Chapters

Chapter 1

Mathematical Statements and Propositions

The majority of this class will be dedicated to learning the language of mathematics.

A mathematical sentence is usually called a **statement**.

A **proposition** is a statement which is either true or false.

**Example**

1. \(1 + 1 = 2\)
2. \(11 = 3\)
3. Every even integer greater than 2 may be written as the sum of two prime numbers
4. \(12 - 11\)
5. \(a \cdot b = 0\)

1 is true, 2 is false, 3 is very hard (Goldbach ~conjecture~) but either true or false if we cannot prove true or false.

4 is not a proposition

5 is a proposition if we assign values to \(a\) and \(b\).
ex. 1: Are the following proportions?

- \( m^2 - 2m > 0 \) \( \Leftrightarrow \) \( m \neq 0 \) \( \text{but:} \), \( m = 3 \) \( \Rightarrow \) \( m^2 - 2m > 0 \)
- \( m^2 - 2m + 1 > 0 \) \( \Rightarrow \) \( \text{confusing, it is nice:} \), \( m^2 - 2m + 1 = (m - 1)^2 \)

For every value of \( m \).

**Notation:** We will denote proportions with capital letters \( \mathbb{R}^+ \)

\( P, Q, \ldots \) (example: \( 3 > 2 \) might be called \( P \))

- \( P(m, m), Q(x, y) \) proportions depending on \( m, m, x, y \),

\( \text{(example:} \ P(m, m) \Leftrightarrow m + m > 2 \) \)

\( m, m, x, y \) are sometimes called free-variables. \( P(m, m) \) becomes a proportion when \( m, m \) are specified.

**11** Connectives: \( \lor \), \( \land \), \( \neg \)

These are operations we can perform to combine simple proportion into complicated ones.

To decide whether the new complicated proportion is true, knowing if the simple ones are true or false, we use the \( \text{truth tables} \)
<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P \lor Q (sometimes denoted ( P \lor Q ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Example: \( P \approx 2 \leq 3 \)

\( Q \approx 2 = 3 \) then \( P \lor Q \approx 2 \leq 3 \)

Maybe it is better (and more useful) to think backward:

"\( 2 \leq 3 \) is the proportion \( 2 \leq 3 \) or \( 2 = 3 \)"

So \( 2 \leq 3 \) true? \( 2 \leq 3 \mid 2 = 3 \mid 2 \leq 3 \lor 2 = 3 \)

\( T \mid F \mid T \)

ex.2: \( a \cdot b = 0 \sim a = 0 \lor b = 0 \) \( \therefore \) Cn

ex.3: \( |a| = |b| \sim a = b \lor a = -b \) \( \therefore 1 \leq 1 = 1 \sim \) true?

\( \text{AND} \)

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P \land Q (obs denoted ( P \land Q ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
\[ \begin{array}{c|c|c|c|c} 
T & T & F & F \\
F & T & F & F \\
T & F & F & F \\
\end{array} \]

\[ (x \leq 4) \land (x > 4) \]

\[ \begin{array}{c|c|c|c|c} 
T & 3 \leq 1 & 1 \leq 4 & 3 \leq 4 & \text{F} \\
F & 3 \leq 1 & 1 \leq 4 & 3 \leq 4 & \text{F} \\
\end{array} \]

\[ \begin{array}{c|c|c|c|c} 
T & 3 \leq \frac{3}{2} & \frac{3}{2} \leq 4 & \frac{3}{2} \leq 4 & \text{T} \\
T & 3 \leq \frac{3}{2} & \frac{3}{2} \leq 4 & \frac{3}{2} \leq 4 & \text{T} \\
\end{array} \]

\[ \text{NOT} \]

\[ \begin{array}{c|c} 
T & \text{F} \\
F & \text{T} \\
\end{array} \]

\[ \begin{array}{c|c|c|c|c} 
T & \text{not } P & \text{(also denoted } \neg P \text{)} \\
F & \text{F} & \text{F} \\
\end{array} \]

\[ \begin{array}{c|c|c|c|c} 
P & \lnot P & \text{X} \geq 3 \text{ then } \lnot P & \text{X} \leq 3 \\
F & \text{F} & \text{F} & \text{F} \\
\end{array} \]

\[ \begin{array}{c|c|c|c|c} 
X & 2 > 3 & \text{F} & \text{F} & \text{F} \\
x = 2 & \text{F} & \text{F} & \text{F} \\
\end{array} \]

---

Given a proposition you should be able to: 

---
1. Reduce it to a combination of $\lor, \land, \neg$.
2. Decide if it's true or false using the truth table.

\[ P \land (Q \lor R) \sim \text{ the brackets tell you the order.} \]

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$R$</th>
<th>$Q \lor R$</th>
<th>$P \land (Q \lor R)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

\[ 3 \leq 4 \land (7 > 3 \lor 5 = 6) \text{ is } T. \]
Recap: Are \( \neg (P \lor Q) \) and \( \neg P \land \neg Q \) the same prop.?

\[\begin{array}{c|c|c|c|c|c}
P & Q & \neg P & \neg Q & P \lor Q & \neg (P \lor Q) \\
T & T & F & F & T & F \\
T & F & F & T & T & F \\
F & T & T & F & T & F \\
F & F & T & T & F & T \\
\end{array}\]

Some table of truth

\[\neg (2n \geq 3 \lor 5 \leq 6) \text{ same as } (2n > 3) \land (5 < 6)\]

Put a square box at the end of a proof!

Chapter 2: Implications

Suppose \( P(n): m \geq 3 \) and \( Q(n): n > 0 \)
Let's see if the notion makes sense with our experience by checking for every $n$:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$P(n)$</th>
<th>$Q(n)$</th>
<th>$P(n) \Rightarrow Q(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m \leq 0$</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>$0 &lt; m \leq 3$</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>$m &gt; 3$</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

In words: There is no value of $n$ for which $P(n)$ is true and $Q(n)$ is false.

Indeed: $P \Rightarrow Q$ comes as $\neg(P \land (\neg Q))$.
**Proof:**

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>( \neg Q )</th>
<th>( P \land (Q) )</th>
<th>( \neg (P \land (\neg Q)) )</th>
<th>( P \Rightarrow Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</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>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

**Notation**

\[ P \Rightarrow Q \quad : \quad \text{P implies Q, } \quad \text{if P then Q,} \]

\[ Q \text{ if P, } \quad P \text{ only if } Q, \]

\[ P \text{ is sufficient for Q, } \quad Q \text{ is necessary for P.} \]

**Equivalence**

\[ P \iff Q \iff P \Rightarrow Q \land Q \Rightarrow P \]

**Notation**

\[ P \iff Q \quad : \quad P \text{ if and only if } Q \]

\[ P \text{ is equivalent to Q,} \]

\[ P \text{ is necessary and sufficient for Q} \]
We want to study the main ways one can prove that \( P \Rightarrow Q \) is true.
**Direct proof:** We suppose that $P$ is true and we show that $Q$ is true.

\[
\begin{array}{c|c|c}
P & Q & P \implies Q \\
\hline
\top & \top & \top \\
\end{array}
\]

**Example:** 1. $0 = 1 \lor 0 = 2 \implies 0^2 - 30 + 2 = 0$

**Proof:** We are going to use $(P \lor Q \implies R) \iff (P \implies R) \lor (Q \implies R)$

- $a = 1 \implies 0^2 - 30 + 2 = 1 - 3 + 2 = 0$
- $a = 2 \implies 0^2 - 30 + 2 = 4 - 6 + 2 = 0$

2. For positive real numbers $a$ and $b$,

- $a < b \implies a^2 < b^2$

**Proof:** You have to do a bit of translating.

P: $a, b > 0$ real numbers

\[
\begin{array}{c}
\land \\
0 < b
\end{array}
\implies Q: a^2 < b^2\]
\[ p \Rightarrow a^2 < ab \land ab < b^2 \]

\[ R \Rightarrow a^2 < b^2 \]

(\text{In words: Assume } a, b > 0 \text{ real numbers and } a < b. Multiply } a < b \text{ by } a, b \text{ respectively and using } a, b > 0 \text{ we get } a^2 < ab \text{ and } ab < b^2. \text{ Chainning these two inequalities the conclusion follows.})

(There is yet another wording in the book)

\text{Proof: We used } \left[ (P \Rightarrow R) \land (R \Rightarrow Q) \right] \Rightarrow P \Rightarrow Q.

