Wed Sept 11

HW 1 due Friday
OH: Mon 2-3
Today 3-4

Descartes (1637) said:

a point ≡ an ordered list of numbers.

OK, fine. But what is a number?

The Pythagoreans (~500 BC) believed that the universe can be expressed in terms of ratios of whole numbers.

But then they discovered a problem.

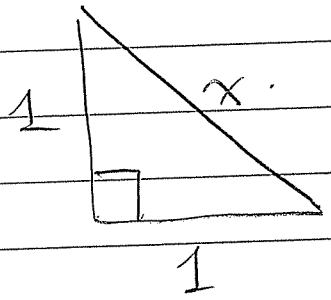
Theorem:

$\sqrt{2}$ can NOT be expressed as a ratio of whole numbers!

Proof: Postponed.

Let's just think about it.

Given a square of side length 1, the diagonal has length $\sqrt{2}$ by Pyth. Thm.



$$x^2 = 1^2 + 1^2 = 2.$$

$$\Rightarrow x = \sqrt{2}.$$

Let's pretend that $\sqrt{2} = a/b$ for some whole numbers a and b.

Then what?

$$a = b\sqrt{2} \implies a^2 = 2b^2$$

So what? We see a^2 is an even number.

What about a? It is also even.
(Could "a" be odd?)

So we could say $a = 2a'$ for some whole number k.
(Such an a' exists.)

Then $2b^2 = a^2 = (2a')^2 = 4(a')^2$

$\Rightarrow$ $b^2 = 2(a')^2$, so b^2 is <u>even</u>.

So what? Then b is even.

$\Rightarrow$ $b = 2b'$ for some whole number b'.

So what? We have

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

Think.....

We could repeat the process to show that a' and b' are even,

Say $a' = 2a''$

$b' = 2b''$

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

So what?

And we could go on FOREVER.

So what?

Key Observation:

If $a = 2a'$ with a and a' positive whole numbers, then

$$a > a' \geq 1$$

Similarly, $a > a' > a'' \geq 1$.

See the Problem?

This CAN'T go on forever!
(Why not?)

We observed the following:

If we can write $\sqrt{2} = \frac{a}{b}$

for positive whole numbers a and b.

then there exist two infinite sequences of whole numbers

$a > a' > a'' > a''' > \cdots \geq 1$

$b > b' > b'' > b''' > \cdots \geq 1.$

But this is NONSENSE (Why?)

Therefore:

It is NOT possible to express $\sqrt{2}$ as a ratio of whole numbers.

Is that a proof?

Yes, but we should clean it up.

We need a better understanding of

LOGIC.

Topic: Informal Logic.

In this class we only have 2 rules:

Rule 1 ("excluded middle")

Every mathematical statement is either T or F.
(NOT both, NOT neither).

Any statement without this property is not a "mathematical statement"

Rule 2 ("material implication").

T flows along arrows $\Longrightarrow$.

i.e.

$T \Rightarrow T$ ✓ $\quad F \Rightarrow T$ ✓ $\quad F \Rightarrow F$ ✓ $\quad T \Rightarrow F$ ✗.

That's it.

Fri Sept 13

HW 1 due NOW.

Today: $\sqrt{2}$

But first, some LOGIC.

We only have two rules:

Rule 1 ("excluded middle")

Any mathematical statement is either T or F (not both, not neither).

Any statement without this property is not a "mathematical statement".

e.g. "$0=1$" is a math. statement

"math is beautiful" is not.

Furthermore, any math. statement P has an opposite statement NOT P with the opposite value

↓

P	NOT P
T	F
F	T

"a truth table"

Rule 2 ("material implication")

T flows along arrows $\Rightarrow$

i.e.

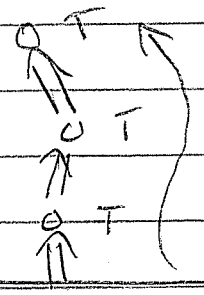
P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Only $T \Rightarrow F$ is bad because the T isn't flowing.

That's All

The idea is that truth flows from the axioms

o ?



axioms = T

axioms T

Logical Principle ("the contrapositive")

F flows backwards. In other words,

$P \Rightarrow Q$ and NOT Q $\Rightarrow$ NOT P

are logically equivalent

Proof: We use a truth table

P	Q	NOT P	NOT Q	$P \Rightarrow Q$	NOT Q $\Rightarrow$ NOT P.
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

They are the same.

Example: Let n be a whole number.

Prove that

"n^2 is even" $\Rightarrow$ "n is even"

Definition: We say n is even if $\exists$ whole number m with $n = 2m$.

We say n is odd if $\exists$ whole number m with $n = 2m+1$.

Exercise: verify that

NOT "n is even" = "n is odd"

Now the Proof:

Let P = "n^2 is even"
Q = "n is even".

Instead of proving $P \Rightarrow Q$ we will prove the (equivalent) contrapositive

NOT $Q \Rightarrow$ NOT P

i.e. "n is odd" $\Rightarrow$ "n^2 is odd".

So, assume that n is odd. i.e. $\exists$ m with $n = 2m+1$.

But then

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1$$
$$= 2(2m+2) + 1.$$

Since $2m+2$ is a whole number (it exists) we conclude that n^2 is odd.

Q: How would you prove

"n^2 is even" $\Rightarrow$ "n is even"

directly?

Assume $n^2 = 2m$ then....

Hmm... this is hard!

Good thing we don't have to. 

Finally, we will write a clean proof that

$\sqrt{2}$ is NOT a ratio of whole numbers

i.e. "$\sqrt{2}$ is irrational"

First we state a

Lemma (little helper Theorem):

For any whole number,

"n^2 is even" $\Rightarrow$ "n is even" ///

Proof of Main Theorem:

We will use proof by contradiction. Assume (for contradiction) that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = a/b$ where a and b are whole numbers with no common divisor (Why? Postponed.)

Then $a = b\sqrt{2}$ and squaring gives $a^2 = 2b^2$. Hence a^2 is even and the Lemma implies that a is even.

i.e. $\exists$ whole number a' with $a = 2a'$.

But then

$$2b^2 = a^2 = (2a')^2 = 4(a')^2$$

$$\Rightarrow \quad b^2 = 2(a')^2$$

Hence b^2 is even and the Lemma says b is even, say $b = 2b'$.

It follows that a and b are both even which contradicts the fact that they have no common divisor.

We conclude that our original assumption was false,

i.e. $\sqrt{2}$ is NOT rational

What did we do?

"$\sqrt{2}$ is rational" ① T?

⇓

"$\sqrt{2} = a/b$ for a, b with no common divisor" ② T

⇓

⋮

⇓

"a and b are both divisible by 2" ③ T

What could the truth values of ①, ②, ③ be?

If ① = T then ② = ③ = T by Rule 2.

But ② and ③ can't both be true by Rule 1, hence 1 can't be true.

By Rule 1, ① is False. ///

Mon Sept 16

HW 2 due Fri Sept 27

Exam 1 Fri Oct 4.

OH: Mon 2-3
Wed 3-4

Today: Boolean Logic

Our standard logic is called "Boolean logic" after George Boole (1815-1864).

It is based on three functions

AND, OR, NOT.

But first, what is a "function"?

