \).

Let's prove it directly. Assume \( a \in \{x \in \mathbb{Z} : 18 \mid x^3 \} \), then we see that \( 18 \mid a \) i.e., \( a = 18n \) for some \( n \in \mathbb{Z} \). Thus \( a = 6(3n) \) which implies \( 6 \mid a \) and hence \( a \in \{x \in \mathbb{Z} : 6 \mid x^3 \} \). Therefore we get,

\( \{x \in \mathbb{Z} : 18 \mid x^3 \} \subseteq \{x \in \mathbb{Z} : 6 \mid x^3 \} \).

**Example 2:** Prove that if \( A \) and \( B \) are sets, then \( \mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B) \).
Proof of example 2: We are going to use direct proof again, i.e. we are going to assume that a set $X$ is an element of $\mathcal{P}(A) \cup \mathcal{P}(B)$ and will show that $X \in \mathcal{P}(A \cup B)$.

Suppose $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Then $X \in \mathcal{P}(A)$ or $X \in \mathcal{P}(B)$. This means we have two cases to consider.

Case 1: $X \in \mathcal{P}(A)$: Then we see $X \subseteq A$. Thus we see $(X \subseteq A$ or $X \subseteq B)$, which implies $X \subseteq A \cup B$. Therefore $X \in \mathcal{P}(A \cup B)$.

Case 2: $X \in \mathcal{P}(B)$: Similar to case 1, if $X \in \mathcal{P}(B)$, then $X \subseteq B$ & thus $X \subseteq A \cup B$. Hence $X \in \mathcal{P}(A \cup B)$.

Therefore we see that any element of the union $\mathcal{P}(A) \cup \mathcal{P}(B)$ is an element of $\mathcal{P}(A \cup B)$ i.e.

\[ \mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B). \]

\[ \Box \]

Example 3: Suppose $A$ and $B$ are sets. Then if
$\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.

**Proof of example 3:** We are going to use direct proof again.

Suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. We want to show $A \subseteq B$, i.e., we want to show if $a \in A$, then $a \in B$. Assume $a \in A$. Then we know that $\exists b \in A$ and hence $\{a\} \in \mathcal{P}(A)$. Since we know that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, we see that $\{a\} \in \mathcal{P}(B)$ i.e., $\{a\} \subseteq B$; or in other words, $b \in B$.

Therefore $(\mathcal{P}(A) \subseteq \mathcal{P}(B)) \Rightarrow (A \subseteq B)$. (Actually we can easily show that this is an "iff" statement).

Now, recall that if $A$ and $B$ are sets, then $A = B \iff (A \subseteq B) \cap (B \subseteq A)$. So, to show $A = B$ we need to show $A \subseteq B$ and $B \subseteq A$.

**Example 4:** Prove that

$\{n \in \mathbb{Z} : 3 \mid n\} = \{n \in \mathbb{Z} : 5 \mid n\} \cap \{n \in \mathbb{Z} : 7 \mid n\}$. 

How to Prove Subset Relations and Equality of Sets Page 7
Proof of example 4: As we mentioned above, we need to show both

1. \( \{ n \in \mathbb{Z} : 35 \mid n \} \subseteq \{ n \in \mathbb{Z} : 5 \mid n \} \cap \{ n \in \mathbb{Z} : 7 \mid n \} \)

And

2. \( \{ n \in \mathbb{Z} : 35 \mid n \} \supseteq \{ n \in \mathbb{Z} : 5 \mid n \} \cap \{ n \in \mathbb{Z} : 7 \mid n \} \)

Let’s prove 1 first: Suppose \( a \in \{ n \in \mathbb{Z} : 35 \mid n \} \), then \( 35 \mid a \), i.e. \( \exists m \in \mathbb{Z} \) s.t. \( a = 35m \). This means \( a = 7(5m) \), i.e. \( 7 \mid a \) and \( a = 5(7m) \), i.e. \( 5 \mid a \). Thus \( a \in \{ n \in \mathbb{Z} : 7 \mid n \} \) and \( a \in \{ n \in \mathbb{Z} : 5 \mid n \} \). Hence \( a \in \{ n \in \mathbb{Z} : 7 \mid n \} \cap \{ n \in \mathbb{Z} : 5 \mid n \} \). This shows part 1.

Now let’s prove part 2: Suppose \( a \) is an element of \( \{ n \in \mathbb{Z} : 5 \mid n \} \cap \{ n \in \mathbb{Z} : 7 \mid n \} \). Then we see that \( 5 \mid a \) and \( 7 \mid a \). This implies \( \exists m, s \in \mathbb{Z} \) st. \( a = 5m \) and \( a = 7s \). Since \( 5 \mid 7 \), we see that \( 5 \mid s \). Thus, \( s = 5t \) for some \( t \in \mathbb{Z} \). Therefore \( a = 7s = 7(5t) = 35t \) for some \( t \in \mathbb{Z} \). Hence
35l, which implies $a \in \{n \in \mathbb{Z} : 35|n\}$. This shows part 2. Therefore we have shown $\{n \in \mathbb{Z} : 35|n\} = \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$. 

**Example 5:** Suppose $A, B, \text{ and } C$ are sets, and $C \neq \emptyset$. Prove that if $A \times C = B \times C$, then $A = B$.

**Proof of example 5:** Suppose $A \times C = B \times C$, then we want to show $A = B$.

**First show $A \subseteq B$:** Let $a \in A$. Then since $C \neq \emptyset$, we know that there exists $c \in C$, and $(a, c) \in A \times C$. We also know that $A \times C = B \times C$, which implies that $(a, c) \in B \times C$. By the definition of the cross product, we see that $a \in B$ (and $c \in C$). Thus $A \subseteq B$.

**Prove $B \subseteq A$:** This argument follows similarly as the previous case.
Therefore we see that \( A \subseteq B \) & \( B \subseteq A \) which means \( A = B \). \( \Box \)