Foundations of Mathematics

Lukas Zamora

April 11, 2018

Contents

Chapter 1

Language, Logic, and Proof

1.1 Language and Logic

Mathematical Statements

Definition 1.1.1. *A **proposition** is any declarative sentence that is either true or false, but not both.*

A proposition cannot be neither true nor false and it cannot be both true and false.

A proposition is an example of a mathematical statement.

- **Set Terminology and Notation (very short introduction)**
  Set is a well-defined collection of objects.
  Elements are objects or members of the set.
- **Roster notation:**
  $A = \{a, b, c, d, e\}$ Read: "Set A with elements a, b, c, d, e."
- **Indicating a pattern:** $B = \{a, b, c, \ldots, z\}$ Read: "Set B with elements being the letters of the alphabet."

If a is an element of a set A, we write $a \in A$ that reads "a belongs to A." However, if a does not belong to A we write $a \notin A$.6

Some numbers sets:

- $\mathbb{R}$ is the set of all *real* numbers.
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, the set of all *integers*.
- $\mathbb{N} = \{1, 2, 3, \ldots\}$, the set of all *natural* numbers.
- $\mathbb{Q}$ is the set of all *rational* numbers.

- $\mathbb{E} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$, the set of all *even* integers.
- $\mathbb{O} = \{\pm 1, \pm 3, \pm 5, \dots\}$, the set of all *odd* integers.
- $n\mathbb{Z}$ is the set of all integer multiples of n, where $n \in \mathbb{N}$.

Trichotomy Axiom: Given fixed real numbers a and b, exactly one of the following statements is true,

$$a < b \qquad a = b \qquad b < a$$

A ***predicate*** is any declarative sentence containing one or more variables, each variable representing a value in some prescribing set, called the ***universe***, and which becomes a proposition when values from their respective universes are substituted for these variables.

Example 1. *Let $P(x) : x + 5 = 7$ where $x \in \mathbb{R}$. Then $P(2)$ is a true proposition, whereas $P(-1)$ is a false proposition. $P(n)$ becomes a true proposition when we substitute for n the values from the set $\{2\}$.*

Negation

Definition 1.1.2. *If P is a mathematical statement, then the* **negation/denial** *of P, written $\neg P$ (read "not P"), is the mathematical statement "P is false."*

Basic Connectivities

We have two types of mathematical statements: propositions and predicates. We can build more complicated (compound) statements using the following logical connectivities:

Logical connectivity	write	read	meaning
Conjunction	$P \wedge Q$	P and Q	Both P and Q are true
Disjunction	$P \vee Q$	P or Q	P is true or Q is true

Example 2. *Let the statements be P : "Ben is a student", Q : "Ben is a grader." Then $P \wedge Q$: "Ben is a student and a grader", $P \vee Q$: "Ben is a student or a grader."*

Truth Tables

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

Implications

Definition 1.1.3. *Let P and Q be statements. The* **implication** *$P \Rightarrow Q$ (read "P implies Q") is the statement "if P is true, then Q is true."*

In implications, P is called *assumption, or hypothesis, or antecedent*; and Q is called *conclusion, or consequent.*

The truth table for implication:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Converse and Contrapositive

Definition 1.1.4. *The statement $Q \Rightarrow P$ is called the* ***converse*** *of the statement $P \Rightarrow Q$.*

Definition 1.1.5. *The statement $(\neg Q) \Rightarrow (\neg P)$ is called the* ***contrapositive*** *of the statement $P \Rightarrow Q$.*

Biconditional

Definition 1.1.6. *For statements P and Q,*

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

is called the ***biconditional*** *of P and Q and is denoted by $P \Leftrightarrow Q$. The biconditional $P \Leftrightarrow Q$ is stated as "P if and only if Q."*

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Logical Equivalence

Definition 1.1.7. *Two compound statements are* ***logically equivalent*** *(write "$\equiv$") if they have the same truth tables, which means they both are true or both are false.*

Some Fundamental Properties of Logical Equivalence

Theorem 1.1.8. *For the statement forms P, Q, and R,*

A. $\neg(\neg P) \equiv P$

B. Commutative Laws
$P \wedge Q \equiv Q \wedge P$
$P \vee Q \equiv Q \vee P$

C. Associative Laws
$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

D. Distributive Laws
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

E. De Morgan's Laws
$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$
$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$

F. $\neg(P \Rightarrow Q) \equiv P \wedge (\neg Q)$

G. $P \Rightarrow Q \equiv (\neg P) \vee Q$

H. $P \Rightarrow Q \equiv (\neg Q) \Rightarrow (\neg P)$

I. $P \Rightarrow Q$ *is NOT logically equivalent to* $Q \Rightarrow P$

Proof. Each part of the theorem is verified by means of a truth table. $\square$

Tautologies and Contradictions

Tautology: statement that is always true.
Contradiction: statement that is always false.

P	$\neg P$	$P \vee (\neg P)$	$P \wedge (\neg P)$
T	F	T	F
F	T	T	F

Remark 1.1.9. *Let P and Q be statements. The biconditional $P \Leftrightarrow Q$ is a tautology if and only if P and Q are logically equivalent.*

Quantified Statements

A predicate can be made into a proposition by using **quantifiers**.