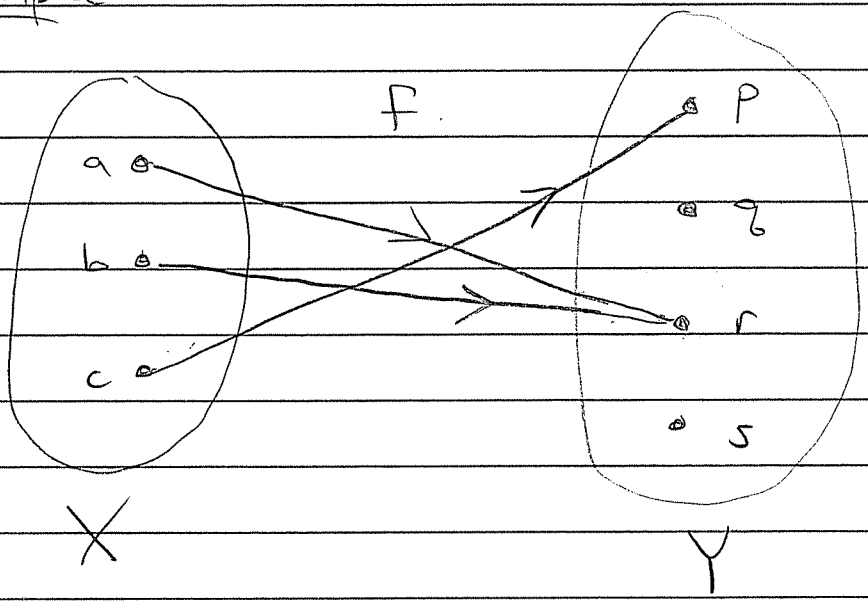
Def:

Let X and Y be sets (collections of things). A function $f: X \to Y$ is a set of arrows satisfying two rules:

(F1) Every arrow points from an element of X to an element of Y.

(F2) Every element of X has exactly one arrow pointing from it.

Example:



We use the notation

$f(a) = r$ " a points to r "

$f(b) = r$ " b points to r "

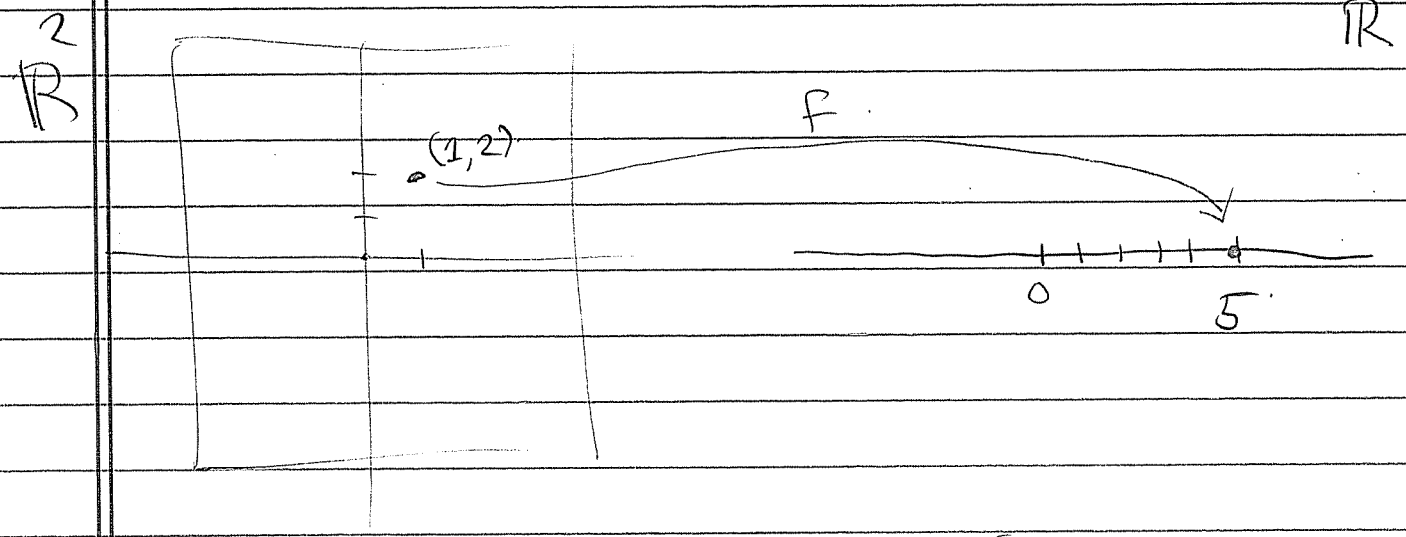
$f(c) = p$ " c points to p "

Example: Sometimes we define a function by a formula. For example, define a function

$$f: \mathbb{R}^2 \to \mathbb{R}$$

by the formula $f(x,y) := x^2 + y^2$.

To each point (x,y) in the plane $\mathbb{R}^2$ we assign the number $x^2 + y^2$.

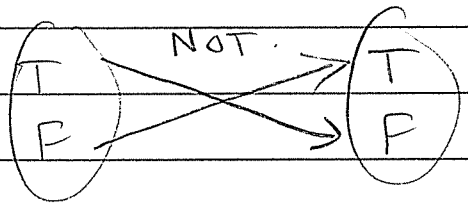


Example: Consider the set $\{T, F\}$ and the set of ordered pairs

$$\{T, F\}^2 := \{(T,T), (T,F), (F,T), (F,F)\}$$

We define 3 important functions.

① NOT : $\{T, F\} \to \{T, F\}$

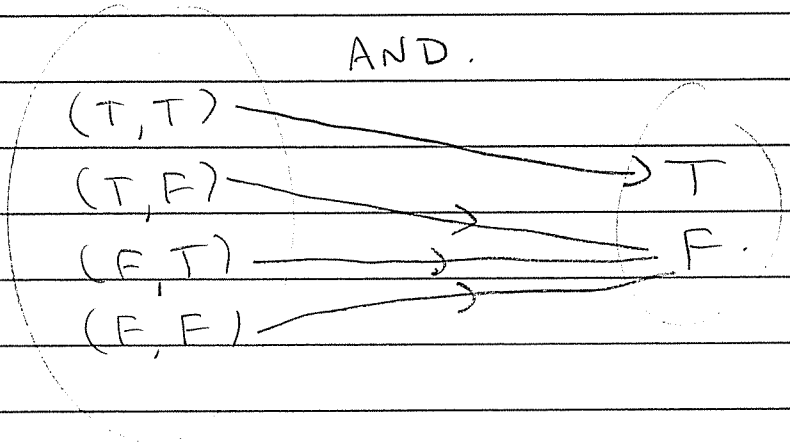


We could write this as a "formula".

$$f(P) = \text{NOT } P$$

where $P \in \{T, F\}$ is a "Boolean variable".

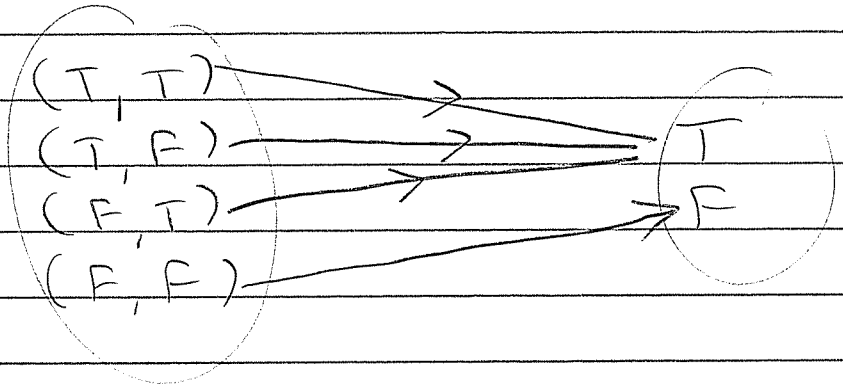
② AND : $\{T, F\}^2 \to \{T, F\}$



As a formula:

$$f(P, Q) = P \text{ AND } Q.$$

③ OR : $\{T,F\}^2 \to \{T,F\}$.



