An Introduction to Proofs

Hassium, Fung San Gann, Tingyu Wu

Introduction

In higher-level mathematics, students need a certain level of "mathematical maturity" to understand and apply abstract ideas. However, there is no clear way to measure this maturity, nor a definitive method to teach someone how to write a proof. This note is intended to be a transition from high/middle school math to proof-based formal mathematics.

You may notice that we use different names for the same object—a common practice in mathematics. For example, the set of all real numbers $\mathbb{R}$ can be viewed as a set, a group, a ring, a field, a topological space, a metric space ... Each term highlights a particular aspect of the same structure. As Poincaré famously said, "Mathematics is the art of giving the same name to different things."

Many people have contributed to this short note. Special thanks to FSG, who wrote §6 and collaborated with me on a general topology note, which serves as an important reference for my writing in §7. Thanks to Tingyu Wu for collaborating on §4. Thanks to Bryce for his suggestions on §1 and §3.

Finally, think deeper and enjoy mathematics!

—— *Hassium*

1 Basic Logic

Logic is the formal framework and rules of inference that ensure the validity and coherence of arguments in math.

Remark. We shall accept that sentences can be either true or false. Moreover, we assume that every English sentence can be stated in symbolic logic form.

A *proposition* is a sentence that is either true or false in a mathematical system. The label "true" or "false" assigned to a proposition is called its *truth value*. We use the letters T and F to represent "true" and "false", respectively. An *axiom* is a proposition that is assumed to be true within a mathematical system without requiring proof. Axioms serve as the foundational building blocks of a mathematical theory, from which other propositions can be derived. A *theorem* is a proposition that has been proven to be true using logical reasoning and the accepted axioms and previously established theorems of the mathematical system. The proof demonstrates why the theorem must hold based on these foundations.

Consider the proposition "π is not a rational number", which is trivially true. However, we could always find some false companion of this proposition, such as "π is a rational number". Similarly, we can find a true companion of a false proposition. Let P be a proposition, such a companion of P is called the *negation* of P, denoted $\neg P$.

Let P and Q be propositions. Those sentences can be combined using the word "and", denoted $P \wedge Q$, and called the *conjunction* of P and Q. The proposition $P \wedge Q$ is true if both P and Q are true. We can combine the propositions by the word "or", denoted $P \vee Q$, and called the *disjunction* of P and Q. The proposition $P \vee Q$ is true if at least one of P or Q is true. A *truth table* is shown below.

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$
T	T	F	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	F

Two propositions P and Q are *logically equivalent* if they have the same truth value in every possible combination of truth values for the variables in the statements, denoted $P \equiv Q$.

Example. Let P be a proposition, then $P \equiv \neg(\neg P)$ is logically equivalent. To prove this statement, consider $\neg P$ as a proposition Q, then we obtain the following truth table.

P	$Q \equiv \neg P$	$\neg Q \equiv \neg(\neg P)$
T	F	T
F	T	F

Here P and $\neg Q$ has the same truth value in each case, so $P \equiv \neg(\neg P)$.

Problem 1.1. Let P, Q, and R be propositions. Consider the following statements:

1. $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$;
2. $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$.

Try to prove or disprove the statements.

Problem 1.2. Let P, Q, and R be propositions. Consider the following statements:

1. $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$;
2. $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$;
3. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

Try to prove or disprove the statements. Based on your results, can you find more properties?

Let P and Q be propositions. Consider the proposition "if n is a natural number, then $2n$ is an even number". Let P denotes "n is a natural number" and let Q denotes "$2n$ is an even number", then the sentence becomes "if P, then Q", denoted $P \implies Q$. This implication called a *conditional proposition*, P is called the *antecedent* and Q is called the *consequent*. The proposition $P \implies Q$ is true if P is true and Q is true. What if P is false? The answer arises from one's intuition.

Imagine your high school teacher say "if you didn't submit your homework, then you haven't completed it". How would you argue against this sentence? The most likely response would be, "I did the homework but I didn't submit it". Whether or not you submitted your homework does not affect the truth value of the implication.

You should be convinced by your own intuition. This case is called a *vacuous truth*. In the proposition $P \implies Q$, when P is false, $P \implies Q$ is true. The truth table of $P \implies Q$ is shown below.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Let P and Q be propositions, $(P \implies Q) \wedge (Q \implies P)$ is called a *biconditional proposition*, denoted $P \iff Q$. We will write this by "P is true if and only if Q is true".

Problem 1.3. Let P and Q be propositions, show $(\neg P \equiv \neg Q) \iff (P \equiv Q)$.

Example. Let P and Q be propositions. Consider the conditional proposition $P \implies Q$. It is false only if P is true and Q is false, that is, $\neg(P \implies Q) \equiv P \wedge (\neg Q)$. Now we take the negation of the right side, $\neg(P \wedge (\neg Q)) \equiv (\neg P) \vee (\neg(\neg Q)) \equiv (\neg P) \vee Q$.

Problem 1.4. Write down the truth table of a biconditional proposition. Based on your truth table and the previous example, try to find a proposition R by "$\vee$", "$\wedge$", and "$\neg$" such that $R \equiv (P \iff Q)$. If $P \iff Q$ is true, does $P \equiv Q$?

Problem 1.5. Let P, Q, R, and S be propositions. Rewrite $P \implies (Q \implies (R \implies S))$ by '$\vee$", "$\wedge$", and "$\neg$". What is the negation of this sentence?

Problem 1.6. Let P, Q, and R be propositions. Try to prove or disprove $P \implies (Q \vee R) \equiv (\neg P) \vee Q \vee R$. What about $P \implies (Q \wedge R)$?

