Thursday June 20

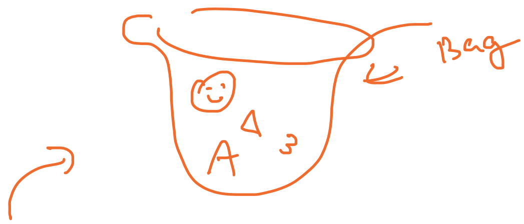
Chapter Zero

The Language of Mathematics:

Sets, Axioms, Theorems & Proofs

Mathematics is a language, and Logic is its grammar.

Part I: Set Theory and Basic Logic



Definition: A $\boxed{\textit{set}}$ is an unordered collection of objects, called the ***elements*** of the set. A set can be described using the ***set-builder notation***:

$$X = \Big\{x \,\big|\, x \text{ possesses certain determinable qualities}\Big\},$$

or the ***roster method***:

$$X = \{a, b, \ldots\},$$

unordered List elements
objects in a set

where we explicitly ***list*** the elements of X. The bar symbol "|" in set-builder notation represents the phrase "such that."

$X = \{1, 2, 3, 3, 3\} = \{1, 2, 3\} = \{3, 1, 2\}$

There is also a special set, called the $\boxed{\textit{empty set}}$ or the ***null-set***, that does not contain any elements:

$$\boxed{\emptyset} \text{ or } \{\quad\}.$$

Important Sets of Numbers:

Natural Numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$. Counting #s

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

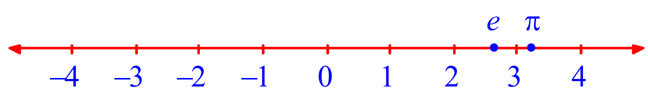
"Zhalen"

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \text{ and } b \text{ are integers, with } b \neq 0 \right\}.$$

$3/4, \frac{-5}{101} \in \mathbb{Q}$ "belongs to"

$\pi \notin \mathbb{Q}$

$\sqrt{2} \notin \mathbb{Q}$



The Real Number Line $\mathbb{R}$

$\mathbb{C}$ = complex #s $\quad i = \sqrt{-1}$ or $\underline{i^2 = -1}$

$= \{a + ib \mid a, b \in \mathbb{R}\}$

$\boxed{e^{\pi i} = -1}$ or $\boxed{e^{\pi i} + 1 = 0}$

Logical Statements and Axioms

Definition: A ***logical statement*** is a complete sentence that is either ***true*** or ***false***.

Which of the following are logical statements? (and if the statement is logical, is it true or false?)

The square of a real number is never negative.

x "$x^2 \geq 0$" yes a logical statement. True

The set of natural numbers has a smallest element.

$\mathbb{N} = \{0, 1, 2, \ldots\}$ logical statement ✓ true

The set of integers has a smallest element.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ logical statement ✓ False

Geometry is more important than Algebra.

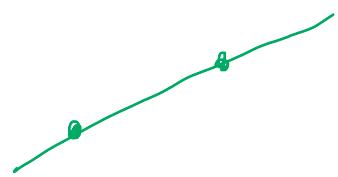
logical statement ✗ not

Definition: An ***Axiom*** is a logical statement that we will ***accept*** as true, that is as reasonable human beings, we can ***mutually agree*** that such Axioms are true.

The empty set Ø exists.

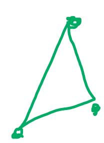
Euclidean Geometry:

existence of ***points***



through two distinct points there must exist a unique ***line***.

any three non-collinear points determine a unique ***triangle***.



Quantifiers

"every integer is positive"
"$\forall z \in \mathbb{Z}, z > 0$" statement? ✓ False.

