Discrete Math for Computer Science

Phanuel Mariano

Contents

CHAPTER 1

Speaking Mathematically

Section 1.1 - Variables, Statements

- **Variables** are simply just placeholders in math that can represent some quantity or some other object,
  - For example, the sentence "Is there a real number x such that $x^2 = 1$?" Can be replaced by
    - "Is there a real number $\heartsuit$ such that $\heartsuit^2 = 1$?"
    - It can also be temporary name, in which you can change afterwards. Like in a computer program.
- **Example:** Write using Variables: "Given any real number, its square is non-negative"
  - Solution:
  - "For any real number x, $x^2 \geq 0$"
  - "For every real number x, $x^2 \geq 0$"

DEFINITION 1. A **universal statement** says that a certain property is true for all elements of a set.

DEFINITION 2. An **existential statement** says some property is true for at least one object.

DEFINITION 3. A **conditional statement** says that if something is true, then something else has to be true.

- **Example:**
  - Of (1) All circles are round.
  - Of (2) There is an ellipse that is a circle.
  - Of (3) If I am in New York, then I am in the U.S.

DEFINITION 4. A **universal conditional statement** is both universal and conditional.

- **Example:** Like the one above. "For all real numbers x, if x is nonzero, then x^2 is positive."
- Rewrite it and fill in the blank:
  - If a real number is nonzero, then its square is positive.
  - For all nonzero real numbers x, x^2 is positive.
  - If x is a nonzero real number, then x^2 is positive.
  - The square of any nonzero real number is positive.
  - All nonzero real numbers have positive squares (or squares that are positive).

DEFINITION 5. A **universal existential statement** is a two-part statement whose first part is universal and second part is existential.

- **Example:** "Every real number has a cube root."
  - Other forms:
  - "All real numbers have cube roots."
  - "For all real numbers x, there is a real number y such that $x = y^3$."
  - Eventually, we'll write things likes "$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $x = y^3$."

DEFINITION 6. An **existential universal statement** is a two-part statement whose first part is existential and second part is universal.

- **Example:** "There is a real number whose product with every real number is 0."
  - Other forms:
  - "There is a number x such that for all real numbers y, $xy = 0$."
  - Eventually, we'll write things likes "$\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}, xy = 0$".

Section 1.2 - The Language of Sets

- A **set** may be thought of as a well-defined collection of objects, called **elements** (or members).
  - **Remarks:**
  - Order doesn't matter, and each object is distinct (so it doesn't matter if they are listed more than once)
    - $\{1,2,3\} = \{3,2,1\} = \{1,2,3,1\}$
  - We use Capital letters for sets; A, S
  - We use lower case letters for elements
  - $a \in A$ means "a is an elements of set A"
  - $a \notin A$ means "a is not an element of set A"
- **Ways to specify or define sets:**
  - Use words: "Let $\mathbb{R}$ be th set of real numbers" , i.e. all the points on a number line.
  - Set-Roster Notation: $\{1,2,3\}$ or $\{1,2,3,\ldots,99,100\}$
    - Note that "$\ldots$ " means that the pattern keeps going.
      - But $4 \in \{1,2,\ldots,100\}$ but $4 \notin \{1,3,100\}$, or $5.19 \notin \{1,2,\ldots,100\}$
  - Set-Builder Notation:
    - Suppose S is a set and $P(x)$ is a property that elements of S may have. Then denotes

$$\{x \in S \mid P(x)\} \text{ or } \{x \in S : P(x)\}$$

      the set of elements x in S such that $P(x)$ is true.
      - Here "|" or ":" means "such that"
    - **Example:** Let $A = \left\{y \in \mathbb{R} \mid y^2 = 1\right\} = \{-1, 1\}$

Definition 7. (Set-Roster) The set of **integers** is the set

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

- Also,
  - $\mathbb{Z}^+ = \{1,2,3,\ldots\} = \mathbb{N}$, is the set of positive integers, or natural numbers
  - $\mathbb{Z}^{\geq 0} = \{0,1,2,3,\ldots\}$, is the set of nonnegative integers

Definition 8. (Set-Builder) The set of **rational numbers** is the set

$$\mathbb{Q} = \left\{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ and } n \neq 0\right\}.$$

- **Cartesian Products:**

Definition 9. An **ordered pair** is an object of the form (a, b) where a and b are any objects.

Definition 10. Two ordered pairs are **equal**, $(a, b) = (c, d)$, provided that $a = c$ and $b = d$.

Definition 11. If A and B are sets, then the **Cartesian product** of A and B, denoted $A \times B$, is the set of ordered pairs (a, b), where $a \in A$ and $b \in B$. That is,

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

- An ordered pair (a, b) is an **object** that is often inside sets.
  - Similarly, we can define an $n-$tuple $(x_1, x_2, \ldots, x_n)$.
- **Examples:**
  - Note $(2,4) \neq (4,2)$.
    - But $\{2,4\} = \{4,2\}$
    - Also $(2,4) \neq \{2,4\}$, one is an object, the other is a set.
  - Let $A = \{3,4\} \times \{a,b,c\} = \{(3,a), (3,b), (3,c), (4,a), (4,b), (4,c)\}$
  - Let $B = \{a,b,c\} \times \{3,4\} = \{(a,3), (a,4), (b,3), (b,4), (c,3), (c,4)\}$
    - Note $A \neq B$
- The **Cartesian Plane**:
  - This is the most important cartesian product you have probably dealt with in the past.

  - It is
$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$
or sometimes we use shorthand
$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}.$$
  - It corresponds to a unique point in the $x - y$ plane.
- **Examples:**
  - One way is to think of $A \times B$ like the $x - y$ plane but with arbitrary sets.
- **Subsets:**

DEFINITION 12. Let A and B be sets. Then A is called a **subset** of B, written $A \subseteq B$ (or $A \subset B$) provided that every element of A is an element of B.

- That is , $A \subseteq B$ means "if $x \in A$, then $x \in B$"
  - **Question:** What kind of statement is this?
  - **Solution:** A universal conditional statement.
    - Why because we can rewrite this as"For all $x \in A$, then $x \in B$"
- It helps to think of Venn Diagrams.
- **Example:** If $A = \{1, 2\}$ and $B = \{1, 2, 3\}$ then
$$A \subseteq B.$$
but
$$B \not\subseteq A.$$
since $3 \notin A$.
- **Example:** True or False?

(1) $2 \in \{1, 2, 3\}$
  - True

(2) $\{2\} \in \{1, 2, 3\}$
  - False

(3) $2 \subseteq \{1, 2, 3\}$
  - False

(4) $\{2\} \subset \{1, 2, 3\}$
  - True

(5) $\{2\} \subset \{\{1\}, \{2\}\}$
  - False
  - Note that this is a set of sets!

(6) $\{2\} \in \{\{1\}, \{2\}\}$
  - True

(7) $\{\{2\}\} \subset \{\{1\}, \{2\}\}$
  - True

- **Strings** are optional. See book for the definition.

Section 1.3 - The Language of Relations and Functions

- Relations:
  - First we start by defining what a relation is

DEFINITION 13. Let A and B be sets. A **relation** R from A to B is a subset of $A \times B$. Given an ordered pair (x, y) in R, we say "x is related to y" and write xRy. The set A is called the **domain** of R and set B is called the **co-domain**.

- **Note:**
  - Thus to see if x is related to y is to simply check if $(x, y) \in R$.
  - We write $x \not R y$ when x is not related to y, i.e. $(x, y) \notin R$.
- **Examples:**

(1) Let $A = \{1, 2, 3\}, B = \{a, b, c, d\}$ and define the relation R by

$$R = \{(1, d), (2, a), (2, c)\}.$$

(a) Is $1Rb$? That is, "is 1 related to b"
   (i) **Solution:** No since $(1, b) \notin R$.

(b) Is $2Ra$? That is, "is 1 related to b"
   (i) **Solution:** Yes since $(2, a) \in R$.

(c) What is the domain?
   (i) **Solution:** This is given in the problem, which is $A = \{1, 2, 3\}$.

(d) What is the co-domain?
   (i) **Solution:** This is given in the problem, which is $B = \{a, b, c, d\}$.

(2) Define a relation L from $\mathbb{R}$ to $\mathbb{R}$ as follows:

$$(x, y) \in L \text{ iff } x < y$$

(here iff means "if and only if")

(a) Is $2L\pi$?
   (i) **Solution:** Using the definition above, to check if 2 is related to π, we need to check the condition if $(2, \pi) \in L$. And by the definition of L, we need to check if $2 < \pi$. Since this is true, then **YES**, $2L\pi$!

(b) Is $(5, \pi) \in L$?
   (i) **Solution:** Using the definition above, to check if $(5, \pi) \in L$ we need to check if $5 < \pi$.Which is not true, hence

$$(5, \pi) \notin L.$$

(3) Define a relation C from $\mathbb{R}$ to $\mathbb{R}$ by

$$(x, y) \in C \text{ means that } x^2 + y^2 = 1.$$

(a) Is $(0, 1) \in C$?
   (i) **Solution:** Using the definition above, we need to check if $x^2 + y^2 = 1$. Since

$$0^2 + 1^2 = 1,$$

   then yes $(0, 1) \in C$.

(b) Is $\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right) \in C$?
   (i) **Solution:** Using the definition above, we need to check if $x^2 + y^2 = 1$. Since

$$\left(\frac{\sqrt{2}}{2}\right)^2 + \left(\frac{\sqrt{2}}{2}\right)^2 = \frac{1}{2} + \frac{1}{2} = 1,$$

   then yes.

(c) Is $-1C0$?
   (i) **Solution**: (BTW, have you noticed yet that we are simply checking if these points lie in the **circle**?) Since

$$(-1)^2 + 0^2 = 1$$

then yes.

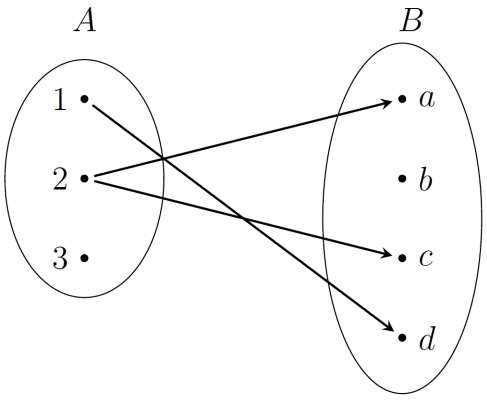
(d) Is $1C1$?

(i) **Solution**: Since

$$1^2 + 1^2 = 2 \neq 1$$

then no!

- You can call C the "circle" relation.
- And L the "less than" relation.
- **Arrow Diagram of a Relation:**
  - One can think of a **relation** as arrows going from one set A to the other B.
  - **Example:**



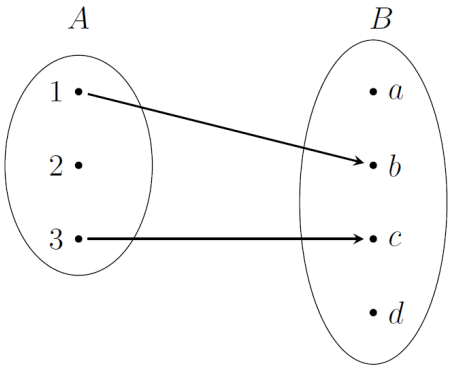
  -
  - **Question:** What relation does this represent?
  - **Solution:** The domain is $A = \{1, 2, 3\}$, the co-domain is $B = \{a, b, c, d\}$ and the relation is given by the set of ordered pairs

$$R = \{(1, d), (2, a), (2, c)\}$$

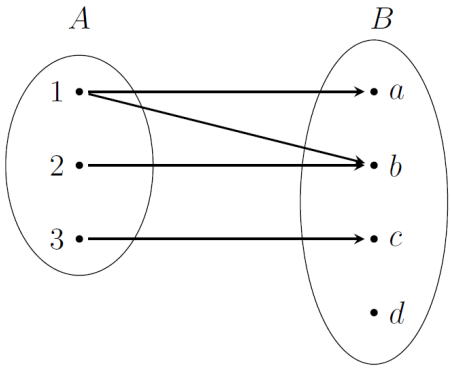
- **Functions:**
- We start with the mathematical definition of a function: The definition of functions involves thinking of a domain, a co-domain, and arrows getting mapped from A to B, but with some additional properties.

DEFINITION 14. A **function** F from A to B is a relation from A to B satisfying
(1) For all $x \in A$, there exists $y \in B$ such that $(x, y) \in F$.
(2) For all $x \in A$ and $y, z \in B$, if $(x, y) \in F$ and $(x, z) \in F$, then $y = z$.

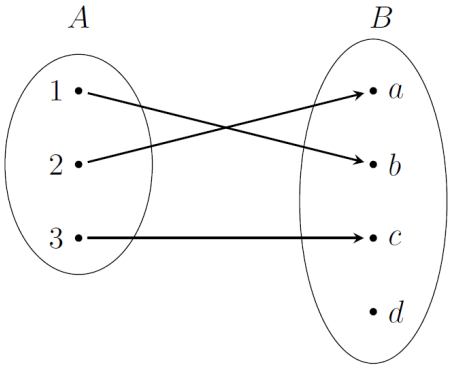
- **Remarks:** Let's break down what this is saying:
  - Part 1 is just saying that every element of x in A gets mapped to at least one element in B.
    - Draw out some arrow example to illustrate this
    - Actually, try drawing a BAD exanmple that violates this
  - Part 2 is just saying that elements in the domain can't be mapped to multiple things
    - Draw out some arrow example to illustrate this
    - What property of functions is this? T**he vertical line test!**
  - Also note here, that a function F is actually a set of ordered pairs! (which is the graph of a function on how we normally are used to thinking of functions)
  - Not every relation is a function!
- **Examples:** Which of the following relations are functions from $A = \{1, 2, 3\}$ to $B = \{a, b, c, d\}$.



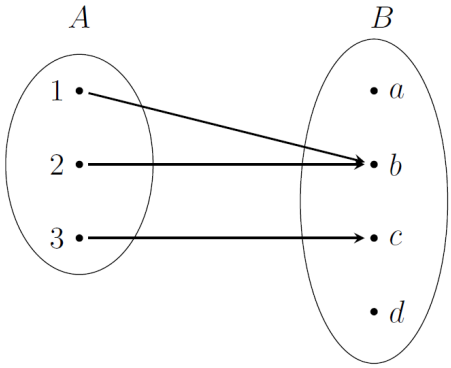
Fcn? NO



Fcn? NO



Fcn? YES



Fcn? YES

-
  - **Part (a)** No, Violates Part 1 of the Definition of a function .
  - **Part (b)** No, Violates Part 2, of the Definition of a function. (The vertical Line test)
    - We can think of this as a graph! Try graphing this on a $A \times B$ plane!
  - **Part (c)** Yes this is a funtion!
    - Try graphing this on a $A \times B$ plane!
  - **Part (d)** Yes this is a funtion!
    - Try graphing this on a $A \times B$ plane!
- **Notation:** We usually write $F : A \to B$ to mean F is a function from domain A to co-domain B.
  - And we take $F(x)$ to mean the unique value y such that $(x, y) \in F$.
  - Though mathematically a function F is actually a set of $A \times B$:
    $$F = \{(x, y) \in A \times B \mid y = F(x)\}$$
  - **Example:** Most functions you dealt with are given by a formula, for example $F : \mathbb{R} \to \mathbb{R}$ defined by
    $$F(x) = x^2.$$

CHAPTER 2

The Language of Compound Statements

Section 2.1 - Logical Form and Logical Equivalence

- First, I will assume that everyone here agrees what true, false, and what a sentence. I won't define this mathematically.

DEFINITION 15. A **statement** (or **proposition**) is a sentence that is true or false but not both.

- For each statement, we can assign a value of T or F to it.
  - **Examples:**
    (1) $1+1=2$,
        (a) T
    (2) $1+1=5$
        (a) F
    (3) Schenectady is in NY
        (a) T
    (4) The millionth digit of π is 7.
        (a) Anyone know if this is true? This is actually false! The true digit is 1.
  - **An example that is NOT a Mathematical Statement:**
    * "This sentence is false"
      · Because a sentence can only be T or F, but no both.
      · If it is T, then it has to be F (by reading the statement)
      · If it is F, then also has to be T.
      · So it's both TRUE or FALSE. Bad!

Compound Statements:

- We are going to define some symbols in mathematical logic.
  - The next definition has a "piecewise function"

DEFINITION 16. Let p and q be statements.
(1) $\sim p$ (or $\neg p$) is read "**not p**" and is called the **negation of** p. It is the statement defined by

$$\sim p : \begin{cases} \text{TRUE} & \text{when } p \text{ is FALSE} \\ \text{FALSE} & \text{when } p \text{ is TRUE} \end{cases}$$

(2) $p \wedge q$ is read "**p and q**" and is called the **conjunction of** p **and** q. It is the statement defined by

$$p \wedge q : \begin{cases} \text{TRUE} & \text{when } \textbf{both } p \text{ and } q \text{ are TRUE} \\ \text{FALSE} & \text{otherwise (i.e., at least one is FALSE)} \end{cases}$$

(3) $p \vee q$ is read "**p or q**" and is called the **disjunction of** p **and** q. It is the statement defined by

$$p \vee q : \begin{cases} \text{TRUE} & \text{when } \textbf{at least one of } p \text{ and } q \text{ is TRUE} \\ \text{FALSE} & \text{otherwise (i.e.,both } p \text{ and } q \text{ are FALSE)} \end{cases}$$

- **Remarks:**
  - **Order of Operations:**
  - The statement "$p \wedge q \vee r$ " is ambiguous
    * It needs parantheses
    * In logic, $\wedge, \vee$ are considered coequal (no PEMDAS here)

        * So we really need paranthese here to specify what is being applied first: such as $(p \wedge q) \vee r$ or $p \wedge (q \vee r)$
    - $\sim$ is done first: so $\sim p \wedge q = (\sim p) \wedge q$
    - As already discussed, Parantheses can override what goes first.
    - Other info:
    - $\vee$ is the "inclusive or"
        * True when at leasy one is true, or both
    - "But" means "and"
    - "neither p nor q" means $\sim p \wedge \sim q$.

Truth Tables:

- A **truth table** is an organizational tool used to help determine the truth/falsity of a compound statement.
    - To form a truth table,
        * list all possible conditions of the simple statements in a compound statement, and
        * then compute T/F of the compound statement based on the definitions of the logical connectives.
- Truth tables will be usefull later when we are trying to prove two statements are equivalent
- **Example:** Let us construct the truth tables for the basic connectives we have just defined: $\neg p$, $p \wedge q$ and $p \vee q$

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Statement Forms and Truth Tables:

- We will want to combine various statements and connectives together to be able to build more complex sentences.

DEFINITION 17. A **statement form** (or **propositional form**) is a well-formed expression made up of statement variables $(p, q, r, \dots)$ and logical connectives $(\sim, \wedge, \vee, \dots)$.

REMARK. The phrase "well-formed" means it becomes a statement when actual statements are substituted for the variables ($\vee \vee pp$ is not well formed)

- **Example:** Construct a truth table for $(p \wedge q) \vee \sim r$.
    - **Solution:** First figure out the number of inputs: p, q, r and figure out all possible combinations:
        * And then apply them:

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

Logical Equivalence (via truth tables).

- How do we determine when two statements are actually equivalent?
    - For example, is true that $\sim (p \vee q) \equiv \sim p \wedge \sim q$?

DEFINITION 18. Two statement forms P and Q are **logically equivalent**, denoted $P \equiv Q$, if they have identical truth values for every possible assignment of truth values to their statement variables.

- **Example:** Use a truth table to show $\sim (p \vee q) \equiv \sim p \wedge \sim q$
  - **Solution:** We contruct a truth table for both statements (side by side).
    - But first remember since we have p, q as are statement variables, then there are 4 possible combinations of their pairing.
    -

p	q	(3) $p \vee q$	(4) $\sim (p \vee q)$	(5) $\sim p$	(6) $\sim q$	(7) $\sim p \wedge \sim q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

    - Comparing columns (4) and (7), we see that the two statements in question have the same truth values under all possible conditions. **Hence they are logically equivalent!**
- **De Morgan's Law:** The example above is actually one of DeMorgan's Law, which is very important in math and logic!
  - It tell us how to negate "and" and "or" statements
- Here is the complete De Morgan's Laws:

PROPOSITION. *(De Morgan's Laws)*
The following are true:

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

Tautologies and Contradictions:

DEFINITION 19. A **tautology** is a statement form that is always true, regardless of the truth values assgined to its variables.
A **contradiction** is one that is always false, regardless of the truth values assigned to its variables.

- **Remark:** The book often uses $\boldsymbol{t}$ for a generic tautology and $\boldsymbol{c}$ for a generic contradiction.
  - **Examples:**
    - **Part (a):** The statement $p \vee \sim p$ is a tautology
      - **Solution:** To prove this, construct a truth tbale yourself and check that all the output values are always True.
    - **Part (b):** The statement $p \wedge \sim p$ is a contradiction
      - **Solution:** To prove this, construct a truth tbale yourself and check that all the output values are always False.

Summary of Logical Equivalences:

- We can summarize various logical equivalences in a Theorem. (Theorem 2.1.1 in the book)
- Some of these we have shown already, some you will be asked to prove in the homework.

THEOREM. *(Theorem 2.1.1 Logical Equivalences)*
Given any statement variables p, q and r, a tautology $\boldsymbol{t}$ and a contradiction $\boldsymbol{c}$, 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:*	$p \wedge \boldsymbol{t} \equiv p$	$p \vee \boldsymbol{c} \equiv p$
5.	*Negation laws:*	$p \vee \sim p \equiv \boldsymbol{t}$	$p \wedge \sim p \equiv \boldsymbol{c}$
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:*	$p \vee \boldsymbol{t} \equiv \boldsymbol{t}$	$p \wedge \boldsymbol{c} \equiv \boldsymbol{c}$
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.	*Negation of* $\boldsymbol{t}$ *and* $\boldsymbol{c}$	$\sim \boldsymbol{t} \equiv \boldsymbol{c}$	$\sim \boldsymbol{c} \equiv \boldsymbol{t}$

- Thus you can prove equivalences, by simplying using these already known equivalences.
- **Example (problem 48):** Show $(p \wedge \sim q) \vee (p \wedge q) = p$ using the equivalences already known.
  - **Solution:**

$$\begin{aligned}(p \wedge \sim q) \vee (p \wedge q) &\equiv p \wedge (\sim q \vee q)\,, \text{ by the distributive property} \\ &\equiv p \wedge (q \vee \sim q)\,, \text{ by the commutative property for} \vee \\ &\equiv p \wedge \boldsymbol{t}, \text{ by the negation law for } \vee \\ &\equiv p, \text{ by the identity law for } \vee\end{aligned}$$

Section 2.2- Conditional Statements

- **Conditional Statements:**
- Premise: Let's say you walk into a store and the store owner has the following promise(contract) to you:

"If I pay for an item, then I receive the item"

  - This is a **conditional statement**.
  - We can think of $p =$ "pay for an item" and $q =$ "receive the item"
  - And rewrite this sentence in symbols:

$$"p \to q"$$

  - **Question:** In what situation would this statement (as a whole) be false?
    - Suppose you do "pay" (i.e. the input fot p is True), but then you don't receive the item (q is false):
      - Then the statement "$p \to q$" is **False**, because you didn't get what you were promised!! (Promise broken)
  - **All other cases are true! (i.e. the promise is not broken in all other cases)**
    - If you do pay (p is true), and you receive it (q is true)
    - If you don't pay (p is false), and you don't receive it (q is false): WELL obviously you didn't receive it so of course you didn't receive it.
    - If you don't pay (p is false), and you receive it (q is true): Because you didn't go to the store anyway and buy anything, so the promise was that to receive it you must have first paid for it. The promise is still true!. So it's still true (Or maybe you stole it!)
- We can break the values of these "" in a Truth Table:
  -

p	q	$p \to q$	
T	T	T	
T	F	F	
F	T	T	←--when this happens, we say it is "vacuously true"
F	F	T	←--when this happens, we say it is "vacuously true

  - **Vacuously true:** means it is true by default
  - **Example:**

$$\text{If } 0 = \pi \text{ then } 1 = 2$$

    - This is a Vacuously TRUE statement, because the first part is false anyways, so the conclusion can be anything.

DEFINITION 20. The **conditional** of q by p is "p implies q" and denoted by $p \to q$. It is the statement defined by

$$p \to q \text{ is } \begin{cases} \text{FALSE} & \text{when } p \text{ is TRUE and } q = \text{FALSE} \\ \text{TRUE} & \text{Otherwise} \end{cases}$$

- **Remarks:**
  - Other terminology: "If p, then q" is equivalent to "q if p."
  - In $p \to q$, p is called the **hypothesis** and q is called the **conclusion**.
- **Order of Operations:** In logic, the order of operations is
  - $\sim$ is performed first,
  - then $\wedge$ and $\vee$,
  - and finally $\to$
  - **Example:** $p \wedge q \to r$ is equivalent to $(p \wedge q) \to r$
- **Truth Tables:**
- Just like last section, we can similarly construct truth tables involving $\to$:
- **Example:** Construct the truth table for $p \vee \sim q \to \sim p$:
  - **Solution:**
  - Hint: when doing "$\to$" easier to find the False statement ($T \to F$) and mark those as F, since all other possibilities must be T.

–

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

Logical Equivalence and $\rightarrow$.

- **Example 1:** Prove (using truth tables) that
$$p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$$
  - **Solution:**
  - Hint: when doing "$\rightarrow$" easier to find the False statement $(T \rightarrow F)$ and mark those as F, since all other possibilities must be T.

–

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

- **Example 2: (Representing If/then as Or)** The following equivalence is true
$$p \rightarrow q \equiv \sim p \vee q$$
  - **Solution:** HW problem. You will need to show that they share the same truth table!
- **Example 3: (The negation of conditional Statement)**The following equivalence is true
$$\sim (p \rightarrow q) \equiv p \wedge \sim q$$
Show this.
  - **Solution:** We can use Truth tables. Or let us use the logical equivalences we already know:
$$\begin{aligned} \sim (p \rightarrow q) &\equiv \sim (\sim p \vee q), \text{ by Example 2} \\ &\equiv (\sim\sim) p \wedge \sim q, \text{ by De Morgan's Law} \\ &\equiv p \wedge \sim q, \text{ by the double negation law.} \end{aligned}$$

More Related Statements.

DEFINITION 21. The **contrapositive** of $p \rightarrow q$ is $\sim q \rightarrow \sim p$.