Universal: $\forall x$ means for all/for every assigned value a of x.
Existential: $\exists x$ means that for some assigned values a of x.

Quantified statements

in symbols	in words
"$\forall x \in D,\ P(x)$." or "$(\forall x \in D)P(x)$."	"For every $x \in D$, $P(x)$."
"$\exists x \in D \ni P(x)$." or "$(\exists x \in D)P(x)$."	"There exists x such that $P(x)$."

Once a quantifier is applied to a variable, the variable is then called a **bound** variable. The variable that is not bound is called a **free** variable.

Negations of Quantified Statements

Quantified statement	Corresponding negation
$\forall x \in D,\ P(x)$	$\exists x \in D \ni (\neg P(x))$
$\exists x \in D \ni P(x)$	$\forall x \in D,\ (\neg P(x))$
$\forall x \in D,\ (P(x) \vee Q(x))$	$\exists x \in D \ni (\neg P(x) \wedge Q(x))$
$\exists x \in D \ni (P(x) \wedge Q(x))$	$\forall x \in D,\ (\neg P(x) \vee \neg Q(x))$
$\forall x \in D,\ (P(x) \Rightarrow Q(x))$	$\exists x \in D \ni (P(x) \wedge \neg Q(x))$

1.2 Proof

Logical arguments

Most theorems (or results) are stated as implications.

Trivial and Vacuous Proofs

Let $P(x)$ and $Q(x)$ be open sentences over a domain D. Consider the quantified statement

$$\forall x \in D,\ P(x) \Rightarrow Q(x) \tag{1.1}$$

Trivial Proof: If it can be shown that $Q(x)$ is true for all $x \in D$ (regardless the truth value for $P(x)$), then 1.1 is true.

Vacuous Proof: If it can be shown that $P(x)$ is false for all $x \in D$ (regardless the truth value for $Q(x)$), then 1.1 is true.

Example 3. *Let $x \in \mathbb{R}$. If $x^6 - 3x^4 + x + 3 < 0$, then $x^4 + 1 > 0$.*

Proof. Let $x \in \mathbb{R}$. Since $x^4 \geq 0$ for all $x \in \mathbb{R}$, we get $x^4 + 1 \geq 0 + 1 > 0$. Hence the statement is true by vacuous proof. $\square$

Integers and some of their basic properties and definitions

Let $a, b, c \in \mathbb{Z}$

property	w.r.t addition	w.r.t multiplication
Closure	$a+b \in \mathbb{Z}$	$a \cdot b \in \mathbb{Z}$
Associative	$(a+b)+c = a+(b+c)$	$(ab)c = a(bc)$
Commutative	$a+b = b+a$	$ab = ba$
Distributive	$a(b+c) = ab+ac$	$a(b+c) = ab+ac$
Identity	$a+0 = a$	$a \cdot 1 = a$
Inverse	There exists a unique integer $-a = (-1) \cdot a$ such that $a+(-a) = 0$	Only 1 and -1 are invertible
Subtraction	$b - a := b + (-a)$	
No divisors of 0		If $ab = 0$ then $a = 0$ or $b = 0$
Cancellation	If $a+c = b$, then $a = b$	If $ab = ac$ and $a \neq 0$, then $b = c$

Order properties

A. If $a < b$ and $b < c$ then $a < c$. (**transitivity**)

B. Exactly one of $a < b$ or $a = b$ or $a > b$ holds. (**trichotomy**)

C. If $a < b$, then $a + c < b + c$.

D. If $c > 0$, then $a < b$ if and only if $ac < bc$.

E. If $c < 0$, then $a < b$ if and only if $ac > bc$.

Mathematical definitions are always <u>biconditional</u> statements.

Definition 1.2.1. *An integer n is defined to be* ***even*** *if $n = 2k$ for some integer k. An integer n is defined to be* ***odd*** *if $n = 2k+1$ for some integer k.*

Definition 1.2.2. *The integers m and n are said to be* ***of the same parity*** *if m and n are both even, or both odd. The integers m and n are said to be $of opposite parity$ if one of them is even and the other is odd.*

Definition 1.2.3. *Let a and b be integers. We say that b* ***divides*** *a, written $b|a$, if there is an integer c such that $bc = a$. We say that b and c are* ***factors*** *of a, or that a is* ***divisible*** *by b and c.*

Definition 1.2.4. *A real number x is* ***rational*** *if $x = \frac{m}{n}$ for some integers m and n.*

Direct Proofs

Let $P(x)$ and $Q(x)$ be open sentences over a domain D.
To prove (directly) a statement of the form, "For all $x \in D$, $P(x)$ is true":

A. Assume x is an arbitrary (but now fixed) element $x \in D$.

B. Demonstrate that $P(x)$ is true.

Example 4. *Let $n \in \mathbb{Z}$. Prove that if n is even, then $5n^5 + n + 6$ is even.*

Proof. Let $n \in \mathbb{E}$. Then $n = 2k$ for some $k \in \mathbb{Z}$. Hence $5n^5 + n + 6 = 5(2k)^5 + (2k) + 6 = 2(5 \cdot 2^4 \cdot k^5 + k + 3) \in \mathbb{E}$, because $5 \cdot 2^4 \cdot k^5 + k + 3 \in \mathbb{Z}$ by closure property. Therefore $5n^5 + n + 6$ is even. $\square$