Given a proposition $P \implies Q$, the *converse* is defined as $Q \implies P$ and the *contrapositive* is defined as $(\neg Q) \implies (\neg P)$. The truth table is shown below, and it suffices to conclude that $(P \implies Q) \equiv (\neg Q \implies \neg P)$.

P	Q	$P \implies Q$	$Q \implies P$	$\neg Q \implies \neg P$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Problem 1.7. Let P and Q be propositions, when does $(P \implies Q) \equiv (Q \implies P)$?

Let P be the proposition "x is a natural number". Here x is a *variable*, and the truth value of this proposition depends on x. For instance, if $x = 1$, then P is true; if $x = 0.86$, then P is false. A *propositional function* is a family of propositions depending on one or more variables. The collection of permitted variables is the *domain*. Now we write $P(x)$ instead of P, so $P(1)$ is true and $P(0.86)$ is false.

Problem 1.8. Let x be a variable and let x be a natural number. Give a proposition $P(x)$ such that $P(x)$ is true when $x \leq 2024$ and false when $x \geq 2025$.

Propositional functions are often quantified. The *universal quantifier* is denoted by "$\forall$", and the proposition $\forall x(P(x))$ is true if and only if $P(x)$ is true for every x in its domain. The *existential quantifier* is denoted by "$\exists$", and the proposition $\exists x(P(x))$ is true if and only if $P(x)$ is true for at least one x in its domain. Consider the proposition $\forall x(P(x))$, this means all x make $P(x)$ true, so there does not exist some x such that $P(x)$ is false, which is $\neg(\exists x(\neg P(x)))$.

Example. Let $P(x)$ be a proposition, then $\neg(\forall x(P(x))) \iff \neg(\neg(\exists x(\neg P(x)))) \iff \exists x(\neg P(x))$.

Problem 1.9. Let $P(x)$ be a proposition, show that $\neg(\exists x(P(x))) \iff \forall x(\neg P(x))$.

The order of quantifiers does matter the meaning of a proposition. Consider the proposition "for all natural number x, there exists a natural number y such that $y > x$". Pick some x, let $y = x+1$, then $y > x$ and y is a natural number, so the proposition is true. However, switching the order of quantifiers gives "there exists a natural number y, for all natural number x, $y > x$". Suppose there exists such y, then $y+1$ is a natural number, so let $x = y+1$, it is trivial that $y < x$, hence the proposition is false.

Example. Let $P(x)$ and $Q(y)$ be propositions. Consider the proposition $\forall x(\exists y(P(x) \vee Q(y)))$. To find its negation, let $R(x) \equiv \exists y(P(x) \vee Q(y))$, now the negation becomes $\exists x(\neg R(x))$. Since P only depends on x, let $S(y) \equiv (P(x) \vee Q(y))$, then we have $\exists x(\neg(\exists y(S(y)))) \equiv \exists x(\forall y(\neg S(y))) \equiv \exists x(\forall y(\neg(P(x) \vee Q(y)))) \equiv \exists x(\forall y((\neg P(x)) \wedge (\neg Q(y))))$.

Problem 1.10. Let $P(x, y, z)$ be a proposition, consider the following propositions.

1. $Q(x, y, z) \equiv \exists x(\forall y(\forall z(P(x, y, z))))$;
2. $R(x, y, z) \equiv \forall x(\exists y(\forall z(P(x, y, z))))$;
3. $S(x, y, z) \equiv \forall x(\forall y(\exists z(P(x, y, z))))$.

What are the negations of those propositions? What is the negation of $Q \vee (R \wedge S)$?

Example. Let $P(x)$ and $Q(x)$ be propositions. Consider the negation of $P(x) \implies Q(x)$, $\neg(P(x) \implies Q(x)) \equiv \neg((\neg P(x)) \vee Q(x)) \equiv P(x) \wedge (\neg Q(x)) \equiv \forall x(P(x) \wedge (\exists x(\neg Q(x)))) \equiv \exists x(P(x) \wedge (\neg Q(x)))$. Notice that taking the negation brings an existential quantifier.

In the following sections, we shall assume readers are familiar with basic logic and use it as a tool to understand or prove propositions. Several expressions and their "translations" are shown below.

$P \implies Q$	$P \iff Q$
P implies Q; if P, then Q	P if and only if Q
P is sufficient for Q; Q is necessary for P	P is necessary and sufficient for Q

Problem 1.11. Given the following propositions, analyze their structures.

1. the number $\sqrt{2}$ is not a rational number;
2. if x is a natural number, then x is an integer;
3. for all natural number x, for all rational number y with $x < y < x + 1$, there exists a real number z such that $y < z < y + 1$ and z is irrational;
4. given a sequence (x_n) of real numbers, we say (x_n) converges to a real number L if, for all real number $\epsilon > 0$, there exists a real number N such that, for all natural number n, $n > N$ implies $|x_n - L| < \epsilon$.

Find the negation of each proposition.

2 Some Axioms of Sets

In this section, we begin investigating sets, the most basic entities in mathematics. It is natural to ask: What is a set? There is no precise definition of sets. Intuitively, a *set* is a collection of objects that satisfy some property, and the objects are called *elements*.

Remark. This note is based on the ZFC set theory. In this system, every object is a set and we allow sets of sets. From now on, assume that there exists a set.

If S is a set and x is an element in S, then we say x belongs to S, denoted $x \in S$. If x does not belong to S, then we write $x \notin S$. If S has no element, then we call it an *empty set*, denoted $\varnothing$.

Axiom of empty set. There exists an empty set.

Axiom of extensionality. Two sets A and B are equal if and only if they have the same elements.

Axiom schema of separation. If P is a property, then for any set X there exists a set $Y = \{x \in X \mid P(x)\}$.

Elements determine a set. One way to describe a set is to explicitly list the elements. For example, we can write a set $S = \{6, 7, 8\}$. Another way is to express the elements by the properties they satisfy.

