CMSC250 - Lecture Notes

Ash Dorsey
ash@ash.lgbt

These are based on Max's lecture notes, with added commentary and typed instead of written.

Contents

Numbers

There are many different types of numbers. For example, from Java, you know `ints` and `floats` store different types of numbers. This is also the case in math.

Whole numbers are all integers greater than or equal to 0[1], and this collection is denoted by $\mathbb{W}$.[2] The natural numbers ($\mathbb{N}$) are the same thing.[3]

But what about negative numbers? Then, it's simply the integers, denoted $\mathbb{Z}$.

But we don't always deal in nice, clean numbers. Division does not always work out, so we need to add more. Combining two integers into a fraction becomes the rationals, denoted $\mathbb{Q}$.

Unfortunately, this still does not cover all numbers. $\sqrt{2}$ and π are not rational but certainly numbers. Both numbers are part of the reals, denoted $\mathbb{R}$, which is an entire continuum of numbers.

But yet, this still does not cover all numbers. What are the solutions to the quadratic $x^2 + 2x + 2 = 0$? They do not exist in the reals, but they do exist in complex numbers, as $-1 - i$ and $-1 + i$, where $i = \sqrt{-1}$. We call this set the complex numbers, denoted $\mathbb{C}$.[4]

There is also a subset (a smaller piece) of complex numbers where the numbers are purely imaginary. These are called imaginary numbers and are often denoted $\mathbb{I}$, but this is not always true (it may also refer to strictly irrational numbers).

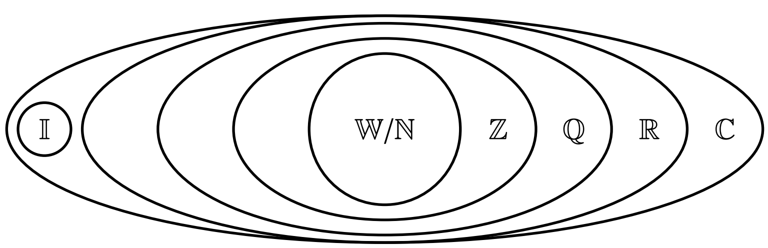


Figure 1: A handy diagram of the different types of numbers.

[1] This is debated. According to Wikipedia, it's American elementary school teachers' fault.

[2] Not always

[3] Shockingly, this is also debated, although, in the real world, nobody talks about whole numbers and mostly talks about naturals. Also, when defining number systems, they always start with zero, so therefore it is "natural" to include zero.

[4] It is algebraically closed, which is a unique property. This means that for any nonconstant polynomial, there will be a solution in the set, which has a lot of other interesting effects. However, it does lose an ordering compared to the reals.

Bases

How do we read numbers now? Via a positional base system, specifically base 10.

For example, when reading the number "563," it means $5 \cdot 100 + 6 \cdot 10 + 3 \cdot 1$. This can be generalized: for example, $683421 = 6 \cdot 10^5 + 8 \cdot 10^4 + 3 \cdot 10^3 + 4 \cdot 10^2 + 2 \cdot 10^1 + 2 \cdot 10^0$.

Even more generally, for each digit in a number, you raise the base to the power of the position (zero-indexed from the right), then multiply by the value of the digit.

This can work in other bases, like base 2 (binary):

$$1101_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 13_{10}$$

Also, subscripts are often used on numbers to indicate their base, which would be confusing otherwise.

Here is another example, now with base 16. It uses a different set of characters:

Value	Digit
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Value	Digit
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

But applying it is very similar:

$$4\text{D}1 = 4 \cdot 16^2 + 13 \cdot 16 + 1 = 1233$$

Propositional Logic

Propositional logic is a type of algebra that works with boolean values (true/false), compared to typical algebra, where you work with, e.g., real numbers.

Operators

Like normal algebra has operations like addition and multiplication, propositional logic also has operations.

Not: $\neg / \sim$

It is a unary operator, which means that it does an operation on only one thing. When negating a variable, you get the opposite. Let's write out the possibilities:

$$\neg \text{ True} \equiv \text{False}$$
$$\neg \text{ False} \equiv \text{True}$$

The $\equiv$ means "equivalent to."

To represent this situation formally, we can create a truth table:

Input	Output
A	$\neg A$
True	False

False	True

In a truth table, you give all inputs on the left side and all resulting outputs on the right side. As expected for a negation/not, you can see that you get the opposite value after negation.

And: $\wedge$
This is also known as a conjunction and is a binary operator, which means it works on two inputs. It returns true when both inputs are true. Once again, let's write out the possibilities:

$$\text{True} \wedge \text{True} \equiv \text{True}$$
$$\text{True} \wedge \text{False} \equiv \text{False}$$
$$\text{False} \wedge \text{True} \equiv \text{False}$$
$$\text{False} \wedge \text{False} \equiv \text{False}$$

We can also make this into a truth table:

Inputs		Output
A	B	$A \wedge B$
True	True	True
True	False	False
False	True	False
False	False	False

We can also derive the negation of that:

Inputs		Output
A	B	$\neg(A \wedge B)$
True	True	False
True	False	True
False	True	True
False	False	True

Or: $\vee$
This is also known as a disjunction and is a binary operator. If either input is true, it returns true.

Inputs		Output
A	B	$A \vee B$
True	True	True
True	False	True
False	True	True
False	False	False

Exclusive or (xor): $\oplus$
True output is when only one of its inputs is on, not both.

Inputs		Output
A	B	$A \oplus B$
True	True	False
True	False	True
False	True	True
False	False	False

How can this be formed via negations, conjunctions and disjunctions?

Either A is on and B is off, or A is off and B is on.[5]

Translating this into propositional logic:

$$(A \land \neg B) \lor (\neg A \land B)$$

Implies: $\rightarrow$
$A \rightarrow B$ means that if A is true, then B is true. This means that if A is false, B can be whatever, and if A is true, B must be true, leading to the following truth table:

Inputs		Output
A	B	$A \rightarrow B$
True	True	True
True	False	False
False	True	True
False	False	True

For example, if x is some object, $x \text{ is a banana} \rightarrow x \text{ is a fruit}$ is an entirely truthful statement for all objects since all bananas are fruits. This does not mean that all objects are fruits or that all fruits are bananas, just that if something is a banana, it is a fruit as well.

Furthermore, you know that if something is not a fruit, it is not a banana. This can be written like $\neg B \rightarrow \neg A$ and, generally $A \rightarrow B \equiv \neg B \rightarrow \neg A$.

