Foundations of Mathematics

MATH 300 HNR, Texas A&M University

Taught by Prof. Mohamad Masri

August 20, 2024 – December 2, 2024

Contents

1 Mathematical Reasoning

1.1 Statements

Definition 1.1: Statement

A **statement** is a declarative sentence which is either true(T) or false(F).

Statements are denoted by P, Q, R, etc.

Example 1

P: $3+1=4$ is true.

Q: $3+1=5$ is false.

R: "There are 30 people in this room" is false.

Definition 1.2: Open Sentence

An **open sentence** is a declarative sentence containing one or more variables which becomes a statement by specifying values of variables.

Open sentences are denoted by $P(X)$, $P(X,Y)$, and $P(X_1,\cdots,X_n)$.

Example 2

If $P(X) : X+1=2$ for $X \in \mathbb{R}$, then $P(1)$ is T, and $P(X)$ is F if $X \neq 1$.

"For all $X \in \mathbb{R}$" is called the *universal quantifier*, and "There exists $X \in \mathbb{R}$" is called the *existential quantifier*.

Example 3

Let $n \in \mathbb{Z}$ and $P(n) : n^2$ is even. Then for all integers n, $P(n)$ is T.

Proof. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. So

$$n^2 = (2k)^2 = 2(2k^2) = 2k'$$

where $k' = 2k^2 \in \mathbb{Z}$. Hence n^2 is even. □

Example 4

Let $n \in \mathbb{Z}$, and $P(n) : n = 3k$ for some $k \in \mathbb{Z}$. Then P: There exists an even integer n such that $P(n)$ is T.

Example 5

Let $P(X, Y)$ be an open sentence, and let

$$P : \forall x,\ \exists y \text{ such that } P(x, y)$$

$$Q : \exists y \text{ such that } \forall x,\ P(x, y)$$

Here, P and Q may not be the same statements. For example, Let X and $Y \in \mathbb{R}$ and $P(X, Y) : y^3 = x$. Then

$$P : \forall x \in \mathbb{R},\ \exists y \in \mathbb{R} \text{ such that } y^3 = x$$

$$Q : \exists y \in \mathbb{R} \text{ such that } \forall x \in \mathbb{R},\ y^3 = x.$$

Here, P and Q are different statements since P is T and Q is F.

Therefore, applying quantifiers in a different order may make different statements.

Definition 1.3: Negation

If P is a statement, then the **negation** of P, $\neg P$, and read "not P", is the statement "P is false".

Example 6

If $P : 3 + 1 = 4$, then $\neg P : 3 + 1 \neq 4$.

The negation of an open sentence is defined similarly.

Example 7

Let $X \in \mathbb{R}$. If $P(X) : X < 5$, then $\neg P(X) : X \geq 5$.

The below are rules for negating quantifiers.

1. If $P : \forall X,\ P(X)$, then $\neg P : \exists X$ such that $\neg P(x)$.
2. If $P : \exists X$ such that $P(X)$, $\neg P : \forall X,\ \neg P(X)$.

Example 8

Let P: Every polynomial is continuous everywhere. With $\mathbb{R}[x]$ the set of polynomials with real coefficients,

$$P : \forall p(x) \in \mathbb{R}[x],\ Q(p)$$

where $Q(p) : p(x)$ is continuous on $\mathbb{R}$. We have

$$\neg P : \exists p(x) \in \mathbb{R}[x] \text{ such that } \neg Q(p),$$

so $\neg P$: There exists a polynomial $p(x)$ and a point $x_0 \in \mathbb{R}$ such that $p(x)$ is discontinuous at x_0.

Example 9

Let $S : \forall x,\, \exists y$ such that $P(x, y)$. Then

$$\neg S : \exists x \text{ such that } \neg\big(\exists y \text{ such that } P(x, y)\big)$$
$$\neg S : \exists x \text{ such that } \forall y,\, \neg P(x, y).$$

Example 10 (Archimedean Principle)

If $P : \forall x \in \mathbb{R},\, \exists n \in \mathbb{Z}$ such that $n > x$.

Then $\neg P : \exists x \in \mathbb{R}$ such that $\forall n \in \mathbb{Z},\, n \leq x$.

Here, P is T and $\neg P$ is false.

1.2 Compound Statements

Definition 1.4: Conjunction and Disjunction

Let P and Q be statements.

- The **conjunction** of P and Q, written $P \wedge Q$ and read "P and Q" is the statement 'both P and Q are true'.
- The **disjunction** of P and Q, written $P \vee Q$ and read "P or Q" is the statement 'P is true or Q is true'.

Remark.

$P \wedge Q$ can fail in three ways:

- P is T and Q is F
- P if F and Q is T
- P is F and Q is F

$P \vee Q$ can fail in one way: P is F and Q is F.

Example 11

Let $x \in \mathbb{R}$, an $S(x) : |x| < 3$. If we let $P(x) : x > -3$ and $Q(x) : x < 3$, then

$$S(x) \Leftrightarrow P(x) \wedge Q(x).$$

So $P(1) \wedge Q(1)$ is T, and $P(4) \wedge Q(4)$ is F.

Example 12

Let $x \in \mathbb{R}$, an $S(x) : |x| \geq 3$. If we let $P(x) : x \leq -3$ and $Q(x) : x \geq 3$, then

$$S(x) \Leftrightarrow P(x) \vee Q(x).$$

So $P(1) \vee Q(1)$ is F, and $P(4) \vee Q(4)$ is T.

Note

Expressions like P, Q, $P \wedge Q$, $P \vee Q$, $\neg P$, $\neg Q$ where P and Q are variables, representing unknown statements are called statement forms.

Here is the truth tables for $P \wedge Q$ and $P \vee Q$.

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

The negation of a conjunction and a disjunction will be done with the truth table.

Claim. $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$.

Definition 1.5: Equivalent Statements and Equivalent Statement Forms

Two statements are **equivalent** if they are both true or both false. Statement forms are **equivalent** if the substitutions of statements in the forms always yields equivalent statements.

We have the following equivalences:

- $\neg\big(\forall x,\ P(x)\big) \Leftrightarrow \exists x$ such that $\neg P(x)$
- $\neg\big(\exists x$ such that $P(x)\big) \Leftrightarrow \forall x,\ \neg P(x)$
- $\neg\big(\forall x,\ P(x) \vee Q(x)\big) \Leftrightarrow \exists x$ such that $\neg\big(P(x) \vee Q(x)\big) \Leftrightarrow \exists x$ such that $\neg P(x) \wedge \neg Q(x)$
- $\neg\big(\forall x,\ P(x) \wedge Q(x)\big) \Leftrightarrow \exists x$ such that $\neg\big(P(x) \wedge Q(x)\big) \Leftrightarrow \exists x$ such that $\neg P(x) \vee \neg Q(x)$
- $\neg\big(\exists x$ such that $P(x) \vee Q(x)\big) \Leftrightarrow \forall x,\ \neg\big(P(x) \vee Q(x)\big) \Leftrightarrow \forall x,\ \neg P(x) \wedge \neg Q(x)$
- $\neg\big(\exists x$ such that $P(x) \wedge Q(x)\big) \Leftrightarrow \forall x,\ \neg\big(P(x) \wedge Q(x)\big) \Leftrightarrow \forall x,\ \neg P(x) \vee \neg Q(x)$

Example 13

Let $P(x)$ and $Q(x)$ be open sentences. Define

$$S : \forall x,\ P(x) \vee Q(x)$$

$$T : \forall x,\ P(x) \vee \forall x,\ Q(x).$$

Then S is not necessarily equivalent to T. As a counterexample, let $P(x) : x > 2$ and $Q(x) : x < 5$. Then, we have

$$S : \text{For all } x \in \mathbb{R},\ x > 2 \text{ or } x < 5$$

$$T : \text{For all } x \in \mathbb{R},\ x > 2 \text{ or for all } x \in \mathbb{R},\ x < 5.$$

Here, S is T and T is F, and $S \not\Leftrightarrow T$.

Example 14

On the other hand, consider

$$S : \exists x \text{ such that } P(x) \vee Q(x)$$

$$Y : \exists x \text{ such that } P(x) \vee \exists x \text{ such that } Q(x).$$

Claim. $S \Leftrightarrow T$.

Proof. We will show if S is true then T is true, and if T is true then S is true.

Suppose S is true. Then there is some $x = a$ such that $P(a)$ or $Q(a)$. If $P(a)$, then there is x such that $P(x)$. If $Q(a)$, then there is x such that $Q(x)$. Hence there is x such that $P(x)$, or there is x such that $Q(x)$. So T is true.

By similar argument, if T is true, then S is true. Therefore, $S \Leftrightarrow T$.

Now, let S false. If T is true, then S should be true, which is a contradiction. So if S is false, then T is false. Similarly, if T is false, then S is false. This completes the proof. □

1.3 Implications

Definition 1.6: Implication

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."

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

Remark.
If P is a false statement, then $P \Rightarrow Q$ is always true.

Let $P(x)$ and $Q(x)$ be open sentences, and let

$$S : \forall x,\ P(x) \Rightarrow Q(x).$$

Assume that $P(a)$ is true for $x = a$. To show that S is true, we should show $Q(a)$ is true (or $P(a)$ is false).

Example 15
Let $n \in \mathbb{Z}$, and

$$P(n) : n \text{ is odd}$$

$$Q(n) : n^2 \text{ is odd.}$$

Now let $S : \forall n \in \mathbb{Z},\ P(n) \Rightarrow Q(n)$.

Claim. S is true.

Proof. Suppose n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Hence

$$n^2 = (2k+1)^2 = 2(2k^2 + 2k) + 1 = 2k' + 1$$

for some $k' \in \mathbb{Z}$. Therefore, n^2 is odd. □

Example 16
Let n, $m \in \mathbb{Z}$, and

$$P(n, m) : n \text{ and } m \text{ is odd}$$

$$Q(n, m) : n + m \text{ is even.}$$

Prove $S : \forall n,\ m \in \mathbb{Z},\ P(n, m) \Rightarrow Q(n, m)$ is true.

Proof. Let n and m be odd. Then $n = 2k + 1$ and $m = 2k' + 1$ for some k, $k' \in \mathbb{Z}$. Hence

$$n + m = 2k + 2k' + 2 = 2(k + k' + 1) = 2l$$

where $l = k + k' + 1 \in \mathbb{Z}$. So $n + m$ is even. □

How do we negate implications? Let $S : \forall x,\ P(x) \Rightarrow Q(x)$. Then

$$\neg S : \exists x \text{ such that } \neg\big(P(x) \Rightarrow Q(x)\big).$$

Claim. Suppose P and Q are statements. Then

$$\neg(P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q.$$

Proof.

P	Q	$\neg Q$	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$P \wedge \neg Q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

□

Therefore $\neg S : \exists x$ such that $P(x) \wedge \neg Q(x)$.

Definition 1.7: Counterexample

Any x such that $\neg S$ is true is called a **counterexample** to S.

Example 17

Let $n,\ m \in \mathbb{Z}$, and

$$P(n, m) : n \text{ and } m \text{ are perfect squares}$$

$$Q(n, m) : n + m \text{ is a perfect square.}$$

Let $S : \forall n,\ m \in \mathbb{Z},\ P(n, m) \Rightarrow Q(n, m)$. Then $\neg S : \exists n,\ m \in \mathbb{Z}$ such that $P(n, m) \wedge \neg Q(n, m)$.

Claim. S is false.

Proof. We will find a counterexample. We need $n,\ m \in \mathbb{Z}$ such that n and m are perfect squares and $n + m$ is not a perfect square. If $n = 4$ and $m = 9$, since $4 + 9 = 13$ is not a perfect square, this is a counterexample. Therefore, S is false. □

Definition 1.8: Necessary and Sufficient Conditions

If $P \Rightarrow Q$ is true, then P is called a **sufficient condition**: for Q to be true, it is sufficient that P be true. Here, Q is called a **necessary condition**: Q must be true for P to be true.

Claim. $P \Rightarrow Q \Leftrightarrow \neg Q \Rightarrow \neg P$.

Proof. We use the truth table.

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

□

Example 18

Let $x \in \mathbb{R}$, and

$$P : x > 5$$

$$Q : x > 0.$$

$P \Rightarrow Q$ is true since if P is true, then $x > 5 > 0$, so Q is true. Hence $x > 5$ is sufficient for $x > 0$ (but not necessary). On the other hand, Q is necessary since for $x > 5$, we must have $x > 0$.

1.4 Contrapositive and Converse

We showed that $P \Rightarrow Q \Leftrightarrow \neg Q \Rightarrow \neg P$.