As a formula: $f(P,Q) := P \text{ OR } Q$.

We can combine AND, OR, NOT to form more complicated Boolean functions.

For example,

$f(P,Q,R) = \text{NOT}\left(P \text{ OR}\left(Q \text{ AND } (P \text{ OR } R)\right)\right)$

These are called

"Boolean functions"

or

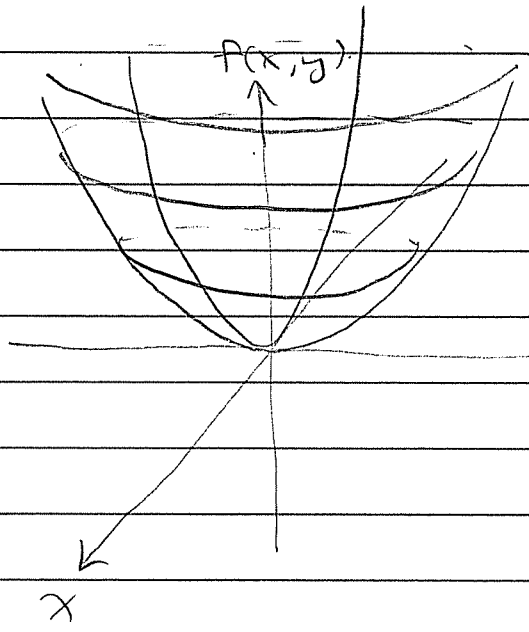
"Boolean polynomials"

Sometimes we visualize a function by drawing its graph (some picture of the set of arrows.

Example: Consider $F: \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x,y) = x^2+y^2$.

If we visualize the arrow $(x,y) \longrightarrow x^2+y^2$ as the point $(x, y, x^2+y^2) \in \mathbb{R}^3$

then the function looks like



a "parabaloid"

Q: What is the graph of a Boolean function ?

Answer: A "truth table".

The graph of $f(P,Q) = P$ OR Q looks like

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

Application: Prove that $f(P,Q) = \text{NOT}(P \text{ OR } Q)$ and $g(P,Q) = (\text{NOT } P) \text{ AND } (\text{NOT } Q)$ are the same function.

P	Q	P OR Q	NOT(P OR Q)	NOT P	NOT Q	(NOT P) AND (NOT Q)
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

This is called "de Morgan's Law".

NOT (P OR Q) = (NOT P) AND (NOT Q)

NOT (P AND Q) = (NOT P) OR (NOT Q).

Terminology:

If two boolean functions are equal, we say they are

logically equivalent

Example:

$P \Rightarrow Q$ and $(\text{NOT } Q) \Rightarrow (\text{NOT } P)$

are logically equivalent.

Wed Sept 18

HW 2 due Fri Sept 27

OH: Mon 2-3
Wed 3-4

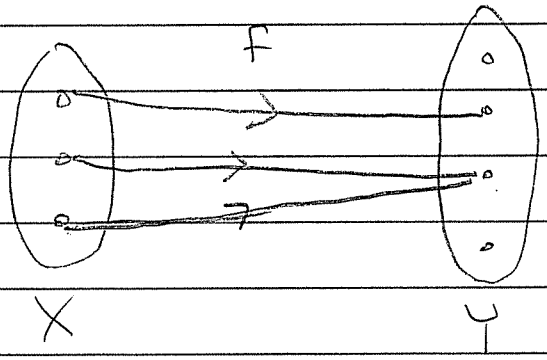
Topic: What is a "number"?

Recall: A function $f: X \to Y$ is a set of arrows from X to Y satisfying

(F1) Every $x \in X$ has ≥ 1 arrows
(F1) Every $x \in X$ has ≤ 1 arrows.

(Together F1 & F2 say: Every $x \in X$ has exactly 1 arrow).

e.g.

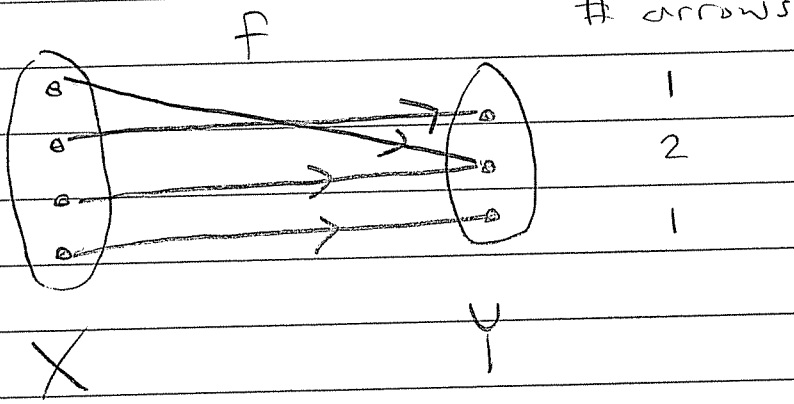


Special Kinds of Functions:

We say the function $f: X \to Y$ is surjective (or "onto") if it satisfies

(F3) Every $y \in Y$ has ≥ 1 arrows.

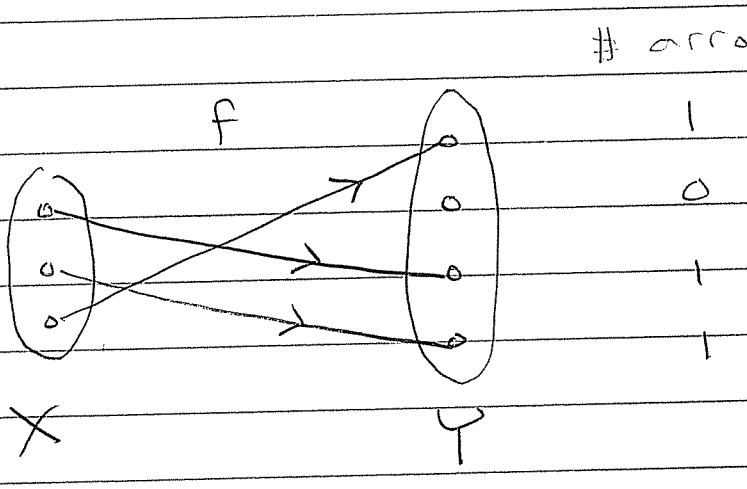
e.g.



We say function $f: X \to Y$ is injective (or "1-to-1") if it satisfies

(F4) Every $y \in Y$ has ≤ 1 arrows.

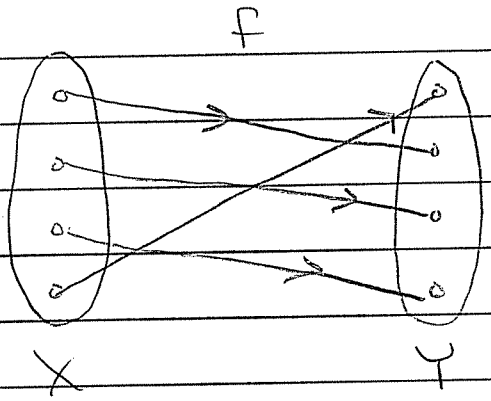
e.g.