Example. Here are several examples of sets.

1. the set $S = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$ has three elements;
2. the set $\{2n \mid n \in \mathbb{N}\}$ is the set of all even numbers, where $\mathbb{N}$ is the set of natural numbers;
3. the set $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$ is the set of rational numbers, where $\mathbb{Z}$ is the set of integers.

We shall provide constructions for $\mathbb{N}$ and $\mathbb{Z}$ later.

Problem 2.1. Write out the set of all positive integers and the set of all prime numbers.

Definition 2.1. Let S be a set. A set R is a *subset* of S, denoted $R \subset S$, if for all $x \in R$, $x \in S$. If there exists some $x \in S$ such that $x \notin R$, then R is called a *proper subset* of S, denoted $R \subsetneq S$.

It suffices to check that axiom schema of separation guarantees that subsets are sets.

Remark. Some textbooks use "$\subseteq$" for subsets and "$\subset$" for proper subsets.

Remark. From now on, try to vertify whether those constructions are actually sets.

Proposition. Let A be a set, then $A \subset A$.

Proof. For all $x \in A$, $x \in A$, so $A \subset A$. $\square$

Proposition. Let X and Y be sets, then $X = Y$ if and only $X \subset Y$ and $Y \subset X$.

Remark. For a biconditional proposition $P \iff Q$, we use the notation "($\Rightarrow$)" in the proof to show $P \implies Q$ and "($\Leftarrow$)" for $Q \implies P$.

Proof. Let X and Y be sets. ($\Rightarrow$) For all $x \in X$, since $X = Y$, $x \in Y$, so $X \subset Y$. For all $y \in Y$, since $X = Y$, $y \in X$, so $Y \subset X$. ($\Leftarrow$) Suppose $X \neq Y$. If $X \subset Y$, then there exists $a \in Y$ such that $a \notin X$, so $X \not\subset Y$, a contradiction. $\square$

Proposition. Let A be any set, then $\varnothing \subset A$.

Proof. Suppose $\varnothing \not\subset A$, then there exists $x \in \varnothing$ such that $x \notin A$, since $x \in \varnothing$ is false, contradiction. $\square$

Problem 2.2. Prove that a set is independent of the order of its elements. For example, $\{1, 2, 3\} = \{3, 2, 1\}$.

Problem 2.3. If X, Y, and Z are sets such that $X \subset Y$ and $Y \subset Z$, prove that $X \subset Z$.

Problem 2.4. List all the subsets of $X = \{1, 2, 3\}$, $Y = \{1, 2, 3, 4\}$, and $Z = \{1, \{1, 2\}, \{2, 1\}, 3\}$.

To construct more complex structures, we need an order between objects.

Axiom of pairing. For two objects a and b, there exists a set $\{a, b\}$ containing exactly a and b.

Definition 2.2. Let a and b be some objects. An *ordered pair* (a, b) is defined as the set $\{\{a\}, \{a, b\}\}$.

Problem 2.5. Show that an ordered pair is indeed a set.

Proposition. Let (a, b) and (c, d) be ordered pairs, then $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Proof. We have $(a, b) = \{\{a\}, \{a, b\}\}$ and $(c, d) = \{\{c\}, \{c, d\}\}$. ($\Rightarrow$) Suppose $a \neq c$, then $\{a\} \neq \{c\}$. If $\{a\} = \{c, d\}$, then $c = d = a$, a contradiction. Suppose $b \neq d$. If $a = c$, then $\{a\} = \{c\}$ and $\{a, b\} \neq \{c, d\}$, a contradiction. ($\Leftarrow$) If $a = c$ and $b = d$, then $\{a, b\} = \{c, d\}$ and $\{a\} = \{c\}$, hence $(a, b) = (c, d)$. $\square$

The definition of ordered pairs can be extended to multiple elements. We call $(a_1, \dots, a_n)$ a *n-tuple*.

Problem 2.6. Prove that $\{a\} = \{a, a\}$. A set with one element is called a *singleton*.

Problem 2.7. Write out the definition to n-tuples, where n is a positive integer.

Axiom of union. For all set X, there exists a set $Y = \bigcup X$, the union of all elements of X.

Definition 2.3. Let A and B be sets. The *union* of A and B is the set $\{x \mid x \in A \text{ or } x \in B\}$, denoted $A \cup B$. The *intersection* of A and B is the set $\{x \mid x \in A \text{ and } x \in B\}$. We say A and B are *disjoint* if $A \cap B = \varnothing$. The *complement* of A in B is the set $\{x \mid x \in B \text{ and } x \notin A\}$, denoted $B \setminus A$.

Problem 2.8. Let A and B be sets. Prove that $A \cup B$, $A \cap B$, and $A \setminus B$ are sets based on the axioms.

Proposition. Let A and B be sets, then $A \cup B = B \cup A$.

Proof. For all $x \in A \cup B$, if $x \in A$, then $x \in B \cup A$; if $x \in B$, then $x \in B$, hence $A \cup B = B \cup A$. $\square$

Problem 2.9. Let A, B, and C be sets. Prove the following propositions.

