(18)

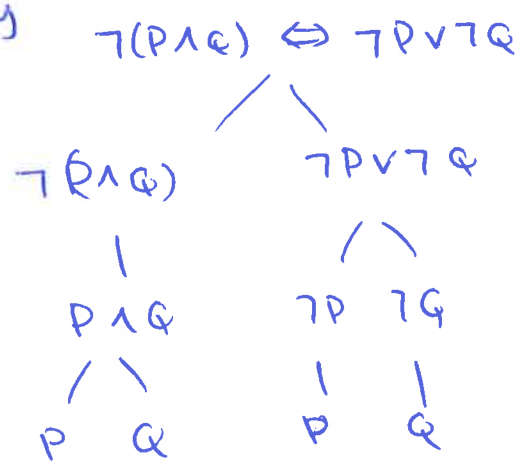
(2)

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$
T	T	F	F	T	F	F	T
T	F	F	T	F	T	T	T
F	T	T	F	F	T	T	T
F	F	T	T	F	T	T	T

always true

use this

to set up this



(3) Similar.

<u>Note:</u> (2) and (3) are called <u>De Morgan's</u> <u>Laws</u>.

Ex's: ① $\neg\neg(1+1=2)$

is equiv to: $1+1=2$ (both true)

② $\neg(1+1=2 \wedge 1+1=3)$

is equiv to: $(1+1\neq 2) \vee (1+1\neq 3)$ (both true)

③ $\neg(1+1=2 \vee 1+1=3)$

is equiv to: $(1+1\neq 2) \wedge (1+1\neq 3)$ (both false)

④ $(\forall x\in\mathbb{R})\, \neg(x<0 \wedge (\exists y\in\mathbb{R})(y^2=x))$

"is equiv to"

$\Leftrightarrow (\forall x\in\mathbb{R})\, [\neg(x<0) \vee \neg(\exists y\in\mathbb{R})(y^2=x)]$

$\Leftrightarrow (\forall x\in\mathbb{R})\, [x\geq 0 \vee (\forall y\in\mathbb{R})(y^2\neq x)]$

(all true)

Equivalences for $\Rightarrow$

Prop'n: For any P, Q the following equivalences hold:

① $(P\Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$

② $(P\Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

③ $(P\Leftrightarrow Q) \Leftrightarrow (P\Rightarrow Q \wedge Q\Rightarrow P)$

Pf of ① and ②:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg P \vee Q$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T	T
T	F	F	F	T	F	F
F	T	T	T	F	T	T
F	F	T	T	T	T	T

$(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$	$P \Rightarrow Q \Leftrightarrow \neg Q \Rightarrow \neg P$
T	T
T	T
T	T
T	T

③ You try.

Note: these three equivalences are very relevant for proving statements of the form $P \Rightarrow Q$ and $P \Leftrightarrow Q$.

Negating over $\Rightarrow$ and $\Leftrightarrow$

Prop'n: the following equivalences hold:

① $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$

② $\neg(P \Leftrightarrow Q) \Leftrightarrow [(P \wedge \neg Q) \vee (\neg P \wedge Q)]$

Pf: you try.

Note: with these and our previous equivalences, we can now put any negated statement in "positive form" (see below).

First: some ex's: Let E, O, P denote the sets of even, odd, and prime positive integers, respectively.

① ~~[illegible]~~ $5 \in O \Rightarrow 6 \in E$

is equiv. to:

$\neg(5 \in O) \vee (6 \in E)$

which we can write:

$(5 \notin O) \vee (6 \in E)$ (True)

② $(\forall x \in \mathbb{N})(x \in O \Rightarrow x+1 \in E)$

equiv to:

$(\forall x \in \mathbb{N})(x \notin O \vee x+1 \in E)$

also equiv to:

$(\forall x \in \mathbb{N})(x+1 \notin E \Rightarrow x \notin O)$ (True)

3 $(\forall x \in \mathbb{N})(x \in P \Leftrightarrow x \in O)$

is equiv. to:

$(\forall x \in \mathbb{N})\,((x \in P \Rightarrow x \in O) \wedge (x \in O \Rightarrow x \in P))$

(False)

4 Consider the following (true) statement.

$(\forall x \in \mathbb{R})\,[\,(x \geqslant 0) \Leftrightarrow (\exists y \in \mathbb{R})(y^2 = x)\,]$

Let's put its negation in "positive form":

$\neg(\forall x \in \mathbb{R})[(x \geqslant 0) \Leftrightarrow (\exists y \in \mathbb{R})(y^2 = x)]$

