Math 2001. Lecture 18.

02. 28. 2022.

Last time: · finished Ch. 3. Midterm on Ch. 1-3.

Today: · Direct proofs of conditional statements (Ch. 4)

1. A typical template for proving if-then statements

Prop: If P, then Q. → Todo: Assume P and then prove Q.

Pf: Suppose P.

↓ unpack/rephrase P (often using definitions) and set up "workable" notation.

↓ work towards Q by suitable manipulations.

Therefore Q, so if P then Q. □

Examples:

- Prop 1: If x is an odd integer, then x^2 is also an odd integer.

Pf: Suppose x is an odd integer.

Unpacking: Then $x = 2k+1$ for some $k \in \mathbb{Z}$.

use k — useful auxiliary quantity.

Therefore $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

So $x^2 = 2N+1$ for an integer N, namely, for $N = 2k^2 + 2k$.

Therefore x^2 is an odd integer, so we are done.

Ex: - If x is an even int., then so is x^2.

- If $x \in \mathbb{Z}$ is even, then $x^2 - 6x + 5$ is odd.

- Prop 2: Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

"divides", i.e., $b = ak$ for some $k \in \mathbb{Z}$.

Pf: Suppose $a, b, c \in \mathbb{Z}$ satisfy $a|b$ and $b|c$.

Then $b = am$ and $c = bn$ for some $m, n \in \mathbb{Z}$,

$$\text{So } c = bn = (am)n = a(mn)$$

(Since $m, n \in \mathbb{Z}$, we have $mn \in \mathbb{Z}$.)

So $c = a \cdot N$ for some integer N, namely, for $N = mn$.

Therefore $a|c$, and we are done. $\square$

2. Using cases

Sometimes a proof requires a discussion of cases that need different techniques / ideas.

E.g. Prop: If $n \in \mathbb{Z}$, then $1 + (-1)^n (2n-1)$ is a (int.) multiple of 4.

Pf: Suppose $n \in \mathbb{Z}$. (or, "Let $n \in \mathbb{Z}$.") Let $x = 1 + (-1)^n (2n-1)$. We consider two cases:

(1) n is even. (so we should prove here "if n is even then x is a multiple of 4")

Then $n = 2k$ for some $k \in \mathbb{Z}$. so $x = 1 + 1 \cdot (2 \cdot 2k - 1) = 1 + 4k - 1 = 4k$, so x is a multiple of 4.

(2) n is odd.

Then $n = 2k+1$ for some $k \in \mathbb{Z}$, so $x = 1 - 1 \cdot (2(2k+1) - 1) = 1 - (4k + 2 - 1) = 1 - (4k+1) = 4(-k)$.

therefore x is a multiple of 4.

By (1) and (2), $1 + (-1)^n (2n-1)$ is a multiple of 4 whenever $n \in \mathbb{Z}$, as desired. $\square$

Sometimes different cases are really similar and don't require separate treatment (when phrased cleverly).

E.g. Prop: If $a, b \in \mathbb{Z}$ are integers with opposite parity, then $a+b$ is odd.

one even, one odd

Pf: Suppose $a, b \in \mathbb{Z}$ have diff. parity. We have two possible cases:

(1) a is even and b is odd. Then $a = 2k$ and $b = 2l+1$ for some $k, l \in \mathbb{Z}$.

Thus, $a+b = 2k + 2l + 1 = 2(k+l) + 1$, so $a+b$ is odd (since $k+l \in \mathbb{Z}$).

(2) a is odd and b is even. Then $b = 2k$ and $a = 2l+1$ for some $k, l \in \mathbb{Z}$.

alternative

Thus, $a+b = b+a = 2k + 2l+1 = 2(k+l)+1$, so $a+b$ is odd.

"(2). a is odd and b is even. Then similarly we have $a+b$ is odd."

It follows that $a+b$ is odd (in both cases), so we are done.

Yet another way to write this:

<u>Pf</u>: Without loss of generality we may assume a is even and b is odd.

(then repeat the argument in the previous "Case (1)".)

Next time:

(harder) practice proofs.