Sets

What is a set?

- A set is a well defined collection of stuff (data)

In ex.

- {1,2,3}
- {dogs}
- {2,4,6,8,10}

Comparing sets:

- {1,2,3} = {3,2,1} (these 2 sets are the same)

Checking if something is in a set:

- $8 \in$ {2,4,6,8,10}
- Huck $\notin$ {dogs}
- 5 $\notin$ {2,4,6,8,10}
- Cat $\notin$ {dogs}

Checking if a set is in another set:

- {2} $\notin$ {1,2,3} (this is because 2 is it's own set and we cannot say it is in another set as {n} $\neq$ n)
- We can however say {2} $\in$ {{1}, {2}}
- Similarly 2 $\notin$ {{1},{2}} (n $\neq$ {n})

Set Builder Notation

{x | x is a robot on Earth}

- $\mathbb{Z}$: Integers
- $\mathbb{R}$: Real Numbers
- $\mathbb{Q}$: Rational Numbers
- $\mathbb{C}$: Complex Numbers

- Ex. $\{n \in \mathbb{Z} \mid n > 0\}$ = $\mathbb{Z}^+$
- Ex. $\{x \in \mathbb{R} \mid \}$
- $A = \{x \in \mathbb{R} \mid 2 < x \leq 5\} = (2, 5]$
- $B = \{x \in \mathbb{Z} \mid 2 < x \leq 5\} = 3, 4, 5$

Subsets

- $A = \{x \in \mathbb{R} \mid 2 < x \leq 5\} = (2, 5]$
- $B = \{x \in \mathbb{Z} \mid 2 < x \leq 5\} = 3, 4, 5$
- $A \subseteq B$ "=" if $x \in A$ then $x \in B$
- $A \not\subseteq B$
- $2.5 \in A$ but $2.5 \notin B$
- $B \subseteq A$
- $3 \in B$ then $3 \in A$
- C = {all even integers}
- $D = \{n \in \mathbb{Z} \mid there \exists k \in Z \text{ such that } n = 2k\}$
- $n \in C$ then $n \in D$; $C \subseteq D$
- $n \in D$ then $n \in C$; $D \subseteq C$
- Notice: $A \subseteq A$ every set is a subset of itself
- If you want a truly smaller set then $A = \{1, 2, 3, 4\}$ $B = \{1, 2\}$

Null Set

- the null set is called the empty set, denoted as ∅ = {}
- no elements

Power Set: P(x) = {all subsets of X}

- x = {a,b}
- P(x) = {{a,b}, {a}, {b}, {∅}}
- y = {a,b,c}
- P(y) = {{a,b,c}, {a,b}, {a,c}, {b,c}, {a}, {b}, {c}, {}}
- Statements: A statement (or proposition) is a sentence (something you say) that is definitively True or False
- Example: It is raining outside (can either be true or false, no in between); False
- Example: It is sunny outside; True

- Not a statment: "x > 7"
- However, 9 > 7, is a true statement
- 9 < 7; is a false statement

Logic

Predicate

- The idea of a predicate is a sentence where theres a variable or variables where if you specify the variable(s) it becomes a sentence
- Example: x > 7 (we need a domain)
  - Domain: The things that x (the variable) could be. It doesn't have to be just the stuff that make the predicate true.
- $x > 7$ Domain: $\mathbb{R}$
- Truth set: $\{x \in \mathbb{R} \mid x > 7\}$
- Domain in logic can sometimes be implied
- Predicate: $x^2 = 4$
  - Statement: $\frac{8}{4} = 4$ False
  - Statement: $\frac{8}{2} = 4$ True

Statement Form:

- p , q ,r
- a place holder for statements

Predicate Form:

- P(x), Q(x)

Compound Statements:

- p and q is written as $p \wedge q$
- p or q is written as $p \vee q$
- not p $\neg p$

S1	logic	S2	OUT
3 > 0	and	3< 0	False

S1	logic	S2	OUT
3 > 0	or	3 < 0	True
3 > 0	or	$\frac{6}{3} = 2$	True
3 > 0	not	$3 \nleq 0$	False

How do we understand the interaction of truth values when you put together statement forms

- Truth Values

Negation: $\neg p$

P	$\neg P$
T	F
F	T

Conjunction: $p \wedge q$

P	Q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction: $p \vee q$

P	Q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

More than 2 statement forms:

- $p \wedge q \wedge r$
- similar to 1 + 2 + 3 = 6
  - (1+2) + 3 = 6
  - 1 + (2+3) = 6
- $(p \wedge q) \wedge r$ is the same as $p \wedge (q \wedge r)$

P	**Q**	**R**	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

We can now say:

- $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

Is this true?

- $\neg(p \wedge q) \equiv \neg p \wedge \neg q$?

P	**Q**	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	F
F	T	F	T	T	F	F
F	F	F	T	T	T	T

- From the table we can see they are not equivalent

What about $\neg(p \wedge q) \equiv \neg p \vee \neg q$

P	**Q**	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

- we can say that they are equivalent

DeMorgan's Laws

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Example:

- $\neg(x < 3 \vee x \geq 5) \equiv \neg(x \leq 3) \wedge \neg(x \geq 5)$
- $\equiv x \geq 3 \wedge x < 5$
- $\equiv 3 \leq x \leq 5$

Distributive Laws

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$
$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

More Logic

$(p \wedge q) \vee \neg r$

Truth Table:

p	**q**	**r**	$p \wedge q$	$\neg r$	$(p \wedge q) \vee \neg r$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	F	T	T

p	q	r	$p \wedge q$	$\neg r$	$(p \wedge q) \vee \neg r$
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

What can we use this for:
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

Thus we can conclude that $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Find the truth values of:
$(p \wedge q) \vee (\neg p \vee (p \wedge \neg q))$

p	q	$p \wedge q$	$\neg p$	$\neg q$	$p \wedge \neg q$	$\neg p \vee (p \wedge \neg q)$	$(p \wedge q) \vee (\neg p \vee (p \wedge \neg q)$
T	T	T	F	F	F	F	T
T	F	F	F	T	T	T	T
F	T	F	T	F	F	T	T
F	F	F	T	T	F	T	T

- Tautology: Statement form that is always true, symbol t
- We can see that since every instance is true this statement is a tautology

- A contradiction is a statement that is always false. symbol c

  $p \wedge \neg p \equiv c$

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

Table of Logic Identities and Laws:

