Math 300–03

Wolmer V. Vasconcelos

Set 2

Fall 2008

Outline

Defining Sets

A **set** is a specified collection of objects. The objects of a given set are called its **elements** (or members).

Notation: $x \in A$

Description: $\{x : P(x)\}$
where $P(x)$ is an open sentence description of the property that defines the set.

Major Examples

- **Class** The students in this class.
- **Natural numbers** $\mathbb{N} = \{1, 2, 3, \ldots, \}$
- **Integers** $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots, \}$
- **Rational numbers** $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$
- **Real numbers** $\mathbb{R}$
- $(a, b) = \{x : x \in \mathbb{R} \text{ and } a < x < b\}$ **open interval from a to b**
- $[a, b] = \{x : x \in \mathbb{R} \text{ and } a \leq x \leq b\}$ **closed interval from a to b**
- $[0, \infty) = \{x : x \in \mathbb{R} \quad x \geq 0\}$

The Empty Set

Definition

Let $\emptyset = \{x : x \neq x\}$. Then $\emptyset$ is a set with no elements and it is called the empty set.

Subsets

Definition

Let A and B be sets. We say that A is a subset of B iff every element of A is an element of B. Written:

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B).$$

DIRECT PROOF OF $A \subseteq B$
Let x be any object.
Suppose $x \in A$.
$\vdots$
Thus $x \in B$.
Therefore $A \subseteq B$.

Exercises

Theorem

For any set A,

1. $\emptyset \subseteq A$.
2. $A \subseteq A$.

Proof.

1. Let A be any set. Let x be any object. We must show $x \in \emptyset \Rightarrow x \in A$. Since the antecedent is false, then sentence $x \in \emptyset \Rightarrow x \in A$ is true. Thus $\emptyset \subseteq A$.
2. Let A be any set. Let x be any object. We must show $x \in A \Rightarrow x \in A$. Here we use the **tautology** $P \Rightarrow P$. Therefore $(\forall x)(x \in A \Rightarrow x \in A)$, and so $A \subseteq A$.

Theorem

If A and B are subsets with no elements, then $A = B$.

Proof. Since A has no elements, the sentence $(\forall x)(x \in A \Rightarrow x \in B)$ is true. Therefore, $A \subseteq B$. Similarly, $(\forall x)(x \in B \Rightarrow x \in A)$ is true. Thus, $B \subseteq A$. By definition of equality of sets, $A = B$. □

Power Set

Definition

Let A be a set. The **power set** of A is the set $\mathcal{P}(A)$ whose elements are the subsets of A is denoted $\mathcal{P}(A)$. Thus

$$\mathcal{P}(A) = \{B : B \subseteq A\}.$$

Example: $A = \{a, b, c\}$

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}.$$

Achtung: The power set of $\emptyset$ is not empty:

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

- How big is the power set of the set **Class**?
-

Theorem

If A is a set with n elements, then $\mathcal{P}(A)$ has 2^n elements.

Proof. If A is the empty set, that is A has 0 elements, then $\mathcal{P}(\emptyset) = \{\emptyset\}$, which has 1 element: $1 = 2^0$.

Suppose A has n elements, $n \geq 1$. List the elements of A

$$x_1, x_2, x_3, \ldots, x_n.$$

A subset B of A is formed by going through the list and selecting/or not selecting each element to place in B. Thus, to form $\emptyset$ pick none, to form A pick all. This gives rise to

$$2 \cdot 2 \cdot 2 \cdots 2 = 2^n$$

possibilities. Thus the number of subsets of A of $\mathcal{P}(A)$ is 2^n.

Element-chasing proof

Theorem

Let A and B be sets. Then $A \subseteq B$ iff $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof. We first prove that $A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

1. Suppose $X \subseteq A$.
2. Since $A \subseteq B$, we have $X \subseteq B$.
3. Thus $X \in \mathcal{P}(B)$.

We must prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B) \Rightarrow A \subseteq B$.

1. Assume that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
2. We have that $A \subseteq A$. Therefore $A \in \mathcal{P}(A)$.
3. Thus $A \in \mathcal{P}(B)$. Therefore $A \subseteq B$.

Example

Suppose that

$$\begin{aligned} X &= \{x : x \in \mathbb{R} \quad x \text{ is a solution of } x^2 - 7x + 12 = 0\} \\ Y &= \{3, 4\} \end{aligned}$$

Prove that $X = Y$

1. For $x = 3$ or $x = 4$, we verify that $x^2 - 7x + 12 = 0$, therefore $Y \subseteq X$.
2. To prove $X \subseteq Y$, we must determine more explicitly the elements of X by solving the quadratic

$$\frac{7 \pm \sqrt{49 - 48}}{2} = \frac{7 \pm 1}{2} = \{3, 4\}$$

Almost same Example

Suppose that

$$X = \{x : x \in \mathbb{R} \quad x \text{ is a solution of } x^3 - 6x^2 + 11x - 6 = 0\}$$
$$Y = \{1, 2, 3\}$$

How do we prove that $X = Y$?

Russell paradox

A set B is called **ordinary** if $B \notin B$. Otherwise the set B is called **extraordinary**. Example: The set of all abstract ideas.

Let $X = \{x : x \quad \text{is an ordinary set}\}$. What is X, an ordinary or an extraordinary set?

What does this teach us? That you cannot go around campus defining all manners of sets!

Outline

Binary Operations on Sets

Forming sets from other sets. Basic:

Definition

Let A and B be sets.

- The **union of** A **and** B is the set $A \cup B = \{x : x \in A \quad \text{or } x \in B\}$.
- The **intersection of** A **and** B is the set $A \cap B = \{x : x \in A \quad \text{and } x \in B\}$.
- The **difference of** A **and** B is the set $A \setminus B = \{x : x \in A \quad \text{and } x \notin B\}$.