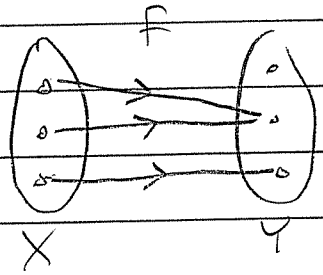
We say the function $f: X \to Y$ is bijective (or a "1-to-1 correspondence") if it satisfies both F3 & F4

i.e. Every $y \in Y$ has exactly 1 arrow.

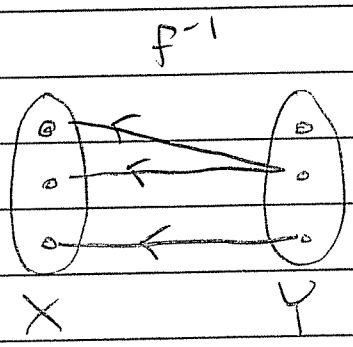
e.g.



If $f: X \to Y$ is a function, let $f^{-1}: Y \to X$ stand for the set of arrows with direction reversed



a function



NOT a function

(Why?)

Q: When is $f^{-1}: Y \to X$ also a function?

Theorem:

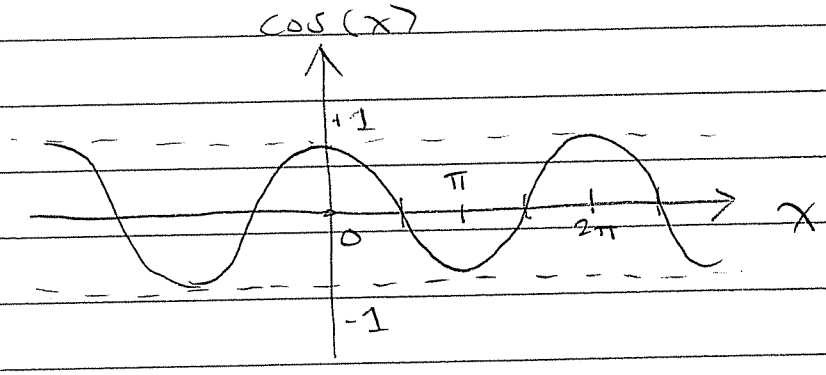
Let $f: X \to Y$ be a function and let $f^{-1}: Y \to X$ be the set of reversed arrows. Then

$f^{-1}: Y \to X$ is a function $\iff$ f is bijective.

(In this case we say f is invertible).

Proof: $f^{-1}: Y \to X$ satisfies the definition of "function" if and only if F3 & F4 are satisfied. ∎

Example: The "cosine" function $\cos: \mathbb{R} \to \mathbb{R}$.



Is cosine invertible? NO.

It is not surjective:

$2 \in \mathbb{R}$ has no arrow pointing to it
($\nexists\, x \in \mathbb{R}$ with $\cos(x) = 2$)

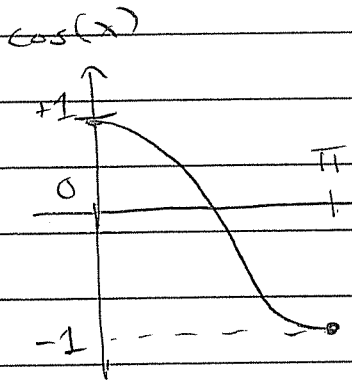
It is not injective:

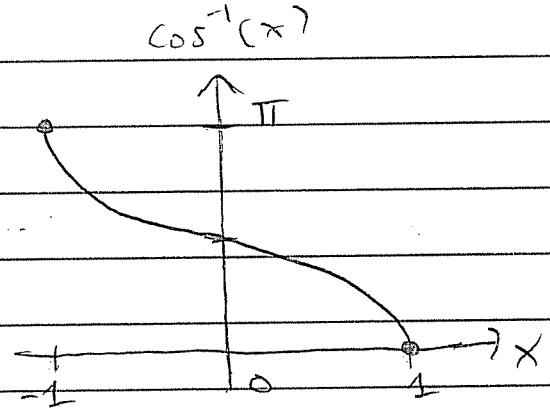
$1 \in \mathbb{R}$ has ∞ many arrows pointing to it.
($\cos(2\pi k) = 1$ for all whole numbers k).

Can we fix it? Yes.

Restrict the domain and range

$\cos : [0, \pi] \to [-1, 1]$





Now $\cos^{-1} : [-1, 1] \to [0, \pi]$ is a function.

(Is this what your calculator does?)

Let X and Y be finite sets

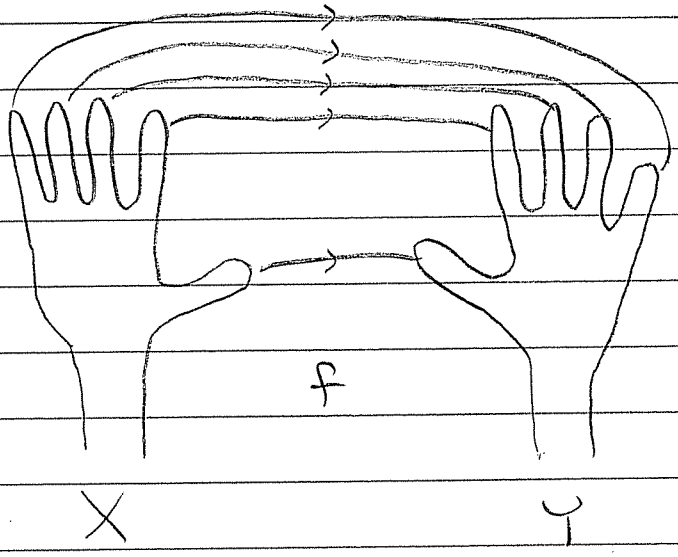
Q: When do X and Y have the same "number" of elements?

A: We say that $|X| = |Y|$ if

$\exists$ a bijection $f: X \to Y$

Q: How do I know my hands have the same "number" of fingers?

A: $\exists$ a bijection



Thinking: So what is a "number"?

Fri Sept 20

HW 2 due Fri Sept 27

Recall: Descartes (1637) says

a point ≡ an ordered list of numbers.

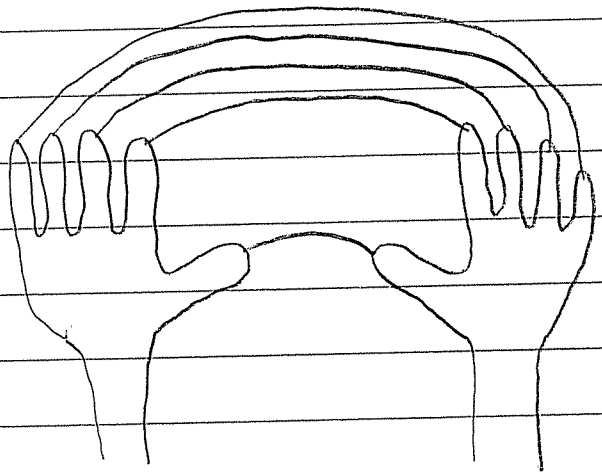
OK, Fine. But what is a "number"?

