Abstract algebras

Yanhua Wang
Shanghai University of Finance and Economics

2022.9

1. Chapter I. Preliminaries

1.1 Sets

Sets

- A *set* is a well-defined collection of objects. The objects that belong to a set are called *elements* or *members*.

Sets

- A *set* is a well-defined collection of objects. The objects that belong to a set are called *elements* or *members*.
- Write a set as $A, B, C, \cdots$.

Sets

- A *set* is a well-defined collection of objects. The objects that belong to a set are called *elements* or *members*.
- Write a set as $A, B, C, \cdots$.
- $a \in A$

Sets

- A *set* is a well-defined collection of objects. The objects that belong to a set are called *elements* or *members*.
- Write a set as $A, B, C, \cdots$.
- $a \in A$
- $a \notin A$

Sets

- A *set* is a well-defined collection of objects. The objects that belong to a set are called *elements* or *members*.
- Write a set as $A, B, C, \cdots$.
- $a \in A$
- $a \notin A$
- Statement, list all elements

Sets

- $\mathbb{N}$ is the set of all natural numbers $\{0, 1, 2, 3, \cdots\}$.
  $\mathbb{Z}$ is the set of all integers $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$.
  $\mathbb{Z}^+$ is the set of all integers $\{1, 2, 3, \cdots\}$.
  $\mathbb{Q}$ is the set of all rational numbers: fraction of the form $\frac{a}{b}$, for $a, b \in \mathbb{Z}$ and $b \neq 0$.

Sets

- $\mathbb{N}$ is the set of all natural numbers $\{0, 1, 2, 3, \cdots\}$.
  $\mathbb{Z}$ is the set of all integers $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$.
  $\mathbb{Z}^+$ is the set of all integers $\{1, 2, 3, \cdots\}$.
  $\mathbb{Q}$ is the set of all rational numbers: fraction of the form $\frac{a}{b}$, for $a, b \in \mathbb{Z}$ and $b \neq 0$.
- $\mathbb{R}$ is the set of all real numbers.
  $\mathbb{C}$ is the set of all complex numbers.
  $\emptyset$ is an empty set.

Sets

- Let A and B be two sets, we say A is *equal* to B if A and B have the same elements, denoted by $A = B$.

Sets

- Let A and B be two sets, we say A is *equal* to B if A and B have the same elements, denoted by $A = B$.
- A is *different* from B if A is not equal to B, i.e. $A \neq B$.

Sets

- Let A and B be two sets, we say A is *equal* to B if A and B have the same elements, denoted by $A = B$.
- A is *different* from B if A is not equal to B, i.e. $A \neq B$.
- A is *contained* in B or that B contains A if every element of A is also an element of B, write $A \subseteq B$ or $B \supseteq A$. If $A \subseteq B$, we say that A is a subset of A.

Sets

- Let A and B be two sets, we say A is *equal* to B if A and B have the same elements, denoted by $A = B$.
- A is *different* from B if A is not equal to B, i.e. $A \neq B$.
- A is *contained* in B or that B contains A if every element of A is also an element of B, write $A \subseteq B$ or $B \supseteq A$. If $A \subseteq B$, we say that A is a subset of A.
- We have $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Sets

- Let A and B be two sets, we say A is *equal* to B if A and B have the same elements, denoted by $A = B$.
- A is *different* from B if A is not equal to B, i.e. $A \neq B$.
- A is *contained* in B or that B contains A if every element of A is also an element of B, write $A \subseteq B$ or $B \supseteq A$. If $A \subseteq B$, we say that A is a subset of A.
- We have $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
- If B is a subset of A and B is different from A, we write $B \subset A$. We say B is a proper subset of A. The inclusion of B in A is *strict*.

Sets

- The *union* $A \cup B$ of two sets A and B is the set whose elements are all elements of A and of B:

$$A \cup B = \{x | x \in A \text{ or } x \in B\}.$$

Sets

- The *union* $A \cup B$ of two sets A and B is the set whose elements are all elements of A and of B:

$$A \cup B = \{x | x \in A \text{ or } x \in B\}.$$

- The *intersection* of A and B is the set whose elements are elements of A and of B:

$$A \cap B = \{x | x \in A \text{ and } x \in B\}.$$

Sets

- If $A \bigcap B = \emptyset$ and $X = A \bigcup B$, we say X is the *disjoint union* of A and B.

Sets

- If $A \bigcap B = \emptyset$ and $X = A \bigcup B$, we say X is the *disjoint union* of A and B.
- The *difference* of A and B is $A \backslash B = \{x | x \in A \text{ and } x \notin B\}$. Let A be a subset of a given set X.