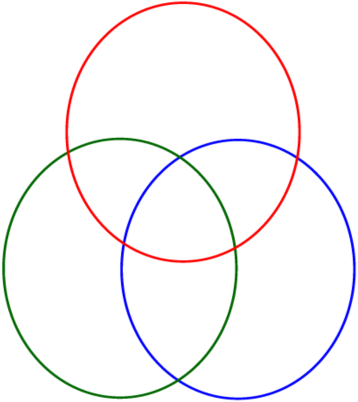
Definition

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

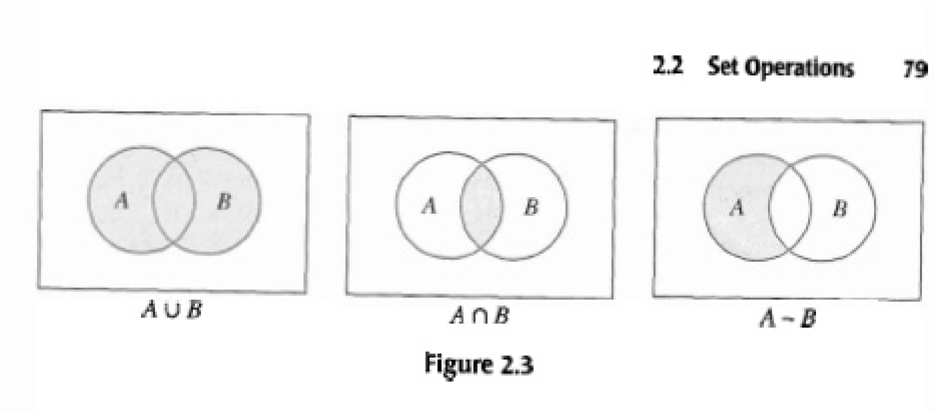
Definition

If U is the universe and $B \subseteq U$, then we define the **complement** of B to be the set $\widetilde{B} = U \setminus B$.

Venn Diagrams



Venn Diagram of Set Operations



A proof by volunteers

Theorem

Let A, B and C be three sets. Then

1. $$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$
2. $$(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

This says that $\cup$ distributes over $\cap$ and that $\cap$ distributes over $\cup$.

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

We will show that the LHS (left hand side) is contained in the RHS, and conversely.

1. Let $x \in (A \cup B) \cap C$
2. Then $x \in (A \cup B) \wedge x \in C$
3. Therefore $(x \in A) \wedge (x \in C)$ OR $(x \in B) \wedge (x \in C)$
4. Then $x \in ((A \cap C) \cup (B \cap C))$, which proves the forward containemnt
5. To prove the reverse containemnt, we read the list of equivalences backwards.

De Morgan's Laws

Theorem

Let U be the universe, and let A and B be subsets of U. Then

1. $\widetilde{A \cup B} = \widetilde{A} \cap \widetilde{B}$.
2. $\widetilde{A \cap B} = \widetilde{A} \cup \widetilde{B}$.

Proof. of (1):

1. The object x is a member of $\widetilde{A \cup B}$
2. iff x is not a member of $A \cup B$
3. iff it is not the case that $x \in A$ or $x \in B$
4. iff $x \notin A$ and $x \notin B$
5. iff $x \in \widetilde{A}$ and $x \in \widetilde{B}$
6. iff $x \in \widetilde{A} \cap \widetilde{B}$

Symmetric difference

Definition

Let A and B be sets. The **symmetric difference** of A and B is the set

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Exercise: Let A, B and C be sets of the universe U. Show that

1. $B \Delta C = (B \cup C) \setminus (B \cap C)$.
2. $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.

Outline

Set of Sets

Definition

A **set of sets** is usually called a family or collection of sets. Let $\mathcal{A}$ be a family of sets of some universe.

1. The **union over** $\mathcal{A}$ is

$$\bigcup_{A\in\mathcal{A}} A = \{x : x \in A \quad \text{for some set } A \in \mathcal{A}\}.$$

2. The **intersection over** $\mathcal{A}$ is

$$\bigcap_{A\in\mathcal{A}} A = \{x : x \in A \quad \text{for every set } A \in \mathcal{A}\}.$$

Definition

Let Δ be a nonempty set such that for every $\alpha \in \Delta$ there is a corresponding set A_α. The family $\{A_\alpha : \alpha \in \Delta\}$ is an **indexed family of sets.** The set Δ is the **indexing set** and each $\alpha \in \Delta$ is an **index.**

Theorem

Let $\mathcal{A} = \{A_\alpha : \alpha \in \Delta\}$ be an indexed collection of sets. Then

1. $$\widetilde{\bigcap_{\alpha\in\Delta} A_\alpha} = \bigcup_{\alpha\in\Delta} \widetilde{A_\alpha}.$$

2. $$\widetilde{\bigcup_{\alpha\in\Delta} A_\alpha} = \bigcap_{\alpha\in\Delta} \widetilde{A_\alpha}.$$

Definition

An indexed family $\mathcal{A} = \{A_\alpha : \alpha \in \Delta\}$ is **pairwise disjoint** iff for all α and β in Δ, if $A_\alpha \neq A_\beta$, then $A_\alpha \cap A_\beta = \emptyset$.

Outline

Homework #3

1. 1.5: 3(d), 6(d), 7(b), 11
2. 1.6: 1(e), 2(d), 5(a), 7(e,f), 8(g)

Outline

Peano and Mathematical Induction

http://upload.wikimedia.org/wikipedia/commons/3/3a/Giuseppe_Peano.jpg

Induction

The set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of **natural numbers** arises logically from the following construction of Peano.

$\mathbb{Z}$ and Peano's Axioms

- $\mathbb{N}$ contains a particular element 1.
- *Successor function:* There is an injective [one-one] function $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$, for each $n \in \mathbb{N}$, $\sigma(n) \neq 1$. [Another notation: $\sigma(n) = n'$]
- *Induction axiom:* Suppose that $S \subset \mathbb{N}$ satisfies
  1. $1 \in S$;
  2. if $n \in S$ then $\sigma(n) \in S$. Then $S = \mathbb{N}$.

The second axiom means 3 things [there are 5 axioms in all]: (1) every natural number has a successor; (2) no two natural numbers have the same successor; (3) 1 is not the successor of any natural number.