Today we will define the set $\mathbb{Z}$ of "integers" (whole numbers)

Step 1: A "number" is a quantity of discrete things (e.g. pebbles on a beach)

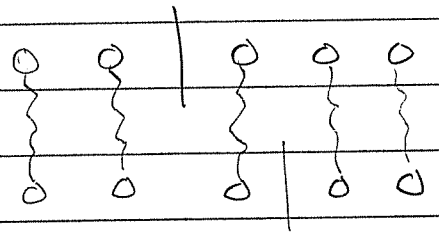
Two collections of things have the same "number" if $\exists$ a bijection between them.

e.g.



✓

"Numbers" can be added and multiplied



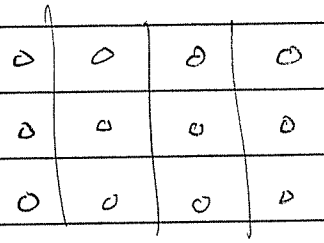
$2+3=5$

$3+2=5$

Theorem: Addition is commutative.

Proof: $\exists$ a bijection. ▨

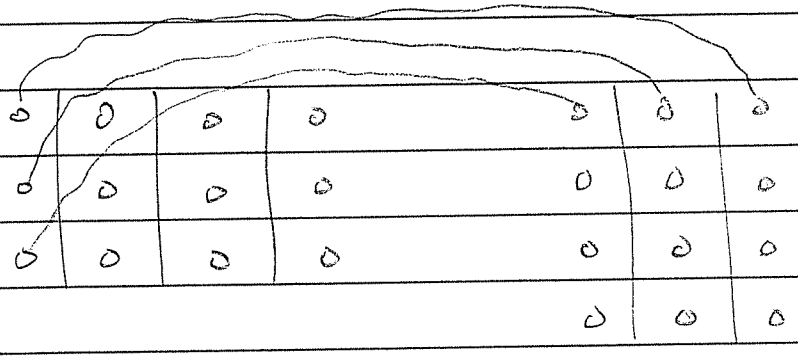
To multiply we arrange pebbles in a rectangle:



$4 \times 3 = 12$

Q: Is mult commutative? Yes!

Proof: $\exists$ a bijection. (rotate 90°).



etc.

$4 \times 3 = 3 \times 4$

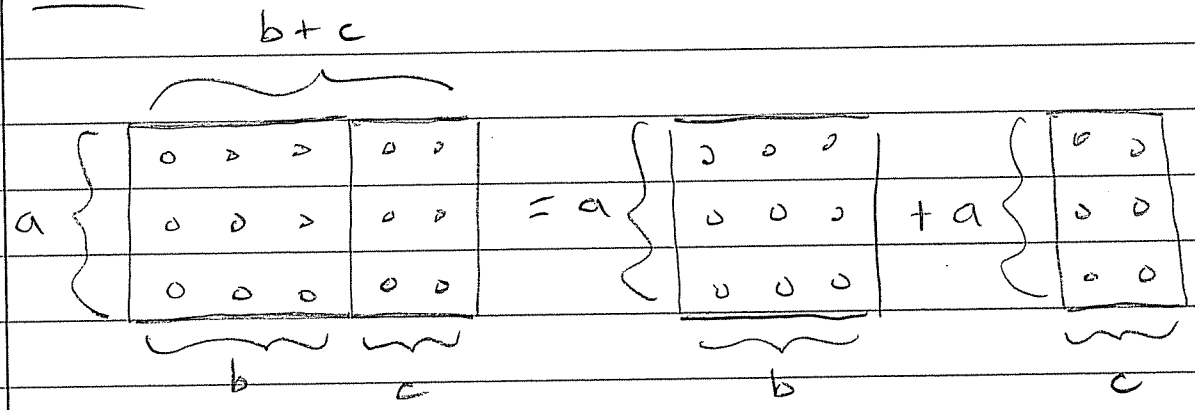
▨

Q: How do + and × interact?

A: × distributes over +

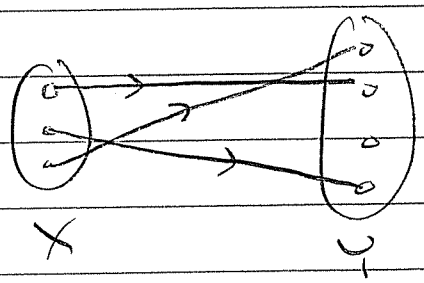
$$a \times (b + c) = a \times b + a \times c$$

Proof:



What about order? What does $a < b$ mean?

Given sets X and Y we say $|X| \leq |Y|$ if $\exists$ an injection $f: X \to Y$.



We say $|X| < |Y|$ if $|X| \leq |Y|$ and $|X| \neq |Y|$

($\exists$ injection but $\nexists$ bijection $X \to Y$)

Thus we can define the "natural numbers" (i.e. the "counting numbers").

$$\mathbb{N} := \{1 < 2 < 3 < \cdots\}$$

Q: Would a Martian know about $\mathbb{N}$?

Leopold Kronecker (1823-1891) thought so.

Quote: "God made $\mathbb{N}$; all else is the work of man."

Over time the natural numbers $\mathbb{N}$ evolved into THE INTEGERS:

$$\mathbb{Z} = \{\cdots < -2 < -1 < 0 < 1 < 2 < \cdots\}$$

$\mathbb{Z}$ is for "Zahlen" (to count)

See the handout.
- There are 12 axioms!
- The first 11 are "obvious", but they can't distinguish $\mathbb{Z}$ from $\mathbb{R}$.

Q: What is the difference between $\mathbb{Z}$ and $\mathbb{R}$.
- This is a subtle question and it leads to the final axiom.

✡ The Well-Ordering Axiom ✡

Every non-empty subset of $\mathbb{N}$ has a smallest element.

[Formally:

"$\forall S \subseteq \mathbb{N}, S \neq \emptyset, \exists a \in S, \forall b \in S, a \leq b$"]

i.e. a is the smallest element of S

$\forall$ = for all
$\exists$ = there exists
$\subseteq$ = is a subset of
$\in$ = is an element of
$\emptyset$ = the empty set

Application of Well-Ordering.

Theorem: There are no uninteresting natural numbers

Proof: Assume for contradiction that there is an uninteresting natural number and let $S \subseteq \mathbb{N}$ be the set of such. Since $S \neq \emptyset$ (by assumption) the Well-Ordering Axiom says that S has a smallest element, say $a \in S$. But then a is "the smallest uninteresting number", which is interesting, contradicting the fact that $a \in S$.

(I learned this theorem and proof from the audio commentary on a "Futurama" DVD.)

Mon Sept 23

HW 2 due this Friday
Exam 1 next Fri Oct 4
OH: Today 2-3
Wed 3-4

Last time we saw the definition of the set of integers

$\mathbb{Z} = \{ \ldots < -2 < -1 < 0 < 1 < 2 < \cdots \}$

It has 12 axioms. Recall the

Axioms of Addition:

(A1) $\forall a, b \in \mathbb{Z}, \quad a+b = b+a$

addition is "commutative"

(A2) $\forall a, b, c \in \mathbb{Z}, \quad a+(b+c) = (a+b)+c$

addition is "associative"

(A3) $\exists 0 \in \mathbb{Z}, \forall a \in \mathbb{Z}, \quad 0+a = a.$

there is a special element called 0.
it is the "additive identity element"

(A4) $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, \; a + b = 0$

every integer has at least one "additive inverse".

Wait a minute! Could $a \in \mathbb{Z}$ have more than one additive inverse?

Theorem: Additive inverses are unique.

i.e. if $a + b_1 = 0 = a + b_2$ then $b_1 = b_2$.

