7/21/14

Quiz 3 now (20 minutes)

OK, let's go back to logic

We're discussed how logic is encoded by computers. Now we'll discuss how logic is used by humans.

Humans use logic for arguments/proofs, and the most important symbol in a proof is "$\Rightarrow$".

Here's the truth table

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

When we read it we say

"$P \Rightarrow Q$" = "if P then Q"
= "P implies Q"

You might worry that $F \Rightarrow F = T$. In other words, "if $1+1=3$ then $1+1=5$" is a true statement.

But don't worry. The truth table of $\Rightarrow$ is NOT THE POINT!

Here's the point:

> T flows along $\Rightarrow$

So, this is OK

$$F \Rightarrow F \Rightarrow T \Rightarrow T \Rightarrow T \quad \checkmark$$

This is OK

$$F \Rightarrow F \Rightarrow F \Rightarrow F \Rightarrow F \quad \checkmark$$

But this is NOT OK

$$T \Rightarrow T \Rightarrow \textcircled{T} \Rightarrow F \Rightarrow F$$

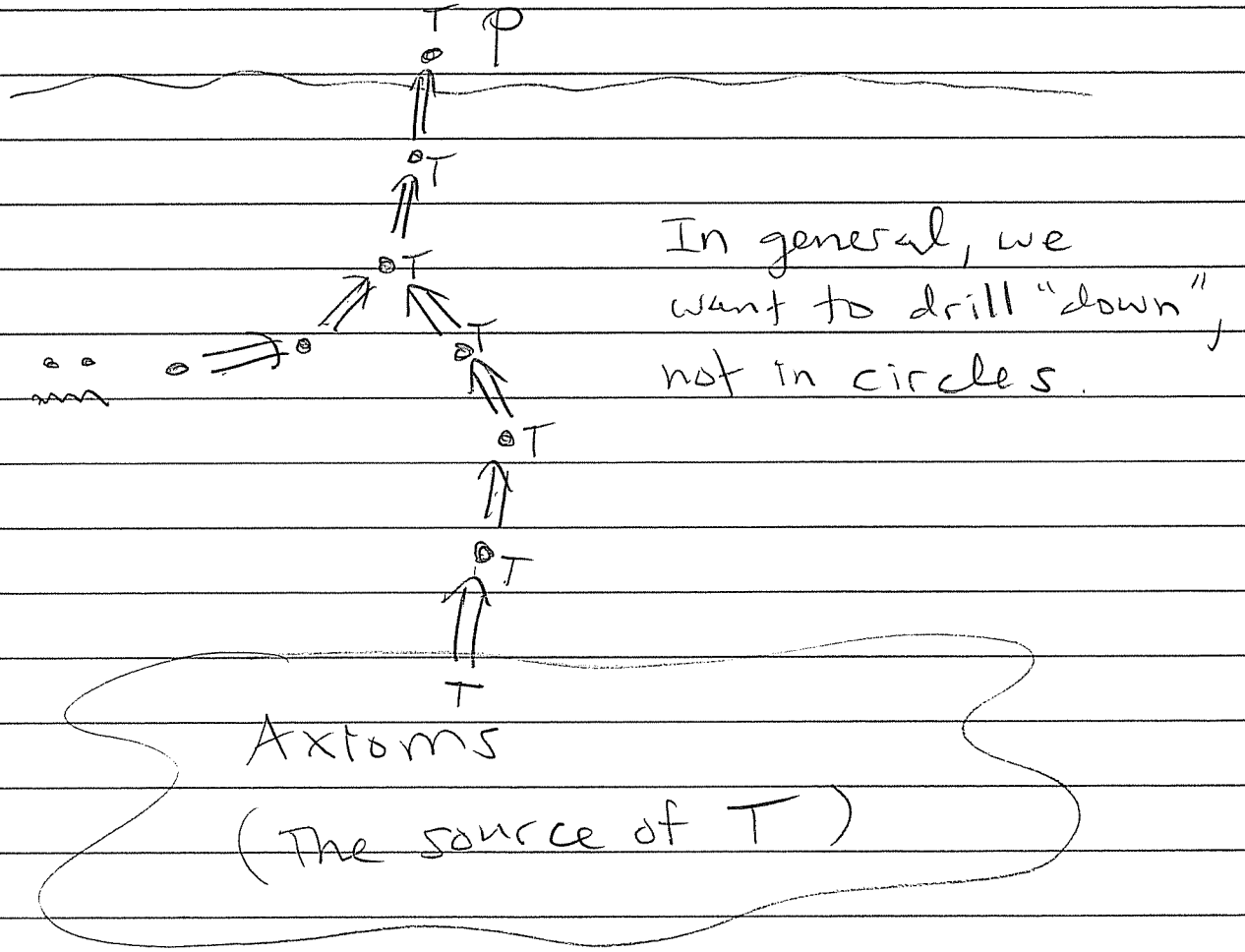
↑

This T is not flowing properly.

What does it mean to prove a mathematical statement P?

It's like drilling a well. We construct a chain of arrows backwards from P until we hit the axioms. Then T flows up!

Picture



The first formal use of proof was in ancient Greece (Thales ⇝ Pythagoras ⇝ Euclid)
The first theory of human argument was written down by Aristotle:

Example: "Syllogism"

All men are mortal	Premise 1
Socrates is a man	Premise 2
∴ Socrates is mortal	Conclusion

∴ = "Therefore"

Aristotle considered this argument self-evidently valid. We can "prove" this with a truth table.

Let P = "x is socrates"
Q = "x is a man"
R = "x is mortal".

The argument is

$$\begin{array}{l} Q \Rightarrow R \\ P \Rightarrow Q \\ \hline \therefore\ P \Rightarrow R \end{array}$$

Here is a truth table

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$P \Rightarrow R$	
T	T	T	T	T	T	✓
T	T	F	T	F	F	
T	F	T	F	T	T	
T	F	F	F	T	F	
F	T	T	T	T	T	✓
F	T	F	T	F	T	
F	F	T	T	T	T	✓
F	F	F	T	T	T	✓

