

1. Quantifiers.

- (a) The quantifier “
- $\forall$
- ” means “for all,” or “for each,” or “for every.”

If X is a set and $Q(x)$ is a statement about a quantity x , then the statement

$$\forall x \in X: Q(x)$$

means the statement $Q(x)$ is true for every x in X .

- (b) The quantifier “
- $\exists$
- ” means “for some,” or “for at least one,” or “there exists.”

If X is a set and $Q(x)$ is a statement about a quantity x , then the statement

$$\exists x \in X: Q(x)$$

means the statement $Q(x)$ is true for some (at least one, possibly more) x in X .

2. Proof templates.

- (a)
- $P \Rightarrow Q$
- , direct proof.

Theorem. $P \Rightarrow Q$.

Proof. Assume P . [Now do what you need to conclude:] Therefore, Q .

So $P \Rightarrow Q$. $\square$

- (b)
- $P \Rightarrow Q$
- , contrapositive proof.

Theorem. $P \Rightarrow Q$.

Proof. Assume $\sim Q$. [Now do what you need to conclude:] Therefore, $\sim P$.

So $P \Rightarrow Q$. $\square$

- (c)
- $P \Leftrightarrow Q$
- .

Theorem. $P \Leftrightarrow Q$.

Proof. Assume P . [Now do what you need to conclude:] Therefore, Q .

So $P \Rightarrow Q$.

Next, assume Q . [Now do what you need to conclude:] Therefore, P .

So $Q \Rightarrow P$.

Therefore, $P \Leftrightarrow Q$. $\square$

- (d) Proofs with universal quantifiers.

Theorem. $\forall x \in X, Q(x)$.

Proof. Assume $x \in X$. [Now do what you need to conclude:] Therefore, $Q(x)$.

So $\forall x \in X, Q(x)$. $\square$

- (e) Proofs with existential quantifiers.

Theorem. $\exists x \in X, Q(x)$.

(Constructive) Proof. [Find a particular $x \in X$, call it x_0 , that has the property $Q(x)$. Then write:] Let $x = x_0$. Then ... [show that $Q(x_0)$ is true]. So $\exists x \in X, Q(x)$. $\square$

(A non-constructive proof would require showing that some such x_0 exists without producing it explicitly.)

- (f) Proof by contradiction.

Theorem. T .

Proof. Assume $\sim T$. [Then do what's necessary to derive a contradiction, and write:] Contradiction. Therefore T is true. $\square$

- (g) Proof by the principle of mathematical induction.

Theorem. $\forall n \in \mathbb{N}, A(n)$.

Proof. Step 1: Is $A(1)$ true? [Now do what you need to conclude:] So $A(1)$ is true.

Step 2: Assume $A(k)$. [Now do what you need to conclude:] So $A(k+1)$ follows. So $A(k) \Rightarrow A(k+1)$.

Therefore, by the principle of mathematical induction, $A(n)$ is true $\forall n \in \mathbb{N}$. $\square$

3. Some special sets.

- (a) $\mathbb{Z} = \{\text{integers}\} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.
 - (b) $\mathbb{N} = \{\text{natural numbers}\} = \{1, 2, 3, \dots\}$.
 - (c) $\mathbb{Z}_{\geq 0} = \{\text{nonnegative integers}\} = \{0, 1, 2, 3, \dots\}$.
 - (d) $\mathbb{R} = \{\text{real numbers}\} = (-\infty, \infty)$.
 - (e) $\mathbb{Q} = \{\text{rational numbers}\} = \{\text{fractions } m/n: m, n \in \mathbb{Z} \text{ and } n \neq 0\}$.
-

4. Facts about integers.

- (a) Let $a, b \in \mathbb{Z}$. We say a divides b , written $a|b$, if $b = na$ for some $n \in \mathbb{Z}$.
- (b) (Division algorithm.) Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.