Advanced Algebra.

MA180-4.

Prof. Götz Pfeiffer

School of Mathematics, Statistics and Applied Mathematics
University of Galway

Semester 2 (2023/2024)

Outline

1. The Language of Mathematics: Logic and Sets.
   - Propositional Logic.
   - Valid Arguments.
   - Sets and Boolean Algebra.
   - Functions and Relations.
2. Examples of Algebraic Objects: Permutations and Polynomials.
   - Composition of Functions.
   - Permutations.
   - Polynomials.
   - Factorisation of Polynomials.
3. Mathematical Tools: Induction and Probability.
   - Mathematical Induction.
   - Probabilities and Sample Spaces
   - Some Probability Rules
   - Binomial Probability Distribution

References.

- Norman L. Biggs.
  Discrete Mathematics.
  Oxford UP 2003.
- Lindsay Childs.
  A Concrete Introduction to Higher Algebra.
  Springer 2000.
- Douglas E. Ensley and J.Winston Crawley
  Discrete Mathematics.
  Wiley 2006.
- Mark V. Lawson
  Algebra & Geometry: An Introduction to University Mathematics
  Taylor & Francis 2016

Introduction: The Language of Mathematics

Mathematics . . .

- . . . is about solving **problems**.
- . . . explains **patterns**.
- . . . is a set of statements deduced **logically** from axioms and definitions.
- . . . uses **abstraction** to model the real world.
- . . . employs a precise and powerful **language** to organize, communicate, and manipulate ideas.

As with any language, in order to participate in a conversation, it helps to be able to **read** and **write**.
In this section, we introduce basic elements of the mathematical language and study their meaning:

- **logic**: the language of mathematical arguments;
- **sets**: the language of relationships between mathematical objects.

Links: The Language of Mathematics.

- http://en.wikipedia.org/wiki/Language_of_mathematics
- http://en.wikipedia.org/wiki/Knights_and_Knaves
- http://www.iep.utm.edu/prop-log/
- http://en.wikipedia.org/wiki/Mathematical_proof
- http://plato.stanford.edu/entries/boolalg-math/
- http://en.wikipedia.org/wiki/Power_set
- http://en.wikipedia.org/wiki/Equivalence_relation
- http://en.wikipedia.org/wiki/Injective_function
- http://en.wikipedia.org/wiki/Surjective_function
- http://mathshistory.st-andrews.ac.uk/Biographies/Smullyan.html is a biography of the American mathematician, logician and magician **Raymond Merrill Smullyan** (1919–2017).
- http://mathshistory.st-andrews.ac.uk/Biographies/Boole.html is a biography of the British mathematician **George Boole** (1815–1864).
- http://mathshistory.st-andrews.ac.uk/Biographies/De_Morgan.html is a biography of the British mathematician **Augustus De Morgan** (1806–1871).

Logic Puzzles.

- A **logic puzzle** is a riddle that can be solved by **logical thinking**.

Example (The Island of Knights and Knaves.)

- A certain island has **two types** of inhabitants: knights and knaves.
- **Knights** always tell the truth.
- **Knaves** always lie.
- Every inhabitant is either a knight or a knave.
- You visit the island, and talk to two of its inhabitants, called A and B.
- A says: "Exactly one of us is a knave".
- B says: "At least one of us is a knight."
- **Who** (if any) **is telling the truth?**

Systematical Solution: Table Method.

- For a systematical solution, we use a **truth table**.
- On the **left**, **list** all possible truth values of the claims 'X is a knight' (T for 'true', F for 'false').

A is a knight	B is a knight	Exactly one is a knave	At least one is a knight
T	T	F	T
T	F	T	T
F	T	T	T
F	F	F	F

- On the **right**, **compute** the corresponding truth values of each of the statements.
- X is a knight if and only if X speaks the truth. Therefore the entry in the **left** column 'X is a knight' **must be equal** to the **right** entry for X's statement.
- Here, row 4 contains the **only match**, hence the **unique solution** of the puzzle.

Further Examples.

- You meet 2 inhabitants of the island.

  A: Exactly one of us is a knight.

  B: All of us are knaves.

  Who (if anyone) is telling the truth?

The following examples illustrate important points.

- You meet 1 inhabitant of the island.

  A: I am a knight.

A	A: . . .	
T	T	*
F	F	*

(There can be more than one solution.)

- You meet 1 inhabitant of the island.

  A: I am a knave.