DEFINITION 22. The **converse** of $p \rightarrow q$ is $q \rightarrow p$.

- **Definition:** The **inverse** of $p \rightarrow q$ is $\sim p \rightarrow \sim q$.
- In Math, the contrapositive is very important, and often makes proving things easier. The reason being the following theorem:

THEOREM. *A conditional statement is logically equivalent to the contrapositive: That is,*
$$p \rightarrow q \equiv \sim q \rightarrow \sim p.$$

PROOF. The proof of this is in the Homework (#26). Show the truth tables are the same. □

- **Example:** Let r denote the (if-then) statement
"If I am at Union College, then I am in Schenectady"
In order words this is the conditional statement $p \rightarrow q$ where
$$p = \text{"I am at Union College"}$$
$$q = \text{"I am in Schenectady"}$$

- **Part (a):** Write the contrapositive of r.
  - **Solution:** We need $\sim q \rightarrow \sim p$: "I am not in Schenectady, then I am not at Union College"
- **Part (b):** Write the converse of r.
  - **Solution:** We need $q \rightarrow p$: "I am in Schenectady, then I am at Union College"
- **Part (c):** Write the negation of r.
  - **Solution:** Recall that the negation is $\sim (p \rightarrow q) \equiv p \wedge \sim q$:
    - "I am at Union College and I am not in Schenectady"
- The original statement is T, hence its contrapositive is true.
- Also the converse in this example is NOT true.
- But the negation of a a true statement will always be false.

Biconditional.

DEFINITION 23. The **biconditional** of p and q is written $p \leftrightarrow q$ (or "p iff q" or "$p \iff q$"), read "p **if and only if** q" , and it means that both

$$p \rightarrow q \text{ and } q \rightarrow p.$$

Truth Table: Using Truth tables, The biconditional $p \longleftrightarrow q$ is true exactly when p and q have the same truth values.

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

- "p **Only if** q":
  - means if q doesn't happen, then p won't happen. That is, $\sim q \rightarrow \sim p$, or equivalently $p \rightarrow q$.
  - **Example:** "John will break the world's record for the mile run only if he runs the mile under four minutes"
    - Rewrite:$(\sim q \rightarrow \sim p)$: If John doesn't run the mule under four minutes he will not break the world's record
    - Rewrite:$(p \rightarrow q)$: "If John breaks the world's record for the mile run then he will have run the mile under four minutes"
  - Caution: "p only if q" does not mean "p if q"
- "p **if** q":
  - Means $p \leftarrow q$

More Language.

- "p **is necessary for** q" means $\sim p \rightarrow \sim q$, or $q \rightarrow p$
- "p **is sufficient for** q" means $p \rightarrow q$
- "p **is necessary and sufficient for** q " means $p \leftrightarrow q$ (also p iff q)

Section 2.3 - Valid and Invalid Arguments

- We will briefly cover Section 2.3.
  - Only need pages 66-69
- **Definition:** An argument is a sequence of statements.
- **Example1:**
  - If .33333333.... $= \frac{a}{b}$ for some integers a, b then $.33\ldots$ is a rational number.
  - It is true that $.333333\cdots = \frac{a}{b}$ where $a = 1$ and $b = 3$.
  - Therefore $.333333\ldots$ is a rational.
- **Definition:** An argument form is a sequence of statement forms
- **Example 1 revisited:** The example above has the following argument form:
  - If p, then q
  - p
  - $\therefore q$
- **Remark:**
  - All statements in an argument form are called premises (or assumption, hypothesis)
  - Last bullet: Conclusion
    - $\therefore$ means therefore

DEFINITION 24. An argument form is **valid** if when the premises are all true, then the conclusion is true, no matter what statements are substituted for the statement variables in the premises. A valid argument form is called a **rule of inference.**

- An argument is called **valid** if its form is.
- See page 67 to determine if an argument form is valid using truth tables.

.

Valid argument forms.

- There are many argument forms
  - See page 76 (Edition 5)
  - Here are two.

DEFINITION 25. The following rule of inference is called **modus ponens**

$$\begin{array}{l} \text{If } p, \text{ then } q. \\ p \\ \therefore q \end{array}$$

- **Remark:** This says, from $p \to q$ and p, we may conclude qq. Our previous example is modus ponens.
- We gave an example this already in Example 1.

DEFINITION 26. The following rule of inference is called **modus tollens**

$$\begin{array}{l} \text{If } p, \text{ then } q. \\ \sim q \\ \therefore \sim p \end{array}$$

- **Remark:** This type of argument is using what we know about contrapositive.
- The following is an example of a modus tollens argument.
  - Which can be used in a court of law.
- **Example2:**
  - If I am the axe murderer, then I can use an axe.
  - I cannot use an axe.
  - Therefore, I am not the axe murderer.

CHAPTER 3

The logic of Quantified Statements

Section 3.1 Introduction to Predicates and quantified Statements I.

DEFINITION 27. A **predicate** is a sentence that contains a finite number of variables and becomes a statement (T or F) when specific values are substituted for the variables. The **domain** of a predicate (variable) is the set of all values that may be substituted in place of the variable.

- **Example:** The sentence
$$P(x): \text{ “}x^2 > x\text{”}$$
is a **predicate** with **domain** $\mathbb{R}$”
  - This sentence is not a “statement”, because we don’t kow for which x this sentence is tru for.
  - It only becomes a statement when we plug actual numbers in.
    - sub-Example:
    - $P(2)$: which is ”$2^2 > 2$”, is a true statement, while
    - $P(\frac{1}{2})$: which is “$\frac{1}{4} > \frac{1}{2}$”, is not a true statement.

DEFINITION 28. If $P(x)$ is a predicate with domain D, then the **truth set of** $P(x)$ is the set of all elements of D that make $P(x)$ true. It is denoted by
$$\{x \in D \mid P(x)\}.$$

- **Example1:** Find the truth set of the predicate
$$P(x): \text{ “}x^2 > x\text{”}$$
  - **Solution:** Graph x^2 and x and using calculus you’ll see that the truth set is
$$\begin{aligned}\text{Truth Set} &= \{x \in D \mid x^2 > x\} \\ &= (-\infty, 0) \cup (1, \infty).\end{aligned}$$

- **Example2:** Find the truth set of the predicate $Q(n)$ with domain D
$$\begin{aligned}Q(n) &: \text{“}n^2 < 10\text{”} \\ D &= \mathbb{Z}^+\end{aligned}$$
  - **Solution:** Since $D = \{1, 2, 3, \dots\}$, and
$$\begin{aligned}1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 9 \\ 4^2 &= 16, \\ &\vdots\end{aligned}$$
and since any other square will certainly be greater than 10, then we must have that the truth set is given by
$$\begin{aligned}\text{Truth Set} &= \{n \in D \mid n^2 < 10\} \\ &= \{1, 2, 3\}.\end{aligned}$$

Quantifiers: Universal and existential statements revisited.

- We will define two symbols $\forall, \exists$,which are a type of quantifer.
  - These two symbols are one of the most important symbols when stating mathematical statements!
  - It is used very, very often!
- **Notation:**
  - The symbol $\forall$ means "for every", "for all", "for each".
  - The symbol $\exists$ means "there exists", "there is".

DEFINITION 29. (Takes over Definition 1) A **universal statement** is one of the form

$$\forall x \in D, Q(x)$$

where $Q(x)$ is a predicate with domain D. It is defined to be true if $Q(x)$ is true for every x in D, and false if $Q(x)$ is false for at least one x in D.

- **Example:** Rewrite the universal statement using the quantifer $\forall$

  "The square of every real number is always nonnegative"

  - **Solution:** "$\forall x \in \mathbb{R}, x^2 > 0$"
- **Remarks:**
  - A **counterexample** to the statement "$\forall x \in, Q(x)$" is an element $c \in D$ that makes $Q(c)$ **false**.
  - The statement "$\forall x, P(x) \to Q(x)$" is called a "universal conditional statement"
- **Example:** Find a **counterexample** to the following universal statement:

  $$\text{"}\forall n \in \mathbb{Z}, \frac{n}{2} \in \mathbb{Z}\text{"}$$

  - **Solution:** A counterexample would be $x = 3$ since $\frac{3}{2} \notin \mathbb{Z}$.

DEFINITION 30. (Takes over Definition 2) An **existential statement** is one of the form

$$\exists x \in D \text{ such that } Q(x)$$

where $Q(x)$ is a predicate with domain D. It is defined to be true if $Q(x)$ is true for at least one x in D, and false if $Q(x)$ is false for every x in D.

- **Example:** Write the statement

  $$\text{"}\exists x \in \mathbb{R} \text{ such that } x^2 = 1\text{"}$$

  using informal language.
  - **Solution:** "There exists a real number whose square is 1"

Universal Conditional Statements.

- A **universal conditional statement** is

  $$\text{"}\forall x, \text{if } P(x) \text{ then } Q(x)\text{"}$$

- This is one of the most common statements in math:
  - **Example:**

    $$\text{"}\forall x \in \mathbb{R}, \text{ if } x > 2 \text{ then } x^2 > 4\text{"}$$

- **Remarks:**
  - Sometimes we shorten statements, for example the statement is often shortened to just

    $$\text{"if } x > 2 \text{ then } x^2 > 4\text{"}$$

  - Hence often $P(x)$ really means $\forall x, P(x)$.
    - I mean it'd obvious that if $x > 2$, then clearly it's a real number.

Some more Notation.

- **Equivalent forms:**

$$\text{“}\forall x \in D, Q(x)\text{”} \equiv \text{“if } x \in D, \text{then } Q(x)\text{”}$$
$$\text{“}\exists x \in D \text{ such that } Q(x)\text{”} \equiv \text{“}\exists x \text{ such that } x \in D \text{ and } Q(x)\text{”}$$

- **Notation:** The book uses

$$P(x) \implies Q(x) \text{ to mean } \forall x, P(x) \to Q(x)$$
$$P(x) \iff Q(x) \text{ to mean } \forall x, P(x) \leftrightarrow Q(x)$$

Section 3.2 Predicates and Quantified Statements II

Negation and Quantifiers:

- Consider the following statement:

  "For all students in this room, the student is taller than $4 feet$."

  - Is this true? Let's just assume everyone this in this class is at least 4 feet.
  - What is the negation of this statement? What would this statement false?
  -

    "There is at least one student that is NOT 4 feet tall"

- **Negation of Universal Statements:**

$$\sim (\forall x \in D, Q(x)) \equiv \exists x \in D \text{ such that } \sim Q(x)$$

- **Negation of Existential Statements:**

$$\sim (\exists x \in D, \text{ such that } Q(x)) \equiv \forall x \in D, \sim Q(x)$$

- **Example:** Consider the statement

  "No math courses have final exams"

  - **Part (a):** Write this formally
    - **Solution:** "$\forall$ math courses x, x has no final exam"
  - **Part (b):** Write the formal negation:
    - **Solution:** "$\exists$ a math course x such that x has a final exam"
  - **Part (c):** What is the informal negation
    - **Solution:** Some math courses have final exams.

- **Remark:**
  - If D is finite , say $D = \{x_1, x_2, \ldots, x_n\}$ then the following are logically equivalent:

$$\text{"}\forall x \in D, Q(x)\text{"} \equiv Q(x_1) \wedge \cdots \wedge Q(x_n)$$

    and

$$\text{"}\exists x \in D, \text{ such that } Q(x)\text{"} \equiv Q(x_1) \vee \cdots \vee Q(x_n)$$

  - **Example:** Let $D = \{0, 1, 2\}$ and $Q(x) =$ "$x \geq 1$" then

$$\text{"}\forall x \in \{0, 1, 2\}, x \geq 1\text{"} \stackrel{?}{\equiv} \text{"}0 \geq 1\text{"} \wedge \text{"}0 \geq 1\text{"} \wedge \text{"}0 \geq 1\text{"},$$

$$F \stackrel{?}{\equiv} F \wedge T \wedge T$$

$$F \stackrel{\checkmark}{\equiv} F$$

- **(Negation of If/Then)**What is the negation of $\rightarrow$? Recall $\sim (p \rightarrow q) \equiv p \wedge \sim q$,
  - Then

$$\sim (\forall x \in D, P(x) \rightarrow Q(x)) \equiv \exists x \in D \text{ such that } P(x) \wedge \sim Q(x)$$

    or similarly

$$\sim (\exists x \in D, P(x) \rightarrow Q(x)) \equiv \forall x \in D \text{ such that } P(x) \wedge \sim Q(x)$$

- **Example:** Write the **negation** of the statement

$$\text{"}\forall n \in \mathbb{Z}, \text{ if } n \text{ is prime then } n \text{ is odd or } n = 2\text{"}$$

  - **Solution:**
    - First as a self check, this statement is clearly true, hence its negation should be false:
    - Now $P(x) =$ "n is prime"
    - $Q(x) =$ "n is odd or $n = 2$"
    - (de Morgan's Law): $\sim Q(x) =$ "n is even and $n \neq 2$",
    - Putting it all together

      "$\exists n \in \mathbb{Z}, \text{ such that } n \text{ is prime and } n \text{ is even and } n \neq 2$"

      which is clearly false.

- **Remark:** We don't negate the universe of elements we live in

Vacuous Truth of Universal Statements:

- A statement of the form
$$\forall x \in D, (P(x) \to Q(x))$$
is said to be **vacuously true** or **true by default** if $P(x)$ is false, for all $x \in D$.
  - Why, consider its negation and consider $P(x) = F$
$$\begin{aligned} \sim (\forall x \in D, (P(x) \to Q(x))) &\equiv \exists x \in D, \text{such that } P(x) \wedge \sim Q(x) \\ &\equiv \exists x \in D, \text{such that } F \wedge \sim Q(x) \\ &\equiv \exists x \in D, \text{such that } F \\ &\equiv F \end{aligned}$$
    taking $\sim$ of both sides we have
$$(\forall x \in D, (P(x) \to Q(x))) \equiv T.$$
- **Example:** The following statement is vacuously true:
$$\text{“}\forall x \in \mathbb{Z}, (x = \pi \to x = 1)\text{”}$$

Converse and Contrapositive of a Universal Conditional Statement:

DEFINITION 31. The **contrapositive** of the statement $\forall x \in D, P(x) \to Q(x)$ is
$$\forall x \in D, \sim Q(x) \to \sim P(x)$$
and the **converse** is
$$\forall x \in D, Q(x) \to P(x).$$

- Read page 128-129 for use of “necessary”, “sufficient”, and “only if” in this contect.
- The Language has basiclly the same meaing except now we're using predicates with variables.
- **Example:** Find the Contrapositive of the statement
$$\text{“}\forall x \in \mathbb{R} \text{ if } x \geq 3 \text{ then } x^2 \geq 9.\text{”}$$
  - **Solution:**
$$\text{“}\forall x \in \mathbb{R} \text{ if } x^2 < 9 \text{ then } x < 3.\text{”}$$

Section 3.3 - Statements with Multiple Quantifiers.

- Compare the following two statements:
  (1) p : "$\forall$ positive integers x, $\exists$ a positive interger y such that $x < y$"
  (2) q: "$\exists$ a positive integers y such that $\forall$ positive intergers x, $x < y$ "
- **Questions:**
  (1) Is p true?
    – [Yes, given x, take $y = x + 1$.]
  (2) Is q true?
    – [No, such a y would be "the largest integer"]
- **Conclusion:**

"$\exists y$ such that $\forall x$" is **not** the same as "$\forall x, \exists y$ such that"

Negations of Multiply Quantified Statements.

- We can negate to get:

$$\begin{aligned} \sim (\forall x, \exists y \text{ such that } Q(x,y)) &\equiv \exists x \text{ such that } \sim (\exists y \text{ such that } Q(x,y)) \\ &\equiv \exists x \text{ such that } \forall y, \sim Q(x,y) \end{aligned}$$

- Similarly,

$$\sim (\exists x \text{ such that } \forall y,\, Q(x,y)) \equiv \forall x,\, \exists y,\, \text{such that } \sim Q(x,y).$$

- **Example:** Write the negation of the following statement p. Which one is true p or $\sim p$?

$$p \equiv \text{"}\forall x \in \{0,1,2\}\,, \exists y \in \{0,1,2\} \text{ such that } xy \geq y\text{"}$$

  – **Solution:**
  – The negation is

$$\sim p \equiv \text{"}\exists x \in \{0,1,2\} \text{ such that } \forall y \in \{0,1,2\}\,, xy < y\text{"}$$

  – Now for p we can check

$$x = 0 : \text{"}\mathbf{0 \cdot 0 \geq 0}\text{?"},\ \text{or "}0 \cdot 1 \geq 1\text{?"},\ \text{or "}0 \cdot 2 \geq 2\text{?"}$$
yes
$$x = 1 : \text{"}\mathbf{1 \cdot 0 \geq 0}\text{?"},\ \text{or "}\mathbf{1 \cdot 1 \geq 1}\text{?"},\ \text{or "}\mathbf{1 \cdot 2} \geq 2\text{?"}$$
yes
$$x = 2 : \text{"}\mathbf{2 \cdot 0 \geq 0}\text{?"},\ \text{or "}\mathbf{2 \cdot 1 \geq 1}\text{?"},\ \text{or "}\mathbf{2 \cdot 2 \geq 2}\text{?"}$$
yes

  – So p is true, so that $\sim p$ is false.
- **Remark:** We **don't** negate the universe of elements we live in (or the domain)
  – for example, don't negate $\forall x \in D$ with $\exists x \notin D$.
- **Example:** True or False?
  – **Part (a):** $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $x + y = \sqrt{2}$
    * **Solution:** True
  – **Part (b):** $\exists y \in \mathbb{R}$ such that $\forall x \in \mathbb{R}$, $x + y = \sqrt{2}$
    * **Solution:** False

CHAPTER 4

Elementary Number Theory and Methods of Proof

Section 4.1/4.2 Direct Proof and Counterexample I. and II.

- In this Chapter and section we'll learn about integers and their properties.
- **Assumptions:**
  - Let us assume we all know the basic laws of algebra and properties of the real numbers $\mathbb{R}$.
    - For example the commutative laws, associative law, etc ...
  - We also assume that the set of integers
    $$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$$
    is **closed** under $+, -, \times$. but not $\div$.
    - What this means is that if $n, m \in \mathbb{Z}$ then $n + m$ will also be an integer.
    - Similarly, $n, m \in \mathbb{Z}$ then $n - m$ will also be an integer.
    - And, $n, m \in \mathbb{Z}$ then $n \times m$ will also be an integer.
    - But, division is not *closed* in the set of integers. Meaning, if you divide two integers, that number may not necessarily be an integer. For example $1 \div 2 = \frac{1}{2} \notin \mathbb{Z}$.
- **Even and Odd:**
  - So now we will define what an **even** and **odd** number means. What do you think is the definition of even and odd, if you were to give a definition?
  - Or another question, let's say I give you a whole number, how can you write a computer program to tell if that number is even or odd?
    - One way to do it is to make a list of all odd and even numbers and simply ask the computer check if it's in the odd list or even lisr. But there is an infinite number integers. And computer would never be able to make an infinite list.
    - These are good questions to think about.
- Here are the mathematical definitions.

DEFINITION 32. An integer n is **even** if and only if there exists $k \in \mathbb{Z}$ such that $n = 2k$.

DEFINITION 33. An integer n is **odd** if and only if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$.

- **Remark:**
  - Notice that mathematical definitions always go both ways. Meaning they have "if and only if"
    - Even if it's not there written explicitly.
  - This means that if I tell you we **know** for a fact that the number n is **even,** then that means
    $$n = 2 \times \text{some integer.}$$
  - Vice Versa, let's say I discover that $n = 2 \times$ some integer, then
    $$n \text{ is an even number.}$$
  - The same goes for odd.
- **Examples:**
  - **Part (a):** Prove 8 is even.
    - **Solution:** Go back to the definition. The integer 8 is even because we can write it as
      $$8 = 2 \cdot 4$$
      and because we know $4 \in \mathbb{Z}$.
  - **Part (b):** Prove 15 is odd.

  - ∗ **Solution:** Go back to the definition. The integer 15 is odd because we can write it as

$$15 = 2 \cdot 7 + 1$$

    and because we know $7 \in \mathbb{Z}$.
- **Part (c):** Prove -15 is odd.
  - ∗ **Solution:** Go back to the definition. The integer -15 is odd because we can write it as

$$-15 = 2 \cdot (-8) + 1$$

    and because we know $-8 \in \mathbb{Z}$.

DEFINITION 34. An integer n is **prime** provided that $n > 1$ and for all positive integers r and s,

$$\text{if } n = rs, \text{ then either } r = n \text{ or } s = n.$$

An integer n is **composite** provided that $n > 1$ and

$$n = rs$$

for some integers r, s with $1 < r < n$ and $1 < s < n$.

- **Remark:** What is this saying? n is **prime** if and only if it can only be divisible by itself. All other positive integers are composite (meaning can be divided by some other integer other than itself)

Proving Existential Statements (constructive proofs of existence).

- The majority of proofs of existence statements (at this level) are **constructive**.
- Constructive Proofs of Existential Statements: Meaning, to **prove** the statement

$$\text{“}\exists x \in D, P(x)\text{”}$$

  you simply need to **produce** an x and **verify** $P(x)$ holds (and also that it is in D).
- **Example:** Prove

$$\text{“There exists a prime } p > 7 \text{ such that } p + 2 \text{ is prime”}$$

  - **Solution:**
  - Before you prove. You first need to do some work. Can you think of any candidates?

PROOF. Let $p = 11$. Then $p + 2 = 11 + 2 = 13$ and 13 is prime. □

- **Example:** (Exercise Section 4.1, #7) Prove there are real numbers a and b such that

$$\sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$

- **Solution:**
- Again before writing a proof down, you need to do some scratch work. Once you found it, then you can formally write the proof.

PROOF. Let $a = 1$ and $b = 0$. Then

$$\sqrt{a+b} = \sqrt{1+0} = \sqrt{1} = 1$$

But also

$$\sqrt{a} + \sqrt{b} = \sqrt{1} + \sqrt{0} = 1.$$

Hence for these values of a and b we have,

$$\sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$

□

Disproving Universal Statements by Counterexample.

- To disprove,
$$\text{“}\forall x, P(x)\text{”}$$
you simply have to find **counterexample**.
  - That is, find x and verify $\sim P(x)$.
- **Example:** Disprove
$$\text{“}\forall x, y \in \mathbb{R}, xy = 1 \to x = 1 \text{ and } y = 1\text{“}$$
  - **Solution:**
  - It is not hard to find a counterexample. Say $x = 2$ and $y = \frac{1}{2}$. Now write a proof formally.

PROOF. Note that $x = 2, y = \frac{1}{2}$ is a counterexample to this statement because
$$xy = 2 \cdot \frac{1}{2} = 1$$
but
$$x \neq 1 \text{ and } y \neq 1.$$
□

- **Example:** Disprove: For all nonnegative real numbers a and b,
$$\sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$
  - **Solution:** As usual, before writing up the proof try to do some scracth work.

PROOF. For a counterexample, let $a = 1$ and $b = 1$. Then
$$\sqrt{a+b} = \sqrt{1+1} = \sqrt{2},$$
However,
$$\sqrt{a} + \sqrt{b} = \sqrt{1} + \sqrt{1} = 2.$$
Since
$$\sqrt{2} \neq 2,$$
then we found values a, b such that
$$\sqrt{a+b} \neq \sqrt{a} + \sqrt{b}.$$
Hence the original statement is disproved. □

Proving Universal Statements of the form $\forall x \in D, P(x) \to Q(x)$.

- **Special Case - Method of Exhaustion**: When there are only finitely many elements in D satifying $P(x)$, then we can verify $Q(x)$ for each x.
  - **Example:** Prove using the method of exhastion: For each natural number n less than 3, $n^2 - n + 11$ is prime.
  - **Solution:** Recall the natural numbers are $\mathbb{N} = \{1, 2, 3, \dots\}$

PROOF. Recall that since $n = 1, 2$ are the only natural numbers less than 5, then we can check each one:
$$\text{When } n = 1, \text{ we have } 1^2 - 1 + 11 = 11 \text{ which is prime,}$$
$$\text{When } n = 2, \text{ we have } 2^2 - 2 + 11 = 13 \text{ which is prime.}$$
Hence the result. □

- In reality, do you think we can efficiently always prove by exhaustion? No! Because most sets are infinite, and we can't check an infinite number of things.
- **About Proofs:**
  - One can think of a proof as simply as an **algorithm** or **computer code**. It is specially useful when we have infinite number of possibilities in which a computer can't check. But we can imagine that if we can write a correct logical proofs, then it's the same thing as writing a correct computer code in which we can put into a magical computer that allows you to check infinite possibilities.
  - So don't think of proofs as nothing else other than a computer code.

- If you are able to write correct proofs, then you'll be able to correctly write correct algorithms (in any language).

- **General Case:** How to prove $\forall x \in D, P(x) \to Q(x)$
  1. Express statement clearly $\forall x \in D, P(x) \to Q(x)$ and figure out what $D, P(x), Q(x)$ are.
  2. Start the proof with
     (a) "Suppose x is an arbitrary of D and suppose $P(x)$ holds....."
     (b) Or you can say, "Let $x \in D$ be arbitrary. Assume $P(x)$. ....."
  3. Then prove $Q(x)$ holds using
     (a) definitions,
     (b) known properties,
     (c) or other results
  4. Last sentence:
     (a) "Hence, $Q(x)$, as desired."

- **Example 1:** Prove:

  "The sum of any two even integers is even."

  using symbols

  "$\forall n, m \in \mathbb{Z},$ if n, m are even, then $n + m$ is even."

  - **Solution:**
  - Before writing the proof formally. First let us do some **scratch work**:
  - How would I go about proving this.
  - Well, I know n, m are even. Use the definition you know about evens:
    * Since n is even, then there exists $k \in \mathbb{Z}$ such that $n = 2k$
    * Since m is even, then there exists $l \in \mathbb{Z}$ such that $m = 2l$.
  - Ok, now let's add them together

    $$n + m = 2k + 2l$$

    and we need to show this sum is even, hence we need to show

    $$n + m = 2 \times \text{some integer}$$

    in fact, we can factor the 2 out to get,

    $$n + m = 2k + 2l = 2(k + l).$$

  - Woohoo! sinve $k + l \in \mathbb{Z}$, then we find an integer such that

    $$n + m = 2 \times \text{some integer}.$$

  - Now let's write the proof down

Proof 1:

PROOF. Suppose $n, m \in \mathbb{Z}$ are arbitrary numbers and suppose n, m are even. We want to show $n + m$ is even. by the defintion of even, there exists integers k and l such that

$$n = 2k,$$
$$m = 2l.$$

Then

$$n + m = 2k + 2l = 2\left(k + l\right).$$

Since $k, l \in \mathbb{Z}$ then $k + l$ is also an integer since $\mathbb{Z}$ is closed. Thus, $n + m$ is even, as desired. □

- There is no one way of writing a proof. Here's another way of writing the proof to the **Example** 1 above.