If the premises are T then the conclusion is T, so the argument is valid.

We can say this formally as follows.

For all values $P, Q, R \in \{T, F\}$ we have

$$(((Q \Rightarrow R) \wedge (P \Rightarrow Q)) \Rightarrow (P \Rightarrow R)) = T.$$

"if $Q \Rightarrow R$ and $P \Rightarrow Q$ then $P \Rightarrow R$".

In general an (Aristotelian) argument looks like

P_1	Premise 1
P_2	Premise 2
$\vdots$	$\vdots$
P_k	Premise k
$\therefore Q$	$\therefore$ Conclusion

We say the argument is valid if for all Boolean inputs we have

$$((P_1 \wedge P_2 \wedge \cdots \wedge P_k) \Rightarrow Q) = T$$

Example: "Modus Ponens"

$P \Rightarrow Q$	If today is Monday I will teach 309.
P	Today is Monday
$\therefore Q$	$\therefore$ I will teach 309.

VALID?

We analyze the statement $((P \Rightarrow Q) \wedge P) \Rightarrow Q$

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge P$	$((P \Rightarrow Q) \wedge P) \Rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

The argument is valid.

Another Example: "Modus Tollens"

$P \Rightarrow Q$ Every dog has hair

$\neg Q$ x has no hair

$\neg P$ x is not a dog

VALID?

We analyze $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$.

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge \neg Q$	$((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

VALID ✓

"Modus Tollens" is related to an important principle of logic.

☆ The Principle of Contrapositive.

For all statements P, Q we have

$$\text{"}P \Rightarrow Q\text{"} = \text{"}\neg Q \Rightarrow \neg P\text{"}$$

↑ logically equivalent

Proof: Look at the truth table

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

same. same

Note that "$P \Rightarrow Q$" = "$\neg Q \Rightarrow \neg P$"

but "$P \Rightarrow Q$" $\neq$ "$Q \Rightarrow P$"

Here's an argument from Lewis Carroll:

Babies are illogical
Nobody is despised who can manage a crocodile.
Illogical persons are despised.
Therefore, babies cannot manage crocodiles.