Definitions — Quantifiers:

There are two kinds of quantifiers: ***universal*** quantifiers and ***existential*** quantifiers. Examples of universal quantifiers are the words ***any, all*** and ***every***, symbolized by:

$$\forall$$

"for all"

They are often used in a logical statement to describe ***all*** members of a certain set. Examples of existential quantifiers are the phrases ***there is*** and ***there exists*** or their plural forms ***there are*** and ***there exist***, symbolized by:

$$\exists$$

"there exists"

Existential quantifiers are often used to claim the existence (or non-existence) of a ***special*** element or elements of a certain set.

The Axioms for the Real Numbers

Axioms — The Field Axioms for the Set of Real Numbers:

There exists a set of Real Numbers, denoted $\mathbb{R}$, together with two binary operations:

$$+ \quad \text{(addition)} \quad \text{and} \quad \bullet \quad \text{(multiplication)}.$$

Furthermore, the members of $\mathbb{R}$ enjoy the following properties:

1. ***The Closure Property of Addition:***

   For all $x,\ y \in \mathbb{R}$: $x + y \in \mathbb{R}$ as well.

2. ***The Closure Property of Multiplication:***

   For all $x,\ y \in \mathbb{R}$: $x \bullet y \in \mathbb{R}$ as well.

3. *The Commutative Property of Addition*

$$\textit{For all } x, y \in \mathbb{R}: x + y = y + x.$$

4. *The Commutative Property of Multiplication*

$$\textit{For all } x, y \in \mathbb{R}: x \cdot y = y \cdot x.$$

5. *The Associative Property of Addition*

$$\textit{For all } x, y, z \in \mathbb{R}: x + (y + z) = (x + y) + z.$$

6. *The Associative Property of Multiplication*

$$\textit{For all } x, y, z \in \mathbb{R}: x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

7. ***The Distributive Property of Multiplication over Addition***

$$\textit{\textbf{For all }} x, y, z \in \mathbb{R}: x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

mix of x & +

8. ***The Existence of the Additive Identity:***

$$\boxed{\textit{\textbf{There exists }} 0} \in \mathbb{R} \text{ such that } \textit{\textbf{for all }} x \in \mathbb{R}:$$

$$\boxed{x + 0 = x = 0 + x.}$$

9. ***The Existence of the Multiplicative Identity:***

$$\boxed{\textit{\textbf{There exists }} 1} \in \mathbb{R},\ 1 \neq 0, \text{ such that } \textit{\textbf{for all }} x \in \mathbb{R}:$$

$$\boxed{x \cdot 1 = x = 1 \cdot x.}$$

10. ***The Existence of Additive Inverses:***

$\exists\, y \in \mathbb{R}$

$$\textit{\textbf{For all }} x \in \mathbb{R}, \boxed{\textit{\textbf{there exists }} -x \in \mathbb{R}}, \text{ such that:}$$

$$\boxed{x + (-x) = 0 = (-x) + x.}$$

$x + y = 0$

$+$

11. ***The Existence of Multiplicative Inverses:***

$$\textit{\textbf{For all }} x \in \mathbb{R}, \text{ where } x \neq 0, \boxed{\textit{\textbf{there exists }} 1/x \in \mathbb{R}},$$

$$\text{such that: } \boxed{x \cdot (1/x) = 1 = (1/x) \cdot x.}$$

$\times$

A, +

1, 3, 5, 8, 10

A, ×

2, 4, 6, 9, 11

Mix

7

"Group Theory"

Theorems and Implications

Definitions: A true logical statement which is not just an Axiom is called a ***Theorem***. Many of the Theorems that we will encounter in Linear Algebra are called ***implications***, and they are of the form:

$$\boxed{\textbf{\textit{if}}\ p\ \textbf{\textit{then}}\ q,}$$

which can also be written symbolically as:

$$\boxed{p \Rightarrow q} \text{ (pronounced as: } \boxed{p \textbf{\textit{ implies }} q}\text{).}$$

P	Q	P ⇒ Q	
T	T	T	
T	F	F	
F	T	T	← strange
F	F	T	

An implication $p \Rightarrow q$ is true if the statement q is true whenever we know that the statement p is also true.