Definition 1.9: Contrapositive

Let P and Q be statements. The statement

$$\neg Q \Rightarrow \neg P$$

is called the **contrapositive** of $P \Rightarrow Q$.

Example 19

Let $x \in \mathbb{R}$, and

$$P : x + 1 > 5$$

$$Q : x > 4$$

Then $P \Rightarrow Q$. We have

$$\neg Q : x \leq 4$$

$$\neg P : x + 1 \leq 5,$$

so $\neg Q \Rightarrow \neg P$. Note that both $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are true.

Example 20

Let $n \in \mathbb{Z}$. If

$$P : n^2 \text{ is even}$$

$$Q : n \text{ is even},$$

Prove that $P \Rightarrow Q$.

Solution We prove the contrapositive $\neg Q \Rightarrow \neg P$, i.e. if n is odd then n^2 is odd. This is true by example 15. Therefore, $P \Rightarrow Q$.

Definition 1.10: Converse

Let P and Q be statements. Then the statement $Q \Rightarrow P$ is the **converse** of the statement $P \Rightarrow Q$.

Remark.

$P \Rightarrow Q$ and $Q \Rightarrow P$ are not equivalent.

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

Example 21

Let m, $n \in \mathbb{Z}$, and

$$P : m \text{ and } n \text{ are odd}$$

$$Q : m + n \text{ is even.}$$

Then $P \Rightarrow Q$ is true, but $Q \Rightarrow P$ is false.

Definition 1.11: Biconditional

The statement $P \Leftrightarrow Q$, read "P if and only if Q", is the statement $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. The symbol $\Leftrightarrow$ is called the **biconditional**.

Remark.
$(P \Leftrightarrow Q) \Leftrightarrow (\neg P \Leftrightarrow \neg Q)$.

One kind of proof methods is the *proof by contradiction*. To prove $P \Rightarrow Q$. Assume that P and $\neg Q$. If we get $\neg P$, then both P and $\neg P$ gets true, which is a contradiction. Therefore, we get $P \Rightarrow Q$.

Claim. $(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q \Rightarrow \neg P)$.

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

Theorem 1.1

Let S be a statement, and let C be a false statement. Then, $S \Leftrightarrow (\neg S \Rightarrow C)$

Proof. We use the truth table.

S	$\neg S$	C	$\neg S \Rightarrow C$
T	F	F	T
F	T	F	F

□

Example 22
Prove S: There are no integers x and y such that $x^2 = 4y + 2$.

Proof. We use proof by contradiction. Assume $\neg S$. Then there exist integers x and y such that $x^2 = 4y + 2$. Then $x^2 = 2(2y+1)$, which is even. Since x^2 is even, then x is even by example 20. Write $x = 2k$ for some $k \in \mathbb{Z}$. Then

$$x^2 = 4y + 2$$

$$4k^2 = 4y + 2$$

$$4k^2 - 4y = 2$$

$$k^2 - y = \frac{1}{2},$$

which is a contradiction because LHS is an integer but RHS is not. Thus S is true. $\square$

Here, C is "there exists α and $\beta \in \mathbb{R}$ with $\alpha = \beta$, such that $\alpha \in \mathbb{Z}$ and $\alpha \notin \mathbb{Z}$.

2 Sets

2.1 Sets and Subsets

Definition 2.1: Sets and Elements

A **set** A is a collection of objects. The objects $a \in A$ are called **elements**

Some examples are $\mathbb{R}$: the real numbers, and $\mathbb{Q}$: the rational numbers.

Let S be a set and $P(x)$ be an open sentence with variable $x \in S$. Define $A = \{x \in S \mid\P(x)\}$. Then A is called the *truth set* of $P(x)$. Let

$$A = 4\mathbb{Z} = \{4m \mid m \in \mathbb{Z}\}.$$

If $P(n) : n = 4m$ for some $m \in \mathbb{Z}$, then A can be also expressed as

$$A = \{n \in \mathbb{Z} \mid P(n)\}.$$

Definition 2.2: Subset

Let A and B be sets. Then A is a **subset** of B, written $A \subset B$, if $a \in A \Rightarrow a \in B$. If $A \subset B$ but $A \neq B$, then A is a **proper subset** of B.

Remark.

Here $A = B$ means $A \subset B$ and $B \subset A$. If $A \subset B$ and $A \neq B$, then $\exists b \in B$ such that $b \notin A$. In this case we'll often write $A \subsetneq B$.

Example 1

$\mathbb{Z}^+ \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$.

Example 2

If $P(x)$ is an open sentence with $x \in S$, then

$$A = \{x \in S \mid P(x)\} \subset S.$$

Example 3

Let N and M be positive integers with $N \mid M$. Prove $M\mathbb{Z} \subset N\mathbb{Z}$.

Proof. Let $n \in M\mathbb{Z}$. Then $n = Mk$ for some $k \in \mathbb{Z}$. Since $N \mid M$, then $M = lN$ for some $l \in \mathbb{Z}$. Hence

$$n = Mk = (lN)k = (lk)N \in N\mathbb{Z}.$$

So $M\mathbb{Z} \subset N\mathbb{Z}$. □

Lemma

If $A \subset B$ and $B \subset C$ then $A \subset C$.

Proof. Let $a \in A$. Since $A \subset B$ then $a \in B$. Now, since $B \subset C$, $a \in C$. So $A \subset C$. □

Recall that $A = B$ if and only if $A \subset B \wedge B \subset A$. We have

$$\neg(A \subset B) \Leftrightarrow \exists a \in A \text{ such that } a \notin B.$$

Here, $a \in A$ but $a \notin B$, so $A \not\subset B$. Similarly, $B \not\subset A$.

Example 4

Let a, $b \in \mathbb{R}$ and $a < b$. Let

$$A = \{f : [a, b] \to \mathbb{R} \mid f \text{ is continuous}\} B \quad = \{f : [a, b] \to \mathbb{R} \mid f \text{ is integrable}\}$$

From calculus, $A \subset B$. However $B \not\subset A$.

Define $f(x) = \begin{cases} 1 & x = \frac{a+b}{2} \\ 0 & x \neq \frac{a+b}{2} \end{cases}$. Then f is discontinuous at $x_0 = \dfrac{a+b}{2} \in [a, b]$, but $\displaystyle\int_a^b f(x)\, dx = 0$. So $f \in B$ but $f \notin A$.

Definition 2.3: Complement

Let A and B be sets. The **complement** of A in B is the set

$$B - A = \{b \in B \mid b \notin A\}.$$

Definition 2.4: Complement of a set

If U is a universal set, we write $U - A = \bar{A}$, called the **complement** of A.

Example 5

Let $U = \mathbb{Z}$. If $A = \mathbb{Z}^+$, then $\bar{A} = \{0, -1, -2, -3, \cdots\}$.

Definition 2.5: Empty Set

A set with no elements is called the **empty set**, denoted $\emptyset$.

If $U = \mathbb{R}$ and $A = \{x \in \mathbb{R} \mid x^2 < 0\}$, then $A = \emptyset$ and $\bar{A} = \{x \in \mathbb{R} \mid x^2 \geq 0\} = U$.

Theorem 2.1

If A, $B \subset U$ with $A \subset B$, then $\bar{B} \subset \bar{A}$.

Proof. Let $x \in \bar{B} = U - B$. So $x \in U$ and $x \notin B$. We want to show that $x \in \bar{A} = U - A \Leftrightarrow x \notin A$. Suppose $x \in A$. Since $A \subset B$, $x \in B$, which contradicts $x \in \bar{B}$. So $x \notin A$. □

2.2 Combining Sets

Definition 2.6: Union and Intersection

Let A and B be sets. The **union** of A and B is

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

The **intersection** of A and B is

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Definition 2.7: Disjoint Sets

Two sets A and B are **disjoint** if $A \cap B = \emptyset$. Generally, if A_1, A_2, $\ldots$, A_n are sets, then these sets are **pairwise disjoint** if $A_i \cap A_j = \emptyset$ for all i and $j \in \{1, 2, \cdots, n\}$ with $i \neq j$.

We have the following properties:

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$
3. $(A \cup B) \cup C = A \cup (B \cup C)$
4. $(A \cap B) \cap C = A \cap (B \cap C)$
5. $A \subset A \cup B$
6. $A \cap B \subset A$
7. $\emptyset \subset A$
8. $A \cup \emptyset = A$
9. $A \cap \emptyset = \emptyset$.

We prove $\emptyset \subset A$.

Proof. It is sufficient to show that $\forall x,\ x \in \emptyset \Rightarrow x \in A$. Fix $x \in U$. Define $P(x) : x \in \emptyset$ and $Q(x) : x \in A$. Then it is sufficient to show that $P(x) \Rightarrow Q(x)$. Since $\emptyset$ is empty, $x \notin \emptyset$, so $P(x)$ is false. Therefore, $P(x) \Rightarrow Q(x)$ is true. □

Next, we prove $A \cup \emptyset = A$.

Proof. Since $A \subset A$ and $\emptyset \subset A$, $A \cup \emptyset \subset A$. By (5), $A \subset A \cup \emptyset$. Therefore, $A \cup \emptyset = A$. □

We now prove $A \cap \emptyset = \emptyset$.

Proof. Suppose $A \cap \emptyset \neq \emptyset$. Then there exists $x \in A \cap \emptyset$. But then $x \in \emptyset$, a contradiction. So $A \cap \emptyset = \emptyset$. □

Theorem 2.2

1. $A - B = A \cap \bar{B}$
2. $A \subset B \Leftrightarrow A \cup B = B$.

Proof. (1) Recall that $A - B = \{x \in A \mid x \notin B\}$. Also, $A \cap \bar{B} = \{x \in A \mid x \notin B\}$. Therefore, $A - B = A \cap \bar{B}$.

(2) Exercise. □

Theorem 2.3

Let A, B, C be sets.

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

Proof. Exercise. □

Theorem 2.4: De Morgan's Law

Let A, $B \in U$. Then

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

Proof. For some $x \in U$, let $P : x \in A$ and $Q : x \in B$. Then $\neg P : x \in \bar{A}$, $\neg Q : x \in \bar{B}$. So

(1) is true if and only if $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

(2) is true if and only if $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$,

which is obviously true. □

Definition 2.8: Cartesian Product

Let A and B be sets. The **cartesian product** of A and B is

$$A \times B = \{(a, b) \mid a \in A,\, b \in B\}.$$

Elements of $A \times B$ are called **ordered pairs**.

Example 6

If $A = B = \mathbb{R}$, then $A \times B = \mathbb{R} \times \mathbb{R}$ or $\mathbb{R}^2$, which also is $\{(c, y) \mid x, y \in \mathbb{R}\}$. Similarly, if $A = B = \mathbb{Z}$, then $\mathbb{Z}^2 = \{(m, n) \mid m, n \in \mathbb{Z}$.

Example 7

If $A = \{1, 2, 3\}$ and $B = \{1, 2, 3\}$, then

$$A \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}.$$

Note that $(1, 2) \neq (2, 1)$. Order matters!

Note that in general, $A \times B \neq B \times A$. In $\{1, 2\} \times \{3, 4\}$, $(1, 3) \in A \times B$ but $(3, 1) \notin A \times B$.

If A and B are finite, then $|A \times B| = |A| \cdot |B|$. Here, $|X|$ is the number of the elements in X, called the *cardinality* of X.

2.3 Collections of Sets

Definition 2.9: Power Set

Let A be a set. The **power set** of A is

$$\mathcal{P}(A) = \{X \mid X \in A\}.$$

Note that $\mathcal{P}(A) \neq \emptyset$ since $\emptyset \subset A$ and $A \subset A$. Also, if A is finite, then $|\mathcal{P}(A)| = 2^{|A|}$.

Definition 2.10: Collection of Sets

Let A_1, A_2, $\ldots$, A_n be subsets of U. The set

$$\mathcal{C} = \{A_1, A_2, \ldots, A_n\}$$

of sets is called the **collection of sets**. We also use the notation

$$\mathcal{C} = \{A_i\}_{i \in I}$$

where $I = \{1, 2, \ldots, n\}$.

The union of sets in $\mathcal{C}$ is

$$\bigcup_{i\in I} A_i = \{x \in U \mid x \in A_i \text{for some } i \in I\}$$

and the intersection of sets in $\mathcal{C}$ is

$$\bigcap_{i\in I} A_i = \{x \in U \mid x \in A_i \text{for all } i \in I\}$$

Definition 2.11: Disjoint Union

If $A \cap B = \emptyset$ then the union of A and B is disjoint and written $A \sqcup B$.