A	A: . . .
T	F
F	T

(No solution? This cannot happen.)

A Puzzle With More Than Two Inhabitants.

- You meet 3 inhabitants of the island.

  A: Exactly one of us is a knight.
  B: All of us are knaves.
  C: The other two are lying.

  Who (if anyone) is lying?

Solution

A	B	C	A: ...	B: ...	C: ...	
T	T	T	F	F	F	
T	T	F	F	F	F	
T	F	T	F	F	F	
T	F	F	T	F	F	*
F	T	T	F	F	F	
F	T	F	T	F	F	
F	F	T	T	F	T	
F	F	F	F	T	T	

Symbols.

Truth Values

T : **true**

F : **false**

Logical Operations

$\wedge$: **and** (conjunction)

$\vee$: **or** (disjunction)

$\neg$: **not** (negation)

Variables

$a, b, c, \ldots, p, q, r, \ldots$: any statement

- Let a stand for 'A is a knight' and b for 'B is a knight.
- Then $\neg a$ means: A is a knave.
- B's statement: 'At least one of us is a knight' (i.e., 'A is a knight' or 'B is a knight') becomes: $a \vee b$.

Note: $\vee$ is an inclusive 'or'.

The disjunction $p \vee q$ allows for **both** p and q to be true.

Propositional Logic.

- Informally, a **proposition** is a statement that is **unambiguously** either **true** or **false**.
- A **propositional variable** is a symbolic name (like p, q, r, $\dots$) that stands for an arbitrary proposition.
- Formally, a proposition is defined recursively:

Definition (Formal Proposition)

1. Any **propositional variable** is a **formal proposition**.

Moreover, if p and q are formal propositions, the following **compound statements** are **formal propositions**:

2. the **conjunction** $p \wedge q$ (read: "p and q"), stating that "both p and q are true";
3. the **disjunction** $p \vee q$ (read: "p or q"), stating that "either p or q are true";
4. the **negation** $\neg p$ (read: "not p"), stating that "it is not the case that p is true".

Truth Tables.

- A **truth table** shows the truth value of a compound statement for every possible combination of truth values of its simple components.

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

p	$\neg p$
T	F
F	T

Example (The truth table for $(p \vee q) \wedge \neg(p \wedge q)$.)

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

A truth table built from the tables of $p \wedge q$, $p \vee q$ and $\neg p$.

Simplifying Negations.

- In mathematics, propositions often involve formulas.
- The negation of such a proposition can usually be reformulated in simpler terms with different symbols.

Example

- The negation of the statement "$x < 18$" is "$\neg(x < 18)$", or simply "$x \geqslant 18$".

- The negation of a **conjunction** is a **disjunction**(!)

Example (Truth tables for $\neg(p \wedge q)$ and $(\neg p \vee \neg q)$.)

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

Logical Equivalence.

- Two statements p and q are **logically equivalent** if they have the **same truth value** for every row of the truth table: We then write $p \equiv q$.

Theorem (DeMorgan's Laws)

Let p and q be propositions. Then

1. $\neg(p \vee q) \equiv \neg p \wedge \neg q$;
2. $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

- A proposition p is a **tautology**, if its truth value is T for all possible combinations of the truth values of its propositional variables: $p \equiv T$.
- A proposition p is a **contradiction**, if its truth value is F for all possible combinations of the truth values of its propositional variables: $p \equiv F$.
- Every logical equivalence is a tautology.

Logical Equivalences.

Theorem (for propositional variables p, q, r.)

All of the following are valid logical equivalences.

- *Commutative Laws:* $p \wedge q \equiv q \wedge p$, *and* $p \vee q \equiv q \vee p$.
- *Associative Laws:* $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$,
  and $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
- *Distributive Laws:* $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$,
  and $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
- *Absorption Laws:* $p \wedge (p \vee q) \equiv p$, *and* $p \vee (p \wedge q) \equiv p$.
- *Idempotent Laws:* $p \wedge p \equiv p$, *and* $p \vee p \equiv p$.
- *Complementary Laws:* $p \wedge \neg p \equiv F$, *and* $p \vee \neg p \equiv T$.
- *Identity Laws:* $p \wedge T \equiv p$, *and* $p \vee F \equiv p$.
- *Universal Bound:* $p \wedge F \equiv F$, *and* $p \vee T \equiv T$.
- *DeMorgan:* $\neg(p \wedge q) \equiv \neg p \vee \neg q$, *and* $\neg(p \vee q) \equiv \neg p \wedge \neg q$.
- *Negation:* $\neg T \equiv F$, *and* $\neg F \equiv T$.
- *Double Negation:* $\neg(\neg p) \equiv p$.