Anyways, how can this be formed via negations, conjunctions and disjunctions?

This one has only one false, so it's probably easiest to target that and then invert it.

$$\neg(A \land \neg B) \overset{\text{DeMorgan's Law}}{\equiv} \neg A \lor B$$

Properties

1. Identity: $A \land \text{True} \equiv A$ and $A \lor \text{False} \equiv A$
2. Idempotent Laws: $A \land A \equiv A$ and $A \lor A \equiv A$
3. Tautology: $A \lor \neg A \equiv \text{True}$
4. Contradiction: $A \land \neg A \equiv \text{False}$
5. Universal Bound: $A \lor \text{True} \equiv \text{True}$ and $A \land \text{False} \equiv \text{False}$
6. Communtative: $A \lor B \equiv B \lor A$
7. Double Negative: $\neg(\neg A) \equiv A$
8. Absorption Laws: $A \lor (A \land B) \equiv A$ and $A \land (A \lor B) \equiv A$
9. DeMorgan's Laws: $\neg(A \lor B) \equiv \neg A \lor \neg B$ and $\neg(A \land B) \equiv \neg A \lor \neg B$
10. Distributive Laws: $A \land (B \lor C) \equiv (A \land B) \lor (A \land C)$ and $A \lor (B \land C) \equiv (A \lor B) \land (A \lor C)$

[5] The lecture notes went a different route and ended up with $(A \lor B) \land \neg(A \land B)$, which is equivalent.

It is highly suggested that you create truth tables, particularly for DeMorgan's Laws, to prove that these are correct.

Showing Equivalences

Example
Show the following:

$$(A \lor B) \to C \equiv (C \lor \neg A) \land (C \lor \neg B)$$

Doing it:

$$\begin{aligned} &(A \lor B) \to C \\ \neg&(A \lor B) \lor C && \text{Equivalence for Implies} \\ &(\neg A \land \neg B) \lor C && \text{DeMorgan's} \\ &C \lor (\neg A \land \neg B) && \text{Commutativity} \\ &(C \lor \neg A) \land (C \lor \neg B) && \text{Distributive Property} \end{aligned}$$

$$\blacksquare$$

Example: Contrapositive
Show that the contrapositive is equivalent to the normal form. In other words:

$$A \to B \equiv \neg B \to \neg A$$

We can do so as such:

$$\begin{aligned} A \to B & \\ \neg A \lor B & \quad \text{Equivalence for Implies} \\ B \lor \neg A & \quad \text{Commutativity} \\ \neg\neg B \lor \neg A & \quad \text{Double Negation} \\ \neg B \to \neg A & \quad \text{Equivalence for Implies} \end{aligned}$$

Arguments

Given a list of axioms, statements you assume to be true, prove a conclusion. You do this through rules of inference, rules for manipulating logical statements while preserving the truth value.

For example:

$$\begin{array}{l} \text{A} \to \text{B} \leftarrow \text{axiom} \\ \text{A} \leftarrow \text{axiom} \\ \hline \therefore \text{B} \leftarrow \text{conclusion} \end{array}$$

This is true because if A is true, then because $A \to B$, B is true. This is called modus ponens.

See the laws sheet posted on Canvas for all the rules of inference.

Example
Prove:

$$\begin{array}{l} \text{A} \land \text{B} \\ \neg\ \text{C} \to \text{D} \\ \neg\ \text{A} \lor \neg\ \text{D} \\ \hline \therefore \text{C} \end{array}$$

1. $A \land B$
2. $\neg C \to D$
3. $\neg A \lor \neg D$

4. A Specialization on 1
5. $\neg D$ Elimination on 3, 4
6. $\neg\neg A$ Modus Tollens on 2, 5
7. A Double Negation on 6

Example
Prove:

$$\begin{array}{l} \text{A} \rightarrow \text{B} \\ \neg\ \text{C} \lor \text{D} \\ \text{B} \rightarrow \neg\ \text{D} \\ \hline \therefore \neg\ \text{A} \lor \neg\ \text{C} \end{array}$$

1. $A \to B$
2. $\neg C \lor D$
3. $B \to \neg D$
4. $A \to \neg D$ Transitivity on 1, 3
5. $\neg\neg D \lor \neg C$ Commutativity and Double Negation on 2
6. $\neg D \to \neg C$ Equivalence for Implies on 5
7. $A \to \neg C$ Transitivity on 6, 4
8. $\neg A \lor \neg C$ Equivalence for Implies on 7

Sound Inference Rules

All the equivalences on the laws sheet are sound inference rules. What does this mean? A rule is sound if the new statement is true whenever the original statement is true.

For example, this is an unsound inference rule:

$$\begin{array}{l} \text{A} \rightarrow \text{B} \\ \hline \therefore \text{B} \rightarrow \text{A} \end{array}$$

We can check this via a truth table:

A	B	$A \to B$	$B \to A$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

This inference rule is unsound because of the region highlighted in blue, where the first is true and the second is false.

Another example, this time of a sound rule:

$$\begin{array}{l} \text{A} \land \text{B} \\ \hline \therefore \text{A} \end{array}$$

A	B	$A \land B$	A
T	T	T	T
T	F	F	T
F	T	F	F
F	F	F	F

As you can see, there are no rows where $A \land B$ is true but A is not, so this rule is valid.

Example

Is this rule valid:

$$\frac{(A \lor B) \land (\neg B \lor C)}{\therefore \text{A} \lor \text{C}}$$

A	B	C	$(A \lor B) \land (\neg B \lor C)$	$A \lor C$
T	T	T	T	T
T	T	F	F	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	F	F
F	F	T	F	T
F	F	F	F	F

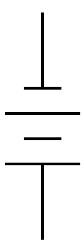
Yes, it is!

Circuits

Circuits are a direct application of propositional logic. Circuits like those you will design in class can be used for real things, like door switches or seven-segment displays. But first, you need to know the basic symbols used when drawing a circuit diagram.

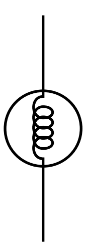
Basic Symbols

Battery



The longer side is the positive terminal, and the shorter is the negative. This can power other components, like light-bulbs.

Lightbulb



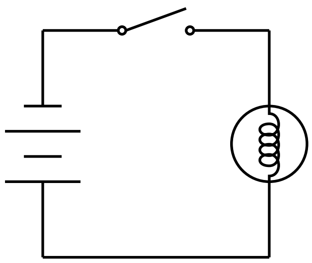
When the lightbulb is powered, it lights.