Proof: Suppose that a has two additive inverses, say $a + b_1 = 0 = a + b_2$.

Then we have

$$
\begin{aligned}
b_1 &= 0 + b_1 && \text{(A3)} \\
&= b_1 + 0 && \text{(A1)} \\
&= b_1 + (a + b_2) && \text{assumption} \\
&= (b_1 + a) + b_2 && \text{(A2)} \\
&= (a + b_1) + b_2 && \text{(A1)} \\
&= 0 + b_2 && \text{assumption} \\
&= b_2 && \text{(A3)}
\end{aligned}
$$

Definition: Given $a \in \mathbb{Z}$, let "$-a$" denote the unique additive inverse.

$$a + x = 0 \iff x = -a$$

This allows us to define the operation of subtraction. For all $a, b \in \mathbb{Z}$ let

"$a - b$" $:= a + (-b)$

(a + the additive inverse of b)

The axioms didn't tell us about subtraction... so what are its properties?

Theorem: $\forall\, a, b, c \in \mathbb{Z}$ we have

- $a(b-c) = ab - ac$
- $-ab = (-a)b = a(-b)$
- $ab = (-a)(-b)$

Proof: You will prove this on HW 3 //

So we can add, subtract and multiply.

Q: what about division?

Claim: $\nexists\, n \in \mathbb{Z}$ such that $2n = 1$.

Hence 1 cannot be divided by 2.

Proof: This is harder than it looks.
It requires the Well-Ordering Axiom.

(Postponed)

Definition: Let $a, b \in \mathbb{Z}$.

We say that "a divides b" and we write $a \mid b$ if

$$\exists\, q \in \mathbb{Z} \text{ such that } b = qa.$$

Example: $2 \mid 4$ $(4 = (2) \cdot 2)$

$2 \mid 2$ $(2 = (1) \cdot 2)$

$2 \nmid 1$ (by the above claim).

$\forall\, a \in \mathbb{Z}$, $1 \mid a$ $\quad (a = (a \cdot 1))$

$\forall\, a \in \mathbb{Z}$, $a \mid 0$ $\quad (0 = (0 \cdot a))$

$\forall\, 0 \neq a \in \mathbb{Z}$, $0 \nmid a$ because

$a = q \cdot 0 \implies a = 0$.

Q: How can we prove that $2 \nmid 1$?

We use "Division with Remainder".

Theorem (2.12 in the text):

Given $a, b \in \mathbb{Z}$ with $b > 0$ we have

① $\exists\, q, r \in \mathbb{Z}$ such that

$a = qb + r$ and $0 \leq r < b$

"quotient" "remainder"

(2) The quotient and remainder are UNIQUE. That is, if we have

$a = q_1 b + r_1$ with $0 \leq r_1 < b$

and $a = q_2 b + r_2$ with $0 \leq r_2 < b$,

it follows that $q_1 = q_2$ and $r_1 = r_2$ //

Proof Postponed.

Application: $2 \nmid 1$.

Proof: Suppose for contradiction that $2 \mid 1$, i.e., $\exists\, q \in \mathbb{Z}$ such that $1 = 2q$.

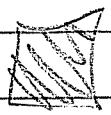
But then we have

$1 = q \cdot 2 + 0$ with $0 \leq 0 < 2$

and $1 = 0 \cdot 2 + 1$ with $0 \leq 1 < 2$

So Theorem 2.12 implies $0 = 1$.

Contradiction



Theorem 2.12 is called the

"Division Algorithm"

Example: Divide 15 by 6.

$15 = 2 \cdot 6 + 3$ ✓

$15 = 3 \cdot 6 - 3$ ×.

We require the remainder to satisfy

$$0 \leq r < 6$$

otherwise we don't call it the remainder

If the remainder satisfies $0 \leq r < 6$ then it exists and is unique

How to prove it ?

Wed Sept 25

HW 2 due Fri (Fix Hint.)
Exam 1 next Fri Oct 4
O.H. Mon 2-3
Today 3-4

Today: The Division Algorithm.

Theorem (2.12 in the text):

Given integers $a, b \in \mathbb{Z}$ with $b \neq 0$,

(1) $\exists\, q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|$$

(2) This q, r are UNIQUE, called "the" quotient and "the" remainder of a by b.

Before we prove this, what does it say?

Divide 14 by 6. ($q = 2, r = 2$)

$$14 = 3 \cdot 6 - 4 \quad \times$$
$$= 2 \cdot 6 + 2 \quad \checkmark \quad 0 \leq 2 < |6|$$
$$= 1 \cdot 6 + 8 \quad \times$$

Divide -14 by 6 $(q=-3, r=4)$

$$-14 = -4\cdot 6 + 10 \quad \times$$
$$= -3\cdot 6 + 4 \quad \checkmark \quad 0 \le 4 < |6|$$
$$= -2\cdot 6 - 2 \quad \times$$
$$= -1\cdot 6 - 8 \quad \times$$

Divide 14 by -6 $(q=\ ,\ r\ )$

$$14 = (-4)(-6) - 10 \quad \times$$
$$= (-3)(-6) - 4 \quad \times$$
$$= (-2)(-6) + 2 \quad \checkmark \quad 0 \le 2 < |-6|$$
$$= (-1)(-6) + 8 \quad \times$$

Application of the Division Algorithm:

Every number is either <u>even</u> or <u>odd</u>, not both. (even XOR odd).

<u>Proof</u>: Given $n \in \mathbb{Z}$, divide it by 2 to get

$$n = q2 + r \quad \text{with} \quad 0 \le r < 2$$

If $r = 0$ we say n is even.
If $r = 1$ we say n is odd.

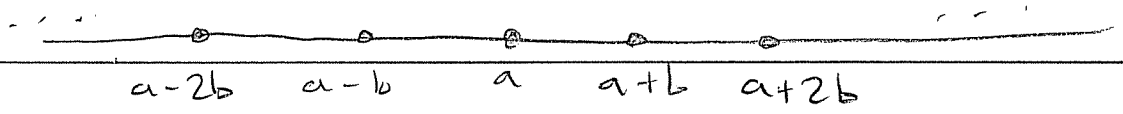
Corollary: $2 \nmid 1$ (i.e. 1 is not even).

Proof: $1 = 0 \cdot 2 + 1$
The remainder is not zero!

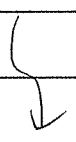
Now let's prove the Division Theorem:

Consider $a, b \in \mathbb{Z}$ with $b \neq 0$.
Easy to find $q, r \in \mathbb{Z}$ with $a = qb + r$,
but can we do it with $0 \leq r < |b|$?

Let $S = \{ a - qb : q \in \mathbb{Z} \}$



Let $S^+ = \{ n \in S : n \geq 0 \}$ be the non-negative elements of S



Since $S^+ \subseteq \mathbb{N}$ and $S^+ \neq \emptyset$ (why?) The Well-Ordering Axiom says S^+ has a smallest element.

Call it $r \in S^+$.

By definition of S, $r = a - qb$ for some q.

$$a = qb + r.$$

Check that $0 \leq r < |b|$. Suppose not, i.e. suppose $r \geq |b|$. Then we have

$$r - |b| \geq |b| - |b| = 0$$

and $r - |b| = a - qb - |b| = a - (q \pm 1)b$

hence $r - |b| \in S^+$. But $r - |b| < r$ contradicts the fact that r is the smallest element of S^+.