Example 8

Let $U = \mathbb{Z}^+$. Define the collecion $\mathcal{C}_N$ by

$$\mathcal{C}_N = \{A_i\}_{i\in I_n}$$

where $A_i = \{i, i+1\}$ for some $i \in I_N = \{1, 2, \ldots, N\}$. Then

$$\mathcal{C}_1 = \{\{1,2\}\}$$
$$\mathcal{C}_2 = \{\{1,2\},\{2,3\}\}$$
$$\cdots = \cdots$$

We have $\bigcap_{i\in I_N} A_i = \begin{cases} A_1 & N=1 \\ A_1 \cap A_2 = \{2\} & N=2 \\ \emptyset & N \geq 3 \end{cases}$.

Prove that $\bigcup_{i\in I_N} A_i = I_{N+1}$ and $\bigcap_{i\in I_N} A_i = \emptyset$ for $N \geq 3$.

Solution We first prove $\bigcup_{i\in I_N} A_i = I_{N+1}$.

($\subset$) Let $x \in \bigcup_{i\in I_N} A_i$. Then $x \in A_k$ for some $k \in I_N$. Since $A_k = \{k, k+1\}$, then $x = k$ or $x = k+1$. Since $1 \leq k \leq N$, if $x = k$ then $1 \leq x \leq N$, and if $x = k+1$ then $2 \leq x \leq N+1$. In either case, $x \in I_{N+1}$.

($\supset$) Let $x \in I_{N+1} = I_N \sqcup \{N+!\}$. Clearly, $x \in A_x = \{x, x+1\}$. If $x \in I_N$ then $x \in \bigcup_{i\in I_N} A_i$. If $x \in \{N+1\}$ then $x = N+1$ and so $x \in A_N = \{N, N+1\}$.

We now prove $\bigcap_{i\in I_N} A_i = \emptyset$ for $N \geq 3$. Let $N \geq 3$. Suppose $x \in \bigcup_{i\in I_N} A_i$. Then

$x \in A_i$ for all $i = 1, 2, \ldots, N$. Since $N \geq 3$ then in particulat,

$$x \in A_1 \cap A_2 \cap A_3 = \emptyset,$$

a contradiction. Therefore $\bigcap_{i \in I_N} A_i = \emptyset$.

Remark.

The index sets I can be infinite sets.

Example 9

Let $I = \mathbb{Z}^+$ and $A_i = (-i, i) \subset \mathbb{R}$. Prove that $\bigcup_{i \in I} A_i = \bigcup_{i=1}^{\infty} (-i, i) = \mathbb{R}$ and $\bigcup_{i \in I} A_i = A_1$.

Solution We first prove $\bigcap_{i \in I} A_i = \mathbb{R}$.

$(\subset)$ Let $x \in \bigcup_{i=1}^{\infty} (-i, i)$. Then $x \in (-k, k)$ for some $k \in \mathbb{Z}^+$. Since $(-k, k) \subset \mathbb{R}$, $x \in \mathbb{R}$.

$(\supset)$ Let $x \in \mathbb{R}$. Show $\exists i \in \mathbb{Z}^+$ such that $x \in (-i, i)$, or equivalently, $-i < x < i$, or $|x| < i$. This is true by the Archimedean principle.

We now prove $\bigcup_{i \in I} A_i = A_1$.

$(\subset)$ Let $x \in \bigcap_{i=1}^{\infty} (-i, i)$. Then $x \in (-i, i)$ for all $i \in \mathbb{Z}^+$. Hence $x \in (-1, 1)$.

$(\supset)$ Let $x \in (-1, 1)$. Since $-1 < x < 1$ then $-i < x < i$ for all $i \geq 1$.

Remark.

Here we have $A_1 \subset A_2 \subset \cdots \subset A_N \subset \cdots$.

Definition 2.12: Increasing/Decreasing Chain of Sets

Suppose $\mathcal{C} = \{A_i\}_{i \in I}$ is a collection of sets. If $A_i \subset A_j$ for all $i \leq j$, then $\mathcal{C}$ is an **increasing chain of sets**. If $A_j \subset A_i$ for all $i \leq j$, then $\mathcal{C}$ is a **decreasing chain of sets**.

If S is a collection of sets, we write $\bigcup_{A \in S} A$ for the union and $\bigcap_{A \in S} A$ for the intersection.

Definition 2.13: Partition

Let A be a set. A partition of A is a subset $\mathcal{P}$ of $\mathcal{P}(A)$ such that

- If $X \in \mathcal{P}$ then $X \neq \emptyset$
- $\bigcup_{X \in \mathcal{P}} X = A$
- If $X, Y \in \mathcal{P}$ with $X \neq Y$ then $X \cap Y = \emptyset$.

That is, the sets $X \in \mathcal{P}$ are pairwise disjoint

Example 10

Let $A = \{1, 2\}$. Then $\mathcal{P} = \big\{\{1\}, \{2\}\big\}$ is one of the partitions. More generally, let $A = \{a \mid a \in A\}$. Let $\mathcal{P} = \big\{\{a\} \mid a \in A\big\}$ is a partition.

Lemma

Let $A_1, A_2, \ldots, A_n$ be finite, pairwise disjoint sets. Then

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|.$$

Theorem 2.5

Let A and B be finite sets. Then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. By the Venn diagram, notice that $A - (A \cap B)$, $A \cap B$, and $B - (A \cap B)$ form a partition for $A \cup B$. That is,

$$A \cup B = \big(A - (A \cap B)\big) \sqcup (A \cap B) \sqcup \big(B - (A \cap B)\big).$$

By the lemma above,

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

since $A = \big(A - (A \cap B)\big) \sqcup (A \cap B)$ and $B = \big(A - (A \cap B)\big) \sqcup (A \cap B)$. □

Theorem 2.6: Pigeonhole Principle

Let $A_1, A_2, \ldots, A_N$ be finite, pairwise disjoint sets. Let $A = \bigcup_{i=1}^{N} A_i$. If $|A| > Nr$ for some $r \in \mathbb{Z}^+$, then $|A_i| \geq r + 1$ for some $i \in I_N$.

Proof. By the lemma, $|A| = \sum_{i=1}^{N} |A_i|$. We prove by contradiction. Assume $|A_i| \leq r$ for all $i \in I_N$. Then

$$Nr < |A| = \sum_{i=1}^{N} |A_i| \leq \sum_{i=1}^{N} r = Nr.$$

Since this is a contradiction, $|A_i| \geq r + 1$ for some $i \in I_N$. □

3 Functions

3.1 Definition and Basic Properties

From now on, assume all sets to be nonempty.

Definition 3.1: Function

Let A and B be sets. A **function** $f : A \to B$ is a rile which assigns to each $a \in A$, a unique $b \in B$.

Here, A is called the domain of f, and B is called the codomain of f. We write $f(a) = b$ for $a \in A$, if b is assigned to a.

Definition 3.2: Identity Function

Let A be a set. The **identity function** is

$$i_A : A \to A$$

by $i_A(a) = a$ for all $a \in A$.

Example 1

If $a, b \in \mathbb{R}$, then $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax + b$, $x \in \mathbb{R}$ is called a *linear function.*

Definition 3.3: Image

Let $f : A \to B$ be a function. The **image** of f is

$$\text{Im}(f) = f(A) = \{f(a) \mid a \in A\}.$$

More generally, if $X \subset A$, then the image of X is

$$f(X) = \{f(x) \mid x \in X\} = \{b \in B \mid b = f(x) \text{ for some } x \in X\}.$$

Definition 3.4: Equal Functions

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

Example 2

Let $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ for $x \in \mathbb{R}$. Find $\text{Im}(f)$.

Solution We claim that $\text{Im}(f) = \mathbb{R}_{\geq 0}$.

($\subset$) Let $y \in \text{Im}(f)$. Then $y = x^2$ for some $x \in \mathbb{R}$. But $x^2 \geq 0$, so $y \geq 0$. Hence $y \in \mathbb{R}_{\geq 0}$.

($\supset$) Let $y \in \mathbb{R}_{\geq 0}$. Let $x = \sqrt{y}$. Then $x^2 = (\sqrt{y})^2 = y$. Hence $y \in \text{Im}(f)$.

Therefore, $\text{Im}(f) = \mathbb{R}_{\geq 0}$.

Example 3

Let $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax + b$ where $a \neq 0$ and b are constants. Find $\text{Im}(f)$.

Solution We claim that $\text{Im}(f) = \mathbb{R}$.

($\subset$) This is immediate since the image is always a subset of the codomain.

($\supset$) Let $y \in \mathbb{R}$. Then $y \in \text{Im}(f)$ since $x = (y - b)/a$ satisfies $ax + b = y$.

Theorem 3.1: Intermediate Value Theorem

Let $f : \mathbb{R} \to \mathbb{R}$. Assume f is continuous on $[a, b]$ with $a < b$. If $f(a) < y < f(b)$ then there is $x \in [a, b]$ such that $f(x) = y$.

Example 4

Let $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 + 4x + 1$. Prove that $f(\mathbb{R}) = \mathbb{R}$.

Solution We only need to show that $\mathbb{R} \subset (\mathbb{R})$.

Let $y \in \mathbb{R}$. We need $x \in \mathbb{R}$ such that $y = x^3 + 4x + 1$. Note that $f(x) = x^3 + 4x + 1$ is continuous on $\mathbb{R}$. Note that

$$\lim_{x \to \infty} f(x) = +\infty$$

$$\lim_{x \to -\infty} f(x) = -\infty,$$

so given $y \in \mathbb{R}$, there is $M > 0$ such that if $x > M$ then $f(x) > y$. Similarly, there is $N < 0$ such that if $x < N$ then $f(x) = y$. Hence there exist $a < b$ as required.

Lemma

Let $f : A \to B$. If $X, Y \subset A$ with $X \subset Y$, then $f(X) \subset f(Y)$.

Proof. Let $a \in f(X)$. Then $a = f(x)$ for some $x \in X$. But $X \subset Y$, so $x \in Y$. Hence $a = f(x) \in f(Y)$. □

Note that this generalizes the *fiber* of a function over a point. Namely, if $b \in B$, the *fiber* of f over b is

$$f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}.$$

Definition 3.5: Inverse Image

Let $f : A \to B$ and $W \subset B$. The **inverse image** of W with respect to f is the set

$$f^{-1}(W) = \{a \in A \mid f(a) \in W\}.$$

Example 5

Let $A = \{0, 1, 2, 3, 4, 5\}$ and $B = \{7, 9, 11, 12, 13\}$. Define $f : A \to B$ by

$$\begin{aligned} 0 &\to 11 \\ 1 &\to 9 \\ f : 2 &\to 7 \\ 3 &\to 9 \\ 4 &\to 11 \\ 5 &\to 9 \end{aligned}$$

Let $W_1 = \{7, 9\}$, $W_2 = \{11, 12\}$, and $W_3 = \{11, 13\}$. Then

$$\begin{aligned} f^{-1}(W_1) &= \{1, 2, 3, 5\} \\ f^{-1}(W_2) &= \{0, 4\} \\ f^{-1}(W_3) &= \emptyset. \end{aligned}$$

Lemma

Let $f : A \to B$. If A is finite, then $|f(A)| \leq |A|$.

Proof. Suppose $|A| = N$. Write $A + \{a_1, a_2, \ldots, a_N\}$. Then $f(A) = \{f(a_1), f(a_2), \ldots, f(a_n)\}$. Since f is a function, then $|f(A)| \leq N = |A|$. Since a_i can't be assigned to more than one value. □

3.2 Surjective and Injective Functions

Definition 3.6: Surjective

Let $f : A \to B$ be a function. Then f is **surjective** or **onto** if $f(A) = B$.

Example 6

$i_A : A \to A$ is onto, namely $i_A(A) = A$.

Example 7

Let

$$\pi_1 : A \times B \to A \ \pi_1((a,b)) = a$$

$$\pi_2 : A \times B \to B \ \pi_1((a,b)) = b.$$

Then π_1 and π_2 are onto. These are called *coordinate projections*. This is because

$$\begin{aligned} \pi_1(A \times B) &= \{\pi_1((a,b)) \mid (a,b) \in A \times B\} \\ &= \{a \mid (a,b) \in A \times B\} \\ &= \{a \mid a \in A\} \\ &= A, \end{aligned}$$

and similarly for π_2.

Example 8

Let $f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(n) = \begin{cases} n+2 & n \in E \\ 2n+1 & n \in O \end{cases}$$

with E the even integers and O the odd integers. Show that f is not onto.

Solution We need to show that $f(\mathbb{Z}) \neq \mathbb{Z}$.

Claim. $5 \notin f(\mathbb{Z})$.