Switch

This is a switch. When it is closed, electricity flows through it. When it is open, like it is above, no electricity flows.

Basic Circuits

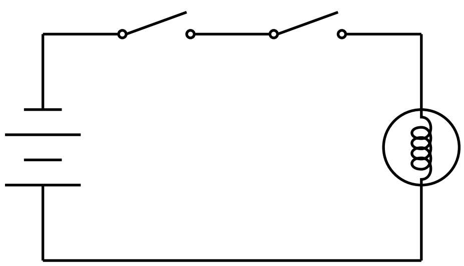
Now that we know a few basics, we can actually create a circuit.



Behold a circuit: when the switch is on, the light is on. When the switch is off, the light is off.

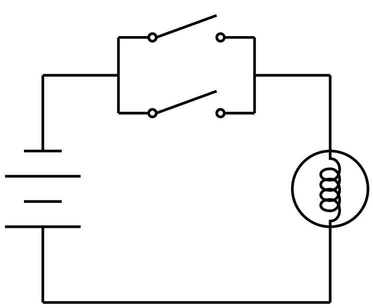
From these basics, we can construct gates.

An and gate can be constructed by putting two switches in series (right after each other):



Only if both switches are on will the lightbulb turn on.

An or gate can be constructed with two switches in parallel (beside each other):



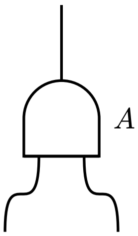
If either switch is on, the lightbulb is on (including if both switches are on).

But writing out circuits like this gets annoying, particularly because you can't throw multiple switches at once if you have the same input more than once, so it is simplified for digital logic.

Digital Logic Gates

AND

Here is an and gate:

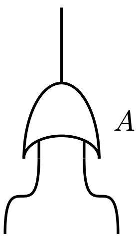


$A \wedge B$

Like the operator, it takes in two outputs, and outputs on iff both inputs are on.

OR

Here is an or gate:

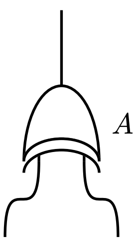


$A \vee B$

Like the operator, it takes in two outputs, and outputs on if either input is on.

XOR

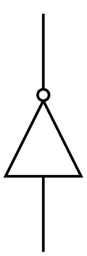
Here is a xor gate:



$A \oplus B$

Like the operator, it takes in two outputs, and outputs on if either input is on, but not if both are on.

NOT

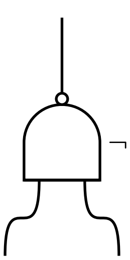


$\neg A$

Like the operator, it takes in one input and negates it.

NAND

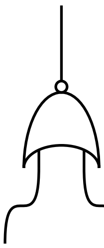
Not and:



$\neg(A \wedge B)$

NOR

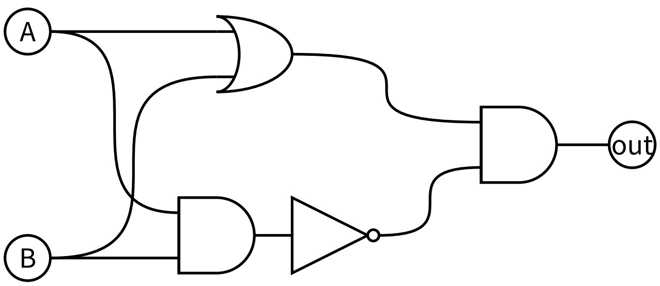
Not or:



Note that a circle signifies negation of the output.

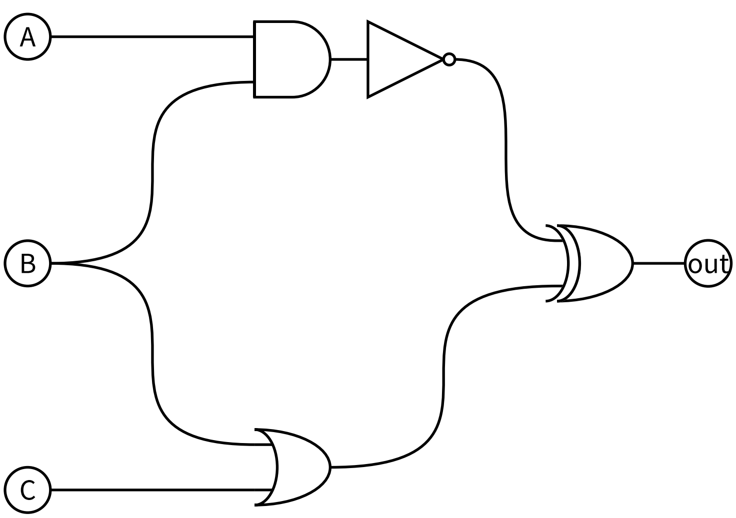
Digital Logic Circuit

We know $A \oplus B \equiv (A \lor B) \land \neg(A \land B)$. Let's create this as a circuit.



Now, we have an exclusive or circuit. Isn't that exciting? Try making a truth table via the circuit (label inputs). It should be the same as the truth table for XOR.

Another one: $\neg(A \land B) \oplus (C \lor B)$



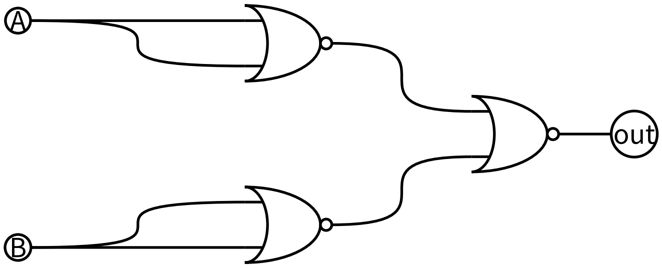
Functional completeness

Either NAND or NOR gates can be used to create any other gate.

For example, using $\downarrow$ as a symbol for NOR:

$$A \land B \equiv \neg(\neg A \lor \neg B) \equiv (\neg A) \downarrow (\neg B) \equiv (A \downarrow A) \downarrow (B \downarrow B)$$

In a circuit, this can be written like this:



First Order Logic

Set notation

- $\{1, 2, 3\}$ is a set of 3 elements
- Sets are collections of nonrepeated elements
- $\{\}$ or $\varnothing$ is the empty set.
- $x \in \{1, 2, 3\}$ means that x is an element of the set $\{1, 2, 3\}$ which means $x = 1 \vee x = 2 \vee x = 3$ here.