$\Leftrightarrow (\exists x \in \mathbb{R})\neg[(x \geqslant 0) \Leftrightarrow (\exists y \in \mathbb{R})(y^2 = x)]$

$\Leftrightarrow (\exists x \in \mathbb{R})\,[((x \geqslant 0) \wedge \neg(\exists y \in \mathbb{R})(y^2 = x)) \vee (\neg(x \geqslant 0) \wedge (\exists y \in \mathbb{R})(y^2 = x))]$

$\Leftrightarrow (\exists x \in \mathbb{R})[((x \geqslant 0) \wedge (\forall y \in \mathbb{R})(y^2 \neq x)) \vee ((x < 0) \wedge (\exists y \in \mathbb{R})(y^2 = x))]$

Defn: A statement P is in positive form if any negation symbols in P only occur next to substatements that contain no connectives or quantifiers.

↳ our rules above enable you to find, for any P, a logically equiv statement P' in positive form.

More useful equivalences:

Prop'n: The following equivalences hold:

① $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$
② $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$

Associative Laws.

③ $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
④ $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

Distributive Laws

Pf: Try the truth tables! (or: see sections 4.6.3 and 4.6.4 in the textbook).

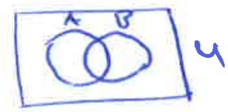
Proving equality of sets using $\Leftrightarrow$

There is a strong analogy between logical connectives and the set operations from ch. 3:

Connective	Operation
$P \wedge Q$	$A \cap B$
$P \vee Q$	$A \cup B$
$P \Rightarrow Q$	$A \subseteq B$
$P \Leftrightarrow Q$	$A = B$
$\neg P$	$\overline{A}$

- analogy gives us new way of proving the equality of two sets 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 $x \in U$ $\leftarrow$ not in A or $\overline{A}$!!!!!

<u>then</u>:
$$x \in \overline{\overline{A}} \Leftrightarrow x \notin \overline{A} \quad \text{def'n of complement}$$
$$\Leftrightarrow \neg(x \in \overline{A})$$
$$\Leftrightarrow \neg(\neg(x \in A)) \quad \text{def'n of compl. again}$$
$$\Leftrightarrow x \in A \quad \neg\neg P \Leftrightarrow P$$

This chain of equivalences shows:
$$x \in \overline{\overline{A}} \Leftrightarrow x \in A$$

i.e. $x \in \overline{\overline{A}} \Rightarrow x \in A$ (this shows $\overline{\overline{A}} \subseteq A$)
<u>and</u> $x \in A \Rightarrow x \in \overline{\overline{A}}$ (this shows $A \subseteq \overline{\overline{A}}$)

hence we've <u>proved</u> $\overline{\overline{A}} = A$.

2 Fix $x \in U$

<u>then</u>: $x \in \overline{A \cap B} \iff \neg(x \in A \cap B)$ def/n of comp.

$\iff \neg((x \in A) \wedge (x \in B))$ def/n of $\cap$

$\iff \neg(x \in A) \vee \neg(x \in B)$ De Morgan's Laws

$\iff x \in \bar{A} \vee x \in \bar{B}$ def/n of $\bar{A}, \bar{B}$

$\iff x \in \bar{A} \cup \bar{B}$

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

(Hint: use the logical distributive laws)

Proof writing

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

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

Existence Proofs

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

Direct proof strategy: define an element $y \in S$ and prove $P(y)$ holds.

Ex: ① Prop'n: There is an even number that can be written as the sum of two primes in two distinct ways.

Pf: consider $n = 10$
Then n is even and we have

$$10 = 5+5 = 7+3$$

since 3, 5, 7 are primes the prop'n is proved.

(Note: $24 = 19+5 = 17+7$ works too, etc...)

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

equivalently,

assume $(\forall x \in S) \neg P(x)$ and derive a contradiction

<u>Ex</u>: ② Fix $n \in \mathbb{N}$ and $a_1, \dots, a_n \in \mathbb{R}$. Then there is an index $k \in \{1, \dots, n\}$ s.t. a_k is at least as large as the average of $a_1, \dots, a_n$.

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

That is:

$$(\exists k \in [n]) \left(a_k \geq \tfrac{1}{n}(a_1 + a_2 + \dots + a_n)\right)$$

$$\tfrac{1}{n}\sum_1^n a_i$$

<u>Pf</u>: - Suppose not, toward a contradiction.

- that is, suppose

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

- for simplicity let $s = a_1 + \dots + a_n$
- then our assumption is, for every $k \in [n]$, we have $a_k < \frac{s}{n}$.

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.