1. $A \cap B = B \cap A$;
2. $A \cup (B \cup C) = (A \cup B) \cup C$;
3. $A \cap (B \cap C) = (A \cap B) \cap C$;
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Theorem 2.1 (De Morgan's law)**.** Let A, B, and C be sets, then $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$ and $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

Proof. Let $x \in C \setminus (A \cap B)$, then $x \in C$ and $x \notin A \cap B$, that is, $x \notin A$ and $x \notin B$. If $x \notin C \setminus A$, then $x \notin A$, so $x \notin B$ and $x \in C \setminus B$. Hence $C \setminus (A \cap B) \subset (C \setminus A) \cup (C \setminus B)$. Now let $x \in (C \setminus A) \cup (C \setminus B)$, then $x \in C$ and $x \notin A$ or $x \notin B$, so $x \notin A \cap B$, that is, $x \in C \setminus (A \cap B)$, hence $(C \setminus A) \cup (C \setminus B) \subset C \setminus (A \cap B)$. The proof of the second part is left as an exercise. □

Some texts assume the existence of an "universal set", denoted U, which has all objects as elements including itself, so we can define complements of any set S as the set $U \setminus S$. However, this assumption leads to a paradox. Consider the set S, defined as the set of all sets that are not members of themselves, that is, $S = \{X \mid X \notin X\}$. Does S belong to S? This is known as Russell's Paradox. Assume $S \in S$, then by the definition of S, $S \in S$ implies $S \notin S$, a contradiction. Assume $S \notin S$, then $S \in S$. This is also a contradiction. Thus, the existence of such a set S leads to a logical inconsistency.

Definition 2.4. Let X be a set, and let the *successor* of X be $X^+ = X \cup \{X\}$. A set S is called an *inductive set* if $\varnothing \in S$ and for all $X \in S$, $X^+ \in S$.

Axiom of infinity. There exists an inductive set.

Proposition. The intersection of two inductive sets is an inductive set.

Proof. Let A and B be inductive sets, then $\varnothing \in A \cap B$. For all $S \in A \cap B$, $S \in A$ and $S \in B$. Since A and B are inductive, $S^+ \in A$ and $S^+ \in B$, hence $A \cap B$ is inductive. □

Definition 2.5. The set of all *natural numbers*, denoted $\mathbb{N}$, is the intersection of all inductive sets.

We denote $0 = \varnothing$, $1 = 0^+$, $2 = 1^+$, ...

Problem 2.10. Prove that the set of all natural numbers is a subset of any inductive set.

Axiom of power set. For any X there exists a set consisting of all subsets of X.

Definition 2.6. Given a set X, the set of all subsets of X is called its *power set*, denoted $\mathscr{P}(X)$.

Example. Let $X = \{a, b\}$, the power set $\mathscr{P}(X) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$.

Definition 2.7. Let X and Y be sets. The *Cartesian product* $X \times Y$ is the set of all ordered pairs (a, b), where $a \in X$ and $b \in Y$.

Problem 2.11. Let X and Y be sets. Write out the set $\mathscr{P}(\mathscr{P}(X \cup Y))$. Prove that $X \times Y = \{z \in \mathscr{P}(\mathscr{P}(X \cup Y)) \mid$ there exists $x \in X$ and $y \in Y$ such that $z = (x, y)\} \subset \mathscr{P}(\mathscr{P}(X \cup Y))$, hence $X \times Y$ is a set.

Problem 2.12. Let S be a set, prove that $S \subsetneq \mathscr{P}(S)$.

Problem 2.13. Let A, B, and C be sets. Prove the following propositions.

1. $A \times B = B \times A$ if and only if $A = B$;
2. $A \times (B \times C) = (A \times B) \times C$;
3. $(A \cup B) \times C = (A \times C) \cup (B \times C)$;

4. $(A \cap B) \times C = (A \times C) \cap (B \times C)$;
5. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

Definition 2.8. The *disjoint union* of two sets A and B, denoted $A \amalg B$, is the set $A \amalg B = (A \times \{0\}) \cup (B \times \{1\})$.

Problem 2.14. Let A and B be sets, prove that $A \amalg B$ is a set.

Definition 2.9. A *binary operation* R is a set of ordered pairs. If $(x, y) \in R$, we write xRy. The *domain* of R is the set $\operatorname{dom}(R) = \{u \mid \text{there exists } v \text{ such that } (u, v) \in R\}$. The *range* of R is the set $\operatorname{ran}(R) = \{v \mid \text{there exists } u \text{ such that } (u, v) \in R\}$.

It suffices to show a binary operation is indeed a set. Let R be a binary operation, then $R \subset X \times Y$ for some sets X and Y. By the axiom schema of separation, R is a set.

Problem 2.15. Let R be a binary operation. Prove that $\operatorname{dom}(R), \operatorname{ran}(R) \subset \bigcup(\bigcup R)$, hence, by axiom of union, $\operatorname{dom}(R)$ and $\operatorname{ran}(R)$ are sets.

Definition 2.10. Let R be a binary operation on a set S, that is, $R \subset S \times S$. We say R is an *equivalence relation* if the following properties hold.

1. For all $a \in X$, aRa. (reflexive)
2. If aRb, then bRa. (symmetric)
3. If aRb and bRc, then aRc. (transitive)

For all $a \in A$, the set $S_a = \{b \mid aRb\}$ is the *equivalence class* of a.

Problem 2.16. Prove that an equivalence class is a set.

Problem 2.17. Prove that $=$ is an equivalence relation in $\mathbb{N}$.

Problem 2.18. Let R be a binary operation on a set X. For all $a, b \in A$, prove that $S_a \cap S_b$ is either $\varnothing$ or S_a. Prove that $\bigcup S_a = X$, where each pair of S_a are disjoint.

Definition 2.11. Let $\leq$ be a binary relation on a set X. We say $\leq$ is a *partial ordering* if the following conditions hold:

1. for all $x \in X$, $x \leq x$;
2. for all $x, y \in X$, $x \leq y$ and $y \leq x$ implies $x = y$;
3. for all $a, b, c \in X$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

The set with a partial ordering is called a *partially ordered set*.

Definition 2.12. A partially ordered set $(X, \leq)$ is *linearly ordered* if for all $p, q \in X$, either $p \leq q$ or $q \leq p$.

Example. The set of natural numbers $\mathbb{N}$ forms a linearly ordered set in set inclusions.

Proposition. Let $(X, \leq)$ be a partially ordered set and let $Y \subset X$, then Y is partially ordered.