1.	*Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2.	*Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3.	*Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4.	*Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5.	*Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6.	*Double negative law:*	$\sim(\sim p) \equiv p$	
7.	*Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8.	*Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9.	*De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10.	*Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11.	*Negations of* $\mathbf{t}$ *and* $\mathbf{c}$ *:*	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

How to use the logical equivalences:

Lets say we're given the statement $\neg(\neg p \wedge q) \wedge (p \vee q) \equiv p$

- we need to show that these two statements are equivalent using the table
  $\neg(\neg p \wedge q) \wedge (p \vee q) \equiv (\neg(\neg p)) \vee \neg q) \wedge (p \vee q)$ by DeMorgan's Law
  $\equiv (p \vee \neg q) \wedge (p \vee q)$ by Double Negative Law
  $\equiv p(\neg q \wedge q)$ by the Distributive Law
  $\equiv p \vee c$ by the Negation Law
  $\equiv p$ by the Identity Law

Conditional Statements

If p then q
$p \rightarrow q$

- If 1 = 1 (true) then 2 = 2 (true) => true overall
- If 0 = 1 (false) then 2 = 2 (true) => true overall
- If 0 = 1 (false) then 1 = 2 (false) => true overall

The truth table is:

p	**q**	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	F

The statement $p \rightarrow q$ is only ever false when p is true and q itself is false

$p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$

p	**q**	**r**	$p \vee q$	$p \vee q \rightarrow r$	$p \rightarrow r$	$q \rightarrow r$	$(p \rightarrow r) \wedge (q \rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T

p	q	r	$p \vee q$	$p \vee q \rightarrow r$	$p \rightarrow r$	$q \rightarrow r$	$(p \rightarrow r) \wedge (q \rightarrow r)$
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

- same truth values therefor they are equivalent

With Predicates: Suppose x is a real number
If $x^2 < 1$ then $x < 1$

What would $\neg(p \rightarrow q)$ look like?
$\neg(p \rightarrow q) \not\equiv \neg p \rightarrow \neg q$

p	q	$p \rightarrow q$	$\neg(p \rightarrow q)$	$\neg q$	$\neg q$	$\neg p \rightarrow \neg q$
T	T	T	F	F	F	T
T	F	F	T	F	T	T
F	T	T	F	T	F	F
F	F	T	F	T	T	T

by the truth table we can conclude that $\neg(p \rightarrow q) \not\equiv \neg p \rightarrow \neg q$

Let's try
$\neg(p \rightarrow q) \equiv q \rightarrow p$

p	q	$p \rightarrow q$	$\neg(p \rightarrow q)$	$q \rightarrow p$
T	T	T	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	F	T

by the truth table we can conclude that
$\neg(p \rightarrow q) \not\equiv q \rightarrow p$

However, we can see that:
$\neg p \rightarrow \neg q \equiv q \rightarrow p$

as well as:
$p \rightarrow q \equiv \neg q \rightarrow \neg p$

If we use $p \rightarrow q$

$q \rightarrow p$ is the converse

$\neg q \rightarrow \neg p$ is the contrapositive

$\neg p \rightarrow \neg q$ is the inverse

Transformation	Definition	Form (Original Statement: $p \to q$)	Example
Contradiction	A proof technique where we assume the opposite of what we want to prove and derive a contradiction.	Assume $\neg p$ and derive a contradiction.	To prove "There is no largest prime," assume there is one and derive a contradiction.
Inverse	Negates both the hypothesis and conclusion.	$\neg p \to \neg q$	"If it rains, then the ground is wet." → "If it does not rain, then the ground is not wet." (Not always true!)
Converse	Swaps the hypothesis and conclusion.	$q \to p$	"If it rains, then the ground is wet." → "If the ground is wet, then it rained." (Not always true!)
Contrapositive	Negates and swaps the hypothesis and conclusion. Always logically equivalent to the original statement.	$\neg q \to \neg p$	"If it rains, then the ground is wet." → "If the ground is not wet, then it did not rain." (Always true if the original is true.)
Generalization	Infers a broader statement from specific cases.	If p is true for a specific case, assume it is true in general.	"This triangle has 180° → All triangles have 180°." (Needs proof!)
Specialization	Deduces a specific case from a general rule.	If $p \to q$ is true and p holds, then q must hold.	"All humans are mortal. Socrates is human → Socrates is mortal."
Elimination (Disjunctive Syllogism)	If one part of a disjunction is false, the other must be true.	$p \lor q, \neg p \Rightarrow q$	"It is either raining or sunny. It is not raining → It must be sunny."
Transitivity	If $p \to q$ and $q \to r$, then $p \to r$.	$(p \to q) \land (q \to r) \Rightarrow (p \to r)$	"If you study, you pass. If you pass, you graduate. → If you study, you graduate."
Division into Cases (Proof by Cases)	Prove a conclusion by covering all possible cases.	If $p \lor q$, and both $p \to r$ and $q \to r$ hold, then r must be true.	"Either it rains or it does not. If it rains, the streets are wet. If it does not, the sprinklers are on → The streets are wet."

Negation	The opposite of a given statement. If a statement is true, its negation is false, and vice versa.	$\neg(p \vee q) \equiv \neg p \wedge \neg q$ (De Morgan's Law)	"It is not raining" is the negation of "It is raining."

We still need to find $\neg(p \to q) \equiv ?$
$p \to q$ 3 T's and 1 F
$\neg(p \to q)$ 3 F's and 1 T

- The negation needs to be $\wedge$ statement

p	q	$p \to q$	$\neg p \vee q$	$p \wedge \neg q$
T	T	T	T	F
T	F	F	F	T
F	T	T	T	F
F	F	T	T	F

$p \to q \equiv \neg p \vee q$
$\neg(p \to q) \equiv p \wedge \neg q$

Using Predicates:
If $x^2 < 1$ then $x < 1$
$x^2 \geq_1$ or $x < 1$
$\neg$(If $x^2 < 1$ then $x < 1) \equiv x^2 < 1$ and $x \geq 1$

Example 1:
x is a real number
¬(If x<1 then x=0)
$x < 1$ and $x \neq$ 0

Example 2:
¬ (If 0 = 1 then 2 = 2)
$0 = 1 \text{ and } 2 \neq 2$

Arguments

Example:
If p then q => True (Premise)

p => True
therefore q => True (Conclusion)

Valid: If all premises are true then the conclusion must be true

Modus Ponens
$p \to q$
p
$\therefore q$
To show that this is a valid argument:

p	q	$p \to q$	p	q
T	T	T	T	T
T	F	F	T	
F	T	T	F	
F	F	T	F	

Only the first row matters as that is when all the premises and conclusion is true therefore the argument is valid

