MAT 108
Winter 2021
LEFT BOARD
Elem → Adv math.
Reading ad writing proofs.
Like essay structure ideas.
Eng is not precise enough.
So use predicate logic.
And some set theory.
Def: A proposition is a sentence which is true or false (T) (F) (or has a truth value).

Examples:

\[
1+1 = 3
\]

Prop \ Y it is F

This sentence is not a prop. \ Prop?

I am liar.

\[\neg \text{Prop} \]

N paradox
Lysol can kill viruses.

1. If $F$ then the sent is a prop.
   \[\text{If } T \text{ then } \text{not a prop}\]

2. Call the sentence $P$.
   
   If $P$ is True then $P$ is not a prop. Is so not True False.
   
   If $P$ is False then $P$ is a prop. Not so either True False.
Using steps from Thm 1.1.1:
~P ∧ Q
by (h) \[ \sim (A ∧ B) \text{ is eq. } \sim A ∨ \sim B \]
\[ \sim (\sim A) \text{ is eq. } A \]
\[ \sim P ∧ Q \text{ is eq. to } \sim \left[ (\sim P ∧ Q) \right] \]
which is eq to

\((b) \sim [\sim (\sim P) \lor \sim Q] \sim [P \lor \sim Q] \sim [P v \sim Q] \)
Building new props from old:

\[ \sim Q \quad (\sim Q) \quad \text{same} \]
\[ Q \land (p \lor R) \]

<table>
<thead>
<tr>
<th>Truth tables</th>
<th>( \sim P )</th>
<th>( p \land q )</th>
<th>( p \lor q )</th>
<th>( P \Rightarrow Q )</th>
<th>( Q \Rightarrow P )</th>
<th>( (\sim Q) \Rightarrow (\sim P) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P )</td>
<td>( Q )</td>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
</tbody>
</table>

\[ \text{equivalent} \]
Note: \( P \Rightarrow Q \) and \( (\neg Q) \Rightarrow (\neg P) \) are equivalent, as is the contrapositive, \( \neg P \lor Q \).

Eng

Ex:

\( P \): My dog is hungry.

\( Q \): My dog is inside.

\( P \Rightarrow Q \): If my dog is hungry then it is inside.

\( Q \Rightarrow P \): If my dog is inside then it is hungry.

\( \neg Q \Rightarrow \neg P \): If my dog is outside then it is full.

\( \neg P \lor Q \): Either my dog is full or it is inside.
1.3.4 have the same meaning.

2 is different.
Today quantifiers: Complete. First order logic notation.

Ex: Everyone I know likes chocolate or dislikes coffee.

Rewriting this in logic:

\( P(x) \) is \( x \) likes chocolate.
Q(x) is \( x \) likes coffee.

Notation: A sentence like \( P(x) \),

is an open sentence with variable \( x \).

The above becomes:

\[ \forall x \in \{ \text{people I know} \} \quad P(x) \lor \neg Q(x) \]

for all in the set of people I know.

or: In the universe (of discourse)
Everyone I know who likes chocolate also likes coffee.

\[ (\forall x) \, P(x) \lor \sim Q(x) \]

\[ \equiv \]

For everyone I know if they like chocolate then they also like coffee.

\[ (\forall x \in \{ \text{people I know} \}) \, P(x) \Rightarrow Q(x) \]
Compare \((\forall x \in \text{appl} \ I \text{know} \ with \ P(x) \ true)\)

(equivalent)

\((Q(x))\).

Thm 1.3.1: If \(P(x)\) is an open sentence then in any universe

① \(\sim (\forall x) P(x)\) is eq to \((\exists x) \sim P(x)\)

② \(\sim (\exists x) P(x)\) is eq to \((\forall x) \sim P(x)\)
Check example:
\[ \neg \left( \forall x \in \{ \text{ppl I know}\} \left( P(x) \lor \neg Q(x) \right) \right) \]
\[ \left( \exists x \in \{ \ldots \} \right) \neg \left( P(x) \lor \neg Q(x) \right) \]
\[ \left( \forall x \in \{ \ldots \} \right) \left( \neg P(x) \land Q(x) \right) \]

Def: The truth set in a universe \( U \) for an open sentence \( P(x) \), is all \( x \) in \( U \) for which \( P(x) \) is true.
Proofs:
see §1.7 pgs 64, 65, 66, 67

Examples:

Def: An integer $a \in \mathbb{Z}$ is even if there is an integer $n$ with $a = 2n$.

$$(\exists n \in \mathbb{Z}) (a = 2n)$$
An integer \( a \in \mathbb{Z} \) is odd if \((\exists n \in \mathbb{Z})(a = 2n+1)\)

**Thm:** If \( x \) is a real number with \( x^2 \leq 1 \) then \( x^2 - 7x > -10 \)

**Proof:** Assume \( x \) is a real number with \( x^2 \leq 1 \).

Hence \( x \leq |x| = \sqrt{x^2} \leq \sqrt{1} = 1 < 2 \).
Hence \( x < 5 \).