Defining Operations $+$ and $\times$

Operations

• *Addition:*

$$m + 1 = m', \quad m + n' = (m + n)'$$

• *Multiplication:*

$$m \cdot 1 = m, \quad m \cdot n' = m \cdot n + m$$

With these operations, $\mathbb{N}$ satisfies:

- Associativity properties: For all x, y and z in $\mathbb{N}$,

$$\begin{aligned} x + (y + z) &= (x + y) + z. \\ x(yz) &= (xy)z. \end{aligned}$$

- Commutativity properties: For all x and y in $\mathbb{N}$,

$$\begin{aligned} x + y &= y + x. \\ xy &= yx. \end{aligned}$$

- Distributivity properties: For all x, y and z in $\mathbb{N}$,

$$\begin{aligned} x(y + z) &= xy + xz. \\ (y + z)x &= yx + zx. \end{aligned}$$

- Order properties: For all x, y and z in $\mathbb{N}$, $x < y$ if there is $w \in \mathbb{N}$ such that $x + w = y$. Several properties arise: e.g. If $x < y$ then $\forall z \in \mathbb{N}\ x + z < y + z$.

$\mathbb{N}$ can extended by 0 and 'negatives': $\mathbb{Z}$. Operations also. Then all the ordinary properties of addition and multiplication are verified:

Let us illustrate with:

Proof of the associative law of addition for $\mathbb{N}$:

$$(a+b)+n = a+(b+n) \quad \forall a, b, n \in \mathbb{N}$$

From the definitions check $n = 1$:

$$(a+b)+1 = (a+b)' = a+b' = a+(b+1)$$

Assume axiom holds for n and let us check for n' (*induction hypothesis*):

$$\begin{aligned}
(a+b)+n' &= (a+b)+(n+1) \text{ (definition)} \\
&= ((a+b)+n)+1 \text{ (case } n=1\text{)} \\
&= (a+(b+n))+1 \text{ (ind. hypothesis)} \\
&= a+((b+n)+1) \text{ (case } n=1\text{)} \\
&= a+(b+(n+1)) \text{ (case } n=1\text{)} \\
&= a+(b+n') \text{ (definition)}
\end{aligned}$$

Principle of Mathematical Induction

Let us state Peano's 5th Axiom again:

Definition (PMI)

If S is a subset of $\mathbb{N}$ and

1. $1 \in S$,
2. for all $n \in \mathbb{N}$, if $n \in S$, then $n + 1 \in S$,

then $S = \mathbb{N}$.

A set with Property (2) is called an **inductive set.** Examples, besides $\mathbb{N}$ are $\emptyset$, $S = \{x : x \in \mathbb{N}, x \geq 10\}$.$\mathbb{N}$ is the only inductive set containing 1: This is **PMI.**

The **PMI** is used to define mathematical objects and in proofs galore.

We are discussing the Principle of Mathematical Induction (**PMI** for short). It is a mechanism to study (i.e. prove) certain open sentences $P(n)$ that depend on $n \in \mathbb{N}$ when we seek to verify that it is true for all values.

The method is rooted in the following property of the natural numbers $\mathbb{N}$:

If S is a subset of $\mathbb{N}$ and

1. $1 \in S$,
2. for all $n \in \mathbb{N}$, if $n \in S$, then $n + 1 \in S$,

then $S = \mathbb{N}$.

Verifying $P(n)$

To verify whether $S = \{n : P(n)\}$ is equal to $\mathbb{N}$, we follow the template:

1. (Base step) $P(1)$ is true;
2. (Inductive step) If for some n, $P(n)$ is true then $P(n+1)$ is also true.

PMI guarantees that $S = \mathbb{N}$.

Example

Exercise: Prove using the PMI that for each $n \in \mathbb{N}$, the sum of the first n odd numbers satisfies

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

1. Let S be he set of all natural numbers for which this statement is true.
2. $1 \in S$, as $= 1^2$.
3. Let $n \in S$, that is $1 + 3 + 5 + \cdots + (2n - 1) = n^2$. We are going to show that $n + 1 \in S$.
4. The sum of the first $n + 1$ odd numbers,

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) &= n^2 + 2n + 1 \\ &= (n + 1)^2. \end{aligned}$$

   This shows that if $n \in S$, then $n + 1 \in S$.
5. By the PMI, $S = \mathbb{N}$. That is, for every natural number n, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Example

Exercise: Prove using the PMI that for each $n \in \mathbb{N}$, the sum of the first n natural numbers satisfies

$$1 + 2 + 3 + \cdots + n = n(n+1)/2.$$

1. Let S be the set of all natural numbers for which this statement is true.
2. $1 \in S$, as $= (1)(2)/2$.
3. Let $n \in S$, that is $1 + 2 + 3 + \cdots + n = n(n+1)/2$. We are going to show that $n + 1 \in S$.
4. The sum of the first $n + 1$ natural numbers,

$$\begin{aligned} 1 + 2 + 3 + \cdots + n + (n+1) &= n(n+1)/2 + (n+1) \\ &= (n+1)(n/2+1) \\ &= (n+1)((n+2)/2)) \\ &= (n+1)(n+2)/2. \end{aligned}$$

   This shows that if $n \in S$, then $n + 1 \in S$.
5. By the PMI, $S = \mathbb{N}$. That is, for every natural number n,

Proof Templates

Proof using the PMI

Let $S = \{n \in \mathbb{N} : \text{the statement is true for } n\}$

(i) Show that $1 \in S$.

(ii) Show that S is inductive (that is, for all n, if $n \in S$ then $n + 1 \in S$).

(iii) By the PMI, $S = \mathbb{N}$.

Proof of $(\forall n \in \mathbb{N})P(n)$ by induction
(i) (Base Step) Show that $P(1)$ is true.
(ii) (Induction Step) Show $P(n) \Rightarrow P(n+1)$: Suppose that $P(n)$ is true fo
and show that $P(n+1)$ is true.
(iii) (Conclusion) By the PMI, $S = \mathbb{N}$.

The assertion "Suppose that $P(n)$ is true for some $n \in \mathbb{N}$" is called the **induction hypothesis.**

Old Theorem...New Proof

Theorem

If A is a set with n elements, then $\mathcal{P}(A)$ has 2^n elements.

Proof. Let us prove the theorem using the **PMI**.

- (Base case) The assertion is true if A is empty or $A = \{x_1\}$.
- (Induction hypothesis) Suppose the number of elements of A is $\overline{\overline{\mathcal{P}(A)}} = 2^n$ if A is a set of n elements.
- Assume that A now has $n+1$ elements, $A = \{x_1, x_2, \ldots, x_n, x_{n+1}\}$.
  Think of x_{n+1} in a different color.
  The subsets of A are of two kinds: Those that do not contain x_{n+1} and those that do.