Statements

A statement or proposition is a sentence that can be evaluated to a boolean.

For example:

- $2 + 2 = 4$ ✓
- $1 + 0 = 2$ ✓
- I have $\geq \$20$ in my wallet ✓
- $x \geq 20$ ✗
- Red is the best color ✗
- Let $x =$ money in wallet, $x \geq 20$ ✓

Quantifiers

When describing events, we often need to state something as true for all things or perhaps just some things.

We can do this with $\forall$ (for all) and $\exists$ (exists). For instance, let's write the statement that all real numbers squared are nonnegative:

$$\forall x \in \mathbb{R}, x^2 \geq 0$$

Note that in this class you must *always* include the set.

These quantifiers can convert non-statements into statements: $x^2 \geq 0$ is not a statement, but $\forall x \in \mathbb{R}, x^2 \geq 0$ is.

What about complex numbers:

$$\forall x \in \mathbb{C}, x^2 \geq 0$$

But this statement is false, although it is a statement.

What about saying there is an object that weighs more than a ton?

$$\exists x \in \text{objects}, x \text{ weighs} \geq 1 \text{ ton}$$

What about saying there is some real number squared that is nonpositive?

$$\exists x \in \mathbb{R}, x^2 \leq 0$$

We can also define functions. For example:

$$P(x) : x > 20$$

Then $P(2)$ is a statement (evaluates to false). This is often useful when making a complicated statement, for example, if a number is prime.

Unwrapping

If you have a statement like $\forall x \in \{1,2,3\}, P(x)$, then you know $P(1) \land P(2) \land P(3)$. Similarly, for there exists, $\exists x \in \{1,2,3\}, P(x) \equiv P(1) \lor P(2) \lor P(3)$.

This can be expanded to infinite sets as well:

$$\forall x \in \mathbb{N}, P(x) \equiv P(0) \land P(1) \land P(2) \land \cdots$$
$$\exists x \in \mathbb{N}, P(x) \equiv P(0) \lor P(1) \lor P(2) \lor \cdots$$

This leads us to some rules:

Specialization

For example, $\forall x \in \{1,2,3\}, P(x) \to P(1)$. More formally, $\forall x \in S, P(x) \to \exists y \in S, P(y)$.

Generalization

For example, $P(1) \to \exists x \in \{1,2,3\}, P(x)$.

More formally, this is like $\exists y \in S, P(y) \to \exists x \in S, P(x)$, but that's not very helpful.

Negation

DeMorgan's rule shows that $\neg(P \land Q) \equiv \neg P \lor \neg Q$. We can apply this infinitely to a qualifier like so:

$$\neg(\forall x \in \{1,2,3\}, P(x)) \equiv \neg(P(1) \land P(2) \land P(3)) \equiv \neg P(1) \lor \neg P(2) \lor \neg P(3) \equiv \exists x \in \{1,2,3\}, \neg P(x)$$

Generally, $\neg(\forall x \in S, P(x)) \equiv \exists x \in S, \neg P(x)$.

This also works in reverse: $\neg(\exists x \in S, P(x)) \equiv \forall x \in S, \neg P(x)$.

Multiple Quantifiers

If you have multiple of the same quantifier next to each other, you can exchange them.

This means that $\forall x \in A, \forall y \in B, P(x,y) \equiv \forall y \in B, \forall x \in A, P(x,y)$, **and** $\exists x \in A, \exists y \in B, P(x,y) \equiv \exists y \in B, \exists x \in A, P(x,y)$

However, this is not the case for dissimilar quantifiers. For example, compare the following two statements:

$$\forall x \in P, \exists y \in P, L(y,x)$$
$$\exists y \in P, \forall x \in P, L(y,x)$$

Let P be the set of people and have $L(y,x)$ be the function that tells you if y likes x.

In the first example, every person has someone who likes them (note that it may be themselves!). In the second example, there is one person who likes everyone. These are different situations, and as such, different quantifiers cannot be interchanged.

Sets

What is a set?

A set is an unordered collection of unique elements.

This means that $[1,0,4,5]$[6] is not a set, as it is ordered, and $\{1,1,2\}$ is not a set because it has duplicates.

$\{1,2,3\}$ is a set because it is unordered and has unique elements.

[6] Square brackets indicate that it is ordered

Because it is unordered, $\{1,2,3\} = \{3,2,1\}$

Terms

Empty Set
The set with nothing in it:

$$\{\} = \varnothing$$

Subset
If all elements in one set are inside another:

$$A \subseteq B$$

Proper/Strict Subset
If all elements in one set are inside another, and the sets are not equal:

$$A \subseteq B \wedge A \neq B \equiv A \subsetneq B$$

Set Intersection
The intersection of two sets is all the elements the sets have in common:

$$A \cap B$$

If the sets have nothing in common, the result is the empty set.

For example, $\{1,2,3\} \cap \{2,3,4\} = \{2,3\}$.

This is the definition:

$$\{x \mid x \in A \wedge x \in B\} \equiv A \cap B$$

Set Union
The union of two sets is all the elements in both sets:

$$A \cup B$$

For example, $\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\}$.

This is the definition:

$$\{x \mid x \in A \vee x \in B\} = A \cup B$$

Set Difference
All the elements in one set that are not in the other:

$$A - B$$

For example, $\{1,2,3,4\} - \{2,5,6,7\} = \{1,3,4\}$

Set Partitions
A grouping of the elements in a set so every element in the set is in one subset.

For example, partitions of $\{1,2,3,4,5,6\}$ include $\{\{1,2,3\},\{4,5,6\}\}$, $\{\{1,5,6\},\{2,3,4\}\}$ and $\{\{1\},\{2\},\{3\},\{4\},\{5\},\{6\}\}$.

Set Cardinality
Cardinality indicates the size of the set. It's the number of things in the set.

$$A = \{1,2,3\} \to |A| = 3$$

Set Compliments

The complement of a set is everything that is not in that set:

$$A^C = A'$$

You must set a universe (set of everything). It is usually denoted by U. Under most axioms, it is impossible to construct a true universal set, so you must always set a U, although it may be implicit.

$A = \{1, 2, 3\} \land U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \to A^C = \{4, 5, 6, 7, 8, 9\}$

Disjoint Sets

Two sets are disjoint if they have no elements in common.

In other words, $A \cap B = \varnothing$.

Set Membership

$x \in A$ means that x is in A and $x \notin A$ means that x is *not* in A.