Sets

- If $A \bigcap B = \emptyset$ and $X = A \bigcup B$, we say X is the *disjoint union* of A and B.
- The *difference* of A and B is $A \backslash B = \{x | x \in A \text{ and } x \notin B\}$. Let A be a subset of a given set X.
- The difference $X \backslash A$ is called the *complement* set of A in X. We write $C(A)$ or A'.

Sets

Proposition

Let A and B be sets. Then

(1) $A \cup B = A$ if and only if $B \subseteq A$.

(2) $A \cup B = \emptyset$ if and only if $A = \emptyset$ and $B = \emptyset$.

(3) $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

(4) $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

Sets

Proposition

Let A and B be sets. Then
(1) Commutative law of union:

$$A \cup B = B \cup A.$$

(2) Commutative law of intersection:

$$A \cap B = B \cap A.$$

(3) Associative law of union:

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

Proposition

(4) Associative law of intersection:

$$(A \cap B) \cap C = A \cap (B \cap C).$$

(5) Distributive law of intersection with respect to union:

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

(6) Distributive law of union with respect to intersection:

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

Sets

Proposition

Let A be a subset of set X. Then

(1) $(A')' = A$.

(2) $A' \cup A = X$.

(3) $A' \cap A = \emptyset$.

Sets

Proposition

Let A, B *and* C *be sets. Then*

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

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

(3) $(B \cup C) \backslash A = (B \backslash A) \cup (C \backslash A)$.

(4) $(B \cap C) \backslash A = (B \backslash A) \cap (C \backslash A)$.

Sets

Proposition

Let A and B be subsets of a set X. Then
(1) $A \subseteq B$ if and only if $B' \subseteq A'$.

(2) $(A \cup B)' = A' \cap B'$.

(3) $(A \cap B)' = A' \cup B'$.

Sets

Definition

Let X be a set. The power set of X is the set whose elements are the subsets of X. We denote it by $P(X) = \{A | A \subseteq X\}$.

-

Sets

Definition

Let X be a set. The power set of X is the set whose elements are the subsets of X. We denote it by $P(X) = \{A | A \subseteq X\}$.

-

Example

Let $X = \{1, 2\}$, then $P(X) = \{\emptyset, X, \{1\}, \{2\}\}$. If there are n elements in X, then $|P(X)| = 2^n$, where $|P(X)|$ denote the order of $P(X)$.

-

Sets

- Exercise: What is $P(X)$?

Sets

- Exercise: What is $P(X)$?
- (1)If $X = \{1, 2, 3\}$.

Sets

- Exercise: What is $P(X)$?
- (1)If $X = \{1, 2, 3\}$.
- (2)If $X = \emptyset$.

Sets

- Exercise: What is $P(X)$?
- (1)If $X = \{1, 2, 3\}$.
- (2)If $X = \emptyset$.
- (3)If $X = \{\emptyset\}$.

1.2 Maps

Maps

Definition

A map(or function) f consists of a nonempty set X, of a nonempty set Y and of a law that assigns to each $x \in X$, exactly one element, denoted by $f(x)$ of Y. Denote

$$f : X \to Y : x \mapsto y.$$

- X is called the domain of map f, Y is called the codomain of map f, $f(x)$ is called the image (value) of x, x is called the preimage of $f(x)$;

Maps

Examples

- (1) $f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$ is a map.

Maps

Examples

- (1) $f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$ is a map.
- (2) $f : \mathbb{N} \to \mathbb{Z} : x \mapsto -x$ is a map.

Maps

Examples

- (1) $f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$ is a map.
- (2) $f : \mathbb{N} \to \mathbb{Z} : x \mapsto -x$ is a map.
- (3) $f : \mathbb{Q} \to \mathbb{Z}$, where

$$\mathbb{Q} = \{x | x = \frac{p}{q} | p, q \in \mathbb{Z}\},$$

define $f(\frac{p}{q}) = p$.

Maps

Examples

- (1) $f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$ is a map.
- (2) $f : \mathbb{N} \to \mathbb{Z} : x \mapsto -x$ is a map.
- (3) $f : \mathbb{Q} \to \mathbb{Z}$, where

$$\mathbb{Q} = \{x | x = \frac{p}{q} | p, q \in \mathbb{Z}\},$$

  define $f(\frac{p}{q}) = p$.
- f is not a mapping since $f(\frac{1}{2}) = 1$, but $f(\frac{2}{4}) = 2$.

Maps

Examples

- (1) $f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$ is a map.
- (2) $f : \mathbb{N} \to \mathbb{Z} : x \mapsto -x$ is a map.
- (3) $f : \mathbb{Q} \to \mathbb{Z}$, where

$$\mathbb{Q} = \{x | x = \frac{p}{q} | p, q \in \mathbb{Z}\},$$

  define $f(\frac{p}{q}) = p$.
- f is not a mapping since $f(\frac{1}{2}) = 1$, but $f(\frac{2}{4}) = 2$.
- Two maps f and g are equal if and only if they have the same domain, codomain and the same law, that is, for every $x \in X$, we have $f(x) = g(x)$.