- Therefore

$$\mathcal{P}(A) = \mathcal{P}(\{x_1, \ldots, x_n\}) \bigcup \{(\{x_{n+1}\} \cup X : X \subseteq \{x_1, \ldots, x_n\})\}$$

- These two sets are disjoint and their number of elements is 2^n.
- Therefore $\overline{\overline{\mathcal{P}(A)}} = 2^n + 2^n = 2^{n+1}$.

Example

Proposition

For all natural numbers $n^3/3 + n^5/5 + 7n/15$ *is an integer.*

Proof.

- (Base case) $1 \in S$: $1/3 + 1/5 + 7/15 = (5 + 3 + 7)/15 = 1 \in \mathbb{N}$.
- (Induction step) Suppose $n^3/3 + n^5/5 + 7n/15$ is an integer.Consider

$$\frac{(n+1)^3}{3} + \frac{(n+1)^5}{5} + \frac{7(n+1)}{15}$$

- We have the following expansions from the Binomial Theorem

$$\begin{aligned}
\frac{(n+1)^3}{3} &= \frac{n^3+3n^2+3n+1}{3} \\
&= \frac{n^3}{3} + \frac{1}{3} + (n^2+n) \\
\frac{(n+1)^5}{5} &= \frac{n^5+5n^4+10n^3+10n^2+5n+1}{5} \\
&= \frac{n^5}{5} + \frac{1}{5} + (n^4+2n^3+2n^2+n) \\
\frac{7(n+1)}{15} &= \frac{7n}{15} + \frac{1}{15}
\end{aligned}$$

Adding we observe: The sum of the red terms is the induction hypothesis, the sum of the blue terms is the base case, the green terms are integers. Thus the sum is an integer. □

Example useful in Calculus

Theorem

Suppose $a \geq -1$. Then for all $n \in \mathbb{N}$, $(1+a)^n \geq 1 + na$.

Proof.

We shall prove the statement by **induction**:

- **(base case):** If $n = 1$, $(1+a)^1 = 1 + a \geq 1 + a$ is true
- **(induction step)**: Suppose $(1+a)^n \geq 1 + na$. Then, since $1 + a \geq 0$ by hypothesis,

$$\begin{aligned} (1+a)^{n+1} &= (1+a)^n(1+a) \geq (1+na)(1+a) \\ &= 1 + na + a + na^2 = 1 + (n+1)a + na^2 \\ &\geq 1 + (n+1)a \end{aligned}$$

□

Example in Algebra

Theorem

The polynomial $x - y$ divides the polynomial $x^n - y^n$ for every natural number n.

Proof.

1. (Base case) $x - y$ divides $x^1 - y^1$: $x^1 - y^1 = 1(x - y)$
2. (Induction hyphothesis) Suppose $x - y$ divides $x^n - y^n$. We must show that $x - y$ divides $x^{n+1} - y^{n+1}$:

$$\begin{aligned} x^{n+1} - y^{n+1} &= xx^n - yy^n = xx^n - yx^n + yx^n - yy^n \\ &= (x - y)x^n + y(x^n - y^n) \end{aligned}$$

3. Thus $x - y$ divides each term of the sum so divides the sum itself.
4. By the **PMI**, $x - y$ divides $x^n - y^n$ for every natural number n.

Revisiting Old Example

Suppose that

$$\begin{aligned} X &= \{x : x \in \mathbb{R} \quad x \text{ is a solution of } x^3 - 6x^2 + 11x - 6 = 0\} \\ Y &= \{1, 2, 3\} \end{aligned}$$

How do we prove that $Y = X$? We use the previous theorem. For $x = 1$, $x = 2$ or $x = 3$, we verify they are roots of the equation:

$$\begin{aligned} x^3 - 6x^2 + 11x - 12 &= \\ (x^3 - 6x^2 + 11x - 12) - (1^3 - 6(1)^2 + 11(1) - 6) &= \\ (x^3 - 1^3) - 6(x^2 - 1^2) + 11(x - 1) + 6(1 - 1) &= \\ (x - 1)(x^2 - x + 1) - 6(x - 1)(x + 1) + 12(x - 1) &= \\ (x - 1)(x^2 + x + 1 - 6x - 6 + 12) & \\ (x - 1)(x^2 - 5x + 6) & \end{aligned}$$

Exercise

Let $\mathbf{f}(x)$ be a polynomial of degree n with real coefficients,

$$\mathbf{f}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_n.$$

Consider the following sets of real numbers

$$\begin{aligned} X &= \{x : x \in \mathbb{R} \quad x \text{ is a solution of } \mathbf{f}(x) = 0\} \\ Y &= \{x_1, x_2, \ldots, x_n\} \end{aligned}$$

where the x_i are distinct roots of $\mathbf{f}(x)$. Prove the following:

Theorem

$X = Y.$

Division Algorithm for Polynomials

The proof above uses the Long Division Algorithm:

Theorem

If $\mathbf{f}(x)$ *and* $\mathbf{h}(x)$ *are polynomials with real coefficients, then there are two polynomials* $q(x)$ *and* $r(x)$ *such that*

$$\mathbf{f}(x) = q(x)\mathbf{h}(x) + r(x),$$

where $r(x)$ *is either* 0 *or degree* $\mathbf{h}(x) >$ *degree* $r(x)$. $q(x)$ *is called a quotient of* $\mathbf{f}(x)$ *by* $q(x)$ *and* $r(x)$ *is the remainder of the division.*

Corollary

If $\mathbf{h}(x) = x - a$, *then* $r(x) = 0$ *or* $r(x) = \mathbf{f}(a)$.

Proof: In the formula $\mathbf{f}(x) = q(x)(x - a) + r(x)$, $r(x)$ is a polynomial of degree 0, or a constant, say r. To evaluate it, we set $x = a$:
$\mathbf{f}(a) = q(a)(a - a) + r = r$.