Hence \((x-2) < 0 \) and \((x-5) < 0 \).

Hence \((x-2)(x-5) \leq 0\).

Hence \( x^2 - 7x + 10 > 0 \).

Therefore \( x^2 - 7x > -10 \). \( \text{q.e.d.} \)
Approach:

\[(x-2)(x-3) = x^2 - 5x + 6 > 0\]

- \(x > 3\) (both positive)
- \(x < 2\) (both negative)

\(x < 1\)
Proofs to grade: (bad example)

Thm: If \( a \) is an odd integer then \( a^2+1 \) is an even integer.

"Proof": Let \( a \).

1. Then by squaring an odd we get an odd.
2. An odd plus an odd is even. So \( a^2+1 \) is even.
Problems: ① Why is this true? ② This is not a sentence. ③ It also not clear.
Recall: §1.7 64-67 should be reread.

From pg 67:
To start working out a proof consider:
Understand the statement
Logical form
Assumptions and Conclusion
Ideas
Step 3: Understand.

Try an example: eg $a=3$ and $b=6$ and $c=q$.

The claim is that $3$ divides $6q - 3$.

Logic: $P \land Q \Rightarrow R$

- $P$ is a divisor of $6$
- $Q$ is a divisor of $c$
- $R$ is a divisor of $6q - 3$

with quantifiers:

$(\forall a, b, c \in \mathbb{Z}) \left( (\forall c \in \mathbb{Z})(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(a, b, c \in \mathbb{Z}) \right)$
Ass & Concl:

Ass: P, Q

\[ a \text{ div } b \text{ or } (\exists n) \ n \cdot a = b \]
\[ a \text{ div } c \text{ or } (\exists m) \ m \cdot a = c \]

Concl: R

\[ a \text{ div } b - c \]

Ideas: With a, b, c as above have

\[ b - c = n \cdot a - m \cdot a = (n - m) \cdot a \]

thus is an integer.
Contra position proof:

Claim: If $m^2$ is an odd integer, then $m$ is an odd integer.

Proof: Assume $m$ is an integer.
   Assume $m$ is even.
   Hence $\exists t \in \mathbb{Z}$ with $2 \cdot t = m$.
   Hence $2t^2$ is also an integer.
   Hence $m^2 = (2t)^2 = 4t^2 = 2(2t^2)$.
   Hence $m^2$ is even.
Therefore if $m^2$ is odd then $m$ is odd. QED.

Example with cases and proof by contradiction:

Idea of proof by contradiction:
To prove $P$, assume $\neg P$ and show $Q$ and $\neg Q$. 
U: understand

eg \[a=1\] \[a^2-2=-1\] ✓
\[a=2\] \[a^2-2=2\] ✓
\[a=4\] \[a^2-2=14\] ✓

L: Logic!

Right now: \((\forall a) P\)

Plan: \((\forall a) \sim P \Rightarrow (Q \land \sim Q)\)

(to see these are equivalent:
\[P \lor (Q \land \sim Q) \lor P\]
\[ \sim (Q \land \sim Q) \Rightarrow P \]

eq. \[ \sim Q \lor Q \Rightarrow P \]

Ass: \( \sim P \)

Concl: \( Q \) and \( \sim Q \)

Ideas: \( \sim P \) is \((4 \text{ divides } a^2 - 2)\)

or \((\exists t)\) with \(4t = a^2 - 2\)

Cases: \( a \) is even
even: \( a = 2s \) so \( 4t = (2s)^2 - 2 = 4s^2 - 2 \) so \( 2t = 2s^2 - 1 \) or \( 1 = 2s^2 - 2t = 2(s^2 - t) \)

Q: \( l \) is even.

\( \neg Q \) is clearly true.

Need to show \( Q \)
210115 Mon. No Lect.
Hw due Wed.

Recall: Claim ①: If $a$ is an integer and $a^2$ is even then $a$ is even.

Proof: Earlier.

Claim ②: If $a$ is an integer then 4 does not divide $a^2 - 2$.

Proof: Note that 1 is not even.
Assume \( a \) is an integer and \( 4 \) divides \( a^2-2 \).

Hence there is an int \( t \) with \( 4t = a^2-2 \).

