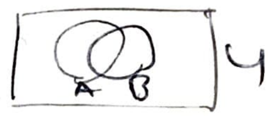
more precise to observe:
that statements "$x \in A \cap B$" etc.
"$x \in A \cup B$"

are <u>equivalent</u> to
"$(x \in A) \wedge (x \in B)$"
"$(x \in A) \vee (x \in B)$" etc.

↳ can use this observation to prove the equality of two sets in a new way, using $\Leftrightarrow$'s.

<u>Theorem</u> Suppose A, B are sets and U is a universal set with $A, B \subseteq U$.



Then we have:

① $\overline{\overline{A}} = A$

② $\overline{A \cap B} = \overline{A} \cup \overline{B}$

③ $\overline{A \cup B} = \overline{A} \cap \overline{B}$

looks like:
$\neg\neg P \Leftrightarrow P$
$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

<u>Pf</u>: ① Fix $x \in U$ ← not in A or $\overline{A}$!!!!

then $x \in \overline{\overline{A}} \Leftrightarrow x \notin \overline{A}$ (def'n of complement)
$\Leftrightarrow \neg(x \in \overline{A})$
$\Leftrightarrow \neg(\neg(x \in A))$ (def'n of comp. ")
$\Leftrightarrow x \in A$ $(\neg\neg P \Leftrightarrow P)$

This chain of equivalences shows:

$(x \in \bar{\bar{A}}) \Leftrightarrow (x \in A)$

i.e. $(x \in \bar{\bar{A}}) \Rightarrow (x \in A)$ ← this shows $\bar{\bar{A}} \subseteq A$

and $(x \in A) \Rightarrow (x \in \bar{\bar{A}})$ ← $A \subseteq \bar{\bar{A}}$

hence we've proved $\bar{\bar{A}} = A$.

② Fix $x \in U$

then $x \in \overline{A \cap B}$
$\Leftrightarrow \neg(x \in A \cap B)$ — def'n of comp.
$\Leftrightarrow \neg((x \in A) \wedge (x \in B))$ — def'n of $\cap$
$\Leftrightarrow \neg(x \in A) \vee \neg(x \in B)$ — De Morgan
$\Leftrightarrow (x \notin A) \vee (x \notin B)$
$\Leftrightarrow (x \in \bar{A}) \vee (x \in \bar{B})$ — def'n of comp.
$\Leftrightarrow x \in \bar{A} \cup \bar{B}$ — def'n of $\cup$.

this proves: $\overline{A \cap B} = \bar{A} \cup \bar{B}$

③ Similar: you try.

<u>Theorem</u>: For any sets A, B, C we have:

① $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
② $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Pf: you try (use the logical distributive laws)

Proof Writing:

Always two approaches: when trying to prove statement P, can either prove directly, or assume $\neg P$ and derive a contradiction.

More generally: can prove any statement logically equivalent to P, or disprove any statement logically equivalent to $\neg P$

Existence ~~Proofs~~ Claims

General form: $(\exists x \in S)\ P(x)$

Direct proof strategy: define a specific $y \in S$ and show $P(y)$ holds.

Ex ① Prop'n: There exists an even number $n \in \mathbb{N}$ that can be written as the sum of two primes in two distinct ways.

Pf: Consider $n = 10$. Then ~~n~~ n is even and we have: $10 = 5+5 = 7+3$ since 3, 5, 7 are prime ~~[illegible]~~ the claim is proved.

(Note: $24 = 19+5 = 17+7$ works too) (27)

Indirect Proof Strategy: Assume $\neg(\exists x \in S) P(x)$ (equiv: $(\forall x \in S) \neg P(x)$) and derive a contradiction

Ex: (2) Fix $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \mathbb{R}$. Then there is a $k \in \{1, 2, \ldots, n\}$ s.t. a_k is at least as large as the average (mean) of $a_1, \ldots, a_k$

Secretly a $\forall\exists$ claim, we focus on $\exists$ part.

That is:

$$(\exists k \in [n])\left(a_k \geq \frac{1}{n}\underbrace{(a_1 + a_2 + \cdots + a_n)}_{\frac{1}{n}\sum_1^n a_i}\right)$$

Pf: – Sps not, toward a contradiction

– that is, suppose

$$(\forall k \in [n])\left(a_k < \frac{1}{n}(a_1 + \cdots + a_n)\right)$$

– For simplicity, let $s = a_1 + a_2 + \cdots + a_n$

– So our assumption is: $(\forall k \in [n])\left(a_k < \frac{s}{n}\right)$

– But then:

$$s = a_1 + a_2 + \cdots + a_n \quad \text{(def'n of } s\text{)}$$

$$< \underbrace{\frac{s}{n} + \frac{s}{n} + \cdots + \frac{s}{n}}_{n \text{ times}} \quad \text{(by our assumption)}$$

$= n \cdot \frac{s}{n} = s$

This shows $s < s$, a contradiction.
Thus our assumption was false.
hence the prop'n is true.