Theorem 1.2.5. *The sum and product of every two rational numbers is rational*

Proof. Let $m, n \in \mathbb{Q}$. Then $m = \frac{a_1}{b_1}$ and $n = \frac{a_2}{b_2}$ for some $a_1, b_1, a_2, b_2 \in \mathbb{Z}$. Then

$$\begin{aligned} m + n &= \frac{a_1}{b_1} + \frac{a_2}{b_2} \\ &= \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \\ &= \frac{z_1}{z_2} \end{aligned}$$

where $z_1 = a_1 b_2 + a_2 b_1$ and $z_2 = b_1 b_2$. Since $z_1, z_2 \in \mathbb{Z}$ by closure property and $z_2 \neq 0$, we conclude that $m + n \in Q$. $\square$

Example 5. *Let $a, b, c \in \mathbb{Z}$. Prove that if $a|b$ and $b|c$, then $a|c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. By definition, $a|b$ is equivalent to $b = ax$, and $b|c$ is equivalent to $c = by$ for some $x, y \in \mathbb{Z}$. Hence $c = by = (ax)y = a(xy) = az$, where $z = xy \in \mathbb{Z}$ by closure property. Therefore $a|c$. $\square$

Proof by Cases

Proof by cases may be useful while attempting to give a proof of a statement concerning an element x in some set D. Namely, if x possesses one of two or more properties, then it may be convenient to divide a case into other cases, called *subcases*.

Example 6. *Prove that if n is an integer, then $n^2 + 3n + 4$ is an even integer.*

Proof. Let $n \in \mathbb{Z}$. Since every integer is either even or odd, consider the following two cases:

- Case 1: Let $n \in \mathbb{E}$. Then $n = 2k$ for some $k \in \mathbb{Z}$. Thus, $n^2 + 3n + 4 = (2k)^2 + 3(2k) + 4 = 2(2k^2 + 3k + 2) \in \mathbb{E}$, because $2k^2 + 3k + 2 \in \mathbb{Z}$ by closure property.
- Case 2: Let $n \in \mathbb{O}$. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Thus, $n^2 + 3n + 4 = (2k + 1)^2 + 3(2k + 1) + 4 = 4k^2 + 4k + 1 + 6k + 3 + 4 = 4k^2 + 10k + 8 = 2(2k^2 + 5k + 4) \in \mathbb{E}$, because $2k^2 + 5k + 4 \in \mathbb{Z}$ by closure property.

$\square$

Disproving Statements

Case 1. Counterexamples

Let $S(x)$ be an open sentence over a domain D. If the quantified statement $(\forall x \in D,\, S(x))$ is false, then its negation is true, i.e,

$$\neg(\forall x \in D,\, S(x)) \equiv \exists x \in D \ni \neg S(x)$$

Such an element x is called a **counterexample** of the false statement $\forall x \in D,\ S(x)$.

Example 7. *Disprove the following statement: "If $n \in \mathbb{O}$, then $3|n^2+2$."*

Solution. A counterexample: Let $n = 3$. Then we have that $3 \in \mathbb{O}$, but $3 \nmid 11$.

Case 2. Existence Statements

Consider the quantified statement $\exists x \in D \ni S(x)$. If this statement is false, then its negation is true, i.e,

$$\neg(\exists x \in D \ni S(x)) \equiv \forall x \in D,\ \neg S(x)$$

Example 8. *Disprove the statement: "There exists an even integer n such that $3n+5$ is even."*

Solution. It is sufficient to prove that for every integer n, the number $3n+5$ is odd. Indeed, if $n \in \mathbb{E}$, then $n = 2k$ for some $k \in \mathbb{Z}$. Hence $3n+5 = 3(2k)+5 = 3(2k)+4+1 = 2(3k+2)+1 \in \mathbb{O}$, since $3k+2 \in \mathbb{Z}$ by closure property.

Chapter 2

Techniques of Proof

2.1 Indirect Proofs: Proofs by Contradiction and Contrapositive

Proof by Contrapositive

Let $P(x)$ and $Q(x)$ be open sentences over a domain D. A proof by contrapositive of an implication is a direct proof of its contrapositive, that is **to prove that for all** $x \in D$, $P(x) \Rightarrow Q(x)$

- Assume that $\neg Q(x)$ is true for an arbitrary (but now fixed) element $x \in D$.
- Draw out consequences of $\neg Q(x)$.
- Use these consequences to show that $\neg P(x)$ must be true as well for this element x.
- It follows that $P(x) \Rightarrow Q(x)$ is true for all $x \in D$.

Example 9. *Let $x, y \in \mathbb{Z}$. If $7 \nmid xy$, then $7 \nmid x$ and $7 \nmid y$.*

Proof. By contrapositive method, it is sufficient to prove that for every $x, y \in \mathbb{Z}$, if $7|x$ or $7|y$, then $7|xy$. Consider the following cases:

- Case 1: Let $7|x$. Then $x = 7k$ for some $k \in \mathbb{Z}$. Thus $xy = (7k)y = 7(ky)$. Since $ky \in \mathbb{Z}$ by closure property, we get that $7|xy$.
- Case 2: Let $7|y$. This case is similar to Case 1 because $xy = yx$. Thus the proof can be omitted.