Proof. For all elements $a, b, c \in Y$, $a, b, c \in X$, so Y inherits the partial ordering of X. $\square$

Problem 2.19. Let $(X, \leq)$ be a partial ordered set, prove that $\leq$ is not an equivalence relation.

Problem 2.20. Let $(X, \leq)$ be a linearly ordered set and let $Y \subset X$, prove that Y is linearly ordered.

Problem 2.21. Let X be a set. If $(\mathscr{P}(X), \subset)$ is a linearly ordered set, prove that X is either a singleton or the empty set.

Definition 2.13. Let $(X, \leq)$ be a partially ordered set and let $Y \subset X$ be an nonempty subset. An element a is the *upper bound* of X if for all $x \in X$, $x \leq a$. An element b is the *lower bound* of X if for all $x \in X$, $b \leq x$. The least upper bound of X is called the *supremum* and the greatest lower bound of X is called the *infimum*.

Definition 2.14. Let $(X, \leq)$ be a partially ordered set. The set is *well-ordered* if for every nonempty subset S of X, there exists $a \in S$ such that for all $s \in S$, $a \leq s$.

Theorem 2.2 (well-ordering principle)**.** The natural numbers $\mathbb{N}$ is well-ordered.

The well-ordering principle is equivalent to the axiom of choice, which will be discussed later. You may assume the well-ordering principle is correct for now.

Theorem 2.3 (finite induction)**.** Given a subset $S \subset \mathbb{N}$ of the natural numbers with $0 \in S$ and $n \in S$ implies $n+1 \in S$, then $S = \mathbb{N}$.

Proof. Suppose $S \neq \mathbb{N}$, then $X = \mathbb{N} \setminus S$ is a nonempty set. By the well-ordering principle, X has a smallest element. Since $0 \in S$, $0 \notin X$, so the minimal element of X can be written in the form $k+1$, where $k \in \mathbb{N}$. Recall that $k+1 = k^+ = k \cup \{k\}$ is the successor of $k \in \mathbb{N}$, since $k+1$ is the smallest element, $k \notin X$, so $k \in S$. Now we have $k \in S$ and $k+1 \notin S$, a contradiction. $\square$

Example. Consider the statement: let $n \in \mathbb{N}$, show that $\sum_{i=0}^{n} = (n(n+1))/2$. If $n = 0$, then the equation trivially holds. Assume $\sum_{i=0}^{k} = (k(k+1))/2$ holds for some $k \in \mathbb{N}$, then $\sum_{i=0}^{k+1} = (k(k+1))/2 + (k+1) = ((k+1)(k+2))/2$. Hence, by induction, $\sum_{i=0}^{n} = (n(n+1))/2$ for all $n \in \mathbb{N}$.

Problem 2.22. Prove that given a subset $S \subset \mathbb{N}$ of the natural numbers with $0 \in S$ and $\{0, 1, \ldots, n\} \subset S$ implies $n+1 \in S$, then $S = \mathbb{N}$. This is known as the complete finite induction.

Problem 2.23. Prove that complete finite induction, finite induction, and well-ordering principle are equivalent.

3 Functions

Definition 3.1. Let X and Y be sets. A *function* f is a binary operation $f \subset X \times Y$ such that for all $x \in X$, there exists a unique $y \in Y$ such that $(x, y) \in f$. We say f is a function from X to Y, denoted $f : X \to Y$. The set Y is called the *codomain* of f, denoted $\mathrm{cod}(f)$.

Definition 3.2. Let $f : X \to Y$ be a function, the *image* of X under f, denoted $\mathrm{im}(f)$, is the range of f. For all $(x, y) \in f$, we write $f(x) = y$. The *preimage* of Y under f, denoted $f^{-1}(Y)$, is the set $\{x \mid x \in X \text{ and } f(x) \in Y\}$. Two functions f and g are the same if $\mathrm{dom}(f) = \mathrm{dom}(g)$, $\mathrm{cod}(f) = \mathrm{cod}(g)$, and for all $x \in \mathrm{dom}(f)$, $f(x) = g(x)$.

Example. Here are some examples of functions.

1. $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n^+$, where $n \in \mathbb{N}$, is a function.
2. $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ defined by $f(x) = (x, x)$, where $x \in \mathbb{R}$, is a function.

Problem 3.1. Let f be a function, prove that $\mathrm{ran}(f) \subset \mathrm{cod}(f)$.

Problem 3.2. Verify whether the following binary operations are functions.

1. $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = \sqrt{x}$ for all $x \in \mathbb{R}$.
2. $f : \{1, 2, 3\} \to \{2, 3\}$ with $f = \{\{1, 2\}, \{2, 2\}, \{3, 2\}\}$.
3. $f : \mathbb{N} \to \mathbb{Q}$ with $f(x) = x^4 - x^2$ for all $x \in \mathbb{N}$.
4. $f : \mathbb{Q} \to \mathbb{Z}$ with $f(x) = |x|$ for all $x \in \mathbb{Q}$.

Definition 3.3. Let $f : X \to Y$ and $g : Y \to Z$ be functions. The *composition* of f and g, denoted $g \circ f$, is defined as $g \circ f : X \to Z$ with $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

Problem 3.3. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Prove that $g \circ f$ is a well-defined function.

Proposition. The composition of functions is associative, that is, for all $f : X \to Y$, $g : Y \to Z$, and $h : Z \to S$, $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof. For all $x \in X$, $(h \circ g \circ f)(x) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. $\square$

Consider a diagram, where every vertex is an object and every arrow preserves the structure of those objects. Such a diagram is said to be *commutative* if all paths between two vertices are equivalent. In this section, every vertex is a set and every arrow is a function.