Suppose $5 \in f(\mathbb{Z})$. Then $5 = f(n)$ for some $n \in \mathbb{Z}$. If $n \in E$ then $n + 2 = 5$ gives $n = 3$, but $3 \notin E$. If $n \in O$ then $2n + 1$ gives $n = 2$, but $2 \notin O$. Therefore $5 \notin f(\mathbb{Z})$.

Definition 3.7: Injective

Let $f : A \to B$ be a function. Then f is **injective** or **one-to-one** if whenever a_1, $a_2 \in A$ with $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$. Equivalently, if a_1, $a_2 \in A$ with $f(a_1) = f(a_2)$ then $a_1 = a_2$.

Example 9

Define f as in the previous example. Show that f is injective.

Solution Let n_1, $n_2 \in \mathbb{Z}$ and suppose $f(n_1) = f(n_2)$. If n_1, $n_2 \in E$ then $n_1 + 2 = n_2 + 2 \Rightarrow n_1 = n_2$.

If n_1, $n_2 \in O$ then $2n_1 + 1 = 2n_2 + 1 \Rightarrow n_1 = n_2$.

If $n_1 \in E$ and $n_2 \in O$, then $n_1 \neq n_2$. Now, $f(n_1) = n_1 + 2$ and $f(n_2) = 2n_2 + 1$, so $f(n_1) = f(n_2)$. Hence f is one-to-one.

Definition 3.8: Bijective

Let $f : A \to B$ be a function. If f is both onto and one-to-one, then f is a bijection.

Example 10

Let $f(x) = x^3$ for $x \in \mathbb{R}$. Then By IVT, $f(\mathbb{R}) = \mathbb{R}$. Since $f'(x) = 3x^2 > 0$ for $x \neq 0$, f is strictly increasing. Let x_1 and $x_2 \in \mathbb{R}$ with $x_1 \neq x_2$. WLOG suppose $x_1 < x_2$. Then $f(x_1) < f(x_2)$, which gives $f(x_1) \neq f(x_2)$.

Definition 3.9: Permutation

Let $f : A \to A$ be a function. If f is a bijection, then f is called a **permutation** of A.

Let $S_A + \{f : A \to f \mid f \text{ is a permutation}\}$. Note that $i_A \in S_A$, so $S_A \neq \emptyset$. If $|A| = N$ then $|S_A| = N!$.

3.3 Compositions and Invertible Functions

Definition 3.10: $F(A, B)$

Let A and B be sets. Write $F(A, B)$ as $\{\text{functions } f : A \to B\}$. If $A = B$, write $F(A)$.

Definition 3.11: Composition

Let A, B, and C be sets. If $f \in F(A, B)$ and $g \in F(B, C)$. Then the **composition** $g \circ f \in F(A, C)$ is the function

$$(g \circ f)(a) = g\big(f(a)\big) \text{ for } a \in A.$$

Example 11

Let f, $g \in F(\mathbb{R})$ be $f(x) = x^2$ and $g(x) = x + 1$. Then

$$(g \circ f)(x) = g\big(f(x)\big) = g(x^2) = x^2 + 1$$

and

$$(f \circ g)(x) = f\big(g(x)\big) = f(x+1) = x^2 + 2x + 1.$$

Remark.

$g \circ f \neq f \circ g$ in general. That is, function composition does not commute.

Theorem 3.2

Let $f \in F(A, B)$. Then $f \circ i_A = f$ and $i_B \cdot f = f$.

Proof. Note that $f \circ i_A : A \to B$ and $i_B \circ f : A \to B$. We have

$$(f \circ i_A)(a) = f\big(i_A(a)\big) = f(a) \text{ for all } a \in A$$
$$(i_B \circ f)(a) = i_B\big(f(a)\big) = f(a) \text{ for all } a \in A. \quad \square$$

Theorem 3.3

Let $f \in F(A, B)$ and $g \in F(B, C)$.

1. If f and g are onto then $g \circ f$ is onto.
2. If f and g are one-to-one then $g \circ f$ is one-to-one.
3. If f and g are bijective then $g \circ f$ is bijective.

Proof. (1) Recall that $g \circ f \in F(A, C)$. We have

$$(g \circ f)(A) = g\big(f(A)\big) = g(B) = C,$$

so $g \circ f$ is onto.

(2) Suppose a_1, $a_2 \in A$ and $(g \circ f)(a_1) = (g \circ f)(a_2)$. Then

$$g\big(f(a_1)\big) = g\big(f(a_2)\big) \Rightarrow f(a_1) = f(a_2)$$

since g is one-to-one. Then, $a_1 = a_2$ since f is one-to-one. Therefore $g \circ f$ is one-to-one.

(3) Follows immediately from (1) and (2). $\square$

Corollary

Let $f, g \in S(A)$. Then $g \circ f \in S(A)$.

Lemma

he function composition is associative. Let $f \in F(A, B)$, $g \in F(B, C)$, and $h \in F(C, D)$. Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof. We have

$$\big(h \circ (g \circ f)\big)(a) = h\big((g \circ f)(a)\big) = h\big(g(f(a))\big)$$
$$\big((h \circ g) \circ f\big)(a) = (h \circ g)\big(f(a)\big) = h\big(g(f(a))\big).$$

□

Definition 3.12: Invertible Functions

Let $f \in F(A, B)$. Then f is **invertible** if there exists $g \in F(B, A)$ such that $f \circ g = i_B$ and $g \circ f = i_A$. If g exists, it is called the **inverse** of f and denoted f^{-1}.

Remark.
If g exists, it is unique.

Proof. Suppose g and h are inverses of f. Then

$$f \circ g = i_B,\ g \circ f = i_A$$
$$f \circ h = i_B,\ h \circ f = i_A$$

Then

$$\begin{aligned} g &= g \circ i_B \\ &= g \circ (f \circ h) \\ &= (g \circ f) \circ h \\ &= i_A \circ h \\ &= h. \end{aligned}$$

□

Example 12
$i_A \in S(A)$ is invertible with $i_A^{-1} = i_A$.

Proof. For $a \in A$, we have

$$(i_A \circ i_A)(a) = i_A\big(i_A(a)\big) = i_A(a),$$

so $i_A^{-1} = i_A$. □

Example 13

Let $f \in F(\mathbb{R})$ with $f(x) = x^2$ for $x \in \mathbb{R}$. Then f is not invertible. If we let $g = f|_{\mathbb{R}_{\geq 0}} \in F(\mathbb{R}_{\geq 0})$. Then $g^{-1}(x) = \sqrt{x}$ for $x \in \mathbb{R}_{\geq 0}$. We can prove that $g \circ g^{-1} = i_{R_{\geq 0}}(x)$, and the other way around.

Theorem 3.4

Let $f \in F(A, B)$. Then f is invertible if and only if f is a bijection.

Proof. ($\Rightarrow$) Suppose f^{-1} exists.

(Injective) Let a_1, $a_2 \in A$ with $f(a_1) = f(a_2)$. Since f^{-1} exists,

$$f^{-1}\big(f(a_1)\big) = f^{-1}\big(f(a_2)\big)$$
$$(f^{-1} \circ f)(a_1) = (f^{-1} \circ f)(a_2)$$
$$i_A(a_1) = i_A(a_2)$$
$$a_1 = a_2.$$

(Surjective) Let $b \in B$, Define $a = f^{-1}(b) \in A$. Then

$$f(a) = f\big(f^{-1}(b)\big) = (f \circ f^{-1})(b) = i_B(b) = b.$$

($\Leftarrow$) Suppose f is a bijection. We must define a function $g \in F(B, A)$ such that $f \circ g = i_B$ and $g \circ f = i_A$. Let $b \in B$. Since f is onto, there is $a \in A$ such that $f(a) = b$. Since f is injective, a is unique. Define $g : B \to A$ by

$$b \mapsto \text{ the unique } a \in A \text{ such that } f(a) = b$$

Then

$$(f \circ g)(b) = f\big(g(b)\big) = f(a) = b = i_B(b)$$
$$(g \circ f)(a) = g\big(f(a)\big) = g(b) = a = i_A(a). \quad \square$$

4 Binary Operations and Relations

4.1 Binary Operations

Definition 4.1: Binary Operation

A **binary operation** on a set A is a function $f : A \times A \to A$ that maps $(a_1, a_2) \mapsto F(a_1, a_2) \in A$.

Example 1

In $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, $+$ and $\cdot$ are binary operations defined by

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (m, n) &\mapsto m + n \\ \cdot : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (m, n) &\mapsto m \cdot n \end{aligned}$$

and similarly for $\mathbb{Q}$ and $\mathbb{R}$.

Remark.

Division is not a binary operation on $\mathbb{Z}$. For example, $1, 2 \in \mathbb{Z}$ but $1/2 \notin \mathbb{Z}$. Division if a binary operation on $\mathbb{Q} - \{0\}$ and $\mathbb{R} - \{0\}$.

Example 2

Let A be a set. Then

$$\begin{aligned} \circ : F(A) \times F(A) &\to F(A) \\ (f, g) \qquad &\mapsto f \circ g \end{aligned}$$

So function composition is a binary operation.

Example 3

In $\mathbb{R}$,

$$\begin{aligned} + : F(\mathbb{R}) \times F(\mathbb{R}) &\to F(\mathbb{R}) \\ (f, g) \qquad &\mapsto f + g \\ \cdot : F(\mathbb{R}) \times F(\mathbb{R}) &\to F(\mathbb{R}) \\ (f, g) \qquad &\mapsto f \cdot g \end{aligned}$$

are binary operations. Here, $(f+g)(a) = f(a)+g(a)$, and $(f \cdot g)(a) = f(a) \cdot g(a)$ for $a \in \mathbb{R}$.

From now, we denote a binary operation on A by

$$* : A \times A \to A$$

that maps $(a_1, a_2) \mapsto a_1 * a_2$.

Definition 4.2: Associativity

A binary operation $*$ on A is **associative** if for all a, b, and $c \in A$,

$$a * (b * c) = (a * b) * c.$$

Definition 4.3: Commutativity

A binary operation $*$ on A is **commutative** if for all a, and $b \in A$,

$$a * b = b * a.$$

Example 4

$+$ and $\cdot$ are associative and commutative on $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$.

Example 5

Define $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $a * b = 2a + b$. Then

$$\begin{aligned} (2 * 3) * 4 &= 7 * 4 \\ &= 18 \\ 2 * (3 * 4) &= 2 * 10 \\ &= 14, \end{aligned}$$

so $*$ is not associative. Also, since

$$\begin{aligned} 2 * 3 &= 7 \\ 3 * 2 &= 8, \end{aligned}$$

$*$ is not commutative.

We will denote $(A, *)$ as a binary operation $*$ on a set A.

Definition 4.4: Identity

Let $*$ be a binary operation on A. Then $e \in A$ is an **identity** for $*$ if $a * e = e * a = a$ for all $a \in A$.

Example 6

Some examples are $(A, *, e)$, $(\mathbb{R}, +, 0)$, $(\mathbb{R}, \cdot, 1)$, $(F(A), \circ, i_A)$.

Example 7

Prove that $(\mathbb{Z}, * : (a, b) \mapsto 2a + b)$ does not have an identity.

Solution Suppose $e \in \mathbb{Z}$ exists for $*$. Then

$$1 = e * 1 = 2e + 1 \Rightarrow e = 0.$$

However,

$$1 * 0 = 2 \neq 1,$$

so 0 cannot be the identity. Therefore, the identity doesn't exist for $(\mathbb{Z}, *)>$

Example 8

Let $A \neq \emptyset$. In $(\mathcal{P}(A), * : (X, Y) \mapsto X \cap Y)$, the identity is A since

$$X * e = X \cap A = X = A \cap X = e * X.$$

Theorem 4.1: Uniqueness

If e is the identity for $*$, then e is unique.

Proof. Suppose e and e' are identities for $*$. Then

$$e * e' = e$$

$$e * e' = e',$$

so $e = e'$. □

Definition 4.5: Invertible

Suppose we have $(A, *, e)$. Then $a \in A$ is **invertible** with respect to $*$ if there exists $b \in A$ such that $a * b = b * a = e$. If b exists, we say that b is an **inverse** of a with respect to $*$.

Example 9

In $(\mathbb{Z}, +, 0)$, the inverse of n is $-n$.

Theorem 4.2

Inverses are unique.

If b exists then we denote it by a^{-1}.

Example 10

The only invertible elements in $(\mathbb{Z}, \cdot, 1)$ are ± 1.

Example 11

In $(F(A), \circ, i_A)$, only those $f \in S_A \subset F(A)$ have inverses with respect to $\circ$.