Proof: Compare the corresponding truth tables. □

Sets.

- Before moving on to **Quantified Predicates**, we need to briefly introduce sets.
- A **set**, naively, is a collection of objects, its **elements**.

Notation.

$a \in S$ means: object a is an element of the set S. And $a \notin S$ means: object a is **not** an element of the set S.

- Two sets A and B are **equal** ($A = B$) if they have the same elements:
  $a \in B$ for all $a \in A$ **and** $b \in A$ for all $b \in B$.

Examples

$\{0, 1\}$,
$\mathbb{N} = \{1, 2, 3, \dots\}$ (the **natural numbers**),
$\{x \in \mathbb{N} \mid x$ is a multiple of $5\}$,
$\varnothing = \{\ \}$ (the **empty set**).

Predicates.

Definition

A **predicate** $P(x)$ is a statement that incorporates a **variable** x, such that whenever x is **replaced by a value**, the resulting statement becomes a **proposition**.

Example

- Suppose $P(n)$ is the **predicate** "n is even".
- Then $P(14)$ is the **proposition** "14 is even".
- The proposition $P(13)$ is false.
- $P(22)$ is true.

- Predicates can be combined using the **logical operators** $\wedge$ (and), $\vee$ (or), $\neg$ (not) to create **compound predicates**.
- A predicate can have more than one variable, e.g., $P(x, y)$ can stand for the predicate "$x \leqslant y$".

Quantified Predicates.

Notation.

- Suppose that $P(x)$ is a predicate and that S is a set.
- "$\forall a \in S, P(a)$" is the proposition:
  "**for all** elements a of S the statement $P(a)$ is true".
- "$\exists a \in S, P(a)$" is the proposition:
  "**there exists** (at least) one element a in the set S such that the statement $P(a)$ is true".

Suppose $S = \{x_1, x_2, \dots\}$.

- "$\forall a \in S, P(a)$" abbreviates "$P(x_1) \wedge P(x_2) \wedge \cdots$".
- "$\exists a \in S, P(a)$" abbreviates "$P(x_1) \vee P(x_2) \vee \cdots$".

Negating Quantified Predicates.

- The negation of "$\forall x \in S, P(x)$" is "$\exists x \in S, \neg P(x)$";
- the negation of "$\exists x \in S, P(x)$" is "$\forall x \in S, \neg P(x)$".

Implications.

Definition

An **implication** is a statement of the form "if p then q". In symbols, we write this as $p \to q$ (read: "p implies q"). We call proposition p the **hypothesis** and proposition q the **conclusion** of the implication $p \to q$.

- The **truth table** of $p \to q$ has the form

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

Remark.

The **only way** for an implication $p \to q$ to be false is when the **hypothesis** p is **true**, but the **conclusion** q is **false**.

Converse, Inverse, Contrapositive.

Various variations of the implication $p \to q$ are of sufficient interest:

- $q \to p$ is the **converse** of $p \to q$.
- $\neg p \to \neg q$ is the **inverse** of $p \to q$.
- $\neg q \to \neg p$ is the **contrapositive** of $p \to q$.

Remark.

1. An implication is logically equivalent to its contrapositive: $p \to q \equiv \neg q \to \neg p$.
2. The converse and the inverse of an implication are logically equivalent: $q \to p \equiv \neg p \to \neg q$.
3. But an implication is not logically equivalent to its converse (and hence not to its inverse).

Proof: Truth tables. □

Biconditional.

- Write $p \leftrightarrow q$ if both $p \rightarrow q$ and $q \rightarrow p$ are true.
- Then $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$.
- The **truth table** of $p \leftrightarrow q$ has the form

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

- Usually, to prove a statement of the form $p \leftrightarrow q$, one proves the two statements $p \rightarrow q$ and $q \rightarrow p$ separately.

Examples

- n is even if and only of n^2 is even.
- The integer n is a multiple of 10 if and only if it is even.

Validating Arguments.

- An **argument** is a list of **statements**, ending in a **conclusion**.
- The logical **form** of an argument can be abstracted from its **content**.

Definition

Formally, an **argument structure** is a list of statements $p_1, p_2, \ldots, p_n, \therefore c$ starting with **premises** $p_1, \ldots, p_n$ and ending in a **conclusion** c.

