Alice and Bob want to exchange private notes. Unfortunately, sitting between them is their "friend" Carl, who they don't really trust. Carl tries to read every note that gets passed, whenever he can. So, Alice buys a special briefcase that you can attach locks to. You can actually attach as many padlocks as you want. Alice and Bob both have their own padlocks and keys.

But they can’t share the locks and keys with each other without Carl getting them. So Alice has her lock and key, and Bob has his.

The Problem:

How can Alice send a secret message to Bob without Carl being able to read it?

Solution:

- Alice puts note in briefcase, locks it A
- Bob adds his lock AB
- Alice removes her lock, passes it back B
- Bob can open it.

Recitations now all exist!

Grading scale: A = clear evidence strong mastery of topics

B = evidence of reasonable competence

C = some evidence of adequacy.

D = you were here and I noticed

F = ? were you here?

Counting numbers $\mathbb{N}$ "the natural numbers"

Peano's Axioms for the counting #s.

Idea of "successor function"

To define the concept of natural numbers (counting / add one)

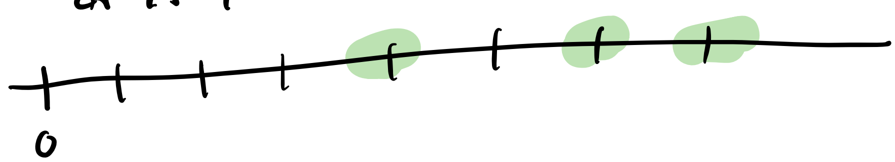
- if n is a counting number, can define a new one called its successor, $S(n)$ $(S(n) = n+1)$
- if n, m are counting #s, and $S(n) = S(m)$ then $n = m$
- There is a number 0 such that $0 \neq S(n)$ for any n.
- If K is a subset of the counting #s, such that
  - $0 \in K$
  - whenever $n \in K$ then also $S(n) \in K$

then K = all the counting #s.

From here, can develop various standard concepts
$+, \times, \leq, \geq, <, >$, etcetera

Example of a proof using these:

Lemma If A is a subset of $\mathbb{N}$, then either A has a smallest element (there exists some $a \in A$ such that $a \leq b$ all $b \in A$) or $A = \emptyset$.



Ex: $A = \{n \in \mathbb{N} \mid n \geq 5\} = \{5, 6, 7, \dots\}$

$\{\frac{1}{x} \mid x \in \mathbb{N}, x \neq 0\} = \{1, 1/2, 1/3, \dots\} \not\subset \mathbb{N}$

Proof: Let $K = \{n \in \mathbb{N} \mid n < a \text{ for all } a \in A\}$

either $0 \in K$ or $0 \notin K$

- if $0 \notin K$ then there is some $a \in A$ w/ $0 \not< a$

$0 \not< a \Leftrightarrow 0 \geq a \Rightarrow 0 = a$

(used if $0 \geq a$ then $0 = a$)

But $0 = a \in A$ so 0 is the smallest element of A.
so done.

- if $0 \in K$

then either A has a smallest element
or it doesn't.

if it does, we're done.

if it doesn't

we claim: $K = \mathbb{N}$ and so $A = \emptyset$

we'll show that $n \in K$ then so is $S(n) = n+1$

if $n \in K$, then $n < a$ all $a \in A$

what if $n+1 \notin K$?

then $n+1 \geq a$ some $a \in A$

but $n \in K$ $\quad n < a \quad$ then $n+1 = a$

$$\begin{array}{cc} & a \\ \bullet & \bullet \\ n & n+1 \end{array}$$

but <u>claim</u>: $\underset{\substack{\shortparallel \\ a}}{n+1}$ = smallest element

since for all $b \in A$ we have $n < b$

$\Rightarrow \underset{\substack{\shortparallel \\ a}}{n+1} \leq b$ so $a \leq b$ all $b \in A$.

so $n+1$ smallest element.

but since A doesn't have a smallest elmt.

this can't happen

So $n+1 \in K$

$\Rightarrow 0 \in K$, whenever $n \in K, n+1 \in K \Rightarrow$

axiom $K = \mathbb{N}$.

$\Rightarrow$ for any $a \in A$ $n \leq a$ for all $n \in \mathbb{N}$

so A can't have any elmts in it.

Once we have counting #s $\mathbb{N}$

$\mathbb{Z}$ = pos & neg #s = integers

$\mathbb{Q}$ = rat'l #s $\left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$

Last time: real #s $\mathbb{R}$ as "infinite decimals"

$\pi = 3.1415926535\ldots$

$\sim 3, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \ldots$

Q: if a decimal

$0.333\ldots$ $\quad 1/3 \quad 0.999\ldots = 1$

$.239257\ldots\ldots$

How can you tell if a number is irrational?

Is $\sqrt{2}$ irrational? Yes ~500BCE Greece.

$.1010101$

$.101001000100001000001$