The statements p and q are called ***conditions***.

p — the ***hypothesis*** (or ***antecedent*** or the ***given*** conditions)

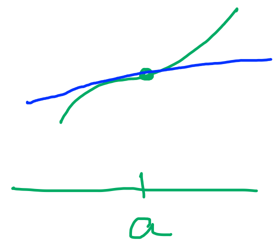
q — the ***conclusion*** or the ***consequent***.

If such an implication is true, we say: "$P \Rightarrow Q$"

condition p is ***sufficient*** for condition q, and

condition q is ***necessary*** for condition p.

True or False?



If $f(x)$ is ***differentiable*** at $x = a$,

then $f(x)$ is also ***continuous*** at $x = a$.

$4 = 1\cdot 4 = 4\cdot 1 = 2\cdot 2$

$5 = 1\cdot 5 = 5\cdot 1$ prime

If p is a prime number, then $2^p - 1$ is also a prime number.

p	$2^p - 1$
$p = 2$	$2^2 - 1 = 3$ ✓
$p = 3$	$2^3 - 1 = 7$ ✓
$p = 5$	$2^5 - 1 = 31$ ✓
$p = 11$	$2^{11} - 1 = 2047 = 23 \cdot 89$ ✗ ← $p = 11$ is a counter-example

In fact, it turns out that the integers of the form $2^p - 1$ where p is a prime number are ***rarely*** prime, and we call such prime numbers ***Mersenne primes***.

As of May 2016, there are only 49 known Mersenne Primes, and the largest of these is:

$$2^{74,207,281} - 1$$

This is also the largest known prime number.

If this number were expressed in the usual decimal form, it will be 22,338,618 digits long.

Large prime numbers have important applications in ***cryptography***, a field of mathematics which allows us to safely provide personal information such as credit card numbers on the internet.

Negations

Definition: The ***negation*** of the logical statement p is written symbolically as:

$$\boxed{\textit{not } p.}$$

$\neg p$ or $\sim p$ or $\neg p$

True or False?

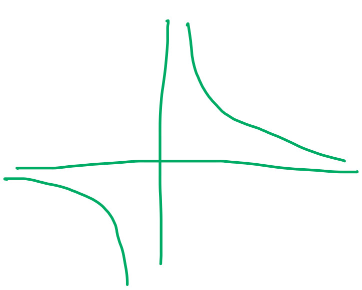
p = an integer is a rational number

$\sim p$ = not ( )

=

An integer is ***not*** a rational number.

The function $g(x) = 1/x$ is ***not*** continuous at $x = 0$.



Converse, Inverse, Contrapositive

Definition: For the implication $p \Rightarrow q$, we call:

$$\boxed{q \Rightarrow p} \qquad \text{the } \textbf{\textit{converse}} \text{ of } p \Rightarrow q,$$

$$\boxed{(\textit{not } p) \Rightarrow (\textit{not } q)} \qquad \text{the } \textbf{\textit{inverse}} \text{ of } p \Rightarrow q, \text{ and}$$

$$\boxed{\textit{not } q \Rightarrow \textit{not } p} \qquad \text{the } \textbf{\textit{contrapositive}} \text{ of } p \Rightarrow q.$$

Example:

$$\sum_{n=0}^{\infty}\left(\frac{1}{2}\right)^n = \sum_{n=0}^{\infty}\frac{1}{2^n}$$ geometric series

$$= 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots$$
$$= 2$$

Complete the following Theorem about Infinite Series:

Theorem: ***If*** $\underbrace{\sum_{n=0}^{\infty} a_n \text{ converges}}_{P}$, ***then*** $\underbrace{a_n \to 0}_{Q}$ "$P \Rightarrow Q$"

series is finite

Now let us write its:

Converse: "If $a_n \to 0$, then $\sum a_n$ converges" False $\sum \frac{1}{n}$ harmonic

$Q \Rightarrow P$ But $\sum \frac{1}{n}$ diverges. $a_n = 1/n$, $a_n \to 0$.