- An argument is **valid** if the conclusion follows **necessarily** from the premises.
- Validity of arguments depends only on the form, not on the content.
- The argument structure '$p_1, \ldots, p_n, \therefore c$' is **valid** if the proposition $(p_1 \wedge \cdots \wedge p_n) \to c$ is a **tautology**, otherwise it is **invalid**.

How to Test Argument Validity.

1. Identify the **premises** and the **conclusion** of the argument.
2. Construct a **truth table** showing the truth values of all premises and the conclusion.
3. A **critical row** is a row of the truth table in which **all** the **premises** are **true**. Check the critical rows as follows.
4. If the **conclusion is true in every critical row** then the **argument structure is valid**.
5. If there is a critical row in which the conclusion is false, then it is possible for an argument of the given form to have a **false conclusion despite true premises** and so the **argument structure is invalid**.

Example of an Invalid Argument Structure.

Example

- Premises: $p_1 = (p \to q \vee \neg r)$, $p_2 = (q \to p \wedge r)$.
- Conclusion: $c = (p \to r)$.
- The argument structure $p_1, p_2, \therefore c$ is **invalid**:

p	q	r	$\neg r$	$q \vee \neg r$	$p \wedge r$	p_1	p_2	c
T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	
T	F	T	F	F	T	F	T	
T	F	F	T	T	F	T	T	F(!)
F	T	T	F	T	F	T	F	
F	T	F	T	T	F	T	F	
F	F	T	F	F	F	T	T	T
F	F	F	T	T	F	T	T	T

Valid Arguments vs Invalid Arguments.

Some Valid Argument Forms.

- Modus ponens: $p \to q$, p, $\therefore q$.
- Modus tollens: $p \to q$, $\neg q$, $\therefore \neg p$.
- Generalization: p, $\therefore p \vee q$.
- Specialization: $p \wedge q$, $\therefore p$.
- Conjunction: p, q, $\therefore p \wedge q$.
- Elimination: $p \vee q$, $\neg q$, $\therefore p$.
- Transitivity: $p \to q$, $q \to r$, $\therefore p \to r$.
- Division into cases: $p \vee q$, $p \to r$, $q \to r$, $\therefore r$.
- Contradiction Rule: $\neg p \to F$, $\therefore p$.

Some Common Fallacies.

- Converse fallacy: $p \to q$, q, $\therefore p$.
- Inverse fallacy: $p \to q$, $\neg p$, $\therefore \neg q$.

"All Humans Are Mortal."

- **Modus Ponens:**
  $p \to q,\ p,\ \therefore\ q.$

Example

- If Socrates is human then he is mortal.
- Socrates is human.
- $\therefore$ Socrates is mortal.

- Proof by truth table:

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

- **Modus Tollens:**
  $p \to q,\ \neg q,\ \therefore\ \neg p.$

Example

- If Zeus is human then he is mortal.
- Zeus is not mortal.
- $\therefore$ Zeus is not human.

- Proof by truth table:

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

Fallacies.

- **Converse Fallacy:**
  $p \to q,\ q,\ \therefore p.$

Example (WRONG!)

- If Socrates is human then he is mortal.
- Socrates is mortal
- $\therefore$ Socrates is human.

- Truth table:

p	q	$p \to q$	q	p
T	T	T	T	T
T	F	F	F	
F	T	T	T	F(!)
F	F	T	F	

- **Inverse Fallacy:**
  $p \to q,\ \neg p,\ \therefore \neg q.$

Example (WRONG!)

- If Zeus is human then he is mortal.
- Zeus is not human.
- $\therefore$ Zeus is not mortal.

- Truth table:

p	q	$p \to q$	$\neg p$	$\neg q$
T	T	T	F	
T	F	F	F	
F	T	T	T	F(!)
F	F	T	T	T

Knights and Knaves Revisited.

- a = 'A is a knight'.
- b = 'B is a knight'.

Example

- You visit the island of knights and knaves and find that:

$$a \to \neg b$$
$$\neg a \to \neg b$$
$$b \to a \vee b$$
$$\neg b \to \neg a \wedge \neg b$$

(a 'formal version' of the original puzzle).

- Who (if any) is telling the truth?