VALID?

Let P = "x is a baby"
Q = "x is illogical"
R = "x can manage a crocodile"
S = "x is despised".

The argument is

$$P \Rightarrow Q$$
$$R \Rightarrow \neg S$$
$$Q \Rightarrow S$$
$$\therefore P \Rightarrow \neg R$$

We can replace $R \Rightarrow \neg S$ by its equivalent contrapositive $S \Rightarrow \neg R$.

to get $P \Rightarrow Q$

$S \Rightarrow \neg R$

$Q \Rightarrow S$

$\therefore P \Rightarrow \neg R$

We can rearrange the order of the premises to get

$P \Rightarrow Q$

$Q \Rightarrow S$

$S \Rightarrow \neg R$

$\therefore P \Rightarrow \neg R$

This is valid. It is just two "syllogisms" put together. The generalized syllogism

$P_1 \Rightarrow P_2$

$P_2 \Rightarrow P_3$

$\vdots$

$P_{k-1} \Rightarrow P_k$

$\therefore P_1 \Rightarrow P_k$

is valid. It is sometimes called a "sorites", or a "polysyllogism". It is proved by induction.

Q: Do you like the word "polysyllogism"?

7/22/14

HW Posted today after class
- due Friday
Quiz 4 next Monday

Today: More about "$\Rightarrow$".

Recall the truth table

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

The disjunctive normal form is

"$P \Rightarrow Q$" = "$(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$"

but this is not very nice. Instead look at $\neg$"$P \Rightarrow Q$" = "$P \not\Rightarrow Q$"

P	Q	$P \not\Rightarrow Q$
T	T	F
T	F	T
F	T	F
F	F	F

The disjunctive normal form is

$$\text{“}P \not\Rightarrow Q\text{”} = \text{“}P \wedge \neg Q\text{”}$$

and this is nice. Then using de Morgan we have

$$\begin{aligned}\text{“}P \Rightarrow Q\text{”} &= \neg \text{“}P \not\Rightarrow Q\text{”} \\ &= \neg(P \wedge \neg Q) \\ &= \neg P \vee \neg\neg Q \\ &= \neg P \vee Q.\end{aligned}$$

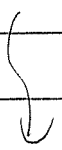
This can be useful:

$$\boxed{\text{“}P \Rightarrow Q\text{”} = \text{“}\neg P \vee Q\text{”}}$$

For example, we can use it to demonstrate the

☆ Principle of Contraposition:

$$\boxed{\text{“}P \Rightarrow Q\text{”} = \text{“}\neg Q \Rightarrow \neg P\text{”}}$$



Proof: "$P \Rightarrow Q$" = "$\neg P \vee Q$"
= "$Q \vee \neg P$"
= "$\neg(\neg Q) \vee (\neg P)$"
= "$\neg Q \Rightarrow \neg P$"

Q: What is the contrapositive in the language of set theory?

Recall the "dictionary"

$A \cup B = \{x \in U : x \in A \text{ OR } x \in B\}$
$A \cap B = \{x \in U : x \in A \text{ AND } x \in B\}$
$A^c = \{x \in U : \text{NOT } x \in A\}$

Now we have one more

"$A \subseteq B$" = "$x \in A \Rightarrow x \in B$"
(if $x \in A$ then $x \in B$)

The contrapositive says

"$A \subseteq B$" = "$x \in A \Rightarrow x \in B$"
= "$x \notin B \Rightarrow x \notin A$"
= "$x \in B^c \Rightarrow x \in A^c$"
= "$B^c \subseteq A^c$"

In summary:

The Contrapositive for Sets says

$$\text{"}A \subseteq B\text{"} = \text{"}B^c \subseteq A^c\text{"}$$

Recall how we define equality of sets:

$$\text{"}A = B\text{"} = \text{"}A \subseteq B \text{ AND } B \subseteq A\text{"}$$
$$= \text{"}x \in A \Rightarrow x \in B \text{ AND } x \in B \Rightarrow x \in A\text{"}$$

We have a name for this operation:

Given $P, Q \in \{T, F\}$ we define

$$\text{"}P \Leftrightarrow Q\text{"} := \text{"}P \Rightarrow Q \text{ AND } Q \Rightarrow P\text{"}$$
$$(P \Leftrightarrow Q) := (P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

Truth table

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

So $\iff$ acts like an equals sign.
We call it logical equivalence.