Example 12

In $(\mathcal{P}(A), * : (X, Y) \to X \cap Y, e = A)$, note that $A^{-1} = A$ since $A \cap A = A$. Suppose $X \subset A$, $X \neq A$. Then $X \cap Y \neq A$ for all $Y \in \mathcal{P}(A)$ since $X \cap Y \subset X \neq A$. So X is not invertible.

Example 13

Let A, $B \in M_2(\mathbb{R}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \middle| \alpha,\ \beta,\ \gamma\ ,\delta \in \mathbb{R} \right\}$. Then

$$A \cdot B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

and

$$A \cdot I = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Definition 4.6: Closure

In $(A, *)$, let $X \subset A$. Then X is **closed** with respect to $*$ if for all x, $y \in X$, $x * y \in X$.

Example 14

Consider $\left(S, +, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right)$ with $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R}, a = 0 \right\}$. Then S is closed under $+$.

Example 15

Let a, $b \in \mathbb{R}$ with $b \neq 0$. Define $\ell_{a,b} = \{(x, ax+b) \mid x \in \mathbb{R}\} \subset \mathbb{R}^2$. Then $\ell_{a,b}$ is the graph of the line $y = ax + b$. We claim that $+|_{\ell_{a,b}} : \ell_{a,b} \times \ell_{a,b} \to \mathbb{R}^2$ is not closed. Since $(x_1, ax_1 + b) + (x_2, ax_2 + b) = \big(x_1 + x_2, a(x_1 + x_2) + 2b\big)$, if $\ell_{a,b}$ is closed, then $2b = b$, which gives $b = 0$, a contradiction. Therefore $\ell_{a,b}$ is not closed under addition.

Definition 4.7: Group

Let G be a nonempty set. If there is a binary operation $*$ on G such that

1. $*$ is associative
2. $\exists e \in G$ with respect to $*$
3. Every $g \in G$ has an inverse g^{-1} with respect to $*$

then $(G, *, e)$ is called a **group**.

Example 16

$(S(A), \circ, i_A)$ is a group since

1. Function composition is associative
2. i_A is the identity
3. Every function has an inverse (since it is a bijection).

Definition 4.8: Relation

A **relation** R on a set A is a subset $R \subset A \times A$. If $(a, b) \in R$, we write aRb.

Example 17

$<$ is a relation on $\mathbb{R}$ where $R = \{(a, b) \in \mathbb{R} \mid a < b\} \subset \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. We have $1R2$ but not $2R1$.

Example 18

Equality is a relation.

Definition 4.9: Reflexive, Symmetric, Transitive, Antisymmetric Relations

Let R be a relation on a set.

1. R is **reflexive** if aRa for all $a \in A$.
2. R is **symmetric** if $aRb \Rightarrow bRa$ for all $a, b \in A$.
3. R is **transitive** if aRb and $bRc \Rightarrow aRc$ for all $a, b, c \in A$.
4. R is **antisymmetric** if for all $a, b \in A$, aRb and $bRa \Rightarrow a = b$.

Example 19

Let $N \in \mathbb{Z}^+$ be fixed. Define R on $\mathbb{Z}$ by

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b = Na\} \subset \mathbb{Z} \times \mathbb{Z}$$

Then $(a, a) \in R$ if and only if $a = Na$, so R is not transitive.

Suppose $(a, b) \in R$. Then $b = Na$. This does not imply $a = Nb$, so R is not transitive.

If $b + Na$ and $c = Nb$, $c = N^2a$, so R is not transitive.

If $b = Na$ and $a = Nb$, then $b = N^2b$, so R is not antisymmetric.

Definition 4.10: Equivalence Relation

Let R be a relation on a set. Then R is an **equivalence relation** if R is reflexive, symmetric, and transitive.

Example 20

Equality is an equivalence relation.

Definition 4.11: Modulo N

Let $N \in \mathbb{Z}^+$ Define a relation on $\mathbb{Z}$ by

$$R_N = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b = Nk \text{ for some } k \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$$

Then aR_Nb if $N \mid a - b$. We write $a \equiv b \pmod{N}$.

Theorem 4.3

R_N is an equivalence relation on $\mathbb{Z}$.

Proof. (Reflexive) We have $a \equiv a \pmod{N} \Leftrightarrow N \mid a - a \Leftrightarrow N \mid 0$, so R_N is reflexive.

(Symmetric) Suppose $a \equiv b \pmod{N}$. Then $N \mid a - b \Leftrightarrow a - b = Nk$ for some $k \in \mathbb{Z}$. Since $b - a = N(-k)$, $b \equiv a \pmod{N}$, so R_N is symmetric.

(Transitive) Suppose $a \equiv b \pmod{N}$ and $b \equiv c \pmod{N}$. Then $a - b = Nk_1$ and $b - c = Nk_2$ for some k_1, $k_2 \in \mathbb{Z}$. Then

$$a - c = a - b + b - c = Nk_1 + Nk_2 = N(k_1 + k_2)$$

so $a \equiv c \pmod{N}$ and R_N is transitive. □

If R is an equivalence relation on A, we write aRb as $a \sim b$.

Definition 4.12: Equivalence Class

Let R be an equivalence relation on A, and let $a \in A$. The **equivalnece class** of a is

$$[a] = \{x \in A \mid x \sim a\}$$

Elements in $[a]$ are said to be equivalent.

Example 21

If $\sim$ on A is $=$ then $[a] = \{a\}$.

Example 22

If $\sim$ on $\mathbb{Z}$ is $a \sim b$ if $|a| = |b|$. Here, if $a \neq 0$, then $[a] = \{-a, a\}$, and if $a = 0$ then $[a] = \{0\}$.

Example 23

Fix $N \in \mathbb{Z}^+$. If $\sim$ is R_N (called congruence modulo N and $a \in \mathbb{Z}$, then

$$\begin{aligned}
[a]_N &= \{x \in \mathbb{Z} \mid x \sim a\} \\
&= \{x \in \mathbb{Z} \mid x \equiv a \pmod{N}\} \\
&= \{x \in \mathbb{Z} \mid N \mid x - a\} \\
&= \{x \in \mathbb{Z} \mid x - a = Nk \text{ for some } k \in \mathbb{Z}\} \\
&= \{x \in \mathbb{Z} \mid x = a + Nk \text{ for some } k \in \mathbb{Z}\} \\
&= \{a + Nk \mid k \in \mathbb{Z}\}.
\end{aligned}$$

Example 24

Let $N = 2$. Then $[0]_2 = \{2k \mid k \in \mathbb{Z}\} = \mathbb{E}$, and $[1]_2 = \{1 + 2k \mid k \in \mathbb{Z}\} = \mathbb{O}$.

Claim. $\mathbb{Z} = [0]_2 \sqcup [1]_2$.

Let R be an equivalence relation on A. Define

$$A/R = \{[a]_R \mid a \in A\} \subset \mathcal{P}(A).$$

Theorem 4.4

A/R is a partition of A.

Proof. If $[a]_R \in A/R$. Then $[a]_R \neq \emptyset$ since R is an equivalence relation implies $a \sim a$ so $a \in [a]_R$.

Note that

$$\bigcup_{X \in A/R} X = \bigcup_{a \in A} [a]_R.$$

We claim this is equal to A.

($\subset$) Let $x \in \bigcup_{a \in A} [a]_R$. Then $x \in [a]_R$ for some $a \in A$. But $[a]_R \subset A$, so $x \in A$.

($\supset$) Let $x \in A$. Then $x \in [x]_R$, so $x \in \bigcup_{a \in A} [a]_R$, so $A \subset \bigcup_{a \in A} [a]_R$.

Now, we must show that the sets in A/R are pairwise disjoint, i.e. if $[a]_R$, $[b]_R \in A/R$ with $[a]_R \neq [b]_R$, then $[a]_R \cap [b]_R = \emptyset$. We prove the contrapositive. Suppose $[a]_R \cap [b]_R \neq \emptyset$. Let $x \in [a]_R \cap [b]_R$. Then $x \sim a$ and $x \sim b$. Since $\sim$ is symmetric, $a \sim x$. Since $\sim$ is transitive, $a \sim x$ and $x \sim b$ implies $a \sim b$. This gives $a \in [b]_R$, and also $b \in [a]_R$ since $b \sim a$ by symmetry.

Claim. $[a]_R = [b]_R$.

($\subset$) Let $x \in [a]_R$. Then $x \sim a$. Since $a \sim b$, then $x \sim b$. So $x \in [b]_R$.

($\supset$) Let $x \in [b]_R$. Then $x \sim b$. Since $b \sim a$, then $x \sim a$. So $x \in [a]_R$.

Therefore, the sets in A/R are pairwise disjoint, so A/R is a partition of A. □

4.2 Partial and Linear Orderings

Theorem 4.5

Let $\mathscr{P}$ be a partition of A. Define a relation R on A by aRb if a, $b \in X$ for some $X \in \mathscr{P}(\subset \mathcal{P}(A))$. Then R is an equivalence relation on A.

Proof. (Reflexive) Let $a \in A$. Since $\mathscr{P}$ is a partition of A, then $a \in X$ for some $X \in \mathscr{P}$.

(Symmetric) Let a, $b \in A$ suppose aRb. Then a, $b \in X$ for some $X \in \mathscr{P}$ hence b, $a \in X$, so bRa.

(Transitive) Let a, b, $c \in A$ and suppose aRb and bRc. Then a, $b \in X$ and b, $c \in Y$

for some X, $Y \in \mathscr{P}$. Since $\mathscr{P}$ is a partition if $X \neq Y$, then $X \cap Y = \emptyset$. However, since $b \in X \cap Y$, then we must have $X = Y$. Since $a \in X$ and $c \in Y = X$, then a, $c \in X$, so aRc. □

Definition 4.13: Linear Ordering

Let (A, R) be a partially ordered set. Then R is a **linear ordering** on A if for all a, $b \in A$, either aRb or bRa. Then A is a **linearly ordered** set.

Example 25

$(R, \leq)$ is linearly ordered. $(\mathcal{P}(A), \subset)$ is not linearly ordered unless $|A| = 1$.

5 Integers

5.1 Axioms of $\mathbb{Z}$

In $(\mathbb{Z}, +, \cdot)$ and x, y, $z \in \mathbb{Z}$,

1. $(x + y) + z = x + (y + z)$
2. $x + y = y + x$
3. 0 is the additive identity
4. $x^{-1} = -x$ for $+$
5. $(xy)z = x(yz)$
6. $xy = yx$
7. $1 \cdot x = x$
8. $x(y + z) = xy + xz$
9. $\mathbb{Z}^+$ is closed in $\mathbb{Z}$ with respect to $+$ and $\cdot$.
10. (Trichotomy Law) For each $x \in \mathbb{Z}$, exactly one of the following is true: $x \in \mathbb{Z}^+$, $-x \in \mathbb{Z}^+$, $x = 0$.

We now have the following propositions.

Lemma

1. $a + b = a + c \Rightarrow b = c$
2. $a \cdot 0 = 0 \cdot a = 0$
3. $(-a)b = a(-b) = -(ab)$
4. $-(-a) = a$

Proof. (1) Suppose $a + b = a + c$. Then

$$\begin{aligned} a + (a + b) &= -a + (a + c) \\ \Rightarrow_{A_1} (-a + a) + b &= (-a + a) + c \\ \Rightarrow_{A_4} 0 + b &= 0 + c \\ \Rightarrow_{A_3} b &= c. \end{aligned}$$

(2) We have $0 + 0 = 0$ by A_3. Then

$$0 + a0 =_{A_3} a0 =_{A_3} a(0 + 0) =_{A_8} a0 + a0.$$

so $0 = a0$ by (1).

(3)

$$\begin{aligned} ab + (-a) + b &=_{A_8} \big(a + (-a)\big)b \\ &=_{A_4} 0b \\ &=_{P_2} 0, \end{aligned}$$

This shows that $(-a)b$ is an additive inverse of ab. By uniqueness of inverses, $(-a)b = -(ab)$.

(4) Since $a + (-a) =_{A_4} 0$, a is the additive inverse of $-a$. By the uniqueness of inverses, $-(-a) = a$. □

Example 1

Prove the following propositions:

1. $(-a)(-b) = ab$
2. $a)(b - c) = ab - ac$
3. $(-1)a = -a$
4. $(-1)(-1) = 1$.

Example 2

Prove the following proposition: if $x \in \mathbb{Z}$ with $x \neq 0$ then $x^2 \in \mathbb{Z}^+$.

Proof. Since $x \neq 0$, by A10 either $x \in \mathbb{Z}^+$ or $-x \in \mathbb{Z}^+$. If $x \in \mathbb{Z}^+$, then by A9, $x^2 = x \cdot x \in \mathbb{Z}^+$. If $-x \in \mathbb{Z}^+$, then $x^2 = x \cdot x =_{P5} (-x)(-x) \in \mathbb{Z}^+$ by A9. □

Definition 5.1: Inequality

Let x, $y \in \mathbb{Z}$. We say $x < y$ if $y - x \in \mathbb{Z}^+$.