\text{Lecture 3: 10/02/2019}

\( \Box \) For nonnegative real numbers \( a, a^2 > 0. \)
\[
\text{proof: } \quad \text{a red number } \land a \neq 0 \quad \Rightarrow \quad a^2 > 0
\]

\[
a \neq 0 \quad \Rightarrow \quad a \geq 0 \lor a < 0. \quad \text{Mut}
\]

\[
a \text{ red number} \quad a > 0 \quad \Rightarrow \quad a^2 > 0
\]

\[
a < 0 \quad \Rightarrow \quad a^2 < 0 \quad (a \lor R) \Rightarrow S
\]

\[
\text{Here we used } \left\{ [P \Rightarrow (a \lor R)] \land \left[ (a \Rightarrow S) \land (R \Rightarrow S) \right] \right\}
\]

\[
\Leftrightarrow (P \Rightarrow S)
\]

\[
(\text{i}) \quad \text{For red numbers } a, b, \quad a < b \quad \Rightarrow \quad ab < (a + b)^2
\]

\[
(\text{ii}) \quad \text{Direct proof backward:}
\]

\[
a \cdot b < (a + b)^2 \quad \Rightarrow \quad a \cdot b < a^2 + 2ab + b^2
\]

\[
\Rightarrow \quad a^2 + b^2 - 2ab > 0
\]

\[
\Rightarrow \quad (a - b)^2 > 0
\]

\[
\Rightarrow \quad a \neq b
\]

\[
\Rightarrow \quad a < b
\]
Want to prove \( P \) is true
Assume \( \neg P \) and prove a false proposition \( Q \)

\[
\begin{array}{c|c|c|c}
\neg P & P & Q & \neg P \Rightarrow Q \\
\hline
T & F & T & T \\
T & F & F & T \\
F & T & T & T \\
F & T & F & F \\
\end{array}
\]

Therefore we are in row 2, that is \( P \) is true

Proposition: 101 is an odd integer

First some definitions:

\( \text{Def} \) Given two integers \( a, b \) we say that \( a \) divides \( b \)
or that \( b \) is a multiple of \( a \) if there is an integer \( q \) such that \( b = a \cdot q \). We write \( a \mid b \)

\[
\text{Ex. } 2 \mid 14 \text{ and } 7 \cdot 2 = 14
\]

1. Given an integer \( e \), we say that:
   - \( e \) is even if \( 2 \mid e \)
   - \( e \) is odd if it is not even

Proof that 101 is odd:

\[
P: 101 \text{ is odd}
\]

\[
\neg P: 101 \text{ is not odd} \iff 101 \text{ is even}
\]

Suppose by contradiction that 101 is even \((\neg P)\). Then by definition \( 2 \mid 101 \), that is there exists an integer \( q \) with
\[
101 = 2 \cdot q.
\]
Therefore \( q = \frac{101}{2} \) is an integer

\[
q \text{ is false}
\]

which is a contradiction \((\exists)\).
Proposition: There are no integers \( m \) and \( n \) such that

\[ 14 \, m + 20 \, n = 101 \]

proof: Suppose, for contradiction, that there are integers \( m, n \) such that \( 14 \, m + 20 \, n = 101 \) \( \text{ (} P \text{)} \).

Then we have

\[ 101 = 14 \, m + 20 \, n = 2 \, (7 \, m + 10 \, n) \]

which is \( 2/101 \). By definition, this implies that \( 101 \) is even.

This is the desired contradiction.  \( \square \)

Tip: Proofs by contradiction are usually useful to deal with negative statements, but not only.

Proposition: Prove that for any real numbers \( a, b \), \( a \neq 0 \),

\[ a^2 + b^2 \neq 1 + 2ab \]

proof: Suppose by contradiction there are real numbers
\[ a, b \text{ odd } \quad a^2 + b^2 = 1 + 2ab \]
\[ \iff \quad 2 + a^2 + b^2 - 1 - 2ab = 0 \]
\[ \iff \quad 1 + (a^2 + b^2 - 2ab) = 0 \]
\[ \iff \quad (a - b)^2 = 0 \]

However \( (a - b)^2 \geq 0 \implies 1 + (a - b)^2 \geq 1 \), which implies that \( 1 + (a - b)^2 = 0 \) is false, thus a contradiction.

**Proving implications by contradiction**

**Proposition** If \( a, b, c \) are integers with \( a > b \), then
\[ ac < bc \iff c \leq 0 \]

We want to prove \([P \implies Q]\) is true by contradiction.

- Assume \((P \implies Q)\) is false (that is, \(\neg(P \implies Q)\) is true)
Prove a false proposition $R$

That is $\neg (P \Rightarrow \neg A) \Rightarrow R, R$ false.

Show:

<table>
<thead>
<tr>
<th>$P \lor \neg A$</th>
<th>$\neg A$</th>
<th>$P$</th>
<th>$A$</th>
<th>$P \Rightarrow A$</th>
<th>$\neg (P \Rightarrow A)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Thus, $\neg (P \lor \neg A) \Rightarrow \neg (P \Rightarrow A)$

we need to prove

$P \lor (\neg A) \Rightarrow R, R$ false.

Proof of proposition: We assume

\[
\begin{cases}
\ a, b, c \text{ integers} \\
\ a > b \quad \text{and} \quad c > 0 \ (\neg A) \\
\ ac < bc
\end{cases}
\]

and by contradiction we want to prove a false
Statement \( R \).

\[ a > b \text{ and } c > 0 \Rightarrow ac > bc \]

\( R \) is a contradiction with \( ac < bc \).

Proving implication by contrapositive

Let's consider again the proposition:

Prop. If \( a, b, c \) are integers such that \( a > b \), then \( ac < bc \) if and only if \( c < 0 \).

There is another way to prove the proposition:

1. We want to prove \( (P \Rightarrow Q) \) is true.
2. We show that \( (P \Rightarrow Q) \) is equivalent to its contrapositive \( (\neg Q) \Rightarrow (\neg P) \), indeed

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( \neg P )</th>
<th>( \neg Q )</th>
<th>( P \Rightarrow Q )</th>
<th>( (\neg Q) \Rightarrow (\neg P) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td></td>
</tr>
</tbody>
</table>
So we prove that \((\neg Q) \Rightarrow \neg P\) is true by direct implication.

**Proof of Proposition:**

\[ P : \quad ac \leq bc \quad \neg P : \quad ac > bc \]

\[ Q : \quad c \leq 0 \quad \neg Q : \quad c > 0 \]

\((\neg Q \Rightarrow \neg P)\) is the statement \(c > 0 \Rightarrow ac > bc\)

Since \(a > b\), multiplying by \(c > 0\) on both sides by \(c\) we get \(ac > bc\) as desired.

---

**Proving \("\lor\"\) Statements**

**Proposition:** If \(a, b\) are real numbers, then

\[ ab = 0 \iff a = 0 \lor b = 0 \]

**Proof:** We need to prove both implications:

\[ ab = 0 \Rightarrow a = 0 \lor b = 0 \]

\[ ab = 0 \Leftarrow a = 0 \lor b = 0 \]

"\(\Leftarrow\)" Direct proof using \([ (P \lor Q) \Rightarrow R ] \iff [ (P \Rightarrow R) \land (Q \Rightarrow R) ]\)
If \( a = 0 \) then \( ab = 0 \).
If \( b = 0 \) then \( ab = 0 \).

\[ \Rightarrow \] Suppose \( ab = 0 \) and \( a \neq 0 \). Then dividing \( ab = 0 \) by \( a \neq 0 \) we get \( b = 0 \), that is the conclusion.

Here we used the fact that

\[ [P \Rightarrow (Q \lor R)] 
\Leftrightarrow [P \land (\neg Q) ] \Rightarrow R \]

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q \land R )</th>
<th>( Q \lor R )</th>
<th>( P \Rightarrow (Q \land R) )</th>
<th>( Q \land (\neg Q) )</th>
<th>( P \land (\neg Q) )</th>
<th>( [P \land (\neg Q)] \Rightarrow R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

are the same.

Lecture 5: 10/7/2019

Recap chapters 1-2-3-4.

Ex 1: Prove that \([P \Rightarrow (Q \lor R)] \Leftrightarrow [P \land (\neg Q)] \Rightarrow R\)
Ex 2: So the universal statement
\[ \left( \frac{m^2 - m - 2 = 0}{\phi 1} \right) \land \left( \frac{m^2 - m - 2 = 0}{\phi 2} \right) \] is true or false?