Example. Consider the following diagrams.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\ & C \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\varphi"'] \arrow[dr, "h"] & B \arrow[d, "g"] \\ D \arrow[r, "\psi"'] & C \end{tikzcd}$$

The left diagram is commutative if $g \circ f = h$. The right diagram is commutative if $g \circ f = h$ and $\psi \circ \varphi = h$.

Problem 3.4. Let $f : S_1 \times S_2 \to S_3$ be a function. We say f is commutative as a composition if $f(a, b) = f(b, a)$. Similarly, f is associative as a composition if $f(f(a, b), c) = f(a, f(b, c))$. Prove that if f is commutative, then $S_1 = S_2$. Prove that if f is associative, then the following diagram commutes.

$$\begin{tikzcd} S_1 \times S_2 \times S_3 \arrow[r, "f"] \arrow[d, "g : S_2 \times S_3 \to S_5"'] & S_4 \times S_3 \arrow[d] \\ S_5 \arrow[r] & S_6 \end{tikzcd}$$

Definition 3.4. A function $f : X \to Y$, where $X, Y \subset \mathbb{R}$, is said to be an *odd function* if for all $x \in X$, $f(x) = -f(-x)$. The function f is said to be an *even function* if for all $x \in X$, $f(x) = f(-x)$.

Example. Here are some examples of odd and even functions.

1. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ for all $x \in \mathbb{R}$ is even.
2. The function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x$ for all $x \in \mathbb{R}$ is odd.
3. The function $0 : \mathbb{R} \to \mathbb{R}$ defined by $0(x) = 0$ for all $x \in \mathbb{R}$ is both odd and even.

Proposition. Any function $f : X \to Y$, where $X, Y \subset \mathbb{R}$, can be written as $f = \varphi + \psi$, where φ is an odd function and ψ is an even function.

Proof. For all $x \in X$, define $\varphi = (f(x) - f(-x))/2$ and $\psi = (f(x) + f(-x))/2$, then $\varphi(-x) = (f(-x) - f(x))/2 = -\varphi(x)$ and $\psi(-x) = (f(-x) + f(x))/2 = \psi(x)$. Moreover, $\varphi(x) + \psi(x) = (f(x) - f(-x) + f(x) + f(-x))/2 = f(x)$. $\square$

Problem 3.5. Write a function $f : \mathbb{R} \to \mathbb{R}$ that is neither odd nor even. Decompose f as a sum of an even and an odd function.

Problem 3.6. Prove that such decomposition for each $f : X \to Y$, where $X, Y \subset \mathbb{R}$, is unique.

Definition 3.5. Let $f : A \to B$ be a function. We say f is *injective* if for all $x, y \in B$ and $x = y$, then $f^{-1}(x) = f^{-1}(y)$. We say f is *surjective* if $\operatorname{ran}(f) = \operatorname{cod}(f)$. The function f is said to be *bijective* if it is both injective and surjective.

Problem 3.7. State an example if such a function exists.

1. $f : \{1, 2, 3\} \to \{4, 5, 6\}$ that is injective but not surjective.
2. $f : \{1, 2, 3\} \to \{4, 5, 6\}$ that is surjective but not injective.
3. $f : \mathbb{R} \to \mathbb{R}$ that is injective but not surjective.
4. $f : \mathbb{R} \to \mathbb{R}$ that is surjective but not injective.
5. $f : \mathbb{R} \to \{1, 2, 3\}$ that is injective but not surjective.

6. $f : \mathbb{R} \to \{1, 2, 3\}$ that is surjective but not injective.

Proposition. The composition of two surjective functions is surjective.

Proof. Let $f : A \to B$ and $g : B \to C$ be surjective functions, then $\operatorname{ran}(f) = \operatorname{cod}(f) = B$ and $\operatorname{ran}(g) = \operatorname{cod}(g) = C$. For all $x \in C$, $g^{-1}(x) \in B$ and $f^{-1}(g^{-1}(x)) \in A$, so $C \subset \operatorname{ran}(g \circ f)$, hence $g \circ f$ is surjective. $\square$

Problem 3.8. Let $f : X \to Y$ be a surjective function. Prove that there exists an injective function $g : Y \to X$.

Problem 3.9. Let f and g be functions. Prove or disprove the following statements.

1. If f and g are injective, then $f \circ g$ is injective.
2. If f and g are bijective, then $f \circ g$ is bijective.
3. If f is surjective and g is injective, then $f \circ g$ is injective.

Problem 3.10. Let S be a set. Prove that there does not exist a surjective function $f : S \to \mathscr{P}(S)$.

Definition 3.6. A set S is said to be *finite* if there exists a bijective function $f : S \to n$, where $n \in \mathbb{N}$. The *cardinality* of S, denoted $|S|$, is the number n. If S is not finite, we say S is *infinite*.

Problem 3.11. Let S and X be finite sets with $|S| = |X|$. Let $f : S \to X$ be a function. Prove that if f is injective, then f is surjective. Does the converse hold?

Definition 3.7. Let $f : X \to Y$ be a function. Let $Z \subset X$, then the *restriction* of f onto Z is the map $f|_Z : Z \to Y$ defined by $f|_Z(z) = f(z)$ for all $z \in Z$.

Definition 3.8. Let A be a set. The *identity function*, denoted id_A, is the function $\mathrm{id}_A(x) = x$ for all $x \in A$.

Problem 3.12. Let $f : A \to B$ be a function, prove that $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$.

Definition 3.9. Let $f : A \to B$ be a function. The function $g : B \to A$ is a *left inverse* of f if $g \circ f = \mathrm{id}_A$. The function $h : B \to A$ is a *right inverse* of f if $f \circ h = \mathrm{id}_B$. A function φ is called an *inverse* of f if it is both a left inverse and a right inverse of f.

Proposition. Let f be a function. If g is an inverse of f, then g is unique.