Inverse:

$\sim P \Rightarrow \sim Q$ "If $\sum a_n$ diverges, then $\{a_n\}$ does not not converge to 0." False see harmonic series above.

Contrapositive:

"If $\{a_n\}$ does not converge to 0, then $\sum a_n$ diverges"

$\sim Q \Rightarrow \sim P$

Do you recognize the contrapositive?

Test for Divergence!

Logical Equivalence

If we know that $p \Rightarrow q$ and $q \Rightarrow p$ are ***both*** true, then we say that the conditions p and q are ***logically equivalent*** to each other, and we write the ***equivalence*** or ***double-implication***:

ie "$p \Rightarrow Q$" and "$Q \Rightarrow P$"

$$p \Leftrightarrow q \quad \text{(pronounced as: } p \text{ } \textbf{\textit{if and only if}} \text{ } q\text{).}$$

iff

An implication is always logically equivalent to its ***contrapositive*** (as proven in Appendix B):

$p \Rightarrow Q$ $\quad$ $\sim Q \Rightarrow \sim P$

$$(p \Rightarrow q) \Leftrightarrow (\textit{not}\, q \Rightarrow \textit{not}\, p).$$

SUPER USEFUL

An equivalence is again equivalent to its contrapositive:

$$(p \Leftrightarrow q) \Leftrightarrow (\textit{not}\, p \Leftrightarrow \textit{not}\, q).$$

Logical Operations

Definition: If p and q are two logical statements, we can form their ***conjunction***:

$$\boxed{p\ \boxed{\textbf{\textit{and}}}\ q,}$$

and their ***disjunction***:

$$\boxed{p\ \boxed{\textbf{\textit{or}}}\ q.}$$

The conjunction p ***and*** q is true precisely if ***both*** conditions p and q are true.

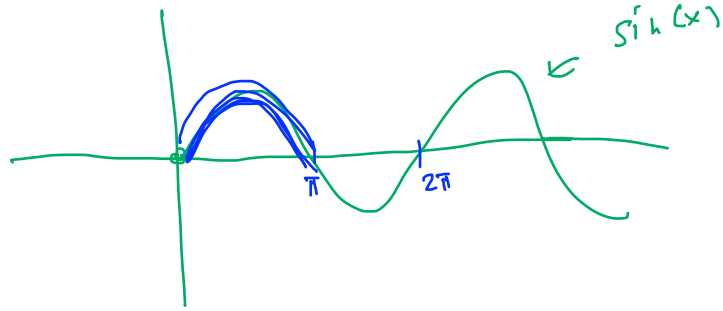
The disjunction p ***or*** q is true precisely if ***either*** condition p or q is true (or possibly both are true).

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

Examples:

True or False?



T

sin(x) is F

$f(x) = \sin(x)$ is positive ***and*** monotonic increasing on the interval $(0, \pi)$.

Every real number is either rational ***or*** irrational. True

De Morgan's Laws

Theorem — De Morgan's Laws: For all logical statements p and q:

$$\mathit{not}\ \left(p\ \boldsymbol{and}\ q\right)\ \text{is logically equivalent to}\ (\mathit{not}\,p)\ \boldsymbol{or}\ (\mathit{not}\,q),$$

and likewise:

$$\mathit{not}\ \left(p\ \boldsymbol{or}\ q\right)\ \text{is logically equivalent to}\ (\mathit{not}\,p)\ \boldsymbol{and}\ (\mathit{not}\,q).$$

$\sim (P \text{ and } Q) \Longleftrightarrow \sim P \text{ or } \sim Q$

$\sim (P \text{ or } Q) \Longleftrightarrow \sim P \text{ and } \sim Q$

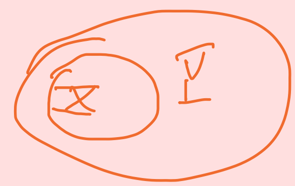
note that negation flips "and" & "or"