Lemma

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

1. Exactly one of the following holds: $a < b$, $b < a$, $a = b$
2. $a > 0 \Rightarrow -a < 0$, $a < 0 \Rightarrow -a > 0$
3. $a > 0$ and $b > 0 \Rightarrow a + b > 0$ and $ab > 0$
4. $a > 0$ and $b < 0 \Rightarrow ab < 0$
5. $a < 0$ and $b < 0 \Rightarrow ab > 0$
6. $a < b$ and $b < c \Rightarrow a < c$
7. $a < b \Rightarrow a + c < b + c$
8. $a < b$ and $c < 0 \Rightarrow ac < bc$
9. $a < b$ and $c > 0 \Rightarrow ac > bc$.

Proof. Exercise. □

A11 (Well-ordering principle): Every nonempty subset of $\mathbb{Z}^+$ has a minimal element; if $S \subset \mathbb{Z}^+$ with $S \neq \emptyset$, then $\exists x_0 \in S$ such that $x_0 \leq x$ for all $x \in S$.

Example 3

Prove that there is no integer $x \in \mathbb{Z}$ with $0 < x < 1$.

Proof. Let $S = \{n \in \mathbb{Z} \mid 0 < n < 1\}$. Note that $S \subset \mathbb{Z}^+$. Suppose $S \neq \emptyset$. By WOP, there exists $x_0 \in S$ such that $x_0 \leq n$ for all $n \in S$. Since $x_0 \in S$ then $x_0 < 1$, hence $x_0 - 1 < 0$. By Q4, since $x_0 > 0$ and $x_0 - 1 < 0$, $x_0^2 - x_0 < 0$, which gives $x_0^2 < x_0$. Since $x_0 < 1$, by Q6, $x_0^2 < 1$. Also, $x_0^2 \in \mathbb{Z}^+$. This contradicts WOP, so $S = \emptyset$. □

Corollary

1 is the minimal element of $\mathbb{Z}^+$.

Corollary

Let $\mathbb{Z}^\times = \{n \in \mathbb{Z} \mid n \text{ has a multiplicative inverse in } \mathbb{Z}\}$. This is called the set of units of $\mathbb{Z}$. Then $\mathbb{Z}^\times = \{\pm 1\}$.

Proof. Clearly $\{\pm 1\} \subset \mathbb{Z}^\times$ since $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$. Suppose $a \in \mathbb{Z}^\times$. Then there exists $x \in \mathbb{Z}$ such that $ax = 1$. Since $ax = 1$, then A10 gives $a \in \mathbb{Z}^+$ or $-a \in \mathbb{Z}^+$. Now, suppose $a \in \mathbb{Z}^+$ and $a \neq 1$. Then $a > 1$ by minimality of

$1 \in \mathbb{Z}^+$, $a > 1$. Also, since $ax = 1 \in \mathbb{Z}^+$ then $x \in \mathbb{Z}^+$ (so $x \geq 1$). We now get $1 = ax > 1x = x \geq 1$, which is a contradiction. So $a = 1$.

A similar argument works if $-a \in \mathbb{Z}^+$. $\square$

We have considered the group $(\mathbb{Z}, +, 0)$ until now. But what if the group was $(\mathbb{Z}_N, +, [0])$? We first need to show that the group is well-defined.

Lemma

$\cdot : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ defined by $[a] \cdot [b] := [a \cdot b]$ is well defined.

Solution Let $[a] = [a']$ and $[b] = [b']$. Then $a \equiv a' \pmod N$ and $b \equiv b' \pmod N$, so $[ab] = [a'b']$ since $ab \equiv a'b' \pmod N$.

Define $\mathbb{Z}_N^\times = \{[a] \in \mathbb{Z}_N \mid [a] \text{ is invertible with respect to } \cdot\}$. For example, let $N = 4$. We construct the multiplication table for $\mathbb{Z}_4$.

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

So $\mathbb{Z}_4^\times = \{1, 3\}$. For $\mathbb{Z}_3$,

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

For $N = 3$, every integer has a multiplicative inverse.

> **Remark.**
> 0 is never in $\mathbb{Z}_N^\times$ for any N.

For $\mathbb{Z}_5$, $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$. This can be generalized to primes.

Theorem 5.1

If p is a prime, every nonzero element has a multiplicative inverse in $\mathbb{Z}_p$. That is, $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$.

5.2 Mathematical Induction

Theorem 5.2: First Principle of Mathematical Induction

Let $P(n)$ be a statement about $n \in \mathbb{Z}^+$. Suppose that

1. $P(1)$ is true
2. If $k \in \mathbb{Z}^+$ such that $P(k)$ is true, then $P(k+1)$ is true

Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proof. Let $S = \{n \in \mathbb{Z}^+ \mid P(n) \text{ is false}\}$.

Claim. $S = \emptyset$.

Suppose $S \neq \emptyset$. Since $S \subset \mathbb{Z}^+$, by WOP, S has a minimal element $k_0 \in S$. Now by (1), we know that $1 \notin S$, so $k_0 > 1$. Hence $k_0 - 1 \in \mathbb{Z}^+$. Further, $k_0 - 1 \notin S$ since $k_0 - 1 < k_0$. Hence $P(k_0 - 1)$ is true. Then by (2), since $P(k_0 - 1)$ is true, $P(k_0)$ is also true. This is a contradiction to $k_0 \notin S$, so $S = \emptyset$. □

Example 4

Show that $\displaystyle\sum_{i=1}^{N} i = \frac{N(N+1)}{2}$.

Solution We use induction. We have

$$P(1) = 1 = \frac{2}{2} = \frac{1(1+1)}{2}.$$

so $P(1)$ is true. Now, suppose $P(k)$ is true. Then $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$. We have

$$\begin{aligned} 1 + 2 + \cdots + k + k + 1 &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

so $P(k+1)$ is true. This completes the proof.

Theorem 5.3: Second Principle of Mathematical Induction

Let $n \in \mathbb{Z}$ and $P(n)$ be a statement. Suppose there is $n_0 \in \mathbb{Z}$ such that

1. $P(n_0)$ is true
2. If $k \geq n_0$ is an integer for which $P(k)$ is true then $P(k+1)$ is true,

then $P(n)$ is true for all $n \geq n_0$.

Proof. Exercise. □

Example 5

If $n \in \mathbb{Z}$ with $n \geq 3$ then $n^2 > 2n + 1$.

Solution Let $n \in \mathbb{Z}^+$ and $P(n) : n^2 > 2n + 1$. Note that $P(3)$ is true since $9 > 7$.

Suppose $k \in \mathbb{Z}$ with $k \geq 3$ such that $P(k)$ is true. Thus $k^2 > 2k + 1$. Now, we show that $P(k+1)$ is true, namely $(k+1)^2 > 2(k+1) + 1$. For $k \geq 3$, we have

$$\begin{aligned}(k+1)^2 &= k^2 + 2k + 1 \\ &> 4k + 2 \\ &> 2k + 3 \\ &= 2(k+1) + 1.\end{aligned}$$

Theorem 5.4: Second Principle of Mathematical Induction

Let $n \in \mathbb{Z}^+$ and $P(n)$ be a statement. Suppose

1. $P(1)$ is true
2. If $k \in \mathbb{Z}^+$ and $P(i)$ is true for all $i \in \mathbb{Z}^+$ with $i \leq k$ then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proof. Exercise. □

Example 6

Let $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ with $f(1) = 1$, $f(2) = 5$, and $f(n+1) = f(n) + 2f(n-1)$ for all $n \geq 2$. Let $P(n) : f(n) = 2^n + (-1)^n$ for all $n \in \mathbb{Z}^+$. Prove that $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Solution Note that $P(1)$ and $P(2)$ is true. Suppose $k \geq 3$ is a positive integer such that $P(i)$ is true for all $i \leq k$. By assumption, $P(k-1)$ and $P(k)$ are true. Then

$$f(k-1) = 2^{k-1} + (-1)^{k-1}$$

$$f(k) = 2^k + (-1)^k.$$

We will show that $P(k+1)$ is true, namely $f(k+1) = 2^{k+1} + (-1)^{k+1}$. We have

$$\begin{aligned} f(k+1) &= f(k) + 2f(k-1) \\ &= \left(2^k + (-1)^k\right) + 2\left(2^{k-1} + (-1)^{k-1}\right) \\ &= 2^k + (-1)^k + 2^k + 2(-1)^{k-1} \\ &= 2^{k+1} - (-1)^{k-1} + 2(-1)^{k+1} \\ &= 2^{k+1} + (-1)^{k-1} \\ &= 2^{k+1} + (-1)^{k+1} \end{aligned}$$

Theorem 5.5: First Principle of Mathematical Induction, reformed

Let $S \subset \mathbb{Z}^+$. Suppose

1. $1 \in S$
2. If $k \in \mathbb{Z}^+$ with $k \in S$ then $k+1 \in S$

then $S = \mathbb{Z}^+$.

Definition 5.2: Binomial Coefficient

Let $n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$ satisfy $0 \leq r \leq n$. The **binomial coefficient** is

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

Remark.
$\binom{n}{r}$ is the number of ways to choose r objects from a collection of n objects.

Theorem 5.6

Let a, $b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then

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

Proof. Exercise. □

Corollary

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

Proof. Let $a = b = 1$. □

This implies if $|A| = n$ then $|\mathcal{P}(A)| = 2^n$.

5.3 Division Algorithm

Theorem 5.7: Division Algorithm

Let a, $b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.

Proof. Let $S = \{n \in \mathbb{Z} \mid n = a - bx \text{ for some } x \in \mathbb{Z}\}$ and $S_0 = \{n \in S \mid n \geq 0\}$.

Claim. $S \neq \emptyset$.

Note that $a = a - b \cdot 0$ so $a \in S$. If $a \geq 0$ then $a \in S_0$. So, suppose $a < 0$. Since $a - ba \in S$ and $a - ba = a(1-b) \geq 0$, then $a - ba \in S_0$. Hence $S_0 \neq \emptyset$.

If $0 \in S_0$ then 0 is the minimal element of S_0. Otherwise, since $S_0 \subset \mathbb{Z}^+$ is nonempty, by the WOP, S_0 has a minimal element r. Since $r \in S$ we have $r = a - bq$ for some $q \in \mathbb{Z}$ and $r \geq 0$.

Claim. $r < b$.

Suppose $r \geq b$. Then

$$0 \leq r - b = (a - bq) - b = a - b(q+1)$$

thus $r - b \in S_0$, which contradicts that r is the minimal element of S_0. So $r < b$.

Now, suppose there exist $q_1, r_1 \in \mathbb{Z}$ such that $a = bq_1 + r_1$ with $0 \leq r_1 < b$. WLOG suppose $r \geq r_1$. We have $bq + r = bq_1 + r_1$, or $b(q_1 - q) = r - r_1 \geq 0$. Suppose $q_1 - q \neq 0$. Then $r - r_1 \geq b$, a contradiction. Therefore, such r is unique. □

Corollary

Let $N \in \mathbb{Z}^+$ and $\mathbb{Z}_N = \{[a]_N \mid a \in \mathbb{Z}\}$. Then $\mathbb{Z}_n = \{[r]\}_{r=0}^{N-1}$.

Proof. Clearly $\{[r]_N\}_{r=0}^{N-1} \subset \mathbb{Z}_N$. Suppose $[a]_N \in \mathbb{Z}_N$.

> **Claim.** There exists $r \in \{0, 1, \dots, N-1\}$ such that $[a]_N = [r]_N$.

Note that $[a]_N = [r]_N$ if and only if $a \equiv r \pmod{N}$. By the division algorithm with $b = N \in \mathbb{Z}^+$ there exist unique q, $r \in \mathbb{Z}$ such that $a = Nq + r$ where $r \in \{0, 1, \dots, N-1\}$. But if $a = Nq+r$, then $N \mid a-r$. Hence $a \equiv r \pmod{N}$. □

Definition 5.3: Divisibility

Let a, $b \in \mathbb{Z}$. Then b **divides** a if there is $c \in \mathbb{Z}$ such that $a = bc$. We say a is **divisible** by b and write $b \mid a$.

We state some propositions.

1. If $a \mid 1$, then $a = \pm 1$.
2. If $a \mid b$ and $b \mid a$, then $a = \pm b$.
3. If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ for any x, $y \in \mathbb{Z}$.
4. If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. (1) Suppose $a \mid 1$. Then $1 = ac$ for some $c \in \mathbb{Z}$. Hence $a \in \mathbb{Z}^\times = \{\pm 1\}$.