Corollary

If $\mathbf{f}(x)$ *is a polynomial of degree* n *and* $x = a$ *is a root, then*

$$\mathbf{f}(x) = q(x)(x - a),$$

where $q(x)$ *is a polynomial of degree* $n - 1$*.*

If $x = b$ is another, but different root of $\mathbf{f}(x)$, then

$$0 = \mathbf{f}(b) = q(b)(b - a),$$

and thus b is a root of $q(x)$. This means that $q(x) = p(x)(x - b)$.
In this manner, we see that if $x_1, \ldots, x_n$ are distinct roots of $\mathbf{f}(x)$, then

$$\mathbf{f}(x) = C(x - x_1)(x - x_2) \cdots (x - x_n),$$

where C is a constant. This implies that the x_i are the only roots of $\mathbf{f}(x)$.

Archimedean Principle

Theorem (Archimedean Principle)

For all natural numbers a and b, there exists a natural number s such that $a < sb$.

Proof.

Let $a, b \in \mathbb{N}$. The proof proceeds by induction on b.

1. (Base Step) If $b = 1$, choose s to be $a + 1$. Then $a < a + 1 = sb$.
2. (Induction Step) Suppose the statement is true for $b = n$. Choosing the same s we have $a < sn < s(n + 1)$.
3. (Conclusion) By the PMI the statement is true for all natural numbers.

□

Of course, a direct proof is simpler: Just take $s = a + 1$. There is a version of the Archimedean Principle where a and b are positive real numbers and s is a natural number. Try!

Generalized PMI

Definition

Let k be a natural number. If S is a subset of $\mathbb{N}$ and

1. $k \in S$,
2. for all $n \in \mathbb{N}$ with $n \geq k$, if $n \in S$, then $n + 1 \in S$,

then S contains all natural numbers greater or equal to k.

Example

Proposition

For $n \geq 5$, $(n+1)! > 2^{n+3}$.

Proof. We are going to use the Generalized PMI. Let S be the set of natural numbers for which $(n+1)! > 2^{n+3}$. We must show that S is an inductive subset of $\mathbb{N}$.

1. (Base case) $5 \in S$: $(5+1)! = 6! = 620 > 256 = 2^{5+3}$.
2. (Inductive step) Let $n \in S$.

$$\begin{aligned} (n+2)! &= (n+1)! \cdot (n+2) \\ &> 2^{n+3} \cdot (n+2) > 2^{n+3} \cdot 2 \\ &= 2^{(n+1)+3} \end{aligned}$$

By the Generalized PMI, $S = \{n : n \in \mathbb{N}, n \geq 5\}$.

Exercise

Exercise: Consider any map formed by drawing straight lines in a plane to represent boundaries. Color the countries so that countries with a common border have different colors.

Task: Argue that 2 colors suffice.

Solution: Will argue by induction of the number n of lines.

Base case: Clear.

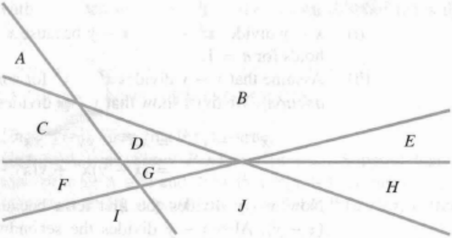


Figure 2.9

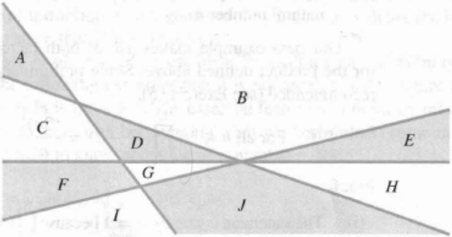


Figure 2.10

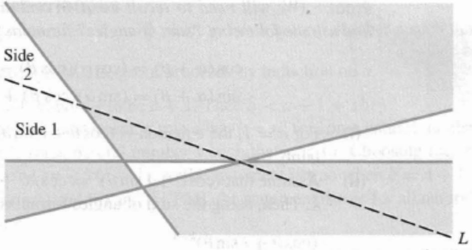


Figure 2.11

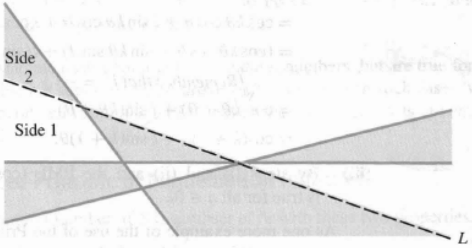


Figure 2.12

Exercise

Exercise: Show that for all nonnegative integers n, $10^n + 3 \cdot 4^{n+2} + 5$ is divisible by 9.

Let S be the set of nonnegative integers for which the statement is true.

1. (Base case) $0 \in S$: $10^0 + (3)4^2 + 5 = 1 + 48 + 5 = 56$, which is divisible by 9.
2. (Induction case) Suppose $n \in S$. Consider

$$\begin{aligned} 10^{n+1} + 3 \cdot 4^{n+1+2} + 5 &= 10 \cdot 10^n + 4 \cdot 3 \cdot 4^{n+2} + 5 \\ &= (9+1)10^n + (3+1)3 \cdot 4^{n+2} + 5 \\ &= (10^n + 3 \cdot 4^{n+2} + 5) + 9(10^n + 4^{n+2}), \end{aligned}$$

   which is divisible by 9.
3. By the Generalized PMI, $S = \{0, 1, 2, \cdots\}$, and the statement is true for all $n \geq 0$.

Exercise

Let $P_1, P_2, \ldots, P_n$ be n points in a plane with no three points collinear. Show that the number of line segments joining all pairs of points is $\frac{n^2-n}{2}$.

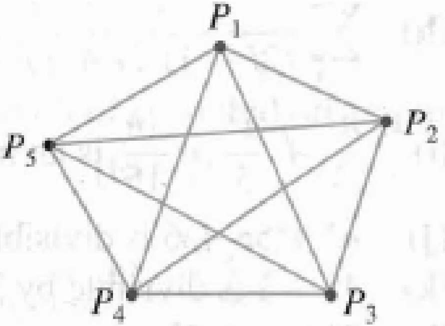


Figure 2.13

We shall use the **PMI**: Call S the set of all natural numbers for which the statement is true.