Maps

Some particular maps:

- (1) Identity map or Identity: Let X be a nonempty set. $1_x : X \to X : x \mapsto x$.

Maps

Some particular maps:

- (1) Identity map or Identity: Let X be a nonempty set. $1_x : X \to X : x \mapsto x$.

- (2) Inclusion map: If A is a nonempty subset of X, the conclusion map of A in X is the function denoted by i_A with A as a domain, X as a codomain, $i_A : A \to X : a \mapsto a$, given by i_A(a)=a.

Maps

Some particular maps:

- (1) Identity map or Identity: Let X be a nonempty set. $1_x : X \to X : x \mapsto x$.

- (2) Inclusion map: If A is a nonempty subset of X, the conclusion map of A in X is the function denoted by i_A with A as a domain, X as a codomain, $i_A : A \to X : a \mapsto a$, given by i_A(a)=a.

- Note that if A is a nonempty proper subset of X. 1_a and i_a have different domain, thus $1_A \neq i_A$. $1_A = i_A$ if and only if $A = X$.

Maps

- (3) Restriction: Let $f : X \to Y$ be a map and A be a nonempty subset of X. The map $f|_A : A \to Y : a \mapsto f(a)$ is called the restriction of f to A. In particular $i_A = 1_X|_A$.

Maps

- (3) Restriction: Let $f : X \to Y$ be a map and A be a nonempty subset of X. The map $f|_A : A \to Y : a \mapsto f(a)$ is called the restriction of f to A. In particular $i_A = 1_X|_A$.

- (4) Constant map: Let X be a nonempty set and let y be a fixed element of Y. The map $f_y : X \to Y : x \mapsto y$ is called the constant map. Note that $f_y(X) = \{y\}$ and $\mathrm{Im}(f) = \{f(x) | x \in X\} \subseteq Y$.

Maps

Examples:

- (1) $f_1 : \mathbb{N} \to \mathbb{N} : x \mapsto 2x$.

$$\mathrm{Im}(f_1) = \{y | \exists\, x \in \mathbb{N}\,,\ \text{such that}\ \ y = 2x\}$$

  is the set of even natural numbers.

Maps

Examples:

- (1) $f_1 : \mathbb{N} \to \mathbb{N} : x \mapsto 2x$.

  $$\mathrm{Im}(f_1) = \{y | \exists\, x \in \mathbb{N}\,, \text{ such that } \; y = 2x\}$$

  is the set of even natural numbers.
- (2) $f_2 : \mathbb{N} \to \mathbb{N} : x \mapsto 2x + 1$.

  $$\mathrm{Im}(f_2) = \{y | \exists\, x \in \mathbb{N}\,, \text{ such that } \; y = 2x + 1\}$$

  is the set of odd natural numbers.

Maps

Examples:

- (1) $f_1 : \mathbb{N} \to \mathbb{N} : x \mapsto 2x$.

$$\mathrm{Im}(f_1) = \{y | \exists\, x \in \mathbb{N}\,,\ \text{such that}\ \ y = 2x\}$$

is the set of even natural numbers.

- (2) $f_2 : \mathbb{N} \to \mathbb{N} : x \mapsto 2x + 1$.

$$\mathrm{Im}(f_2) = \{y | \exists\, x \in \mathbb{N}\,,\ \text{such that}\ \ y = 2x + 1\}$$

is the set of odd natural numbers.

- (3) $f_3 : \mathbb{Z} \to \mathbb{Z} : x \mapsto 3x$. $\mathrm{Im}(f_3)$ is the set of integers of multiple of 3.

Maps

Examples:

- (1) $f_1 : \mathbb{N} \to \mathbb{N} : x \mapsto 2x$.

$$\mathrm{Im}(f_1) = \{y | \exists\, x \in \mathbb{N}\,, \text{ such that } \ y = 2x\}$$

  is the set of even natural numbers.
- (2) $f_2 : \mathbb{N} \to \mathbb{N} : x \mapsto 2x + 1$.

$$\mathrm{Im}(f_2) = \{y | \exists\, x \in \mathbb{N}\,, \text{ such that } \ y = 2x + 1\}$$

  is the set of odd natural numbers.
- (3) $f_3 : \mathbb{Z} \to \mathbb{Z} : x \mapsto 3x$. $\mathrm{Im}(f_3)$ is the set of integers of multiple of 3.
- (4) $f_4 : \mathbb{Z} \to \mathbb{Z} : x \mapsto -3x$. $\mathrm{Im}(f_4)$ is the set of integers of multiple of -3. We have $\mathrm{Im}(f_4) = \mathrm{Im}(f_3)$, but $f_4 \neq f_3$.