Solution

- Start with the tautology $a \vee \neg a$.
- Division into cases:

$$\begin{array}{l} a \vee \neg a, \\ a \to \neg b, \\ \underline{\neg a \to \neg b,} \\ \therefore \neg b. \end{array}$$

- Modus ponens:

$$\begin{array}{l} \neg b \to \neg a \wedge \neg b, \\ \underline{\neg b,} \\ \therefore \neg a \wedge \neg b. \end{array}$$

- Both are knaves!

- This solution is a 'formal version' of the original solution.

Subsets and Set Operations.

- A set B is a **subset** of a set A if each element of B is also an element of A:
  $B \subseteq A$ if $b \in A$ for all $b \in B$.
- $A = B$ if and only if $B \subseteq A$ and $A \subseteq B$.
- We assume that all our sets are subsets of a (big) **universal set**, or **universe** U.

Definition

Let $A, B \subseteq U$.

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

Set Equations.

Theorem

Let A, B, C be subsets of a universal set U. Then all of

$$
\begin{aligned}
A \cap B &= B \cap A, & A \cup B &= B \cup A,\\
(A \cap B) \cap C &= A \cap (B \cap C), & (A \cup B) \cup C &= A \cup (B \cup C),\\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), & A \cup (B \cap C) &= (A \cup B) \cap (A \cup C),\\
A \cap (A \cup B) &= A, & A \cup (A \cap B) &= A,\\
A \cap A &= A, & A \cup A &= A,\\
A \cap A' &= \varnothing, & A \cup A' &= U,\\
A \cap U &= A, & A \cup \varnothing &= A,\\
A \cap \varnothing &= \varnothing, & A \cup U &= U,\\
(A \cap B)' &= A' \cup B', & (A \cup B)' &= A' \cap B',\\
U' &= \varnothing, & \varnothing' &= U,\\
(A')' &= A
\end{aligned}
$$

are valid properties of set operations.

Proof: element-wise. □

Boolean Algebra.

- An example of **abstraction** in mathematics ...

- **Sets** (together with the operations $\cap$, $\cup$, $'$, and the constants $\varnothing$, $\mathcal{U}$) behave similar to **Propositions** (together with the operations $\wedge$, $\vee$, $\neg$, and the constants $\mathbb{F}$, $\mathbb{T}$)
- Both are examples of an **abstract structure** (with $\cdot$, $+$, $'$, and 0, 1) called a **Boolean algebra**

- For any **logical equivalence**, there is a corresponding **set equality**, and vice versa.

Duality

- The **dual** of a set equality is obtained by swapping $\cap$ with $\cup$ and swapping $\varnothing$ with $\mathcal{U}$.
- The dual of a valid set equality is also a valid set equality ...

Sets of Sets.

Definition

Let A be a set. The **power set** of A is the set
$P(A) = \{B : B \subseteq A\}$
of **all** subsets B of A.

Example

The power set of $A = \{1, 3, 5\}$ is the set
$P(A) = \{\varnothing, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}, \{1, 3, 5\}\}$

Definition

A **partition** of a set A is a set $P = \{P_1, P_2, \ldots\}$ of **parts** $P_1, P_2, \ldots \subseteq A$ such that

1. no part is empty: $P_i \neq \varnothing$ for all i;
2. distinct parts are disjoint: $P_i \cap P_j = \varnothing$ for all $i \neq j$;
3. every point is in some part: $A = P_1 \cup P_2 \cup \cdots$.

Products of Sets.

Definition

The **Cartesian product** of sets A and B is the set
$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$
of all **(ordered) pairs** (a, b).

Examples

- $A = \{1, 2, 3\}$, $B = \{X, Y\}$.
  $A \times B = \{(1, X), (1, Y), (2, X), (2, Y), (3, X), (3, Y)\}$.
- $A = \{1, 3\}$. $A^2 = A \times A = \{(1, 1), (1, 3), (3, 1), (3, 3)\}$

- More generally, for $n \in \mathbb{N}$, the Cartesian product of n sets $S_1, S_2, \dots, S_n$ is the set
  $S_1 \times S_2 \times \cdots \times S_n = \{(x_1, x_2, \dots, x_n) : x_i \in S_i\}$
  of all **n-tuples** $(x_1, x_2, \dots, x_n)$.
- $A^n = A \times A \times \cdots \times A$ (n factors).

Relations are Sets.

- A **relation** from a **domain** X to a **codomain** Y is a subset $R \subseteq X \times Y$.

Notation.

Write xRy (and say "x is related to y") for $(x, y) \in R$.