Hence \( a^2 = 2(2t-1) \)

so \( a^2 \) is even

and by claim 0 \( a \) is even.

Hence there is an integer \( s \) with \( a=2s \)

and \( s^2-t \) is an integer.

Hence \( 4t = (2s)^2-2 \) so \( 1 = 2(s^2-t) \) is even.

Therefore \( 1 \) is even and \( 1 \) is not even

which is a contradiction. \( \text{qed} \).


A: \( \neg Q \lor p \) is even so \( p = 2s \)

\[ \neg R \lor q \] is even so \( q = 2k \)

Concl.: \( \neg P \lor q \) is not the smallest possible denominator.

I: \( a = \frac{p}{q} = \frac{2s}{2k} = \frac{s}{k} \)

and \( k < q \) and hence a smaller denom. so \( \neg P \).
Proof: Assume $a = \frac{p}{q}$ with $p$ and $q$ both even integers.

Hence there are integers $s$ and $k$ with $p = 25$, $q = 2k$ so $a = \frac{p}{q} = \frac{25}{2k} = \frac{5}{k}$.

Therefore $q$ is not the smallest possible denominator.\[\text{ged}\]
\[ 1^2 + 15 = 16 \]
\[ 8 \cdot 1 = 8 \]
\[ 16 \neq 8 \quad \text{oops} \]

maybe noth else

\[ L: \left( \exists n \in \mathbb{Z} \right) \left( n^2 + 15 < 8n \right) \]

A: No ass. want

\[ \text{Concl.} \quad n^2 + 15 < 8n \]

I:

\[ n^2 + 15 - 8n < 0 \]

or \[ (n-5)(n-3) < 0 \]
need $n-5 \neq n-3$
to have different signs,
so take $n = 4$
Pythagorean's Thm

Thm: \( \sqrt{2} \) is irrational.

Plan Proof:

\[ U: \ \text{try} \ (\frac{7}{5})^2 = 1.96 \]
\[ (\frac{10}{7})^2 = 2.040816 \]

\[ L: \ \sim P \]

\( P \) is irrational or (contradiction approach)

\( P \Rightarrow (Q \land \sim Q) \)
Ass: \( \sqrt{2} = \frac{p}{q} \)

Concl: \( Q \) and \( \sim Q \).

Still have not had to choose \( Q \).

I: If \( \sqrt{2} = \frac{p}{q} \). \( \boxed{3} \)

Recall: If \( q \) is as small as possible \( \Rightarrow \) \( \sqrt{2} \) is even or \( q \) is odd.

\( p \) is odd or \( q \) is odd.

Compute \( 2 = \frac{p^2}{q^2} \) or \( 2q^2 = p^2 \). \( \boxed{4} \)

Tidy.

\( p^2 \) is even \( \Rightarrow \) \( p \) is even.

Also should have this means: \( p \) even. \( q \) is odd. \( \boxed{5} \)

Recall.
and $\textcolor{red}{\text{I}} p = 2k$ and $\textcolor{red}{\text{I}} q = 2M+1$ \hspace{1cm} \textcolor{red}{\text{I}}

**Proof:** Note that $b$ is not even.

Say that if $a$ is rational, $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $a = \frac{p}{q}$ and $q$ as small as possible.

Then $a = \frac{p}{q}$ is in **reduced form**.

Recall we proved last time that if $a = \frac{p}{q}$, is a rat. number in reduced form then $p$ or $q$ is odd.

Recall we proved before that if $n$ is an int. and $n^2$ is even then $n$ is even.

For contradiction assume $\sqrt{2}$ is rational
\[ \sqrt{2} = \frac{p}{q} \text{ is in reduced form.} \]

Hence \( 2 = \frac{p^2}{q^2} \) so \( 2q^2 = p^2 \) so \( p^2 \) is even so \( p \) is even so \( p = 2k \) for some int. \( k \).

Hence \( q \) must be odd so \( q = 2m + 1 \) for some int. \( m \).

Hence \( k^2 - 2m^2 - 2m \) is an integer and
\[
4k^2 = (2k)^2 = p^2 = 2q^2 = 2(2m + 1)^2 = 8m^2 + 8m + 2
\]

Hence \( 2[k^2 - 2m^2 - 2m] = 1 \) and \( l \) is even.

Therefore \( l \) is even and \( l \) is not even a contradiction so \( \sqrt{2} \) is irrational.
Recall \( \exists! x \) \( (P(x)) \)

is equivalent to:

\[
\exists x \, (P(x)) \land (\forall u, v)[(P(u) \land P(v)) \Rightarrow (u = v)]
\]

find an example.