$(p \to q) \land p\ q$
T T

Elimination
$p \lor q$
$\neg q$
$\therefore p$

p	q	$p \lor q$	$\neg q$	p
T	T	T	F	
T	F	T	T	T
F	T	T	F	
F	F	F	T	

Let's look at an invalid argument
$p \to q$
q
$\therefore p$

p	q	$p \rightarrow q$	q	p
T	T	T	T	T
T	F	F	F	
F	T	T	T	F
F	F	F	F	

this is invalid because the premises are true but the conclusion is false

Modus tollens
$p \rightarrow q$
$\neg q$
$\therefore \neg p$

Example with predicates:

P(x) $\rightarrow$ Q(x) If f(x) is differentiable then f(x) is continuous

P(a) $f(x) = x^2$ is differentiable

$\therefore$ Q(a) $f(x) = x^2$ is continuous

Proving Modus Tollens is a valid argument

p	q	$p \rightarrow q$	$\neg q$	$\neg p$
T	T	T	F	
T	F	F	T	
F	T	T	F	
F	F	T	T	T

Thus we proved that it is a valid argument

Inverse Error:

If $x^2 < 1$ then x>1,

$x^2 = (-5)^2 = 25 \geq 1$ True

$\therefore x = -5 \geq 1$ False

A valid argument would be

If x^2 then $x < 1$
$x = 5 \geq 1$
$\therefore x^2 = 25 \geq 1$

What about more complicated things?

Is the following a valid argument?

$p \to q \vee \neg r$
$q \to p \wedge r$
$\therefore p \to r$

We can use a truth table to verify

p	**q**	**r**	$\neg r$	$q \vee \neg r$	$p \wedge r$	$p \to q \vee \neg r$	$q \to p \wedge r$	$p \to r$
T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	
T	F	T	F	F	T	F	T	
T	F	F	T	T	F	T	T	F
F	T	T	F	T	F	T	F	
F	T	F	T	T	F	T	F	
F	F	T	F	F	F	T	T	T
F	F	F	T	T	F	T	T	T

Not a valid argument

More Examples of Valid Arguments

Generalization

p
$\therefore p \vee q$
q
$\therefore p \vee q$

Transitivity

$p \to q$
$q \to r$
$\therefore p \to r$

Contradiction Rule

$\neg p \to c$
$\therefore p$

Predicates

If $x^2 \leq 1$ then $x \leq 1$

- this is a predicate but not a statement

We need to add Quantifiers
$\text{For all } x \in \mathbb{R}, \text{if } x^2 \leq 1 \text{ then } x \leq 1$

$\forall$ and For all are called the universal quantifier

$\forall$ functions f(x), if f(x) is continuous then f(x) is differentiable

- The statement is false as f(x) is differentiable is sometimes true

There exists $x \in \mathbb{R}, x * \frac{1}{x} = 1$

- Can also be written $\exists x \in R, \frac{x*1}{x} = 1$
  this essentially means there is at least one thing that works

For example:
$\exists x \in \mathbb{R} \text{ such that } 5x = 0$
true as x = 0 would validate the statement

Truth Sets and Domains:

P(x) is $x^2 - 1 = 0$

What domain can we plug into P(x) to make it true?

- Using the domain $D = \mathbb{R}$
- Plugging in 0 would make it false
- Plugging in 1 would make it true
- thus $1 \in \mathbb{R}$
- Truth set is $\{a \in D | P(a) \text{ is true }\}$

Another Example would be
$\forall x \in \mathbb{R}$ if $x \geq 1$ then $x^2 \geq x$

Negating Quantifiers

$\neg(\forall x \in \mathbb{Z}, x^2 \geq x) \equiv \exists x \in \mathbb{Z}, x^2 < x$

- $\forall$ becomes $\exists$
- $\exists$ becomes $\forall$
- just negate the predicate as usual

Negating multiple quantifiers

$\forall x \in \mathbb{R}+, \forall y \in \mathbb{R}+, xy > 0$ which is true

the negation:

$\exists x \in \mathbb{R}+\text{ and } \exists y \in \mathbb{R}+\text{ such that } xy \leq 0$ This is false

Wrapping up logic

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } 5x = y$ -True

we can prove this with an example:

$x = 6, 5(6) = 30$

$\neg(\forall x \in \mathbb{R}, \exists x \in \mathbb{R}, \text{ such that } 5x = y)$
$\equiv \exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, 5x \neq y$
$x = 3, y = ?$
$5(3) = y$

Be careful swapping just the quantifiers might not change truth values

$\forall x \in \mathbb{R}, \exists y \in R \text{ such that } 5x = y$ -True

$\exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, 5x = y$ -False

Another Example

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } xy = 0$ -True as you can just pick any x and pick y = 0

$\exists x \in \mathbb{R} \text{ such that} fora;; y \in \mathbb{R} xy = 0$ -true pick x = 0, therefor any y that you pick xy=0

$\neg(\exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R} xy = 0)$
$\equiv \forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } xy \neq 0$

Negating Universal Conditional Statements

$\forall x, P(x) \to Q(x)$

$\neg(p \to q) \equiv p \wedge \neg q$

For example:

$\forall x \in \mathbb{Z}, \text{if 4 divides x then 2 divides x}$ -True
$\frac{x}{4} = \text{integer} \to \frac{x}{2} = \text{integer}$

What is the negation of this?

$\exists x \in \mathbb{Z}, \text{ 4 divides x and 2 doesn't divide x}$ - This is never going to be true as if 4 is dividing something evenly, then that number must be even, therefore 2 can also divide it

Example from calculus

$\forall$ functions f, if f is differentiable then f is continuous

False Example:
¬(∀ functions f, if f is continuous then f is differentiable)
≡ ∃ function f such that f is continuous and f is not differentiable
you can find a continuous function that isn't differentiable

Logical Equivalences:

Summary of Logical Equivalences (1/1)