□

Proving Biconditional Statements

Prove that $\forall x \in D$, $P(x) \Rightarrow Q(x)$.

Proof. Let $x \in D$.
Assume $P(x)$. Then show $Q(x)$.
Conversely, assume $Q(x)$. Then show $P(x)$. □

Example 10. *Let $x, y \in \mathbb{Z}$. Prove that x and y are of opposite parity **if and only if** $x+y$ is odd.*

Proof. Let $x, y \in \mathbb{Z}$. Assume that x and y are of opposite parity. Then consider the following cases:

- Case 1: Let $x \in \mathbb{E}$, $y \in \mathbb{O}$. Then $x = 2k$, $y = 2j + 1$ for some $k, j \in \mathbb{Z}$. Hence $x + y = 2k + 2j + 1 = 2(k + j) + 1 \in \mathbb{O}$, since $k + j \in \mathbb{Z}$ by closure property.

- Case 2: Let $x \in \mathbb{O}$, $y \in \mathbb{E}$. This case is similar to case 1 because of a symmetry between x and y, so it can be omitted.

(Conversely, let $x + y \in \mathbb{O}$. Then show that x and y are of same parity.)

By contrapositive method, it is sufficient to show that if x and y are of the same parity, then $x + y \in \mathbb{E}$. Assume that x and y are of the same parity, then consider the following two cases:

- Case 1: Let $x, y \in \mathbb{E}$. Then $x = 2k$, $y = 2j$ for some $k, j \in \mathbb{Z}$. Thus $x + y = 2k + 2j = 2(k + j) \in \mathbb{E}$, since $k + j \in \mathbb{Z}$ by closure property.

- Case 2: Let $x, y \in \mathbb{O}$. Then $x = 2k + 1$, $y = 2j + 1$ for some $k, j \in \mathbb{Z}$. Thus $x + y = 2k + 1 + 2j + 1 = 2(k + j + 1) \in \mathbb{E}$, since $k + j + 1 \in \mathbb{Z}$ by closure property.

□

Proof by Contradiction

To prove a statement S is true by contradiction:

- Assume that $\neg S$ is true.

- Deduce a contradiction.

- Then conclude that S is true.

Example 11. *Prove that there is no smallest positive real number.*

Proof. By contradiction, assume that there is a smallest positive real number, say x. But if $x \in \mathbb{R}^+$, then $\frac{x}{2} \in \mathbb{R}^+$ and $\frac{x}{2} < x$, a contradiction, since $\frac{x}{2}$ is smaller than the smallest positive real number. □

One Important Theorem

Recall that a real number x is **rational** if $x = \frac{m}{n}$ for some integers m and n. Note that if necessary, we may assume (without loss of generality) that the integers m and n have no common positive factors other than 1. (In other words, we may assume that every fraction can be reduced to least terms.)

Theorem 2.1.1. *The number $\sqrt{2}$ is irrational.*

Proof. By contradiction, assume that $\sqrt{2}$ is rational, i.e,

$$\sqrt{2} = \frac{m}{n} \tag{2.1}$$

for some $m, n \in \mathbb{Z}$. Without loss of generality, we may assume that m and n have no common factors other than 1 or -1. Then squaring both sides of (2.1), we get

$$m^2 = 2n^2 \tag{2.2}$$

In other words, $m^2 \in \mathbb{E}$. Hence $m \in \mathbb{E}$. Thus $m = 2k$ for some $k \in \mathbb{Z}$. By substituting this into (2.2), we obtain $(2k)^2 = 2n^2$, or $n^2 = 2k^2$, i.e, $n^2 \in \mathbb{E}$, which implies that $n \in \mathbb{E}$. If om and n are both even, this implies that they share a common factor of 2, a contradiction. □

Theorem 2.1.2. *Let S and C be statements. Then $\neg S \Rightarrow (C \wedge \neg C)$ is logically equivalent to S.*

Proof. By truth table,

S	$C \wedge \neg C$	$\neg S$	$\neg S \Rightarrow (C \wedge \neg C)$
T	F	F	T
F	F	T	F

□

To prove a statement $P \Rightarrow Q$ by contradiction:

- Assume that P is true.
- To derive a contradiction, assume that $\neg Q$ is true.
- Prove a false statement C, using negation: $\neg(P \Rightarrow Q) \equiv (P \wedge \neg Q)$.
- Prove $\neg C$. It follows that Q is true. (The statement $C \wedge \neg C$ must be false, i.e, a contradiction.)