Subsets and Set Operations

$\mathbb{Z} \subseteq \mathbb{Q}$

sub collection of objects from X

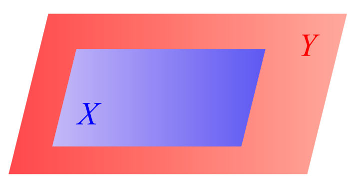
Definition: We say that a set X is a ***subset*** of another set Y if every member of X is also a member of Y. We write this symbolically as:

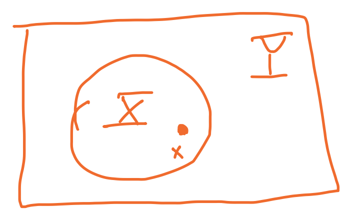


"if $x \in X$, then $x \in Y$" $\iff X \subseteq Y$

$$\boxed{X \subseteq Y.}$$

If X is a subset of Y, we can also say that X is ***contained*** in Y, or Y ***contains*** X. We can visualize sets and subsets using ***Venn diagrams*** as follows:





We say X ***equals*** Y if and only if X is a subset of Y and Y is a subset of X :

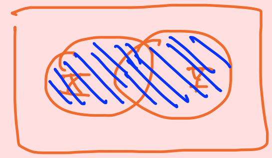
$$(X = Y) \Leftrightarrow \big(X \subseteq Y \textbf{\textit{ and }} Y \subseteq X\big).$$

Equivalently, every member of X is also a member of Y, and every member of Y is also a member of X :

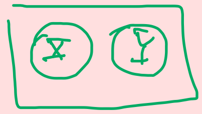
$$(X = Y) \Leftrightarrow \big(x \in X \Rightarrow x \in Y \textbf{\textit{ and }} y \in Y \Rightarrow y \in X\big).$$

We combine two sets into a single set that contains precisely all the members of the two sets using the ***union*** operation:

$$X \cup Y = \left\{ z \middle| z \in X \textbf{\textit{ or }} z \in Y \right\}.$$

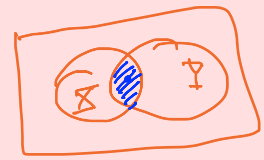


We determine all members common to both sets using the ***intersection*** operation:



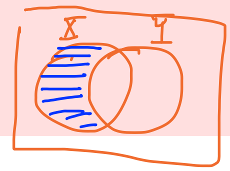
$X \cap Y = \emptyset$ ← empty set

$$X \cap Y = \left\{ z \middle| z \in X \textbf{\textit{ and }} z \in Y \right\}.$$

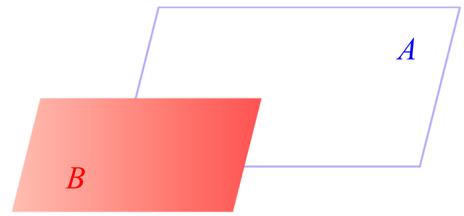


We can also take the ***difference*** or ***complement*** of two sets:

$$X - Y = \left\{ z \middle| z \in X \textbf{\textit{ and }} z \notin Y \right\}.$$

