"How to Create a Proof" by Allan Yashinski, condensed by Theodore

1. Proving conditional statement
("If P then Q")

1.1. Direct Proof

① Assume P.
② ⋮ (n−1) } working
(n) ∴ Q.

This shows that
$P \Rightarrow Q$.

1.2. Contrapositive

① Assume $\sim Q$.
② ⋮ (n−1) } working
(n) ∴ $\sim P$.

This shows that
~~$P \Rightarrow Q$~~
$\Leftrightarrow$ $\sim Q \Rightarrow \sim P$
∴ $P \Rightarrow Q$
by contraposition.

1.3. Contradiction

① Assume that P.
Additionally, assume $\sim Q$.
② ⋮ (n−1) } working
(n). This gives us a contradiction.
∴ $P \Rightarrow Q$

For 1.3. (contradiction), any contradiction ~~is~~ could work.
Some common ones: $0 = 1$, 8 is odd, $\varnothing$ contains an element, etc.

2. Proving Quantified Statements

2.1 a) Universal quantification, i.e. $\forall x \in X$, $P(x)$.
e.g. $\forall x \in \mathbb{R}$, $x^2 \geq 0$.

① Let x be an arbitrarily chosen element of X.
② ⋮ (n)] Prove P(x), without substituting in any value of x in. ~~($\Leftarrow$ This can be done)~~

∴ $\forall x \in X$, $P(x)$.

Example: $\forall x \in \mathbb{Z}$, 4x is even.
Answer: 1. Let x be an arbitrarily chosen ~~element~~ integer
2. ~~Consider 4x~~: We shall show that 4x is even
2.1. $4x = 2(2x)$ by basic algebra.
2.2. Let $k = 2x$. By closure of $\mathbb{Z}$ under multiplication, $k \in \mathbb{Z}$.
2.3. ∴ $4x = 2k$, $k \in \mathbb{Z}$
2.4 By the definition of even numbers, 4x is even.
3. ∴ $\forall x \in \mathbb{Z}$, 4x is even.

2.1 b) Universal quantification w/ conditional, i.e. $\forall x \in X \, (P(x) \Rightarrow Q(x))$

①. Let x be an arbitrary element of X.

② Prove that $P(x) \Rightarrow Q(x)$ without substituting specific value of x.
⋮ The proof for $P(x) \Rightarrow Q(x)$ is covered in T.1, 1.2, 1.3.
ⓝ

2.2) Existential quantification, i.e. $\exists x \in X, P(x)$

①. Consider x = something that makes $P(x)$ true.

② Show that $P(x)$ is true for the
⋮ value of x you have chosen in ①.
ⓝ

e.g. "There is an even prime number"

$\exists p \in \mathbb{Z}$ (p is even $\wedge$ p is prime).

Answer: 1. Consider $x = 2$, $x \in \mathbb{Z}$ as $2 \in \mathbb{Z}$.

2. 2 is even as $2 = 2 \times 1$ (basic algebra & definition of even nº).

3. 2 is a prime (by ...)

4. $\therefore$ 2 is even $\wedge$ 2 is prime

5. ~~[illegible]~~ $\therefore$ There is an even prime number.

* Provide an explicit example and ~~write down~~ make sure that it lies within the domain of discourse (write it down, like above I wrote $2 \in \mathbb{Z}$).

* You do not need to tell me how you get your specific value of x. Save that for your own rough paper.

* Don't try to be smart! Keep your answer simple. For example, if asked to prove "there is an odd prime number", don't say "every prime number p that is not 2 is odd" — you're opening a can of worms. Just give the explicit example $p = 3$ and you're done.

2.3 Multiple Quantifiers

2.3.1. Mixed Quantifiers.

I will illustrate with an example:

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}\ (y > x)$: Read this as $\forall x \in \mathbb{R}\ (\exists y \in \mathbb{R}\ (y > x))$.

Proof

1. Choose an arbitrary real number x.
   <This step is same as 2.1a.>
   <Notice that what you're left with is $\exists y \in \mathbb{R}\ y > x$>.
   <What's left is follow 2.2>.
2. Consider $y = x + 1$.
   $y \in \mathbb{R}$ due to closure of $\mathbb{R}$ under $+$.
   <After this, all that's left is to show $y > x$>.
3. Now, $x + 1 > x$ by basic algebra.
   $\therefore y > x$
4. $\therefore \forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\ y > x$.

2.3.2. Quantifiers of same type

Example : Show that $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 5x - 2$ is injective.

Definition of injective : A function $f : X \to Y$ is injective if
$\forall x_1 \in X, \forall x_2 \in X, \left((f(x_1) = f(x_2)) \Rightarrow x_1 = x_2 \right)$.

Example (rephrased):
Show that $\forall x_1 \in \mathbb{R}\ \forall x_2 \in \mathbb{R}, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
where $f(x) = 5x - 2$.

Answer :

1. Let x_1 and x_2 be arbitrary real numbers.
   <For quantifiers of the same type, you can do this in 1 step>.
2. <We will do direct proof>
   Assume $f(x_1) = f(x_2)$
   - 2.1 $5x_1 - 2 = 5x_2 - 2$
   - 2.2 $5x_1 = 5x_2$
   - 2.3 $x_1 = x_2$ (by basic algebra).

   $\therefore f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
3. $\therefore \forall x_1 \in \mathbb{R}, \forall x_2 \in \mathbb{R}, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
4. $\therefore f$ is an injective function.

Another example: Show that $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is not injective.
Rephrased: Show that $\exists x_1 \in \mathbb{R}, \exists x_2 \in \mathbb{R} \left((f(x_1) = f(x_2)) \wedge (x_1 \neq x_2) \right)$ where $f(x) = x^2$.

Answer.

1. Consider $x_1 = 1 \in \mathbb{R}$, $x_2 = -1 \in \mathbb{R}$.
2. Then $f(x_1) = 1^2 = 1$ and $f(x_2) = (-1)^2 = 1$
   $\therefore f(x_1) = f(x_2)$.
   But $x_1 \neq x_2$ as $1 \neq -1$.
3. $\therefore \exists x_1 \in \mathbb{R}, \exists x_2 \in \mathbb{R} \left((f(x_1) = f(x_2)) \wedge (x_1 \neq x_2) \right)$.
4. $\therefore f$ is not injective.

3. Definitions

1. X is a <term being defined> if <some logical statement about X>.
2. <term being defined> is <logical statement>

*Note: the if here really means if and only if.
This is the case only for definitions!

e.g

1. n is <u>even</u> if $\exists k \in \mathbb{Z}, n = 2k$.
1. a set A is <u>a subset of set B</u> if $(\forall x)(x \in A \Rightarrow x \in B)$
2. the <u>power set</u> of a set A is the set $\mathcal{P}(A) = \{S : S \subseteq A\}$.

Definitions are useful because they are equivalent statements!
For example, to prove that x is even, you just need to show that $\exists k \in \mathbb{Z}, x = 2k$.
Or, if you want to show that $\mathbb{Z}$ is a subset of $\mathbb{Q}$, you just need to show $(\forall x)(x \in \mathbb{Z} \Rightarrow x \in \mathbb{Q})$.

TL;DR: The logical structure of a statement determines the general structure of its proof.