Proof. Suppose g and h are inverses of f, then $h = h \circ f \circ g = (h \circ f) \circ g = g$. $\square$

Problem 3.13. Let f be a function with a left inverse g. Prove that if f has a right inverse, then the right inverse is g, conclude that g is the inverse of f.

Problem 3.14. Prove that a function has a left inverse if and only if it is injective. Prove that a function has a right inverse if and only if it is surjective, conclude that a function is bijective if and only if it has an inverse.

Definition 3.10. A *category* $\mathtt{C}$ consists of

1. a collection, denoted $\mathrm{Ob}(\mathtt{C})$, of *objects*;
2. for each pair of objects (X, Y), there exists a collection $\mathrm{Hom}_{\mathtt{C}}(X, Y)$ of *morphisms* from X to Y;
3. a *composition operation*, which gives, for each pair of morphisms $f : X \to Y$ and $g : Y \to Z$, a morphism $g \circ f : X \to Z$.

such that

1. given any $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$, we have the identity $(h \circ g) \circ f = h \circ (g \circ f)$;
2. for each object X, there exists a morphism $\mathrm{id}_X : X \to X$ with the property that $f \circ \mathrm{id}_X = f$ and $\mathrm{id}_X \circ g = g$ for any $f : X \to Y$ and $g : Z \to X$.

Let sets be objects, let functions be morphisms, and let the composition of morphisms be the composition of functions. By our previous observations, it suffices to check this defines a category of sets, denoted `Set`.

Example. Let X be a set, then $\mathrm{Hom}_{\mathtt{Set}}(X, X)$ is a category.

Example. In the following diagram, each vertex is an object and each arrow is a morphism. This defines a category.

$$\begin{tikzcd} \bullet \arrow[loop above] \arrow[r, shift left] & \bullet \arrow[loop above] \arrow[l, shift left] \end{tikzcd}$$

Problem 3.15. Morphisms are not guaranteed to be functions. Let $(S, \leq)$ be a partially ordered set. Let $\mathrm{Ob}(\mathtt{C}) = S$ and $x \to y$ be a morphism if $x \leq y$. Prove that $\mathtt{C}$ is a category.

Problem 3.16. Let $\mathtt{C}$ be a category. Let a system $\mathtt{C}^{\mathtt{op}}$ consists of all objects in $\mathtt{C}$ and all morphisms $f : A \to B$ if $B \to A$ is a morphism in $\mathtt{C}$. Prove that $\mathtt{C}^{\mathtt{op}}$ is indeed a category. This is called the *dual category* of $\mathtt{C}$.

Definition 3.11. Let $\mathtt{C}$ be a category. A morphism $f : A \to B$ is a *monomorphism* if for all $g, h : C \to A$, $f \circ g = g \circ h$ implies $g = h$. A morphism $f : A \to B$ is called an *epimorphism* if for all $i, j : B \to D$, $i \circ f = j \circ f$ implies $i = j$.

Problem 3.17. Prove that an injective function is a monomorphism in $\mathtt{Set}$. Prove that a surjective function is an epimorphism in $\mathtt{Set}$.

Definition 3.12. Let $\mathtt{C}$ be a category. A morphism $f : A \to B$ is an *isomorphism* if there exists $g \in \mathrm{Hom}_{\mathtt{C}}(B, A)$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. If there exists a morphism between two objects A and B, then we say they are *isomorphic*, denoted $A \approx B$.

Definition 3.13. Let $\sim$ be an equivalence relation on a set X. The *quotient set*, denoted $X_\sim$, is the set $\{[x] \mid x \in X\}$.

Example. Let $S = \{a, b, c, d\}$. Let $\sim$ be an equivalence relation on S such that $a \sim b$ and $c \sim d$. The quotient set $S_\sim$ is $\{a, c\}$.

Problem 3.18. Consider the set of all integers $\mathbb{Z}$. Fix $n \in \mathbb{Z}$, Let $\sim_n$ be an equivalence relation on $\mathbb{Z}$ such that $a \sim_n b$ if and only if $a - b = kn$ for some $k \in \mathbb{Z}$. Prove that $\sim_n$ is indeed an equivalence relation. Find the quotient set $\mathbb{Z}_{\sim_2}$. Find the quotient set $\mathbb{Z}_{\sim_n}$ for all n.

Definition 3.14. Let X and Y be sets. Let $\sim$ be an equivalence relation on X. A function $f : X \to Y$ is *invariant* under the equivalence relation such that, $x \sim y$ if and only if $f(x) = f(y)$.

Problem 3.19. Let X be a set and let $\sim$ be an equivalence relation on X. Prove that $\pi : X \to X_\sim$ defined by $x \mapsto [x]$ is a well-defined surjective function. Prove it is invariant under $\sim$.

Proposition. Let $f : X \to Y$ be a function, then f is an invariant fuction under some equivalence relation on X.

Proof. Define $\sim$ on X by $x \sim y$, where $x, y \in X$, if and only if $f(x) \sim f(y)$. For all $x = y$, $f(x) = f(y)$. For all $x = y = z$, $f(x) = f(y) = f(z)$. Hence $\sim$ is a well-defined equivalence relation on X, and f is trivially invariant under $\sim$. □

Universal property for quotient sets. Let X and Y be sets. Let $\sim$ be an equivalence relation on X and let $f : X \to Y$ be invariant under the equivalence relation. Then there exists a unique function $\bar{f} : X_\sim \to Y$ such that $f = \bar{f} \circ \pi$.

$$\begin{tikzcd} X_\sim \arrow[dr, dashed, "\bar{f}"'] & X \arrow[l, "\pi"'] \arrow[d, "f"] \\ & Y \end{tikzcd}$$

The proof of the universal property has two parts. We first verify that a quotient set has the universal property. Then we verify that a quotient set is characterized by this universal property, that is, any set satisfying the universal property must be a quotient set. This proof will be separated into multiple propositions.