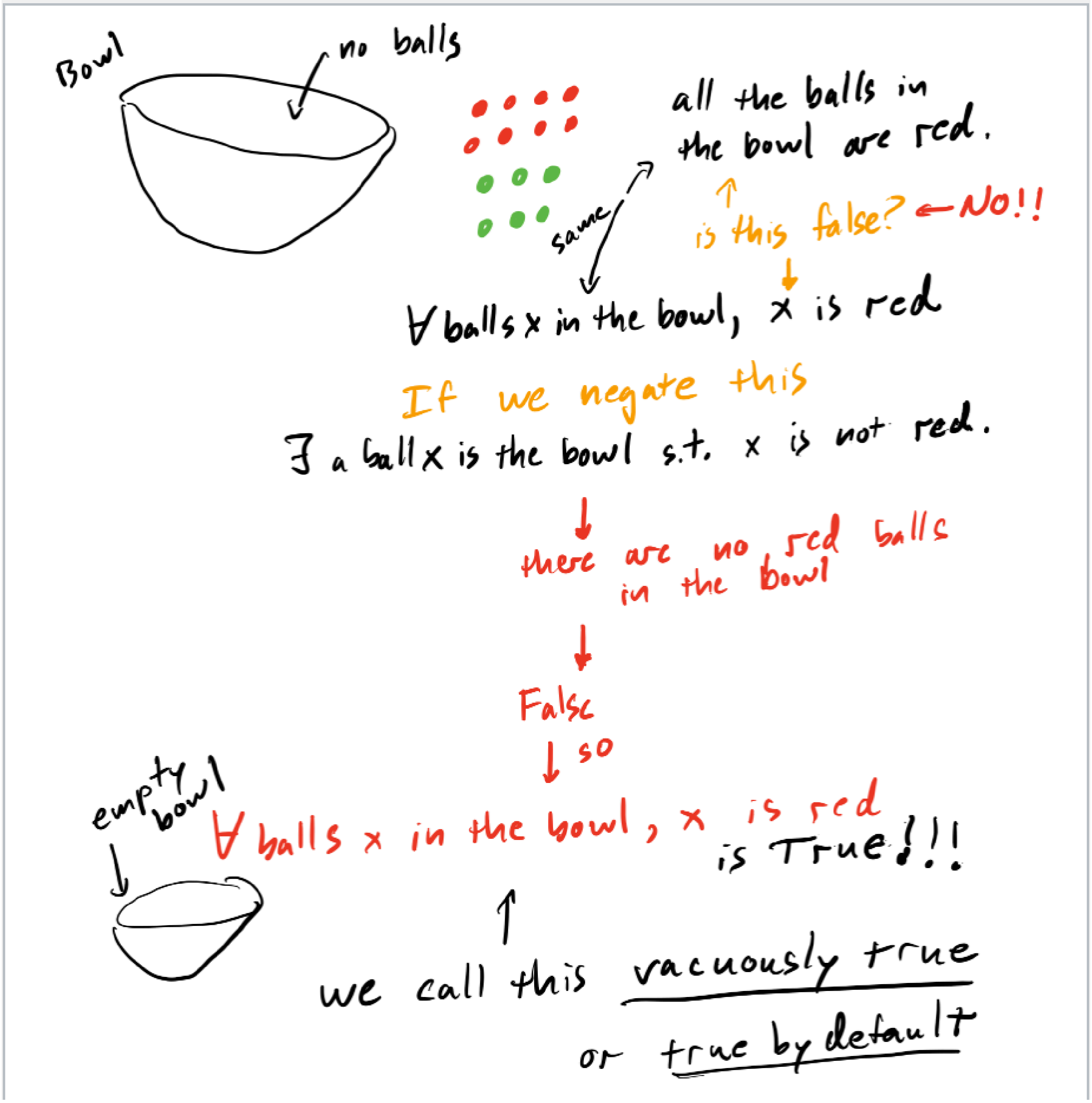
Theorem 2.1.1 Logical Equivalences

Given any statement variables p, q, and r, a tautology **t** and a contradiction **c**, the following logical equivalences hold.

1. *Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2. *Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3. *Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. *Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5. *Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6. *Double negative law:*	$\sim(\sim p) \equiv p$	
7. *Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8. *Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9. *De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10. *Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11. *Negations of* **t** *and* **c**:	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

Vacuously True = True by Default

Example:


Bowl
no balls
all the balls in the bowl are red.
same
is this false? ← No!!
∀ balls x in the bowl, x is red
If we negate this
∃ a ball x is the bowl s.t. x is not red.
there are no red balls in the bowl
False
so
empty bowl
∀ balls x in the bowl, x is red is True!!!
we call this vacuously true
or true by default

Valid Argument Forms:

Valid Argument Forms

Modus Ponens	$p \to q$ p $\therefore q$	**Elimination**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Proof by Division into Cases**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	**Contradiction Rule**	$\sim p \to \mathbf{c}$ $\therefore p$

Set Theory

set = collection of stuff

A = $x \in U \mid P(x)$ where x is in some universal set

some property where P(x) is true

Some Set Examples:

A = $\{x \in \mathbb{Z} |\text{ x is even}\}$

B = $\{\text{dog} \in U | \text{x is a poodle}\}$ where U is the set of all dogs, or the

C = $\{x \in R | 0 < x \leq 5\}$ = (0,5]

D= $\{x \text{ is a dog} | x \text{ is a cat}\}$ = $\emptyset$

$\emptyset$ is the empty set, set with no elements

Subsets in Set Theory

$A \subseteq B \leftrightarrow \forall x, if x \in A \text{ then } x \in B$

A is a subset of B

Example 1:

A = {1,2,3}

B = {-3, -2, -1, 0, 1, 2, 3}

$A \subseteq B$

Example 2:

C = {x is a German Shepard}

D = {x is a dog}
$C \subseteq D$

Example 3:

E = $\{x \in \mathbb{Z} | x \text{ is even}\}$

F = $\{x \in \mathbb{Z} | x = 2t \text{ where } t \in \mathbb{Z}\}$
$E \subseteq F$
$F \subseteq E$

When are sets equal?