Ans:

\( \circ \) \( \circ \) \( 3 \) has more than 1 \] false
4. \((x-2)^2 = 0\)

5. \(4 \pm \sqrt{-4} \neq \text{not in } \mathbb{R}\)
   \[\frac{4 \pm 2i}{2}\]
   no answers

6. True

7. False

3. Find a different example and done.

4. Example for \(\exists\) more work to do.
Claim: \( \exists \ x \in \mathbb{R} \) \( x^2 - 4x + 4 = 0 \).

Proof: First show \( \exists \ x \in \mathbb{R} \) \( x^2 - 4x + 4 = 0 \) by taking \( x = 2 \) so \( 2^2 - 4 \cdot 2 + 4 = 0 \). Check.

Uniqueness: Assume \( u^2 - 4u + 4 = 0 \) and \( v^2 - 4v + 4 = 0 \), hence \( (u-2)^2 = 0 \) and \( (v-2)^2 = 0 \).

So \( u - 2 = 0 \) and \( v - 2 = 0 \) so \( u = 2 \) and \( v = 2 \) so \( u = v \).
If \( P \) then \( Q \),

\[ P \Rightarrow Q \]

By cont. eq.

\[ \left[ \neg (P \Rightarrow Q) \right] \Rightarrow (R \land \neg R) \]

Possibly can choose \( R = \emptyset \)

eq. \[ \left[ \neg (\neg P \lor Q) \right] \Rightarrow (R \land \neg R) \]
\[ \varphi_1 : (P \land \neg Q) \Rightarrow (R \land \neg R) \]

\[ \varphi_2 : (P \land \neg Q) \Rightarrow (Q \land \neg Q) \]

\[ \varphi_3 : P \land \neg Q \Rightarrow Q \]

or maybe choose 
\[ R = P \]

\[ (P \land \neg Q) \Rightarrow (P \land \neg P) \]

or 
\[ P \land \neg Q \Rightarrow \neg P \]

enough to show 
\[ \neg Q \Rightarrow \neg P \]
210122 §1.8 Number Theory (for proofs).

Next week Set Theory (\( \ldots \)).

Recall: If \( a \) and \( b \) are integers then \( a \) divides \( b \) iff there is an integer \( c \) with \( a \cdot c = b \).

If \( p \) is an integer then \( p \) is prime iff the only positive integers dividing \( p \) are 1 and \( p \).
Def (pg 77): If \( a, b \) and \( d \) are integers nonzero then \( \gcd(a, b) = d \) if

1. \( d \) divides both \( a \) and \( b \) (say \( d \) is a common divisor of \( a \) and \( b \))
2. every common divisor of \( a \) and \( b \) is at most \( d \).

In first order logic:

\[(\forall a, b, d \in \mathbb{Z}_{>0}) [\gcd(a, b) = d] \iff \]
\[ \left( \exists s, t \in \mathbb{Z} \right) \left( d \cdot s = a \right) \wedge \left( d \cdot t = b \right) \]
\[ \wedge \left( \forall e \in \mathbb{Z} \right) \left[ \left( \exists u, v \in \mathbb{Z} \right) \left( e \cdot u = a \right) \wedge \left( e \cdot v = b \right) \right] \Rightarrow \left( e \leq d \right) \]

\text{Brk Rm: Translate lcm def. into logic.}
Claims: \{10, 11, 12\} \rightarrow 3

(∀a ∈ N_{≥ 10} ) (∃b ∈ N) (gcd(a, b) = 1) \land (a ≤ b)

(∃a ∈ N_{≥ 10} ) (∀b ∈ N) (gcd(a, b) = 1) \lor (a ≤ b)

Proof sketch for a:

Assume \( a \geq 10 \) is an integer.

Choose \( b = a + 1 \).

Note that 1 and \(-1\) are the only divisors of 1.

Assume that \( d \) is a common divisor of \( a \)
and \( b = a + 1 \).

Hence there are integers \( s \) and \( t \), with \( d \cdot t = a + 1 \) and \( d \cdot s = a \), so \( d \cdot (t-s) = a + 1 - a = 1 \) so \( d \) is 1 or -1.

Hence \((a, \phi) = 1\). \( \text{qed} \)
More number theory from §1.8. Division and Euclid's Alg.

Def: If $a, b, x, y, n$ are integers and $n = a \cdot x + b \cdot y$ then $n$ is a linear combination of $a$ and $b$.

Thm 1.8.1 (Prove later by induction) If $a$ and $b$ are nonzero integers, then $\gcd(a, b)$ is equal to the smallest
positive linear comb in. of a and b.