Proof 2:

PROOF. Suppose $n, m \in \mathbb{Z}$ and n, m are both even. There $n = 2r$ and $m = 2s$, for some $r, s \in \mathbb{Z}$. Let $k = r + s$. Then, since $r, s \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition, we know $k \in \mathbb{Z}$. Moreover,

$$n + m = 2r + 2s = 2(r + s) = 2k.$$

Thus, $n + m$ is even, as desired. □

- **Find the mistake:** Finally, find the mistake is this proof for **Example1:**

Wrong Proof:

PROOF. Suppose $n, m \in \mathbb{Z}$ and n, m are both even. There $n = 2k$ and $m = 2k$, for some $k \in \mathbb{Z}$. Let $k = r + s$. Then

$$n + m = 2k + 2k = 2(k + k).$$

Since $k \in \mathbb{Z}$ then $k + k$ is also an integer since $\mathbb{Z}$ is closed. Thus, $n + m$ is even, as desired. □

- **Mistake?**
  - The mistake is that we used the same k for n and m. Remember n, m are arbitrary integers, hence they don't have to have the same even multiple.
- **Homework:** Read Section 4.2 (pages 173-177). No Seriously!
  - There is good advice there about good proof writing and about common mistakes.

Section 4.3 Direct Proof and Counterexample III. Rational Numbers

- We start with the definition of rational numbers.

DEFINITION 35. A real number r is **rational** if and only if there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $r = \frac{a}{b}$. The set of rational numbers is denoted by

$$\mathbb{Q} = \left\{ x \in \mathbb{R} \mid x = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

A real number that is not rational is called **irrational**.

- **Example:** Examples of rational numbers include
  - $\frac{1}{3}$,
  - .88888.... and -0.45.
  - In fact, any decimal number with a repeating pattern is rational. Like

    $$.263818274545454545.....$$

    is rational.
  - But

    $$\pi, \sqrt{2}, e$$

    are not rational numbers. For now it is now so obvious why $\pi, \sqrt{2}, e$ are irrational. We will look at prof later one.
- Here's an important property we'll use often.
- **Zero Product Property:**

  $$\text{If } a, b \neq 0, \text{ then } ab \neq 0.$$

  - You may be more familiar with the contrapositive of this statement:

    $$\text{If } ab = 0, \text{ then either } a \text{ or } b \text{ is zero.}$$

THEOREM. *(Theorem 4.3.2 in book) The sum of any two rational numbers is rational*

- **Example:** Prove 4.3.2
  - **Solution:**
  - First let us do some scratch wook before writing a formal proof.
  - Suppose $r = \frac{a}{b}$, $s = \frac{c}{d}$ are rational and $b, d \neq 0$. Then let's trying adding them together:

    $$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{\text{integer}}{\text{some other integer } \neq 0}$$

  - Since this is a fraction of integers then $r + s$ is a rational number.
  - Now let's write a formal proof:

PROOF. Suppose r and s are rational. Then there exists integers a, b, c, d with $b, d \neq 0$ such that $r = \frac{a}{b}$ and $s = \frac{c}{d}$. Thus,

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Since $\mathbb{Z}$ is closed under $\times$ and $+$, then $ad + bc$ and bd are integers. Further, we know that $bd \neq 0$ since neither b or d are zero (Zero product property). Therefore, $r + s$ is a rational number, as needed. □

Section 4.4 Direct Proof and Counterexample IV: Divisibility Properties

- We start with a definition.

DEFINITION 36. Let $n, d \in \mathbb{Z}$. Then n is **divisible** by d if and only if $n = dk$ for some $k \in \mathbb{Z}$ and $d \neq 0$.

- Other Terminology:
  - n is a **multiple** of d,
  - d is a **factor** of n,
  - d is a **divisor** of n,
  - d is a **divisor** of n,
  - d **divides** n , written
$$d \mid n.$$
    - This is the one that is most commonly used in (upper level) mathematics. This is the one I will use most frequently.
    - Think of $\frac{n}{d} = k$ or $n = dk$.
    - Also, the notation $d \mid n$ is a statement, not a number.
- **Examples:**
  - **Part (a):** Does $3 \mid 15$?
    - Yes since $15 = 3 \cdot 5$ and $5 \in \mathbb{Z}$.
  - **Part (b):** Is 7 a factor of 28?
    - Yes, $28 = 7 \cdot 4$ and $4 \in \mathbb{Z}$
  - **Part (c):** Does $3 \mid 8$?
    - No, $8 = 3 \cdot \frac{8}{3}$ but $\frac{8}{3} \notin \mathbb{Z}$
  - **Part (d):** What are the divisors of 1?
    - They ± 1. This is proved on page 191.

THEOREM. *(Theorem 4.4.3, Transitivity of Divisibility) For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

- **Example:** Prove Theorem 4.4.3.
  - **Solution:**
  - Scratch Work:
  - Okay, so how do we start writing proofs? First just write the definitions of the assumptions given in the theorem.
  - **Given:** Okay, so what do I know? I know $a, b, c \in \mathbb{Z}$ and I know $a \mid b$ and $b \mid c$. So write that first:
$$b = ak, \text{ for some } k \in \mathbb{Z}$$
$$c = bl, \text{ for some } l \in \mathbb{Z}$$
  - Want to show what? Want to show $a \mid c$, or in other words, need to show
$$c = a \cdot (\text{some integer}).$$
    - Let us find this integer.
    - Using what we know we have
$$c = bl = (ak)\, l = a \cdot (kl)$$
    - Woohoo! we found the integer! It is kl !
  - Let's write the **formal proof:**

PROOF. Suppose $a, b, c \in \mathbb{Z}$ and that $a \mid b$ and $b \mid c$. By the definition, this means
$$b = ak, \text{ for some } k \in \mathbb{Z}$$
$$c = bl, \text{ for some } l \in \mathbb{Z}.$$
Thus,
$$c = bl = (ak)\, l = a \cdot (kl)\,.$$
Call $n = kl$. Since $\mathbb{Z}$ is closed under multiplication, then we know $kl \in \mathbb{Z}$. Thus
$$c = an, \text{ where } n \text{ is an integer.}$$

Then it follows that $a \mid c$, as desired. □

Section 4.5 Direct Proof and Counterexample V: Division Into Cases; the Quotient-Remainder Theorem.

- Consider the following theorem:

THEOREM. *(Theorem 4.5.1, The Quotient-Remainder Theorem) Given an integer n and a positive integer d, there exists unique integers q and r such that*

$$n = dq + r, \qquad \text{and } 0 \leq r < d.$$

*Here q is called the **quotient** and r is called the **remainder**.*

PROOF. See book for a proof. □

- **What is this Theorem saying:**
  - This theorem tells us what happens when you can't divide two integers. It basically says that there is always a remainder.
  - If you are trying to divide n by d, then this gives the best *approximate* way of doing this.
- **Example1:**
  - **Part(a):** If $n = 55$ and $d = 4$, then

$$\begin{aligned} 55 &= 4 \cdot ? + ? \\ &= 4 \cdot 13 + 3 \end{aligned}$$

    * $q = 13$ and $r = 3$.
  - **Part (b):** If $n = -55$ and $d = 4$, then

$$\begin{aligned} -55 &= 4(?) + ? \\ &= 4 \cdot (-14) + 1 \end{aligned}$$

DEFINITION 37. Given a *non-negative integer* n and a positive integer d,

$$n \; div \; d = \text{the integer quotient of } n \text{ divided by } d$$

and

$$n \mod d = \text{the integer remainder of } n \text{ divided by } d$$

- **Example1-revisited:**
  - **Part(a):** $55 \text{ div } 4 = 13$ and $55 \mod 4 = 3$.
  - **Part(b):** Find $38 \text{ div } 5$ and $38 \mod 5$.
    * Note that $38 = 5 \cdot ? + ?$
    * We have that $38 = 5 \cdot 7 + 3$ hence

$$\begin{aligned} 38 \text{ div } 5 &= 7 \\ 38 \mod 5 &= 3 \end{aligned}$$

- **Representation of Integers**
- Let's rewrite here the Quotient-Remainder (Q-R) Theorem using symbols:

$$\forall n \in \mathbb{Z}, \forall d \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z} \text{ s.t.} n = dq + r, \text{ and } 0 \leq r < d.$$

  - Here $\exists!$ means **"there exists a unique".**
- One interesting application of the Quotient-Remainder Theorem is that it proves the following statement.

THEOREM. *Every integer is either even or odd but not both.*

- **Remark:** This may seem obvious to us. But how do we know we haven't missed a number that is neither even or odd? There is no way we can check all the integers, since they are infinite.
- Here is why this theorem is true:
  - Sketch of Proof: Using the Q-R Theorem with $n \in \mathbb{Z}$ being **any** integer and $d = 2$, we have that there exists a unique $q, r \in \mathbb{Z}$ such that

$$n = 2q + r, \text{ where } 0 \leq r < 2.$$

  - But the only integers r that satify $0 \leq r < 2$ are $r = 0, 1$.

- Hence n is either
$$n = 2q \text{ or } n = 2q + 1.$$
- Meaning either n is even or odd.

- **Generalization:** In fact, you can generalize this type of argument to break the integers into pieces:
  - Using $d = 3$, in the E-R Therem being **any** integer N and with $d = 3$, we have that there exists a unique $q, r \in \mathbb{Z}$ such that
  $$n = 3q + r, \text{ where } 0 \leq r < 3.$$
  - But the only integers r that satify $0 \leq r < 3$ are $r = 0, 1, 2$.
  - **Q-R when $d = 3$:** Hence every integer n can be write as either
  $$n = 3q, n = 3q + 1 \text{ or } n = 3q + 2.$$
    - **Example:** If $n = 5$ use the previous result to figure out which one n belongs to
    $$5 = 3q?$$
    $$5 = 3q + 1? \text{ or}$$
    $$5 = 3q + 2?$$
    - **Solution:** The answer is the third option with $q = 1$:
    $$5 = 3 \cdot 1 + 2.$$

- **Proof by cases:**
- **Example(Harder):** Use the Q-R statement with $d = 3$ to prove the following statement:

  "The square of any integer has the form $3k$ or $3k + 1$ for some integer k"

  - **Solution:**
  - First start with a sketch by (1) Writing what you know, the given (2) Understand what you want to show (3) Use what you know to prove it
  - **Sketch of Proof:**
  - (1) What do we know? In this case, the problem tellus you use the Q-R statement with $d = 3$: For any integer $n \in \mathbb{Z}$ there exists a unique $q, r \in \mathbb{Z}$ such that
  $$n = 3q + r, \text{ where } 0 \leq r < 3.$$
  - But the only integers r that satify $0 \leq r < 3$ are $r = 0, 1, 2$. Thus this splits n into 3 cases:
  - Either
    - Case 1: $n = 3q$,
    - Case 2: $n = 3q + 1$, or
    - Case 3: $n = 3q + 2$.
  - (2) What do you want to show? (WTS) I want to show n^2 can be written as (a) $n^2 = 3k$ or (b) $n^2 = 3k + 1$ for some k. We need to find k!
  - (3) Try to prove it:
    - Case 1: If $n = 3q$, then
    $$n^2 = (3q)^2 = 9q^2 = 3 \cdot \left(3q^2\right) = 3\underbrace{\left(3q^2\right)}_{k}$$
    and the k is equal to $k = 3q^2$. Thus n^2 can be written in the type (a):
    $$n^2 = 3k.$$
    - Case 2: If $n = 3q + 1$, then
    $$\begin{aligned} n^2 &= (3q + 1)^2 = 9q^2 + 6q + 1 = 3\left(3q^2 + 2q\right) + 1 \\ &= 3\underbrace{\left(3q^2 + 2q\right)}_{k} + 1 \end{aligned}$$
    and the k is equal to $k = 3q^2 + 2q$. Thus n^2 can be written in the type (b):
    $$n^2 = 3k + 1$$

* Case 3: If $n = 3q + 2$, then

$$n^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3\underbrace{\left(3q^2 + 4q + 1\right)}_{k} + 1$$

and the k is equal to $k = 3q^2 + 4q + 1$. Thus n^2 can be written in the type (b):

$$n^2 = 3k + 1.$$

- **The formal proof would look like this:**
- Try it yourself as an exercise to write the formal Theore/proof of this Example:

THEOREM. *If $n \in \mathbb{Z}$ then n^2 is either equal to $3k$ or $3k+1$ for some integer k.*

PROOF. Suppose $n \in \mathbb{Z}$. Using the Quotient Remainder Theorem with $d = 3$, there exists a unique $q, r \in \mathbb{Z}$ such that

$$n = 3q + r, \text{ where } 0 \leq r < 3.$$

But the only integers r that satify $0 \leq r < 3$ are $r = 0, 1, 2$. Thus this splits n into 3 cases. Either

$$\text{Case 1:} n = 3q$$
$$\text{Case 2:} n = 3q + 1, \text{or}$$
$$\text{Case 3:} n = 3q + 2.$$

We want to prove n^2 is either of the form (a) $3k$ or of the form (b) $3k + 1$.

Case 1: If $n = 3q$, then

$$n^2 = (3q)^2 = 9q^2 = 3 \cdot \left(3q^2\right) = 3\underbrace{\left(3q^2\right)}_{k}$$

and the k is equal to $k = 3q^2$. Since $\mathbb{Z}$ is closed under multiplication then $k \in \mathbb{Z}$. Thus n^2 can be written in the type (a):

$$n^2 = 3k.$$

Case 2: If $n = 3q + 1$, then

$$\begin{aligned} n^2 &= (3q+1)^2 = 9q^2 + 6q + 1 = 3\left(3q^2 + 2q\right) + 1 \\ &= 3\underbrace{\left(3q^2 + 2q\right)}_{k} + 1 \end{aligned}$$

and the k is equal to $k = 3q^2 + 2q$. Since $\mathbb{Z}$ is closed under multiplication and addition then $k \in \mathbb{Z}$. Thus n^2 can be written in the type (b):

$$n^2 = 3k + 1.$$

Case 3: If $n = 3q + 2$, then

$$n^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3\underbrace{\left(3q^2 + 4q + 1\right)}_{k} + 1$$

and the k is equal to $k = 3q^2 + 4q + 1$. Since $\mathbb{Z}$ is closed under multiplication and addition then $k \in \mathbb{Z}$. Thus n^2 can be written in the type (b):

$$n^2 = 3k + 1.$$

This is what we desired to show. □

- **Example:** See Theorem 4.5.3 and its proof in the book for more practice in using the Q-R Theorem in a proof.
  - Exercise 27 is done similarly.
  - Execise 29 is the Example we did today.

Section 4.6 - Direct Proof and Counterexample VI: Floor and Ceiling.

- We start by defining the **floor** and **ceiling** function for real numbers.

DEFINITION 38. Given a real number x, the **floor** of x, denoted $\lfloor x \rfloor$, is the unique integer n such that

$$n \leq x < n+1.$$

DEFINITION 39. Given a real number x, the **ceiling** of x, denoted $\lceil x \rceil$, is the unique integer n such that

$$n-1 < x \leq n.$$

- **Remarks:**
  - The **floor** function is basically the function that rounds any real number x down to the closest integer n
  - The **ceiling** function is basically the function that rounds any real number x up to the closest integer n
- **Example:**
  - **Part (a):** If $x = \frac{21}{4}$ then
  $$\left\lfloor \frac{21}{4} \right\rfloor = 5$$
  $$\left\lceil \frac{21}{4} \right\rceil = 6$$
  since $\frac{21}{4} = 5.25$ and $5 < 5.25 < 6$.
  - **Part (b):** If $x = -\frac{3}{4}$ then
  $$\left\lfloor -\frac{3}{4} \right\rfloor = -1$$
  $$\left\lceil -\frac{3}{4} \right\rceil = 0.$$
  - **Part (c):** If $x = .999$ then
  $$\lfloor .999 \rfloor = 0$$
  $$\lceil .999 \rceil = 1.$$
  - **Part (d):** If $x = 5$ then
  $$\lfloor 5 \rfloor = 5$$
  $$\lceil 5 \rceil = 5.$$

THEOREM. *(Theorem 4.6.2) For any integer,*

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

- **Example:** Prove the odd case in Theorem 4.6.2. That is, prove

"If n is odd then $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$."

(The even case is for Homework)

  - **Sketch of Proof:**
  - Given: What is given is that n is odd. That means
  $$n = 2k+1 \text{ for some } k \in \mathbb{Z}.$$
  - Definitions: I also know the definition of floor function $\lfloor x \rfloor$, it is equal to the unique integer j such that
  $$j \leq x < j+1.$$
  - I want to show: that $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$.

– Try to prove it: Well first let's just plug in $n = 2k + 1$ and get

$$\begin{aligned}\left\lfloor \frac{n}{2} \right\rfloor &= \left\lfloor \frac{2k+1}{2} \right\rfloor \\ &= \left\lfloor k + \frac{1}{2} \right\rfloor\end{aligned}$$

but since

$$k < k + \frac{1}{2} < k + 1$$

then rounding down we have that

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

– But remenber that $n = 2k + 1$, solving for n we get $k = \frac{n-1}{2}$ thus

$$\left\lfloor \frac{n}{2} \right\rfloor = k = \frac{n-1}{2}.$$

as needed.

Section 4.7 - Indirect Argument: Contradiction and Contrapositive.

- Sometimes a **direct** proof (all the proofs we've done so far were direst) are impossible or mayve very difficult.
  - Thus we look for different ways of proving theorems.
- **Proof by Contradiction:**
  - Outline of Method:
  - (1) Assume that the statement you want to show is actually false.
  - (2) Show that by assuming it's false actually leads to a "contradiction" (something absurd that we know is not true)
  - (3) Conclude that the original statement must have been true.
- **Example:** Prove "There is no integer that is both even and odd".
  - **Sketch of proof:**
  - Assume by **contradiction** that the statement is false. Meaning, that there is an integer that is both even and odd. Let $n \in \mathbb{Z}$ be this integer that is both even and odd. Then this means
$$n = 2k, \text{ for some } k \in \mathbb{Z}$$
$$n = 2l + 1, \text{ for some } l \in \mathbb{Z}.$$
  - Now we need to find something absurd!
  - Try using the only thing that you know: That $n = 2k$ and $n = 2l + 1$. I don't know. Maybe let's try setting them equal to each since they are equal.
$$2k = n = 2k + 1$$
or
$$2k = 2l + 1$$
  - Then let's bring the variables to the same side.
$$2k - 2l = 1$$
and divising by 2 we get
$$k - l = \frac{1}{2}.$$
  - Okay. Does anybody see anything absurd yet?
    - Well since $k, l \in \mathbb{Z}$ and since $\mathbb{Z}$ is closed under subtraction then
$$k - l = \frac{1}{2} \in \mathbb{Z}$$
which is absurd since we know $\frac{1}{2} \notin \mathbb{Z}$.
    - Thus this is a contradiction. Hence the original statement must have been true.
  - **Formal proof:**

PROOF. Assume by contradiction that the statement is false. Meaning, that there is an integer that is both even and odd. Let $n \in \mathbb{Z}$ be this integer that is both even and odd. Then this means
$$n = 2k, \text{ for some } k \in \mathbb{Z}$$
$$n = 2l + 1, \text{ for some } l \in \mathbb{Z}.$$
Thus means
$$2k = 2l + 1.$$
After doing some algebra
$$k - l = \frac{1}{2}.$$
But $k, l \in \mathbb{Z}$ and since $\mathbb{Z}$ is closed under subtraction then
$$k - l = \frac{1}{2} \in \mathbb{Z},$$
which is absurd since we know $\frac{1}{2} \notin \mathbb{Z}$. Thus this is a contradiction. Hence the original statement must have been true. □

- **Proof of an If/Then by Contrapositive:**
  - Sometime proving $p \to q$ is harder. But remember that "$p \to q$" is equivalent to its contrapositive "$\sim q \to \sim p$".
- **Example (The even number Theorem):** Prove using the contrapositive the statement

  "For $n \in \mathbb{Z}$ if n^2 is even, then n is even."

  - **Solution:**
  - A direct proof of this would be difficult because it would involve taking square roots. Which we'd like to avoid/
  - First let's write the **contrapositive**:

    "For $n \in \mathbb{Z}$ if n is odd, then n^2 is odd."

  - Let's go straight to proving it. Thought you should always try to write the sketch of the proof first.

PROOF. We will prove by contrapositive. Suppose $n \in \mathbb{Z}$ and that n is odd. By the definition of odd this means

$$n = 2k + 1, \text{ where } k \in \mathbb{Z}.$$

Squaring we have

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\underbrace{\left(2k^2 + 2k\right)}_{l} + 1.$$

Let $l = 2k^2 + 2k$, and we know that $l \in \mathbb{Z}$. Thus

$$n^2 = 2l + 1$$

hence n^2 is odd. □

- **Example:** Try yourself to prove the similar statement:

  "For $n \in \mathbb{Z}$ if n^2 is odd, then n is odd."

  using the contrapositive.

Section 4.8 - Two Classical Theorems

- Here we present two very classical and important theorems in math and theoretical computer science.

THEOREM. ***1*** *The number $\sqrt{2}$ is irrational*

THEOREM. ***2*** *The set of prime numbers is infinite.*

- We'll focus on Theorem 1.
- But Theorem 2 is very important, and computers have been able to find the largest prime number known to humans, so far.
- **See the wikipedia page**: `https://en.wikipedia.org/wiki/Largest_known_prime_number`
  - https://en.wikipedia.org/wiki/Largest_known_prime_number
  - Where as of August 20,2020, the largest known prime number is
$$n = 2^{82,589,933} - 1.$$
  - This is a massiv number with over 24 million digits.
  - Unfortunately we'll never know all of them.
  - But we can prove that there is an infinite number of them! And the proof is not too hard. See the book.
- **Irrational Numbers:**
- Before proving Theorem 1 about $\sqrt{2}$.
- We'll focus on proving an easier theorem.
- **Example:** Prove the statement

"If r is irrational then $5r + 3$ is irrational."

using Theorem 1.
  - **Solution:**
  - **Sketch of Proof:**
  - It is very hard to prove a number is irrational. It is much easier to prove it is rational.
  - So let us prove by contradiction.
  - Suppose the statement is not true. Meaning suppose r is irrational but somehow $5r + 3$ is rational. But if it's rational then
$$5r + 3 = \frac{a}{b} \text{ where } a, b \in \mathbb{Z}, b \neq 0.$$
  - Let's find something absurd (a contradiction).
  - Remember that the problem gave you hint. Use the fact that you know r is irrational.
  - So let's solve for it
$$\begin{aligned} 5r + 3 = \frac{a}{b} &\iff 5r = \frac{a}{b} - 3 \\ &\iff r = \frac{a}{5b} - \frac{3}{5} \end{aligned}$$
    but by finding a common denominator
$$r = \frac{a - 3b}{5b}$$
    but $a - 3b$ and $5b$ are integers hence this means r is a rational number, which is absurd!
  - Thus we found a contradiction. Hence the original statement must have been true. That $5r+3$ is actually an irrational number.
  - **Formal Proof:**

PROOF. Let us prove by contradiction. Suppose the statement is not true. But this means $5r + 3$ is rational. But if it's rational then
$$5r + 3 = \frac{a}{b} \text{ where } a, b \in \mathbb{Z}, b \neq 0.$$

Thus

$$\begin{aligned} 5r+3=\frac{a}{b} &\iff 5r=\frac{a}{b}-3 \\ &\iff r=\frac{a}{5b}-\frac{3}{5} \end{aligned}$$

by finding a common denominator

$$r=\frac{a-3b}{5b}$$

but $a-3b$ and $5b$ are integers hence this means r is a rational number, which is absurd! This is a contradiction. Hence the original statement must have been true. That $5r+3$ is actually an irrational number. □

- **Example:** A similar proof would be prove the statement:

  "Suppose $n, m \in \mathbb{Z}$ and x is irrational, then $n+xm$ is irrational."

- **Proof of Theorem 1:**
- Now let's prove the famous theorem. I'll restate it here again:

THEOREM. ***1*** *The number $\sqrt{2}$ is irrational.*

PROOF. (Proof by contradiction) Suppose that the statemement is not true and that $\sqrt{2}$ is rational. Then

$$\sqrt{2}=\frac{a}{b}, \text{ where } a, b \in \mathbb{Z}, b \neq 0.$$

Now assume that the fraction $\frac{a}{b}$ is **reduced**. (Has no common divisors). We can do this with any fraction.

Now, let's come up with a contradiction. Squaring both sides we get

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

and

$$2b^2=a^2. \text{ (Equation 1)}$$

Now since $a^2=2(b^2)$, then we now that a^2 is even. By the Even Number Theorem (from section 4.7), then a is also even. This means,

$$a=2k, \text{ for some } k \in \mathbb{Z}.$$

Substituting this in Equation 1, we have that

$$\begin{aligned} 2b^2=a^2 &\iff 2b^2=(2k)^2 \\ &\iff 2b^2=4k^2 \\ &\iff b^2=2k^2, \end{aligned}$$

and this shows that b^2 is even. Again by the Even Number Theorem, then this means b is even a well.

(Do you see the contradiction yet?) We just proved that both a, b are even, but remenber that we said above that a, b have no comon diviors. But if they are both even, then clearly they have 2 as a common divisor. Thus this is a contradiction. Hence the original statement must have been true. That is, $\sqrt{2}$ is irrational. □

CHAPTER 5

Sequences, Mathematical Induction, and Recursion

Section 5.1 - Sequences

- Informally, a **sequence** is a list.
  - It can be finite: $a_1, a_2, \ldots, a_n$
  - It can be infinite: $a_1, a_2, \ldots$
- **Examples:**
  - (1) Consider the infinite sequence $a_1, a_2, \ldots$ given by $a_i = \frac{i+1}{i+2}$. This is the sequence
$$\frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots$$
  - (2) Write out the first five terms of the sequence $a_2, a_3, \ldots$ where $a_k = \frac{(-1)^k}{2^k}$.(Note we can start the sequence with any index)
    - **Solution:**
$$\frac{1}{4}, -\frac{1}{8}, \frac{1}{16}, -\frac{1}{32}, \frac{1}{64}.$$

Finding an explicit formula for a Sequence.