Power Set

The power set of A is the set of every subset of A:

$$\mathcal{P}(A)$$

For example:

$$\mathcal{P}(A) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Symbolically, this means:

$$x \in \mathcal{P}(A) \iff x \subseteq S$$

Cartesian Products

The cartesian product of two sets is a set of tuples such that each tuple corresponds to one pair from each set:

$$A \times B$$

For example:

$$A = \{a, b, c\}$$
$$B = \{1, 2, 3\}$$
$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$$

Symbolically, this means:

$$A \times B = \{(a, b) \mid a \in A \land b \in B\}$$

Note that $A \times B \neq B \times A$.

Set Builder Notation

To the left of the $|$, you have an expression with variables to fill in; on the right, you have an expression constraining the variables.

For example, all integers greater than 2:

$$\{x \mid x \in \mathbb{Z}, x > 2\}$$

Exercise

- All even integers
  - $\{2x \mid x \in \mathbb{Z}\}$ or $\{x \mid x \in \mathbb{Z} \land 2|x\}$

- Every third positive integer, starting at 2.
  - $\{3x + 2 \mid x \in \mathbb{Z} \land x \geq 0\}$
- The set of all numbers divisible by three and five
  - $\{x \mid 3|x \land 5|x\}$

Cardinality

Often, we want to know if two sets are the same size. For finite sets, this is pretty easy: count them. But what do you do for infinite sets?

One way to do this is to construct a bijection between two sets.

Bijections

A bijection is a function that maps each element from set A onto set B and vice-versa.

Exercise

The set of integers is infinite, and so is the set of all even integers. Which one is bigger?

Create a function that maps each integer to a corresponding even integer:

$$\begin{gathered} 0 \leftrightarrow 0 \\ 1 \leftrightarrow 2 \\ -1 \leftrightarrow -2 \\ 2 \leftrightarrow 4 \\ -2 \leftrightarrow -4 \\ 3 \leftrightarrow 6 \\ -3 \leftrightarrow -6 \\ \vdots \end{gathered}$$

Multiplying each integer by two seems to work! We now have one integer for every even integer and one even integer for every integer.

Countably Infinite

The natural numbers and any sets of the same cardinality are called countably infinite.

Are the rationals? Yes!

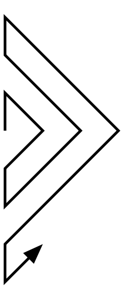
Rational Countability

We know that the rational numbers can be represented by $\frac{a}{b}$ where $a \in \mathbb{Z}, b \in \mathbb{N}$.

This means that $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}|$.

Furthermore, we know that all integers can be represented by the rationals, so therefore $|\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}|$.

Simply zigzag around to reach all of the pairs in $\mathbb{Z} \times \mathbb{N}$:



Are the real numbers countably infinite? No, by Cantor's diagonalization argument.

Set Identities

Just like with propositional logic, sets have their own set of equivalences:

Property	Rule
Commutative	$A \cup B = B \cup A$ and $A \cap B = B \cap A$
Associative	$A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$
Distribitive	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Identity	$A \cup \varnothing = A$ and $A \cap U = A$
Complement	$A \cup A^C = U$ and $A \sec A^C = \varnothing$
Double Complement	$\left(A^C\right)^C = A$
Idempotent	$A \cup A = A$ and $A \cap A = A$
Universal Bound	$A \cup U = U$ and $A \cap \varnothing = \varnothing$
DeMorgan's	$(A \cap B)^C = A^C \cup B^C$ and $(A \cup B)^C = A^C \cap B^C$[7]
Absorption	$A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$
Complement of $\varnothing$ and U	$U^C = \varnothing$ and $\varnothing^C = U$
Set Difference	$A - B = A \cap B^C$

Practice

Prove that $A - (B \cup C) = (A - B) \cap (A - C)$.

$$\begin{aligned}
& A - (B \cup C) & \\
&= A \cap (B \cup C)^C & \text{Set Difference} \\
&= A \cap \left(B^C \cap C^C\right) & \text{DeMorgan's} \\
&= (A \cap A) \cap \left(B^C \cap C^C\right) & \text{Idempotent} \\
&= \left(A \cap B^C\right) \cap \left(A \cap C^C\right) & \text{Commutative and Associative} \\
&= (A - B) \cap \left(A \cap C^C\right) & \text{Set Difference} \\
&= (A - B) \cap (A - C) & \text{Set Difference}
\end{aligned}$$

Prove that $\left(\left(A^C \cup B^C\right) - A\right)^C = A$.

$$\begin{aligned}
& \left(\left(A^C \cup B^C\right) - A\right)^C & \\
&= \left((A \cap B)^C - A\right)^C & \text{DeMorgan's} \\
&= \left((A \cap B)^C \cap A^C\right)^C & \text{Set Difference} \\
&= (A \cap B) \cup A & \text{DeMorgan's} \\
&= A \cup (A \cap B) & \text{Commutative} \\
&= A & \text{Absorption}
\end{aligned}$$

Set Equality

What does it mean for sets to be equal anyway? By definition, $A = B \iff A \subseteq B \land B \subseteq A$.

This can be shown by further going down to the definition of subset and showing that if a variable is in A, it is in B, and if a variable is in B, show that it is in A.

Example

Show that $A \cup (A \cap B) = A$.

[7] Remember that you cannot remove parenthesis in most cases when simplifying.

To prove $(A \cup (A \cap B)) \subseteq A$, let $x \in (A \cup (A \cap B))$.

Therefore, $x \in A \vee x \in (A \cap B)$.

Therefore, $x \in A \vee (x \in A \wedge x \in B)$

Therefore, by absorption, $x \in A$.

To prove $A \subseteq (A \cup (A \cap B))$, let $x \in A$.

Since the proposed superset is unioned with A, anything in A is a part of the superset.

QED ■

Relations

Generally, relations are going to be operations that relate two different things. You already know a few, for example:

$$x > y$$
$$y = x - 2$$
$$x\%y = 0$$

Defintion

A n-ary relation is a subset of a cartesian product of n sets.

A binary relation is a subset of the cartesian product of two sets.

Usually, we will talk about the latter in this class.

Examples of relations with charts

Lets have our sets be $S_1 = S_2 = \mathbb{Z} \cap [1, 4] = \{1, 2, 3, 4\}$.