$A \subseteq B$ and $B \subseteq A \leftrightarrow A = B$

When are sets not subsets (A not a subset of B)
$A \nsubseteq B \leftrightarrow \exists x \in A \text{ and } x \notin B$

Example 1:

A = {a, b, c, d, e, f, g}

B = {a, b, c, d, e, f}

g is in A but not in B therefore $A \nsubseteq B$

Example 2:

A = $\{n \in \mathbb{Z}, | n = 4k \text{ where } k \in \mathbb{Z}\}$

B = $\{m \in \mathbb{Z}, | m = 2l + 4 \text{ where } l \in \mathbb{Z}\}$

Proof that $A \subseteq B$

Let $x \in A$. Then x = 4k where $k \in \mathbb{Z}$
$x = 4k$
$= 4k - 4 + 4$
$= 2(2k - 2) + 4$

So $x = 2(2k - 2) + 4$ Let l = 2k-2 which is an integer then x = 2l + 4

So $x \in B$

Proof that $B \nsubseteq A$

$\text{Let } x = 2 \in B$ and $x = 2 \notin A$

So A $\neq$ B

Another Proof:
$A = \{n \in \mathbb{Z} | n = 3a \text{ for some } a \in \mathbb{Z}\}$
$B = \{m \in \mathbb{Z} | m = 3b - 6 \text{ for some } a \in \mathbb{Z}\}$

- Let $n \in A$. Then n = 3a for some $a \in \mathbb{Z}$
- n = 3a

- n = 3a+6-6
- n = 3(a+2)-6
- Let a+2 = t which is an integer
- Then n = 3t-6.
- So $n \in B$ and $A \subseteq B$
  Show $B \subseteq A$
- Let $m \in B$ then m = 3b-6
- m = 3(b-2)
- where b - 2 is some integer s
- then m = 3s
- So $m \in A$ and $B \subseteq A$
- Since $A \subseteq B$ and $B \subseteq A$
- A =B

Set Operations

Union: $A \cup B \leftrightarrow x \in A \cup B$ then $x \in A$ or $x \in B$

Intersection: $A \cap B \leftrightarrow x \in A \cap B \text{ then } x \in A \text{ and } x \in B$

Difference: B - A =$\{x \in B | x \notin A\}$

Complement of A: $A^C = \{x \in U | x \notin A\}$

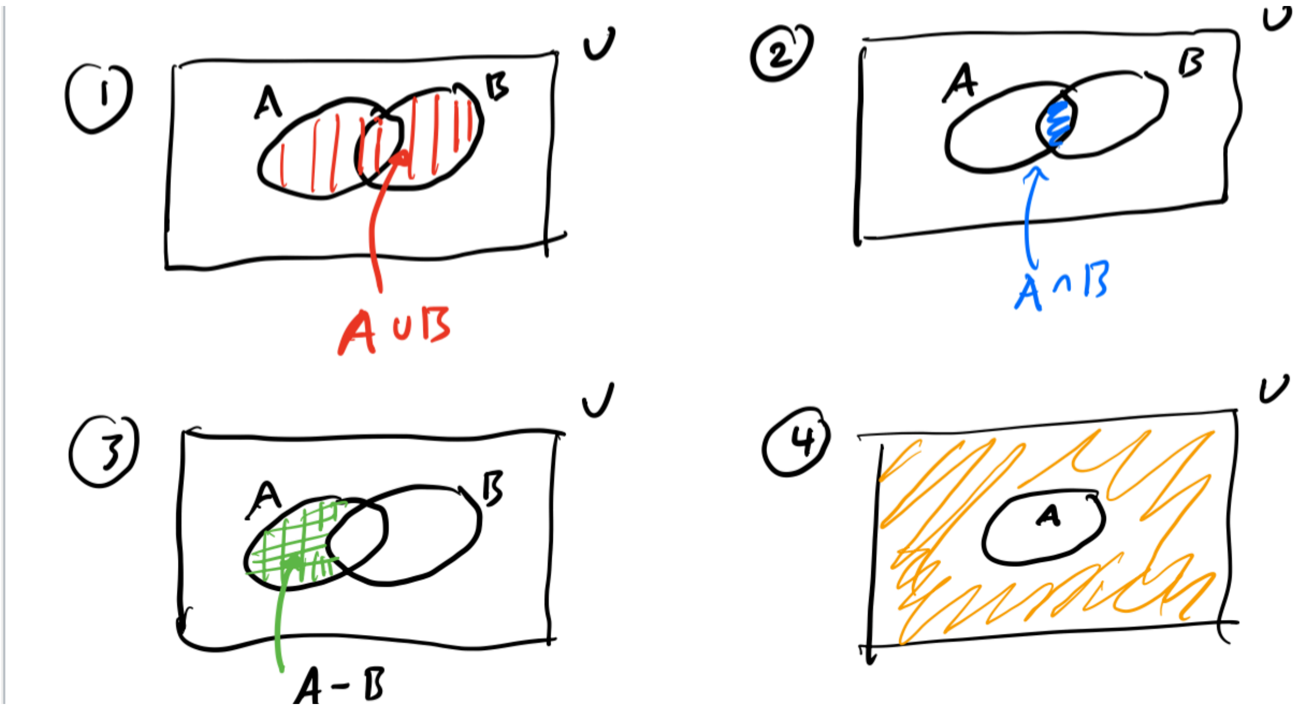
Example 1:

Assume U = {-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5}
A = {1,2,3,4,5}
B = {-1,2,-3,4,-5,6}

$A \cup B = \{1, 2, 3, 4, 5, -1, -3, -5, 6\}$
$A \cap B = \{2, 4\}$
$A - B = \{1, 3, 5\}$
$A^C = \{-5, -4, -3, -2, -1, 0, 6\}$

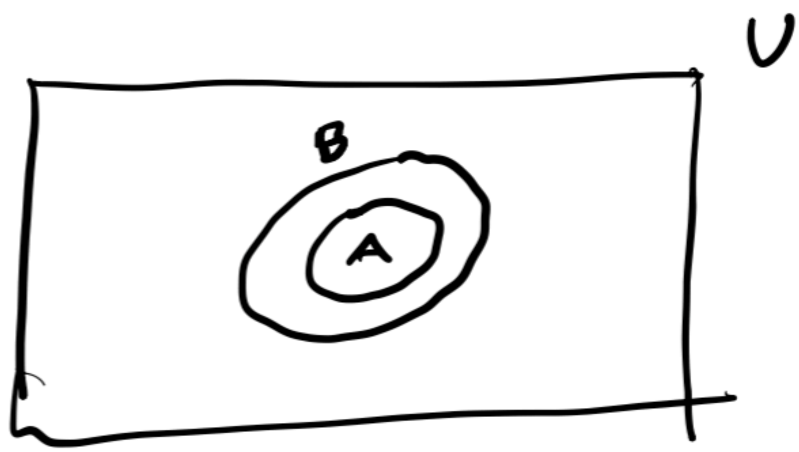
Partitions of a set
$A_1 \cup A_2 \cup A_3 \cup \cdots \cup An = X$
A = {1,2}
B = {3,4}