- **Example:** Find an explicit formula for the sequence
$$1, -\frac{1}{4}, \frac{1}{9}, \frac{-1}{16}, \frac{1}{25}, \ldots$$
  - **Part(a):** Find a formula where you start with $a_1, a_2, a_3, \ldots$
    - **Solution:**
      - First look how the signs are changing: $1, -1, 1, -1$. So whenever you have an alternating sequence, it will have a factor of
$$(-1)^{\text{power}}.$$
      - Note that $(-1)^{k+1}$ works.
      - The denominators are $1^2, 2^2, 3^2, \ldots$ hence
$$a_k = \frac{(-1)^{k+1}}{k^2}.$$
  - **Part(b):** Find a formula where you start with $a_0, a_1, a_2, \ldots$
    - **Solution:**
$$a_k = \frac{(-1)^k}{(k+1)^2}.$$

Summation notation.

- **Notation:** For a fixed integer n,
$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_n.$$
  Similarly,
$$\sum_{k=m}^{n} a_k = a_m + a_2 + \cdots + a_n.$$

- **Example:** Evaluate $\sum_{k=2}^{6}\left(k^2+1\right)$
  - **Solution:**

$$\begin{aligned}\sum_{k=2}^{6}\left(k^2+1\right) &= \left(2^2+1\right)+\left(3^2+1\right)+\left(4^2+1\right)+\left(5^2+1\right)+\left(6^2+1\right)\\ &= 5+10+17+26+37\\ &= 95\end{aligned}$$

Expressing a Finite Sum in Summation Notation.

- **Exanple:** Write $1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}$ in summation notation:
  - **Solution:**

$$\sum_{k=1}^{5}(-1)^{k+1}\frac{1}{k} \text{ or } \sum_{k=0}^{4}(-1)^{k}\frac{1}{k+1}.$$

Product Notation.

- **Notation:** For a fixed integer n,

$$\prod_{k=1}^{n} a_k = a_1\cdot a_2\cdot\cdots\cdot a_n.$$

- Similarly,

$$\prod_{k=n}^{n} a_k = a_n\cdot a_2\cdot\cdots\cdot a_n.$$

- **Example:** Evaluate $\prod_{k=1}^{3}\frac{k}{k+1}$:
  - **Solution:**

$$\begin{aligned}\prod_{k=1}^{3}\frac{k}{k+1} &= \frac{1}{1+1}\cdot\frac{2}{2+1}\cdot\frac{3}{3+1}\\ &= \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{3}{4}\\ &= \frac{1}{4}.\end{aligned}$$

Factorial Notation.

- We start with a definition.

DEFINITION 40. Given $n\in\mathbb{N}$, we define $n! = n\left(n-1\right)\cdots 3\cdot 2\cdot 1$ also $0!=1$.

- **Example:**
  (1) $5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$
  (2) $\frac{10!}{9!} = \frac{10\cdot 9!}{9!} = 10$
  (3) $\frac{(n+1)!}{n!} = \frac{(n+1)\cdot n!}{n!} = n+1$
  (4) And

$$\begin{aligned}\frac{(n-2)!}{n!} &= \frac{(n-2)!}{n\left(n-1\right)(n-2)!}\\ &= \frac{1}{n\left(n-1\right)}\\ &= \frac{1}{n^2-n}\end{aligned}$$

Properties of Sums and Products.

- The following properties are very useful:

THEOREM. *The following hold for any* $n \in \mathbb{N}$

(1) $\displaystyle\sum_{k=1}^{n}(a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k$

(2) $\displaystyle\sum_{k=1}^{n}(ca_k) = c\sum_{k=1}^{n} a_k$ *where* $c \in \mathbb{N}$ *or* $c = f(n)$

(3) $\displaystyle\prod_{k=1}^{n}(a_k \cdot b_k) = \left(\sum_{k=1}^{n} a_k\right) \cdot \left(\sum_{k=1}^{n} b_k\right)$

- **Example:** Express

$$\sum_{k=1}^{n}\left(k^2+1\right) + 3\sum_{k=1}^{n}\left(1-2k^2\right)$$

as a single sum.

  - **Solution:** Using the properties above we obtain

$$\begin{aligned}\sum_{k=1}^{n}\left(k^2+1\right) + 3\sum_{k=1}^{n}\left(1-2k^2\right) &= \sum_{k=1}^{n}\left(k^2+1\right) + \sum_{k=1}^{n} 3\left(1-2k^2\right)\\ &= \sum_{k=1}^{n}\left[\left(k^2+1\right) + 3\left(1-2k^2\right)\right]\\ &= \sum_{k=1}^{n}\left(k^2+1+3-6k^2\right)\\ &= \sum_{k=1}^{n}\left(4-5k^2\right).\end{aligned}$$

Section 5.2 - Mathematical Induction - Proving formulas

- Consider the following sum
$$\sum_{i=1}^{n} i = 1 + 2 + \cdots + n$$
  - There's got to be a better way to compute this sum rather than summing term by term.
  - For example, the sum
$$1 + 2 + \cdots + 100$$
  - Do you know what this sum is? It turns out it's
$$5050.$$
  - But I didn't figure this out by adding every term. It turn's there is a nice formula for it:
$$\sum_{i=1}^{n} i = \frac{n\,(n+1)}{2}.$$
- **Example:**
  - **Part(a):** Compute $1 + 2 + 3 + \cdots + 100$ using the formula:
    - **Solution:** Using $n = 100$, we have
$$\sum_{i=1}^{100} i = \frac{100 \cdot 101}{2} = 50 \cdot 101 = 5050.$$
  - **Part (b):** What about $1 + 2 + 3 =$?
    - **Solution:** Well obviously we know that $1 + 2 + 3 = 6$. But, just as a reality check, let's use the formula to confirm this:
$$\sum_{i=1}^{3} i = \frac{3 \cdot 4}{2} = \frac{12}{2} = 6.$$
- The following principle is useful then proving formulas like the these:
  - Please make sure you have this memorized:
- The **Principle of Mathematical Induction:**
  - Let $P(n)$ be a property that is defined for integers n and let a be a fixed integer. Suppose the following two properties hold:
    (1) $P(a)$ is true
    (2) $\forall k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true.
  - Then $P(n)$ is true for all $n \geq a$.
- **Method of Proof:** How to prove $P(n)$ is true for all $n \geq a$.
  - Base case: Show $P(a)$ is true.
  - Inductive hypothesis: Assume the formula holds for $n = k$.
  - Inductive step: Show the formula is true for $n = k + 1$.
- **Example:** Prove that for all integers $n \geq 1$,
$$1 + 2 + \cdots + n = \frac{n\,(n+1)}{2},$$
using mathematical induction.

Proof. For $n \in \mathbb{N}$ let $P(n)$ be the statement
$$1 + 2 + \cdots + n = \frac{n\,(n+1)}{2}.$$
Base Case: For $n = 1$, we have that the left hand side is
$$\text{LHS} = 1$$
and the right hand side is
$$\text{RHS} = \frac{1 \cdot 2}{2} = 1.$$
Thus the formula is true for $n = 1$.

Inductive hypothesis: We assume the formula holds for $n = k$. That is, assume

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}. \quad (\star)$$

is true.

Inductive step: Using the inductive hypothesis, we want to show that the formula holds for $n = k + 1$, that is

$$1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}. \quad (\star\star)$$

To prove this, we start with the Left Hand side(LHS),

$$\begin{aligned}
1 + 2 + \cdots + (k+1) &= \underbrace{1 + 2 + \cdots + k}_{} + (k+1) \\
&= \underbrace{\frac{k\,(k+1)}{2}} + (k+1)\,, \text{ by inductive hypothesis } (\star) \\
&= \frac{k\,(k+1)}{2} + \frac{2\,(k+1)}{2} \\
&= \frac{k\,(k+1) + 2\,(k+1)}{2} \\
&= \frac{(k+1)\,(k+2)}{2}, \text{ by factoring } k+1.
\end{aligned}$$

Thus we have shown $(\star\star)$.

Thus by induction, the formula holds for all integers $n \geq 1$. □

- **Geometric Sum:**
- The sequence,

$$a, ar, ar^2, ar^3, \ldots$$

is called a **geometric sequence** with ratio r.

THEOREM. *(Geometric Sum)*
For any real number $r \neq 1$ and any integer $n \geq 0$,

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

Or using summation notation,

$$\sum_{k=0}^{n} r^k = \frac{r^{n+1} - 1}{r - 1}.$$

- Remark:
  - Note the formula doesn't work when $r = 1$. Since

$$1 + 1^1 + \cdots + 1^n \neq \frac{1^{1+1} - 1}{1 - 1}.$$

- **Examples:**
  - **Part (a):** Use the geometric sum formula to compute

$$1 + 2 + 4 + 8 + \cdots + 2^{10}.$$

  - **Solution:** This sum is the sum

$$1 + r^2 + r^3 + \cdots + r^{10}$$

where $r = 2$. Hence

$$\begin{aligned}\sum_{k=0}^{10} 2^k &= \frac{2^{10+1}-1}{2-1} \\ &= \frac{2^{11}-1}{1} \\ &= 2048 - 1 \\ &= 2047\end{aligned}$$

- **Part (b):** Use the geometric sum formula to compute

$$2^5 + 2^6 + \cdots + 2^{12}.$$

- **Solution:** We have

$$\begin{aligned}2^5 + 2^6 + \cdots + 2^{12} &= 2^5\left(1 + 2 + \cdots + 2^7\right) \\ &= 32\left(\frac{2^8-1}{2-1}\right) \\ &= 32(256-1) \\ &= 8160.\end{aligned}$$

- **Example:** Prove

$$\sum_{k=0}^{n} r^k = \frac{r^{n+1}-1}{r-1},$$

for all $n \geq 0$.

- **Solution:**

PROOF. For $n \in \mathbb{N}$ let $P(n)$ be the statement

$$1 + r + r^2 \cdots + r^n = \frac{r^{n+1}-1}{r-1}.$$

Base Case: For $n = 0$, we have that the left hand side is

$$\text{LHS} = 1$$

and the right hand side is

$$\text{RHS} = \frac{r^{0+1}-1}{r-1} = \frac{r-1}{r-1} = 1.$$

Thus the formula is true for $n = 0$.

Inductive hypothesis: We assume the formula holds for $n = k$. That is, assume

$$1 + r + r^2 \cdots + r^k = \frac{r^{k+1}-1}{r-1}. \quad (\star)$$

is true.

Inductive step: Using the inductive hypothesis, we want to show that the formula holds for $n = k+1$, that is

$$1 + r + r^2 \cdots + r^{k+1} = \frac{r^{k+2}-1}{r-1}. \quad (\star\star)$$

To prove this, we start with the Left Hand side(LHS),

$$\begin{aligned}
1+r+r^2\cdots+r^{k+1} &= \underbrace{1+r+r^2\cdots+r^k}+r^{k+1} \\
&= \underbrace{\frac{r^{k+1}-1}{r-1}}+r^{k+1}, \text{ by inductive hypothesis } (\star) \\
&= \frac{r^{k+1}-1}{r-1}+\frac{(r-1)\,r^{k+1}}{r-1} \\
&= \frac{r^{k+1}-1+r^{k+2}-r^{k+1}}{r-1} \\
&= \frac{r^{k+2}-1}{r-1}.
\end{aligned}$$

Thus we have shown $(\star\star)$.

Thus by induction, the formula holds for all integers $n \geq 0$. □

- **Example (HW Problem, if time):** Prove

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

for all $n \geq 1$.

  - **Solution:**

PROOF. For $n \in \mathbb{N}$ let $P(n)$ be the statement

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

Base Case: For $n = 1$, we have that the left hand side is

$$\text{LHS} = 1$$

and the right hand side is

$$\text{RHS} = \frac{1\,(1+1)\,(2+1)}{6} = \frac{6}{6} = 1.$$

Thus the formula is true for $n = 1$.

Inductive hypothesis: We assume the formula holds for $n = k$. That is, assume

$$\sum_{i=1}^{k} i^2 = \frac{k\,(k+1)\,(2k+1)}{6}. \quad (\star)$$

is true.

Inductive step: Using the inductive hypothesis, we want to show that the formula holds for $n = k+1$, that is

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{(k+1)\,(k+2)\,(2(k+1)+1)}{6} \\
&= \frac{(k+1)\,(k+2)\,(2k+3)}{6}. \quad (\star\star)
\end{aligned}$$

To prove this, we start with the Left Hand side(LHS),

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \underbrace{1+2^2+3^2\cdots+k^2}+(k+1)^2 \\
&= \underbrace{\frac{k(k+1)(2k+1)}{6}}+(k+1)^2, \text{ by inductive hypothesis } (\star) \\
&= \underbrace{\frac{k(k+1)(2k+1)}{6}}+\frac{6(k+1)^2}{6} \\
&= \frac{k(k+1)(2k+1)+6(k+1)^2}{6} \\
&= \frac{(k+1)[k(2k+1)+6(k+1)]}{6} \\
&= \frac{(k+1)\left[2k^2+k+6k+6\right]}{6} \\
&= \frac{(k+1)\left[2k^2+7k+6\right]}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6}
\end{aligned}$$

Thus we have shown $(\star\star)$.

Thus by induction, the formula holds for all integers $n \geq 1$. □

Section 5.3 - Mathematical Induction: Applications

- Recall
- The **Principle of Mathematical Induction:**
  - Let $P(n)$ be a property that is defined for integers n and let a be a fixed integer. Suppose the following two properties hold:
    (1) $P(a)$ is true
    (2) $\forall k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true.
  - Then $P(n)$ is true for all $n \geq a$.
- Mathematical inductions can be used to prove any statement that has a variable $n \in \mathbb{N}$. It doesn't have to be just formulas, like in the previous section.

Divisibility Examples:

- **Example:** Use induction to prove $6 \mid (7^n - 1)$ for all integers $n \geq 0$.
  - **Divides:** Recall, what does $a \mid b$ mean? it means

$$b = am \text{ for some } m \in \mathbb{Z}.$$

  - **Solution:**

PROOF. For $n \geq 0$ let $P(n)$ be the statement

$$6 \mid (7^n - 1).$$

Base Case: For $n = 0$, we want to show $6 \mid \left(7^0 - 1\right)$, which means $6 \mid 0$. But this is true since

$$0 = 6 \cdot 0 \text{ and } 0 \in \mathbb{Z}.$$

Thus the statement is true for $n = 0$.

Inductive hypothesis: We assume the statement holds for $n = k$. That is, assume

$$6 \mid \left(7^k - 1\right).$$

This means that

$$7^k - 1 = 6m \text{ for some } m \in \mathbb{Z}. \quad (\star)$$

Inductive step: Using the inductive hypothesis, we want to show that the formula holds for $n = k + 1$, that is

$$6 \mid \left(7^{k+1} - 1\right).$$

Meaning, we want to show that

$$7^{k+1} - 1 = 6\,(\text{some integer}). \quad (\star\star).$$

To prove this, we start with the Left Hand side(LHS) of $(\star\star)$.

$$\begin{aligned} 7^{k+1} - 1 &= 7 \cdot \underbrace{7^k} - 1 \\ &= 7 \cdot \underbrace{(6m+1)} - 1, \text{ by inductive hypothesis } (\star) \\ &= 7 \cdot 6m + 7 - 1 \\ &= 7 \cdot 6m + 6 \\ &= 6\,(7m+1). \end{aligned}$$

Thus we have shown $(\star\star)$, with the integer being $7m + 1 \in \mathbb{Z}$ (because $\mathbb{Z}$ is closed under multiplication and addition).

Thus by induction, the statement holds for all integers $n \geq 0$. □

Formulas for Recursion Relations:

- **Example:** Use induction to prove the following: If $a_1, a_2, \ldots$ is a sequence defined by the recursion

$$\begin{cases} a_1 = 35 \\ a_n = 7a_{n-1} \quad \text{for } n \geq 2, \end{cases}$$

then $a_n = 5 \cdot 7^n$, for all integers $n \geq 1$.

  - **Solution:**

PROOF. Let a_n be the sequence defined by the recursion above. For $n \in \mathbb{N}$ let $P(n)$ be the assertion that

$$a_n = 5 \cdot 7^n.$$

Base Case: For $n = 1$, we have that $a_1 = 35$ by definition, and using the fomula

$$5 \cdot 7^1 = 35$$

hence $a_1 = 5 \cdot 7^1$ and so $P(1)$ holds.

Inductive hypothesis: We assume $P(k)$ holds for $n = k$ where $k \geq 1$. That is, assume

$$a_k = 5 \cdot 7^k. \quad (\star)$$

Inductive step: Using the inductive hypothesis, we want to show that the formula holds for $n = k + 1$. Meaning, we want to show that

$$a_{k+1} = 5 \cdot 7^{k+1}. \quad (\star\star).$$

To prove this, we start with the Left Hand side(LHS) of $(\star\star)$: (Recall we can only prove this using **recursion** defined in the problem, and **equation** $(\star)$)

$$\begin{aligned} a_{k+1} &= 7a_k, \text{ by definition of recursion and since } k+1 \geq 2 \\ &= 7 \cdot \underbrace{a_k} \\ &= 7 \cdot \underbrace{5 \cdot 7^k}, \text{ by inductive hypothesis } (\star) \\ &= 7 \cdot 5 \cdot 7^k \\ &= 5 \cdot 7^{k+1}. \end{aligned}$$

Thus we have shown $(\star\star)$..

Thus by induction, the statement holds for all integers $n \geq 1$. □

Section 5.4 - Strong Induction

- We use the principle of Strong Induction, whenever we need to assume multiple things from the past are true.
- This is surprisingly useful in computer science in showing the time complexity in recursion relations.
- The **Principle of Strong Induction:**
  - Let $P(n)$ be a property that is defined for integers n and let $a \leq b$ be integers. Suppose
    (1) $P(a), P(a+1), \ldots, P(b)$ are true
    (2) $\forall k \geq b$, if $P(a), P(a+1), \ldots, P(k)$ are true, then $P(k+1)$ is true.
  - Then $P(n)$ is true for all $n \geq a$.
- **Example:** Use strong induction to prove the following: If $b_1, b_2, \ldots$ is sequence defined by the recursion relation:

$$\begin{cases} b_1 = 4 \\ b_2 = 12 \\ b_n = b_{n-1} + b_{n-2} \quad \text{for } n \geq 2. \end{cases}$$

Prove: The sequence b_n is divisible by 4, for all integers $n \geq 1$.
  - **Solution:**

PROOF. Let b_n be the sequence defined by the recursion relation above. For $n \in \mathbb{N}$ let $P(n)$ be the assertion that

"b_n is divisible by 4".

Base Case: (we now have 2 base cases) We need to show $P(1)$ and $P(2)$ are true. Since $b_1 = 4$ and $b_2 = 12 = 3 \cdot 4$ is it clear that both are integers are divisible by 4.

Inductive hypothesis: We assume for $k \geq 2$, $P(1), P(2), \ldots, P(k)$ all hold. That is, assume

"b_1 is divisible by 4"
"b_2 is divisible by 4"
$\vdots$
"b_{k-1} is divisible by 4"
"b_k is divisible by 4" $(\star)$

Inductive step: Using the inductive hypothesis, we want to show that the statement holds for $n = k+1$. Meaning, we want to show that

"b_{k+1} is divisible by 4". $(\star\star)$

To prove this, we start with the Left Hand side(LHS) of $(\star\star)$: (Recall we can only prove this using **recursion** defined in the problem, and **statements in** $(\star)$)

Now

$$\begin{aligned} b_{k+1} &= b_k + b_{k-1}, \text{ by definition of recursion} \\ &= \underbrace{b_k} + \underbrace{b_{k-1}} \\ &= \underbrace{4r} + \underbrace{4s}, \text{ for some } r, s \text{ by inductive hypothesis } (\star) \\ &= 4(r+s) \end{aligned}$$

This shows that b_{k+1} is divisible by 4. Thus we have shown $(\star\star)$.

Thus by strong induction, the statement holds for all integers $n \geq 1$. □

- **Example:** Use strong induction to prove the following: If $c_1, c_2, \ldots$ is sequence defined by the recursion relation:

$$\begin{cases} c_1 = \frac{1}{2} \\ c_2 = \frac{1}{3} \\ c_n = c_{n-1} \cdot c_{n-2} \quad \text{for } n \geq 3. \end{cases}$$

Prove: The sequence c_n satisfies $0 < c_n \leq 1$ for all integers $n \geq 1$.
  - **Solution:**

PROOF. Let c_n be the sequence defined by the recursion relation above. For $n \in \mathbb{N}$ let $P(n)$ be the assertion that

$$\text{“}0 < c_n \leq 1\text{”}.$$

Base Case: (we now have 2 base cases) We need to show $P(1)$ and $P(2)$ are true. Since $c_1 = \frac{1}{2}$ and $c_2 = \frac{1}{3}$ is it clear that both are integers are strictly bigger than 0 and smaller than 1.

Inductive hypothesis: We assume for $k \geq 1$, $P(1), P(2), \ldots, P(k)$ all hold. That is, assume

$$\begin{aligned}
&\text{“}0 < c_1 \leq 1\text{”}\\
&\text{“}0 < c_2 \leq 1\text{”}\\
&\vdots\\
&\text{“}0 < c_{k-1} \leq 1\text{”}\\
&\text{“}0 < c_k \leq 1\text{”} \quad (\star)
\end{aligned}$$

Inductive step: Using the inductive hypothesis, we want to show that the statement holds for $n = k+1$. Meaning, we want to show that

$$\text{“}0 < c_{k+1} \leq 1\text{”}. \quad (\star\star)$$

To prove this, we can only do this using **recursion** defined in the problem, and **statements in** $(\star)$)

Now

$$\begin{aligned}
c_{k+1} &= c_k \cdot c_{k-1}, \text{ by definition of recursion}\\
&= \underbrace{c_k} \cdot \underbrace{c_{k-1}}\\
&\leq 1 \cdot 1, \text{ by inductive hypothesis } (\star)\\
&= 1
\end{aligned}$$

similarly,

$$\begin{aligned}
c_{k+1} &= c_k \cdot c_{k-1}, \text{ by definition of recursion}\\
&= \underbrace{c_k} \cdot \underbrace{c_{k-1}}\\
&\geq 0 \cdot 0, \text{ by inductive hypothesis } (\star)\\
&= 0.
\end{aligned}$$

This shows that $0 \leq c_{k+1} \leq 1$. Thus we have shown $(\star\star)$.

Thus bystrong induction, the statement holds for all integers $n \geq 1$. □

- **Example: Prove:** For all integers $n \geq 2$, n is divisible by a prime.
  - **Solution:**

PROOF. For $n \geq 2$, let $P(n)$ be the assertion that

$$\text{“ there exists prime } p \text{ such that } p \mid n\text{”}.$$

Base Case: We need to show $P(2)$ is true. Since $n = 2$ is obviouly divisible by the prime $p = 2$, then $P(2)$ is true.

Inductive hypothesis: We assume for $k \geq 2$, $P(2), P(2), \ldots, P(k)$ all hold. That is, assume

$$\begin{aligned}
&\text{“ there exists prime } p \text{ such that } p \mid 1\text{”}\\
&\text{“ there exists prime } p \text{ such that } p \mid 2\\
&\vdots\\
&\text{“ there exists prime } p \text{ such that } p \mid (k-1)\\
&\text{“ there exists prime } p \text{ such that } p \mid k \quad (\star)
\end{aligned}$$

Inductive step: Using the inductive hypothesis, we want to show that the statement holds for $n = k+1$. Meaning, we want to show that

$$\text{“ there exists prime } p \text{ such that } p \mid (k+1). \quad (\star\star)$$

To prove this, we split into 2 cases.

Case 1: Suppose $k+1$ is prime.

Then choose $p = k+1$ then clearly $p \mid k+1$.

Case 2: Suppose $k+1$ is not prime.

Then this means $k+1$ is composite and hence

$$k+1 = rs$$

here $2 \leq r < k+1$ and $2 \leq s < k+1$. Since we know $P(r)$ is true, then k is divisible by a prime. This means $p \mid r$ and $r \mid k+1$, hence by the transitivity of divides, we have that

$$p \mid k+1$$

as desired.

Thus by principle of strong induction, the statement is true for all $n \geq 2$. □

CHAPTER 6

Set Theory

Section 6.1 - Set Theory: Definitions and the Element Method of Proof

- We start with a definition

DEFINITION 41. (takes over Definition 12) Let A and B be sets. Then A is a subset of B, denoted $A \subseteq B$, provided that

$$\forall x \, (x \in A \to x \in B)$$

- This means: "For all $x \in A$ then $x \in B$"
- It is easier to visualize using Venn Diagrams.
- Other terminology:
  - Other terminology for $A \subseteq B$ are,
    - $A \subset B$
    - A is contained in B
    - B contains A
    - B is a **superset** of A
- **Remark:**
  - To show $A \not\subseteq B$: Show that there exists $x \in A$ but $x \notin B$.
- **Examples:**
  - $\{1, 2\} \subset \{1, 2, 3\}$
  - $\{1, 2, 4\} \not\subseteq \{1, 2, 3\}$
  - $\{0, 1, 2\} \not\subseteq \mathbb{Z}^+$
  - $\{1, 2\} \subset \mathbb{Z}^+$
  - $\{1, 2\} \notin \mathbb{Z}^+$but $1, 2 \in \mathbb{Z}^+$
- **How to prove $A \subset B$:**
  - **Proof:** "Let $x \in A$ be arbitrary element. Then .....(do work to show) $x \in B$, as desired. "
- **Example:** Describe the following sets

$$A = \{m \in \mathbb{Z} \mid m = 8r - 7 \text{ for some } r \in \mathbb{Z}\}$$
$$B = \{n \in \mathbb{Z} \mid n = 4s + 1 \text{ for some } s \in \mathbb{Z}\}$$

  and show $A \subset B$.
  - **Solution:**
  - Note that

$$A = \{\ldots, -15, -7, 1, 9, 17, \ldots\}$$
$$B = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$

PROOF. Let $x \in A$ be arbitrary. We want to show $x \in B$.
If $x \in A$ then

$$x = 8r - 7 \text{ for some } r \in \mathbb{Z}.$$

We want to show $x \in B$, meaning that

$$x = 4\,(\text{some integer}) + 1.$$

By algebra,

$$\begin{aligned} x &= 8r - 7 \\ &= 8r - 8 + 1 \\ &= 4(2r - 2) + 1. \end{aligned}$$

Let $s = 2r - 2$. Since $\mathbb{Z}$ is closed under multiplication and subtration then $s \in \mathbb{Z}$, hence we showed that

$$x = 4s + 1 \text{ for some } s \in \mathbb{Z}$$

thus $x \in B$. □

- Here are some more definitions

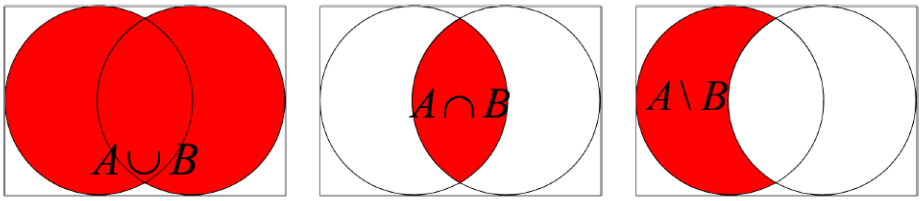
DEFINITION 42. (Set Equality) If A and B are sets, then $A = B$ provided that both $A \subseteq B$ and $B \subseteq A$.

