3.2: Direct Proofs

$$\forall\, x \in S,\ P(x) \rightarrow Q(x)$$

Since you choose arbitrarily, it must be true for all $x \in S$

- Direct Proof (otherwise known as Generalization from the Generic Particular): Choose an arbitrary element from the domain S satisfying the hypothesis $P(x)$ and show $Q(x)$ must also be true.

  because of vacuous truth
- Most "standard" way to prove a universal statement.
- Note: The book examples in this section are a little too sketchy - for now, we want details!

“Step-by-step method” to writing a direct proof

1. Rewrite the statement formally, in the form $\forall x \in S, P(x) \to Q(x)$.
2. “Proof: Let x be an arbitrary element of S such that $P(x)$.”
   Leave space
3. Write down what you would like to conclude – namely, $Q(x)$.
4. Apply definitions, both moving forward from $P(x)$ and backwards from $Q(x)$.
5. Make the two ends meet! (Hard part...)
6. End with, “Therefore, $Q(x)$ (and you’ll usually want some justification in this sentence, too).”

Example - Following outline above.

Prove: The sum of any two even integers is even.

Rewrite: $\forall n, m \in \mathbb{Z}$, if n and m are even, then $n+m$ is even.

Proof: Let n and m be arbitrary integers such that n and m are even. By the definition of even, $n = 2k$ for some integer k and $m = 2\ell$ for some integer ℓ. Now substituting,

$$n+m = 2k + 2\ell = 2(k+\ell).$$

Since k and ℓ are integers, $k+\ell$ is an integer.

Therefore, $n+m$ is even by the definition of even.

scrap:
$n+m = 2(\text{int})$
any integer!

Example - more concise.

Prove: The sum of any two even integers is even.

$\forall\, n, m \in \mathbb{Z},\ n, m \text{ even} \longrightarrow n+m \text{ even}$

Proof: Let n and m be arbitrary even integers. By the definition of even, $n=2k$ and $m=2\ell$ for some $k, \ell \in \mathbb{Z}$. Now substuting, $n+m=2k+2\ell=2(k+\ell)$. Since integers are closed under addition, $k+\ell \in \mathbb{Z}$. Therefore $n+m$ is even by definition.

3.3: Proof by Contrapositive

- Recall that conditional statements are logically equivalent to their contrapositives:

$$\forall x \in S, P(x) \to Q(x) \equiv \forall x \in S, \sim Q(x) \to \sim P(x)$$

- If we prove the contrapositive of a statement is true, we can conclude that the original statement is true.
- When to use this: When it's easier to say what it means for $Q(x)$ to be *false* than it is to say what it means for $P(x)$ to be *true*.

Proving biconditionals

$(P \to Q) \wedge (Q \to P)$

$\downarrow$

Proving statements of the form $\forall x \in S,\ P(x) \Leftrightarrow Q(x)$:

- Two things to prove:
  1. $\forall x \in S,\ P(x) \to Q(x)$
  2. $\forall x \in S,\ Q(x) \to P(x)$
- If it is easier (or prettier), you can prove $\forall x \in S$, $\underbrace{\sim P(x) \to \sim Q(x)}_{\text{the contrapositive of (2)}}$ in place of (2).

Example - biconditional.

Prove: Suppose $n \in \mathbb{Z}$. Then n is even if and only if $11n - 1$ is odd.

To prove: $\underbrace{n \text{ even} \rightarrow 11n-1 \text{ odd}}_{\text{looks easy to do directly}}$ and $\underbrace{11n-1 \text{ odd} \rightarrow n \text{ even}}$

- Assuming $11n-1$ is odd isn't so helpful.
- If we use contrapositive: Prove n not even $\rightarrow 11n-1$ not odd

Easier!

Pf: ($\rightarrow$) Suppose first that n is even. By definition, $n=2k$ for some integer k. Now substituting,

$$11n-1 = 11(2k)-1 = 2(11k)-1 = 2(11k-1)+2-1 = 2(11k-1)+1$$

Since $k \in \mathbb{Z}$, $11k-1 \in \mathbb{Z}$. Thus $11n-1$ is odd by definition.

($\leftarrow$) Now suppose that n is not even. Hence n is odd, and $n = 2k+1$ for some integer k. Substituting,

$$11n - 1 = 11(2k+1) - 1 = 22k + 11 - 1 = 22k + 10 = 2(11k+5)$$

and since $k \in \mathbb{Z}$, $11k+5$ is an integer. Thus $11n-1$ is even by the definition of even, and therefore $11n-1$ is not odd.

Example - Using a lemma

Prove: Let $n \in \mathbb{Z}$. If $3n+1$ is even, then $5n-2$ is odd.

Idea: Assuming $3n+1$ is even isn't particularly helpful, nor is assuming $5n-2$ is not odd.

But: If $3n+1$ is even, I see that $3n$ is odd, so n must be odd. This would help me show that $5n-2$ is odd.

Lemma: $\forall\, n \in \mathbb{Z}$, if $3n+1$ is even, then n is odd.

Pf: Let n be an arbitrary integer, and suppose that n is not odd. Thus n is even, and $n=2k$ for some integer k. Now $3n+1 = 3(2k)+1 = 2(3k)+1$. Since

k is an integer, $3k \in \mathbb{Z}$, hence $3n+1$ is odd by definition. Therefore $3n+1$ is not even.

Proof of theorem: Suppose $3n+1$ is even. By the lemma, n must be odd. Thus $n = 2k+1$ for some $k \in \mathbb{Z}$. By substitution,

$$5n-2 = 5(2k+1)-2 = 10k+5-2 = 10k+3 = 2(5k+1)+1.$$

Since the integers are closed under addition and multiplication, $5k+1 \in \mathbb{Z}$. Therefore $5n-2$ is odd by the definition of odd.

Example - Proof by cases

Prove: For $x, y \in \mathbb{Z}$, $x + y$ is even if and only if x and y have the same parity.

To prove:

$x+y$ even $\rightarrow$ x, y same parity

Not super helpful to assume this

Would rather assume not (same parity) (i.e. different parity)

x, y same parity $\rightarrow$ $x+y$ even

But if x and y are arbitrary, what parity? Two cases: ① even and ② odd

Note: Since $x+y$ is symmetric ($x+y=y+x$), we can arbitrarily choose either x even, y odd or vice versa

Pf: ($\leftarrow$) Suppose first that x and y are arbitrary integers with the same parity. We consider two cases.

Case 1: x and y are even. Then $x=2k$ and $y=2m$ for some $k, m \in \mathbb{Z}$. Now $x+y = 2k+2m = 2(k+m)$, and since $k+m$ is an integer, $x+y$ is even.

Case 2 : x and y are odd. Now $x = 2n+1$ and $y = 2\ell+1$ for some $n, \ell \in \mathbb{Z}$, and $x+y = (2n+1)+(2\ell+1) = 2(n+\ell+1)$. Again, we see that $x+y$ is even.

$(\rightarrow)$ Now assume x and y have different parity. By symmetry, we may assume that x is even and y is odd. By definition, $x = 2s$ and $y = 2t+1$ for some $s, t \in \mathbb{Z}$. Substituting,

$$x+y = 2s + (2t+1) = 2(s+t)+1.$$

Since the integers are closed under addition, $s+t \in \mathbb{Z}$. Therefore $x+y$ is odd by definition, and $x+y$ is not even.