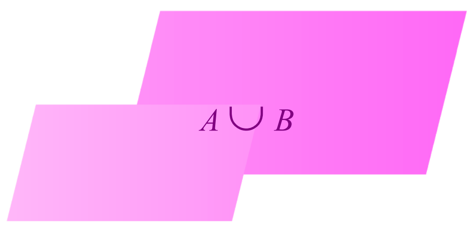


A

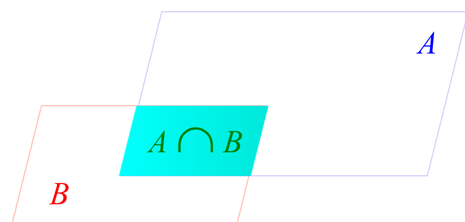


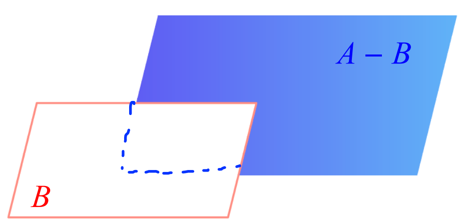
B

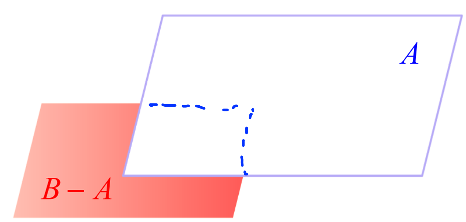
$A \cup B$



$A \cap B$







Example:

$$A = \{b, e, f, h\}$$

$$B = \{a, b, d, e, f, g, h, k\}$$

$$C = \{a, b, c, e, k\}$$

$$D = \{b, e, f, k, n\}$$

Is $A \subseteq B$?

$C \cup D =$

$C \cap D =$

$C - D =$

$D - C =$

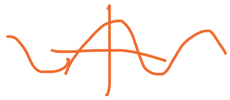
Part II: Proofs

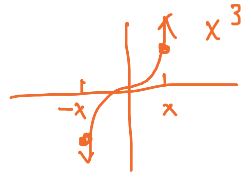
Definition: A ***proof*** for a Theorem is a sequence of true logical statements which ***convincingly*** and ***completely explains*** why a Theorem is true.

The Glue that Holds a Proof Together — Modus Ponens

- Suppose you already know that an implication $p \Rightarrow q$ is true.
- Suppose you also established that condition p is satisfied.
- Therefore, it is logical to conclude that condition q is also satisfied.

Example: Let us demonstrate modus ponens on the following logical argument:





f is odd if $f(-x) = -f(x)\ \forall x \in [-a,a]$

In Calculus, we proved that ***if*** $f(x)$ is an ***odd*** function on $[-a, a]$, ***then*** $\int_{-a}^{a} f(x)\,dx = 0.$ $(P \Rightarrow Q)$

The function $f(x) = x^7\cos(3x)$ is an odd function on $[-\pi, \pi]$, since:

$$f(-x) = (-x)^7\cos(-3x) = -\left(x^7\cos(3x)\right) = -f(x).$$

Therefore: $\int_{-\pi}^{\pi} x^7\cos(3x)\,dx = 0.$

Basic Tips to Write Proofs

understanding the ***meaning*** of the given conditions and the conclusion

state the ***definitions*** of a variety of ***words*** and ***phrases*** involved

be familiar with special ***symbols*** and ***notation***

a previously proven Theorem can also be helpful to prove another Theorem

☆

identify what is ***given*** (the hypotheses), and what it is that we want to ***show*** (the conclusion)

WTS = want to show   NTS = need to show

emulate examples from the book and from lecture as you learn and develop your own style

We often use unconsciously:

Axiom — The Substitution Principle:

If $x = y$ and $F(x)$ is an arithmetic expression involving x, then $F(x) = F(y)$.

A Proof Based only on Axioms

Theorem 1 — The Multiplicative Property of Zero: For all $a \in \mathbb{R}$:

$$0 \bullet a = 0 = a \bullet 0.$$

Pf Let $a \in \mathbb{R}$ be arbitrary. WTS: $0 \cdot a = 0$.

By A8, we have $0 + 0 = 0$. Then multiplying by a,

$$\begin{aligned} 0 \cdot a &= (0+0)\cdot a \\ &= a \cdot (0+0) && (A4) \\ &= a \cdot 0 + a \cdot 0 && (A7) \end{aligned}$$

So: $0 \cdot a = a \cdot 0 + a \cdot 0$.

