Math 2001. Lecture 14. Midterm 2. Friday, June 24. 06. 20. 2022.

Last time:

- Direct proofs of conditional statements (more exercises)
  (possibly with cases)
- Worksheets

Today:

- Proving a conditional statement by proving its contrapositive
- proofs by contradiction

1. Contrapositive proofs

Recall: · The contrapositive of a conditional statement

(1) "if P then Q"

is the statement

(2) "if not Q then not P" (P cannot happen without Q happening).

· The statements (1) and (2) are equivalent.

Thus, to prove $\underbrace{(P \Rightarrow Q)}_{(i)}$ it suffices to $\underbrace{\text{prove the contrapositive } (\sim Q \Rightarrow \sim P)}_{(ii)}$.

Why would (ii) be more convenient sometimes?

Because it might be more natural to pass information from the "Q-side" to the "P-side".

Examples:

1. Let $x \in \mathbb{Z}$. If $\underbrace{7x+9 \text{ is even}}_{P}$, $\underbrace{\text{then } x \text{ is odd}}_{Q}$.

Note: It's easier to deduce properties of $\underbrace{7x+9}_{P}$ from those of $\underbrace{x}_{Q}$.

than the other way around,

so it may be easier to prove the contrapositive.

Pf: We prove the contrapositive, i.e., that $\underbrace{7x+9 \text{ is not even}}_{\sim P}$ if $\underbrace{x \text{ is not odd}}_{\sim Q}$.

Thus, suppose x is not odd.

Then x is even, hence $7x$ is even, hence $7x+9$ is odd since 9 is odd.

So $7x+9$ is not even, and we are done. $\square$

A direct (but trickier) proof (of "$7x+9$ is even $\Rightarrow$ x is odd"):

Suppose $7x+9$ is even.

Note that $x = (7x+9) - 6x - 9$. (*)

Since 6 is even, $-6x$ is even.

Since $7x+9$ is even (by assumption), $-6x$ is even, and -9 is odd, it follows from (*) that x is odd. So we are done. $\square$

2. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. If $\underbrace{12a \not\equiv 12b \pmod{n}}_{P}$, then $\underbrace{n \nmid 12}_{Q}$.

"simpler"

Pf: We prove the contrapositive, i.e., that

if $n \mid 12$ then $12a \equiv 12b \pmod{n}$.

Suppose $n \mid 12$. Then $12 = kn$ for some $k \in \mathbb{Z}$.

$$12a - 12b = 12(a-b) = kn(a-b) = n \cdot \left((a-b)k \right)$$

It follows that $n \mid 12a - 12b$,

So $12a \equiv 12b \pmod{n}$, and we are done.

2. Proof by contradiction

To prove a statement (not necessarily a conditional statement), we may to prove that the negation of it / its conclusion would lead to a contradiction / absurdity / violation of its assumptions.

(That is, it suffices to assume the opposite and derive a contradiction).

Examples

1. (irrationality of $\sqrt{2}$). Prop: The real number $\sqrt{2}$ is not rational, i.e., we cannot write $\sqrt{2}=\frac{m}{n}$ for any integers m, n with $n \neq 0$.

Pf: We prove the claim by contradiction: suppose otherwise, i.e., suppose, for the sake of a contradiction, that $\sqrt{2}=\frac{m}{n}$ for some $m, n \in \mathbb{Z}$ w/ $n \neq 0$.

Then we may pick $m, n \in \mathbb{Z}$ s.t. $\sqrt{2} \overset{(*)}{=} \frac{m}{n}$ and $\gcd(m,n)=1$. (i.e. they are coprime)

Squaring both sides of $(*)$, we get $2=\frac{m^2}{n^2}$, so $m^2=2n^2$.

Thus, m^2 is even. It follows that m is even (otherwise m, hence m^2, would be odd).

We can now assume $m=2k$ for some $k \in \mathbb{Z}$, and we have $2n^2=m^2=(2k)^2=4k^2$.

It follows that $n^2=2k^2$.

It further follows that n^2 is even, and hence n is even.

But then since both m, n are even, $\gcd(m,n) \geq 2 > 1$,

Contradicting our assumption that $\gcd(m,n) = 1$.

It follows that $\sqrt{2}$ must be irrational. $\square$

Ex: Prove that $\sqrt{3}$ is irrational.

2. (infinitude of primes) Prop: There are infinitely many prime integers.

Pf: Suppose otherwise, i.e., Suppose that there are only finitely many primes. Then we can list them as $p_1, p_2, \cdots, p_k$ for some $k \in \mathbb{Z}_{>1}$ in increasing order (so $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \cdots$).

Consider the number $N := p_1 p_2 \cdots p_k + 1$. The number N must have a prime factor, which has to be p_i for some $1 \leq i \leq k$.