Universal Claims

General Form: $(\forall x \in S)\, P(x)$

Direct Strategy: – Let $x \in S$ be arbitrary but fixed.
– Prove $P(x)$ holds

Ex ① Prop'n $(\forall x, y \in \mathbb{R}) \left(xy \leq \left(\frac{x+y}{2}\right)^2 \right)$

Pf: – Fix $x, y \in \mathbb{R}$.
– then: $(x-y)^2 \geq 0$ (squares always ≥ 0)
– hence $x^2 - 2xy + y^2 \geq 0$

$\Rightarrow x^2 + y^2 \geq 2xy$.

$\Rightarrow x^2 + 2xy + y^2 \geq 4xy$ (adding $2xy$ to both sides)

i.e. $(x+y)^2 \geq 4xy$

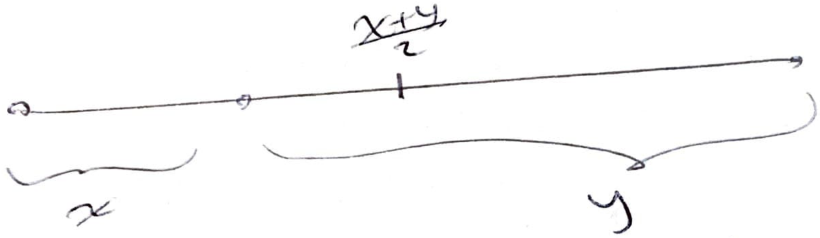
$\Rightarrow \frac{(x+y)^2}{4} \geq xy$

$\Rightarrow \left(\frac{x+y}{2}\right)^2 \geq xy$, as desired.

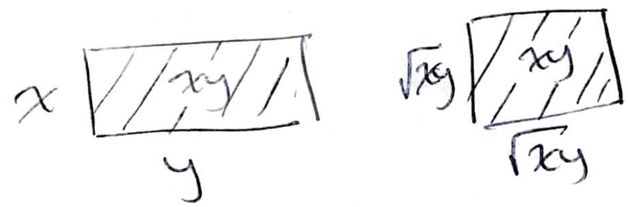
$\Rightarrow$ Since $x, y \in \mathbb{R}$ were arbitrary, the claim is proved.

<u>Aside</u>: prop'n is one version of the "AM–GM inequality"

- <u>arithmetic</u> <u>mean</u> (AM) of x, y is $\frac{x+y}{2}$



- <u>geometric</u> <u>mean</u> (GM) of x, y is $\sqrt{xy}$



$\Rightarrow$ prop'n proves (for $x, y \geq 0$) that

$$\sqrt{xy} \leq \frac{x+y}{2}$$

i.e. $\quad GM \leq AM.$

<u>Indirect</u> <u>Strategy</u>: Assume $\neg(\forall x \in S) P(x)$ (equiv: $(\exists x \in S) \neg P(x)$) and derive a contradiction)

Ex ② $\sqrt{2}$ is irrational, that is,

$(\forall a, b \in \mathbb{Z}) \left(\frac{a}{b} \neq \sqrt{2} \right)$

PF:- Sps not, that is, suppose $\exists a, b \in \mathbb{Z}$ s.t. $\frac{a}{b} = \sqrt{2}$

- We may assume $\frac{a}{b}$ is in reduced form, i.e. that a, b share no common factors; if they did, we could cancel these factors to get $a', b' \in \mathbb{Z}$ without common factors s.t. $\frac{a'}{b'} = \sqrt{2}$ and is reduced.

- Now: since $\frac{a}{b} = \sqrt{2}$

we have $a = \sqrt{2}\, b$

$\Rightarrow \quad a^2 = 2b^2$

- hence a^2 is even. It follows a itself is even (why?)
- hence $\exists k \in \mathbb{Z}$ s.t. $a = 2k$
- so then $a^2 = 4k^2$
- which gives $2b^2 = 4k^2$
-

which gives: $b^2 = 2k^2$

- reasoning as before we see that b^2, and hence b, is even.
- so both a, b are even: hence they share a factor of 2.
- a contradiction, as a, b share no common factors!
- the prop'n follows.

Conditional Claims

General Form: $P \Rightarrow Q$

Three Strategies: ① **Direct**: Assume P holds, prove Q.