DEFINITION 43. A is a **proper subset** of B provided that $A \subseteq B$ and $A \neq B$.

Operations on Sets.

DEFINITION 44. Let A and B be sets. Then
(1) The **union** of A and B is the set $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
(2) The **intersection** of A and B is the set $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
(3) A **minus** B is the set $A - B = \{x \mid x \in A \text{ and } x \notin B\}$. This is also (more commonly) written $A \backslash B$ and is also called the **set difference**, A minus B.

- Also helpful to picture a **Venn Diagram:**



-
- **Example:** Let

$$\begin{aligned} A &= \{1, 2, 3, 4\} \\ B &= \{2, 3, 8\}. \end{aligned}$$

Then

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 8\} \\ A \cap B &= \{2, 3\} \\ A - B &= \{1, 4\} \\ B - A &= \{8\} \end{aligned}$$

- We can generalize to man unions and intersectons.

DEFINITION 45. Given sets $A_1, A_2, A_3, \ldots$ and a nonegative integer n, define:
(1) $\bigcup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n = \{x \mid x \in A_i \text{ for at least one } i = 1, 2, \ldots, n\}$
(1) $\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ for at least one } i \geq 1\}$
(3) $\bigcap_{i=1}^{n} A_i = A_1 \cap \cdots \cap A_n = \{x \mid x \in A_i \text{ for all } i = 1, 2, \ldots, n\}$
(3) $\bigcap_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ for all } i \geq 1\}$

- **Notation:** The sets $A_1, A_2, \ldots$ are said to be **mutually disjoint** if A_i and A_j are **disjoint** (i.e. $A_i \cap A_j = \emptyset$) for any pair $i \neq j$

- **Example:** Let
$$A_i = \left\{ x \in \mathbb{R} \mid 0 \leq x \leq \frac{1}{i} \right\} = \left[0, \frac{1}{i}\right].$$
  - Then we compute the following:
$$\bigcup_{i=1}^{3} A_i = [0,1] \cup \left[0, \frac{1}{2}\right] \cup \left[0, \frac{1}{3}\right] = [0,1]$$
    and
$$\bigcup_{i=1}^{\infty} A_i = [0,1].$$
    Also
$$\bigcap_{i=1}^{3} A_i = [0,1] \cap \left[0, \frac{1}{2}\right] \cap \left[0, \frac{1}{3}\right] = \left[0, \frac{1}{3}\right]$$
    and finally
$$\bigcap_{i=1}^{\infty} A_i = \{0\}.$$
- The Empty Set:

DEFINITION 46. The **empty set**, denotes $\emptyset$, is the set with no elements.
$$\emptyset = \{\}.$$

- **Question:** Consider any set A, then is $\emptyset \subset A$?
  - **Solution:** Yes, the empty set is a subset of every set!

Power Set.

DEFINITION 47. Let A be a set. The power set of a set A, denotes $\mathcal{P}(A)$, is the set of all subsets of A. That is,
$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

- **Remarks:**
  - The elements of $\mathcal{P}(A)$ are sets! Don't get confused/
  - $B \in \mathcal{P}(A) \iff B \subset A$
  - $\mathcal{P}(A)$ always contains the sets $\emptyset$ and A.
  - When A is finite, then the number of elements in $\mathcal{P}(A)$ is $2^{\#(A)}$.
- **Examples:** What is
  - **Part (a):** The power set of a two-element set?
    - **Solution:**
$$\mathcal{P}(\{x,y\}) = \{\emptyset, \{x\}, \{y\}, \{x,y\}\}.$$
  - **Part (b):** The power set of a one-element set?
    - **Solution:**
$$\mathcal{P}(\{x\}) = \{\emptyset, \{x\}\}.$$
  - **Part (c):** The power set of the emptyset?
    - **Solution:**
$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$
    - Note that $\mathcal{P}(\emptyset) \neq \emptyset$. It contains one element. (Remember - thinking of a set as a fishbowl, we think of the empty set as an empty fishbowl. Then the set containing the empty set is a fishbowl containing an empty fishbowl!)
- **HW Problem:** Find $\mathcal{P}(\{x,y,z\})$. How many elements does it have?
- **Example:** Let $A = \{1,2,3\}$
  - Is $1 \in \mathcal{P}(A)$?
    - No
  - Is $\{2\} \in \mathcal{P}(A)$?
    - Yes

- Is $\{\emptyset\} \in \mathcal{P}(A)$?
  - No
- Is $\{\emptyset\} \subset \mathcal{P}(A)$?
  - Yes
- Is $\emptyset \in \mathcal{P}(A)$?
  - Yes
- Is $\emptyset \subset \mathcal{P}(A)$?
  - Yes

Section 6.2 - Set Proofs; properties of sets

- See Theorems 6.2.1 and Theorems 6.2.2 for some set properties.
- We will learn how to prove several properties of sets.

Proving $X \subseteq Y$.

- We will learn how to prove how one set is a subset of another.
- **Procedure:** To prove $X \subseteq Y$
  - **Proof:**
  - (1) Assume $x \in X$ is an abitrary element.
  - (2) Show, after doing some **work**, that $x \in Y$. □
- Some advice: The **work** part, involves using the definitions and basic logic.
  - You need to **unravel** the definitions.
  - Think of "unraveling definitions" like opening a box. At step, write down what you know each part means.
  - For example, If you write "$x \in A \cap B$". Then you need to remember how $\cap$ is defined , this means "$x \in A$ **and** $x \in B$"
- Here are some examples.
- **Example 1:** Prove $A \subseteq A \cup B$
  - **Solution:**

PROOF. Assume $a \in A$ is arbitrary. Then $a \in A$ or $a \in B$, because the former is true. Thus, $a \in A \cup B$, as desired. □

- **Example 2:** Prove $A \times (B - C) \subseteq A \times B$
  - **Solution:**

PROOF. Assume $(x, y) \in A \times (B - C)$ is an arbitrary element. Then this means that $x \in A$ and $y \in B - C$. Thus, $y \in B$ but $y \notin C$.

Since we know $x \in A$ and $y \in B$, then this means that $(x, y) \in A \times B$, as desired. □

Proving a set is empty.

- The typical proof to show a set is empty involves contradiction.
- **Procedure:** To prove $X = \emptyset$
  - **Proof:**
  - (1) Assume for contradiction that $X \neq \emptyset$. Then this means we can find an $x \in X$
  - (2) Show, after doing some **work**, that you can a contradiction (something absurd).
  - Hence, X should have been empty in the first place. Thus $X = \emptyset$. □
- **Example 3:** Prove $A \cap (B - A) = \emptyset$
  - **Solution:**

PROOF. Assume for the sake of contradiction that $A \cap (B - A) \neq \emptyset$. Then this means that there exists an $x \in A \cap (B - A)$. Then this means that $x \in A$ and $x \in B - A$. Since $x \in B - A$, then this means that $x \in B$ but $x \notin A$.

In particular, we just showed that $x \in A$ and $x \notin A$, which is absurd (a contradiction). Hence, the original statement must have been true, meaning we showed that $A \cap (B - A) = \emptyset$, as desired. □

Proving two sets are equal.

- **Procedure (Proof by Mutual inclusion):** To prove $X = Y$
  - **Proof:**
  - To show two sets are equal, we show each is a subset of the other.
  - Part (a) First we show $X \subseteq Y$.....
  - Part (b): Now we show $Y \subseteq X$.....
  - Combining the two sections of our proof, by Mutual Inclusion we conclude $X = Y$. □
- **Example 4:** Prove the *distributive* law: For all sets A, B and C,

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

– **Solution:**

PROOF. To show two sets are equal, we show each is a subset of each other.

Part(a): We show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$:

Let $x \in A \cup (B \cap C)$ be an arbitrary element. Then this means $x \in A$ **or** $x \in B \cap C$. We split this into two cases.

[We WTS: $x \in (A \cup B) \cap (A \cup C)$].

Case 1 : If $x \in A$. Then in this case we know that since $x \in A$ then $x \in A \cup B$ (by Example 1), and also similarly $x \in A \cup C$ (also by Example 1). Since $x \in A \cup B$ **and** $x \in A \cup C$, then we have that

$$x \in (A \cup B) \cap (A \cup C)\,,$$

which is what we wanted to show.

Case 2 : If $x \in B \cap C$. Then in this case we know that since $x \in B$ **and** $x \in C$.

Since $x \in B$ then $x \in (A \cup B)$ (by Example 1). Similarly, since $x \in C$ then $x \in (A \cup C)$. Since $x \in A \cup B$ **and** $x \in A \cup C$, then we have that

$$x \in (A \cup B) \cap (A \cup C)\,,$$

which is what we wanted to show.

As Cases 1 and 2 exaust all possibilities of Part (a), then we showed that in each case that

$$x \in (A \cup B) \cap (A \cup C)\,.$$

Thus we showed that if $x \in A \cup (B \cap C)$ then $x \in (A \cup B) \cap (A \cup C)$, which means

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)\,.$$

Part(b): We show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$:

Let $x \in (A \cup B) \cap (A \cup C)$ be an arbitrary element. Then this means $x \in A \cup B$ **and** $x \in A \cup C$.

[We WTS: $x \in A \cup (B \cap C)$].

We split this into two cases. Because, at the end of the day, either $x \in A$ or $x \notin A$.

Case 1 : Suppose $x \in A$. Then in this case, it means $x \in A$ or $x \in (B \cap C)$ since the former is true. Hence

$$x \in A \cup (B \cap C)\,,$$

as desired.

Case 2 : Suppose $x \notin A$. Then recall from above, since $x \in A \cup B$ **and** $x \in A \cup C$, but $x \notin A$, then it must be that

$$x \in B \text{ and } x \in C.$$

Hence $x \in (B \cap C)$. This means that $x \in A$ **or** $x \in (B \cap C)$, since the latter is true. This means

$$x \in A \cup (B \cap C)\,,$$

as desired.

As Cases 1 and 2 exaust all possibilities of Part (b), then we showed that in each case that

$$x \in A \cup (B \cap C)\,.$$

Thus we showed that if $x \in (A \cup B) \cap (A \cup C)$ then $x \in (A \cup B) \cap (A \cup C)$, which means

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)\,.$$

Combining the two parts of our proof, by Mutual Inclusion we conclude that

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

as desired. □

CHAPTER 7

Functions

Section 7.1 - Functions defined on general sets

- Recall from Definition 14, paraphrased,
  - "A function f from X to Y is a relation from domain X to co-domain Y such that every $x \in X$ is related to a unique $y \in Y$. "
- Here it is formally:

DEFINITION. A **function** F from A to B is a relation from A to B satisfying
(1) For all $x \in A$, there exists $y \in B$ such that $(x, y) \in F$.
(2) For all $x \in A$ and $y, z \in B$, if $(x, y) \in F$ and $(x, z) \in F$, then $y = z$.

- Note that, before our notion of a function, is actualy of its **graph** F.
- **Notation and Terminology:**
  - We write $f : X \to Y$ to say "f is a **function** from X to Y"
  - The unique output for input x is denoted by $f(x)$, and called the **value** of f at x, or the **image** of x under f.
  - The **range** or **image** of f is the set

$$\text{range of } f = \text{image of } f = \{y \in Y \mid y = f(x), \text{ for some } x \in X\}.$$

  - If $f(x) = y$, then x is called a **preimage** of y or an **inverse image** of y.
  - The set of all **preimages** of y is called the inverse image of y, written $f^{-1}(y)$, that is,

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}.$$

    * I.e. $f^{-1}(y)$ is a set, since there may be more than one preimages.
    * **Example:** If $f(x) = x^2$, then

$$f^{-1}(4) = \{-2, 2\}.$$

Arrow Diagrams.

- **Example:** Consider the following function $f : X \to Y$ where

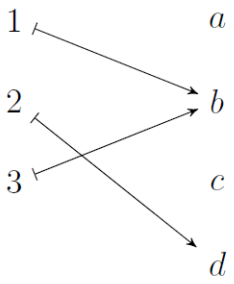
$$X = \{1, 2, 3\}$$
$$Y = \{a, b, c, d\}.$$

  defined by

$$f(1) = b$$
$$f(2) = d$$
$$f(3) = b.$$

  - **Part (a):** Draw an arrow diagram:
    * **Solution:**

$$\underline{\text{Domain}} \xrightarrow{f} \underline{\text{Codomain}}$$



  - *
  - **Part (b):** What is the domain of f
    - * **Solution:**
    - * Domain is the set $\{1, 2, 3\}$
  - **Part (c):** What is the co-domain of f
    - * **Solution:**
    - * Co-domain is the set $\{a, b, d, c\}$
  - **Part (d):** What is the range/image of f
    - * **Solution:**
    - * The range/image is the set $\{b, d\}$
  - **Part (e):** What is the inverse image of a, b, c, d:
    - * **Solution:**

$$\begin{aligned} f^{-1}(a) &= \emptyset \\ f^{-1}(b) &= \{1, 3\} \\ f^{-1}(d) &= \emptyset \\ f^{-1}(d) &= \{2\}. \end{aligned}$$

Functions defined by formulas.

- **Examples:**
  - **Part (a):** Consider $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.
    - * The **range/image** of f is $[0, \infty)$
  - **Part (b):** Consider $g : \mathbb{Z} \backslash \{0\} \to \mathbb{N}$ defined by $g(x) = x^2$.
    - * The **range/image** of g is $\{1, 2^2, 3^2, 4^2, \dots\} = \{1, 4, 9, 16, \dots\}$
  - **Part (c):** Consider $h : \mathbb{Z} \to \mathbb{R}$ defined by $h(x) = \sqrt[3]{x}$.
  - **Part (d):** Consider any sequence $a_1, a_2, a_3 \dots$ of real numbers. Then we can define a function

$$\begin{aligned} &a : \mathbb{N} \to \mathbb{R} \\ &\text{defined by } a(k) = a_k \end{aligned}$$

  - **Part (e):** Consider $f : \mathcal{P}(\{1, 2, 3, 4\}) \to \mathbb{Z}$ defined by

$$\begin{aligned} f(S) &= \#(S) \\ &= \text{the number of elements in set } S. \end{aligned}$$

    - * For example,

$$\begin{aligned} f(\{1, 2, 4\}) &= 3, \\ f(\{4\}) &= 3, \\ f(\emptyset) &= 0, \end{aligned}$$

    - * The **image/range** of f is $\{0, 1, 2, 3, 4\}$.

DEFINITION 48. (Equality of Functions) Suppose f and g are functions from X to Y. Then f **equals** g, written $f = g$, provided that $f(x) = g(x)$, for all $x \in X$.

DEFINITION 49. Given a set X, the **identity function** X is the function $I_X : X \to X$ defined by $I_X(x) = x$.

- **Example:** Find $I_{\mathbb{R}}(5)$ and $I_{\mathbb{R}}\left(\sqrt{5}\right)$.
  - **Solution:** We have $I_{\mathbb{R}}(5) = 5$ and $I_{\mathbb{R}}\left(\sqrt{5}\right) = \sqrt{5}$.

Boolean Functions.

- Define

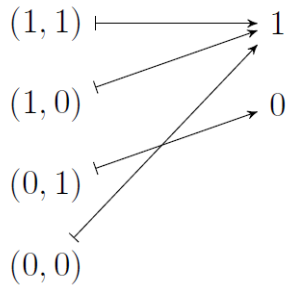
$$\{0,1\}^n := \underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{n \text{ times}}$$

DEFINITION 50. An ($n-$place) **Boolean function** is a function $f : \{0,1\}^n \to \{0,1\}$.

- Such a function is often presented in an input/output table with n columns (for the inputs) and one column for the output. Across the rows, we put the entries of the ordered n-tuples with the value of the function on this entry in the last column.
- **Example:**
  - Here is an input/output table for a 2-place boolean function $f : \{0,1\}^2 \to \{0,1\}$:

	P	Q	R
	1	1	1
*	1	0	1
	0	1	0
	0	0	1

  - The corresponding arrow diagram:



  -
- **Remainders:**
  - Before doing the next example, we recall Quotient-Remainder Theorem and the notation $n \mod d =$ remainder when divising by d.
  - In particular,

$$\begin{aligned} 5 &\mod 2 = 1 \\ 8 &\mod 2 = 0 \\ 9 &\mod 2 = 1 \\ 0 &\mod 2 = 0 \end{aligned}$$

- **Example:**
  - Consider the 3-place boolean function

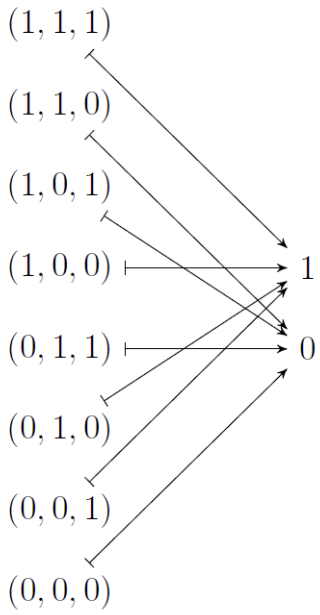
$$f : \{0,1\}^3 \to \{0,1\}$$

$$\text{defined by } f(x_1, x_2, x_3) := (x_1 + x_2 + x_3) \mod 2$$

    * The input/output table for f is

	x_1	x_2	x_3	$f(x_1, x_2, x_3)$
	1	1	1	$(1+1+1) \mod 2 = 3 \mod 2 = 1$
	1	1	0	0
	1	0	1	0
*	1	0	0	1
	0	1	1	0
	0	1	0	1
	0	0	1	1
	0	0	0	0

- The corresponding arrow diagram:



-

A function that is not well defined.

- A function is **not well-defined** if it fails to satify at least one condition of being a function.
- **Example:** Why is the following "function" is not well-defined

$$f : \mathbb{Q} \to \mathbb{Z}$$
$$f\left(\frac{m}{n}\right) = m \text{ for all } , m, n \in \mathbb{Z}, n \neq 0.$$

  - **Solution:**
  - At first glance, it seems like a perfectly fine function.
  - But this is not well-defined. Because rational numbers can be written in different forms, for example suppose $x = \frac{1}{2}$ then

$$f(x) = f\left(\frac{1}{2}\right) = 1$$

    but you can also write $x = \frac{1}{2} = \frac{500}{1000}$ so that using this formula we have

$$f(x) = f\left(\frac{500}{1000}\right) = 1000$$

    but this is BAD, because functions can only assign a unique value to each x.
  - So f is not a well-defined function.

Section 7.2 - One-to-one and Onto Functions.

One-to-one Functions.

- We start with a definition

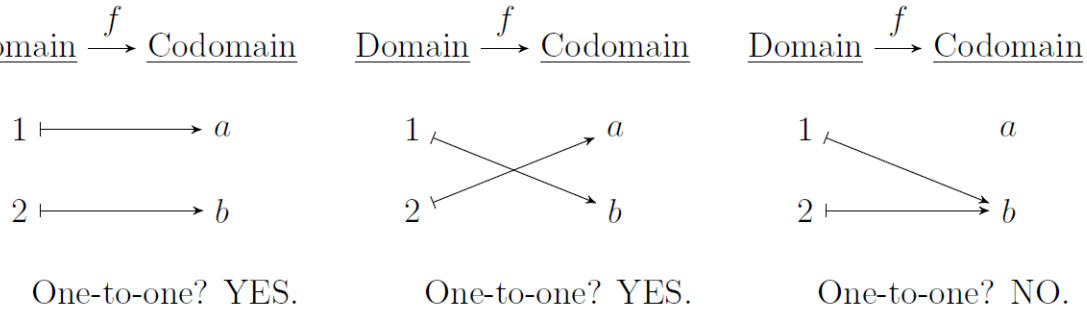
DEFINITION 51. Let$f : X \to Y$ be a function. Then f is **one-to-one** provided that

$$\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2$$

or equivalently,

$$\forall x_1, x_2 \in X, \text{ if } x_1 \neq x_2 \text{ then } f(x_1) \neq f(x_2).$$

- **Example:** Figure out if the following functions $f : \{1, 2\} \to \{a, b\}$ are one-to-one.



-
- .
- **To prove $f : X \to Y$ is one-to-one:**
  - **Proof Method:**
  - Let $x_1, x_2 \in X$ and suppose $f(x_1) = f(x_2)$. Then....after some work.... show $x_1 = x_2$. □
- **To prove $f : X \to Y$ is NOT one-to-one:**
  - **Proof Method:**
  - Produce somehow two distinct inputs, $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$.
- **Tips to determine if a given function is one-to-one:**
  - Start by studying $f(x_1) = f(x_2)$. Play with this equation, and see if this **forces** $x_1 = x_2$. If so, then f is one-to-one.
  - If in playing, you discover that it is possible that x_1 does NOT necessarily need to equal x_2, then you should be able to
    - produce two different actual values x_1 and x_2
    - then show that $f(x_1) = f(x_2)$.
- **Question:** What test do we have for "graphable" functions to help us see if f is one-to-one?
  - **Answer:** The Horizotal Line test! If a function passes the horizontal line test, then f is one-to-one.
- **Example:** Prove or Disprove: f is one-to-one
  - **Part (a):** $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$.
    - **Solution:**
    - Using the horizonal line test, it is clear this funciton is one-to-one. Here is a proof.

    PROOF. To show f is one-to-one, let $x_1, x_2 \in \mathbb{R}$ and assume $f(x_1) = f(x_2)$. Then this means

    $$\begin{aligned} 2x_1 + 1 = 2x_2 + 1 &\iff 2x_1 = 2x_2 \\ &\iff x_1 = x_2, \end{aligned}$$

    which is what we needed to show. □
  - **Part (b):** $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 5$.
    - **Solution:**
    - Using the horizonal line test, it is clear this funciton is NOT one-to-one. For any horizontal line, it passes through 2 points!

* For example, $x_1 = 2$ and $x_2 = -2$ are different but yet maps to the same point.
* Here is a proof.

PROOF. To show f is not one-to-one, we must produce $x_1, x_2 \in \mathbb{R}$ such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$. Taking

$$x_1 = 2$$
$$x_2 = -2$$

we see that

$$f(2) = 9 \text{ and } f(-2) = 9$$

hence $f(x_1) = f(x_2)$, which is what we needed to show. □

– **Part (c):** Let $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 5$. We already know from the previous example that f is NOT one-to-one. So here is wrong proof that f is one-to-one. Find the mistake!

PROOF. To show f is one-to-one, let $x_1, x_2 \in \mathbb{R}$ and assume $f(x_1) = f(x_2)$. Then this means

$$\begin{aligned} x_1^2 + 5 = x_2^2 + 5 &\iff x_1^2 = x_2^2 \\ &\iff x_1 = x_2, \end{aligned}$$

which is what we needed to show.

* **Solution**
* The mistake is this WRONG proof is that

$$x_1^2 = x_2^2 \text{ does not imply that } x_1 = x_2.$$

* When you take square root of both sides you get:

$$x_1^2 = x_2^2 \text{ implies } |x_1| = |x_2|.$$

* But if $|x_1| = |x_2|$, this DOES NOT mean $x_1 = x_2$.

□

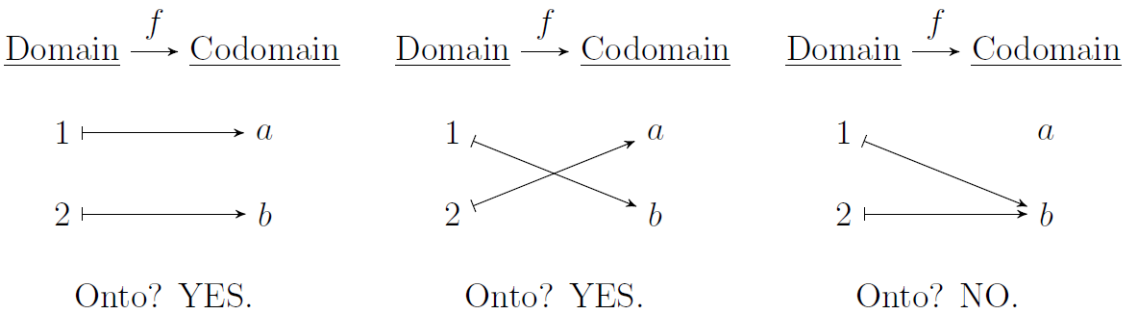
Onto Functions.

- **Intuition:** Every element of Y gets "hit" by f, i.e., the range is all of Y .

DEFINITION 52. Let $f : X \to Y$. Then f is **onto** provided that

$$\forall y \in Y, \exists x \in X \text{ such that } y = f(x).$$

- **Examples:** Onto or not? $f : \{1, 2\} \to \{a, b\}$



–

- .
- **To prove $f : X \to Y$ is onto:**
  - **Proof Method:**
  - Let $y \in Y$ be arbitrary.

