THE AXIOM OF CHOICE ALLOWS YOU TO SELECT ONE ELEMENT FROM EACH SET IN A COLLECTION AND HAVE IT EXECUTED AS AN EXAMPLE TO THE OTHERS.

MY MATH TEACHER WAS A BIG BELIEVER IN PROOF BY INTIMIDATION.
• Formal treatment dates from late 19\textsuperscript{th} century
• Direct ties between set theory and logic
• Important foundational language
some common sets

\[ \mathbb{N} \text{ is the set of Natural numbers; } \mathbb{N} = \{0, 1, 2, \ldots\} \]
\[ \mathbb{Z} \text{ is the set of Integers; } \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \]
\[ \mathbb{Q} \text{ is the set of Rational numbers; e.g. } \frac{1}{2}, -17, \frac{32}{48} \]
\[ \mathbb{R} \text{ is the set of Real numbers; e.g. } 1, -17, \frac{32}{48}, \pi \]
\[ [n] \text{ is the set } \{1, 2, \ldots, n\} \text{ when } n \text{ is a natural number} \]
\[ \{\} = \emptyset \text{ is the empty set; the only set with no elements} \]

EXAMPLES
Are these sets?
A = \{1, 1\}
B = \{1, 3, 2\}
C = \{☐, 1\}
D = \{\}, 17\}
E = \{1, 2, 7, \text{ cat, dog, } \emptyset, \alpha\}

Set membership:
We write \(2 \in E; 3 \notin E\).
A and B are *equal* if they have the same elements

\[ A = B \equiv \forall x \ (x \in A \iff x \in B) \]

A is a *subset* of B if every element of A is also in B

\[ A \subseteq B \equiv \forall x \ (x \in A \rightarrow x \in B) \]

**QUESTIONS**

- \( \emptyset \subseteq A? \)
  - \( \checkmark \)
- \( A \subseteq B? \)
  - \( \times \)
- \( C \subseteq B \)
  - \( \checkmark \)
• A and B are equal if they have the same elements

\[ A = B \equiv \forall x (x \in A \iff x \in B) \]

• A is a subset of B if every element of A is also in B

\[ A \subseteq B \equiv \forall x (x \in A \implies x \in B) \]

• Note: \( (A = B) \equiv (A \subseteq B) \land (B \subseteq A) \)
• The following says “S is the set of all x’s where P(x) is true.”

\[ S = \{x : P(x)\} \]

• The following says “S is the set of those elements of A for which P(x) is true.”

\[ S = \{x \in A : P(x)\} \]

• “The set of all the real numbers less than one”

\[ \{x \in \mathbb{R} : x < 1\} \]

• “The set of all powers of two”

\[ \{x \in \mathbb{N} : \exists j \ (x = 2^j)\} \]
**A ∪ B = \{ x : (x ∈ A) ∨ (x ∈ B) \}**

Union

**A ∩ B = \{ x : (x ∈ A) ∧ (x ∈ B) \}**

Intersection

**A \ B = \{ x : (x ∈ A) ∧ (x ∉ B) \}**

Set difference

A = \{1, 2, 3\}
B = \{4, 5, 6\}
C = \{3, 4\}

**QUESTIONS**

Using A, B, C and set operations, make...

[6] = ?  \( A \cup B \)

\{3\} = ?  \( A \cap C \)

\{1,2\} = ?  \( A \setminus C \)

\{1,3\} = ?  (Can we ever separate 1 and 2?)
more set operations

\[ A \oplus B = \{ x : (x \in A) \oplus (x \in B) \} \]

Symmetric difference

\[ \overline{A} = \{ x : x \notin A \} \]

Complement (with respect to universe U)

A = \{1, 2, 3\}
B = \{1, 4, 2, 6\}
C = \{1, 2, 3, 4\}

QUESTIONS

Let \( S = \{1, 2\} \).
If the universe is A, then \( \overline{S} \) is... \( \{3\} \)
If the universe is B, then \( \overline{S} \) is... \( \{4, 6\} \)
If the universe is C, then \( \overline{S} \) is... \( \{3, 4\} \)
it's Boolean algebra again! (yay...?)