Maps

- (5) $f_y : X \to Y : x \to y$. $\mathrm{Im}(f_y) = \{y\}$.

Maps

- (5) $f_y : X \to Y : x \to y$. $\mathrm{Im}(f_y) = \{y\}$.
- (6) $i_A : A \to X : a \mapsto a$. $i_A(A) = A$.

Maps

- (5) $f_y : X \to Y : x \to y$. $\mathrm{Im}(f_y) = \{y\}$.
- (6) $i_A : A \to X : a \mapsto a$. $i_A(A) = A$.
- (7) $f_5 : \mathbb{Q} \to \mathbb{Q} : x \mapsto 3x$. $\mathrm{Im}(f_5) = \mathbb{Q}$.

Maps

Definition

Let $f : X \to Y$ be a map, f is said to be a surjective map(or onto) if $Im(f) = Y$.

-

Maps

Definition

Let $f : X \to Y$ be a map, f is said to be a surjective map(or onto) if $Im(f) = Y$.

-
- f is surjective $\iff \forall y \in Y, \exists x \in X$, such that $f(x) = y$.

Maps

Definition

Let $f : X \to Y$ be a map, f is said to be injective(or one-to-one) if given any $x, x' \in X$, $x \neq x'$ implies that $f(x) \neq f(x')$.

-

Maps

Definition

Let $f : X \to Y$ be a map, f is said to be injective(or one-to-one) if given any $x, x' \in X$, $x \neq x'$ implies that $f(x) \neq f(x')$.

-

Definition

Let $f : X \to Y$ is called bijective if f is surjective and injective.

-

Maps

Definition

Let $f : X \to Y$ be a map, f is said to be injective(or one-to-one) if given any $x, x' \in X$, $x \neq x'$ implies that $f(x) \neq f(x')$.

-

Definition

Let $f : X \to Y$ is called bijective if f is surjective and injective.

-
- f is bijective $\iff \forall y \in Y$, there exists an unique $x \in X$, such that $f(x) = y$.

Maps

- Let $f : X \to Y$ and $g : Y \to Z$ be maps, such that the codomain of f coincides with the domain of g. Then the *composition* of f and g is given by $g \circ f : X \to Z : x \to g(f(x))$.

Maps

- Let $f : X \to Y$ and $g : Y \to Z$ be maps, such that the codomain of f coincides with the domain of g. Then the *composition* of f and g is given by $g \circ f : X \to Z : x \to g(f(x))$.
- Let $f : Z \to Z : x \to x + 1, g : Z \to Z : x \to x^2$, then $g \circ f : Z \to Z : x \to (x + 1)^2$.

Maps

- Let $f : X \to Y$ and $g : Y \to Z$ be maps, such that the codomain of f coincides with the domain of g. Then the *composition* of f and g is given by $g \circ f : X \to Z : x \to g(f(x))$.
- Let $f : Z \to Z : x \to x + 1, g : Z \to Z : x \to x^2$, then $g \circ f : Z \to Z : x \to (x + 1)^2$.
- Let $f : X \to Y$ and A be a nonempty subset of X, then $f|_A = f \circ i_A : a \to f(a)$.

Maps

- Let $f : X \to Y$ and $g : Y \to Z$ be maps, such that the codomain of f coincides with the domain of g. Then the *composition* of f and g is given by $g \circ f : X \to Z : x \to g(f(x))$.
- Let $f : Z \to Z : x \to x + 1, g : Z \to Z : x \to x^2$, then $g \circ f : Z \to Z : x \to (x + 1)^2$.
- Let $f : X \to Y$ and A be a nonempty subset of X, then $f|_A = f \circ i_A : a \to f(a)$.
- $f : Z \to Z, g : Z \to Z$, then $g \circ f \neq f \circ g$.

Maps

Proposition

Let $f : X \to Y, g : Y \to Z, h : Z \to T$ *be maps. Then*
(1) $f \circ 1x = f = 1y \circ f$.
(2) $h \circ (g \circ f) = (h \circ g) \circ f$.

Maps

Proposition

Let $f : X \mapsto Y$ and $g : Y \mapsto Z$ be maps
(1) If f and g are both injective, then $g \circ f$ is injective.
(2) If f and g are both surjective, then $g \circ f$ is surjective.
(3) If $g \circ f$ is injective, then f is injective.
(4) If $g \circ f$ is surjective, then g is surjective.

Maps

- Consider the following maps

$$f : \mathbb{N} \to \mathbb{Z} : x \mapsto -x$$

and

$$g : \mathbb{Z} \to \mathbb{N} : x \mapsto x^2$$

Then $g \circ f$ is injective, but g is neither injective nor not surjective.