  - Produce *somehow*....after some work.. a candidate $x \in X$(usually dependent on y) and verify that $f(x) = y$. □
- **To prove $f : X \to Y$ is NOT onto:**
  - **Proof Method:**
  - Produce *somehow* a particular element $y \in Y$ and
  - show, for this y, that for all $x \in X$, $f(x) \neq y$. There are two ways you can do this:
    - (Directly) With y in hand,
      - Let $x \in X$ be arbitrary, and then
      - verify that $f(x) \neq y$.
    - (indirectly - by contradiction) With y in hand,
      - Assume, for the sake of contradiction, that there is an element $x \in X$ such that $f(x) = y$.
      - The proceed logically and derive a contradiction.
- **Tips to determine if a given function is onto:**
  - Start by studying $f(x) = y$. Play with this equation, and see if this places any restrictions on y. If so, then f is likely not onto.
  - Also, try to solve for x to find a preimage of y.
    - If there are some y's for which this is impossible (and by this, I mean not mathematically possible, not "*it's really hard and I can't do it*"), then f is not onto.
- **Question:** What test do we have for "graphable" functions to help us see if f is onto?
  - **Answer:** Bear Hug! If a function $f : X \to Y$ bear hugs all elements of Y, then it is onto.
- **Example:** Prove of Disprove: f is onto.
  - **Part (a):** $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$.
  - **Solution:**
  - By graphing, this function, you'll notice that this function bearhugs all of the y-axis. Hence it is onto.
  - Sketch work: Looking for at the equation $f(x) = y$ we have

$$y = 2x + 1$$

    can we solve for x? Yes, $x = \frac{y-1}{2}$.
  - Formal Proof:

PROOF. To show that f is onto, let $y \in \mathbb{R}$. We must produce $x \in \mathbb{R}$ such that $f(x) = y$. Take $x = \frac{y-1}{2}$.Then $x \in \mathbb{R}$, the domain, further

$$\begin{aligned} f(x) &= f\left(\frac{y-1}{2}\right) \\ &= 2\left(\frac{y-1}{2}\right) + 1 \\ &= y - 1 + 1 \\ &= y, \end{aligned}$$

thus, f is onto. □

  - **Part (b):** $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 5$.
  - **Solution:**
  - Sketch work: By graphing, this function, you'll notice that this function DOES NOT bearhug all of the y-axis. In fact, it completely misses everything below $y = 5$.
  - For example, pick $y = 0$. Can you find $f(x) = 0$, in other words, can find x such that

$$x^2 + 5 = 0 \iff x^2 = -5$$

    no because a negative number can't be positive. (well this is like a proof by contradiction)
  - Formal Proof:

PROOF. To show that f is not onto, we must produce $y \in \mathbb{R}$ such that $f(x) \neq y$ for any $x \in \mathbb{R}$.

Take $y = 0$, then $y \in \mathbb{R}$, and assume for contradiction that $f(x) = y$, for some $x \in \mathbb{R}$. Then

$$x^2 + 5 = 0 \iff x^2 = -5,$$

which is a contradiction, since a real number square cann never be negative. Hence f is not onto. □

DEFINITION 53. Let $f : X \to Y$. Then f is a **bijection** or a **one-to-one correspondence** provided that f is both one-to-one and onto.

- **Example:** Show that $f : \mathbb{Z} \to \mathbb{Z}$ defined by
$$f(n) = 5n - 10$$
is a one-to-one but not onto. Therefore, not a bijection..
  - **Solution:**
  - Sketch of Proof:
  - First do a sketch. One-to-one is easier to prove.
$$\begin{aligned} f(n_1) = f(n_2) &\iff 5n_1 - 10 = 5n_2 - 10 \\ &\iff 5n_1 = 5n_2 \\ &\iff n_1 = n_2, \end{aligned}$$
  - For onto we study the equation
$$\begin{aligned} y = f(n) &\iff y = 5n - 10 \\ &\iff n = \frac{y+10}{5} \end{aligned}$$
but notice, that this is bad, because there is no way that
$$\frac{y+10}{5}$$
is always an integer. For example, pick $y = 1$.

PROOF. First we show f is one to one: This means we need to show that if $f(n_1) = f(n_2)$ then $n_1 = n_2$. Suppose $f(n_1) = f(n_2)$, then

$$\begin{aligned} f(n_1) = f(n_2) &\iff 5n_1 - 10 = 5n_2 - 10 \\ &\iff 5n_1 = 5n_2 \\ &\iff n_1 = n_2, \end{aligned}$$

as needed. Hence f is one-to-one.

Now we show that f is not onto. We must produce $y \in \mathbb{R}$ such that $f(n) \neq y$ for any $n \in \mathbb{Z}$.

Take $y = 1$, then $y \in \mathbb{Z}$, and assume for contradiction that $f(n) = 1$, for some $n \in \mathbb{Z}$. Then if this is true, then

$$\begin{aligned} 1 = 5n - 10 &\iff 11 = 5n \\ &\iff n = \frac{11}{5}. \end{aligned}$$

which is a contradiction, since $n = \frac{11}{5} \notin \mathbb{Z}$. Hence f is not onto. □

CHAPTER 8

Properties of Relations

Section 8.1 - Relations on Sets

- Recall, that a **relation** R is simply a subset

$$R \subseteq A \times B$$

and is called a **(binary) relation** R from A to B.

DEFINITION 54. Let R be a relation from A to B. The **inverse relation** R^{-1} from B to A is defined by

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}.$$

- **Remark:**
  - Remember that not all relations are functions.
  - Don't get the inverse relation with an inverse fuction. An inverse relation need not be a function!
- **Example:** Let R be the "divides" relation from $A = \{2, 3, 4\}$ to $B = \{2, 6, 7, 8\}$, that is,

$$(x, y) \in R \text{ if and only if } x \mid y.$$

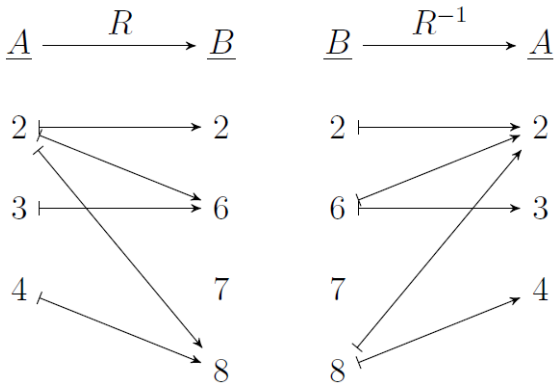
  - **Part (a):** Express R and R^{-1} as sets of ordered pairs.
    - **Solution:**
    - We need to check each possibility and we get

$$R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$$

      then by simply by inverting the order of the order pairs we get

$$R^{-1} = \{(2, 2), (6, 2), (8, 2), (6, 3), (8, 4)\}$$

  - **Part (b):** Draw the arrow diagrams for R and R^{-1}.
    - **Solution:**
    - Draw R first. To draw R^{-1}, we could just reverse the arrowheads. or we could rewrite as below



    -
  - **Part (c):** Are R and R^{-1} functions?
    - **Solution:**
    - R is not a function since 2 is related to more than one element: $(2, 2), (2, 6) \in R$.
    - R^{-1} is not a function since 7 is not sent anywhere.

        - This wouldn't have happened if R was onto. (even though R isn't even a function)
    - Other reasons, for R^{-1} not being a function? 6 is related to more than one element: $(6,2),(6,3) \in R^{-1}$
        - This wouldn't have happened if R was one-to-one. (even though R isn't even a function)
- **Remark:** If R happens to be a one-to-one function and onto, then so is R^{-1}.

Relations on sets.

- We start with a definition

DEFINITION 55. A **relation on a set** A is a relation from A to A.

- **Example:**
  - Let A denote the set of **strings** of length 3 consisting of x's and y's, (For example xxy is a string, oryyx)
  - Define a relation R from A to A by: If s,t are strings then

$$sRt \iff s \text{ and } t \text{ start with the same 2 characters.}$$

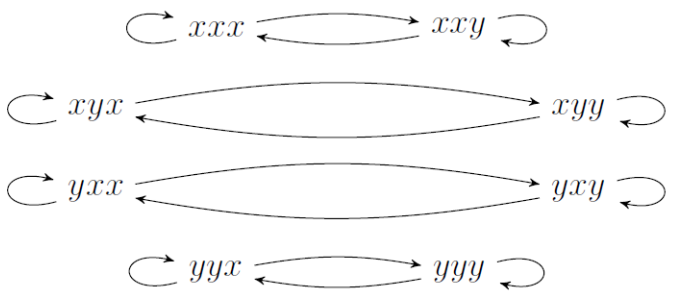
  - **Part (a):** List the elements of A.
    - **Solution:**
    - We have

$$A = \{xxx, xxy, xyx, xyy, yxx, yxy, yyx, yyy\}$$

  - **Part (b):** Is $xxyRxxx$?
    - **Solution:**
    - Yes because both strings start with the same 2 characters, in this case xx.
  - **Part (c):** Is $xyxRyyx$?
    - **Solution:**
    - No because both strings do not start with the same 2 characters. One starts with xy and the other starts with yy.
  - **Part (d):** Is $(yxy, yxx) \in R$?
    - **Solution:**
    - Yes because both strings start with the same 2 characters, in this case yx.

Directed Graph of a Relation on a (single) set A.

- **IDEA:**
  - As of now, a relation A to A, treats the domain and co-domain as two separate set of points
  - Instead of doing this, we can instead represent A only once and draw an arrow from each point of A to each related point.
- **Example:** Draw the directed graph of the string relation (above).
  - **Solution:**



  -

A relation on an infinite set.

- **Example:(The Congruence Modulo 2 Relation)** Define a relation E on $\mathbb{Z}$ by

$$mEn \text{ if and only if } m-n \text{ is even}$$

  - Note: There are equivalent ways to phrase this relation (using some easy to prove results). Can you think of any?
    - mEn if and only if $2 \mid (m-n)$
    - mEn if and only if $m \mod 2 = n \mod 2$, or
    - mEn if and only if m and n have the same remainder when dividing by 2.
    - mEn if and only if m and n have the same parity
- **Example:** List 5 integers that are realted to 1 by E.
  - **Solution:** $31, 35, -3, -9$

Section 8.2 - Reflexivity, Symmetry, and Transitivity.

- **Question:** What should R satisfy so that related objects can be treated as *equal*?
  - In other words, think about which properties of the symbol "=" makes objects equal?
  - The answer to this question is the following definition.
  - Meaning, think that are *equal* usually have the following properties:

DEFINITION 56. Suppose R is a relation on a set A. Then
(r) R is **reflexive** means: $\forall x \in A, xRx$
(s) R is **symmetric** means: $\forall x, y \in A$, if xRy, then yRx.
(t) R is **transitive** means: $\forall x, y, z \in A$ if xRy and yRz, then xRz.

- **Remark:**
  - Using ordered pairs this means:
  - (r) R is **reflexive** means: $\forall x \in A, (x, x) \in R$
  - (s) R is **symmetric** means: $\forall x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
  - (t) R is **transitive** means: $\forall x, y, z \in A$ if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.
- **Examples:** Is R reflexive? symmetric? transitive?
  - **Part (a):** Let $A = \{a, b, c, d\}$ with all the relations being $aRa, aRb, bRa, bRd, dRb, dRd$
    - **Solution:** Let's check each type
    - (r) No, need bRb and cRc
    - (s) Yes!
    - (t) No, need bRb, aRd and dRa
  - **Part (b):** Let $A = \{1, 2, 3\}$ with $R = \{(1, 1), (2, 2), (3, 3), (2, 3), (2, 1)\}$
    - **Solution:** Let's check each type
    - (r) Yes!
    - (s) No, need $(3, 2)$ and $(1, 2)$
    - (t) Yes
  - **Part (c):** Let $A = \mathbb{R}$ with $R = \left\{(x, y) \in \mathbb{R}^2 \mid x < y\right\}$
    - **Solution:** Let's check each type
    - (r) No need $(1, 1)$
    - (s) No, need $(3, 2)$
    - (t) Yes
  - **Part (d):** Let $A = \mathbb{R}$ with $R = \left\{(x, y) \in \mathbb{R}^2 \mid x = y\right\}$
    - **Solution:** Let's check each type
    - (r) Yes
    - (s) Yes
    - (t) Yes
- **Examples:** Let $A = \{1, 2, 3\}$. Construct a relation on A which is:
  - **Part (a):** Relexive only
    - **Solution:**
    - Start by writing some relations that would make it what you want.
    - Let
$$R = \left\{ \underbrace{(1, 1), (2, 2), (3, 3)}_{\text{need at least these to be reflexive}}, (1, 2), (2, 3) \right\}$$
      - This is not symmetric since $1R2$ but $2 \not R1$
      - This is not transitive since $1R2$ and $2R3$ but $1 \not R3$.
  - **Part (b):** Symmetric only
    - **Solution:**
    - Start by writing some relations that would make it what you want.
    - Let
$$R = \left\{ \underbrace{(1, 2), (2, 1)}_{\text{at least this makes symmetric}} \right\}$$

· Other options are possible
· This is not reflexive since $3 \not R 3$
· This is not transitive since $1R2$ and $2R1$ but $1 \not R 1$.

– **Part (c):** Transitive only
  * **Solution:**
  * Start by writing some relations that would make it what you want.
  * We get

$$R = \left\{ \underbrace{(1,2), (2,3), (1,3)}_{\text{at least this makes symmetric}} \right\}$$

· This is not reflexive since $3 \not R 3$
· This is not symmetric since $1R2$ but $2 \not R 1$.

Properties of Relations on Infinite Sets (Writing proofs).

- **Example:** Define a relation R on $\mathbb{Z}$ by

$$mRn \text{ if and only if } 3 \mid (m-n).$$

– **Part(a):** Show R is reflexive.
– We will unravel these definitions to help us prove what we need to prove.
– **Solution:**

PROOF. We must show that $\forall m, n \in \mathbb{Z}, mRm$. This means, we must show that $3 \mid (m-m)$. This is obvious since clearly $3 \mid 0$. Thus mRm, and it follows that R is reflexive. □

– **Part(b):** Show R is symmetric.
– **Solution:**

PROOF. We must show that " $\forall m \in \mathbb{Z}$ if mRn then nRm." This means, we must show that

$$\text{"if } 3 \mid (m-n) \text{ then } 3 \mid (n-m)."$$

In other words, this means

$$\text{"if } (m-n) = 3k, \text{for some } k \in \mathbb{Z} \text{ then } (n-m) = 3(\text{some integer})"$$

So let us suppose that $(m-n) = 3k$, then by multiplying by -1 we get

$$(n-m) = 3(-k).$$

Since $-k \in \mathbb{Z}$ then we showed that $3 \mid (n-m)$
Thus nRm, and it follows that R is symmetric. □

– **Part(c):** Show R is transitive.
– **Solution:**

PROOF. We must show that " $\forall x, y, z \in \mathbb{Z}$ if xRy and yRz then xRz." This means, we must show that

$$\text{"if } 3 \mid (x-y) \text{and } 3 \mid (y-z) \text{ then } 3 \mid (x-z)."$$

In other words, this means

$$\text{"if } (x-y) = 3k, \text{and } (y-z) = 3l \text{for some } k, l \in \mathbb{Z} \text{ then } (x-z) = 3(\text{some integer})"$$

So let us suppose that $(x-y) = 3k$ and $(y-z) = 3l$ then by substitution (and solving the two former equations for x and z) we have

$$\begin{aligned}(x-z) &= (3k+y) - (y-3l) \\ &= 3k + y - y + 3l \\ &= 3k + 3l \\ &= 3(k+l).\end{aligned}$$

Since $k + l \in \mathbb{Z}$ then we showed that $3 \mid (x-z)$
Thus if xRy and yRz then we just showed that xRz, and it follows that R is transitive. □

Section 8.3 - Equivalence Relations

Equivalence Relations (making "different" objects equal).

- We start with a definition.

DEFINITION 57. A binary relation R on a set A is an **equivalence relation** provided that it is reflexive, symmetric, and transitive.

- **Example:** R defined on $\mathbb{Z}$ by

$$mRn \text{ if and only if } 3 \mid (m-n)\,.$$

  is an equivalence relation.
  - We literally just proved this in the last example!
- **Example:** Is R an equivalence relation on $A = \{1,2,3\}$?
  - **Part (a):** When $R = \{(1,1),(2,2),(1,2),(2,1)\}$
    - **Solution:**
    - No, R is not reflexive.
  - **Part (b):** When $R = \{(1,1),(2,2),(3,3),(2,3)\}$
    - **Solution:**
    - No, R is not symmetric.
  - **Part (c):** When $R = \{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3),(3,2)\}$
    - **Solution:**
    - No, R is not transitive.
  - **Part (d):** When $R = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$
    - **Solution:**
    - Yes!
- **Example:** Let $A = \{a, b, \heartsuit, 9\}$, find the missing 3 relations in order to make the following an equivalence relation:

$$R = \{(a,a),(b,b),(\heartsuit,\heartsuit),(a,\heartsuit),(\heartsuit,a),(\heartsuit,b),(a,b),(?,?),(?,?),(?,?)\}$$

  - **Solution:** The missing relations are

$$(b,a),(b,\heartsuit),(9,9)\,.$$

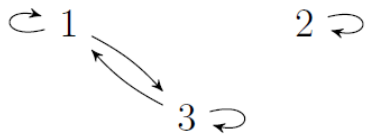
Equivalence Classes.

- We start with a definition

DEFINITION 58. Let R be an equivalence relation on A and let $a \in A$. Then the **equivalence class** of a is denoted by $[a]$ and is defined by

$$[a] := \{x \in A \mid xRa\}$$

- Paraphrasing: The equivalence class of a includes all the other elements related to it. (or equal to it)
- Why are equivalence classes nice. Many reasons. Here's a nice property
  - **Theorem:** We have that xRy if and only if $[x] = [y]$.
- **Example:** Find $[a]$, for each $a \in A$.
  - **Part (a):** Let $A = \{1,2,3\}$ and $R = \{(1,1),(2,2),(3,3),(1,3),(3,1)\}$
  - **Solution:**
  - It helps to draw directed graph:



  -

- Hence

$$[1] = \{1, 3\}$$
$$[3] = \{1, 3\}$$
$$[2] = \{2\}$$

- **Part (b):** Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (a, d), (d, a), (b, d), (d, b)\}$
- **Solution:**
- It helps to draw directed graph:

-
- Hence

$$[a] = \{a, b, d\}$$
$$[b] = \{a, b, d\}$$
$$[d] = \{a, b, d\}$$
$$[c] = \{c\}$$

- **Part (c):** Let $A = \mathbb{R}$ and $R = \{(x, y) \in \mathbb{R} \mid x = y\}$
- **Solution:**
- Each element is only related to itself hence

$$[a] = \{a\} \text{ for all } a \in \mathbb{R}$$

- **Part (d):** Let $A = \mathbb{Z}$ and R be the equivalence relation defined by

$$mRn \text{ if and only if } 3 \mid (m - n).$$

- **Solution:**
- Then recall Q-R Theorem with $d = 3$ then

$$[0] = [3] = [6] = \cdots = \{3k \mid k \in \mathbb{Z}\}$$
$$[1] = [4] = [7] = \cdots = \{3k + 1 \mid k \in \mathbb{Z}\}$$
$$[3] = [5] = [8] = \cdots = \{3k + 2 \mid k \in \mathbb{Z}\}$$

Equivalence Relations and Partitions.

- Recall that an **Equivalence relation** R is a relation on A that is reflexive, symmetric and transitive. And equivalence classes are the sets

$$[a] = \{x \in A \mid xRa\}.$$

From Section 6.1: Partitions of a set. From Section 6.1 (pages 384 – 386).

- We first consider the following definitions. Some of which we have seen before.

DEFINITION 59. Two sets A and B are called **disjoint** if $A \cap B = \emptyset$.

DEFINITION 60. A finite or infinite collection $\mathcal{P}$ of nonempty subsets A_i of a set A is a **partition** of A provided that
(1) $\forall x \in A$, there is some A_i in $\mathcal{P}$ such that $x \in A_i$, and
(2) For all A_i and A_j in $\mathcal{P}$, if $A_i \neq A_j$, then A_i and A_j are disjoint.

- **Paraphrase:** A **partition** is simply a collection of sets $\mathcal{P} = \{A_1, A_2, A_3, \dots\}$ where all the A_i are mutually disjoint and that $A = \cup_{i=1} A_i$.
  - In other words, a **partition** is simply a way to cut a set A into different disjoint pieces.
- **Examples:**
  - **Part (a):** Let $A = \{1, 2, 3\}$ and example of a partition of A is

$$\mathcal{P} = \{\{1, 2\}, \{3\}\}.$$

- **Part (b):** Let $A = \{1, 2, 3, \dots, 10\}$ and example of a partition of A is
$$\mathcal{P} = \{\{1, 3, 5\}, \{2, 7\}, \{4, 9, 10\}, \{6\}, \{8\}\}.$$
- **Part (c):** Let $A = \mathbb{Z}$ and example of a partition of A is
$$\mathcal{P} = \{\{\dots, -6, -3, 0, 3, 6, \dots\}, \{\dots, -5, -2, 1, 4, 7, \dots\}, \{\dots, -4, -1, 2, 5, 8, \dots\}\}.$$
These sets are the $3q, 3q+1, 3q+2$ integer, the $r = 0, 1, 2$ when dividing by 3 from the Q-R Theorem.
- **Part (d):** Let $A = \mathbb{Z}$ and example of a partition of A is
$$\mathcal{P} = \{\{0\}, \{\pm 1\}, \{\pm 2\}, \dots\}.$$
Note the cells in this partition capture a sameness within the integers, that of "same size".

Back to Section 8.3:

- We have the following theorem that connects partitions with equivalence relations.

THEOREM. *(Theorem 1) If A is a set and R is an equivalence relation on A, then the set of equivalence classes of R forms a partition $\mathcal{P}$ of A.*

PROOF. Omited. □

- **Example:** Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$
  - The equivalence classes are
$$[1] = [2] = \{1, 2\},$$
$$[3] = \{3\}.$$
and observe that
$$\mathcal{P} = \{\{1, 2\}, \{3\}\}$$
is a partition, just like the theorem said it would.

DEFINITION 61. Let $\mathcal{P}$ be a partition of A. The **relation $R_{\mathcal{P}}$ on A induced by $\mathcal{P}$** is defined by
$$(x, y) \in R_{\mathcal{P}} \text{ iff } \exists A_i \in \mathcal{P} \text{ such that } x \text{ and } y \text{ are both in } A_i.$$

- **Paraphrase:** The Relation $R_{\mathcal{P}}$ is simply relation that says if $\mathcal{P} = \{A_1, A_2, \dots\}$ is a partition then we define all the elements in the same group A_i to be related to each other.
- **Example:** Find $R_{\mathcal{P}}$ for the following partitions.
  - **Part (a):** Let $A = \{1, 2, 3\}$ and $\mathcal{P} = \{\{1, 2\}, \{3\}\}$
    - **Solution:**
    - It might help to draw a directed graph by drawing dots for each point and connecting all the points that are in the same set/group.
      - In this example $1, 2$ will be related to each since it's in the same group
      - And 3 will only be realted to itself since it's in a group by itself.
    - We get
$$R_{\mathcal{P}} = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}.$$
  - **Part (b):** Let $A = \{a, b, c, d, e, f\}$ and $\mathcal{P} = \{\{a, b, f\}, \{c\}, \{d, e\}\}$
    - **Solution:**
    - It might help to draw a directed graph by drawing dots for each point and connecting all the points that are in the same set/group.
      - There three groups, and within each group, everything will be related to each other.
    - We get
$$R_{\mathcal{P}} = \left\{ \begin{array}{ccccccc} (a,a) & (a,b) & (a,f) & & (d,d) & (d,e) \\ (b,a) & (b,b) & (b,f) & (c,c) & (e,d) & (e,e) \\ (f,a) & (f,b) & (f,f) & & & \end{array} \right\}.$$

- We have the following theorem that says that $R_{\mathcal{P}}$ is not only a relation, but it's an equivalence relation!

THEOREM. *(Theorem 2) Let $\mathcal{P}$ be a partition of a set A. Then $R_{\mathcal{P}}$ is an equivalence relation on A, i.e. reflexive, symmetric, and transitive.*

PROOF. Omited □

THEOREM. *(Theorem 3) Every equivalence relation on A is of the form $R_{\mathcal{P}}$ for some partition $\mathcal{P}$ of A, namely, the se of equivalence classes.*

PROOF. Omited □

- What these theorems are saying are: To find all possible equivalence relations on A, just find all partitions.
- **Example:** Let's find all equivalence relations of $A = \{1, 2, 3\}$.
  - **Solution:**
  - We have the following complete list of partitions of A:
    - (1) $\mathcal{P}_1 = \{\{1\}, \{2\}, \{3\}\}$
    - (2) $\mathcal{P}_2 = \{\{1\}, \{2, 3\}\}$
    - (3) $\mathcal{P}_3 = \{\{2\}, \{1, 3\}\}$
    - (4) $\mathcal{P}_4 = \{\{3\}, \{1, 2\}\}$
    - (5) $\mathcal{P}_5 = \{\{1, 2, 3\}\}$
  - Consequently, the equivalence relations $R = R_{\mathcal{P}}$ are
    - (1) $R_{\mathcal{P}_1} = \{(1, 1), (2, 2), (3, 3)\}$
    - (2) $R_{\mathcal{P}_2} = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$
    - (3) $R_{\mathcal{P}_3} = \{(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)\}$
    - (4) $R_{\mathcal{P}_4} = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$
    - (5) $R_{\mathcal{P}_5} = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\}$

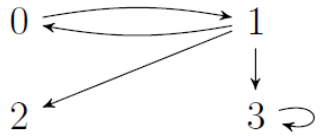
Section 8.5 - Partial Order Relations

Anti-symmetry.

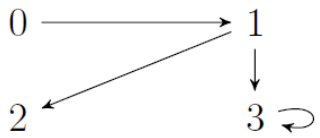
- We start with a definition.

DEFINITION 62. Let R be a relation on a set X. Then R is **anti-symmetric** provided that $\forall x, y \in X$ if xRy and yRx, then $x = y$.

- **Remark:** In terms of the directed graph of the relation, this says there aren't arrows ging both ways between elements.
- **Example 1:** Is R anti-symmetric on $X = \{0, 1, 2, 3\}$?
  - **Part (a):** When $R = \{(0,1), (1,0), (1,2), (1,3), (3,3)\}$
    - **Solution:** Drawing the directed graph we have



    - No! Note that we have $(0,1)$ and $(1,0) \in R$ but $0 \neq 1$.
  - **Part (b):** When $R = \{(0,1), (1,2), (1,3), (3,3)\}$
    - **Solution:** Drawing the directed graph we have



    - Yes! Note that there are no arrows going back and forth.
- **Example 2:** Is the "divides" relation ($aRb \iff a \mid b$) antisymmetric on
  - **Part(a):** On the set $X = \mathbb{Z}$?
    - **Solution:** No, because $2 \mid (-2)$ and $(-2) \mid 2$ but $2 \neq -2$.
  - **Part(b):** On the set $X = \mathbb{N}$?
    - **Solution:** Yes,
    - *Proof:* Suppose $a \mid b$ and $b \mid a$. Then this means

$$b = ak, \text{ for some } k \in \mathbb{N}$$
$$a = bl, \text{ for some } l \in \mathbb{N}.$$

By substitution, this means

$$b = ak = blk,$$

since $b \neq 0$, then

$$lk = 1.$$

Since $l, k \in \mathbb{N}$ then the only solution to this is that $l = 1$ and $k = 1$. Hence

$$b = a,$$

as desired.