C = {5,6}
is a partition of X = {1, 2, 3, 4, 5, 6}

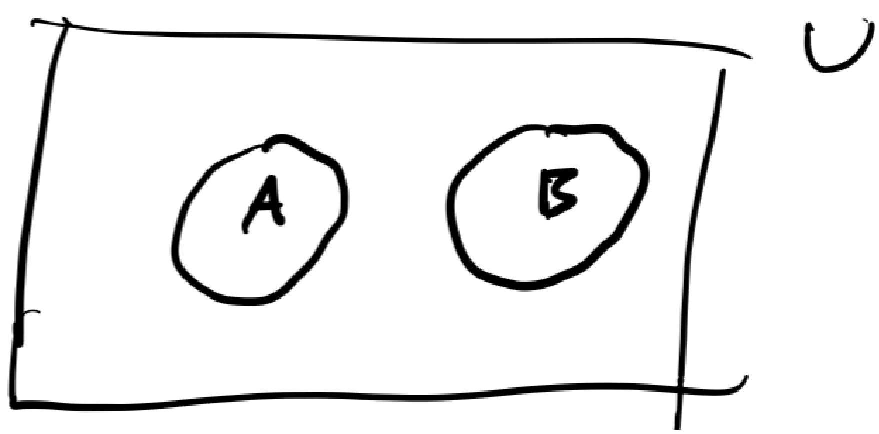


Examples with Venn Diagrams:

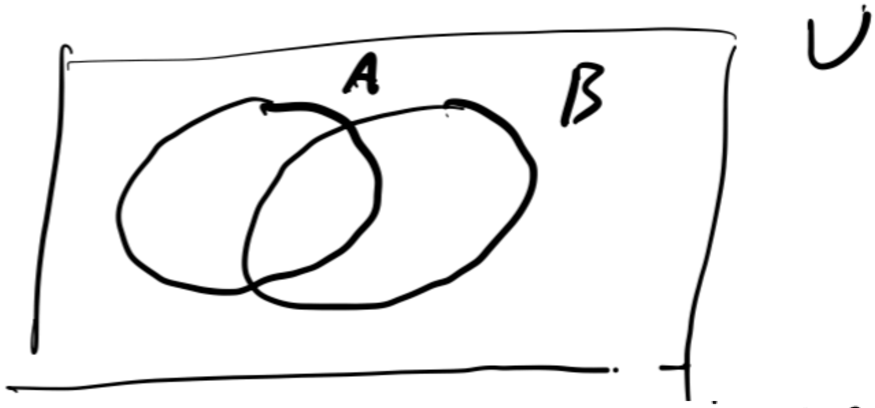
$A \subseteq B$



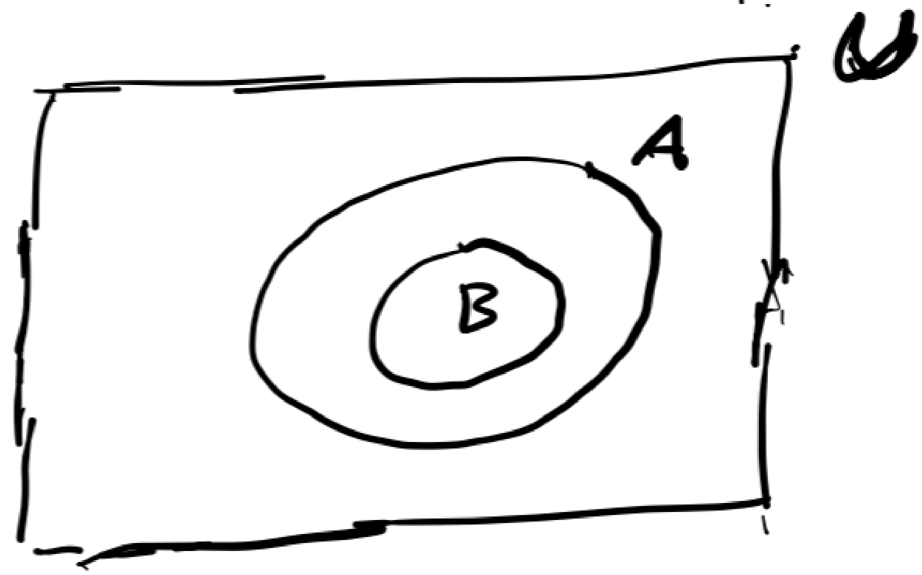
$A \not\subseteq B$



$A \nsubseteq B$



$A \nsubseteq B$



Properties of Sets:

$A \cap B \subseteq A$ and $A \cap B \subseteq B$

$A \subseteq A \cup B$ and $B \subseteq A \cup B$

If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$

Prove $A \cap B \subseteq A$:

Let $x \in A \cap B$, then $x \in A$ and $x \in B$. So $x \in A$ and $A \cap B \subseteq A$

Proof using element Argument

Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Part 1: Prove $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$
Then $x \in B$ or $x \in C$. Then $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$
Hence $x \in A \cap B$ or $x \in A \cap C$
Therefore $x \in (A \cap B) \cup (A \cap C)$ and $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

Part 2: Prove $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$
Let $x \in (A \cap B) \cup (A \cap C)$. Then $x \in A \cap B$ or $x \in A \cap C$

Case 1: If $x \in A \cap B$ then $x \in A$ and $x \in B$
so $x \in A$ and $x \in B \cup C$. Then $x \in A \cap (B \cup C)$

Case 2: If $x \in A \cap C$ then $x \in A$ and $x \in C$
so $x \in A$ and $x \in B \cup C$. Then $x \in A \cap (B \cup C)$
Therefore $x \in A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$
So $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Algebraic proof:

$(A \cup B) - C = (A - C) \cup (B - C)$
$(A \cup B) - C = (A \cup B) \cap C^c$ (set difference law)
$= C^c \cap (A \cup B)$ (commutative law)
$= (C^c \cap A) \cup (C^c \cap B)$ (distributive law)
$= (A \cap C^c) \cup (B \cap C^c)$ (commutative law)
$= (A - c) \cup (B - C)$ (set difference law)

Set Theory Properties & Identities:

Commutative laws:	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Associative laws:	$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$
Distributive laws:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Identity laws:	$A \cap U = A$	$A \cup \emptyset = A$
Complement laws:	$A \cup A^c = U$	$A \cap A^c = \emptyset$
Double complement law:	$(A^c)^c = A$	
Idempotent laws:	$A \cap A = A$	$A \cup A = A$
Universal bound laws:	$A \cup U = U$	$A \cap \emptyset = \emptyset$
De Morgan's laws:	$(A \cap B)^c = A^c \cup B^c$	$(A \cup B)^c = A^c \cap B^c$
Absorption laws:	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements of U and $\emptyset$:	$U^c = \emptyset$	$\emptyset^c = U$
Set Difference Law:	$A - B = A \cap B^c$	