Thm 2.5.1 (Division Alg).
If a and b are nonzero integers, there is a unique pair of integers q and r with
\[ b = a \cdot q + r \]
and \( 0 \leq r < |a| \).
Notation for Euclid's Alg:

\[ b = a \cdot q_0 + r_1 \]
\[ a = r_1 \cdot q_2 + r_2 \]
\[ r_1 = r_2 \cdot q_3 + r_3 \]
\[ \vdots \]
\[ r_{k-2} = r_{k-1} \cdot q_k + r_k \]
\[ r_{k-1} = r_k \cdot q_{k+1} \]
Thm: 1.8.2: If $b > a > 0$ are integers then \( \gcd(a, b) = r_k \) from Euclid's algorithm.

Birk. Rm: Apply Euclid's Alg to

\[ b = 256 \geq a = 81 > 0 \]

Find \( r_k = 1 \) and \( k \), and the \( q_i \)’s.

\[ k = 3 \quad q_1 = 13 \quad q_2 = 3 \quad q_3 = 1 \]
Claim: (1.8.3):
If a, b and p are integers with p prime and p divides ab then p divides a or p divides b.

Proof: Assume a, b and p are integers with p prime, p dividing ab but not a.
Hence there only pos. divisors of p are 1 and p so gcd(p,a) = 1.
Hence by Thm 1.8.1 there are integers x and y with 1 = x·p + y·a.
Also there is an int. \( n \) with 
\[ ab = np \]
and 
\[ b = b \cdot x \cdot p + y \cdot a \cdot b \]
so 
\[ b = b \cdot x \cdot P + y \cdot n \cdot p \]
and 
\[ b \cdot x + y \cdot n \cdot p \]
\[ = [b \cdot x + y \cdot n] \cdot p \]
and 
\[ b \cdot x + y \cdot n \]
is an integer.

Therefore \( p \) divides \( b \).

\[ q.e.d. \]

Set Notation examples:

\[ \{3, 4, 5, 6\} = \{x \in \mathbb{Z} | x \geq 3, \; x \leq 6\} = \{\ldots : \} \]
Write $3 \in \{3,4,5,6\}$ is an element of.

$2 \notin \{3,4,5,6\}$ is not an element.

$\{3,4\} \subseteq \{3,4,5,6\}$ is a subset of.

$\{3\} \not\subseteq \{3,4,5,6\}$
\[ 3 \notin \{3, 4, 5, 6\} \]
\[ \{3\} \in \{\{3\}, \{1, 5, 6\}\} \text{ has 2 elts} \]

Power sets:
\[ P(\{2, 3\}) = \{\{\}, \{2\}, \{3\}, \{2, 3\}\} \]

The set of subsets. \[ \emptyset = \text{the empty set} \]

Which are true:
\[ \exists \ A, B, C \text{ sets with} \]
① True: \( A \leq B, \ B \neq C, \ A \leq C \)

② True: \( A \leq B, \ B \subseteq C, \ c \subseteq A \)

③ False: \( A \neq B, \ B \subseteq C, \ c \subseteq A \)

④ False
Set operations.
Related to operations on predicates.

Notation: If A and B are sets write:

1. $A \cup B = \{x \mid (x \in A) \lor (x \in B)\}$
2. $A \cap B = \{x \mid (x \in A) \land (x \in B)\}$
3. $A - B = \{x \mid (x \in A) \land (x \notin B)\}$

If $A$ is a subset of a universe $U$ write:

4. $A^c = U - A$
Example: \( A = [3, 8) \subseteq \mathbb{R} = \mathbb{U} \)
\( B = (6, 10] \subseteq \mathbb{R} \)

Find

1. \( A \cup B \)
2. \( A \cap B \)
3. \( A - B \)
4. \( A^c \)
5. \( A \cap B^c \)

**Ans:**

1. \([3, 10]\)
2. \((6, 8)\)
3. \([3, 6]\)
4. \((-\infty, 3) \cup [8, \infty)\)
5. this just \( A - B \) which is \([3, 6]\).
Dictionary: If $P(x)$ and $Q(x)$ are open propositions with variable $x$ in $U$, take

$$A = \text{Truth}(P) = \{ x \in U \mid P(x) \text{ is true} \}$$

$$B = \text{Truth}(Q) = \{ x \in U \mid Q(x) \text{ is true} \}$$

$$\text{Truth}(P \land Q) = A \cap B$$

$$\text{Truth}(P \lor Q) = A \cup B$$

$$\text{Truth}(\sim P) = A^c$$

$$\text{Truth}(P \land \sim Q) = A - B$$
Truth \( (P \implies Q) \) = \( A^c \cup B \)

Truth Table: similar to Venn Diagram

\( = (A - B)^c \)