By A10, there exist ($\exists$) $-[a \cdot 0]$. So, by the substitution principle

$$0 \cdot a + -[a \cdot 0] = (a \cdot 0 + a \cdot 0) + -[a \cdot 0]$$

(def of $-[a\cdot 0]$)

$$\begin{aligned} 0 &= a \cdot 0 + (a \cdot 0 + -a \cdot 0) && A5 \\ 0 &= a \cdot 0 + 0 && (\text{def of } -[a \cdot 0] \text{ aka } A10) \\ 0 &= a \cdot 0 && (A8) \\ 0 &= 0 \cdot a. && (A4) \end{aligned}$$

So we're done! $\square$ (QED)

$P =$ "$a \cdot b = 0$"
$Q =$ "$a = 0$ or $b = 0$"

Case-by-Case Analysis

$P \Rightarrow Q$ and $Q \Rightarrow P$

Theorem 2 — The Zero-Factors Theorem: For all $a, b \in \mathbb{R}$:

$$a \bullet b = 0 \ \boxed{\textit{if and only}} \textit{ if} \text{ either } a = 0 \ \textit{or} \ b = 0.$$

"implication"

Pf ($\Rightarrow$) Assume that $a \cdot b = 0$. WTS: $a = 0$ or $b = 0$.

Case 1 One possibility is $a = 0$.

Since $a = 0$ then "$a = 0$ or $b = 0$" is true. And we're done.

Case 2 The other possibility is $a \neq 0$.

Since $a \neq 0$, by A11, there exists $\frac{1}{a} \in \mathbb{R}$ so that $a \cdot \left(\frac{1}{a}\right) = 1$.
Then by the substitution principle:

$$\frac{1}{a}(a \cdot b) = \frac{1}{a}(0) \quad \text{by Thm 1}$$

A6

$$\left(\left(\frac{1}{a}\right)a\right) \cdot b = 0$$

A11

$$1 \cdot b = 0$$

A9

$$b = 0.$$

So since $a \neq 0$ we got $b = 0$ so "$a = 0$ or $b = 0$" is true.

Since Case 1 & Case 2 exhausts all possibilities, we are done!

"converse"

($\Leftarrow$) Assume that $a = 0$ or $b = 0$. WTS: $a \cdot b = 0$.

Case 1 $a = 0$

Since $a = 0$, $a \cdot b = 0 \cdot b$ by substitution principle.
Then Thm 1 says $0 \cdot b = 0$ so $a \cdot b = 0 \cdot b = 0$. Yay! Done,
so $a \cdot b = 0$.

Case 2 $b=0$

"excercize" very similar to case 1

So since Case 1 & Case 2 exhaust all possibilities, we conclude "$a \cdot b = 0$" is true. $\square$

Proof by Contrapositive

We will need for the next Example:

Axioms — Closure Axioms for the Set of Integers:

If $a,\ b \in \mathbb{Z},$ then $a + b \in \mathbb{Z},\ a - b \in \mathbb{Z},$ and $a \cdot b \in \mathbb{Z}$ as well.

Definitions — Even and Odd Integers:

$\exists c \in \mathbb{Z}$

An integer $a \in \mathbb{Z}$ is ***even*** if there exists $c \in \mathbb{Z}$ such that $\boxed{a = 2c.}$
An integer $\cancel{b}$ a $\in \mathbb{Z}$ is ***odd*** if there exists $d \in \mathbb{Z}$ such that $\boxed{a = 2d + 1.}$

$\exists c$ $\exists d$

$\boxed{a = 2c}$ $\boxed{a = 2d+1}$

even odd

Ex

- if a is even then a^2 is even.
- if a^2 is even then a is even.
-
- If a^2 is odd, then a is odd.