Example 12. *If m and n are integers, then $m^2 \neq 4n + 2$.*

Proof. By contradiction, assume that there exists $m, n \in \mathbb{Z}$ such that $m^2 = 4n + 2$. But $m^2 = 2(2n + 1) \in \mathbb{E}$, since $2n + 1 \in \mathbb{Z}$ by closure property. We then have that $m \in \mathbb{E}$. So $m = 2k$ for some $k \in \mathbb{Z}$. Hence $(2k)^2 = 4n + 2$, $4k^2 = 4n + 2$, or $k^2 - n = \frac{1}{2}$, a contradiction (since $\frac{1}{2} \notin \mathbb{Z}$). □

Existence Proofs

An existence theorem can be expressed as a quantified statement $\exists x \in D \ni S(x)$:

$$\text{There exists } x \in D \text{ such that } S(x) \text{ is true.}$$

Example 13. *There exists real numbers a and b such that $\sqrt{a^2+b^2} = a+b$.*

Proof. Let $a = 0$, $b = 1$. Then $a, b \in \mathbb{R}$ and $\sqrt{a^2+b^2} = \sqrt{0^2+1^2} = 1 = 0+1 = a+b$. □

Theorem 2.1.3. (Intermediate Value Theorem of Calculus) *If f is a real-valued function that is continuous on the closed interval $[a, b]$ and m is a number between $f(a)$ and $f(b)$, then there exists a number $c \in (a, b)$ such that $f(c) = m$.*

Chapter 3

Induction

3.1 Principle of Mathematical Induction

Theorem 3.1.1. (Principle of Mathematical Induction) *Let $P(n)$ be a statement about the positive integer n so that n is a free variable in $P(n)$.* ***Suppose the following:***

- ***(PMI 1)*** *The statement $P(1)$ is true.*
- ***(PMI 2)*** *For all positive integers k, if $P(k)$ is true, then $P(k+1)$ is true.*

Then*, for all positive integers n, $P(n)$ is true.*

Strategy

The proof by induction consists of the following steps:

- **Base Case:** Verify that $P(1)$ is true.
- **Inductive Hypothesis:** Assume that k is a positive integer for which $P(k)$ is true.
- **Conclusion:** $P(n)$ is true for every positive integer n.

Example 14. *Prove that $3|8^n - 5^n)$ for every positive integer n.*

Proof. Apply PMI. Let $P(n) : 3|(8^n - 5^n$, $n \in \mathbb{Z}^+$.

Base Case: $P(1) : 3|8 - 5 = 3|3$ which is true.

Inductive Hypothesis: Assume $P(k) : 3|8^k - 5^k$ for some $k \in \mathbb{Z}^+$.

Inductive Step: (Prove that $P(k+1)$ is true.) We have if $3|(8^k - 5^k)$ then there exists $j \in \mathbb{Z}$ such that $8^k - 5^k = 3j$, or $8^k = 3j + 5^k$. Then

$$\begin{aligned} 8^{k+1} - 5^{k+1} &= 8 \cdot 8^k - 5^{k+1} \\ &= 8(3j + 5k) - 5^{k+1} \\ &= 8 \cdot 3j + 8 \cdot 5^k - 5 \cdot 5^k \\ &= 8 \cdot 3j + 3 \cdot 5^k \\ &= 3(8j + 5^k) \end{aligned}$$

Since $8j + 5^k \in \mathbb{Z}$ by closure property, we conclude that $3|(8^{k+1} - 5^{k+1})$.

Conclusion: $P(n)$ is true for all $n \in \mathbb{Z}^+$ $\square$

Chapter 4

Sets

4.1 The Language of Sets

Set Terminology and Notation

Set is a well-defined collection of objects.
Elements are objects or members of the set.

Describing a Set

- **Roster Notation:**
  $A = \{a, b, c, d, e\}$ Read: Set A with elements a, b, c, d, e.

- **Indicating a pattern:**
  $B = \{a, b, c, \ldots, z\}$ Read: Set B with elements being the letters of the alphabet.

If a is an element of set A, we write $a \in A$ that reads "a belongs to A". If a does not belong to A, we write $a \notin A$.

Set-Builder Notation

Definition 4.1.1. *Let $P(x)$ be a predicate. Then the notation*

$$\{x | P(x)\} \qquad or \qquad \{x : P(x)\}$$

denotes the set of all elements x such that $P(x)$ is a true statement. (The symbol "$|$" is read "such that".)

When D is a set,

$$\{x \in D | P(x)\} = \{x | x \in D \wedge P(x)\}$$

Interval Notation

Bounded Intervals

- Closed interval $[a, b] = \{x \in \mathbb{R} | a \leq x \leq b\}$
- Open interval $(a, b) = \{x \in \mathbb{R} | a < x < b\}$
- Half-open, half-closed interval $(a, b] = \{x \in \mathbb{R} | a < x \leq b\}$
- Half-closed, half-open interval $[a, b) = \{x \in \mathbb{R} | a \leq x < b\}$

Unbounded Intervals

- $[a, \infty) = \{x \in \mathbb{R} | a \leq x\}$
- $(a, \infty) = \{x \in \mathbb{R} | a < x\}$
- $(-\infty, a] = \{x \in \mathbb{R} | x \geq a\}$
- $(-\infty, a) = \{x \in \mathbb{R} | x > a\}$
- $(-\infty, \infty) = \{x \in \mathbb{R}\}$

Subsets

- Two sets, A and B, are **equal**, written $A = B$ if and only if they have exactly the same elements. (NOTE: they do not have to be in the same order!)
- If every element in set A is also an element in set B, then A is a subset of B, written $A \subseteq B$.
- If $A \subseteq B$, but $A \neq B$, then A is a **proper** subset of B, written $A \subset B$.
- The **empty set** is the set that does not have any elements, denoted by $\emptyset$ or $\{\}$.
- The **universal set** is the set that contains all of the elements for a problem, denoted by $\mathcal{U}$.