Proof:

<table>
<thead>
<tr>
<th>( m )</th>
<th>( \phi 1 )</th>
<th>( \phi 2 )</th>
<th>( \phi 1 \rightarrow \phi 2 )</th>
<th>( \phi 2 \rightarrow \phi 1 )</th>
<th>( \phi 2 \rightarrow \phi 1 )</th>
<th>( \phi 1 \rightarrow \phi 2 )</th>
<th>( \phi 1 \rightarrow \phi 2 \rightarrow \phi 1 \land \phi 2 \rightarrow \phi 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m = 2 )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( m = -1 )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( m \neq 2, -1 )</td>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
</tbody>
</table>

Alternative proof: Notice that \( \phi 1 \rightarrow \phi 2 \), then recall

\[ \left( \left( \phi 1 \rightarrow \phi 2 \right) \land \left( \phi 2 \rightarrow \phi 1 \right) \right) \Rightarrow \left( \phi 1 \lor \phi 2 \right) \Rightarrow \phi 1 \]

<table>
<thead>
<tr>
<th>( m )</th>
<th>( \phi 1 \lor \phi 2 )</th>
<th>( \phi 2 \rightarrow \phi 1 )</th>
<th>( \left( \phi 1 \lor \phi 2 \right) \rightarrow \phi 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m = -1 )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
</tbody>
</table>
| \( m 
eq 1 \) | \( F \) | \( F \) | \( T \) |

Proposition: If the integer \( m \) is even, then \( m^2 \) is even.

Proof: Direct proof: Suppose that \( m \) is even, then \( m = 2k \) for some integer \( k \). Then \( m^2 = (2k)^2 = 4k^2 = 2(2k^2) \), which is even.
definition \( n = 2k \), for some integer \( k \). Then
\[ n^2 = (2k)^2 = 4k^2 = 2(2k^2), \quad \text{let} \, \text{be} \, 2 \mid n^2. \]

Therefore \( n^2 \) is even.

**Proposition**

If the integer \( n^2 \) is even, then \( n \) is even.

**Proof:** By contraposition. Suppose \( n \) is odd. We want to show that \( n^2 \) is odd. Since \( n \) is odd, there is an integer \( k \) such that \( n = 2k + 1 \). Thus \( n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k + 1) + 1 \), which is odd.

Proposition: \( \sqrt{2} \) is not a rational number.
**Proof:** By contradiction. Recall that a number $x$ is rational if there exist integers $a, b$ such $x = \frac{a}{b}$. Moreover we say that $\frac{a}{b}$ is in lowest terms if $a$ and $b$ has no common factors other than one. (e.g., $\frac{14}{15}$ is in lowest term, let $\frac{14}{15}$ is not and $\frac{7}{8}$ is the corresponding lowest term).

Now suppose by contradiction that $\frac{12}{12}$ is not rational. Then there exist $a, b$ s.t. $12 = \frac{a}{b}$ and $a, b$ are in lowest term. Then $12 = \frac{a^2}{b^2}$, let $a = \sqrt{12}$, and $a^2 = 12$. This implies that $a$ is even (see previous proposition). Then $a = 2k$ for some integer $k$. But follows that

$$2b^2 = a^2 = (2k)^2 = 4k^2,$$

let $b^2 = 2k^2$ as $b^2$ is even and $a = b$ is even.
Therefore \(2 \mid b\) and \(2 \mid a\), i.e. \(a, b\) are not in distinct terms. 

**Proposition**

For every real number \(x \in \left[\frac{1}{2}, 2\right]\), we have

\[m x + c x \geq 1\]

**Proof:** Suppose by contradiction that this is not true. Then there is \(x \in \left[\frac{1}{2}, 2\right]\) with \(m x + c x < 1\).

Since \(m x, c x \geq 0\) for \(x \in \left[\frac{1}{2}, 2\right]\), we get

\[0 \leq (m x + c x)^2 < 1 \Rightarrow 0 \leq m^2 x + 2 m x c x + c^2 x^2 < 1\]

\[\Rightarrow 0 \leq 1 + 2 m x c x < 1 \Rightarrow 2 m x c x < 1\]

Since \(m x, c x \geq 0\) for \(x \in \left[\frac{1}{2}, 2\right]\).
Proposition: Every nonzero rational number can be expressed as a product of two irrational numbers.

Proof: Suppose \( r \) is a nonzero rational number, then

\[ r = \frac{r}{\sqrt{2}} \cdot \frac{r}{\sqrt{2}}, \]

and we know that \( \frac{r}{\sqrt{2}} \) is not rational.

We only need to show that \( \frac{r}{\sqrt{2}} \) is irrational.

Suppose by contradiction \( \frac{r}{\sqrt{2}} \) is rational, then there are integers \( a, b \) such that

\[ \frac{r}{\sqrt{2}} = \frac{a}{b} \]

where \( c, d, e \) are integers,

\[ \Rightarrow \frac{r}{\sqrt{2}} \text{ is rational} \]
Goal: Prove that a proposition $P(n)$ is true for every positive integer $n \geq 1$.

(for example $P(n): m \leq 2^n$)

Proof by Induction:

1. $P(1)$ is true
2. $P(k) \Rightarrow P(k+1)$ for all positive integers $k \geq 1$

Solve: verify $P(1)$ is true, then by (ii) we have

\[ P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow P(5) \Rightarrow \ldots \]
and we can reach every possible \( n \in \mathbb{N} \).

**Example:**  
**Proposition:** \( 2^m \geq m \) for every \( m \geq 1 \)  
**Proof:** We prove the statement by induction, with  
\[ P(m) : 2^m \geq m \]

**Base case:** \( P(1) : 2^1 \geq 1 \) is true.

**Inductive step:** We have to prove the implication for \( k \geq 1 \)
\[
1 \leq 2^k \quad \Rightarrow \quad k+1 \leq 2^{k+1}
\]

2 ways:
1. \( k+1 \leq 2^{k+1} \leq 2^k + k \leq 2^k + 2^k \leq 2^{k+1} \)

2. (backward proof) \( 2^{k+1} = 2 \cdot 2^k \geq 2k = k + k \geq k+1 \)

**Proposition** For all positive integers \( n \), the number \( n^2 + n \) is even.  
**Proof:** We use induction on \( n \). (Recall we need to show)

\[ 2 \mid m^2 + n \]
Box of induction: \( m=1 \Rightarrow 1+1=2 \mid 2 \).

Inductive step: \( 2 \mid n^2 + m \Rightarrow 2 \mid (n+1)^2 + m+1 \)

We proceed by direct proof: \( 2 \mid n^2 + m \Rightarrow \exists p \text{ integer } \Rightarrow m^2 + m = 2p \).

Then \( (n+1)^2 + m+1 = m^2 + 2m+1 + m+1 = m^2 + m + 2m + 2 = 2p + 2m + 2 = 2(p+m+1) \).

Since \( p+m+1 \) is an integer, we conclude \( 2 \mid (n+1)^2 + m+1 \).

\[ \text{(Proposition)} \] Prove that \( 2^m \geq m^2 \) for any \( m \geq 1 \) integer.

Proof: Box of induction: \( 2 \geq 1 \)

Inductive step: \( n^2 \leq 2^{k} \Rightarrow (k+1)^2 \leq 2^{k+1} \)

We know \( (k+1)^2 = n^2 + 2 + 1 \leq 2^k + 2 \text{ for } k \geq 1 \).

\( \Rightarrow 2k+1 \leq 2^k \text{ Whence: } k=2 \Rightarrow 4 + 1 \leq 2^2 \Rightarrow 1 \leq 4 \)!!!
Maybe this is not true: \( n=2 \Rightarrow 4 \geq 4 \) or
\( n=3 \Rightarrow 8 \geq 9 \) !!

Ok! Proposition is false! Maybe there is a value of
\( n_0 \) for which \( P(n_0) \) is true for every \( n \geq n_0 \), that is

**Proposition**

\[ 2^n \geq n^2 \quad \text{for every } n \geq n_0 \]

**Proof by induction with different base step**

1. \( P(n_0) \) is true
2. \( P(n) \Rightarrow P(n+1) \) for every integer \( n \geq n_0 \)

Proof of prop. with \( a_0 = 4 \): Want to prove \( 2^n \geq n^2 \) for any \( n \geq 4 \)

**Base step**: \( P(4) \): \( 2^4 = 16 \geq 4^2 \) ✓

**Inductive step**: \( 2^{n+1} = 2 \cdot 2^n \geq 2 \cdot n^2 \)
We show not $2n^2 > (n+1)^2$ if $n \geq 4$. Indeed

$$2n^2 > (n+1)^2 \Leftrightarrow \quad 2n^2 > n^2 + 2n + 1 \Leftrightarrow \quad n^2 > 2n + 1.$$ 

Since $n \geq 4$, we have $n^2 > 4n = 2n + 2n = 2n + 2 > 2n + 1$.