Take the relation $x > y$

We can write out the full cartesian product of these two sets and then label it whenever it is true.

x, y	1	2	3	4
1	1, 1	1, 2	1, 3	1, 4
2	**2, 1**	2, 2	2, 3	2, 4
3	**3, 1**	**3, 2**	3, 3	3, 4
4	**4, 1**	**4, 2**	**4, 3**	4, 4

The relation $x \mid y$:

x, y	1	2	3	4
1	**1, 1**	**1, 2**	**1, 3**	**1, 4**
2	2, 1	**2, 2**	2, 3	**2, 4**
3	3, 1	3, 2	**3, 3**	3, 4
4	4, 1	4, 2	4, 3	**4, 4**

The relation $2 \mid x + y$

x, y	1	2	3	4
1	**1, 1**	1, 2	**1, 3**	1, 4
2	2, 1	**2, 2**	2, 3	**2, 4**
3	**3, 1**	3, 2	**3, 3**	3, 4

4	4, 1	4, 2	4, 3	4, 4

Inverse relation

An inverse relation R^{-1} can be given by interchanging all of the ordered pairs in the original relationship. If our first cartestian product was $A \times B$, the inverse is $B \times A$.

If our relationship was $x > y$, some of the points would be $(10, 2)$, $(11, 3)$ and $(9, 8)$. When we take the inverse these become $(2, 10)$, $(3, 11)$ and $(8, 9)$.

Now what would the inverse of $x > y$ be?[8]

Now what would the inverse of $x|y$ be?[9].

Note

The examples shown have so far been only for $\mathbb{Z}$ onto $\mathbb{Z}$, but these can be on any sets, like noninfinite sets or even two different sets.

Properties

Let there be a relation R on a set A.

Reflexive

R is reflexive iff $\forall x \in A, xRx$

Symmetric

R is symmetric iff $\forall x, y \in A, xRy \rightarrow yRx$

Transitive

R is transitive iff $\forall x, y, z \in A, xRy \wedge yRz \rightarrow xRz$.

Antisymmetric

R is antisymmetric iff $\forall x, y \in A, xRy \wedge yRx \rightarrow x = y$.

In other words, the only way (a, b) and (b, a) are in the resulting subset is if $a = b$.

Example of proving properties

Reflexive, $xRy \leftrightarrow x - y = 0$.

To prove a relation is reflexive, we must prove $\forall x \in \mathbb{R}, xRx$.

We will do so by universal generalization.

Let x be arbitrarily chosen from $\mathbb{R}$. We are to prove xRx.

By definition of equality, $x = x$.

$$x = x$$
$$x - x = 0$$
$$xRx$$

Therefore, since x was arbitrarily chosen, this is true for any real number, and consequently, the relation R is reflexive.

Reflexive, $aRb \leftrightarrow 7 \mid 2a + 5b$

To prove a relation is reflexive, we must prove $\forall x \in \mathbb{Z}, xRx$.

We will do so by universal generalization.

[8] $x < y$

[9] $y|x$

Let x be arbitrarily chosen from $\mathbb{Z}$. We are to prove xRx.

By definition of equality, $x = x$.

$$x = x$$
$$7x = 7x$$

Since $x \in \mathbb{Z}$, by definition of divisibility, $7 \mid 7x$

$$7 \mid 7x$$
$$7 \mid 2x + 5x$$
$$xRx$$

Therefore, since x was arbitrarily chosen, this is true for any integer, so the relation R is reflexive.

Symmetric, $xRy \leftrightarrow xy = 1$
To prove a relation is symmetric, we must prove $\forall x, y \in \mathbb{R}, xRy \rightarrow yRx$.

Let $x, y \in \mathbb{R}$ such that xRy. Therefore, by given $xy = 1$. Since multiplication is commutative, $yx = 1$. Therefore, by given, yRx. Therefore, since $xRy \rightarrow yRx$, the relation R is transitive.

Transitive, $xRy \leftrightarrow x > y$
To prove a relation is transitive, we must prove that $\forall x, y, z \in \mathbb{R}, xRy \land yRz \rightarrow xRz$.

Let $x, y, z \in \mathbb{R}$ such that xRy and yRz. Therefore $x > y$ and $y > z$, by given.

$$\begin{cases} x > y \\ y > z \end{cases}$$

Since addition is monotonically increasing, we can add the two statements.

$$x + y > y + z$$
$$x > z$$
$$xRz$$

Therefore, since $xRy \land yRz \rightarrow xRz$, R is transitive.

Exercises

If R is reflexive, is R^{-1} reflexive?

If R is symmetric, is R^{-1} symmetric?

If R is transitive, is R^{-1} transitive?

Let C be the circle relation, $xCy \leftrightarrow x^2 + y^2 = 1$. Prove or disprove that C is reflexive, symmetric and/or transitive.

Let D be defined by $xDy \leftrightarrow xy \geq 0$. Prove or disprove that D is reflexive, symmetric and/or transitive.

Transitive Closure of a Relation

Let A be a set and R a relation on A. The transitive closure of R is the relation R^+ on A that satisfies the following three properties:

1. R^+ is transitive
2. $R \subseteq R^+$
3. If S is any other transitive relation that contains R, then $R^+ \subseteq S$

Basically, take a relationship and then add the minimum number of pairs you need to make it transitive.

Partial Order Relation

R is a partial order relation iff R is antisymmetric, reflexive, and transitive.

Total Order Relation

A relation R over the set A is a total order relation if $\forall a, b \in A, aRb \lor bRa$, and R is a partial order relation.[10]

Intuitively, this means that the relations will form a chain, and the relation will create an order over the entire set.

Topological Sorting

We can construct a topological sort of partial ordering by starting at the top of each chain and moving down a level.

More Exercises

Let R be defined over the set of all real numbers and $xRy \leftrightarrow x < y$. Is R antisymmetric? Prove or provide a counterexample.[11]

Let P be the set of all people who have ever lived and define a relation R on P such that $\forall r, s \in P, rRs \leftrightarrow r \text{ is an ancestor of s} \lor r = s$. Is R a partial order relation?

Given the relation $mRn \leftrightarrow m + n \text{ is even}$, is R antisymmetric?

Equivalence Relations

Let A be a set and R a relation on A. R is an equivalence relation iff R is reflexive, symmetric, and transitive.

The classic example of one of them is $xRy \leftrightarrow x = y$, but they can be more general like $xRy \leftrightarrow \text{the first four letters of } x \text{ and } y \text{ are the same.}$

Equivalence Classes

Given a set A and a relation R, for each element $a \in A$, the equivalence class of a, denoted $[a]$, is the set defined by $[a] = \{x \mid x \in A, xRa\}$.