- Let R be a relation on X, i.e, $R \subseteq X \times X$.
- R is **reflexive** if xRx for all $x \in X$.
- R is **symmetric** if xRy then yRx for all $x, y \in X$.
- R is **transitive** if xRy and yRz then xRz, for all $x, y, z \in X$.
- A relation $R \subseteq X \times X$ that is reflexive, symmetric and transitive is called an **equivalence relation**.

Equivalence Relations are Partitions.

- Suppose R is an **equivalence relation** on a set X.
  For $x \in X$, denote by $[x] = \{y : xRy\}$ the **equivalence class** of x, i.e., the set of all $y \in X$ that x is R-related to.
  Also denote by $X/R = \{[x] : x \in X\}$ the **quotient set**, i.e., the set of all equivalence classes.
- Suppose that P is a **partition** of X.
  For $x \in X$, denote by $P(x)$ the **unique part** of P that contains x.

Theorem

1. *If R is an **equivalence relation** on the set X, then the quotient set X/R is a **partition** of X.*
2. *Conversely, if P is a **partition** of a set X, then the relation $R = \{(x, y) \in X^2 : P(x) = P(y)\}$ is an **equivalence relation**.*

Functions are Relations are Sets.

- A **function** f from a **domain** X to a **codomain** Y is a **relation** $f \subseteq X \times Y$, with the property that,

  for every $x \in X$,
  there is a **unique** $y \in Y$ such that $(x, y) \in f$.

- (This is often called the **Vertical Line Test**.)

Notation.
Write $f\colon X \to Y$ for a function f from X to Y
and $f(x) = y$ for the unique $y \in Y$ such that if $(x, y) \in f$.

- A **function** thus consists of three things: a **domain** X and a **codomain** Y together with a **rule** $f \subseteq X \times Y$ that associates to each point $x \in X$ a **unique value** $f(x) = y \in Y$.

Injective and Surjective Functions.

- A function $f\colon X \to Y$ is called **surjective** (or **onto**) if,

  for every $y \in Y$,
  there is **at least** one $x \in X$ such that $f(x) = y$.

- A function $f\colon X \to Y$ is called **injective** (or **one-to-one**) if,

  for every $y \in Y$,
  there is **at most** one $x \in X$ such that $f(x) = y$.

- A function $f\colon X \to Y$ is called **bijective** (or a **one-to-one correspondence** if it is both **injective** and **surjective**, i.e., if,

  for every $y \in Y$,
  there is a **unique** $x \in X$ such that $f(x) = y$.

- A function is injective/surjective/bijective if it passes a suitable **Horizontal Line Test**.

Bijections of Partitions and Subsets.

- Consider a **function** $f\colon X \to Y$.
- The **image** $f(X) = \{f(x) : x \in X\}$ is a **subset** of Y.
- The **relation** $\sim_f$ on X by $x \sim_f x'$ if $f(x) = f(x')$ is an **equivalence** relation and the equivalence classes $[x] = \{x' \in X : f(x) = f(x')\}$ form **partition** $X/{\sim_f}$ of X, called the **kernel** of f.

Theorem

1. *Let* $f\colon X \to Y$*. Then the function* $F\colon X/{\sim_f} \to f(X)$ *defined by* $F([x]) = f(x)$ *for* $x \in X$ *is a well-defined bijection between the kernel* $X/{\sim_f}$ *of* f *and the image* $f(X)$ *of* f*.*
2. *Conversely, if* $Y' \subseteq Y$ *is any subset of* Y*, if* $\sim$ *is any equivalence relation on* X *and* $F\colon X/{\sim} \to Y'$ *is a bijection then the rule* $f(x) = F([x])$ *defines a function* f *from* X *to* Y*.*

Summary: The Language of Mathematics.

- **Formal propositions** consist of **propositional variables**, combined by the **logical connectives** $\wedge$ (and), $\vee$ (or), and $\neg$ (not).
- A **truth table** determines the truth value of a proposition depending on the truth values of its propositional variables.
- Truth tables can be used to **validate** or invalidate **argument structures**.
- Sets, with the operations $\cap$ (intersection), $\cup$ (union), and $'$ (complement in a universal set $\mathcal{U}$) form a **Boolean algebra**, like the formal propositions with their logical operations.
- Claims about sets are **proved** by valid arguments.
- **Functions** and **relations** are sets (of pairs).
- A function is a one-to-one **correspondence** between a **partition** of its **domain** and a **subset** of its **codomain**.