We conclude that $a = qb + r$ with $0 \leq r < |b|$. ☺

"q, r EXIST".

But are they UNIQUE?

Suppose that

$$\left.\begin{array}{l} a = q_1 b + r_1 \\ 0 \le r_1 < |b| \end{array}\right\} \text{ and } \left.\begin{array}{l} a = q_2 b + r_2 \\ 0 \le r_2 < |b|. \end{array}\right\}$$

We claim that $q_1 = q_2$ and $r_1 = r_2$.

Suppose NOT, i.e suppose that $r_1 \neq r_2$, say $r_1 < r_2$. Then we have

$$(*) \quad 0 = r_1 - r_1 < r_2 - r_1 \le r_2 < |b|$$

But $q_1 b + r_1 = a = q_2 b + r_2$.

$$\Longrightarrow \quad q_1 b - q_2 b = r_2 - r_1$$
$$\Longrightarrow \quad (q_1 - q_2) b = (r_2 - r_1)$$
$$\Longrightarrow \quad b \mid (r_2 - r_1).$$

By HW 2.2(b) this implies

$$|b| \le |r_2 - r_1| = r_2 - r_1.$$

Contradicting $(*)$.

Hence $r_1 = r_2$ and.

$$(q_1 - q_2)b = r_2 - r_1 = 0.$$

Since $b \neq 0$ we get $q_1 - q_2 = 0$

$$q_1 = q_2$$

That's a real theorem!

Fri Sept 27

HW 2 due Now

Exam 1 next Fri Oct 4.

- closed book
- no cheating.

(Look at last year's exam)

Today: Discuss HW 2

Important Fact:

Let n be a positive integer. Then the set $\mathbb{Z}$ breaks up into n disjoint pieces.

Let $[a]_n := \{nk + a : \text{for some } k \in \mathbb{Z}\}$

$= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$

Then we have

$$\mathbb{Z} = \underbrace{[0]_n \cup [1]_n \cup \cdots \cup [n-1]_n}$$

disjoint union "partition".

Example

$$\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3$$

"Every integer has the form

$3k+0$, or $3k+1$, or $3k+2$

for some $k \in \mathbb{Z}$."

Proof?

Given $n \in \mathbb{Z}$, divide n by 3.
The Division Algorithm says the remainder is UNIQUE.

$$\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3$$

$[0]_3$: numbers that have rem. 0 ~~when divided~~ by 3

$[1]_3$: rem. 1

$[2]_3$: rem. 2

Application: Prove that for all $n \in \mathbb{Z}$,

"$3 \mid n^2$" $\Longrightarrow$ "$3 \mid n$".

Proof: We will show the contrapositive,

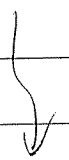
"$3 \nmid n$" $\Longrightarrow$ "$3 \nmid n^2$",

which is equivalent. So, assume that $3 \nmid n$ (i.e. n is not of the form $3k+0$ for some $k \in \mathbb{Z}$).
There are two cases:

Case 1: $n = 3k+1$ for some $k \in \mathbb{Z}$.
Then we have

$$n^2 = (3k+1)^2 = 9k^2 + 6k + 1$$
$$= 3(3k^2 + 2k) + 1,$$

which is not of the form $3(\text{something}) + 0$.
Hence $3 \nmid n^2$.



Case 2: $n = 3k+2$ for some $k \in \mathbb{Z}$.

Then we have

$$n^2 = (3k+2)^2 = 9k^2 + 12k + 4$$
$$= 9k^2 + 12k + 3 + 1$$
$$= 3(3k^2 + 4k + 1) + 1.$$

which is not $3(\text{something}) + 0$.

Hence $3 \nmid n^2$.

Recall that "$a \mid b$" is really an existence statement

"$a \mid b$" = "$\exists\, q \in \mathbb{Z},\ b = qa$"

Q: What does "$a \nmid b$" mean formally?

"$a \nmid b$" = NOT "$a \mid b$"

= "$\forall\, q \in \mathbb{Z},\ b \neq qa$"

This is a universal statement.

Logical Principle:

NOT "$\exists\, x \in S$, property $P(x)$ holds"

||

"$\forall\, x \in S$, property NOT $P(x)$ holds"

(NOT exchanges $\exists \leftrightarrow \forall$)

Exercise: Prove that $\forall\, n \in \mathbb{Z}$,

"$5 \nmid n$" $\Longrightarrow$ "$5 \nmid n^2$".

Use this to prove that $\sqrt{5}$ is <u>not</u> a fraction of integers.

Q: Is the following true?

$\forall\, n \in \mathbb{Z}$, "$12 \nmid n$" $\Longrightarrow$ "$12 \nmid n^2$"

↓

A: NO!

Because if $n = 12k + 6$ then $12 \nmid n$.

But

$$n^2 = (12k+6)^2 = 144k^2 + 144k + 36$$

$$= 12(12k^2 + 12k + 3) + 0,$$

hence $12 \mid n^2$, which is bad.

"$12 \nmid n$" $\Rightarrow$ "$12 \nmid n^2$" for some n.

T F

Oops!

We showed that

$\exists n \in \mathbb{Z}$, "$12 \nmid n$" $\not\Rightarrow$ "$12 \nmid n^2$"

which is the opposite of

$\forall n \in \mathbb{Z}$, "$12 \nmid n$" $\Rightarrow$ "$12 \nmid n^2$"

Nevertheless:

It is still true that $\sqrt{12}$ is not a fraction, but our favorite proof fails.

Problem: Find new proof.

Idea: $\sqrt{12} = \sqrt{2 \cdot 2 \cdot 3} = 4\sqrt{3}$

Mon Sept 30

Exam 1 this Friday.

Today: Discussion & Review

Problem: Prove that $\forall m, n \in \mathbb{Z}$ we have.

"(m is even OR n is even) $\Leftrightarrow$ m is even"

How?

Let P = "m is even"
Q = "n is even"
R = "mn is even"

Want to show $(P \text{ OR } Q) \Rightarrow R$

i.e. $(P \text{ OR } Q) \Rightarrow R$ ①
and $R \Rightarrow (P \text{ OR } Q)$. ②

Must prove ① & ② separately.

Proof of ①: $(P \text{ OR } Q) \Rightarrow R$.

Assume that P OR Q i.e. assume m is even or n is even.

There are three cases:

- m even, n odd $\Rightarrow$ mn even
- m odd, n even $\Rightarrow$ mn even
- m even, n even $\Rightarrow$ mn even.

Can we do it without cases? Yes.

Use a truth table to show.

"$(P \text{ OR } Q) \Rightarrow R$" $\equiv$ "$(P \Rightarrow R)$ AND $(Q \Rightarrow R)$"

To prove (1) we will prove.

$P \Rightarrow R$ i.e. m even $\Rightarrow$ mn even ✓

and

$Q \Rightarrow R$ i.e. n even $\Rightarrow$ mn even ✓

Easy.

Next try to prove (2)

$R \Rightarrow (P \text{ OR } Q)$

mn even $\Rightarrow$ (m even or n even)

So assume that mn is even.

Now what ? ....

Try the contrapositive

NOT (P OR Q) $\Rightarrow$ NOT R.

[(NOT P) AND (NOT Q)] $\Rightarrow$ NOT R.

[m odd and n odd] $\Rightarrow$ mn odd.