We often say

"$P \iff Q$" = "P if and only if Q"

based on the old-fashioned uses

"$Q \Rightarrow P$" = "P if Q"
"$P \Rightarrow Q$" = "P only if Q"

Finally, we can say this:

"$A = B$" = "$x \in A \iff x \in B$"
= "$x \in A$ if and only if $x \in B$"

We have now seen all the logic we will ever need.

Q: How is logic used in mathematics?

First we need a bit of math to work with.
Recall the set of integers

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

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

"Was sind und was sollen die Zahen?"
Richard Dedekind, 1888.

Given $n \in \mathbb{Z}$ we say that n is even if there exists $k \in \mathbb{Z}$ such that $n = 2k$.

"n is even" := "$\exists k,\ n = 2k$"

Otherwise we say that n is odd.

"n is odd" := $\neg$ "n is even"
= $\neg$ "$\exists k \in \mathbb{Z},\ n = 2k$"
= "$\forall k \in \mathbb{Z},\ n \neq 2k$".

$\wr$

Maybe there is a nicer way to say that n is odd? Yes, in fact we have

"n is odd" = "$\exists k \in \mathbb{Z}, n = 2k+1$"

but we won't prove this today. (Thinking Problem: How could we possibly prove this? We would need a formal definition of the integers, which we don't have yet.)

Let's just assume it for now.

Problem: Given $m, n \in \mathbb{Z}$, prove that

"if mn is even then m is even or n is even."

First attempt at proof:

If mn is even then $\exists k \in \mathbb{Z}$ such that $mn = 2k$. We want to show that $\exists a \in \mathbb{Z}$ such that $m = 2a$, or $\exists b \in \mathbb{Z}$ such that $n = 2b$, or both.

Where would this a or b come from?

First attempt fails.

Second attempt at proof:

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

We want to prove that

$$P \Rightarrow (Q \vee R).$$

Does this help? Maybe we can use Boolean algebra to put this in a more convenient form...

Let's try the contrapositive:

"$P \Rightarrow (Q \vee R)$" = "$\neg(Q \vee R) \Rightarrow \neg P$"
= "$(\neg Q \wedge \neg R) \Rightarrow \neg P$"

= "if m and n are both odd, then the product mn is odd"

Let's try to prove that.

If m and n are both odd, then there exist $k, l \in \mathbb{Z}$ such that

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

Then the product is

$$\begin{aligned} mn &= (2k+1)(2l+1) \\ &= 4kl + 2k + 2l + 1 \\ &= 2(2kl + k + l) + 1. \end{aligned}$$

Hence $\exists z \in \mathbb{Z}$ (in particular, $z = 2kl + k + l$) such that $mn = 2z + 1$.

We conclude that mn is odd, as desired.

Done.

Second attempt succeeded. :)

Now let's write it up nicely.

Theorem: Given $m, n \in \mathbb{Z}$ we have that

if mn is even then m or n is even.

Proof: We will show the contrapositive statement. That is, we will show that if m and n are both odd, then mn is odd.

So assume that $m = 2k+1$ and $n = 2\ell+1$. Then the product is

$$\begin{aligned} mn &= (2k+1)(2\ell+1) \\ &= 4k\ell + 2k + 2\ell + 1 \\ &= 2(2k\ell + k + \ell) + 1, \end{aligned}$$

wich is odd.

Q.E.D.

□

///

or whatever victory symbol you like.