Maps

- Consider the following maps

$$f : \mathbb{N} \to \mathbb{Z} : x \mapsto -x$$

  and

$$g : \mathbb{Z} \to \mathbb{N} : x \mapsto x^2$$

  Then $g \circ f$ is injective, but g is neither injective nor not surjective.

- Consider the following maps:

$$f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$$

  and

$$g : \mathbb{R} \to \mathbb{R}^+ \cup \{0\} : x \mapsto x^2.$$

  We have $g \circ f$ is surjective. So g is surjective, but f is neither surjective nor injective.

Maps

Corollary

Let $f : X \to Y$ and $g : Y \to Z$ be maps,
(1) If f and g are both bijective, then also $g \circ f$ is bijective.
(2) If $g \circ f$ is bijective, then f is injective and g is surjective.

- Let $f : \mathbb{N} \to \mathbb{Z} : x \mapsto -x$, and $g : \mathbb{Z} \to \mathbb{N} : x \mapsto |x|$. Then $g \circ f = 1_N$. We have f is injective and g is surjective.

Maps

Definition

Let $f : X \to Y$ be a map. A map $g : Y \to X$ is called a *left inverse* of f if $g \circ f = 1_X$. A map $h : Y \to X$ is called a *right inverse* of f if $f \circ h = 1_Y$. A map $g : Y \to X$ is called a *two-sided inverse*, if g is a left inverse and a right inverse, i.e. $g \circ f = 1_X$, $f \circ g = 1_Y$.

Theorem

Let $f : X \to Y$ be a map , then
(1) f is injective if and only if f has (at least) a left inverse.
(2) f is surjective if and only if f has (at least) a right inverse.

-

Maps

Examples:

- (1) Let $f : \mathbb{N} \to \mathbb{N}$ be the map defined by $f(x) = x + 2$. Then f is injective and $Im(f) = \{x \in \mathbb{N} | x \geq 2\}$.
  The map $g_0 : \mathbb{N} \to \mathbb{N}$ defined by $g_0(x) = x - 2$ if $x \geq 2$ and $g_0(x) = 0$ if $x < 2$, is a left inverse of f.

Maps

Examples:

- (1) Let $f : \mathbb{N} \to \mathbb{N}$ be the map defined by $f(x) = x + 2$. Then f is injective and $Im(f) = \{x \in \mathbb{N} | x \geq 2\}$. The map $g_0 : \mathbb{N} \to \mathbb{N}$ defined by $g_0(x) = x - 2$ if $x \geq 2$ and $g_0(x) = 0$ if $x < 2$, is a left inverse of f.
- (2) Let $f : \mathbb{Z} \to \mathbb{N}$ be the map defined by $f(x) = |x|$. The map $h = i_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ is a right inverse of f. Also $g : \mathbb{N} \to \mathbb{Z}$ defined by $g(x) = -x$ is a right inverse of f.

Maps

Corollary: Let $f : X \to Y$ be a map. The following are equivalent

- (1) f is bijective.
  (2) f has a left inverse and a right inverse.
  (3) f has a two-sided inverse.

Maps

Corollary: Let $f : X \to Y$ be a map. The following are equivalent

- (1) f is bijective.
  (2) f has a left inverse and a right inverse.
  (3) f has a two-sided inverse.
- Moreover, if f satisfies one of the above conditions, then
  (i) every left inverse of f is a two-sided inverse of f.
  (ii) every right inverse of f is a two-sided inverse of f.
  (iii) f has a unique two-sided inverse.

Maps

Corollary: Let $f : X \to Y$ be a map. The following are equivalent

- (1) f is bijective.
  (2) f has a left inverse and a right inverse.
  (3) f has a two-sided inverse.
- Moreover, if f satisfies one of the above conditions, then
  (i) every left inverse of f is a two-sided inverse of f.
  (ii) every right inverse of f is a two-sided inverse of f.
  (iii) f has a unique two-sided inverse.
- Such an inverse of f is called the *inverse* of f and it is denoted by f^{-1}. Also f^{-1} is bijective and $((f^{-1})^{-1}) = f$.

Maps

Corollary

Let $f : X \to Y$ *and* $g : Y \to Z$ *be bijections. Then* $g \circ f : X \to Z$ *is a bijection and* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Maps

Theorem

A map is invertible if and only if it is both injective (one-to-one) and surjective (onto).

Maps

Proposition

Let $f : X \longrightarrow Y$ *be a map and left* $(A_i)_{i\in I}$ *be a family of subsets of* X*. Then*

$$(1) f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$$

$$(2) f(\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I} f(A_i)$$

Maps

Proposition

Let $f : X \longrightarrow Y$ *be an injective map and left* $(A_i)_{i\in I}$ *be a family of subsets of* X*. Then*

$$f(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f(A_i)$$

Maps

Example

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the constant map equal to 0 Let $A_1 = \{x \in \mathbb{Z} | x \leq 0\}$, $A_2 = \{x \in \mathbb{Z} | x < 0\}$. Then $A_1 \bigcap A_2 = \emptyset$, while $f(A_1) = \{0\} = f(A_2)$, so that $f(A_1) \bigcap f(A_2) = \{0\}$.