② **Contrapositive**: Prove $\neg Q \Rightarrow \neg P$, i.e. assume $\neg Q$ and prove $\neg P$

③ **Indirect**: Assume $\neg(P \Rightarrow Q)$ (equiv: $P \wedge \neg Q$) and derive a contradiction

② and ③ often similar in practice

Ex ① (Direct). Let $O = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$ denote the set of all odd integers (negatives)

Prop'n $(\forall n \in \mathbb{Z})(n \in O \Rightarrow n^2-1$ is divisible by 4)

(or: even more symbolically

$(\forall n \in \mathbb{Z})(n \in O \Rightarrow (\exists k \in \mathbb{Z})(n^2-1 = 4k)))$

Pf: [[overall: this is a universal claim, so we begin as usual]]

- Fix $n \in \mathbb{Z}$

[[now we deal with the conditional]]

- Assume $n \in O$

[[we're allowed to do this, because if $n \notin O$, the conditional claim holds vacuously]]

- then $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$
- then $n^2 = (2k+1)^2 = 4k^2+4k+1$

$\Rightarrow n^2-1 = 4k^2+4k$

$\Rightarrow n^2-1 = 4(k^2+k) = 4M$ (where $M = k^2+k$)

- hence n^2-1 is divisible by 4
- since n was arbitrary, the claim is proved. ✓

② (contrapositive) Let $E = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$ be the set of all even integers. (33)

Prop'n: $(\forall m, n \in \mathbb{Z})\ (mn \in E \Rightarrow ((m \in E) \vee (n \in E)))$

Pf: - Fix $m, n \in \mathbb{Z}$. We argue the conditional by contrapositive.

- Assume $\neg(m \in E \vee n \in E)$

i.e. $m \notin E \wedge n \notin E$

- then m, n are both odd.

- hence $\exists k, l \in \mathbb{Z}$ s.t.

$m = 2k + 1$

$n = 2l + 1$

- then $mn = (2k+1)(2l+1)$

$= 4kl + 2k + 2l + 1$

$= 2(2kl + k + l) + 1$

$= 2M + 1$ (where $M = 2kl + k + l$)

- hence mn is odd, i.e. $mn \notin E$.

- we've proved

$(m \notin E \wedge n \notin E) \Rightarrow mn \notin E$

i.e. $\neg(m \in E \vee n \in E) \Rightarrow \neg(mn \in E)$

- by contrapositive, we've proved

$$mn \in E \Rightarrow m \in E \vee n \in E$$

- since $m, n \in \mathbb{Z}$ were arbitrary, the claim is proved. ✓

---

③ (Indirect) Prop'n: $(\forall x \in \mathbb{R})\ (x > 0 \Rightarrow x + \frac{1}{x} \geq 2)$

Pf: - fix $x \in \mathbb{R}$

- Sps $\overset{P}{x > 0}$ but $\overset{\neg Q}{x + \frac{1}{x} < 2}$

$\Rightarrow x^2 + 1 < 2x$ (inequality doesn't flip since $x > 0$)

$\Rightarrow x^2 - 2x + 1 < 0$

$\Rightarrow (x-1)^2 < 0$

a contradiction, as the quantity $(x-1)^2$ is ≥ 0.

- hence we must have

$$x > 0 \Rightarrow x + \frac{1}{x} \geq 2$$

- since x was arbitrary, the claim is proved.

Biconditional Claims

General Form: $P \Leftrightarrow Q$.

Strategy Prove $P \Rightarrow Q$ and $Q \Rightarrow P$.

Ex: **Prop'n** An integer is even if and only if its square is even.

i.e.

$$(\forall n \in \mathbb{Z})\ (n \in E \Leftrightarrow n^2 \in E)$$

Pf: - Fix $n \in \mathbb{Z}$

($\Rightarrow$) - Assume $n \in E$

- then $\exists k \in \mathbb{Z}$ s.t. $n = 2k$
- hence $n^2 = (2k)^2 = 4k^2$

$$= 2(2k^2)$$

$$= 2M \quad (\text{where } M = 2k^2)$$

- hence n^2 is even i.e. $n^2 \in E$. ✓

($\Leftarrow$) To prove $n^2 \in E \Rightarrow n \in E$ we show the contrapositive: $n \notin E \Rightarrow n^2 \notin E$

- So suppose $n \notin E$
- then n is odd, i.e. $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$
- hence $n^2 = (2k+1)^2$

$$= 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1$$

$$= 2M + 1 \qquad (M = 2k^2 + 2k)$$

hence n^2 is odd, i.e. $n^2 \notin E$.

- by contrapositive we've proved $n^2 \in E \Rightarrow n \in E$.
- hence $n \in E \Leftrightarrow n^2 \in E$
- since n was arbitrary, the prop'n is proved