Elementary Number Theory and Methods of Proof

Ground Rules:

- If you add, multiply, subtract integers you get an integer
- If you add multiply, subtract, divide rational numbers you get a rational number
- You can use usual algebra rules: like factoring and distribution

Even and Odd Definition

- Even and Odd Numbers: For all $n \in \mathbb{Z}$
- n is even $\leftrightarrow \exists k \in \mathbb{Z} | n = 2k$
- n is odd $\leftrightarrow \exists k \in \mathbb{Z} | n = 2k + 1$

Example:

- Prove: If a and b are integers where a is odd and b is even then 5a+4b is odd
- $\exists k \in Z | a = 2k + 1$
- $\exists l \in \mathbb{Z} | b = 2l$
- then $5a + 4b = 5(2k + 1) + 4(2l)$
- $10k + 5 + 8l$
- $10k + 8l + 4 + 1$
- $2(5k + 4l + 2) + 1$
- let $5k + 4l + 2$ = t
- thus we get $2(t) + 1$ proving that it is odd

Prime Numbers:

- For all integers p > 1
- p is prime $\leftrightarrow \forall r, s \in \mathbb{Z}$ where r > 0 and s > 0
- If p = rs then r = 1 and s = p
- or r = o and s = 1
- p is composite $\leftrightarrow$ p is not prime
- $\exists r, s \in \mathbb{Z}$ where r >0 and s >0
- such that p = rs and 1<r<p and 1 < s < p

Existential proofs:
simply find a case where it is true

Example 1: There exists a prime number, p such that p is even

- p = 2
  Example 2: There exists an integer n that can be written in two ways as a sum of two primes
- let n = 10 (5+5) & (7+3)

Disproving Universal Conditional Statements

$\neg(\forall x \in D, \text{ if } P(x) \to Q(x)) \equiv \exists x \in D | P(x) \text{ and } \neg Q(x)$

Example: For all $a, b \in \mathbb{R}, \text{ if } a^2 = b^2 \to a = b$
the negation of this is:

- $\exists a, b \in \mathbb{R} | a^2 = b^2 \text{ and } a \neq b$
- Let a = 2, b= -2
- $a^2 = 4, b^2 = 4 \text{ but } a \neq b$

Divisibility

- If $n, d \in \mathbb{Z}$
- n is divisible by d $\leftrightarrow \exists k \in \mathbb{Z} | n = dk \text{ and } d \neq 0$
- n is a multiple of d
- d is a factor of n
- d is a divisor of n
- d divides n = $d|n$ = $\exists k \in \mathbb{Z} | n = dk$

Prove:

- $\forall a, b, c \in \mathbb{Z}$ if a divides b and a divides c then a divides $b + c$

Proof:

- Let $a, b, c \in \mathbb{Z}$ where a divides b and a divides c
- Then $\exists k \in \mathbb{Z} | b = ak$ and $\exists l \in \mathbb{Z} | c = al$
- Then $b + c = ak + al$
- $= a(k + l)$
- Let $k + l = t$ which is an integer. So $b + c = at$ Therefore a divides $b + c$

Theorem:

- Any integer $n > 1$ is divisible by a prime number

Proof

- Suppose $n > 1$ is an integer. If n is prime, we are done. If n isn't prime there exists integers r and s such that $n = r_0 s_0$ with $1 < r_0 < n$ and $1 < s_0 < n$
- If r_0 is prime we are done. If not there exists $r_1, s_1 \in \mathbb{Z}$ such that $r_0 = r_1 s_1$ with $1 < r_1 < r_0$, $1 < s_1 < r_0$
- If r_1 is prime we are done. If not, there exists $r_2, s_2 \in \mathbb{Z}\text{ such that } r_1 = r_2 s_2$ with $1 < r_2 < r_1, 1 < s_2 > r_1$
- If r_2 is prime we are done. If not, then we repeat this process. We get a sequence $r_0, r_1, r_2, r_3, \ldots$
- Where $n > r_0 > r_1 > r_2 > r_3 > \ldots$
- Where $r_i > 1$ So there exists $k \in \mathbb{Z}$ such that $r_0, r_1, r_2, \ldots, r_k$
- (This is a finite list). And r_k must be prime, because if $r_k = r_{k+1}$ then $r_{k+1} = 1$ or r_k and s_{k+1} or r_k. Now $r_k | r_{k-1}$ and $r_{k-1} | r_{k-2}, \ldots, r_1 | r_0, r_0 | n$. Therefore, $r_k | n$

Fundamental Theorem of Arithmetic

- (Unique Factorization of Integers)
- For any integer $n > 1$, there exists prime numbers $p_1, p_2, \ldots, p_k$ and positive integers $e_1, e_2, \ldots, e_k$ such that $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$
- If $p_1 < p_2 < p_3 < \cdots < p_k$ then this factorization is unique. It is called standard factored form in this case
- Example:
  - Write 3,300 in standard factored form
  - $3300 = 100 * 33$
  - $= 10 * 10 * 11 * 3$
  - $= 5 * 2 * 5 * 11 * 3$
  - $= 2^2 * 3 * 5^2 * 11$
- Example 2: Suppose $m \in \mathbb{Z}$
  - $8 * 7 * 6 * 5 * 4 * 3 * 2 * m = 17 * 16 * 15 * 14 * 13 * 12 * 11 * 10$
  - $\text{does } 17 | m?$
  - Yes, because unique factorization and both sides =
  - $2^3 * 7 * 3 * 2 * 5 * 2^2 * 3 * 2 = 2^4 * 5 * 3 * 7 * 2 * 13 * 2^2 * 3 * 11 * 5 * 2$
  - $8 * 7 * 6 * 5 * 4 * 3 * 2 * m = 17 * 16 * 15 * 14 * 13 * 12 * 11 * 10$
  - $m = 17 * 13 * 11 * 2$

Existence of a Prime Divisor

- Let $n > 1$. If n is prime we are done. Otherwise write

$$n = r_0 = r_1 s_1, \quad 1 < r_1 < r_0,\ 1 < s_1 < r_0.$$

- If r_1 is prime we are done. Otherwise write

$$r_1 = r_2 s_2, \quad 1 < r_2 < r_1,\ 1 < s_2 < r_1.$$

- Continuing gives the strictly decreasing chain

$$r_0 > r_1 > r_2 > \cdots > 1.$$

- Since the r_i are positive integers, the process terminates at some r_k.
- That final r_k is prime and

$$r_k \mid r_{k-1} \mid \cdots \mid r_1 \mid r_0 = n.$$

- Hence every integer $n > 1$ has at least one prime divisor.