In Symbols

Let $A, B \subseteq \mathcal{U}$. Then

- $A = B \Leftrightarrow \forall x \in \mathcal{U}, (x \in A \Leftrightarrow x \in B)$
- $A \subseteq B \Leftrightarrow \forall x \in \mathcal{U}, (x \in A \Rightarrow x \in B)$
- $A \subset B \Leftrightarrow \forall x \in \mathcal{U}, (x \in A \Rightarrow x \in B) \wedge (\exists x \ni x \notin A \wedge x \in B)$
- $A \neq B \Leftrightarrow \exists x \in \mathcal{U} \ni [(x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin B)]$

Example 15. *Let $A = \{n \in \mathbb{Z} | n = 3t - 2, t \in \mathbb{Z}\}$, $B = \{n \in \mathbb{Z} | n = 3t + 1, t \in \mathbb{Z}\}$. Prove that $A = B$.*

Proof. Let $n \in \mathbb{Z}$. It is sufficient to prove that $n \in A \Leftrightarrow n \in B$. Let $n \in A$. Then $n = 3t - 2$ for some $t \in \mathbb{Z}$. Hence $n = 3t - 2 = 3t - 2 - 1 + 1 = (3t - 3) + 1 = 3(t - 1) + 1 = 3s + 1$, where $s = t - 1 \in \mathbb{Z}$. So $n \in B$.

Let $n \in B$. Then $n = 3t+1$ for some $t \in \mathbb{Z}$. Hence $n = 3t+1 = 3t+1+2-2 = 3(t+1)-3 = 3s-2$, where $s = t + 1 \in \mathbb{Z}$. So $n \in A$. □

Cardinality

The cardinality of A, written $|A|$, is the number of elements in A.

4.2 Operations on Sets

Venn Diagrams

Venn diagrams are visual representations of sets (the universal set $\mathcal{U}$ is represented by a rectangle, and subsets of $\mathcal{U}$ are represented by regions lying inside of the rectangle).

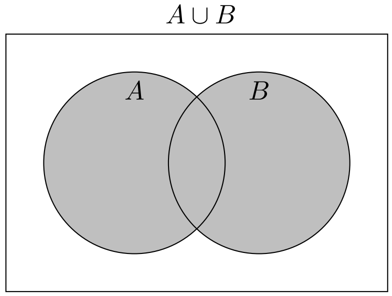
Definition 4.2.1. *Let A and B be sets in a universal set $\mathcal{U}$. The* ***union*** *of A and B, written $A \cup B$, is the set of all elements that belong to either A or B or both. Symbolically,*

$$A \cup B = \{x \in \mathcal{U} | x \in A \vee x \in B\}$$

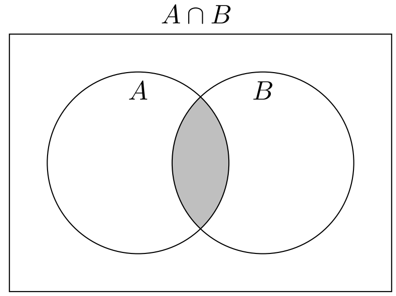
Definition 4.2.2. *Let A and B be sets in a universal set $\mathcal{U}$. The* ***intersection*** *of A and B, written $A \cap B$, is the set of all elements in common with A and B or both. Symbolically,*

$$A \cap B = \{x \in \mathcal{U} | x \in A \wedge x \in B\}$$

$A \cup B$

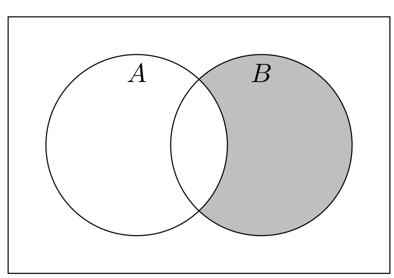


$A \cap B$



Definition 4.2.3. *Let A and B be sets in a universal set $\mathcal{U}$. The* ***complement of*** *A* ***in*** *B, denoted $B - A$, is*

$$B - A = \{x \in \mathcal{U} | x \in B \wedge x \notin A\}$$



set notation	$=$	$\subset, \subseteq$	$\cup$	$\cap$	-	$\emptyset$	$\mathcal{U}$
logical connectivity	$\Leftrightarrow$	$\Rightarrow$	$\vee$	$\wedge$	$\neg$	contradiction	tautology

Power Set

Definition 4.2.4. *Let A be a set. The power set of A, written $\mathcal{P}(A)$, is the following set,*

$$\mathcal{P}(A) = \{X | X \subseteq A\}$$

In other words, it is the set of all possible subsets of A.

