S. KIMMEL

Goals

- Improve clarity & style of proof writing
- Be able to describe + write
    - Direct Proofs
    - Proof by contrapositive
    - Proof by cases (Friday)

Announcements

- PS3 Quiz Friday
- Test 1^{st} Pages
    - Up to PS4
    - Up to today/friday
- Other

S.KIMMEL

Direct Proof

- Usually used to prove implication like $P \to Q$.

Structure:

Assume P. Explain, explain, ... explain. Therefore Q

"By definition..."

- Also used to prove universal implication: $\forall x\,(P(x) \to Q(x))$

x in some Domain

Structure:

Let x be [any / an arbitrary] element of the domain

Assume $P(x)$

Explain, explain, explain.

Therefore $Q(x)$

☆ Connection to Inductive step ☆

Inductive step, we prove $\forall k \in \mathbb{Z}, (k \geq \text{base case}) \to (P(k) \to P(k+1))$

"Let $k \geq 1$. Assume for induction $P(k)$ is true ...

Explain

Explain

Explain

Therefore $P(k+1)$ is true

S.KIMMEL

Q: Use a direct proof to show: For all $a, b, c \in \mathbb{Z}$, if $a|b$ and $b|c$ then $a|c$.

($a|b$ means a divides b, that $\exists\, e \in \mathbb{Z}: ae = b$.

Let $a, b, c \in \mathbb{Z}$. Assume $a|b$ and $b|c$. This means $\exists\, e, f \in \mathbb{Z}$ such that $b = ae$ and $c = bf$. Then

$$c = bf = (ae)f = a(ef).$$

But this means $a|c$, since $c = ak$, for $k = ef$, an integer.

S.KIMMEL

Proof By Contrapositive

- used to prove implication like $P \to Q$.

Recall: $P \to Q$ is logically equivalent to $\neg Q \to \neg P$

Structure:

We prove the contrapositive

Assume $\neg Q$. Explain, explain, ... explain. Therefore $\neg P$

- Also used to prove universal implication: $\forall x\,(P(x) \to Q(x))$

$\uparrow$ x in some Domain

Structure:

Let x be $\begin{bmatrix} \text{any} \\ \text{an arbitrary} \end{bmatrix}$ element of the domain

We prove the contrapositive.

Assume $\neg Q(x)$

Explain, explain, explain.

Therefore $\neg P(x)$

S.KIMMEL

If a^2 is not divisible by 4, then a is odd.

- We prove the contrapositive. Let $a \in \mathbb{Z}$. Suppose a is even. Then there exists $k \in \mathbb{Z} : 2k = a$. This means $a^2 = 4k^2$. Since k is an integer, $4 | a^2$.

* There is an implied "for all" in the proof statement. (otherwise it is a predicate & we can't prove true or false). Therefore, we need "Let $a \in \mathbb{Z}$."