Fundamental Theorem of Arithmetic

- Every integer $n > 1$ can be written uniquely (up to order) as

$$n \ = \ p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad p_1 < p_2 < \cdots < p_k,\ e_i \geq 1.$$

- **Example 1.** Write 3300 in standard form:

$$3300 = 100 \cdot 33 = 10 \cdot 10 \cdot 11 \cdot 3 = 5 \cdot 2 \cdot 5 \cdot 11 \cdot 3 = 2^2 \cdot 3 \cdot 5^2 \cdot 11.$$

- **Example 2.** Suppose

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \ \cdot m \ = \ 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

  Comparing prime factorizations shows $17 \mid m$ and in fact

$$m \ = \ 17 \cdot 13 \cdot 11 \cdot 2.$$

Quotient–Remainder Theorem

- For any integer n and any positive integer d, there exist unique integers q and r such that

$$n \ = \ d\,q \ + \ r, \quad 0 \ \leq \ r \ < \ d.$$

- Equivalently,

$$\frac{n}{d} = q + \frac{r}{d}, \qquad r = n - d\,q, \qquad d \mid (n - r).$$

- **Example 1.** Divide 621 by 4:

$$621 = 4 \cdot 155 + 1, \quad q = 155,\ r = 1.$$

- **Example 2.** Divide -76 by 3:

$$-76 = 3 \cdot (-26) + 2, \quad q = -26,\ r = 2.$$

Quotient–Remainder Theorem:
For any $n \in \mathbb{Z}$ and $d \in \mathbb{Z}_{>0}$, $\exists!\, q, r \in \mathbb{Z}$ such that $n = dq + r,\ 0 \le r < d$.

Consequence for $d = 6$:
$n = 6q + r,\ r \in \{0,1,2,3,4,5\} \implies n \equiv r \pmod 6$,
so every integer is exactly one of $6q,\ 6q+1,\ 6q+2,\ 6q+3,\ 6q+4,\ 6q+5$.

Odd Squares are $1 \pmod 8$:
If n is odd then $n = 2k+1,\ \ n^2 = (2k+1)^2 = 4k(k+1)+1$.
Since $k(k+1)$ is even, $4k(k+1) = 8m,$ so $n^2 = 8m+1$.

Quotient–Remainder Theorem

- For any integer n and positive integer d, there exist unique integers q, r such that

$$n = d\,q + r, \quad 0 \le r < d.$$

- Equivalently, $\dfrac{n}{d} = q + \dfrac{r}{d}$ and $r = n - d\,q$, so $d \mid (n - r)$.
- **Example:** $621 = 4 \cdot 155 + 1$, hence $q = 155$, $r = 1$.
- **Example:** $-76 = 3 \cdot (-26) + 2$, hence $q = -26$, $r = 2$.

Existence of a Prime Divisor

- Let $n > 1$. If n is prime we are done. Otherwise write

$$n = r_0 = r_1 s_1, \quad 1 < r_1 < r_0,\ 1 < s_1 < r_0.$$

- If r_1 is prime we are done. Otherwise write

$$r_1 = r_2 s_2, \quad 1 < r_2 < r_1,\ 1 < s_2 < r_1.$$

- Continuing yields a strictly decreasing chain

$$r_0 > r_1 > r_2 > \cdots > r_k > 1,$$

which must terminate at some r_k.

- That final r_k is prime and

$$r_k \mid r_{k-1} \mid \cdots \mid r_1 \mid r_0 = n.$$

- Hence every integer $n > 1$ has at least one prime divisor.

Fundamental Theorem of Arithmetic

- Every integer $n > 1$ can be written uniquely (up to order) as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad p_1 < p_2 < \cdots < p_k, \; e_i \geq 1.$$

- **Example 1:**
$3300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11.$
- **Example 2:** If

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \;\cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10,$$

then comparing prime factorizations shows $17 \mid m$ and

$$m = 17 \cdot 13 \cdot 11 \cdot 2.$$

Proofs:

9. For all integers $a, b, c, \; (a \mid b \;\wedge\; a \mid c) \implies a^2 \mid (bc)$.

Proof. Suppose $a \mid b$ and $a \mid c$. Then $\exists\, k, \ell \in \mathbb{Z}$ such that

$$b = k\,a, \quad c = \ell\,a.$$

Multiplying gives

$$bc = (k\,a)(\ell\,a) = (k\ell)\,a^2.$$

Let $t = k\ell \in \mathbb{Z}$. Then $bc = t\,a^2$, so $a^2 \mid (bc)$.

10. For all integers $n, \; n^3$ odd $\implies n$ odd.

Proof (by contrapositive). We prove "if n is even then n^3 is even." Suppose n is even, so $n = 2k$ with $k \in \mathbb{Z}$. Then

$$n^3 = (2k)^3 = 8k^3 = 2\big(4k^3\big),$$

which is even. Hence the contrapositive holds, and the original statement is true.

11. The product of a rational number and an irrational number is irrational.

Proof (by contradiction). Assume to the contrary that $x \in \mathbb{Q}$, $y \notin \mathbb{Q}$, but $xy \in \mathbb{Q}$. Write

$$x = \frac{a}{b}, \quad a, b \in \mathbb{Z},\, b \neq 0, \quad xy = \frac{c}{d}, \quad c, d \in \mathbb{Z},\, d \neq 0.$$

Then

$$\frac{a}{b}\, y = \frac{c}{d} \quad \Longrightarrow \quad y = \frac{c}{d}\, \frac{b}{a} = \frac{cb}{da},$$

which is rational, contradicting that y is irrational.

12. For all integers $n \geq 1$, $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

Proof (by induction).
Base case $n = 1$:

$$\sum_{i=1}^{1} \frac{1}{i(i+1)} = \frac{1}{1 \cdot 2} = \tfrac{1}{2}, \quad \left.\frac{n}{n+1}\right|_{n=1} = \tfrac{1}{2}.$$

Inductive step: Assume for some $k \geq 1$ that

$$\sum_{i=1}^{k} \frac{1}{i(i+1)} = \frac{k}{k+1}.$$

Then

$$\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} = \frac{k(k+2)+1}{(k+1)(k+2)} = \frac{(k+1)^2}{(k+1)(k+2)} = \frac{k+1}{k+2}.$$

This completes the induction.