$\mathcal{P}(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$

Cartesian Product

Definition 4.2.5. *Let A and B be sets. The* ***Cartesian product*** *of A and B, written $A \times B$, is the following set,*

$$A \times B = \{(a, b) | a \in A \wedge b \in B\}$$

Fundamental Properties of Sets

Theorem 4.2.6. *The following statements are true for all sets A, B, and C contained in a universal set $\mathcal{U}$.*

A. $A \cup B = B \cup A$ *(commutative)*

B. $A \cap B = B \cap A$ *(commutative)*

C. $(A \cup B) \cup C = A \cup (B \cup C)$ *(associative)*

D. $(A \cap B) \cap C = A \cap (B \cap C)$ *(associative)*

E. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributive)*

F. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(distributive)*

G. $\overline{A \cup B} = \bar{A} \cap \bar{B}$ *(DeMorgan's Law)*

H. $\overline{A \cap B} = \bar{A} \cup \bar{B}$ *(DeMorgan's Law)*

Proving Set Properties

Use the following tautologies:

- $x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B)$
- $x \in A \cup B \Leftrightarrow (x \in A \vee x \in B)$
- $x \in A - B \Leftrightarrow (x \in A \wedge x \notin B)$
- $(x, y) \in A \times B \Leftrightarrow (x \in A \wedge y \in B)$

Example 16. *Let A and B be subsets of a universal set $\mathcal{U}$. Prove that $(A - B) \cap B = \emptyset$.*

Proof. Let $x \in \mathcal{U}$. Assume, by contradiction, that $(A - B) \cap B \neq \emptyset$. Then there exists $x \in (A - B) \cap B$. Thus,

$$\begin{aligned} x \in (A - B) \cap B &\Rightarrow x \in ((A - B) \wedge x \in B) \\ &\Rightarrow (x \in A \wedge x \notin B) \wedge (x \in B) \\ &\Rightarrow x \in A \wedge (x \notin B \wedge x \in B) \\ &\Rightarrow x \notin B \wedge x \in B, \end{aligned}$$

a contradiction. □

Example 17. *Let A, B, C be subsets in a universal set $\mathcal{U}$. Prove that*

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

Proof. Let $x, y \in \mathcal{U}$. Then

$$\begin{aligned} (x, y) \in A \times (B \cup C) &\Leftrightarrow (x \in A) \wedge (y \in (B \cup C)) \\ &\Leftrightarrow (x \in A) \wedge (y \in B \vee y \in C) \\ &\Leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\ &\Leftrightarrow ((x, y) \in A \times B) \vee ((x, y) \in A \times C) \\ &\Leftrightarrow (x, y) \in (A \times B) \cup (A \times C) \end{aligned}$$

□

4.3 Arbitrary Unions and Intersections

Definition 4.3.1. *Let I be a set. An **indexed collection of sets** $\{A_\alpha\}_{\alpha \in I}$ represents a collection of sets that for every $\alpha \in I$, there is a corresponding set A_α. In this case we call I the **indexed set**.*

Collection of sets	Indexed set	Shortened notation
$A_0, A_1, A_2, A_3, \ldots, A_{2016}$	$I = \{0, 1, 2, 3, \ldots, 2016\}$	$\{A_\alpha\}_{\alpha \in I}$
$B_3, B_6, B_9, \ldots, B_77$	$J = \{3, 6, 9, \ldots, 77\}$	$\{B_\beta\}_{\beta \in J}$
$C_5, C_{10}, C_{15}, \ldots, C_{2015}$	$k = \{5t \mid 1 \leq t \leq 403,\ t \in \mathbb{Z}\}$	$\{C_i\}_{i \in k}$

Example 18. *Given $B_i = \{i, i+1\}$ for $i = 1, 2, \ldots, 10$.*

(a) $\bigcap_{i=1}^{10} = (B_1 \cap B_2) \cap B_3 \cap \cdots \cap B_{10} = (\{2\} \cap B_3) \cap (B_4 \cap \cdots \cap B_{10}) = \emptyset \cap (B_4 \cap \cdots \cap B_{10}) = \emptyset$

(b) $B_i \cap B_{i+1} = \{i, i+1\} \cap \{i+1, i+2\} = \{i+1\}$

Chapter 5

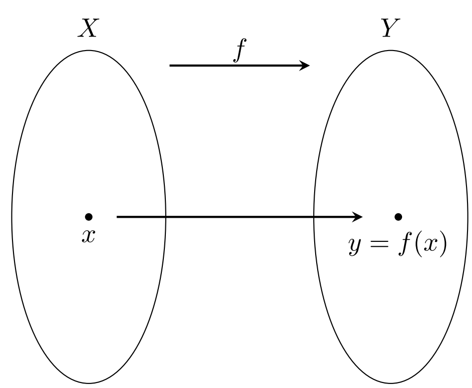
Functions

5.1 Definition and Basic Properties

Definition 5.1.1. *Let X and Y be nonempty sets. A **function** from the set X to the set Y is a correspondence that assigns to each element x in the set X one and only one element y in the set Y, which is denoted by $f(x)$.*

*We call X the **domain** of f and Y the **codomain** of f.*

*If $x \in X$ and $y \in Y$ are such that $y = f(x)$, then y is called the **value** of f at x, or the **image** of x under f. We may also say that f **maps** x to y. Using diagram,*



Definition 5.1.2. *Two functions f and g are **equal** if they have the same domain and the same codomain and if $f(x) = g(x)$ for all x in the domain.*

Definition 5.1.3. *The **graph** of $f : X \to Y$ is the set*

$$G_f = \{(x, y) \in X \times Y | y = f(x)\}$$

Some common functions

- **Identity function** $I_X : X \to X$ maps every element to itself,

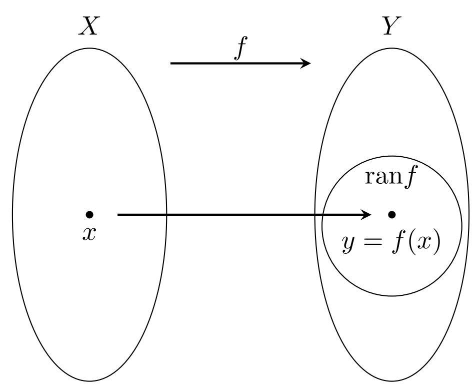
$$\forall x \in X,\ i_X(x) = x$$

- **Polynomial function** of degree n with real coefficients $a_0, a_1, \ldots, a_n$ is a function from $\mathbb{R}$ to $\mathbb{R}$:
$$P_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$
If $a_0 \neq 0$, then $\deg P_n(x) = n$.