We use logic in mathematics to be clear about what exactly we are proving, and to express it in the most convenient way.

Epilogue: Given $n \in \mathbb{Z}$, why is it true that

"$\forall k \in \mathbb{Z}, n = 2k$" = "$\exists \ell \in \mathbb{Z}, n = 2\ell + 1$"

??

This has nothing to do with logic. It is a special fact about the integers called the Division Theorem.

✡ The Division Theorem:

Given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist integers $q, r \in \mathbb{Z}$ such that

- $a = qb + r$
- $0 \leq r < |b|$

This q, r are called the "quotient" and "remainder" when a is divided by b. ∎

They are unique in the sense that if

$$a = q_1 b + r_1 \quad \text{and} \quad a = q_2 b + r_2$$
$$0 \leq r_1 < |b| \qquad 0 \leq r_2 < |b|,$$

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

Proof postponed ☹

As a consequence of the Division Theorem, we see that every integer $n \in \mathbb{Z}$ has the form $n = 2k$ or $n = 2k+1$ for some $k \in \mathbb{Z}$.

Proof: Given $n \in \mathbb{Z}$, we can divide it by 2 to get

$$n = 2q + r$$
$$0 \leq r < 2 \quad (r = 0 \text{ or } r = 1)$$

If $r = 0$ we say n is even. If $r = 1$ we say n is odd. Note that this expression is unique (i.e. it is not possible for n to be both even and odd.) ///

7/23/14

HW 4 due Friday
Quiz 4 on Monday

Last time we discussed how logic is used in mathematics.

As an example we considered "number theory", which is the study of the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

We have not yet seen a formal definition of $\mathbb{Z}$ but we tried to do some things.

For example, given $n \in \mathbb{Z}$ we defined

"n is even" := "$\exists k \in \mathbb{Z}, n = 2k$"

and then we tried to prove that

"mn is even" $\Rightarrow$ "m is even" OR "n is even"

To do this we needed the fact that

$\neg$ "n is even" = "$\exists k \in \mathbb{Z},\ n = 2k+1$"

But we did not prove this. No logical proof can be given because this is a special property of $\mathbb{Z}$.

It follows from

✡ The Division Theorem:

Given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist $q, r \in \mathbb{Z}$ such that

- $a = qb + r$
- $0 \leq r < |b|$.

Furthermore, these q, r are unique in the sense that if

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

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

//

This theorem is the FOUNDATION of number theory. I will show you the traditional proof, and maybe this will suggest what the formal definition of $\mathbb{Z}$ should be....

☆ Traditional Proof of the Div. Theorem:

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We want to somehow find $q, r \in \mathbb{Z}$ with the desired properties.

Here's the trick. Consider the set

$$S = \{a - kb : k \in \mathbb{Z}\}$$
$$= \{\ldots, a-2b, a-b, a, a+b, a+2b, \ldots\}$$

Since $b \neq 0$ this set contains both negative and positive numbers. Let

$$S^+ = \{x \in S : x \geq 0\} \subseteq S$$

Since $S^+ \neq \emptyset$, it contains a smallest element. Call this smallest element

$$r \in S^+.$$

Since $r \in S$ we know that there exists $k \in \mathbb{Z}$ such that

$$r = a - kb$$

Why don't we just call this $k = q$?
Then we have

$$a - qb = r$$
$$a = qb + r.$$

Good. But we still need to show that $0 \leq r < |b|$. Since $r \in S^+$ by definition we know that $0 \leq r$. If $r = 0$ we're done, so suppose that we have $0 < r$.

Now we want to show that

$$r < |b|$$

In other words, we want to show that $r \geq |b|$ is impossible.

↓

To demonstrate that $r \geq |b|$ is impossible we will show that it leads to a CONTRADICTION. If $r \geq |b|$ then subtracting $|b|$ from both sides gives

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

But note that

depending if b is positive or negative

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

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

$= a - (\text{something})b$

and $r - |b| \geq 0$

we conclude that $r - |b|$ is an element of the set S^+. But note that

$$-|b| < 0$$
$$r - |b| < r.$$

(We added r to both sides of $-|b| < 0$.)