1.3 Cartesian product

Cartesian product

Definition

Given sets X and Y, we can define a new set

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

$X \times Y$ is called the Cartesian product of X and Y.

- Examples: Let $X = \{x, y\}, Y = \{1, 2, 3\}$, and $Z = \emptyset$.

Cartesian product

Definition

Given sets X and Y, we can define a new set

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

$X \times Y$ is called the Cartesian product of X and Y.

- Examples: Let $X = \{x, y\}, Y = \{1, 2, 3\}$, and $Z = \emptyset$.
- $X \times Y = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$
- $X \times Z = \emptyset$.

Cartesian product

Definition

Given sets X and Y, we can define a new set

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

$X \times Y$ is called the Cartesian product of X and Y.

- Examples: Let $X = \{x, y\}, Y = \{1, 2, 3\}$, and $Z = \emptyset$.
- $X \times Y = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$
- $X \times Z = \emptyset$.
- $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

Cartesian product

Definition

Given sets X and Y, we can define a new set

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

$X \times Y$ is called the Cartesian product of X and Y.

- Examples: Let $X = \{x, y\}, Y = \{1, 2, 3\}$, and $Z = \emptyset$.
- $X \times Y = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$
- $X \times Z = \emptyset$.
- $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.
- Cartesian product of n sets to be

  $$X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \cdots, x_n) | x_i \in X_i, i = 1, \cdots n\}.$$

  and $X^n = X \times X \times \cdots \times X$.

Cartesian product

Definition

Let X be a set. We say X admits a *binary operation* if there exists a map $f : X \times X \to X$.

-

Cartesian product

Definition

Let X be a set. We say X admits a *binary operation* if there exists a map $f : X \times X \to X$.

-
- Let X and Y be sets. A *relation* R between X and Y is a subset of the set product $X \times Y$. If $(x, y) \in R$, then x is said to be related to y by R and we write xRy.

Cartesian product

- Examples

Cartesian product

- Examples
- (1) let X be a set, define $\triangle(x) = \{(x, y)|x, y \in X, x = y\} \subseteq X \times X$. $\triangle(x)$ is a binary relation of $X \times X$. We call $\triangle(x)$ as diagonal relation of X.

Cartesian product

- Examples
- (1) let X be a set, define $\triangle(x) = \{(x, y) | x, y \in X, x = y\} \subseteq X \times X$. $\triangle(x)$ is a binary relation of $X \times X$. We call $\triangle(x)$ as diagonal relation of X.
- (2) Let P be the set of prime numbers. Define $R = \{(x, y) \in P \times \mathbb{N} | x \text{ divides } y\}$, R is a binary relation of $P \times \mathbb{N}$. R is called divisibility relation.

1.4 Equivalence relations and equivalence classes

Equivalence

Definition

An *equivalence relation* on a set X is a relation $R \subseteq X \times X$ satisfy

- (1) reflexive property: $(x, x) \in R$ for all $x \in X$;

Equivalence

Definition

An *equivalence relation* on a set X is a relation $R \subseteq X \times X$ satisfy

- (1) reflexive property: $(x, x) \in R$ for all $x \in X$;
- (2) symmetric property: $(x, y) \in R$ implies $(y, x) \in R$;

Equivalence

Definition

An *equivalence relation* on a set X is a relation $R \subseteq X \times X$ satisfy

- (1) reflexive property: $(x, x) \in R$ for all $x \in X$;
- (2) symmetric property: $(x, y) \in R$ implies $(y, x) \in R$;
- (3) transitive property: $(x, y), (y, z) \in R$ imply $(x, z) \in R$.

Equivalence

Definition

An *equivalence relation* on a set X is a relation $R \subseteq X \times X$ satisfy

- (1) reflexive property: $(x, x) \in R$ for all $x \in X$;
- (2) symmetric property: $(x, y) \in R$ implies $(y, x) \in R$;
- (3) transitive property: $(x, y), (y, z) \in R$ imply $(x, z) \in R$.

- Write $x \sim y$ instead of $(x, y) \in R \subset X \times X$.

Equivalence

Examples:

- Let A and B be $n \times n$ matrix. We define $A \sim B$ if there exist an invertible matrix P, such that $PAP^{-1} = B$.

Equivalence

Examples:

- Let A and B be $n \times n$ matrix. We define $A \sim B$ if there exist an invertible matrix P, such that $PAP^{-1} = B$.
- Suppose that $f(x)$ and $g(x)$ are differentiable functions on $\mathbb{R}$. We can define $f(x) \sim g(x)$ if $f'(x) = g'(x)$.