1. (Base case) $1 \in S$: For a single point there are no line segments: $0 = (1^1 - 1)/2$.
2. (Induction step) Let $n \in \mathbb{N}$ be in S. For n no collinear points $P_1, \ldots, P_n$ the number of line segments is $(n^2 - n)/2$.
3. Adding another point, P_{n+1}, not collinear with any of the P_i, $i \leq n$, we add n new linear segments by joining P_{n+1} to each of the P_i, $i \leq n$.
4. The total number of line segments is then

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

5. Thus $n + 1 \in S$, and by PMI $S = \mathbb{N}$.

Therefore the statement is true for all $n \in \mathbb{N}$.

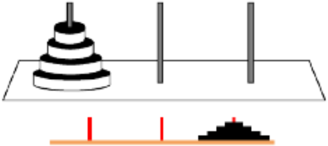
Towers of Hanoi

Exercise: The Towers of Hanoi puzzle consists of a board with 3 pegs and several disks of different diameters that fit over the pegs. In the start position, all disks are placed on one peg in order of their sizes [with the largest at the bottom]. A move is made by removing one disk off a peg and placing it on another peg so that there is no smaller disk under it. The object of the puzzle is to transfer all the disks from one peg to another. Use the PMI to show that with a board with n disks, this can be done in $2^n - 1$ moves.

Towers of Hanoi

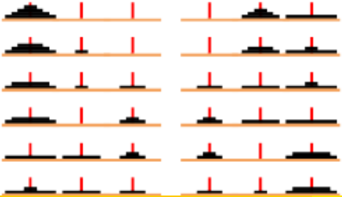
Tower of Hanoi

DOWNLOAD Mathematica Notebook



The tower of Hanoi (commonly also known as the "towers of Hanoi"), is a puzzle invented by E. Lucas in 1883. Given a stack of n disks arranged from largest on the bottom to smallest on top placed on a rod, together with two empty rods, the towers of Hanoi puzzle asks for the minimum number of moves required to move the stack from one rod to another, where moves are allowed only if they place smaller disks on top of larger disks. The puzzle with $n = 4$ pegs and n disks is sometimes known as Reve's puzzle.

The problem is isomorphic to finding a Hamiltonian path on an n-hypercube (Gardner 1957, 1959).



Solution

Call the pegs A, B and C and suppose that initially the n disks are in peg A and we want to move them to peg B.

1. (Base case) If $n = 1$, the statement is true: $1 = 2^1 - 1$
2. (Induction step) While keeping the largest disk in peg A, move the $n - 1$ other disks to peg C. This can be done in $2^{n-1} - 1$ moves.
3. Move the largest disk to peg B. Then move the $n - 1$ disks in peg C to B.
4. Total number of moves

$$(2^{n-1} - 1) + 1 + (2^{n-1} - 1) \quad = \quad 2^n - 2 + 1 = 2^n - 1.$$

By the PMI, the statement is true for all natural numbers.

Outline

Homework #4

1. Let A, B and C be sets of the universe U. Prove that
   1. $B \Delta C = (B \cup C) \setminus (B \cap C)$.
   2. $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
2. Use the **PMI** to prove that for all $n \in \mathbb{N}$,
$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$
3. 2.4: 15(d).
4. 2.5: 4, 6(b), 15(a)

Outline

Principle of Complete Induction

Definition (PCI)

Suppose S is a subset of $\mathbb{N}$ with the property:
For all natural numbers n, if $\{1, 2, 3, \ldots, n-1\} \subseteq S$, then $n \in S$. Then $S = \mathbb{N}$.

Theorem

The Principle of Complete Induction is equivalent to the Principle of Mathematical Induction.

$$\text{PCI} \Leftrightarrow \text{PMI}.$$

Why the PCI is needed?

Fibonacci Sequences

$$1, 1, 2, 3, 5, 8, 13, \dots$$

$$f_1 = 1, f_2 = 1, \quad \text{and} \quad f_{n+2} = f_n + f_{n+1}, \quad n \geq 1.$$

Variations: $f_1 = 2$, $f_2 = 3$, $f_3 = 2$. For $n \geq 4$,

$$f_{n+3} = f_n + 2f_{n+1} + 4f_{n+2}$$

Exercise

Example: Let α be the positive of $x^2 = x + 1$. Prove that $f_n \leq \alpha^{n-1}$ for all $n \geq 1$.

$$x^2 - x - 1 = 0 \quad \Rightarrow \quad \alpha = \frac{1 \pm \sqrt{5}}{2}$$

1. Let m be a natural number and assume that for all $k \in \{1, 2, \ldots, m-1\}$, $f_m \leq \alpha^{m-1}$.
2. If $m = 1$, $f_1 = 1 \leq \alpha^0 = 1$, $f_2 = 1 \leq \alpha^1 = (1 + \sqrt{5})/2$.
3. For $m \geq 3$,

$$\begin{aligned} f_m &= f_{m-1} + f_{m-2} \\ &\leq \alpha^{m-2} + \alpha^{m-3} \quad \text{ind. hyp. for} \quad m-1, m-2 \in \{1, 2, \ldots, m-1 \\ &= \alpha^{m-3}(\alpha + 1) \\ &= \alpha^{m-3}\alpha^2 = \alpha^{m-1} \end{aligned}$$

Therefore $f_m \leq \alpha^{m-1}$. By the PCI, $f_n \leq \alpha^{n-1}$ for all $n \geq 1$.

Proof of PMI $\Rightarrow$ PCI

Assume that the PMI holds for $\mathbb{N}$. Suppose S is a subset of $\mathbb{N}$ with the following property: For all natural numbers m, if $\{1, 2, 3, \ldots, m-1\} \subseteq S$, then $m \in S$.
We are going to show that for every natural number n, $\{1, 2, 3, \ldots, n\} \subseteq S$.

1. For $n = 1$, the set $\{1, 2, 3, \ldots, n-1\}$ is the empty set. But $\emptyset \subseteq S$, so by the property of S, $1 \in S$. Thus $\{1\} \subseteq S$.
2. Assume that $\{1, 2, 3, \ldots, n\} \subseteq S$. We must show that $\{1, 2, 3, \ldots, n+1\} \subseteq S$. But this follows from the defining property of S.
3. By (1) and (2), and PMI, $\{1, 2, 3, \ldots, n\} \subseteq S$ for every natural number n. Now let n be a natural number. Since $\{1, 2, 3, \ldots, n\} \subseteq S$, $n \in S$. Since S is a subset of $\mathbb{N}$, we conclude $S = \mathbb{N}$.