Didn't we define define r as the smallest element of S^+?

Yes we did. So we have reached the desired CONTRADICTION.

We conclude that $r \geq |b|$ is impossible and hence we have

$$0 \leq r < |b|$$

as desired.

[Remark: This is already enough to prove that if $n \in \mathbb{Z}$ is not even then $n = 2k+1$ for some $k \in \mathbb{Z}$.

Indeed, suppose $n \in \mathbb{Z}$ is not even. By the above proof $\exists\, q, r \in \mathbb{Z}$ such that

$$n = 2q + r$$
$$\text{and} \quad 0 \leq r < 2 \quad (\text{i.e. } r = 0 \text{ or } 1).$$

Since n is not even we know that $r \neq 0$. Hence $r = 1$ and we have $n = 2q + 1$.]

We have shown that $\exists\, q, r \in \mathbb{Z}$ with the desired properties, but we still need to show that they are UNIQUE.

So suppose that we have

$$a = q_1 b + r_1 \quad \text{and} \quad a = q_2 b + r_2$$
$$0 \le r_1 < |b| \qquad 0 \le r_2 < |b|.$$

In this case we want to prove that

$$q_1 = q_2 \quad \text{and} \quad r_1 = r_2.$$

First we will show that $r_1 \neq r_2$ is impossible. Indeed, if $r_1 \neq r_2$ (let's say $r_1 < r_2$) then we have

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

[Here we used the facts

$$r_1 < r_2 \implies r_1 - r_1 < r_2 - r_1$$

and $$-r_1 \le 0 \implies r_2 - r_1 \le r_2.$$]

But since $a = q_1 b + r_1$ and $a = q_2 b + r_2$ we have

$$\begin{aligned} q_1 b + r_1 &= q_2 b + r_2 \\ q_1 b - q_2 b &= r_2 - r_1 \\ (q_1 - q_2) b &= (r_2 - r_1) \end{aligned}$$

Since $r_2 - r_1 \neq 0$ and $b \neq 0$ we know that $q_1 - q_2 \neq 0$. Since $q_1 - q_2$ is an integer (i.e. a "whole number"), this implies that

$$\begin{aligned} 1 &\leq |q_1 - q_2| \\ |b| &\leq |q_1 - q_2| \cdot |b| \\ |b| &\leq |(q_1 - q_2) b| \\ |b| &\leq |r_2 - r_1| \\ |b| &\leq r_2 - r_1 . \end{aligned}$$

But this CONTRADICTS the fact that $r_2 - r_1 < |b|$, which we know from (*).

This contradiction shows that $r_1 \neq r_2$ is impossible, and hence $r_1 = r_2$, as desired.

Finally, we have

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

Since $b \neq 0$, this implies that

$$q_1 - q_2 = 0$$
$$q_1 = q_2.$$

We are done. ///

wow. That was a real theorem!

To know what the integers are, we should take careful account of all of the properties that we used in the proof.

Here are the properties I think we used . . . . .

Properties of Addition:

$$a + b = b + a$$

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

$$a + 0 = a$$

$$\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, \; a + b = 0 \quad (\text{"subtraction"})$$

Properties of Multiplication:

$$ab = ba$$

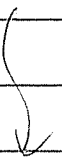
$$a(bc) = (ab)c$$

$$a1 = a$$

(there is no property of "division", but we did use the property of "cancellation". That is, if $ab = ac$ and $a \neq 0$, then $b = c$)

Property of Distribution:

$$a(b + c) = ab + ac.$$



Properties of Order:

$0 < 1$ (meaning $0 \leq 1$ and $0 \neq 1$)

$a \leq b \implies a + c \leq b + c$

$a \leq b$ and $0 \leq c \implies ac \leq bc$

.... Did we think of everything?

NO. Because the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ also satisfy all of these properties.

What is it about $\mathbb{Z}$ that distinguishes it from, say, $\mathbb{Q}$ and $\mathbb{R}$?