**Example:** Assume to have an infinite supply of 4 and 5 dollar coins. Then you can pay any bill larger than or equal to 12 dollars.

**Proof:** $P(m) \iff m = k \cdot 4 + l \cdot 5$ for some integers $k, l$ and for $m \geq 12 = m_0$.

**Base case:** $12 = 3 \cdot 4$

**Inductive step:** $m+1 = k \cdot 4 + l \cdot 5 + 1$. Now we have 2 possibilities:

1) $k \geq 1$, then $m+1 = (k-1) \cdot 4 + l \cdot 5 + (l+1) = (k-1) \cdot 4 + (l+1) \cdot 5 \geq 20$.
\[ b) \quad \text{if } n = 1 \text{, then } m+1 = 2 - 5 + 1, \text{ but since } n > 12, \text{ we have } \]
\[ 2 - 5 = m > 12 \implies m > 3, \text{ therefore } \]
\[ m+1 = 2 - 5 + 1 = (2-3)\cdot 5 + (5+1) = (2-3)\cdot 5 + 4 \cdot 4 \quad \vline \]

Lecture 7: 10/11/2019

\textbf{Proposition} \quad \text{Everybody in the class has the same name}

(Also called \textit{base - paradigm}).

\textit{Proof:} \quad \text{Plan: a student always have the same name}

\underline{Base step:} \quad n = 1 \implies \text{Trivially true.}

\underline{Inductive step:} \quad \text{Now consider a group of } (m+1) \text{ students.}

\text{Suppose one of them is called \textit{Felicity}. Then the group } (m+1) \text{ - \textit{Felicity} has } m \text{ students, so they all have the same name. Since Felicity is in the group they...}
are all called Pelaty.

However (not), Pelaty also is an m-group and contains Earl, as they all have the same name, so Earl's name is actually Pelaty!!!

Ok, we know this can't be true, so what did I do wrong?

Base step: ok!

Inductive step: P(1) -> P(2), so if I have only Earl and Pelaty, the inductive step fails as there is no overlap of the m groups: Be Careful!!!
Examples: (i) For every non-negative integer \( n \), the factorial of \( n \) is
\[ m! \text{ def by: } (1) \; 0! = 1 \]
\[ (2) \; (k+1)! = (k+1) \cdot k! \quad k \geq 0. \]

(ii) For any real number \( x \), the power \( x^n \) is def
\[ x^0 = 1 \]
\[ x^{k+1} = x \cdot x^k \quad k \geq 0 \]

We can also use recursion to define sequences, for instance

\[ a_0 = 0 \]
\[ a_{n+1} = a_n + (n+1) \quad n \geq 0 \]

The seq. \( c_m = \text{sum of the first } m \text{ integers} \) is often defined by
\[ \sum_{i=0}^{m} i = c_m. \]

More generally, given a seq. of numbers \( a_0, a_1, a_2, a_3, \cdots \)
we can define for every \( n \geq 0 \),
\[ \sum_{i=0}^{n} a_i = a_0 \quad \text{and} \quad \sum_{i=0}^{m} a_i = \sum_{i=0}^{n} a_i + a_{n+1}. \]

**Type:** Whenever you have to prove something about objects defined recursively, induction is a good method.

**Proposition:** \( \sum_{i=1}^{m} i = \frac{m(m+1)}{2} \)

**Proof:** We use induction on \( m \).

**Base case:** \( \sum_{i=1}^{1} i = 1 \) and \( \frac{1(1+1)}{2} = 1 \) \( \checkmark \)

**Inductive step:** \( \sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) \) (by definition)

\[ = \frac{1}{2} k (k+1) + (k+1) \] (by inductive assumption)

\[ = \frac{1}{2} (k^2 + k + 2k + 2) = \frac{1}{2} (k^2 + 3k + 2) \]

\[ = \frac{1}{2} (k+2)(k+1) \]

\( \square \).
**Definition (Fibonacci sequence)** For each positive integer \( n \), define the number \( u_n \) inductively as follows:

\[
\begin{align*}
    u_1 &= 1 \\
    u_2 &= 1 \\
    u_{n+1} &= u_{n-1} + u_n \quad \text{for } n \geq 2
\end{align*}
\]

**Proposition (Binet formula)** The Fibonacci numbers \( u_n \) are given by the following formula:

\[
    u_n = \frac{L^n - \beta^n}{\sqrt{5}}
\]

where \( L = \frac{1 + \sqrt{5}}{2} \) and \( \beta = \frac{1 - \sqrt{5}}{2} \).

We would like to use proof by induction, as the sequence is defined inductively, but

\[
    u_{n+1} = u_n + u_{n-1}
\]

goes back 2 indices!?!?

So we introduce the following form of induction:
Strong induction principle

\( \Phi(n) \) is true for every positive integer \( n \geq 1 \)

(i) \( \Phi(1) \) is true

(ii) [ \( \Phi(n) \) holds for every \( n \leq K \) \( \Rightarrow \) \( \Phi(K+1) \). for every \( K \geq 1 \)

Here it goes: \( \Phi(1) \) is true, then \( \Phi(1) \Rightarrow \Phi(2) \)

then \( (\Phi(1) \land \Phi(2)) \Rightarrow \Phi(3) \), \( (\Phi(1) \land \Phi(2) \land \Phi(3)) \Rightarrow \Phi(4) \).

Proof of proposition: We use strong induction.

Base step: \( m = 1 \)

\[ \frac{\lambda - \beta}{\sqrt{3}} = \frac{1 + \sqrt{3} - (1 - \sqrt{3})}{2} = \frac{1}{\sqrt{3}} \]  \( \Rightarrow \) \( 1 = \nu_1 \)

Inductive step: Suppose the formula is true for every \( m \leq k \), then

\[ \nu_{k+1} = \nu_k + \nu_{k-1} \]  \( \text{Ch. 61 of the text.} \)
Recall on induction

**Definition:** An integer $p \geq 2$ is called a prime number if the only positive integers that divide $p$ are 1 and $p$.

**Fact:** If an integer $c \geq 2$ is not prime, then there are integers $a, b$ with $2 \leq a, b < c$ such that $c = a \cdot b$.

**Proposition:** Every integer greater than 1 can be written as the product of prime numbers.
By strong induction, we prove P(n): \( n \) is a product of prime numbers.

Base step: \( n = 2 \) \( \mathbb{V} \)

Inductive step: Suppose \( 2 \leq k \leq n \) \( k \) is a product of primes. Then we have two cases:

1. \( m+1 \) is a prime number, then we are done.
2. \( m+1 \) is not a prime number, then \( m+1 = a \cdot b \), \( 1 \leq a, b \leq m \).

Then by strong inductive assumption, \( a \) and \( b \) are product of primes and therefore \( m+1 \) is \( m+1 \).

---

Prove: Let \( a_m \) be the sequence defined by \( a_1 = 1 \), \( a_2 = 2 \), \( a_n = a_{n-1} + 2a_{n-2} \) for \( n \geq 3 \). Prove that \( a_n = 3 \cdot 2^{m-1} + 2(-1)^m \).

**Proof:** By strong induction:

Base step: \( a_1 = 1 \), \( 3 \cdot 2^0 + 2(-1) = 3 - 2 = 1 \) \( \mathbb{V} \)
\[ a_2 = 8 \quad 3 \cdot 2 + 2 \ (-1)^2 = 6 + 2 = 8 \quad V \]

\underline{Inductive step:} Let \( k \geq 2 \) be given and suppose that
\[ a_m = 3 \cdot 2^{a_{m-1}} + 2 (-1)^{m-1} \quad 1 \leq m \leq k. \]

\[ a_{k+1} = a_k + a_{k-1} = 3 \cdot 2^{k-1} + 2 (-1)^k + 2 \left( 3 \cdot 2^{k-2} + 2 (-1)^{k-2} \right) \]
\[ = 3 \left( 2^{k-1} + 2^{k-2} \right) + 2 \left( (-1)^k + 2 (-1)^{k-2} \right) \]
\[ = 3 \cdot 2^k + 2 (-1)^{k-1} (-1 + 2) = 3 \cdot 2^k + 2 (-1)^k \]

\[ = 3 \cdot 2^k + 2 (-1)^{k+1} \quad \Box \]

\[ \text{Prove that } \quad \prod_{i=1}^{m} \frac{1}{i (i+1)} = \frac{m}{m+1} \]

\[ \underline{Proof:} \text{ By induction.} \]

\[ \text{Base step} \quad \prod_{i=1}^{1} \frac{1}{i (i+1)} = \frac{1}{2} \quad \frac{m}{m+1} = \frac{1}{2} (m+1) \quad V \]
Inductive step:

\[
\sum_{i=1}^{n+1} \frac{1}{i(i+1)} = \frac{n+1}{n} + \sum_{i=1}^{n} \frac{1}{i(i+1)} + \frac{1}{(n+1)(n+2)}
\]

\[
\frac{1}{2} \frac{m}{m+1} + \frac{1}{m+1} = \frac{m^2 + 2m + 1}{(m+1)(m+2)} = \frac{(m+1)^2}{(m+1)(m+2)}
\]

\[
\frac{1}{2} \frac{m+1}{m+2}
\]

Proposition

Let \(a_1 = 1\) and \(a_{n+1} = \frac{3a_{n+1}}{2a_{n+1}}, \quad n \geq 1.\) Prove it.