Exercise: Fibonacci

Prove the following properties of Fibonacci numbers:

1. $f_{n+6} = 4f_{n+3} + f_n$ for all natural numbers n.
2. For any natural number a, $f_a f_n + f_{a+1} f_{n+1} = f_{a+n+1}$ for all natural numbers n.
3. **[Binet]** If α and β are the positive and negative roots of $x^2 = x + 1$, respectively, then for all natural numbers n

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Well-Ordering Principle

Definition (WOP)

Every nonempty subset of $\mathbb{N}$ has a smallest element.

Theorem

The Well-Ordering Principle is equivalent to the Principle of Mathematical Induction.

$$\text{WOP} \Leftrightarrow \text{PMI}.$$

Since we already know that PMI is equivalent to PCI, we will have

$$\text{WOP} \Leftrightarrow \text{PMI} \Leftrightarrow \text{PCI}$$

Proof that PMI $\Rightarrow$ WOP

Proof. Part 1: Assume that PMI holds for $\mathbb{N}$. To show WOP we show that every nonempty subset T of $\mathbb{N}$ has a minimal element.
Let $S = \mathbb{N} \setminus T$. Since $T \neq \emptyset$, $S \neq \mathbb{N}$. Suppose that T has no smallest element.

1. Since 1 is the smallest element of $\mathbb{N}$ and T has no smallest element, $1 \notin T$.
2. Suppose $n \in S$. No number less than n belongs to T, because if any of the numbers $1, 2, 3, \ldots, n-1$ were in T, then one of these numbers would be the smallest element of T. We know $n \notin T$ because $n \in S$. Therefore $n+1$ cannot be in T, or else it would be the smallest element of T. Thus $n+1 \in S$.
3. By (1), (2) and the PMI, $S = \mathbb{N}$, which is a contradiction since $T \neq \emptyset$. Thus T has a smallest element.

Outline

Last Class...

We studied 3 organizing principles that occur in many proofs:

- PMI: Principle of Mathematical Induction
- PCI: Principle of Complete Induction
- WOP: Well-Ordering Principle

They are all equivalent.
Let us give a refresh of their usage:

Prime Factorization

Proposition

Every natural number $n > 1$ has a prime factor.

Proof.

If n is prime, then n is a prime factor of n. If n is composite, hen it has factors other than 1 and n. Let p be the smallest of these factors. Guaranteed by WOP. We must show that p is prime.
If p is composite, then p has a factor d, $1 < d < p$. Since $n = pm$, $p = qd$, $n = d(mq)$, so d would be a factor of n smaller than p. This contradiction shows that p is prime. □

Theorem

Every natural number $n > 1$ has a factorization

$$n = p_1 \cdot p_2 \cdots p_m,$$

where the p_i are prime.

Proof. We will argue by contradiction. Suppose the set T of natural numbers $n > 1$ without such factorizations is nonempty. By WOP, let a be the smallest element of T.

- a cannot be prime because it then have the stated representation.
- Let $a = bc$ be a decomposition of a as a product of natural numbers $a > 1$, $b > 1$. Since $a > b$, $a > c$, neither b nor c belong to T.

- Thus both a and b have factorizations

$$\begin{aligned} a &= p_1 \cdot p_2 \cdots p_s \\ b &= p_{s+1} \cdot p_{s+2} \cdots p_m \end{aligned}$$

  where the p_i are prime.
- Multiplying the factorizations of a and b gives a factorization for n. The contradiction proves the statement.

The Division Algorithm for $\mathbb{N}$

Theorem

Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$, with $b \leq a$. Then there exists $q \in \mathbb{N}$ and $r \in \mathbb{N} \cup \{0\}$ such that $a = qb + r$, where $0 \leq r < b$. The numbers q and r are the quotient and the remainder of the division of a by b, respectively.

Proof.

Let $T = \{s \in \mathbb{N} : a < sb\}$. By the Archimedean Principle, T is nonempty. By WOP, T contains a minimal element w. Let $q = w - 1$ and $r = a - sb$. Since $a \geq b$, $w > 1$ and $q \in \mathbb{N}$, $a \geq qb$ and $r \geq 0$. By definition, $r = a - qb$. Now suppose $r \geq b$. Then $a - (w-1)b \geq b$, so $a \geq wb$. This contradicts the fact that $a < wb$. Therefore $r < b$. □

Outline

Art of Counting

Counting a set A means setting up a one-one corresponding between A and some standard set. We say that A is finite if $A = \emptyset$, or there is such a correspondence

$$A \leftrightarrow \{1, 2, 3, \ldots, n\},$$

some natural number n. We say that n is the number of elements of A, and write:

$\overline{\overline{A}} = n$ and $\overline{\overline{\emptyset}} = 0$.

Later in the semester, we return to a proper study of **cardinality**. Now we treat so basic rules to count sets since these numbers appear often in our proofs.

Sum Rule

Theorem

If A and B are disjoint finite sets with $\overline{\overline{A}} = m$ and $\overline{\overline{B}} = n$, then $\overline{\overline{A \cup B}} = m + n$.

Corollary

If $B \subseteq A$ are finite sets, then $\overline{\overline{A \setminus B}} = \overline{\overline{A}} - \overline{\overline{B}}$.

Proof.

B and $A \setminus B$ are disjoint sets, and $A = B \cup (A \setminus B)$. Now apply the Sum Rule. □

Generalized Sum Rule

Theorem

If $\mathcal{A} = \{A_i : i = 1, 2, \ldots, n\}$ is a family of distinct pairwise disjoint sets and $\overline{\overline{A_i}} = a_i$, then

$$\overline{\overline{\bigcup_{i=1}^{n} A_i}} = \sum_{i=1}^{n} a_i.$$

Proof. The proof is by induction on the number n of subsets in the family $\mathcal{A}$.

- If $n = 1$, then $\overline{\overline{\bigcup_{i=1}^{1} A_i}} = \overline{\overline{A_1}} = a_1 = \sum_{i=1}^{1} a_i$.