This one puzzled people for a long time.

Stay tuned!

7/24/14

HW 4 due tomorrow
Quiz 4 on Monday

Q: Was sind und was sollen die Zahlen?
(What are numbers and what should they be?)

Last time we discussed.

☆ The Division Theorem:

$\forall a, b \in \mathbb{Z}$ with $b \neq 0$, $\exists!\ q, r \in \mathbb{Z}$ such that

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

[Remark: $\exists!$ means "there exist unique"]

This is the true foundation of number theory. Any potential formal definition of $\mathbb{Z}$ should make it true.

Last time I showed you the standard proof of the Div. Thm. and we scoured it to see what properties $\mathbb{Z}$ should have.

Here we are following in the footsteps of Richard Dedekind (1831–1916). I'll encapsulate his ideas in a

Friendly Definition of $\mathbb{Z}$

$\mathbb{Z}$ is a set equipped with

- an equivalence relation "$=$"
  - $\forall a \in \mathbb{Z}$, $a = a$,
  - $\forall a, b \in \mathbb{Z}$, $a = b \Rightarrow b = a$,
  - $\forall a, b, c \in \mathbb{Z}$, $a = b$ and $b = c \Rightarrow a = c$.
- a total ordering "$\leq$"
  - $\forall a, b \in \mathbb{Z}$, $a \leq b$ and $b \leq a \Rightarrow a = b$,
  - $\forall a, b, c \in \mathbb{Z}$, $a \leq b$ and $b \leq c \Rightarrow a \leq c$,
  - $\forall a, b \in \mathbb{Z}$, $a \leq b$ or $b \leq a$.
- two binary operations
  - $+ : \mathbb{Z}^2 \to \mathbb{Z}$
  - $\times : \mathbb{Z}^2 \to \mathbb{Z}$
- two special elements $0, 1 \in \mathbb{Z}$

satisfying approximately twelve axioms.

(See the handout.)

Eleven of the axioms are fairly obvious, but there is one axiom that is fairly subtle. It took a long time for people to realize that this is an axiom and not a theorem.

★ Axiom of Well-Ordering:

Every non-empty set of positive (or non-negative; it's not important) integers has a smallest element.

Formally: $\forall\, X \subseteq \mathbb{N}$ such that $X \neq \emptyset$, $\exists\, x \in X$ such that $\forall\, y \in X,\ x \leq y$.

[Remark: While the first 11 axioms are "algebraic", the well-ordering property is "logical" in nature.]

Yes, indeed, we needed well-ordering in our proof of the Division Theorem (look back and see).

Now our definition of $\mathbb{Z}$ is complete. ///

Dedekind did this in 1888.
Giuseppe Peano (1858–1932) came along in 1889 and compactified Dedekind's definition.

Peano's Definition of $\mathbb{N}$

$\mathbb{N}$ is a set equipped with

- an equivalence relation "$=$"
- a function $S : \mathbb{N} \to \mathbb{N}$
- a special element $0 \in \mathbb{N}$

satisfying just <u>three axioms</u>:

1. $\forall n \in \mathbb{N}$, $S(n) \neq 0$.
2. $\forall m, n \in \mathbb{N}$ we have

$$S(m) = S(n) \implies m = n.$$

3. If a set $X \subseteq \mathbb{N}$ satisfies
   - $0 \in X$
   - $\forall n \in \mathbb{N}$, $n \in X \Rightarrow S(n) \in X$.

   then it follows that $X = \mathbb{N}$.

Remarks on Peano:

- We are supposed to think

$$S(n) = \text{“}n+1\text{”}$$

(S is for “successor”).

- The third axiom is called the principle (or axiom) of induction. It is logically equivalent to well-ordering but we probably won't prove this.

- Induction is subtle in the friendly definition (we almost missed it!) but it becomes the very heart of Peano's definition

Moral of the story:

It is not obvious, but

principle of induction $=$ concept of number

Thanks for your attention.

Back to earth. How is induction used?