(a) \(a_m < a_{m+1}\), \(m \geq 1\)

(b) \(a_m < \frac{1 + \sqrt{3}}{2}\), \(m \geq 1\)

Proof:

Base step: \(a_2 = \frac{3 \cdot 1}{2 + 1} = \frac{3}{2} > 1 = a_1\)

Inductive step: \(a_{m+1} - a_m = \frac{3a_{m+1}}{2a_{m+1}} - \frac{3a_m}{2a_m} = \)

\[
= \frac{3a_m(2a_{m+1} - 3a_m)}{(2a_{m+1})(2a_{m+1} - 2a_m)}
\]

\[
= \frac{3a_m(2a_{m+1} + 3a_m)}{(2a_{m+1})(2a_{m+1} - 2a_m)}
\]
\[
\frac{6a_n a_{n-1} + 3a_n - 6 a_{n-2} a_n - 3 a_{n-1} + 2a_{n-2} - 2a_n}{(2a_{n+1})(a_{n-1})} = \frac{a_n - a_{n-1}}{(2a_{n+1})(2a_{n-1})} > 0 \quad \text{by inductive assumption} \quad (a_n > a_{n-1})
\]

0) Base step: \[\frac{1 + \sqrt{3}}{2} > \frac{1 + 1}{2} = 1 = a_1 \quad \checkmark\]

Inductive step: \[a_n < \frac{1 + \sqrt{3}}{2}\]

Since \[a_m > a_n \quad \text{for} \quad m > n \quad \text{and} \quad \frac{a_m}{2} \quad \text{is an integer}\]

we have \[a_m > 1 \quad \text{for} \quad m > 1 \quad \text{then} \quad \frac{1 + a_m}{2} \quad \text{and} \quad 2a_{m+1} = 2 \cdot \frac{2a_m + 1}{2} = a_m + 1 \quad \text{is also an integer} \quad \text{for} \quad m > 1\]

\[
a_{m+1} = 1 + \frac{a_m}{2} \leq 1 + \frac{a_m}{2} \cdot 1 + \frac{1}{2} \cdot \frac{2 + \sqrt{3}}{2} = \frac{2 + \sqrt{3}}{2} \quad \leq \frac{2 + \sqrt{3}}{2} = \frac{1 + \sqrt{3}}{2}
\]

---

Lecture 9: 10/16/2019

Chapter 6: The language of Set Theory.
A set is any well-defined collection of objects, in a way we will see later.

Ex.: 
- \( \mathbb{Z} \) is the set of integers
- \( \mathbb{N} \) or \( \mathbb{Z}^+ \) set of positive integers
- \( \mathbb{Q} \) set of rational numbers
- \( \mathbb{R} \) set of real numbers
- \( \mathbb{C} \) set of complex numbers.

Notation: If \( E \) is a set, we denote that \( x \) is an element of \( E \) by \( x \in E \); \( x \) is not an element of \( E \) by \( x \notin E \).

Ex.: If \( E = \mathbb{R} \), then \( 12 \notin \mathbb{A} \), \( \frac{1}{2} \in \mathbb{A} \), \( \frac{1}{2} \notin \mathbb{Z} \), \(-3 \notin \mathbb{Z} \).

How to describe a set?

1. By words: e.g. The set of odd integers between 2 and 10.
(i) **Notation:** Let us by listing the elements of the set

- \( \{3, 5, 7, 9\} \)
- \( \mathbb{N} = \{1, 2, 3, \ldots\} \)

(ii) **Set builder: conditional notation**

Here, we have a set \( A \) and a property \( P \) on the element of \( A \).

We define the set \( B := \{ e \in A : P(e) \text{ is true} \} \)

\( = \{ e \in A \mid P(e) \text{ is true} \} \)

Equivalent notations

- \( \{ x \in \mathbb{N} : 2 \leq x \leq 10 \text{ and } x \text{ is odd} \} = B \)
- \( \{ a \in \mathbb{R} : a^2 - a - 2 = 0 \} = \{-1, 2\} = \{ x \in \mathbb{R} \mid x^2 - x - 2 = 0 \} \)
(\(a, x\) are placeholder, you can change them as you wish)

\(\Box\)

Set builder: constructive notation

We have a set \(A\) and a function \(f(x)\) on its elements.

We define the set \(B := \{ f(a) : a \in A \}\)

**Ex.**

\[ \{ x^2 + 1 : x \in \mathbb{N} \text{ and } 1 \leq x \leq 4 \} = B \]

\[ \{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \} = A. \]

\(\Box\)

Two sets \(A, B\) are equal, written \([A = B]\), if they have the same elements, that is,

\[ x \in A \iff x \in B \]

**Ex.**

\[ A := \{ x \in \mathbb{N} : x^2 - (\sqrt{2} + 1)x + \sqrt{2} - 0 \} = \{ \sqrt{2}, 1 \} := B \]

**Proof**

\[ x \in A \iff 0 = x^2 - (\sqrt{2} + 1)x + \sqrt{2} = (x-1)(x-\sqrt{2}) \iff x = \sqrt{2} \text{ or } x = 1. \]
\[ A \subseteq \{ x \in \mathbb{N} : x^2 - (\sqrt{2}+1)x + 1 = 0 \} \]

\[ A \cap B = \emptyset, \quad A = \{ 1 \} \]

**Def.** The empty set is the unique set with no elements, denoted by \( \emptyset \).

**Def.** Given sets \( A, B \) we say that:

- **A is a subset of B** if \( x \in A \implies x \in B \), denoted \( A \subseteq B \).
- **A is a proper subset of B** if \( x \in A \implies x \in B \) and there is \( b \in B \) with \( b \notin A \), denoted \( A \subset B \).

By def. \( A = B \iff A \subseteq B \text{ and } B \subseteq A \).

Let: \( \{ x \in \mathbb{R} : x^2 - x - 2 = 0, x > 0 \} \subset \{ x \in \mathbb{R} : x^2 - x - 2 = 0 \} \).
Operations on sets:

**Def.** Given two sets $A$ and $B$, we can define:

- the intersection of $A$ and $B$, \( A \cap B = \{ x : x \in A \land x \in B \} \)
- the union of $A$ and $B$, \( A \cup B = \{ x : x \in A \lor x \in B \} \)
- the difference of $A$ and $B$, \( A \setminus B = \{ x : x \in A \land x \notin B \} \)

Moreover, we say that $A$ and $B$ are disjoint if \( A \cap B = \emptyset \)

**Proposition.** Given $A, B$, we have:

1. $A \cap B$, $A \setminus B$, $B \setminus A$ are pairwise disjoint
2. $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$
Proof: To prove these types of formulas there are 3 ways:

- **Rules of Truth**: Suppose
  
  \[ A := \{ x \in C : P(x) \} \]
  \[ B := \{ x \in C : Q(x) \} \]

  Then:
  
  \[ A \land B := \{ x \in C : P(x) \land Q(x) \} \]
  \[ A \lor B := \{ x \in C : P(x) \lor Q(x) \} \]
  \[ A \setminus B := \{ x \in C : P(x) \lor \neg Q(x) \} \]
  \[ A \subseteq B := \{ x \in C : P(x) \Rightarrow Q(x) \} \]
  
  and so on...

