§ 3.3 Proofs including quantifiers

Strategy: To prove a goal of form $\forall x P(x)$,
Let x be arbitrary, change goal to $P(x)$.

Form: Let x be arbitrary,
[proof of $P(x)$].
Since x is arbitrary, we have show $\forall x P(x)$.

Ex: Suppose $A \setminus B$ and C are disjoint, prove $A \cap C \subseteq B$.

Given	Goal
$(A \setminus B) \cap C = \phi$	$A \cap C \subseteq B$. $\rightarrow$ reexpress.
$\cancel{\forall x \in A \cap C}$	$\cancel{\forall x (x \in A \cap C \rightarrow x \in B)}$.
$\cancel{\forall x (x \in A \wedge x \in C)}$	contradiction.
$\forall x\, x \in A$, $\forall x, x \in C$.	
$x \notin B$	
$\neg \exists y (y \in A \wedge y \notin B \wedge y \in C)$	

Proof: to show $A \cap C \subseteq B$, we must show that for every element of $A \cap B$ is in B. Let x be arbitrary, $x \in A \cap C$, Therefore $x \in A \wedge x \in C$, [Suppose $x \notin B$, Since $x \in A$ and $x \notin B$, $x \in A \setminus B$. Since $x \in C$, $x \in (A \setminus B) \cap C$, This contradict our assumption. So since x is arbitrary, we conclude that every element of $A \cap B$ is in B $\square$.

Shortcut: to proof $\forall x (P(x) \rightarrow Q(x))$
- Let x be arbitrary,
- Add $P(x)$ to given
- Change goal to $Q(x)$

Ex: $\forall x \in A\ P(A)$ is a shortcut $\forall x$
Let x be assumption.
Add $x \in A$ to givens,
Change goal to $P(x)$.

Ex: 3.3.2. if $A \cap B = A$, then $A \subseteq B$.

Given	Goal
$A \cap B = A$	$\cancel{A \cap B = A \rightarrow A \subseteq B}$.
$x \in A$	$x \in B$

Proof: Assume $A \cap B = A$, and $x \in A$, show $A \cap B = A$, we have $x \in A \cap B$, so $x \in B$ Since x is arbitrary, $x \in B$.
Therefore, if $A \cap B = A$, then $A \subseteq B$.

过个 San Check 吧 23]

Ex: Let A, be a. $P(A) \neq \emptyset$

Given Goal.

$P(A) \neq \emptyset$.

$\Leftarrow 2^{2^2}$

Prove: To show $P(A) \neq \emptyset$, we give an element of $P(A)$. Since $\emptyset \subseteq A$, $\emptyset \in P(A)$.

Form: Let x be ....

[proof of P cthe value].

Therefore there exist x that $P(x)$.

Def: For $a, b \in \mathbb{Z}$, write $a|b$ to mean $\exists k \in \mathbb{Z} (b = ka)$

Ex: Prove that for all integer a, b, c, if $a|b$, $a|c$, then $a|(b+c)$.

Proof: Since $a|b$, there exist $k_1 \in \mathbb{Z}$ that $b = k_1 a$. $a|c$, so there is $k_2 \in \mathbb{Z}$ that $c = k_2 a$. Thus $b + c = k_1 a + k_2 a = (k_1 + k_2) a$. Since k_1, k_2 are all integers, so $a|(b+c)$ $\square$.