(2) Suppose $a \mid b$ and $b \mid a$. Then $b = ak_1$ and $a = bk_2$ for some k_1, $k_2 \in \mathbb{Z}$. Hence $a = bk_2 = (ak_1)k_2 = a(k_1k_2)$, so $k_1k_2 = 1$. So k_1, $k_2 \in \mathbb{Z}^\times$ and $k = \pm 1$, $k_2 = \pm 1$. Thus $a = \pm b$.

(3) Since $a \mid b$, $a \mid bx$ for all $x \in \mathbb{Z}$, and since $a \mid c$, then $a \mid cy$ for all $y \in \mathbb{Z}$. Now if $a \mid \alpha$ and $a \mid \beta$ for α, $\beta \in \mathbb{Z}$ then $a \mid \alpha + \beta$. Let $\alpha = bx$ and $\beta = cy$. This completes the proof. □

Definition 5.4: Greatest Common Divisor

Let a, $b \in \mathbb{Z}$ with a and b not both zero. Then $d \in \mathbb{Z}^+$ is called the **greatest common divisor** of a and b if

- $d \mid a$ and $d \mid b$.
- If $c \in \mathbb{Z}$ with $c \mid a$ and $c \mid b$, then $c \mid d$.

We denote this d by $d = (a, b) = \gcd(a, b)$.

Theorem 5.8

The gcd of a and b exists and is unique. Moreover, there exist integers x, y such that $d = ax + by$.

Proof. Let $S = \{n \in \mathbb{Z} \mid n = ax + by \text{ for some } x, y \in \mathbb{Z}\}$. Clearly $S \subset \mathbb{Z}$ which contains a and b. By the same argument, S contains $-a$ and $-b$. Thus S contains positive integers, and by WOP, S contains a minimal positive element. Call this element d.

Claim. $d = \gcd(a, b)$.

First, note that $d \in S \Rightarrow d = ax + by$ for some x, $y \in \mathbb{Z}$. Applying the division algorithm to a and d, there exist q, r such that $a = dq + r$ where $0 \leq r < d$. But

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)q \\ &= a(1 - xq) + b(-yq), \end{aligned}$$

so $r \in S$. If $r > 0$, then it contradicts the minimality of d, so $r = 0$. Hence $a = dq$, and $d \mid a$. Similarly, $d \mid b$, and d is a common divisor of a and b.

Now, suppose $c \mid a$ and $c \mid b$. Then there exist u, $v \in \mathbb{Z}$ such that $a = uc$ and $b = vc$. Hence $d = ax + by = c(ux + vy)$, so $c \mid d$. This proves $d = \gcd(a, b)$.

For the uniqueness, suppose d and d' are the greatest common divisors of a and b. Then d, $d' \in \mathbb{Z}^+$, $d \mid d'$, and $d' \mid d$. Hence $d = d'$. □

Lemma

Let a, $b \in \mathbb{Z}$, not both zero. Suppose there exist q, $r \in \mathbb{Z}$ such that $a = bq + r$. Then $(a, b) = (b, r)$.

Let a, $b \in \mathbb{Z}^+$ with $a > b$. By repeated application of the division algorithm,

$$\begin{aligned} a &= bq_1 + r_1, & q_1, r_1 &\in \mathbb{Z}, & 0 &\leq r_1 < b \\ b &= r_1 q_2 + r_2, & q_2, r_2 &\in \mathbb{Z}, & 0 &\leq r_2 < r_1 \\ &\vdots & &\vdots & &\vdots \\ r_{n-1} &= r_n q_{n+1} + r_{n+1}, & q_{n+1} &\in \mathbb{Z}, & 0 &\leq r_{n+1} = 0 \end{aligned}$$

By the lemma, $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_n, 0) = r_n$.

Example 7

Let $a = 9180$ and $b = 1122$. Find (a, b).

Solution Division algorithm gives

$$9180 = 1122 \cdot 8 + 204$$
$$1122 = 204 \cdot 5 + 102$$
$$204 = 102 \cdot 2 + 0,$$

so $(9180, 1122) = (1122, 204) = (204, 102) = (102, 0) = 102$.

We now go back the process of the division algorithm. We have

$$\begin{aligned} 102 &= 1122 + 204(-5) \\ &= 1122 + \big(9180 + 1122(-8)\big)(-5) \\ &= 9180(-5) + 1122 \cdot 41 \end{aligned}$$

Theorem 5.9

Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Proof. ($\Rightarrow$) If $d = \gcd(a, b)$, then there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. If $d = 1$, then we are done.

($\Leftarrow$). Suppose there exist $x, y \in \mathbb{Z}$ with $ax + by = 1$. Let $d = \gcd(a, b) = 1$. We have $d \mid a$ and $d \mid b$. Then $d \mid ax + by = 1$, so $d = 1$ since $d > 0$. ☐

Recall that $\mathbb{Z}_N^\times = \{a \in \mathbb{Z}_N \mid a \text{ has a multiplicative inverse mod } N\}$.

Claim. $\mathbb{Z}_N^\times = U_N$ where $U_N = \{a \in \mathbb{Z}_N \mid \gcd(a, N) = 1\}$.

Proof. ($\supset$) Let $a \in U_N$. Then $\gcd(a, N) = 1$. By the theorem, there exist $x, y \in \mathbb{Z}$ such that $ax + Ny = 1$. Hence $ax = 1 - Ny = 1 \pmod N$, so $a \in \mathbb{Z}_N^\times$ and $a^{-1} = x$.

($\subset$) Let $a \in \mathbb{Z}_N \times$. Then there exists $x \in \mathbb{Z}_N$ such that $ax = 1 \pmod N$. Hence $N \mid ax - 1$, so $ax - 1 = Nk$ for some $k \in \mathbb{Z}$. Letting $y = -k$ gives $ax + Ny = 1$, and $\gcd(a, N) = 1$ by the theorem. ☐

Theorem 5.10

$(\mathbb{Z}_N^\times, \cdot, 1)$ is a group.

Proof. We only need to show closure. Suppose a, $b \in \mathbb{Z}_N^\times$. We claim that $(ab)^{-1} = b^{-1}a^{-1}$. We have

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b \\ &= b^{-1}1b \\ &= b^{-1}b \\ &= 1\end{aligned}$$

and $(b^{-1}a^{-1})(ab) = 1$, so $\mathbb{Z}_N^\times$ is closed under $\cdot$. □

Corollary

$\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\} = \mathbb{Z}_p - \{0\}$.

Proof. $\mathbb{Z}_p = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\}$ but the set is $\mathbb{Z}_p - \{0\}$. □

Definition 5.5: Unit Group

U_N is called the **unit group** of $\mathbb{Z}$ mod N.

Lemma

Let a, b, and $b \in \mathbb{Z}$. Suppose $a \mid bc$ and $\gcd(a, b) = 1$. Then $a \mid c$.

Proof. Suppose $a \mid bc$. Then $bc = ak$ for some $k \in \mathbb{Z}$. Also, there exist x, $y \in \mathbb{Z}$ such that $ax + by = 1$. Then

$$\begin{aligned}c &= c \cdot 1 \\ &= c(ax + by) \\ &= cax + bcy \\ &= cax + aky \\ &= a(cx + ky).\end{aligned}$$

Therefore, $a \mid c = a(ck + ky)$. □

5.4 Prime Factorization

Definition 5.6: Prime and Composite Number

An integer $p > 1$ is called a **prime number** if the only divisors of p are 1 and p. If $p > 1$ is not prime, it is called a **composite number**.

Lemma

Let $n \in \mathbb{Z}^+$ with $n > 1$. Then n is composite if and only if there exist a, $b \in \mathbb{Z}$ with $n = ab$ where $1 < a < n$ and $1 < b < n$.

Proof. Exercise. □

Lemma

Let $n \in \mathbb{Z}_{\geq 2}$. Then there exists a prime p such that $p \mid n$.

Proof. Let $T = \{n \in \mathbb{Z}_{\geq 2} \mid n \text{ has no prime divisors } \}$.

Claim. $T = \emptyset$.

Assume $T \neq \emptyset$. Since $T \subset \mathbb{Z}^+$, by WOP, there exists a minimal element $n_0 \in \mathbb{T}$. Note that n_0 is not prime, otherwise $n_0 \mid n_0$. So n_0 is composite. By the lemma above, there exist $a, b \in \mathbb{Z}$ such that $1 < a < n$ and $1 < b < n$. Now, since $a < n_0$, then $a \notin T$ by minimality of n, and hence $p \mid a$ for some prime p. Thus $p \mid n_0$, which is a contradiction. Therefore, $T = \emptyset$. □

Note that we used the transitivity of the division, so that if $a \mid b$ and $b \mid c$ then $a \mid c$.

Corollary

If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$ then we are done. Suppose $p \nmid a$. Then $a \neq 0$ and thus $\gcd(p, a) = 1$. By the previous theorem, $p \mid ab$ and $\gcd(p, a) = 1$, then $p \mid b$. □

Corollary

Let p be a prime and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid {}_{i=1}^{n} a_i$ then $p \mid a_i$ for some $i \in \{1, 2, \ldots, n\}$.

Proof. Write $\prod_{i=1}^{n} a_i = a_1 \left(\prod_{i=2}^{n} a_i\right)$. By the proposition, $p \mid a_1$ or $p \mid \prod_{i=2}^{n} a_i$. If $p \mid a_1$, then we are done. Otherwise, $p \mid \prod_{i=2}^{n} a_i$. We can repeat this process $n-1$ times until we find the desired a_i. □

Example 8

Prove that $\sqrt{2} \notin \mathbb{Q}$.

Solution Suppose $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = a/b$ for a, $b \in \mathbb{Z}$, $b \neq 0$.

Assume $\gcd(a, b) = 1$. (such a/b is called *reduced*) We have $2 = a^2/b^2$, so $a^2 = 2b^2$. Hence $2 \mid a^2$. Since 2 is prime, $2 \mid a$, and $a = 2c$ for some $c \in \mathbb{Z}$. We now get $a^2 = 4c^2 = 2b^2$, so $b^2 = 2c^2$. Hence $2 \mid b$. This contradicts $\gcd(a, b) = 1$, so such a/b does not exist.

Theorem 5.11: Fundamental Theorem of Arithmetic

Let $n \in \mathbb{Z}_{\geq 2}$. Then n is either prime or can be written as a product of prime numbers. Moreover, the product is unique up to the order in which the factors appear. Equivalently, given $n \in \mathbb{Z}_{\geq 2}$, there exist unique primes p_1, p_2, $\ldots$, p_r and unique integers α_1, α_2, $\ldots$, $\alpha_r \in \mathbb{Z}^+$ such that

$$n = \prod_{i=1}^{r} p_i^{\alpha_1}.$$

Proof. (Existence) Let $P(n)$: $n = 1$, or n is prime, or n is a product of primes. Then $P(1)$ is true.

Suppose $k \in \mathbb{Z}^+$ and $P(i)$ is true for all $1 \leq i \leq k$.

If $k = 1$, then $P(k+1) = P(2)$ is true since 2 is prime. Now suppose $k \geq 2$. The induction hypotheses implies that every i such that $2 \leq i \leq k$ is either a prime of a product of primes.

If $k+1$ is prime, then $P(k+1)$ is true. If $k+1$ is not prime, then $k+1$ is composite, so $k+1 = ab$ for integers $1 < a < k+1$ and $1 < b < k+1$. By the induction hypothesis, a and b are primes or products of primes. Thus $k+1$ is a product of primes, and $P(k+1)$ is true.

Therefore, by the second principle of induction, $P(n)$ is true for all n.

(Uniqueness) Suppose $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$ where p_1, p_2, $\ldots$, p_s, q_1, q_2, $\ldots$, q_s are primes.

Claim. $s = t$ and $p_i = q_i$ for all $i = 1$, 2, $\ldots$, s.

WLOG suppose $s \leq t$. Since $p_1 \mid n = q_1 q_2 \cdots q_t$, $p_1 \mid q_j$ for some $j \in \{1, 2, \ldots, t\}$. Now, rearrange the q_is so that $q_j = q_1$. Continuing this process, after s stems we get $p_i = q_i$ for $i = 1, 2, \ldots, s$. If $s < t$ then $1 = q_{s+1}q_{s+2}\cdots q_t$. This is impossible sine $q_i > 1$ for all i. Therefore $s = t$ and $p_i = q_i$ for all $i = 1, 2, \ldots, s$. □

So if $n \in \mathbb{Z}_{\geq 2}$, then

$$n = \prod_{i=1}^{r} p_i^{m_i}$$

where $p_1, p_2, \ldots, p_r$ are distinct primes, $p_1 < p_2 < \cdots < p_r$, and $m_1, m_2, \ldots, m_r \in \mathbb{Z}^+$.