- Suppose $\overline{\overline{\bigcup_{i=1}^{n} A_i}} = \sum_{i=1}^{n} a_i$. Since $\bigcup_{i=1}^{n} A_i$ and A_{n+1} are disjoint, by the Sum Rule,

$$\begin{aligned} \overline{\overline{\bigcup_{i=1}^{n} A_i \cup A_{n+1}}} &= \overline{\overline{\bigcup_{i=1}^{n} A_i}} + \overline{\overline{A_{n+1}}} \\ &= \sum_{i=1}^{n} a_i + a_{n+1} = \sum_{i=1}^{n+1} a_i. \end{aligned}$$

- By the PMI, the assertion is true for every family of n sets, for all $n \in \mathbb{N}$.

More Rules

Theorem

For finite sets A and B,

1. $\overline{\overline{A \cup B}} = \overline{\overline{A}} + \overline{\overline{B}} - \overline{\overline{A \cap B}}.$
2. $\overline{\overline{A \cap B}} = \overline{\overline{A}} + \overline{\overline{B}} - \overline{\overline{A \cup B}}.$

Proof. of (1): Write $A \cup B$ the union of 3 disjoint subsets

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

Now apply the sum rule:

$$\begin{aligned} \overline{\overline{A \cup B}} &= \overline{\overline{(A \setminus A \cap B)}} + \overline{\overline{(B \setminus A \cap B)}} + \overline{\overline{(A \cap B)}} \\ &= \overline{\overline{A}} - \overline{\overline{A \cap B}} + \overline{\overline{B}} - \overline{\overline{A \cap B}} + \overline{\overline{A \cap B}} \\ &= \overline{\overline{A}} + \overline{\overline{B}} - \overline{\overline{A \cap B}}. \end{aligned}$$

Principle of Inclusion and Exclusion

Theorem

1. *For finite sets A, B and C,*

$$\overline{\overline{A\cup B\cup C}} \;=\; [\overline{\overline{A}}+\overline{\overline{B}}+\overline{\overline{C}}]-[\overline{\overline{A\cap B}}+\overline{\overline{A\cap C}}+\overline{\overline{B\cap C}}]-\overline{\overline{A\cap B\cap C}}.$$

2. *For finite sets A, B, C and D,*

$$\begin{aligned}
\overline{\overline{A\cup B\cup C\cup D}} \;&=\; [\overline{\overline{A}}+\overline{\overline{B}}+\overline{\overline{C}}+\overline{\overline{D}}]\\
&-\; [\overline{\overline{A\cap B}}+\overline{\overline{A\cap C}}+\overline{\overline{A\cap D}}+\overline{\overline{B\cap C}}+\overline{\overline{B\cap D}}+\overline{\overline{C\cap D}}]\\
&=\; [\overline{\overline{A\cap B\cap C}}+\overline{\overline{A\cap B\cap D}}+\overline{\overline{A\cap C\cap D}}+\overline{\overline{B\cap C\cap D}}]\\
&-\; [\overline{\overline{A\cap B\cap C\cap D}}.
\end{aligned}$$

Product Rules

Theorem

1. *If two independent tasks T_1 and T_2 are to be performed, and T_1 can be performed in m ways and T_2 in n ways, then the two tasks can be performed in mn ways.*
2. *If k independent tasks $T_1, T_2, \ldots, T_k$ are to be performed, and the number of ways task T_i can be performed is n_i, then the number of ways the tasks can be performed in sequence is*

$$\prod_{i=1}^{k} a_i = n_1 \cdot n_2 \cdots n_k.$$

Permutations

Definition

A **permutation** of a set with n elements is an arrangement of the elements of the set in a specific order.

Theorem

The number of permutations of a set of n elements is $n!$.

Permutation Rule

Theorem

The number of permutations of any r distinct elements from a set of n objects is

$$\frac{n!}{(n-r)!}.$$

Combinations

Definition

A **combination of** n **elements taken** r **at a time** is the selection of an r-element subset from an n-element set. The number of combinations of n elements taken r at a time is denoted $\binom{n}{r}$, and read "n choose r" or "n binomial r." The number $\binom{n}{r}$ is called a **binomial coefficient.**

Theorem

Let n *be a positive integer and* r *an integer such that* $0 \leq r \leq n$. *Then*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Binomial Theorem

Theorem (Binomial Theorem)

For $a, b \in \mathbb{R}$*,*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

Lemma

Let n be a positive integer and r an integer such that $0 \leq r \leq n$. Then

1. *For $r \geq 0$,*

$$\binom{n}{r} = \binom{n}{n-r}.$$

2. *For $r \geq 1$,*

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}.$$

Proof.

1. Selecting r objects of an n-set to form an r-subset, determines also an $(n-r)$-subset: the objects not selected. This is a one-one correspondence: $\binom{n}{r} = \binom{n}{n-r}$.
2. The r-subsets of $\{1, 2, 3, \ldots, n-1, n\}$ are of kinds:

$$r \text{ subsets of } \{1, 2, 3, \ldots, n-1\}$$
$$\{n\} \cup (r-1)\text{-subsets of } \{1, 2, 3, \ldots, n-1\}$$

Since these collections are disjoint, by the Sum Rule, $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$.

Proof of the Binomial Theorem

Proof. We will use the PMI to show

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

1. (Base case) $n = 1$: $(a+b)^1 = a + b$.
2. (Induction step) For $n \geq 2$,

$$\begin{aligned}
(a+b)^n &= (a+b)^{n-1}(a+b) \\
&= (a+b)^{n-1}a + (a+b)^{n-1}b \\
&= \sum_{r=0}^{n-1} \binom{n-1}{r} a^{r+1} b^{n-1-r} + \sum_{r=0}^{n-1} \binom{n-1}{r} a^r b^{n-r} \\
&= a^n + \sum_{r=1}^{n-1} \left[\binom{n-1}{r} + \binom{n-1}{r-1}\right] a^r b^{n-r} + b^n.
\end{aligned}$$

Now we apply the Lemma.

Corollary

Let n be a positive integer. Then

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

Proof.

Set $a = b = 1$ in

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

□

Pascal's Triangle

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \end{array}$$

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}.$$

Outline

Homework #5

- 2.6: 2(a,d), 3, 11(c), 18(a,b)