Relation Induced by a partition

You can partition a set A into pieces A_i where each piece is a subset of A, nonempty, and mutually disjoint.

Given those partitions, define a relation R such that $\forall x, y \in A, xRy \leftrightarrow \exists A_i, x \in A_i \land y \in A_i$.

Furthermore, any relation induced by a partition is reflexive, symmetric and transitive, and therefore, an equivalence relation and the relation's equivalence classes are the same as the pieces the set was partitioned into.

Rational Numbers, $\mathbb{Q}$

Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Define a relation R on A such that $(a, b)R(c, d) \leftrightarrow ad = bc$. Then, $\mathbb{Q}$ is the set of equivalence classes for A using the relation R.

Congruence

Let $m, n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. m is congruent to n modulo d iff $d \mid (m - n)$.

This is often written as $m \equiv n \pmod{d}$.

Another way of thinking of this is that integers m and n are congruent modulo d if their difference is a multiple of d.

Properties of the Modulus Congruence class

Let $a, b, n \in \mathbb{Z}$ and $n > 1$. The following statements are equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $\exists k \in \mathbb{Z}, a = b + kn$
4. a and b have the same remainder when divided by n.

---

[10] If $aRb \lor bRa$ is true, then it is automatically reflexive.

[11] A silly proof would be that since $x > y$ forms a total order over the reals, it forms a partial order, and is therefore antisymmetric. Don't do this, it is a circular proof.

5. $a \% n = b \% n$

Sequences

Informally, a sequence is an infinite list of numbers:

$$1, 2, 3, 4, 5, \ldots$$
$$1, 3, 5, 7, 9, \ldots$$
$$1, 0.1, 0.01, 0.001, 0.0001, \ldots$$

Formally, a sequence is a function $f : D \to \mathbb{R}$, where D is $[n_0, \infty) \cap \mathbb{Z} = \{n_0, n_0 + 1, n_0 + 2, \ldots\}$ where $n_0 \in \mathbb{Z}^{\geq 0}$. The domain D is called the set of indices, and n_0 is the starting index.

Example

If $D = \{3, 4, 5, 6, \ldots\}$ and $f(n) = n^2$, this results in the sequence:

$$f(3), f(4), f(5), \ldots = 9, 16, 25, \ldots$$

Example

Usually, we give the starting index and the function:

$$a_n = n^2 \text{ for } n \geq 3$$
$$\Rightarrow f(3), f(4), f(5), \ldots = 9, 16, 25, \ldots$$

Recursive Sequences

We can also define sequences recursively by specifying a formula and a starting element:

$$a_1 = 4$$
$$a_k = 2a_{k-1} + 1 \text{ for } k > 1$$

We can then calculate:

$$a_2 = 2a_1 + 1 = 2(4) + 1 = 9$$
$$a_3 = 2a_2 + 1 = 2(9) + 1 = 19$$
$$\vdots$$

Shifting the starting index

Suppose we have $a_k = k^2$ for $k \geq 4$, but we want $n_0 = 0$ instead of $n_0 = 4$.

Then, change k to $k + 4$: $a_k = (k + 4)^2$.

Generally, to change the starting index from a to b, replace all k with $k + (a - b)$.

Summations

- How to add multiple elements
- Used heavily

Common Sums

$$\sum_{k=1}^{n} 1 = 1 + 1 + 1 + \cdots + 1 = n$$

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \qquad \text{Gauss's Sum}$$

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad \text{Sum of Squares}$$

$$\sum_{k=0}^{n} r^k = 1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r} \qquad \text{Geometric Sum}$$

Note the zero on the geometric sum!

These are useful because you can break down more complicated sums into these sums for simplification.

Examples

$$\begin{aligned}
&\sum_{k=0}^{5} 3(2)^{4k+1} \\
&= \sum_{k=0}^{5} 3 \cdot 2(2)^{4k} \\
&= 6 \sum_{k=0}^{5} 2^{4k} \\
&= 6 \sum_{k=0}^{5} 16^{k} \\
&= 6 \left(\frac{1 - 16^6}{1 - 16} \right) \\
&= 6710886
\end{aligned}$$

You can put a sum inside of another sum:

$$\begin{aligned}
&\sum_{n=1}^{10} \sum_{n=1}^{n} 1 \\
&= \sum_{n=1}^{10} n \\
&= \frac{(10)(10+1)}{2} \\
&= 55
\end{aligned}$$

A more complicated example:

$$
\begin{aligned}
&\sum_{n=5}^{50}\sum_{i=1}^{n+1} i \\
&= \sum_{n=5}^{50}\left(\frac{(n+1)(n+1+1)}{2}\right) \\
&= \sum_{n=5}^{50}\frac{1}{2}(n+1)(n+2) \\
&= \sum_{n=5}^{50}\frac{1}{2}(n^2+3n+2) \\
&= \frac{1}{2}\sum_{n=5}^{50} n^2 + \frac{3}{2}\sum_{n=5}^{50} n + \sum_{n=5}^{50} 1 \\
&= \frac{1}{2}\left(\sum_{n=5}^{50} n^2 - \sum_{n=1}^{4} n^2\right) + \frac{3}{2}\left(\sum_{n=1}^{50} n - \sum_{n=1}^{4} n\right) + \left(\sum_{n=1}^{50} 1 - \sum_{n=1}^{4} 1\right) \\
&= \frac{1}{2}\left(\frac{50(50+1)(2(50)+1)}{6} - \frac{4(4+1)(2(4)+1)}{6}\right) + \frac{3}{2}\left(\frac{50(50+1)}{2} - \frac{4(4+1)}{2}\right) + (50-4) \\
&= 23391
\end{aligned}
$$

Sum Properties

$$\sum_{n=1}^{x} a = xa$$

$$\sum_{n=1}^{x}(a+b) = \sum_{n=1}^{x} a + \sum_{n=1}^{x} b$$

$$\sum_{n=1}^{x} af(n) = a\sum_{n=1}^{x} f(n)$$

Products

Products are very similar to sums, except they work with products:

$$\prod_{i=1}^{10} i = 1\times 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9\times 10 = 10! = 3628800$$

Induction

Suppose I told you two things:

- It will be sunny on January 1st, 2022. *(base case)*
- Any day after January 1st, 2024, if it is sunny that day, it will be sunny the next day. *(recursive rule)*

You could then conclude that it will be sunny every day past January 1st, 2022.