Example 9

$22540 = 2^2 \cdot 5 \cdot 7^2 \cdot 23$.

Theorem 5.12: Euclid

There exist infinitely many primes.

Proof. Suppose there are finitely many primes $p_1, p_2, \ldots, p_n$. Then if we let $m = p_1p_2\cdots p_n + 1$, since $m > 1$, there is a prime p with $p \mid m$. Since $p_1, p_2, \ldots, p_n$ are the only primes, the p such that $p \mid m$ is p_i for some $i \in \{1, 2, \ldots, n\}$. Since $p \mid p_1p_2\ldots p_n$ and $p \mid m$, $p \mid 1$, which contradicts that p is prime. Therefore there are infinitely many primes. □

6 Selected Topics

6.1 More Group Theory

Definition 6.1: Subgroup

Let $(G, *, e)$ be a group. Let $H \subset G$ be a nonempty subset of G. Then H is a **subgroup** of G if $\forall a,\, b \in H$, $a * b \in H$ and $a^{-1} \in H$. If H is a subgroup of G, then we write $H < G$.

Example 1

Let $G = (\mathbb{Z}, +, 0)$. If we let $N \in \mathbb{Z}^+$, then $N\mathbb{Z} = \{Nk \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$, so $N\mathbb{Z} < \mathbb{Z}$.

Definition 6.2: Left Coset

Let $H < G$. Define

$$G/H = \{gH \mid g \in G\}$$

where $gH = \{gh \mid h \in H\}$. Here gH is called a **left coset** of H in G.

Right cosets are defined similarly.

Theorem 6.1

G/H is a partition of G.

Proof. 1. $gH \neq \emptyset$ since $g = ge \in gH$. $(e \in H)$

2. We need to prove $G = \bigcup_{g \in G} gH$. Let $g \in G$. Then $g \in gH$ so $g \in \bigcup_{g \in G} gH$. Conversely, $gH \subset G$ for all $g \in G$ so $\bigcup_{g \in G} gH \subset G$.

3. We need to show if $g_1 H \neq g_2 H$ then $g_1 H \cap g_2 H = \emptyset$. Suppose $g_1 H \cap g_2 H \neq \emptyset$. Let $x \in g_1 H \cap g_2 H$, then $x = g_1 h_1 = g_2 h_2$ for some $h_1,\, h_2 \in H$. (must show that $g_1 J \subset g_2 H$ and vise versa: exercise) $\square$

Definition 6.3: Abelian Group

A group $(G, *, e)$ is abelian if the binary operation $*$ is commutative.

Theorem 6.2

If G is an abelian group and $H < G$, then G/H is a group under the binary operation $g_1H * g_2H = (g_1 * g_2)H$.

Proof. Exercise. □

Let $G = \mathbb{Z}$ and $H = N\mathbb{Z} < \mathbb{Z}$ where the group operation is addition. Since addition is commutative, the cosets $\mathbb{Z}/N\mathbb{Z} = \{a + N\mathbb{Z} \mid a \in \mathbb{Z}\}$ forms a group. Note that $a + N\mathbb{Z} = \{a + Nk \mid k \in \mathbb{Z}\} = [a]_N$, the equivalence classes modulo N.

6.2 Field Theory

Definition 6.4: Field

A **field** is a nonempty set with two binary operations: addition and multiplication satisfying the following axioms:

1. F is an abelian group under $+$
2. $F^\times$ is a commutative group under $\cdot$ where $F^\times = F - \{0\}$.
3. $a \cdot (b + c) = a \cdot b + a \cdot c$. (Left distribution)

Example 2

$\mathbb{Z}$ is not a field since $\mathbb{Z}_{\text{unit}} = \{\pm 1\} \neq \mathbb{Z}^\times = \mathbb{Z} - \{0\}$.

Example 3

$\mathbb{Q}$ and $\mathbb{R}$ are fields.

Example 4

Let $N \in \mathbb{Z}^+$. Then $(\mathbb{Z}_N, +, 0)$ is an abelian group. Also, $(U_N, \cdot, 1)$ is an abelian group where $U_N = \{\text{set of } a \in \mathbb{Z}_N \text{ with a multiplicative inverse}\} = \{a \in \mathbb{Z}_N \mid \gcd(a, N) = 1\}$. Finally, $a \cdot (b + c) = a \cdot b + a \cdot c$. So $\mathbb{Z}_N$ is a field if and only if $U_N = \mathbb{Z}_N - \{0\}$.

Theorem 6.3

$\mathbb{Z}_N$ is a field if and only if $N = p$ is prime.

Proof. ($\Leftarrow$) Suppoose $N = p$ is prime. Then

$$U_p = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\} = \{1, 2, \ldots, p - 1\} = \mathbb{Z}_p - \{0\}.$$

($\Rightarrow$) We prove the contrapositive, i.e. if N is composite then $\mathbb{Z}_N$ is not a field. Suppose N is composite. Then $N = ab$ for a, $b \in \mathbb{Z}$ where $1 < a < N$ and $1 < b < N$. In particular,

$$[a] \cdot [b] = [ab] = [N] = [0].$$

Also note that $[a] \neq [0]$ and $[b] \neq [0]$.

> **Claim.** $[a] \notin U_N$.

Suppose $a \in U_N$. Hence there is $[x] \in \mathbb{Z}_N$ such that $[x][a] = [1]$. It follows that $([x][a])\,[b] = [1][b] = [b]$. Butt $[a][b] = [0]$, so $[b] = [x][0] = [0]$, contradicting $[b] \neq [0]$. Therefore, $\mathbb{Z}_N$ is not a field if N is composite, and this completes the proof. □

> **Remark.**
> $\mathbb{Z}_p$ is called the *finite field of order* p and denoted $\mathbb{F}_p$.

Definition 6.5: Polynomial

Let F be a field. A **polynomial** over F in the varible x is an expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_N x^N$$

where $a_0, a_1, a_2, \ldots, a_N \in F$, and $N \in \mathbb{Z}_{\geq 0}$.

The a_is are called the *coefficients* of $f(x)$. If $a_N \neq 0$ then a_N is called the *leading coefficient*, and a_0 is called the *constant term* of $f(x)$. N is called the *degree* of $f(x)$, denoted $\deg(f(x))$. If $f(x) = a_0 \neq 0$, then $f(x)$ is called a *nonzero constant polynomial* and has degree 0. If $f(x) = 0$ then $f(x)$ is called the *zero polynomial*, which is not assigned a degree.

Definition 6.6: $F(x)$

$F[x]$ is the set of all polynomials with coefficients in F.

Let

$$f(x) = a_0 + a_1 x + \cdots + a_N x^N$$
$$g(x) = b_0 + b_1 x + \cdots + b_M x^M.$$

If $N \neq M$, say $N > M$, and write

$$g(x) = \sum_{i=0}^{M} b_i x^i + b_{m+1} x^{m+1} + \cdots + b_N x^N$$

where $b_i = 0$ for $i = M + 1, \ldots, N$. Then

$$f(x) + g(x) = \sum_{i=0}^{N} (a_i + b_i)x^i \in F[x].$$

Thus $F[x]$ is closed under addition. For multiplication, we have

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1 x + \cdots + a_N x^N)(b_0 + b_1 x + \cdots + b_M x^M) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_N b_M x^{N+M}. \end{aligned}$$

The coefficient of x^k in fg is

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i}$$

where $a_i = 0$ if $i > N$ and $b_j = 0$ if $j > M$.

Remark.

- $f(x) = 0$ is the additive identity, and $f(x) = 1$ is the multiplicative identity.
- $(F[x], +, 0)$ is an abelian group.
- There exist a nonzero polynomial without a multiplicative inverse, so $F[x]$ is not a field.

Example 5

Let $F = \mathbb{Z}_5$. Let $f(x) = 4 + 2x + 3x^3$ and $g(x) = 1 + 4x^2 + x^3$. Then $f(x)g(x) = 4 + 2x + x^2 + 2x^4 + 2x^5 + 3x^6$.

Theorem 6.4

Let F be a field and $f(x)$, $g(x) \in F[x]$ with $f(x) \not\equiv 0$, $g(x) \not\equiv 0$, and $f(x) + g(x) \not\equiv 0$. Then

1. $\deg\big(f(x) + g(x)\big) \leq \max\{\deg\big(f(x)\big), \deg\big(g(x)\big)\}$
2. $\deg\big(f(x)g(x)\big) = \deg\big(f(x)\big) + \deg\big(g(x)\big)$.

Remark.

The symbol $\not\equiv$ is used for identically zero, which means the value is zero for any x.

Proof. (1) Let $\deg\big(f(x)\big) = N$ and $\deg\big(g(x)\big) = M$. If $N > M$, then $\deg\big(f(x) + g(x)\big) = N$. Similarly, if $M > N$ then $\deg\big(f(x) + g(x)\big) = M$. If $N > M$, then $\max\{\deg\big(f(x)\big), \deg\big(g(x)\big)\} = \max\{N, M\}, N$. Similarly, if $M > N$ then

$\max\{\deg\big(f(x)\big), \deg\big(f(x)\big)\} = M$. Finally, suppose $N = M$. Then, $\deg\big(f(x) + g(x)\big) = N$ unless $a_N = -b_N$, which in this case $\deg\big(f(x)+g(x)\big) \leq N-1 < N$. This completes the proof.

(2) Exercise. □

Theorem 6.5

Let F be a field, and $f(x)$, $g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist $q(x)$, $r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

where $r(x) = 0$ or $0 \leq \deg\big(r(x)\big) < \deg\big(g(x)\big)$.

Proof. Define

$$S = \{h(x) \in F[x] \mid h(x) = f(x) - g(x)q(x) \text{ for some } q(x) \in F[x]\}.$$

Then $S \neq \emptyset$ since $f(x) \in S$ (this can be attained by taking $q(x) = 0$). If the zero polynomial is in S, then $0 = f(x) - g(x)q(x)$ for some $q(x) \in F[x]$, which proves the theorem with $r(x) = 0$. So, suppose the zero polynomial is not in S. Define

$$D = \{n \in \mathbb{Z}_{\geq 0} \mid \deg\big(h(x)\big) = n \text{ for some } h(x) \in S\}$$

If S contains a constant polynomial, then $r(x)$ is constant and has degree 0. In particular, $\alpha = f(x) - g(x)q(x)$ for some $q(x) \in F[x]$, so $f(x) = g(x)q(x) + r(x)$ with $r(x) = \alpha$ and $\deg\big(r(x)\big) = 0$.

Now, if $D \subset \mathbb{Z}^+$, $D \neq \emptyset$, and $r(x)$ of smallest degree exists by the WOP. Since $r(x) \in S$ we have $r(x) = f(x) - g(x)q(x)$ or $f(x) = g(x)q(x) + r(x)$ for some $q(x) \in F[x]$. We must show that $\deg\big(r(x)\big) < \deg\big(g(x)\big)$. Suppose $\deg\big(r(x)\big) \geq \deg\big(g(x)\big)$. Let $m = \deg\big(g(x)\big)$ and $t = \big(r(x)\big)$. We have

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

$$r(x) = c_0 + c_1x + \cdots + c_tx^t$$

for $b_0, \ldots, b_m, c_0, \ldots, c_t \in F$ with $b_m, c_t \neq 0$. Define $r_1(x) = r(x) - c_tb_m^{-1}x^{t-m}g(x) \in S$.

Claim. $r_1(x) \in S$ and $\deg\big(r_1(x)\big) < \deg\big(r(x)\big)$.

Note that

$$c_tb_m^{-1}x^{t-m}g(x) = c_tb_m^{-1}b_0x^{t-m} + c_tb_m^{-1}b_1x^{t+1-m} + \cdots + c_tx^t$$

Hence $\deg\big(r_1(x)\big) < \deg\big(r(x)\big)$. This gives a contradiction and completes the proof. □

Corollary

Let $f(x) \in F[x]$ and $c \in F$. Then there exists $q * x(\in F[x]$ such that

$$f(x) = (x - c)q(x) + f(c).$$

Proof. Apply the division algorithm to get $g(x) = x - c$. Then $r(x)$ has degree 0, so it must be a constant. Substitute $x = c$ to get $r(c) = r = f(c)$. □

Corollary

If $f(x) \in F[x]$ and $f(x) = 0$ for some $c \in F$ then $f(x) = (x - c)g(x)$ for some $g(x) \in F[x]$ with $\deg\big(g(x)\big) < \deg\big(f(x)\big)$.