So to check our claims we have \( P(x) : x \in A \), \( Q(x) : x \in B \)

<table>
<thead>
<tr>
<th>( x \in A )</th>
<th>( x \in B )</th>
<th>( x \in (A \land B) )</th>
<th>( (A \lor B) )</th>
<th>( x \notin B \setminus A )</th>
<th>( x \in A \lor B )</th>
<th>( x \in (A \land B) \lor (B \setminus A) )</th>
<th>( x \in A \lor B )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

These are the same.
Venn's diagram:

Let's prove that $A \cap B$ and $A \cap B'$ are disjoint. By definition, we need to show that

$$(A \cap B) \cap (A \cap B') = \emptyset.$$ 

Indeed, if $x \in A \cap B$, then $x \in A$ and $x \in B$. But then $x \notin A \cap B'$.

Analogously, if $x \in (A \cap B')$, then $x \in A$ and $x \notin B$. But then $x \notin A \cap B$. 

$\Box$
(Def) Let $U, A \subseteq U$ be two sets. The complement of $A$ in $U$ is
\[ A^c = U - A = \{ x \in U : x \notin A \} \]

$\mathbb{Z} - \mathbb{N} = \{ n \in \mathbb{Z} : n \leq 0 \}$

(Def) Given a set $X$, the power set of $X$, denoted by $\mathcal{P}(X)$, is the set of all subsets of $X$, that is
\[ A \in \mathcal{P}(X) \iff A \subseteq X \]

Ex.: $X = \{ 1, 2 \}$, $\mathcal{P}(X) = \{ \emptyset, \{ 1 \}, \{ 2 \}, \{ 1, 2 \} \}$.

(Def) Given two sets $X, Y$, the Cartesian product of $X$ and $Y$ is the set, defined by
\[ X \times Y = \{ (x, y) : x \in X \text{ and } y \in Y \} \]
The elements of \( X \times Y \) are ordered pairs, that is \((x_1, y_1) = (x_2, y_2) \iff x_1 = x_2 \quad \text{and} \quad y_1 = y_2\). The \( x, y \) are called the coordinates of \((x, y)\).

Example \( X = \{1, 2, 3\} \) \( Y = \{1, 2\} \)

\[
X \times Y = \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,2)\}
\]

\[
Y \times X = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}
\]
Chapter 7: Quantifiers

This chapter is about notations, we are going to learn the most common symbols of math.

Universal and existential statements in one free variable

(1) The notation " ∀x ∈ A, P(x) " means:
- for each element x in the set A, P(x) is true
- P(x) is true for every x ∈ A
- { x ∈ A : P(x) } = A.

And it is called universal statement. " ∀ " is called universal quantifier.

ex.: ∀x ∈ R \{0\} x^2 > 0

(equivalent to { x ∈ R \{0\} : x^2 > 0 } = R \{0\}

and \( a \in R \{0\} \Rightarrow a^2 > 0 \)

(2) The notation " ∃x ∈ A, P(x) " means
There exist $a \in A$ with $P(a)$ is true
$P(a)$ is true for at least one $a \in A$
$\{a \in A : P(a)\} \neq \emptyset$

and it is called existential statement
"$\exists$" is called existential quantifier.

\[ \exists a \in \mathbb{Z}, \; a > 0 \]
\[ \exists x \in \mathbb{R}, \; x^2 = 2 \]

*Remark:* Variables attached to $\forall, \exists$ are dummy variables.
$\forall a \in A \; P(a)$ is the same as $\forall x \in A, \; P(x)$. 

**Example:** 1. How universal statement: $\forall x \in (1, +\infty), \; x^2 > x$

(then $(1, +\infty) = \{ x \in \mathbb{R} : \; x > 1 \}$.)

**Proof:** $\forall x \in (1, +\infty), \; x^2 - x > 0$ is equivalent to $(x > 1 \implies x^2 - x > 0)$

So we prove the implication, assume $x > 1$, then
\[ x > 0 \text{ and } x - 1 > 0 \implies x (x - 1) > 0 \]
\[ \frac{x^2 - x}{x^2} \]

\[ \text{Show the existential statement: } \exists x \in \mathbb{N}, \ x^2 = 9 \]

**Proof:** Choose \( x = 3 \), then \( 3^2 = 9 \)

(We don't need to use \(-3\), one value is enough as this is an existential statement)

**Disproving universal and existential statements**

\[ \neg \left( \forall a, P(a) \right) \text{ is equivalent to } \left( \exists a \in A, \neg P(a) \right) \]

\[ \neg \left( \exists a, P(a) \right) \text{ is equivalent to } \left( \forall a \in A, \neg P(a) \right) \]

e.g. (ii) Disprove the statement \( \forall x \in \mathbb{N}, x \geq 2 \)

\[ \neg \text{; Need to prove } \exists x \in \mathbb{N}, x \leq 2 \text{; take } x = 1. \text{ Then } 1 \in \mathbb{N} \text{ and } 1 \leq 2. \]

\[ \text{ii: } \exists \text{; Need to prove } \exists x \in \mathbb{N}, x \leq 2 \text{; take } x = 1. \text{ Then } 1 \in \mathbb{N} \text{ and } 1 \leq 2. \]
There is no real number $x \in \mathbb{R}$ with $x^2 = -1$.

\[ \forall x \in \mathbb{R} \quad x^2 \geq 0 \implies \forall x \in \mathbb{R}, \quad x^2 \neq -1 \quad \text{if} \quad x = 1. \]

\text{(Universal statements with many free variables)}

Suppose $P(a, b)$ with $a \in A$, $b \in B$. Then we can form many different statements like

$\forall a \in A \quad \exists b \in B, \quad P(a, b)$

$\exists a \in A \quad \exists b \in B, \quad P(a, b)$

$\forall a \in A \quad \forall b \in B, \quad P(a, b)$

$\exists a \in A \quad \forall b \in B, \quad P(a, b)$

$\forall b \in B \quad \exists a \in A, \quad P(a, b)$

$\exists b \in B \quad \exists a \in A, \quad P(a, b)$

\[ \text{Determine if the following universal/existential statements are true or false.} \]

a) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad x < y$

b) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \quad x < y$

c) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad x < y$

d) $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, \quad x < y$
Set 1: a) False, negation $\exists x \in \mathbb{N} \forall y \in \mathbb{N} x < y$ (x=1, y=2)
b) True, take $y = x+1$ (negation $\exists x \in \mathbb{N}, \forall y \in \mathbb{N} x < y$)
c) False, negation $\forall x \in \mathbb{N} \exists y \in \mathbb{N} x < y$ (told $y=x$)
d) True, take $y = 2, x = 1$ (negation $\forall x \in \mathbb{N} \exists y \in \mathbb{N} x < y$).

Let's read the problem as using cartesian product of set.

We look at $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$

$A = \{(x, y) \in \mathbb{N}^2 : x < y\}$

a) $A = \mathbb{N}^2$ False

d) $A = \phi$, True

b) $\forall x \in \mathbb{N} \Rightarrow A \cap \{x \times \mathbb{N}\} \neq \phi$ False!

c) $\exists x \in \mathbb{N} \Rightarrow \{x \times \mathbb{N}\} \subseteq A$ False!
A very common use of quantifiers is the definition of limit in analysis.

**Def:** Let $(a_n)_n$ be a sequence. We say that $L \in \mathbb{R}$ is the limit of $(a_n)_n$, and denote it by $\lim_{n \to \infty} a_n = L$, if

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \text{ s.t. } |a_n - L| < \varepsilon \quad \forall n \geq N$$

**Example:** Consider the seq. $a_n = \frac{1}{n^2}$. Prove that

$$\lim_{n \to \infty} \frac{1}{n^2} = 0$$

**Proof:** We have to show that $\forall \varepsilon > 0 \exists N \in \mathbb{N}$ s.t. $|\frac{1}{n^2} - 0| = \frac{1}{n^2} < \varepsilon \quad \forall n \geq N$

Fix $\varepsilon > 0$ arbitrary number, then choose $N = \frac{1}{\sqrt{\varepsilon}}$. Then

$$\frac{1}{n^2} < \frac{1}{N^2} = \frac{1}{\left(\frac{1}{\sqrt{\varepsilon}}\right)^2} = \varepsilon \quad \forall n \geq N.$$
Small recap on Set theory and quantifiers

\[ (x \in C \subseteq (A \cup B) \land (A \cap C) \subseteq (A \cap B) \implies C \subseteq B. \]

\[ (x \in A \times B = B \times A \implies A = B) \]

\[ (A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) \]

**proof:**
1. We need to show that \( x \in C \implies x \in B \). To prove this by contradiction, assume \( x_0 \in C \) and \( x_0 \notin B \). Now there are 2 possibilities:
   a) \( x_0 \in A \cap C \implies x_0 \notin A \cup B \implies x_0 \notin B \)
   b) \( x_0 \in (A \setminus C) \implies x_0 \in A \cup B \) and \( x_0 \notin A \)
\( \Rightarrow x_0 \in B \implies \exists y \in A \times C \)  