Let us now prove the following:

"a is odd and b is odd"

Theorem: For all $a,\ b \in \mathbb{Z}$:

If the product $\boxed{a \bullet b \text{ is } \textbf{odd},}$ then $\boxed{\textbf{both } a \text{ and } b \text{ are } \textbf{odd}.}$

P Q

"DeMorgan's Laws" not odd = even :)

$\sim Q \Rightarrow \sim P$

Contrapositive is: "If a is not odd or b is not odd then a·b is not odd"

Pf We'll prove the contrapositive. Assume that a is even or b is even.

WTS a·b is even.

Case 1 a is even.

Since a is even, by the definition there exist $c \in \mathbb{Z}$ such that $a = 2c$. Then

$$a \cdot b = (2c) \cdot b \quad \text{(substitution principle)}$$
$$= 2(c \cdot b) \quad (A6)$$

Since $c \cdot b \in \mathbb{Z}$ (A2 but for $\mathbb{Z}$) then by definition of even, $a \cdot b$ is even (since $a \cdot b = 2(cb)$).

Case 2 b is even.

Similar to case 1.

So by Case 1 & Case 2, we showed that a·b is even in all cases. $\square$

Proof by Contradiction

- $P \Rightarrow Q$ implication
- $\sim Q \Rightarrow \sim P$ contrapositive
- Assume P and $\sim Q$. Show Q,

Known formally as: ***reductio ad absurdum***

often used in order to show that an object does not exist, or in situations when it is difficult to show that an implication is true directly

assume that the mythical object does exist, or more generally, the opposite of the conclusion is true.

arrive at a condition which ***contradicts*** one of the given conditions, or a condition which has already been concluded to be true (thus producing an ***absurdity*** or contradiction).

not guaranteed to work :(

Theorem: The real number $\sqrt{2}$ is ***irrational.***

Proof by Induction

Note: Not covered yet! Will cover this material later!

Theorem: For all positive integers n :

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}.$$

Proof of $\sqrt{2}$ is irrational (not rational) $\sqrt{2}\notin\mathbb{Q}$,

- Assume $\sqrt{2}$ is rational ($\sqrt{2}\in\mathbb{Q}$) and arrive at a contradiction.

Since $\sqrt{2}\in\mathbb{Q}$, there exist $a,b\in\mathbb{Z}$, $b\neq 0$ so that

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

Let's assume (by cancelling) that $\frac{a}{b}$ is written in lowest terms (ie a & b dont have any common factors).

Then squaring both sides:

$$\left(\sqrt{2}\right)^2=\left(\frac{a}{b}\right)^2$$

$$2=\frac{a^2}{b^2}$$

Then $a^2=2\cdot b^2$. So, a^2 is even!

claim If a^2 is even then a is even.

Pf By contrapositive ($\sim Q\Rightarrow\sim P$). Assume a is odd. WTS: a^2 is odd. Since a is odd, by definition there exists $d\in\mathbb{Z}$ so that $a=2d+1$. Thus,

$$a^2=[2d+1]^2=4d^2+4d+1=2[2d^2+2d]+1$$

Since $2d^2+2d \in \mathbb{Z}$ this shows a^2 is odd. $\square$

By claim, a is even! So, $a = 2c$ for some $c \in \mathbb{Z}$ ($\exists c \in \mathbb{Z}$). Then $a^2 = 2b^2$ gives $4c^2 = 2b^2$ cancelling 2 gives;

$2c^2 = b^2$.

So b^2 is even.
so b is even.

Thus, a & b are even which have 2 as common factor! This contradicts our assumptions so we're done! $\square$

Conjectures and Demonstrations

Many statements in mathematics have not been determined to be true or false.

They are called ***conjectures***.

We can try to ***demonstrate*** that it is ***plausible*** for the conjecture to be true by giving examples.

These demonstrations are ***not*** replacements for a complete proof.

Goldbach's Conjecture: Every ***even*** integer bigger than 2 can be expressed as the ***sum*** of two prime numbers.