Equivalence

Examples:

- Let A and B be $n \times n$ matrix. We define $A \sim B$ if there exist an invertible matrix P, such that $PAP^{-1} = B$.
- Suppose that $f(x)$ and $g(x)$ are differentiable functions on $\mathbb{R}$. We can define $f(x) \sim g(x)$ if $f'(x) = g'(x)$.
- For (x_1, y_1) and $(x_2, y_2) \in \mathbb{R}^2$, define $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$.

Equivalence

Exercise:

Let p, q, r and s be integers, where q and s are nonzero. Define $p/q \sim r/s$ if $ps = qr$. Then $\sim$ is an equivalence relation.

Example

The binary relation R on $\mathbb{Q}$ given by $xRy \iff x - y \in \mathbb{Q}$ is an equivalence relation.

-

Equivalence

Definition

A *partition* $\mathfrak{P}$ of a set X is a collection of sets $X_1, X_2, \cdots, X_n$, such that $X_i \cap X_j = \emptyset, i \neq j$ and $\cup_i X_i = X$.

Equivalence

Let $\sim$ be an equivalence relation on a set X, and $x \in X$, $[x] = \{y \in X | y \sim x\}$ is called the *equivalence class* of x.

Theorem

Let $\sim$ be an equivalence relation on a set X. Then the equivalence classes of X from a partition of a set X. Conversely, if $\mathfrak{P} = \{X_i\}$ is a partition of a set X. Then there is a equivalence relation on X with equivalence classes X_i.

Equivalence

- Proof: Suppose that there exists an equivalence relation $\sim$ on a set X. For $x \in X$, we have $x \sim x$, i.e. $x \in [x]$, so $[x]$ is nonempty. It is clear that $\bigcup_{x \in X} [x] = X$.

Equivalence

- Proof: Suppose that there exists an equivalence relation $\sim$ on a set X. For $x \in X$, we have $x \sim x$, i.e. $x \in [x]$, so $[x]$ is nonempty. It is clear that $\bigcup_{x \in X} [x] = X$.
- Next, we will show that $X_i \cap X_j = \emptyset$ or $X_i = X_j$.

Equivalence

- Proof: Suppose that there exists an equivalence relation $\sim$ on a set X. For $x \in X$, we have $x \sim x$, i.e. $x \in [x]$, so $[x]$ is nonempty. It is clear that $\bigcup_{x \in X} [x] = X$.
- Next, we will show that $X_i \cap X_j = \emptyset$ or $X_i = X_j$.
- Assume that $z \in X_i \cap X_j$, write $X_i = [x], X_j = [y]$, let $z \in [x] \cap [y]$ i.e $z \sim x$ and $z \sim y$. So $x \sim y$, $[x] \subseteq [y], [y] \subseteq [x]$. Hence $[y] = [x]$,

Equivalence

- Proof: Suppose that there exists an equivalence relation $\sim$ on a set X. For $x \in X$, we have $x \sim x$, i.e. $x \in [x]$, so $[x]$ is nonempty. It is clear that $\bigcup_{x \in X} [x] = X$.
- Next, we will show that $X_i \cap X_j = \emptyset$ or $X_i = X_j$.
- Assume that $z \in X_i \cap X_j$, write $X_i = [x], X_j = [y]$, let $z \in [x] \cap [y]$ i.e $z \sim x$ and $z \sim y$. So $x \sim y$, $[x] \subseteq [y], [y] \subseteq [x]$. Hence $[y] = [x]$,
- Conversely, if $\mathfrak{P}$ is a partition of X, $X = \bigcup_i X_i$, define $x \sim y$ if $x \in X_i, y \in X_i$. We have $x \sim x$, then $\sim$ is reflexive. If $x \sim y$, that means $x \in X_i$ and $y \in X_i$, then $y \sim x$, $\sim$ is symmetric. If $x \sim y, y \sim z$, then $x \sim z$. In a word, $\sim$ is a equivalence relation.

Equivalence

- Let r and s be two integers and suppose that $n \in \mathbb{N}$. We say that r is *congruent* to s module n if $r - s$ is divisible by n, i.e. $r - s = nk$ for some $k \in \mathbb{Z}$. We write $r \equiv s (\mathrm{mod} n)$.

Equivalence

- Let r and s be two integers and suppose that $n \in \mathbb{N}$. We say that r is *congruent* to s module n if $r - s$ is divisible by n, i.e. $r - s = nk$ for some $k \in \mathbb{Z}$. We write $r \equiv s(\mathrm{mod} n)$.
- Let $n = 3$, $11 - 5 = 3 \cdot 2$. Let $n = 5$. $7 - 17 = 5 \cdot 2$.