- Definition for $\cup$ based on $\lor$
  \[ A \cup B = \{ x : x \in A \lor x \in B \} \]

- Definition for $\cap$ based on $\land$
  \[ A \cap B = \{ x : x \in A \land x \in B \} \]

- Complement works like $\neg$
  \[ \bar{A} = \{ x : \neg(x \in A) \} \]
Power set of a set \( A = \) set of all subsets of \( A \)

\[
\mathcal{P}(A) = \{ B : B \subseteq A \}
\]

e.g. Days = \{M, W, F\}

\[
\mathcal{P}(\text{Days}) = \{ \emptyset, \\
\{M\}, \{W\}, \{F\}, \\
\{M, W\}, \{W, F\}, \{M, F\}, \\
\{M, W, F\} \}
\]

e.g. \( \mathcal{P}(\emptyset) = \) ? \( (\mathcal{P}(\emptyset) = \{\emptyset\}) \)
$A \times B = \{ (a, b): a \in A, b \in B \}$

$A = \{1, 2\}$  
$B = \{a, b, c\}$

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

$A \times \emptyset = \emptyset$

$|A \times B| = |A| \cdot |B|$
de Morgan’s laws

\[ \overline{A \cup B} = \overline{A} \cap \overline{B} \]
\[ x \in \overline{A \cup B} \iff \neg (x \in A \lor x \in B) \]
\[ \iff (\neg (x \in A) \land \neg (x \in B)) \]
\[ \iff (x \in \overline{A} \land x \in \overline{B}) \iff x \in \overline{A} \cap \overline{B} \]

\[ \overline{A \cap B} = \overline{A} \cup \overline{B} \]
\[ x \in \overline{A \cap B} \iff \neg (x \in A \land x \in B) \]
\[ \iff (\neg (x \in A) \lor \neg (x \in B)) \]
\[ \iff (x \in \overline{A} \lor x \in \overline{B}) \]
\[ \iff x \in \overline{A} \cup \overline{B} \]

Proof technique:
To show \( C = D \) show
\( x \in C \rightarrow x \in D \) and
\( x \in D \rightarrow x \in C \)
distributive laws

\[ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \]
\[ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \]

Just like \( p \land (q \lor r) \equiv (p \land q) \lor (p \land r) \)
Russell’s paradox

\[ S = \{ x : x \notin x \} \]
• Suppose universe $U$ is $\{1, 2, \ldots, n\}$

• Can represent set $B \subseteq U$ as a vector of bits:  
\[ b_1b_2\ldots b_n \text{ where } b_i = 1 \text{ when } i \in B \]
\[ b_i = 0 \text{ when } i \notin B \]

  – Called the characteristic vector of set $B$

• Given characteristic vectors for $A$ and $B$
  – What is characteristic vector for $A \cup B$? $A \cap B$?
unix/linux file permissions

• **ls -l**
  
  drwxr-xr-x ... Documents/
  -rw-r--r-- ... file1

• Permissions maintained as bit vectors
  – Letter means bit is 1
  – “--” means bit is 0.
bitwise operations

\[
\begin{array}{c}
\text{01101101} \quad \text{Java:} \quad z = x \lor y \\
\lor \quad 00110111 \\
\text{01111111}
\end{array}
\]

\[
\begin{array}{c}
\text{00101010} \quad \text{Java:} \quad z = x \land y \\
\land \quad 00001111 \\
\text{00001010}
\end{array}
\]

\[
\begin{array}{c}
\text{01101101} \quad \text{Java:} \quad z = x \oplus y \\
\oplus \quad 00110111 \\
\text{01011010}
\end{array}
\]
• If $x$ and $y$ are bits: $(x \oplus y) \oplus y = ?$  \(\times\)

• What if $x$ and $y$ are bit-vectors? \(\text{Same thing, bitwise}\)
Alice wants to communicate message secretly to Bob so that eavesdropper Eve who hears their conversation cannot tell what Alice’s message is.

Alice and Bob can get together and privately share a secret key $K$ ahead of time.
one-time pad

- Alice and Bob privately share random n-bit vector $K$
  - Eve does not know $K$
- Later, Alice has n-bit message $m$ to send to Bob
  - Alice computes $C = m \oplus K$
  - Alice sends $C$ to Bob
  - Bob computes $m = C \oplus K$ which is $(m \oplus K) \oplus K$
- Eve cannot figure out $m$ from $C$ unless she can guess $K$