Thus, we have $N = cp_i$ for some $c \in \mathbb{Z}$.

We now have $p_1 p_2 \cdots p_k + 1 = cp_i$, so $1 = cp_i - p_1 p_2 \cdots p_k$

Since $p_i \mid cp_i$ and $p_i \mid p_1 p_2 \cdots p_k$, we have $p_i \mid 1$.

This is impossible, so there must be infinitely many primes. $\square$

Rmk: To prove a conditional statement $P \Rightarrow Q$ by its contrapositive is to assume $\sim Q$ (i.e., assume the opposite of the desired conclusion) and derive $\sim P$ (i.e., derive a contradiction to the assumption). So such a proof is a special case of proof by contradiction.

An (easy) example: Let $a \in \mathbb{Z}$. If $\underbrace{a^3 \text{ is even}}_{P}$, then $\underbrace{a \text{ is even}}_{Q}$.

Pf: Suppose otherwise, i.e., $\underbrace{a \text{ is not even}}_{\sim Q}$. Then a is odd,

so $a^3 = \underbrace{a \cdot a}_{\text{even}} \cdot a$ is odd, so $\underbrace{a^3 \text{ cannot be even}}_{\sim P}$.

It follows that if a^3 is even then a is even.

3. Proving equivalences

(a) "if and only if" statements ($P \Leftrightarrow Q$)

Typical pf strategy: prove $P \Rightarrow Q$ and $Q \Rightarrow P$ separately.

E.g. Let $x \in \mathbb{Z}$. Prove that $\underbrace{x \text{ is even}}_{P}$ iff $\underbrace{3x+5 \text{ is odd}}_{Q}$.

Pf: (1) The only if ($\Rightarrow$) direction:

Suppose x is even.

Then $3x$ is even, so $3x+5$ is odd since 5 is odd.

(2) The if ($\Leftarrow$) direction: We prove the contraposition of the if implication, i.e., we prove that if x is not even, then $3x+5$ is not odd.

Suppose x is not even. Then x is odd, so $3x$ is odd,

hence $3x+5$ is even and not odd.

By (1) and (2), we conclude that x is even iff $3x+5$ is odd. $\square$

(b) Equivalences of more than two statements / conditions.

("The following are equivalent ... / TFAE ...)

Note: If $P \Rightarrow Q$ and $Q \Rightarrow R$ then $P \Rightarrow R$.

Thus, to prove $(a) \Leftrightarrow (b) \Leftrightarrow (c)$ it suffices to prove that

$$\begin{tikzcd} (a) \arrow[rr, Rightarrow] & & (b) \arrow[dl, Rightarrow] \\ & (c) \arrow[ul, Rightarrow] & \end{tikzcd}$$

to prove (a), (b), (c), (d) are equivalent it suffices to show that

$$\begin{array}{ccc} (a) & \Rightarrow & (b) \\ \Uparrow & & \Downarrow \\ (d) & \Leftarrow & (c) \end{array}$$

E.g. Let $x \in \mathbb{Z}$. Prove that TFAE.

(a) x is odd.

(b) $3x$ is odd.

(c) $3x+5$ is even.

Pf (sketch) $(a) \Rightarrow (b)$: This follows since the product of two odd int. is always odd. $(b) \Rightarrow (c)$: "odd + odd = even"; $(c) \Rightarrow (a)$: we proved this in the previous problem. $\rightarrow$ It follows that (a), (b), (c) are pairwise equiv. $\square$

4. Writing advices from the textbook

1. Begin each sentence with a word, not a math symbol.

   "A is a subset of B." ✗

   "The set A is a subset of B." ✓

2. End each sentence with a period, even if the sentence ends with a symbol or expression.

   "The binomial thm states that $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$" ✗

   "– – – – – – – – – – – . . y^{n-k}." ✓

3. Separate math symbols/expressions with words.

"As $x^2-1=0$, $x=0$ or $x=-1$."

→ "As $x^2-1=0$, we have $x=0$ or $x=-1$." ✓

4. Avoid misuse of symbols.

e.g. $1 \in \mathbb{Z}$, ✓ "$1 \subseteq \mathbb{Z}$" ✗. $\{1\} \subseteq \mathbb{Z}$. ✓

5. Avoid unnecessary symbols.

No set ~~A~~ has negative cardinality.

6. Use the first person plural.

"We conclude / we will show", not "I".

7. Use the active voice.

8. Introduce / declare / describe / quantify new symbols.

"Since $a \mid b$, we have $a = bc$." ✗

"Since $a \mid b$, we have $a = bc$ for some $c \in \mathbb{Z}$." ✓

9. Avoid "it / this / there" when there might be ambiguity.

10/11. Use conjunctions in suitable places.

(since, because, hence, therefore, thus, ...)

12. Be clear / avoid ambiguities!