Range (or Image) of a Function

Definition 5.1.4. *Let $f : X \to Y$ be a function. The* ***range*** *of f (also called the* ***image*** *of f) is the set*
$$\{y \in Y | y = f(x) \text{ for some } x \in X\}$$

We denote the range (or image) of the function f by $\operatorname{ran} f$ (or $\operatorname{Im} f$).



Example 19. *Let $f : [\frac{1}{3}, \infty] \to \mathbb{R}$ be defined by $f(x) = \sqrt{3x-1}$ and $S = \{y \in \mathbb{R} | y \geq 0\}$. Prove that $\operatorname{ran} f = S$.*

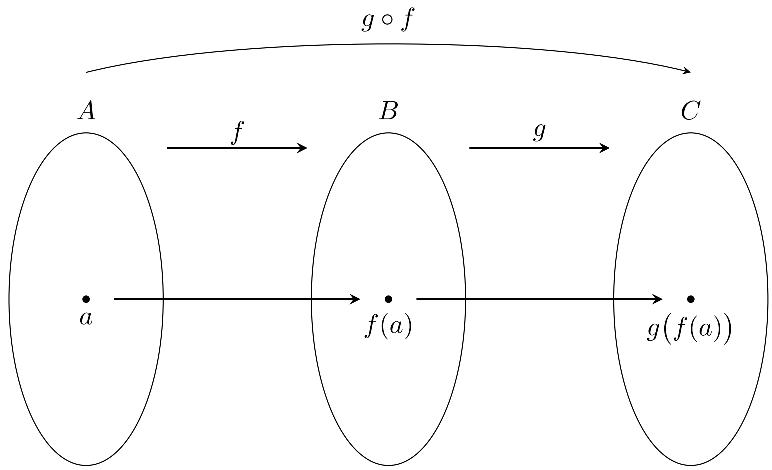
Proof. Let $y \in \operatorname{ran} f$. Then $y = f(x)$ for some $x \in [\frac{1}{3}, \infty]$. But $f(x) = \sqrt{3x-1}$, so $y = \sqrt{3x-1} \geq 0$ and hence $y \in S$. Thus $\operatorname{ran} f \subseteq S$.

Conversely, let $y \in S$. In order to show that $y \in \operatorname{ran} f$, we must find $x \in [\frac{1}{3}, \infty]$ such that $f(x) = y$. Indeed, if $x = \frac{y^2+1}{3}$ then $x \in [\frac{1}{3}, \infty]$ (because $y \in S \Rightarrow y \geq 0 \Rightarrow y^2 \geq 0 \Rightarrow y^2 + 1 \geq 1 \Rightarrow x = \frac{y^2+1}{3} \geq \frac{1}{3}$) and $f(x) = f(\frac{y^2+1}{3}) = \sqrt{3\left(\frac{y^2+1}{3}\right) - 1} = \sqrt{y^2+1-1} = \sqrt{y^2} = |y| = y$ (since $y \geq 0$). Thus $S \subseteq \operatorname{ran} f$. $\square$

5.2 Composition of Functions

Definition 5.2.1. *Let A, B, C be nonempty sets, and let $f : A \to B$, $g : B \to C$ be functions. we define a function*
$$g \circ f : A \to C$$
called the ***composition*** *of f and g, by*
$$(g \circ f)(a) = g(f(a))$$

Using diagram,



Example 20. *Let* $f, g : \mathbb{R} \to \mathbb{R}$ *be defined by* $f(x) = e^x$ *and* $g(x) = x\sin(x)$. *Find* $f \circ g$ *and* $g \circ f$.

Solution. First note that $f \circ g : \mathbb{R} \to \mathbb{R}$ and $g \circ f : \mathbb{R} \to \mathbb{R}$. Let $x \in \mathbb{R}$.

$$(f \circ g)(x) = f(g(x)) = f(x\sin(x)) = e^{x\sin(x)}$$
$$(g \circ f)(x) = g(f(x)) = g(e^x) = e^x \sin(e^x)$$

We conclude that $f \circ g \neq g \circ f$, so function composition is **not** commutative.

Proposition 5.2.2. *Let* $f : A \to B$, $g : B \to C$ *and* $h : C \to D$. *Then*

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Proof. First note that $(h \circ g) \circ f : A \to D$ and $h \circ (g \circ f) : A \to D$. Let $x \in A$. Then $((h \circ g) \circ f)(x) = h(g(f(x)))$ and $(h \circ (g \circ f))(x) = h(g(f(x)))$. $\square$

h

5.3 Surjective and Injective Functions

5.4 Invertible Functions

5.5 Functions and Sets