So assume m, n both odd. i.e.
$\exists\, k, l \in \mathbb{Z}$ such that

$m = 2k+1$ and $n = 2l+1$. Then

$$mn = (2k+1)(2l+1) = 4kl + 2k + 2l + 1$$
$$= 2(2kl + k + l) + 1$$

is odd. ✓ Done.

Another proof of (2):

Use a truth table to show that

"$R \Rightarrow (P \text{ OR } Q)$" $\equiv$ "$(R \text{ AND NOT } P) \Rightarrow Q$".

i.e. (mn even and m odd) $\Rightarrow$ n even.

Proof: Assume mn is even and m is odd. Assume (for contradiction) that n is odd. Then we have

m odd AND n odd $\Rightarrow$ mn odd,

which contradicts the fact that mn is even.

Problem: Prove that 3^n is odd for all integers $n \geq 1$.

HOW?

$3 = 2 \cdot 1 + 1$ is odd.

$3^2 = 9 = 2 \cdot 4 + 1$ is odd.

$3^3 = 27 = 2 \cdot 13 + 1$ is odd.

$3^4 = ? = 3 \cdot 3^3$

$= (\text{odd})(\text{odd}) = \text{odd}$ ✓

I can't go on forever.

Try an indirect proof:

Assume for contradiction that 3^n is even for some $n \geq 1$

"$\exists\, n \geq 1$, 3^n is even"

↯

[Recall

"NOT ($\forall n \geq 1$, 3^n is odd)"

$=$ "$\exists\, n \geq 1$, 3^n is even"]

Let $S = \{ n \in \mathbb{N} : n \geq 1,\ 3^n \text{ even} \}$.

By assumption $S \neq \emptyset$ so by well-ordering, S has a smallest element. Call it $m \in S$

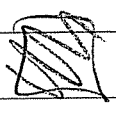
i.e. 3^m is even
3^{m-1} is odd.

But then

$$3^m = 3 \cdot 3^{m-1}$$
$$= (\text{odd})(\text{odd}) = \text{odd}.$$

Contradiction!

$\Rightarrow$ 3^n is odd $\forall n \geq 1$



Wed Oct 2

Exam 1 Friday In Class
- closed book / phone / etc.
- no cheating

Today: Review.

- We are interested in proving theorems.
- To prove anything one must first have

Definitions & Axioms

to work with
- We use tools of logic to deduce theorems from the definitions and axioms.

- The original axioms (Euclid, ~300 BC) talked about points, lines & circles.

- Modern axioms talk about sets and numbers ($\mathbb{N}$, $\mathbb{Z}$, etc.)

↓

In practice, we don't reduce theorems all the way to the axioms;

we just try to convince the audience (and ourselves) that we could if we wanted to (and had enough time).

Topics:

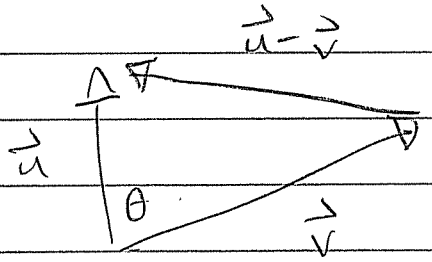
1. Geometry
2. Logic
3. Numbers

(1) Modern geometry is based on Cartesian coordinates and the dot product

$$\vec{u} \cdot \vec{v} = (u_1, u_2, \ldots, u_n) \cdot (v_1, v_2, \ldots, v_n)$$

$$:= u_1 v_1 + u_2 v_2 + \cdots + u_n v_n.$$

Given two vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$ consider the triangle:



Theorem:

$$\vec{u} \cdot \vec{v} = \|\vec{u}\| \cdot \|\vec{v}\| \cos\theta$$

Proof: Use algebra to show

(*) $$\|\vec{u}-\vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2 - 2(\vec{u} \cdot \vec{v})$$

Now use the law of Cosines. ///

Corollary: We have

$$\vec{u} \perp \vec{v} \iff \vec{u} \cdot \vec{v} = 0.$$

(i.e. $\theta = 90^\circ$)

[The Corollary is equivalent to the Pythagorean Theorem and its converse.]

Proof of Corollary:

First we show $\vec{u} \perp \vec{v} \Rightarrow \vec{u} \cdot \vec{v} = 0$.

So assume $\vec{u} \perp \vec{v}$, i.e. $\theta = 90^\circ$. Then Pythagoras says $\|\vec{u} - \vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2$. Then (*) implies $\vec{u} \cdot \vec{v} = 0$.

Next we show $\vec{u} \cdot \vec{v} = 0 \Rightarrow \vec{u} \perp \vec{v}$.

So assume $\vec{u} \cdot \vec{v} = 0$. Then (*) says $\|\vec{u} - \vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2$. Then the converse of Pythagoras says $\vec{u} \perp \vec{v}$.

(2) Logic.

Basic Operations

AND, OR, NOT, $\Rightarrow$

Let's show that

"NOT $(P \Rightarrow Q)$" $\equiv$ "P AND NOT Q"

Proof:

P	Q	NOT Q	P AND NOT Q	$P \Rightarrow Q$	NOT $(P \Rightarrow Q)$
T	T	F	F	T	F
T	F	T	T	F	T
F	T	F	F	T	F
F	F	T	F	T	F

///

Useful facts.

- "$P \Leftrightarrow Q$" $\equiv$ "$(P \Rightarrow Q)$ AND $(Q \Rightarrow P)$"
- "NOT (P OR Q)" $\equiv$ "NOT P AND NOT Q"
  "NOT (P AND Q)" $\equiv$ "NOT P OR NOT Q".

- "$P \Rightarrow Q$" $\equiv$ "NOT $Q \Rightarrow$ NOT P".

Disprove the statement

$$\forall x \in \mathbb{R},\ x^2 > 0 \Rightarrow x > 0.$$

i.e. Prove the statement

$$\text{NOT}\left(\forall x \in \mathbb{R},\ x^2 > 0 \Rightarrow x > 0\right)$$

$$\equiv \exists x \in \mathbb{R},\ \text{NOT}(x^2 > 0 \Rightarrow x > 0)$$

$$\equiv \exists x \in \mathbb{R},\ x^2 > 0 \text{ AND } x \leq 0.$$

To prove $\exists$ it is sufficient to give one example.

Let $x = -1$. Then

$$(-1)^2 = +1 > 0 \text{ AND } -1 \leq 0$$

(3) Numbers.

Theorem (The Division Algorithm):

$\forall a, b \in \mathbb{Z}$ with $b \neq 0$.

- $\exists q, r \in \mathbb{Z}$ with
  - $a = qb + r$
  - $0 \leq r < |b|$.

- These q, r are unique, i.e. if

$a = q_1 b + r_1$ and $a = q_2 b + r_2$
$0 \leq r_1 < |b|$ $0 \leq r_2 < |b|$

Then $q_1 = q_2$ and $r_1 = r_2$

=

Know what it says.
Know how to use it.

Example: Prove that $2 \nmid 1$. i.e.

$\forall q \in \mathbb{Z}, \quad 1 \neq 2q$.

Proof: Assume for contradiction that $\exists q \in \mathbb{Z}$ with $1 = 2q$.

Then we have

$1 = 2q + 0$ and $1 = 2 \cdot 0 + 1$

$0 \leq 0 < |2|$ $\qquad$ $0 \leq 1 < |2|$

So the Division Algo. $\Rightarrow 0 = 1$.

Contradiction

Warning:

Avoid the notation a/b when you are trying to talk about integers $\mathbb{Z}$.

Good Reason: We never defined a/b.