Proving 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 $(x-y)^2 \geq 0$ (since squares always ≥ 0)

– hence $x^2 - 2xy + y^2 \geq 0$

– hence $x^2 + y^2 \geq 2xy$

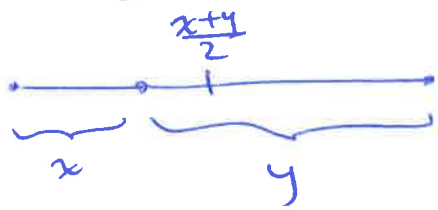
– hence $x^2 + 2xy + y^2 \geq 4xy$ (adding $2xy$ to both sides)

- i.e. $(x+y)^2 \geq 4xy$
- hence $\frac{(x+y)^2}{4} \geq xy$
- i.e. $\left(\frac{x+y}{2}\right)^2 \geq xy$

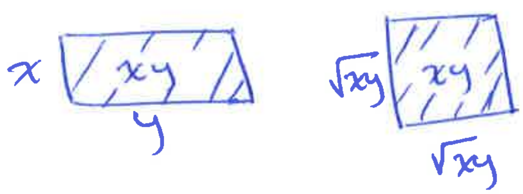
→ since $x, y \in \mathbb{R}$ were arbitrary, the prop'n is proved. ✓

<u>Note</u>: the prop'n is one version of the "AM-GM inequality".

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



- geometric <u>mean</u> (GM) of x, y (for $x, y \geq 0$) is $\sqrt{xy}$:



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

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

i.e. GM ≤ AM.

Indirect Strategy: Assume $\neg(\forall x\in S)P(x)$ (i.e. $(\exists x\in S)\neg P(x)$) and get a contradiction.

Ex: $\sqrt{2}$ 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 that $\frac{a}{b}$ is in reduced form, that is, that a and b have no common factors; if they did: we could cancel these factors to get integers a', b' s.t. $\frac{a'}{b'}=\sqrt{2}$ and is in reduced form.

- Now: since

$$\frac{a}{b}=\sqrt{2}$$

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

hence $a^2=2b^2$.

- Hence a^2 is even. It follows a is even too (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 b^2, and hence b, is even.
- So both a, b are even, hence share a factor of 2.
- A contradiction, as ~~assumed~~ 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: Show $\neg Q \Rightarrow \neg P$, i.e. assume $\neg Q$ and prove $\neg P$.

③ Indirect: Assume $\neg(P \Rightarrow Q)$, i.e. assume $\neg P \wedge Q$, and derive a contradiction

often similar in practice

Ex's: ① (direct strategy) For this ex, let $\mathbb{O} = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$ denote the set of all odd integers (including 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 $n \in \mathbb{Z}$ arbitrarily

(now we deal with the conditional)

- Assume $n \in O$.

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

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

$$= 4(k^2 + k)$$
$$= 4M \quad (\text{where } M = k^2 + k)$$

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

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

Prop'n $(\forall m, n \in \mathbb{Z})$ (if $m \cdot n$ is even, then either m or n is even)

Symbolically: $(\forall m, n \in \mathbb{Z})(mn \in E \Rightarrow [(m \in E) \vee (n \in E)])$

Pf: – Fix $m, n \in \mathbb{Z}$ arbitrary
(we'll argue 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.

$$m = 2k+1 \quad \text{and}$$
$$n = 2l+1$$

– but then
$$\begin{aligned} m \cdot n &= (2k+1)(2l+1) \\ &= 4kl + 2k + 2l + 1 \\ &= 2(2kl + k + l) + 1 \\ &= 2M + 1 \quad (\text{where } M = 2kl + k + l) \end{aligned}$$

– hence $m \cdot n$ 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 contraposition we have

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

- since m, n were arbitrary, prop'n is proved.

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

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

- Suppose $\overset{P}{x > 0}$ 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 always ≥ 0.

- Hence we must have

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

- Since x was arbitrary, prop'n 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 $n \in \mathbb{Z}$.

($\Rightarrow$) - Suppose $n \in E$.

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

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

$$= 2M \qquad M = 2k^2$$

- hence n^2 is even.

($\Leftarrow$) - To prove $n^2 \in E \Rightarrow n \in E$ we show the contrapositive, i.e. $n \notin E \Rightarrow n^2 \notin E$.

- So suppose $n \notin E$
- then n is odd, i.e. $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$
- hence $n^2 = 4k^2 + 4k + 1$

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

$$= 2M + 1 \quad (\text{where } M = 2k^2 + 2k)$$

- hence n^2 is odd, i.e. $n^2 \notin E$.
- by contrapositive we've shown $n^2 \in E \Rightarrow n \in E$.
- since n was arbitrary, prop'n is proved. ✓