2. \( \subseteq \) trivial

\[ A \times B = B \times A \iff [(x, y) \in A \times B \iff (x, y) \in B \times A] \]

\[ \Rightarrow [x \in A \land y \in B \implies x \in B \land y \in A] \]

\[ \Rightarrow [x \in A \iff x \in B] \implies A = B \]

3. \( (x, y) \in (A \times B) \cap (C \times D) \iff (x, y) \in A \times B \land (x, y) \in C \times D \)

\[ \Rightarrow x \in A \land y \in B \land x \in C \land y \in D \]

\[ \Rightarrow x \in B \land y \in B \land \implies B \land y \in D \]

\[ \Rightarrow x \in A \land y \in C \land y \in D \]

\[ \Rightarrow (x, y) \in (A \cap C) \times (B \cap D) \]
(Ex 2) Prove or disprove:

1. \( \exists x \in \mathbb{N} \ \forall y \in \mathbb{N} \quad y^2 > 2019 + x \)
2. \( \exists x \in \mathbb{N} \ \forall y \in \mathbb{N} \quad y^3 > 2019 + x \)

Proof:
1. True, choose \( x = -2020 \), then \( y^2 > 2019 - 2020 + 1 \) \( \forall y \in \mathbb{N} \).
   (the negation would be \( \forall x \in \mathbb{N} \ \exists y \in \mathbb{N} \) \( y^2 \leq 2019 + x \))

2. False, indeed the negation is \( \forall x \in \mathbb{N} \ \exists y \in \mathbb{N} \ y^3 \leq 2019 + x \).
   Choose \( y = \sqrt[3]{2019 + x} - 1 \) and it proves the negation.
   \( \forall x \in \mathbb{N} \ \exists y \in \mathbb{N} \) \( y^3 \leq 2019 + x \)
   \( \text{} \) (let us give me \( x \) and I give you \( y \)!) 

(Ex 3) Prove that \( \lim_{n \to \infty} \frac{1}{1 + n^3} = 0 \)

Proof: Let \( \varepsilon > 0 \), Notice that \( \frac{1}{1 + n^3} < \varepsilon \) \( \iff n^3 > \frac{1}{\varepsilon} - 1 \)
\[ n > \sqrt[3]{\frac{1}{\varepsilon} - 1} \]
So choosing \( N = \sqrt[3]{\frac{1}{\varepsilon} - 1} \) we have
\[
\frac{1}{n^2+1} \leq \frac{1}{n^2} \leq 3 \quad \forall n \geq N
\]

Week 6: Lectures 14-15-16 see Brandon Seward's webpage for MATH 109: Chapters 8 and 9.

Lecture 17: 11/04/2019

Chapter 10: Counting

For every \( m \in \mathbb{N} \), we define the set

\[ N_m : = \{ 1, 2, \ldots, m \} = \{ n \in \mathbb{N} : 1 \leq n \leq m \} \]

and we say that \( N_m \) has \( m \) elements.

When we "count" the elements of a finite set, we essentially building a bijection from the set \( N_m \), for some \( m \),
to the set being counted.

(\text{Remember that } f: X \to Y \text{ is a bijection if it is injective and surjective, that is if: } \begin{align*}
&\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \\
&\forall y \in Y \exists x \in X \text{ so } f(x) = y
\end{align*}
\text{ that they have the same \# of elements})

\textbf{Def: Let } X \text{ be a set. If there is a bijection } f : \mathbb{N}_m \to X
\text{ then we say that the cardinality of } X \text{ is } m \text{ and we write } |X| = m.
\text{The cardinality of } |f| \text{ in defined to be } |f| = |X| = \mathbb{N}_m.

\textbf{Example:} \text{ The set } X = \{1, 5, 9, 10, 17\} \text{ has cardinality } 5,
\text{ indeed:}
\begin{array}{c|ccccc}
| & 1 & 2 & 3 & 4 & 5 \\
\hline
f & 1 & 5 & 9 & 10 & 17
\end{array}
\text{ (} f(1) = 1, f(2) = 5 \text{ ...)}
Q: There are other ways of counting $X$, for example

<table>
<thead>
<tr>
<th>$f$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f(X)$</td>
<td>5</td>
<td>9</td>
<td>10</td>
<td>17</td>
<td>4</td>
</tr>
</tbody>
</table>

So there are many bijections \( f : \mathbb{N} \to X \)

In order to say that our definition is well-posed, we need to show that for every such bijection \( f \) in $\mathbb{N}$, the number of the form \( f(n) \) is always the same, that is there are no two different bijections \( f : \mathbb{N} \to X \) and \( g : \mathbb{N} \to X \) such that \( n \neq m \).

**Theorem:** If \( f : \mathbb{N} \to X \) and \( g : \mathbb{N} \to X \) are bijections, then \( m = n \).

Idea:

\[
\begin{align*}
\mathbb{N} & \xrightarrow{f} X \xrightarrow{g} \mathbb{N} \\
\mathbb{N} & \xrightarrow{f^{-1}} X \xrightarrow{g^{-1}} \mathbb{N}
\end{align*}
\]

If \( f, g \) bijections, \( \exists g^{-1} : X \to \mathbb{N} \) and \( f^{-1} : X \to \mathbb{N} \).

Then one can consider the functions \( g^{-1} \circ f : \mathbb{N} \to \mathbb{N} \) and \( f^{-1} \circ g : \mathbb{N} \to \mathbb{N} \).
They are bijections (exercise: prove that they are injective and surjective).

In particular \( f \circ g \) and \( g^{-1} \circ f \) are injections.

Lemma: If \( f \) is an injection \( f: \mathbb{N}_n \to \mathbb{N}_m \), then \( n \leq m \).

Proof: See chapter II, next class.

Proof of theorem (assuming the lemma). The function \( g^{-1} \circ f: \mathbb{N}_m \to \mathbb{N}_m \) is a composition of bijections, and so it is a bijection. In particular \( g^{-1} \circ f \) is an injection and by the lemma \( n \leq m \). Changing the role of \( g \) and \( f \) shows that \( f^{-1} \circ g \) is an injection \( \mathbb{N}_m \to \mathbb{N}_m \) by the lemma \( m \leq n \). Since \( n \leq m \) and \( m \leq n \), we conclude \( n = m \).
**Def.** We say that $X$ is finite if $|X| = n$ for some integer $n \in \mathbb{N}$. Otherwise we say that $X$ is infinite.

**Rem.:** At the end, to prove that a set is finite we still need to find a bijection $\mathbb{N}_n \rightarrow X$, but only one!

**Rem.:** We used the following exercises:

1. If bijection $\Rightarrow f^{-1}$ bijection
2. If $g$ bijections $\Rightarrow f \circ g$ bijection

Meet us and see some country pigeons.

**Theorem.** Suppose $X$, $Y$ are disjoint finite sets. Then $X \cup Y$ is finite and $|X \cup Y| = |X| + |Y|$

**Proof:** Let $n = |X|$ and $m = |Y|$, we need to show that $|X \cup Y| = n + m$. 
If \( m = 0 \), then \( X = \emptyset \) and \( X \cup Y = Y \) as let
\[
|X \cup Y| = |Y| = m = m + 0 = |Y| + |X|
\]

If \( m = 0 \), done.

If \( m, m > 0 \), then we have bijections \( f: N_m \to X \)
\( g: N_m \to Y \)

Next define the function \( h: N_{m+m} \to X \cup Y \) by
\[
h(i) = \begin{cases} f(i) & \text{if } 1 \leq i \leq m \\ g(i - m) & \text{if } m + 1 \leq i \leq m + m \end{cases}
\]

To conclude the proof we need to show that \( h \) is bijection.
Let \( x \in X \cup Y \), then if \( x \in X \cap \in \mathbb{N} \) and 
\[
h(x) = f(h) = x
\]
if \( x \in Y \cap \in \mathbb{N} \) and 
\[
h(x) = f(h) = y
\]

Let \( h(i) = h(j) \in X \cup Y \), then, since \( X \cap Y = \emptyset \), 
\[
\begin{align*}
\text{either } h(i) &= h(j) \in X \implies f(h) = f(j) \implies i = j \ \\
\text{or } h(i) &= h(j) \in Y \implies g(h) = g(j) \implies i = j.
\end{align*}
\]

Therefore, by definition 
\[
\left| X \cup Y \right| = m + m = |X| + |Y|.
\]

In particular \( |X \cup Y| \) is finite. \( \Box \)

**Corollary** If \( X, X_2, \ldots, X_m \) are a collection of pairwise disjoint 
(meaning \( i \neq j \implies X_i \cap X_j = \emptyset \)) finite sets \( \text{then} \) 
\[
\left| X_1 \cup \ldots \cup X_m \right| = \sum_{i=1}^{m} |X_i|
\]

**Proof**: Using previous theorem and induction (Exercise) \( \Box \)
Theorem: If \( X, Y \) are finite sets with \(|X| = m, |Y| = n\), then \(|X \times Y| = m \cdot n\).