Partial Order Relation.

- Somewhat analogous to how **equivalence relations** are generalizations of equality "="
  - **Partial order relations** are generalizations of the relation "$\leq$" on numbers.

DEFINITION 63. Let R be a relation on X. Then R is a **partial order relation** provided that R is reflexive, antisymmetric, and transitive.

- One can think of this a the one-way relation!
  - One can think of partial relations as a set of roads/connections/relations where you can only move up in one direction but not the other way around.
- **Examples:**

  - **Part (a):** The Relation "$\leq$" is a partial order relation on any set of real numbers.
    - **Solution:**
    - Note obviously that if $A \subset \mathbb{R}$.
    - (r) Then any real number is related to itself since $x \leq x$
    - (anti-s) It's antisymetric since if $x \leq y$ then $y \not\leq x$ if $x \neq y$.
    - (t) Obviously if $x \leq y$ and $y \leq z$ then $x \leq z$.
  - **Part (b):** The "Divides" relation "$|$" is a partial order relation on $\mathbb{N}$.
    - **Solution:**
    - (r) Note that for all $n \in \mathbb{N}$, $n \mid n$.
    - (anti-s) This was done in Example 2 of the previous subsection
    - (t) We've proved this before: if $x \mid y$ and $y \mid z$ then $x \mid z$.
  - **Part (c):** The relation "$\subseteq$" is a partial order relation on $\mathcal{P}(A)$ for any set A.
    - **Solution:**
    - (r) Any set is a subset of itself: $A \subseteq A$
    - (anti-s) If $A \subseteq B$ and $B \subseteq A$ then by definition we know this means $A = B$.
    - (t) If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.
- **Notation:** Rather than writing R for a general partial order relation. We will use "$\leq$" or more generally

$$\preceq$$

The Lexicographic Order.

- In English, there is a well known defined order on the set of letters of the alphabet

$$A = \{a, b, c, \ldots, w, x, y, z\}\,.$$

  - From this, we have learned to how to order any names, or words alphabetically on the **set of all words.**
  - This is the so called **dictionary ordering.**

$$a \preceq b \preceq \cdots$$

- **Example:** If $\preceq$ is the dictionary ordering then

$$\begin{aligned} \text{ship} &\preceq \text{shop} \\ \text{ship} &\preceq \text{ships} \\ \text{Carlos} &\preceq \text{Kara} \end{aligned}$$

- There is a (natural) way to generalize this to order the set of strings of characters that have an ordering.
- This is the lexicographic order. See Theorem 8.5.1 in "Discrete Mathematics with Applications" S. Epp, Fifth Edition, for a formal definition:

Theorem 8.5.1

Let A be a set with a partial order relation R, and let S be a set of strings over A. Define a relation $\preceq$ on S as follows:

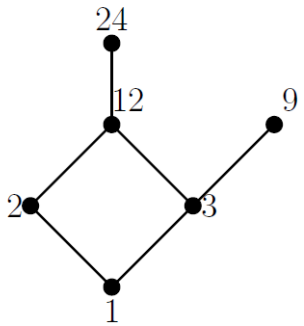
For any two strings in S, $a_1a_2\cdots a_m$ and $b_1b_2\cdots b_n$, where m and n are positive integers,

1. If $m \leq n$ and $a_i = b_i$ for all $i = 1, 2, \ldots, m$, then
$$a_1a_2\cdots a_m \preceq b_1b_2\cdots b_n.$$
2. If for some integer k with $k \leq m$, $k \leq n$, and $k \geq 1$, $a_i = b_i$ for all $i = 1, 2, \ldots, k-1$, and $a_k \neq b_k$, but $a_k \; R \; b_k$ then
$$a_1a_2\cdots a_m \preceq b_1b_2\cdots b_n.$$
3. If ε is the null string and s is any string in S, then $\epsilon \preceq s$.

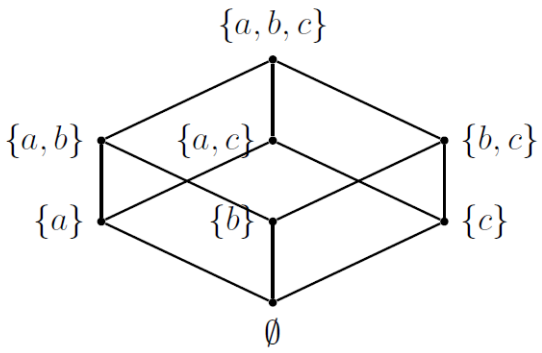
If no strings are related other than by these three conditions, then $\preceq$ is a partial order relation.

- **Lexicographic order summary:**
  - Let A be a starting set that is called an **alphabet**. And let R be a partial order on A.
  - The string in S are called **words**.
  - The partial lexicographic order $\preceq$ on strings is defined in the usual way oe would do with English words.

Hasse Diagram of a Partial Order Relation.

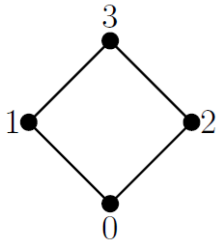
- **Hasse Diagrams:**
  - Start with the directed graph of the relation with "smaller" elements drawn lower and all arrows pointing up.
  - Then declutter the graph by removing things we know given the relation is a partial order relation.
    - Delete all loops. (Implied from refexivity)
    - Delete all arrows whose existence is implied by transitivity.
    - Delete the arrowheads. (Becomes unnecessary by our positioning smaller below larger.)
- **Example:** Draw the Hasse diagram for the given partial order relation.
  - **Part (a):** The "divides" relation "$|$" on $A = \{1, 2, 3, 9, 12, 24\}$.
  - **Solution:**
    - We have
    - 

  - **Part (b):** The relation "$\subseteq$" on $A = \mathcal{P}(\{a, b, c\})$.
  - **Solution:**
    - We have that



*

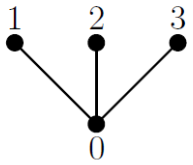
- Now Let's reverse engineer the partial order relation from the Hasse Diagram:
- **Example:** Let $A = \{0, 1, 2, 3\}$. Given the Hasse diagam, find the (partial) order relation.



  - **Part (a):** Suppose the Hasse diagram is given by
  - **Solution:**
    - In the bottom layer we have $0 \leq 1, 2, 3$
    - From the middle layer we also know that $1 \leq 3$ and $2 \leq 3$
    - We also need to add all the reflexive orderings: $0 \leq 0$, $1 \leq 1$ $2 \leq 2$ and $3 \leq 3$
    - Hence

$$R = \{(0,0), (1,1), (2,2), (3,3), (0,1), (0,2), (0,3), (1,3), (2,3)\}$$

    - Note that, we don't have a comparison between 1 and 2 at all!



  - **Part (b):** Suppose the Hasse diagram is given by
  - **Solution:**
    - From bottom layer we have $0 \leq 1, 2, 3$
    - We also need to add all the reflexive orderings: $0 \leq 0$, $1 \leq 1$ $2 \leq 2$ and $3 \leq 3$
    - Hence

$$R = \{(0,0), (1,1), (2,2), (3,3), (0,1), (0,2), (0,3)\}$$

    - Note that, we don't have a comparison between $1, 2$ and 3 at all!

Partially and Totally Ordered Sets.

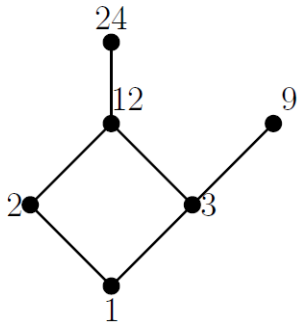
- We start with a definition

DEFINITION 64. A set X together with the partial order R on X is called a **partially ordered set** or **poset**.

- Posets are pronounced POsets. (like poahsets)
- **Notation:** We like to use the notation (X, R) for a poset.
  - For example, the poset given by the power set of a set A, ordered by subset inclusion, might be denoted $(\mathcal{P}(A), \subseteq)$

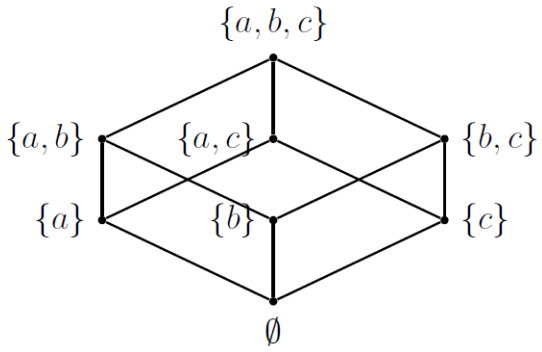
DEFINITION 65. A **total order relation** on X is a partial order R such that $\forall x, y \in X$, either xRy or yRx.

- **Remarks:**
  - Recall that in some previous examples, not all elements were related (or ordered in some way). Thus a total order relation, means all elements of X has some kind of ordering between each other!
  - A set X with a total order relation is called a **totally ordered set**. (Should we called it **toset**?)
  - If $x \leq y$ or $y \leq x$ in some poset $(X, \leq)$, then we say that x and y are **comparable**.
- **Examples: Here are some posets and tosets**
  - **Part (a):** The set $A = \{1, 2, 3, 9, 12, 24\}$ with the relation "$x \mid y$" is a partially ordered set, a poset. That is, $(A, |)$ is a poset.

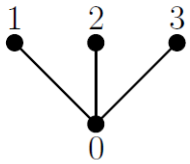


    * Recall that we got the Hasse diagram:
    * This is NOT a totally ordered set, since 2 and 9 are NOT comparable!
  - **Part (b):** Consider the poset $(\mathcal{P}(A), \subseteq)$ is a poset. In general, this poset is not a totally ordered set. Consider the previous example where we had

$$(\mathcal{P}(\{a, b, c\}), \subseteq)$$



    * Recall that we got the Hasse diagram:
    * This is NOT a totally ordered set, since for example, $\{a\}, \{b\}$ and $\{c\}$ are all NOT comparable!
      · Why? Well neither $\{a\} \subseteq \{b\}$ or $\{b\} \subseteq \{a\}$!!

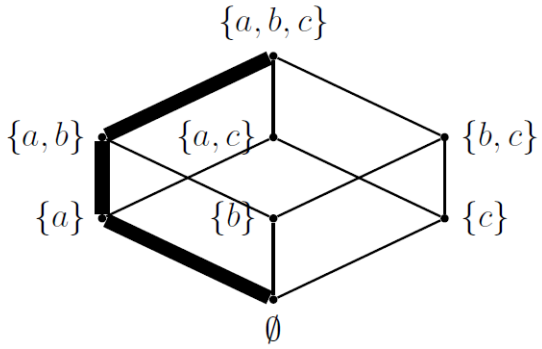


  - **Part (c):** The example given before by the Hasse diagram is not totally ordered.
  - **Part (d):** Let $A \subseteq \mathbb{R}$ then $(A, \leq)$is a poset. In fact, it is a totally ordered set.
    * You can always compare any real number.

Chains.

DEFINITION 66. Let $(X, \leq)$ be a poset.
A subset $C \subseteq X$ is called a chain provided that $\forall x, y \in C$, $x \leq y$ or $y \leq x$.

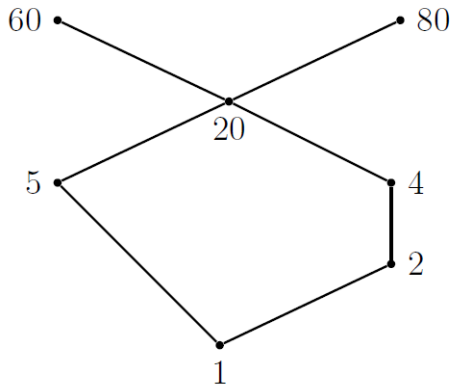
The length of C is one less than the number of elements in C.

- **Example:** A **chain** C of length 3 in $(\mathcal{P}(\{a,b,c\}),\subseteq)$ is
$$C = \{\emptyset, \{a\}, \{a,b\}, \{a,b,c\}\}.$$
  - Here it is embedded within the Hasse Diagram:
  - 

Maximal/minimals Elements.

- We consider the following definitions

DEFINITION 67. Let $(X,\leq)$ be a poset. Then $a \in X$ is called a:
(1) **maximal element** iff $\forall x \in X$, $x \leq a$, or x, a are not comparable
(2) **greatest element** iff $\forall x \in X$, $x \leq a$
(2) **minimal element** iff $\forall x \in X$, $a \leq x$ or, x, a are not comparable
(3) **greatest element** iff $\forall x \in X$, $a \leq x$

- **Example:** Let $X = \{1,2,4,5,20,60,80\}$ with partially ordered relation "$n \mid m$". Draw the Hasse diagram and find all maximal, greatest, minimal and least elements
  - **Solution:**
  - We have
  - 

  - **Maximal:** $60, 80$
    - Clearly $60, 80$ is greater than or equal to all the elements.
  - **Greatest:** None
    - But since we can't compare 60, and 80 than there is no greatest element!
  - **Minimal:** 1
  - **Least:** 1

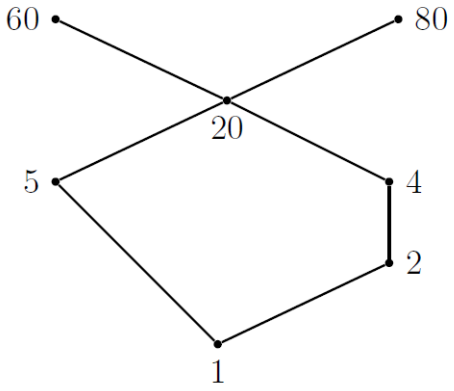
Topological Sorting:

- We want to find a total order "compatible" with a partial one.

DEFINITION 68. Suppose $\leq$ and $\leq'$ are partial orders one a set X. Then $\leq'$ is a **refinement** of $\leq$ provided that for all $x, y \in X$, if $x \leq y$, then $x \leq' y$.

The book says $\leq'$ is **compatible** with $\leq$.

- **Example:** Let's look again at $X = \{1, 2, 4, 5, 20, 60, 80\}$ ordered by "divides". This is not a total ordering as some elements in X are not comparable, for example, 4 and 5.
  - **Question:** Can we find a total ordering that is compatible with the divides ordered? I.e., can we find a total odering that still has the divides ordering in which the following ordering we obtain is still true:



  -
  - There are many possible answers:
  - **Solution 1:** The usual ordering of $\leq$ on X is a totally ordered refinement of "divides": Since

$$1 \leq 2 \leq 4 \leq 5 \leq 20 \leq 60 \leq 80.$$

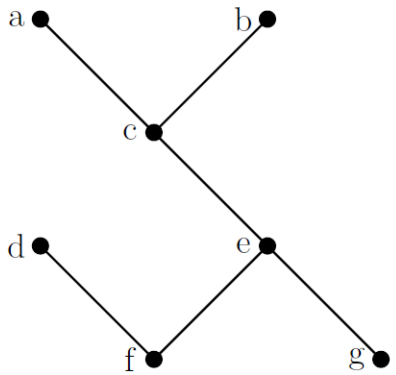
    as it still maintains the same ordering that divides provide.
  - **Solution 2:** The usual ordering of $\leq$ on X is a totally ordered refinement of "divides": Since

$$1 \preceq 5 \preceq 2 \preceq 4 \preceq 20 \preceq 80 \preceq 60$$

    as it still maintains the same ordering that divides provide.

Topological Sorting Algorithm:

- Here is an algorithm that can always build a total ordering from a partial ordering:
  - The algorithm does not produce a unique total ordering!
- **Algorithm:** Let $\preceq$ be a partial order relation on a finite set X. To construct a totally ordered refinement:
  (1) Pick *any* minimal element $x \in X$. (*which exists since X is finite*)
  (2) Let $X' = X - \{x\}$
  (3) Repeast the following steps while $X' \neq \emptyset$.
    (a) Pick any minimal element y in X'
    (b) Define $x \preceq' y$
    (c) Set $X' := X' - \{y\}$
- Remarks:
  - Note that the the loop in Step 3 will halt since X is finite.
  - This will give a total ordering $x_1 \preceq' x_2 \preceq' \cdots \preceq' x_n$ where n is the number of elements in X.
  - The ordering is NOT unique.
- **Example:** Use the Topological Sorting Algorithm to find a total ordering compatible with $\preceq$ given by the following Hasse Diagram:



-
  - **Solution 1:** One answer using the algorithm can be
    $$g \preceq' f \preceq' e \preceq' c \preceq' a \preceq' b \preceq' d$$
  - **Solution 2:** Another answer using the algorithm can be
    $$f \preceq' d \preceq' g \preceq' e \preceq' c \preceq' b \preceq' a$$

CHAPTER 9

Probability

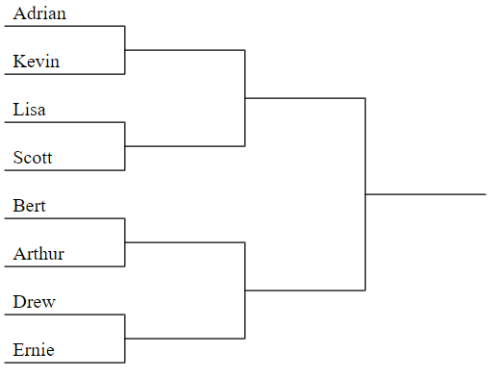
Section 9.1 - Counting

Section 9.1.1 - The Counting Principle.

- **Remark:**
  - These **notes** do not directly correspond with the same order and sections covered in the textbook.
  - The Homework will be assigned separately from the textbook problems.
- We need a way to help us count faster rather than counting by hand one by one.

DEFINITION 69. (**Basic Counting Principle**) Suppose 2 experiments are to be performed.
If one experiement can result in m possibilities
Second experiment can result in n possibilities
Then together there are mn possibilities

- I like to use the box method. For example. Each box represents the number of possibilities in that experiement.
- **Example1:** There are 20 teachers and 100 students in a school. How many ways can we pick a teacher and student of the year?
  - **Solution:** Use the box Method: $20 \times 100 = 2000$.
- The counting principle can be generalized to any amount of experiments: $n_1 \cdots n_r$ possibilities
- **Example2:**
  - A college planning committee consists of 3 freshmen, 4 sophomores, 5 juniors, and 2 seniors.
  - A subcomittee of 4 consists 1 person from each class. How many?
  - **Solution:** Box method $3 \times 4 \times 5 \times 2 = 120$.
- **Example3:** How many different 6−place license plates are possible if the first 3 places are to be occupied by letters and the finals 3 by numbers?
  - **Solution:** $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 =$?
  - Question: What if no repetition is allowed?
  - **Solution:**$26 \cdot 25 \cdot 24 \cdot 10 \cdot 9 \cdot 8$



- **Example4:** Consider the following 1v1 basketball tournament Bracket:
  - How many possible outcomes can occur for this tournament?
  - **Solution:**
    - Note that there are only two outcomes for the the result of each individual game.

* Since there are 7 games, then there are total of

$$\underbrace{2\cdot 2\cdot 2\cdot 2}_{\text{quarterfinals}}\cdot\ \underbrace{2\cdot 2}_{\text{semifinals}}\ \cdot\underbrace{2}_{\text{finals}}=2^7=128.$$

- **Example 5:** How many $n-$ place Boolean functions exist?
  - **Solution:** A $n-$place Boolean function is a function $f:\{0,1\}^n\to\{0,1\}$.
    * First let us find how many inputs there exists in $\{0,1\}^n$. We note that

$$\text{number of elements in } \{0,1\}^n=\underbrace{2\cdot 2\cdot\cdots\cdot 2}_{n\text{ times}}=2^n.$$

    * Now each input has 2 possible outputs, so

$$\underbrace{2}_{\text{possible outputs for 1st input}}\cdot\ \underbrace{2}_{\text{possible outputs for 2nd input}}\ \cdots\ \underbrace{2}_{\text{possible outputs for the } 2^n \text{ input}}$$

    $=2^{2^n}$.

Section 9.1.2 - Permutations.

- How many different ordered arrangements of the letters a, b, c are possible?
  - abc, acb, bac, bca, cab Each arrangement is a permutation
  - Can also use the box method to figure this out: $3 \cdot 2 \cdot 1 = 6$.

DEFINITION 70. With n objects, a **permutation** is an arrangement/ordering of n objects. There are

$$n\,(n-1)\cdots 3\cdot 2\cdot 1 = n!$$

different **permutations** of the n objects.

- **Remark:** Note that ORDER matters when it comes to Permutations!
- **Example1:** What is the numnber of possible batting order with 9 players?
  - **Answer:** 9!(Box Method or permutations)
- **Example2:** How many ways can one arrange 4 math books, 3 chemistry books, 2 physics books, and 1 biology book on a bookshelf so that all the math books are together, all the chemistry books are together, and all the physics books are together.
  - **Answer:** We can arrange the math books in 4! ways, the chemistry in 3! ways, the physics in 2! ways, and B in $1! = 1$ way.
  - But we also have to decide which set of books go on the left, which next, and so on. That is the same as the number of ways of arranging the letters M,C, P,B, and there are 4! ways of doing that. $MCPB$, $PBPB$ ect..
  - So $4!\,(4!3!2!1!)$ ways.
- **Example3:** Repetitions: How many ways can one arrange the letters a, a, b, c?
  - Let us label them A, a, b, c. There are 4!, or 24, ways to arrange these letters. But we have repeats: we could have Aa or aA. So we have a repeat for each possibility (**so divide!!!**), and so the answer should be $4!/2! = 12$.
  - If there were 3 a's, 4 b's, and 2c's, we would have

$$\frac{9!}{3!4!2!}$$

- **Example4:** How many different letter arrangements can be formed from the word PEPPER?
  - **Answer:** There 3 P's 2 E's and one R. So $\frac{6!}{3!2!1!} = 30$.

FACT. *There are*

$$\frac{n!}{n_1!\cdots n_r!}$$

different permutations of n objects of which n_1 are alike, n_2 are alike, n_r are alike.

- **Example4:** Suppose there are 4 Czech tennis players, 4 U.S. players, and 3 Russian players, in how many ways could they be arranged?
  - Answer: $\frac{11!}{4!4!3!}$.

Section 9.1.2 - Combinations.

- We are often interested in selecting r objects from a total of n objects.
- How many ways can we choose 3 letters out of 5? (Does order matter here? NO)If the letters are a, b, c, d, e then there would be 5 for the first position, 4 for the second, and 3 for the third, for a total of $5 \times 4 \times 3$. But order doesn't matter here. So we're over counting here....
  - But suppose the letters selected were a, b, c. If order doesn't matter, we will have the letters a, b, c $3! = 6$ times, because there are 3! ways of arranging a group of 3. The same is true for any choice of three letters. So we should have
  $$\frac{5 \cdot 4 \cdot 3}{3!} = \frac{5!}{3!2!} = 10.$$
  Or what we did was $5 \cdot 4$, or $n(n-1)\cdots(n-r+1)$ then divided by the repeats 3!.
  - This is often written $\begin{pmatrix} 5 \\ 3 \end{pmatrix}$, read *"5 choose 3". More generally..*

DEFINITION 71. If $r \leq n$, then
$$\begin{pmatrix} n \\ r \end{pmatrix} = \frac{n!}{(n-r)!r!}$$
and we say "n choose r", represents the number of possible **combinations** of objects taken r at a time.

- **Remark:** Order DOES NOT Matter here
- Recall in Permutations order did matter.
- **Example1:** How many ways can one choose a committee of 3 out of 10 people?
  - **Answer:** $\begin{pmatrix} 10 \\ 3 \end{pmatrix} = \frac{10!}{3!7!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2} = 10 \cdot 3 \cdot 4 = 120.$
- **Example2:** Suppose there are 9 men and 8 women. How many ways can we choose a committee that has 2 men and 3 women?
  - **Answer:** We can choose 2 men in $\begin{pmatrix} 9 \\ 2 \end{pmatrix}$ ways and 3 women in $\begin{pmatrix} 8 \\ 3 \end{pmatrix}$ ways. The number of committees is then the product $\begin{pmatrix} 9 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ 3 \end{pmatrix}$.
- **Example3:**A person has 8 friends, of whom 5 will be invited to a party. (We've all been through this)
  - **(a)** How many choices are there if 2 of the friends are feuding and will not attend together?
    - Box it: $[none] + [$ one of them$]\,[others]$
    - $\begin{pmatrix} 6 \\ 5 \end{pmatrix} + \begin{pmatrix} 2 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 4 \end{pmatrix}$ (recall that when we have OR, use +)
  - **(b)** How many choices if 2 of the friends will only attend together?
    - Box it: $[none] + [$with both$]$
    - $\begin{pmatrix} 6 \\ 5 \end{pmatrix} + 1 \cdot 1 \cdot \begin{pmatrix} 6 \\ 3 \end{pmatrix}$
- The value of $\begin{pmatrix} n \\ r \end{pmatrix}$ are called binomials coefficients because of their prominence in the binomial theorem.

THEOREM. *(The Binomial Theorem)*
$$(x+y)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} x^k y^{n-k}.$$

PROOF. To see this, the left hand side is $(x+y)(x+y)\cdots(x+y)$. This will be the sum of 2^n terms, and each term will have n factors. How many terms have k x's and $n-k$ y's? This is the same as asking in a sequence of n positions, how many ways can one choose k of them in which to put x's? (Box it) The answer is $\begin{pmatrix} n \\ k \end{pmatrix}$, so the coefficient of $x^k y^{n-k}$ should be $\begin{pmatrix} n \\ k \end{pmatrix}$. □

- **Example:** Expand $(x+y)^3$.

– **Solution:** $(x+y)^3 = y^3 + 3xy^2 + 3x^2y + x^3$.

Section 9.1.3 - Multinomial Coefficients.