We can apply this idea to sequences as well. If we're looking at a sequence and we have some formula for it, $f(x)$, and we know:

$$f(0)$$

$$f(n) + \text{next item} = f(n+1)$$

We have proved that $f(x)$ predicts the sequence.

Examples

Example: $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$
Show, for every positive integer n, that:

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Let's start by rewriting this into a form that is more easily proven:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Now, it is clear what our base case is ($n = 1$), so let's prove it:

Base case ($n = 1$):

Substitute for n on both sides of the equation:

$$\sum_{i=1}^{1} i^2 \stackrel{?}{=} \frac{1(1+1)(2 \cdot 1 + 1)}{6}$$

$$1^2 \stackrel{?}{=} \frac{1 \cdot 2 \cdot 3}{6}$$

$$1 \stackrel{?}{=} \frac{6}{6}$$

$$1 = 1$$

Because $1 = 1$, we have proven the base case.

Now, it is time for the inductive hypothesis. We plan to do weak induction, so we should state that all we assume is that the previous (n) statement is true, which we can then use to prove the following ($n + 1$) statement.

Inductive hypothesis: Assume, for some $n \geq 1$, that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

I used $n \geq 1$ for the inductive hypothesis because we plan to go more positive, and our base case is $n = 1$. Notice that this statement is undoubtedly true because our base case proves it. In other words, by applying induction, we will expand it from a $\exists$ to a $\forall$.

Now, for the inductive step.

Inductive step: Show using the n case that

$$\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+1+1)(2(n+1)+1)}{6}$$

Note that this is equal to $((n+1)(n+2)(2n+3))/6$, which is equal to $(2n^3 + 9n^2 + 13n + 6)/6$, which will likely be easier to identify.

$$\sum_{i=1}^{n+1} i^2 \stackrel{?}{=} \frac{(n+1)(n+1+1)(2(n+1)+1)}{6}$$

$$\sum_{i=1}^{n+1} i^2 \stackrel{?}{=} \frac{(n+1)(n+2)(2n+3)}{6}$$

$$\sum_{i=1}^{n} i^2 + (n+1)^2 \stackrel{?}{=} \frac{2n^3 + 9n^2 + 13n + 6}{6}$$

Now we will apply the inductive hypothesis, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$:

$$\frac{n(n+1)(2n+1)}{6} + (n+1)^2 \stackrel{?}{=} \frac{2n^3 + 9n^2 + 13n + 6}{6}$$
$$\frac{n(n+1)(2n+1)}{6} + n^2 + 2n + 1 \stackrel{?}{=} \frac{2n^3 + 9n^2 + 13n + 6}{6}$$
$$n(n+1)(2n+1) + 6n^2 + 12n + 6 \stackrel{?}{=} 2n^3 + 9n^2 + 13n + 6$$
$$n(n+1)(2n+1) + 6n^2 + 12n \stackrel{?}{=} 2n^3 + 9n^2 + 13n$$
$$n(n+1)(2n+1) + 6n^2 \stackrel{?}{=} 2n^3 + 9n^2 + n$$
$$n(n+1)(2n+1) \stackrel{?}{=} 2n^3 + 3n^2 + n$$
$$n(n+1)(2n+1) \stackrel{?}{=} n(2n^2 + 3n + 1)$$
$$n(2n^2 + 3n + 1) = n(2n^2 + 3n + 1)$$

These are the same statement therefore they are equal. Therefore, since $n \to n+1$, by induction,

$$\forall n \geq 1, \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Example: $3 + \sum_{i=1}^{n} (3 + 5i) = \frac{(n+1)(5n+6)}{2}$
Prove:

$$3 + \sum_{i=1}^{n} (3 + 5i) = \frac{(n+1)(5n+6)}{2}$$

This will once again be weak induction. Since you've already seen it above, I will have fewer explanations.

Base case ($n = 1$):

Plug in $n = 1$:

$$3 + \sum_{i=1}^{1} (3 + 5i) \stackrel{?}{=} \frac{(1+1)(5(1)+6)}{2}$$
$$3 + (3 + 5(1)) \stackrel{?}{=} \frac{2 \cdot 11}{2}$$
$$6 + 5 \stackrel{?}{=} 11$$
$$11 = 11$$

Because $11 = 11$, the base case is proven.

Below, notice that you can use whatever variable you want to. I decided to use $n - 2$ in this case because that leads to the inductive step factoring.

Inductive hypothesis: Assume for some $n - 2 \geq 1$ that:

$$3 + \sum_{i=1}^{n-2} (3 + 5i) = \frac{((n-2)+1)(5(n-2)+6)}{2}$$

Inductive step: Show the $n - 1$ case:

$$3+\sum_{i=1}^{n-1}(3+5i) \stackrel{?}{=} \frac{((n-1)+1)(5(n-1)+6)}{2}$$

$$3+\sum_{i=1}^{n-1}(3+5i) \stackrel{?}{=} \frac{n(5n+1)}{2}$$

$$3+\sum_{i=1}^{n-2}(3+5i)+(3+5(n-1)) \stackrel{?}{=} \frac{n(5n+1)}{2}$$

$$3+\sum_{i=1}^{n-2}(3+5i)+3+5n-5 \stackrel{?}{=} \frac{n(5n+1)}{2}$$

$$3+\sum_{i=1}^{n-2}(3+5i)+5n-2 \stackrel{?}{=} \frac{n(5n+1)}{2}$$

Apply the inductive hypothesis:

$$\frac{((n-2)+1)(5(n-2)+6)}{2}+5n-2 \stackrel{?}{=} \frac{n(5n+1)}{2}$$

$$\frac{(n-1)(5n-10+6)}{2}+5n-2 \stackrel{?}{=} \frac{n(5n+1)}{2}$$

$$\frac{(n-1)(5n-4)}{2}+5n-2 \stackrel{?}{=} \frac{n(5n+1)}{2}$$

$$(n-1)(5n-4)+10n-4 \stackrel{?}{=} n(5n+1)$$

$$5n^2-9n+4+10n-4 \stackrel{?}{=} n(5n+1)$$

$$5n^2-9n+10n \stackrel{?}{=} n(5n+1)$$

$$5n^2+n \stackrel{?}{=} n(5n+1)$$

$$n(5n+1)=n(5n+1)$$

Since the statements are the same, they are equal. By induction, since $n-2 \to n-1$:

$$\forall n \geq 1, 3+\sum_{i=1}^{n}(3+5i) = \frac{(n+1)(5n+6)}{2}$$