Example: Prove that for all integers $n \geq 1$ we have

$$2^{n-1} \leq n!$$

First let's test it.

$n=1$ $\quad 2^0 = 1 \leq 1! = 1$ ✓

$n=2$ $\quad 2^1 = 2 \leq 2! = 2$ ✓

$n=3$ $\quad 2^2 = 4 \leq 3! = 6$ ✓

$n=4$ $\quad 2^3 = 8 \leq 4! = 24$ ✓

Ok, I believe it. Now what?

Idea: I'll ask my computer to check it. My computer proves that it's true for all $n \leq 10^{10000000000}$. Then my computer breaks down.

OK, now what? We're supposed to prove it for all integers $n \geq 1$, not just "a lot" of them.

Do you see that this is impossible without some extra help?

Let's think abstractly. Suppose, hypothetically, that we have some integer $k \geq 1$ such that

$$2^{k-1} \leq k! \qquad (*)$$

What logical consequences does this have (again, hypothetically)?

I can do lots of things.... like

$$2^{k-1} \leq k!$$
$$2 \cdot 2^{k-1} \leq 2 \cdot k!$$
$$2^k \leq 2 \cdot k!$$

But wait a minute! Isn't

$$2 \cdot k! \leq (k+1) \cdot k! \quad ?$$
$$2 \cdot k! \leq (k+1)! \quad ?$$

Certainly if (hypothetically) we have $2 \leq k+1$, then it follows that

$$2 \leq k+1$$
$$2 \cdot k! \leq (k+1) \cdot k!$$
$$2 \cdot k! \leq (k+1)!$$

OK great. Put it together:

If $k \geq 1$ and $2^{k-1} \leq k!$, then we have

$$2^{k-1} \leq k!$$
$$2 \cdot 2^{k-1} \leq 2 \cdot k!$$
$$2^k \leq 2 \cdot k! \leq (k+1)!$$

Hence $2^k \leq (k+1)!$

You can imagine repeating the same argument to show that

$$2^{k+1} \leq (k+2)!$$

Q: It looks good. Are we done?

A: I don't know. Are we?

I think we both agree that this is a proof, but we should draw up a legal contract, just in case.

☆ The Axiom of Induction:

Consider a statement $P: \mathbb{N} \to \{T, F\}$ about natural numbers. If

- $P(b) = T$ for some $b \in \mathbb{N}$

and

- For any $k \geq b$ we have that $P(k) \Rightarrow P(k+1)$

then we will agree to say that

$P(n) = T$ for all $n \geq b$.

(Please sign here.)

Now let's write up our proof in the legal way.

Theorem: Given $n \in \mathbb{N}$ we define the statement

$$P(n) := \text{“ } 2^{n-1} \leq n! \text{ ”}$$

We claim that $P(n) = T$ for all $n \geq 1$.

Proof: We will use induction.

First we verify the base case. Note that $2^{1-1} = 2^0 = 1$ and $1! = 1$, hence

$$P(1) = \text{“ } 2^{1-1} \leq 1! \text{ ”} = T.$$

Next we verify the "induction step". Suppose (hypothetically) that we have some $k \geq 1$ such that $P(k) = T$, i.e., such that

$$2^{k-1} \leq k!$$

In this case, since $k+1 \geq 2$, it follows that

$$2^{k-1} \leq k!$$
$$2 \cdot 2^{k-1} \leq 2 \cdot k!$$
$$2^k \leq 2 \cdot k! \leq (k+1)\, k!$$
$$2^k \leq (k+1)\, k!$$
$$2^k \leq (k+1)!$$

and hence $P(k+1) = T$. We have proved that for all $k \geq 1$ we have

$$P(k) \Longrightarrow P(k+1)$$

(hypothetically, of course ☺)

By the Axiom of Induction, we conclude that $P(n) = T$ for <u>all</u> $n \geq 1$.

//

You may think you understand what we did here, but a word of warning:

Be careful to use the Axiom of Induction exactly as written, or I might sue you!