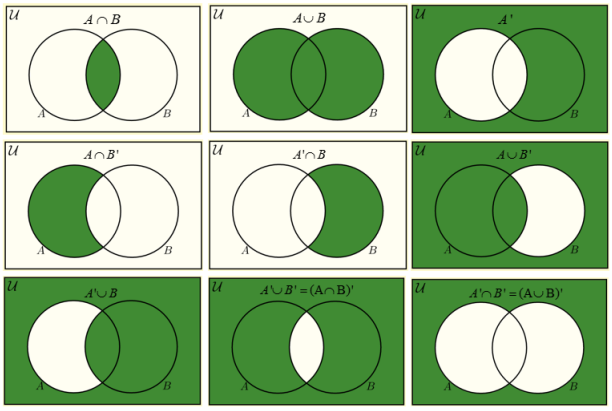
- **Example:** Suppose one has 9 people and one wants to divide them into one committee of 3, one of 4, and a last of 2. How many different ways are there?
  - **Solution:** (Box it) There are $\begin{pmatrix} 9 \\ 3 \end{pmatrix}$ ways of choosing the first committee. Once that is done, there are 6 people left and there are $\begin{pmatrix} 6 \\ 4 \end{pmatrix}$ ways of choosing the second committee. Once that is done, the remainder must go in the third committee. So there is 1 one to choose that. So the answer is
$$\frac{9!}{3!6!}\frac{6!}{4!2!} = \frac{9!}{3!4!2!}.$$
- **In general:** Divide n objects into one group of n_1, one group of n_2, ... and a kth group of n_k, where $n = n_1 + \cdots + n_k$, the answer is there are
$$\frac{n!}{n_1!n_2!\cdots n_k!} \text{ ways.}$$
- These are known as multinomial coefficients. We write them as
$$\begin{pmatrix} n \\ n_1, n_2, \ldots, n_k \end{pmatrix} = \frac{n!}{n_1!n_2!\cdots n_k!}.$$
- **Example:** Suppose we are to assign Police officers their duties . Out of 10 officers: 6 patrols, 2 in station, 2 in schools.
  - **Answer**: $\frac{10!}{6!2!2!}$.
- **Example:** There are 10 flags:5 indistinguishable Blue flags, 3 indistinguishable Red flags, and 2 indistinguishable Yellow flags. How may different ways can we order them on a flag pole?
  - **Answer:** $\frac{10!}{5!3!2!}$.

Section 9.2 - Introduction to Probability

Section 9.2.1 - Events.

- We will define a **sample space**, denoted S (sometimes Ω, or $\mathcal{U}$) that consists of all possible outcomes from an experiment.

DEFINITION 72. A **sample space** S is the set of all possible outcomes of a random experiment. An element $x \in S$ is called an **outcome**. An **event** E is a subset of S.

- **Example1:**
  - Experiment: Roll two dice,
    - **Sample Space:** $S =$ would be all possible pairs made up of the numbers one through six. List it here like this:
    $$S = \{(i,j) : i,j = 1,\dots 6\}$$
    . Using the Box Method, this Experiment as 36 outcomes.
  - **Example 2:**
    - Experiment: Toss a coin twice
    - We can list the sample space as
    $$S = \{HH, HT, TH, TT\}\,.$$
  - **Example3:**
    - Experiment: Measuring the number of accidents of a random person before they had turn 18.
      - $S = \{0, 1, 2, \dots\}$
  - **Others:**
    - Let S be the possible orders in which 5 horses finish in a horse race;
    - Let S be the possible price of some stock at closing time today; or $S = [0, \infty)$;
    - The age at which someone dies, $S = [0, \infty)$.
- **Events:** An event A is a subset of S. In this case we use the notation $A \subset S$, to mean A is a subset of S.
  - $A \cup B$: points in S such that is in A OR B OR BOTH.
  - $A \cap B$, points in A AND B. (you may also see AB)
  - A^c is the compliment of A, the points NOT in A. (you may also see A')
  - Can extend to $A_1, \dots, A_n$ events. $\bigcup_{i=1}^{n} A_i$ and $\bigcap_{i=1}^{n} A_i$.
  - 

- **Example1**: Roll two dice.
  - Example of an Events
  - $E = \{\text{the two dies come up even and equal}\} = \{(2,2), (4,4), (6,6)\}$
  - $S_8 = \{\text{the sum of the two dice is 8}\} = \{(2,6), (3,5), (4,4), (5,3), (6,2)\}$.
  - $E \cup S_8 = \{(2,2), (2,6), (3,5), (4,4), (5,3), (6,2), (6,6)\}$
  - $E \cap S_8 = \{(4,4)\}$.
  - $S_8^c =$ all the 31 other ways that does not include $\{(2,6), (3,5), (4,4), (5,3), (6,2)\}$.
- **Example2:** $S = [0, \infty)$ age someone dies.

  - Event A = person dies before they reached 30.
    * $A = [0, 30)$.
  - Interpret $A^c = [30, \infty)$
    * The person dies after they turned 30.
  - $B = (15, 45)$. Do $A \cup B, A \cap B$ and so on.
- **Properties:** Events also have commutative and associate and Distributive laws.
- What is $A \cup A^c$? $= S$.
- **DeMorgan's Law:**
  - $(A \cup B)^c = A^c \cap B^c$ .Try to draw a picture
  - $(A \cap B)^c = A^c \cup B^c$.
  - This works for general $A_1, \ldots, A_n$: $(\cup_{i=1}^n A_i)^c = \cap_{i=1}^n A_i^c$ and $(\cap_{i=1}^n A_i)^c = \cup_{i=1}^n A_i^c$.
- The empty set $\emptyset = \{\}$ is the set that has nothing in it.
- A and B are **disjoint** if $A \cap B = \emptyset$.
  - In Probability we may say that events A and B are "mututally exclusive" if they are disjoint.
  - mutually exclusive means the same thing as disjoint

Section 9.2.2 - Axioms of Probability.

- Let E be an event. How do we defined the probability of an event?
  - We can attempt to define a probability by the relative frequency,
  - Perform an experiment (e.g. Flipping a coin)
  - Perform that experiment n times and let $n(E)$ = the number of times the event occured in n repetitions
    - (e.g. Flip a coin $n = 1000$ times, and let's say that $n(\{Tails\}) = 551$) Then it's reasonanble to think $\mathbb{P}(\{Tails\}) \approx \frac{551}{1000}$
  - So maybe we can define the probability of an event as $\mathbb{P}(E) = \lim_{n\to\infty} \frac{n(E)}{n}$. But we don't know if this limit exists, or if $n(E)$ is even well defined!!!
  - So we need a new approach.
- Probability will be a rule given by the following Axioms (Laws that we all agree on)

DEFINITION 73. A **probability** $\mathbb{P}$ is a function $\mathbb{P} : S \to \mathbb{R}$ where the input is a set/event such that
Axiom 1: $0 \leq \mathbb{P}(E) \leq 1$ for all events E.
Axiom 2: $\mathbb{P}(S) = 1$.
Axiom 3: (disjoint property) If the events $E_1, E_2, \ldots$ are pairwise disjoint/mutually exclusive then

$$\mathbb{P}\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{\infty} \mathbb{P}(E_i).$$

Mutually exclusive means that $E_i \cap E_j = \emptyset$ when $i \neq j$.

- **Remark:** Note that you take a probability of a subset of S, not of points of S. However it is common to write $P(x)$ for $P(\{x\})$.
  - Say if the experiment is tossing a xoin. Then $S = \{H, T\}$. The probability of heads should be written as $\mathbb{P}(\{H\})$, but it is common to see $\mathbb{P}(H)$.
- **Example1:**
  - (a) Suppose we toss a coin and they are equally likely then $S = \{H, T\}$ and
    - $\mathbb{P}(\{H\}) = \mathbb{P}(\{T\}) = \frac{1}{2}$. We may write $\mathbb{P}(H) = \mathbb{P}(T) = \frac{1}{2}$.
  - (b) If biased coin is tosse then one could have a different assignment of probability $\mathbb{P}(H) = \frac{2}{3}, \mathbb{P}(T) = \frac{1}{3}$.
- **Example2:**
  - Rolling a fair die, the probability space consists of $S = 1, 2, 3, 4, 5, 6$, each point having probability $\frac{1}{6}$.
  - We can compute the probability of rolling an even number by

$$\begin{aligned} \mathbb{P}(\{\text{even}\}) &= \mathbb{P}(\{2, 4, 6\}) \\ &= \mathbb{P}(2) + \mathbb{P}(4) + \mathbb{P}(6) = \frac{1}{2} \end{aligned}$$

    where we used the rules of probability by breaking it down into a sum.

PROPOSITION. *(Properties of Probability)*
(a) $\mathbb{P}(\emptyset) = 0$
(b) If $A_1, \ldots, A_n$ *are pairwise disjoint,* $\mathbb{P}(\cup_{i=1}^{n} A_i) = \sum_{i=1}^{n} \mathbb{P}(A_i)$.
(c) $\mathbb{P}(E^c) = 1 - \mathbb{P}(E)$.
(d) If $E \subset F$, *then* $\mathbb{P}(E) \leq \mathbb{P}(F)$.
(e) $\mathbb{P}(E \cup F) = \mathbb{P}(E) + \mathbb{P}(F) - \mathbb{P}(E \cap F)$.

- **Example:** Union Basketball is playing Skidmore this year.
  - Home game has .5 chance of winning
  - Away game has .4 chance of winning.
  - .3 that Union wins both games.
  - What's the probability that Union loses both games?
  - **Answer.**
    - Let $\mathbb{P}(A_1) = .5$, $\mathbb{P}(A_2) = .4$ and $\mathbb{P}(A_1 \cap A_2) = .3$.

* We want to find $\mathbb{P}(A_1^c \cap A_2^c)$. Simplify as much as we can:

$$\begin{aligned}\mathbb{P}(A_1^c \cap A_2^c) &= \mathbb{P}((A_1 \cup A_2)^c) \text{ by DeMorgan's Law} \\ &= 1 - \mathbb{P}(A_1 \cup A_2), \text{ by Proposition 1c}\end{aligned}$$

* Using Proposition 1e, we have

$$\mathbb{P}(A_1 \cup A_2) = .5 + .4 - .3 = .6,$$

  Hence $\mathbb{P}(A_1^c \cap A_2^c) = 1 - .6 = .4$ as needed.
* Another way is to draw Venn Diagram and fill it in.

Section 9.3 - Computing Probabilities

- In many experiments, a probability space consists of finitely many points, all with equally likely probabilities.
  - Basic example was a tossing a coin $P(H) = P(T) = \frac{1}{2}$
  - Fair die: $P(i) = \frac{1}{6}$ for $i = 1, \ldots, 6$.
- In this case from Axiom 3 we have that if each utcome in S is equally likely, then

$$\mathbb{P}(E) = \frac{\text{number of outcomes in } E}{\text{number of outcomes in } S}.$$

DEFINITION 74. If S is a finite sample space of equally likely outcomes and $E \subseteq S$, then the **probability** of E is given by

$$\mathbb{P}(E) = \frac{N(E)}{N(S)}.$$

- **Example1:** What is the probability that if we roll 2 dice, the sum is 7?
  - **Answer:** There are 36 total outcomes , of which 6 have a sum of 7:
    - E = "sum is 7" $= \{(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)\}$. Since they are all equally likely, the probability is $\mathbb{P}(E) = \frac{6}{6\cdot 6} = \frac{1}{6}$.
- **Example 2:** If 3 balls are "randomly drawn" from a bowl containing 6 white and 5 black balls, what is the probability that one ball is white and the other two are black?
  - **Method 1:** (regard as a ordered selection)

$$\begin{aligned} P(E) &= \frac{WBB + BWB + BBW}{11 \cdot 10 \cdot 9} \\ &= \frac{6\cdot 5\cdot 4 + 5\cdot 6\cdot 4 + 5\cdot 4\cdot 6}{990} = \frac{120+120+120}{990} = \frac{4}{11}. \end{aligned}$$

  - **Method2:** (Regard as unordered set of drawn balls)

$$P(E) = \frac{(1 \text{ white})\,(2 \text{ black})}{\binom{11}{3}} = \frac{\binom{6}{1}\binom{5}{2}}{\binom{11}{3}} = \frac{4}{11}.$$

- We can always choose which way to regard our experiements.
- **Example 3** A committee of 5 is to selected from a group of 6 men and 9 women. What is probability consistsd of 3 men and 2 women
  - Answer: Easy $\frac{men\cdot women}{all} = \frac{\binom{6}{3}\binom{9}{2}}{\binom{15}{5}} = \frac{240}{1001}$.
- **Example 4:** Seven balls are randomly withdrawn from an urn that contains 12 red, 16 blue, and 18 green.
  - (b) Find probability that "**at least** 2 red balls are withdrawn;"
  - **Ans:** Let E be this event then $P(E) = 1 - P(E^c)$, $P(\text{at least 2 red}) = 1 - \mathbb{P}(\text{drawing 0 or 1 balls})$. Now

$$\mathbb{P}(\text{drawing 0 or 1 red balls}) = \frac{\binom{16+18=34}{7}}{\binom{46}{7}} + \frac{\binom{12}{1}\binom{34}{6}}{\binom{46}{7}}.$$

- **Example 5:** (Birthday Problem) In a class of 32 people, what is the probability that at least two people have the same birthdays? (We assume each day is equally likely.)
  - **Solution:** Let the first person have a birthday on some day. The probability that the second person has a different birthday will be $\frac{364}{365}$. The probability that the third person has a

different birthday from the first two people is $\frac{363}{365}$. So the answer is

$$\begin{aligned}\mathbb{P}\,(\text{at least 2 people}) &= 1-\mathbb{P}\,(\text{Everyone different birthday})\\ &= 1-\frac{365}{365}\cdot\frac{364}{365}\cdot\frac{363}{365}\cdots\frac{(365-31)}{365}\\ &= 1-1\cdot\frac{364}{365}\cdot\frac{363}{365}\cdots\frac{334}{365}\approx 0.752374.\end{aligned}$$

– Really High!!!

Section 9.4 - Independent Events and Conditional Probability

DEFINITION 75. We say E and F are **independent events** if

$$\mathbb{P}(E \cap F) = \mathbb{P}(E)\,\mathbb{P}(F).$$

- **Example1:** Suppose you flip two coins.
  - The event that you get heads on the second coin is independent of the event that you get tails on the first.
  - This is why: Let A_t be the event of getting is tails for the first coin and B_h is the event of getting heads for the second coin, and we assume we have fair coins (although this is not necessary), then

$$\begin{aligned} \mathbb{P}(A_t \cap B_h) &= \frac{1}{4}, \text{ list out all outcomes} \\ \mathbb{P}(A_t)\,\mathbb{P}(B_h) &= \frac{1}{2}\frac{1}{2} = \frac{1}{4}. \end{aligned}$$

- **Example2:** Experiment: Draw a card from an ordinary deck of cards
  - Let $A =$ draw ace, $S =$ draw a spade.
    - These are independent events since you're taking one at a time, so one doesn't effect the other. To see this using the definition we have compute
    - $\mathbb{P}(A)\,\mathbb{P}(S) = \frac{1}{13}\frac{1}{4}$.
    - White $\mathbb{P}(A \cap S) = \frac{1}{52}$ since there is only 1 Ace of spades.
- **Remark**: Independence and mutually exclusive, are two different things!
- **Remark:** This generalizes to events $A_1, \ldots, A_n$. We say events $A_1, \ldots, A_n$ are independent if for all subcollections $i_1, \ldots, i_r \in \{1, \ldots, n\}$ we have that $\mathbb{P}\left(\bigcap_{j=1}^{r} A_{i_j}\right) = \prod_{j=1}^{r} \mathbb{P}(A_{i_j})$.

Conditional Probability.

- Suppose there are
  - 200 men, of which 100 are smokers,
  - 100 women, of which 20 are smokers.
  - Question1: What is the probability that a person chosen at random will be a smoker? $\frac{120}{300}$
  - Question2: Now, let us ask, what is the probability that a person chosen at random is a smoker given that the person is a women? $\frac{20}{100}$ right?
    - Note this is

$$\frac{\#(\text{women smokers})}{\#(\text{women})} = \frac{P(\text{women and a smoker})}{P(\text{woman})}.$$

- Thus we make the following definition:

DEFINITION 76. If $\mathbb{P}(F) > 0$, we define the **conditional probability of E given F**, by

$$\mathbb{P}(E \mid F) = \frac{\mathbb{P}(E \cap F)}{\mathbb{P}(F)}.$$

Now, $\mathbb{P}(E \mid F)$ is read "the probability of E given F."

PROPOSITION. *Note that* $\mathbb{P}(E \cap F) = \mathbb{P}(E \mid F)\,\mathbb{P}(F)$.

- This is the *conditional probability* that E occurs given that F has already occured!
- **Remark:** Suppose $\mathbb{P}(E \mid F) = \mathbb{P}(E)$, i.e. knowing F doesn't help predict E. Then this implies that E and F are **independent** of each other. Rearranging $\mathbb{P}(E \mid F) = \frac{\mathbb{P}(E \cap F)}{\mathbb{P}(F)} = \mathbb{P}(E)$ we see that $\mathbb{P}(E \cap F) = \mathbb{P}(E)\mathbb{P}(F)$.
- **Example1:** Experiment: Roll two dice.
  - (a) What is the probability the sum is 8?
    - Solution: Note that $S_8 = \{(2,6), (3,5), (4,4), (5,3), (6,2)\}$ so we know $\mathbb{P}(S_8) = \frac{5}{36}$.
  - (b) What is the probability that the sum is 8 given that the first die shows a 3? (In other words, find $\mathbb{P}(\text{first dies shows a } 3 \mid \text{sum is } 8)$)
    - Solution: Let $A_3 = \{\text{first die shows three}\}$.

* Then

$$\begin{aligned}\mathbb{P}(S_8 \mid A_3) &= \mathbb{P}(\text{sum is } 8 \mid \text{1st is a } 3) \\ &= \frac{\mathbb{P}(\text{sum is } 8 \cap \text{1st is a } 3)}{\mathbb{P}(\text{1st is a } 3)} \\ &= \frac{1/36}{1/6} = \frac{1}{6}.\end{aligned}$$

  - Here we used $\mathbb{P}(\text{sum is } 8 \cap \text{1st is a } 3) = \mathbb{P}(\{(3,5)\}) = \frac{1}{36}$ is probability that the first die shows a 3 **and** the sum is 8

Section 9.5- Bayes's Formula

- Sometimes it's easier to compute a probability once we know something has or has not happened.
  - The formula in this sections has many applications, including applications to Machine learning and AI.
  - Machine Learning/AI: As you (or a computer) learns more information, the probability changes.
  - **Question:** How does an artificial intelligence makes decisions?
    - **Answer:** By computing probabilities and making decisions based off of those probabilities.
- Note that we can compute,

$$\begin{aligned}\mathbb{P}(E) &= \mathbb{P}(E \cap F) + \mathbb{P}(E \cap F^c) \\ &= \mathbb{P}(E \mid F)\mathbb{P}(F) + \mathbb{P}(E \mid F^c)\mathbb{P}(F^c) \\ &= \mathbb{P}(E \mid F)\mathbb{P}(F) + \mathbb{P}(E \mid F^c)(1 - \mathbb{P}(F)).\end{aligned}$$

- This formula is called: **The Law of Total Probability:**

$$\mathbb{P}(E) = \mathbb{P}(E \mid F)\mathbb{P}(F) + \mathbb{P}(E \mid F^c)(1 - \mathbb{P}(F))$$

- The following problem will describe the types of problems of this section.
- **Example1:** Insurance company believes
  - The probability that "an accident prone person" has an accident within a year is .4.
  - The probability that "Non-accident prone person" has an accident with year is .2.
  - 30% of the population is "accident prone".
  - **Part (a):** Find $\mathbb{P}(A_1)$ where A_1 =new policy holder will have an accident within a year?
    - Let $A = \{\text{Policy holder IS accident prone.}\}$

$$\begin{aligned}\mathbb{P}(A_1) &= \mathbb{P}(A_1 \mid A)\mathbb{P}(A) + \mathbb{P}(A_1 \mid A^c)(1 - \mathbb{P}(A)) \\ &= .4(.3) + .2(1 - .3) \\ &= .26\end{aligned}$$

  - **Part (b):** Suppose new policyholder has accident with one year. What's probability that he or she is accident prone?

$$\begin{aligned}\mathbb{P}(A \mid A_1) &= \frac{\mathbb{P}(A \cap A_1)}{\mathbb{P}(A_1)} \\ &= \frac{\mathbb{P}(A)\mathbb{P}(A_1 \mid A)}{.26} \\ &= \frac{(.3)(.4)}{.26} = \frac{6}{13}.\end{aligned}$$

- **In general:**
  - So in Part (a) we had to break a probability into two cases: If $F_1, \ldots, F_n$ are mutually exclusive events such that they make up everything $S = \bigcup_{i=1}^n F_i$ then

$$\mathbb{P}(E) = \sum_{i=1}^{n} \mathbb{P}(E \mid F_i)\mathbb{P}(F_i).$$

    - This is called **Law of Total Probability.**
  - In Part (b), we wanted to find a probability of a separate conditional event: then

$$\mathbb{P}(F_j \mid E) = \frac{\mathbb{P}(E \mid F_j)\mathbb{P}(F_j)}{\sum_{i=1}^{n} \mathbb{P}(E \mid F_i)\mathbb{P}(F_i)}.$$

    - This is known as **Baye's Formula**
    - Note that the denominator of the Bayes's formula is the Law of total probability.
- We summarize these terminologies in a definition here:

DEFINITION 77. If $F_1, \ldots, F_n$ are mutually exclusive (disjoint) events such that they make up everything, $S = \bigcup_{i=1}^{n} F_i$, then the **Law of Total Probability** says

$$\mathbb{P}(E) = \sum_{i=1}^{n} \mathbb{P}(E \mid F_i)\,\mathbb{P}(F_i).$$

Bayes's Formula says that, for any j,

$$\mathbb{P}(F_j \mid E) = \frac{\mathbb{P}(E \mid F_j)\,\mathbb{P}(F_j)}{\sum_{i=1}^{n} \mathbb{P}(E \mid F_i)\,\mathbb{P}(F_i)}.$$

- When $n = 2$, then $S = F_1 \cup F_2$, hence

$$\mathbb{P}(F_1 \mid E) = \frac{\mathbb{P}(E \mid F_1)\,\mathbb{P}(F_1)}{\mathbb{P}(E \mid F_1)\,\mathbb{P}(F_1) + \mathbb{P}(E \mid F_2)\,\mathbb{P}(F_2)},$$
$$\mathbb{P}(F_2 \mid E) = \frac{\mathbb{P}(E \mid F_2)\,\mathbb{P}(F_2)}{\mathbb{P}(E \mid F_1)\,\mathbb{P}(F_1) + \mathbb{P}(E \mid F_2)\,\mathbb{P}(F_2)},$$

- **Example2:** Suppose the test for HIV is
  - 98% accurate in both directions
  - 0.5% of the population is HIV positive.
  - Question: If someone tests positive, what is the probability they actually are HIV positive?
  - Solution: Let $T_+ = \{\text{tests positive}\}$, $T_- = \{\text{tests negative}\}$, while $+ = \{\text{actually HIV positive,}\}$ $- = \{\text{actually negative}\}$.
    - Want

$$\begin{aligned}\mathbb{P}(+ \mid T_+) &= \frac{\mathbb{P}(+ \cap T_+)}{\mathbb{P}(T_+)} \\ &= \frac{\mathbb{P}(T_+ \mid +)\,\mathbb{P}(+)}{\mathbb{P}(T_+ \mid +)\,\mathbb{P}(+) + \mathbb{P}(T_+ \mid -)\,\mathbb{P}(-)} \\ &= \frac{(.98)(.005)}{(.98)(.005) + .02(.995)} \\ &= 19.8\%.\end{aligned}$$

- **Example3:** Suppose
  - 30% of the women in a class received an A on the test
  - 25% of the men/or else received an A.
  - 60% of the class are women.
  - Question: Given that a person chosen at random received an A, what is the probability this person is a women?
    - Solution: Let A the event that a students receives an A. Let W =being a women, M =not a women. Want

$$\begin{aligned}\mathbb{P}(W \mid A) &= \frac{\mathbb{P}(A \mid W)\,\mathbb{P}(W)}{\mathbb{P}(A \mid W)\,\mathbb{P}(W) + \mathbb{P}(A \mid M)\,\mathbb{P}(M)}, \text{ by Bayes's} \\ &= \frac{.3(.6)}{.3(.6) + .25(.4)} = \frac{.18}{.28} \approx .64.\end{aligned}$$

- (General Baye's Theorem) Here's one with more than 3 possibilities:
- **Example4:** Suppose in Factory with Machines I,II,III producing Iphones
  - Machines I,II,III produce 2%,1%, and 3% defective iphones, respectively.
  - Out of total production, Machines I makes 35% of all Iphones, II-25%, III- 40%.
  - If one Iphone is selected at random from the factory,
  - Part (a): what is probability that one Iphone selected is defective?

$$\begin{aligned}\mathbb{P}(D) &= P(I)\,\mathbb{P}(D \mid I) + P(II)\,\mathbb{P}(D \mid II) + P(III)\,\mathbb{P}(D \mid III) \\ &= (.35)(.02) + (.25)(.01) + (.4)(.03) \\ &= \frac{215}{10,000}.\end{aligned}$$

- Part (b): What is the conditional prob that if an Iphone is defective, that it was produced by machine III?

$$\begin{aligned}\mathbb{P}(III \mid D) &= \frac{\mathbb{P}(III)\,\mathbb{P}(D \mid III)}{\mathbb{P}(D)} \\ &= \frac{(.4)\,(.03)}{215/10,000} = \frac{120}{215}.\end{aligned}$$

- **Example5:** In a Multiple Choice Test, students either knows the answer or randomly guesses the answer to a question.
  - Let m =number of choices in a question.
  - Let p = the probability that the students knows the answer to a question.
  - **Question:** What is the probability that the student actually knew the answer, given that the student answers correctly.
  - Solution:
  - Let $K = \{\text{Knows the answer}\}$ and $C = \{\text{Answer's correctly}\}$. Then

$$\begin{aligned}\mathbb{P}(K \mid C) &= \frac{\mathbb{P}(C \mid K)\,\mathbb{P}(K)}{\mathbb{P}(C \mid K)\,\mathbb{P}(K) + \mathbb{P}(C \mid K^c)\,\mathbb{P}(K^c)} \\ &= \frac{1 \cdot p}{1 \cdot p + \frac{1}{m}(1-p)} = \frac{mp}{1 + (m-1)p}.\end{aligned}$$