Idea: \[ X = \{ x_1, \ldots, x_m \}, \quad Y = \{ y_1, \ldots, y_n \} \]

\[
X \times Y = \{ (x_1, y_1), (x_1, y_2), \ldots, (x_1, y_n), (x_2, y_1), (x_2, y_2), \ldots, (x_2, y_n), \ldots, (x_m, y_1), (x_m, y_2), \ldots, (x_m, y_n) \}
\]

Let \( X \times Y = \bigcup_{i=1}^{m} \{ x_i \} \times Y \). If \( f: N \to Y \) is a bijection

Then define \( F: N \to \{ x_i \} \times Y \)

\[ i \mapsto (x_i, f(i)) \] is a bijection

\[ \Rightarrow |\{ x_i \} \times Y| = n \] for every \( i \), and \( (|x_i| \times Y) \cap (|x_i| \times Y) \)

\[ \Rightarrow \text{By the Theorem} \quad |X \times Y| = m \cdot n. \]
Example: Let \( \Delta N_q : = \{ (m, n) : m, n \in N_q \} \subseteq N_q \times N_q \)

1. What is \( |\Delta N_q| = ? \)
2. What is \( |(N_q \times N_q) \setminus \Delta N_q| = ? \)

Sol: (2) Let \( f : N_q \to \Delta N_q \) where \( f \) is a bijection (easy delt)
\[
i \to (i, i)
\]
\[
\Rightarrow |\Delta N_q| = q = |N_q|^2
\]

(1) Note that \( |N_q \times N_q| = q \cdot q = 81 \) and
\[
|(N_q \times N_q) \setminus (\Delta N_q)| \cup (\Delta N_q) = N_q \times N_q
\]
\[
\Rightarrow |N_q \times N_q| = |(N_q \times N_q) \setminus (\Delta N_q)| + |\Delta N_q|
\]
\[
\Rightarrow 81 = |(N_q \times N_q) \setminus \Delta N_q| + q = 78.
\]
The inclusion–exclusion principle: If $X, Y$ are finite sets, then
\[ |X \cup Y| = |X| + |Y| - |X \cap Y|. \]

Proof: Recall that $X \cup Y = (X \setminus Y) \cup (Y \setminus X) \cup (X \cap Y)$
and the union is pairwise disjoint.

On the other hand, $X = (X \setminus Y) \cup (X \cap Y)$ and
$Y = (Y \setminus X) \cup (X \cap Y)$ disjoint unions.
Example: \( A, A_2, A_3, A_4 \) — \( N_3 \), I can be \{1, 2, 3\}.
\[ I = \{1, 2, 3\} \]
\[ I = \{1\} \]
\[ I = \{2, 3\} \]

Plan
\[ A = A_1 + A_2 + A_3 + A_4 \]
\[ I = I_1 + I_2 + I_3 + I_4 \]

- Define \( A = A_1, A_2, A_3, A_4 \)
- Define \( I = I_1, I_2, I_3, I_4 \)

Note:
\[ A = A_1 + A_2 + A_3 + A_4 \]
\[ I = I_1 + I_2 + I_3 + I_4 \]

\[ A_1 = \{1, 2, 3\}, A_2 = \{1\}, A_3 = \{2, 3\} \]

So:
\[ A = A_1 + A_2 + A_3 + A_4 \]
\[ I = I_1 + I_2 + I_3 + I_4 \]

\[ A = I \]
\[ \{1, 2, 3\} + \{1\} + \{2, 3\} = \{1, 2, 3\} \]

\[ I = I_1 + I_2 + I_3 + I_4 \]
\[ \{1\} + \{2, 3\} = \{1, 2, 3\} \]
Problem: There are 144 tiles. They are triangular or square, red or blue, wooden or plastic. Assume there are
68 wooden tiles,
69 red tiles,
75 triangular tiles,
36 red wooden tiles,
40 triangular wooden tiles,
38 red triangular tiles,
28 red triangular wooden tiles.
How many blue plastic square tiles?

Sol: If a tile is not (blue and plastic and square)
then it is (red or wooden or triangular).
Let
\[ R = \text{red tiles}, \quad W = \text{wooden tiles}, \quad T = \text{triangular tiles}. \]
Then the answer to the question is \( 144 - |R \cup W \cup T| \).
We use inclusion-exclusion principle:

\[
|R \cup W \cup T| = |R| + |W| + |T| - |R \cap T| - |W \cap T| - |R \cap W|
+ |R \cap W \cap T|
\]
Now we prove the lemma from last class:

**Lemma:** If \( f : \mathbb{N}_m \to \mathbb{N}_m \) is injective, then \( m \leq m \).

**Proof:** We will prove this by induction on \( m \in \mathbb{N} \).

**B.1:** \( m = 1 \): Let \( f : \mathbb{N}_m \to \mathbb{N}_1 \) be an injection. Suppose by contradiction that \( m > 1 \). Then \( 1, 2 \in \mathbb{N}_m \) and since \( \mathbb{N}_1 = \{1\} \) we must have

\[ f(1) = 1 = f(2) \]

This \( f \) is injective, this implies \( 1 = 2 \) \( \implies \) \( m \leq 1 \)

\[ = 68 + 69 + 75 - 36 - 40 - 38 + 23 = 121 \]

\[ \Rightarrow 144 - 121 = 23 \]
Now as inductive assumption assume $k \geq 1$ is an integer with the property that if $m \in \mathbb{N}$ and $f: \mathbb{N}_m \to \mathbb{N}_k$ is injective, then $m \leq k$.

Let $m \in \mathbb{N}$ and let $f: \mathbb{N}_m \to \mathbb{N}_{k+1}$ be an injection. Then there are two possibilities:

$(\forall i \in \mathbb{N}_m \ f(i) \leq k)$ or $(\exists i \in \mathbb{N}_m \ f(i) = k+1)$

**Case 1:** Assume $\forall i \in \mathbb{N}_m \ f(i) \leq k$. Then $\text{Im}(f) = \mathbb{N}_k$ and $f: \mathbb{N}_m \to \text{Im}(f) = \mathbb{N}_k \subseteq \mathbb{N}_{k+1}$ is injective, by inductive assumption $m \leq k < k+1$.

**Case 2:** Assume $\exists i_0 \in \mathbb{N}_m \text{ s.t. } f(i_0) = k+1$. Define

$$h(i) = \begin{cases} f(i) & \text{if } i \leq i_0 \\ f(i_0) & \text{if } i > i_0 \end{cases}$$

for all $i \in \mathbb{N}_{m-1}$. Then $h$ is injective and $h: \mathbb{N}_{m-1} \to \mathbb{N}_k$ (Lemma). By inductive assumption $m-1 \leq k \Rightarrow m \leq k+1$.
Continuing these 2 cases we see that if \( m \in \mathbb{N} \) and

\[
f: \mathbb{N}_m \rightarrow \mathbb{N}_{m+1}\]

then

\[m \leq m+1\]

By induction we conclude \( \forall m, m \in \mathbb{N}, f: \mathbb{N}_m \rightarrow \mathbb{N}_m \) injective implies \( m \leq m \).

Suppose \( X, Y \) are finite sets. Let there be an injection \( f: X \rightarrow Y \) then \( |X| \leq |Y| \).

pf: By assumption \( \exists m, m \in \mathbb{N}, |X| = m, |Y| = m \) and the one injection

\[
g_1: \mathbb{N}_m \rightarrow X
\]

\[
g_2: \mathbb{N}_m \rightarrow Y
\]

Let \( h := g_2^{-1} \circ f \circ g_1: \mathbb{N}_m \rightarrow \mathbb{N}_m \), \( h \) is injective

\[m \leq m \Rightarrow |X| \leq |Y|\]
(The pigeonhole principle) If \( f : X \to Y \) is a function between finite sets with \(|X| > |Y|\), then \( f \) is not injective, i.e., \( \exists x_1, x_2 \in X \) s.t. \( f(x_1) = f(x_2) \).

**Proof:** This is the contrapositive of the previous corollary.

**Example:**