Proposition. There exists a map $\overline{f} : X_\sim \to Y$ such that $f = \overline{f} \circ \pi$.

Proof. Define the relation $\{([x], y)\} \in \overline{f}$ if and only if $f(x) = y$. Let $[x] \in X$ and $y, z \in Y$. Suppose $([x], y), ([x], z) \in \overline{f}$, then there exists $u, v \in X$ such that $[u] = [v] = [x]$, $f(u) = y$, and $f(v) = z$, so $u \sim v$. Since f is invariant under $\sim$, $y = z$. Hence $\overline{f}$ is well-defined. For all $x \in X$, $(\overline{f} \circ \pi)(x) = \overline{f}([x]) = f(y)$. □

Problem 3.20. Prove that such $\overline{f}$ is unique.

Problem 3.21. Let $f : X \to Y$ be a function that induces an equivalence relation $\sim_f$ on X. Since $X_{\sim_f}$ satisfies the universal property, prove that $X_{\sim_f} \approx \operatorname{im}(f)$.

Proposition. Let S be any set satisfying the universal property for quotient sets. Let X be a set and let $\sim_1$ be an equivalence relation on X, so $\pi_1 : X \to X_{\sim_1}$ is invariant under the equivalence relation induced by $\pi_2 : X \to S$. Then $S \approx X_{\sim_1}$.

$$\begin{tikzcd}
S \arrow[dr, "\overline{\pi_1}"'] & X \arrow[l, "\pi_2"'] \arrow[d, "\pi_1"] \\
 & X_{\sim_1}
\end{tikzcd}$$

Proof. Since π_1 is surjective, $\overline{\pi_1}$ is surjective. For all $[x], [y] \in X_{\sim_1}$, □

This completes our proof of the universal property for quotient sets.

Theorem 3.1 (canonical decomposition of functions)**.** Let $f : A \to B$ be a function, then there exists a surjective function π, a bijective function g, and an injective function i, such that $f = i \circ g \circ \pi$.

$$\begin{tikzcd}
A \arrow[r, "\pi"] \arrow[rrr, bend left, "f"] & A_\sim \arrow[r, "g"] & \operatorname{im}(f) \arrow[r, "i"] & B
\end{tikzcd}$$

Proof. Let $i : \operatorname{im}(f) \to B$ be the identity map, then i is injective. The function $f : A \to B$ induces an equivalence relation $\sim$ on X, so g is bijective. The projection map $\pi : A \to A_\sim$ is surjective. For all $a \in A$, $(i \circ g \circ \pi)(a) = (i \circ g)([a]) = i(f(a)) = f(a)$. □

Definition 3.15. Let $\mathtt{C}$ be a category. Let A and B be objects in $\mathtt{C}$. The *product* of A and B, denoted P, is an object in $\mathtt{C}$ with morphisms $p_1 : P \to A$ and $p_2 : P \to B$ such that for all object X in $\mathtt{C}$ with morphisms $\varphi_1 : X \to A$ and $\varphi_2 : X \to B$, there exists a unique $u : X \to P$.

$$\begin{tikzcd}
 & X \arrow[dl, "\varphi_1"'] \arrow[d, dashed, "u"] \arrow[dr, "\varphi_2"] & \\
A & P \arrow[l, "p_1"] \arrow[r, "p_2"'] & B
\end{tikzcd}$$

Problem 3.22. Prove that in $\mathtt{Set}$, the Cartesian product satisfies the universal property for product.

Proposition. Let A and B be objects in a category $\mathtt{C}$. Then their product is unique.

Proof. □

$$\begin{tikzcd}
& Q \arrow[dl, "\varphi_1"'] \arrow[d, "u"] \arrow[dr, "\varphi_2"] & \\
A & P \arrow[l, "p_1"] \arrow[r, "p_2"'] \arrow[d, "v"'] & B \\
& Q \arrow[ul, "\varphi_1"] \arrow[ur, "\varphi_2"'] &
\end{tikzcd}$$

Definition 3.16. Let `C` be a category. Let A and B be objects in `C`. The *coproduct* of A and B, denoted Q, is an object in `C` with morphisms $q_1 : A \to Q$ and $q_2 : B \to Q$ such that for all object Y in `C` with morphisms $\varphi_1 : A \to Y$ and $\varphi_2 : B \to Y$, there exists a unique $v : Q \to Y$.

Problem 3.23. Prove that in `Set`, the disjoint union satisfies the universal property for coproduct.

Problem 3.24. Let A and B be objects in a category `C`. Then their coproduct is unique.

Axiom of choice. Let F be a function defined on a set I such that $F(i)$ is a nonempty set for all $i \in I$. Then there exists a *choice function* d defined on I such that $f(i) \in F(i)$ for all $i \in I$.

Theorem 3.2 (Zermelo's well-ordering theorem)**.** Every set S can be well-ordered.

Proof. □

Problem 3.25. Prove that the axiom of choice implies that every epimorphism in `Set` has a right inverse.

Notice that the Zermelo's well-ordering theorem does not imply the well-ordering principle. To prove the well-ordering principle, you have to show $\leq$ in $\mathbb{N}$ is the desired ordering. Check Jech's Set Theory to see a proof.

4 Integers and Cardinality

Theorem 4.1 (recursion)**.** Given a set X and $x \in X$. Let $f : X \to X$ be a function, then there exists a unique function $F : \mathbb{N} \to X$ such that $F(0) = x$ and $F(n^+) = f(F(n))$ for all $n \in \mathbb{N}$.

Proof. Define $F : \mathbb{N} \to X$ by □

5 Introduction to Groups

6 Real Numbers

7 Topology

Alphabetical Index