Equivalence

- Let r and s be two integers and suppose that $n \in \mathbb{N}$. We say that r is *congruent* to s module n if $r - s$ is divisible by n, i.e. $r - s = nk$ for some $k \in \mathbb{Z}$. We write $r \equiv s (\mathrm{mod} n)$.
- Let $n = 3$, $11 - 5 = 3 \cdot 2$. Let $n = 5$. $7 - 17 = 5 \cdot 2$.

Proposition

Congruence modulo n forms an equivalence relation of $\mathbb{Z}$.

-

Equivalence

- Let r and s be two integers and suppose that $n \in \mathbb{N}$. We say that r is *congruent* to s module n if $r - s$ is divisible by n, i.e. $r - s = nk$ for some $k \in \mathbb{Z}$. We write $r \equiv s(\mathrm{mod} n)$.
- Let $n = 3$, $11 - 5 = 3 \cdot 2$. Let $n = 5$. $7 - 17 = 5 \cdot 2$.

Proposition

Congruence modulo n forms an equivalence relation of $\mathbb{Z}$.

-
- Proof: Define $r \sim s$ is congruent to s mod n. We have $r - r = 0 \times n$, $\sim$ is reflexive. If $r \sim s$, i.e. $r - s = nk$ for some $k \in \mathbb{Z}$. Then $s - r = n(-k)$, that means $s \sim r$. If $r \sim s, s \sim t$, then $r - s = nk, s - t = nl$ for some $k, l \in \mathbb{Z}$, then $r - t = n(k + l)$. Transitive property is true.

Equivalence

Definition

A *factor set* of X about an equivalence relation R is a set which elements are equivalence classes.

- Let $X = \{1, 2, 3, 4\}$. Define an equivalence relation R by $(x, y) \sim (u, v)$ if $x + y = u + v$.

Equivalence

Definition

A *factor set* of X about an equivalence relation R is a set which elements are equivalence classes.

- Let $X = \{1, 2, 3, 4\}$. Define an equivalence relation R by $(x, y) \sim (u, v)$ if $x + y = u + v$.
- There are seven equivalence class on $X \times X$.

Equivalence

Definition

A *factor set* of X about an equivalence relation R is a set which elements are equivalence classes.

- Let $X = \{1, 2, 3, 4\}$. Define an equivalence relation R by $(x, y) \sim (u, v)$ if $x + y = u + v$.
- There are seven equivalence class on $X \times X$.
- $[(1, 1)]$; $[(1, 2)]$; $[(1, 3)]$; $[(1, 4)]$; $[(3, 3)]$; $[(3, 4)]$; $[(4, 4)]$.

Equivalence

Definition

A *factor set* of X about an equivalence relation R is a set which elements are equivalence classes.

- Let $X = \{1, 2, 3, 4\}$. Define an equivalence relation R by $(x, y) \sim (u, v)$ if $x + y = u + v$.
- There are seven equivalence class on $X \times X$.
- $[(1, 1)]$; $[(1, 2)]$; $[(1, 3)]$; $[(1, 4)]$; $[(3, 3)]$; $[(3, 4)]$; $[(4, 4)]$.
- The factor set

$$\begin{aligned} & X \times X / R \\ = \; & \{[(1,1)], [(1,2)], [(1,3)], [(1,4)], [(3,3)], [(3,4)], [(4,4)]\}. \end{aligned}$$

Equivalence

- Let $\mathbb{Z}$ be the set of integers. We have a factor set $\mathbb{Z}_n$ given by integers module n.

Equivalence

- Let $\mathbb{Z}$ be the set of integers. We have a factor set $\mathbb{Z}_n$ given by integers module n.
- Define

$$a \pmod{n} + b \pmod{n} = a + b \pmod{n}, \tag{1}$$

$$(a \pmod{n})(b \pmod{n}) = ab \pmod{n}. \tag{2}$$

Equivalence

- Let $\mathbb{Z}$ be the set of integers. We have a factor set $\mathbb{Z}_n$ given by integers module n.
- Define

$$a \pmod{n} + b \pmod{n} = a + b \pmod{n}, \tag{1}$$
$$(a \pmod{n})(b \pmod{n}) = ab \pmod{n}. \tag{2}$$

- $\mathbb{Z}_3$

Equivalence

Proposition

Let $\mathbb{Z}_n$ be the set of equivalence classes of the integer module n, and $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$. Then

$$
\begin{aligned}
&\overline{a} + \overline{b} = \overline{b} + \overline{a},\\
&\overline{a}\overline{b} = \overline{b}\overline{a},\\
&(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}),\\
&(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c}),\\
&\overline{a} + \overline{0} = \overline{a},\\
&\overline{a}\overline{1} = \overline{a},\\
&\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{ac},\\
&\overline{a} + (\overline{-a}) = \overline{0}.
\end{aligned}
$$

1.5 Arithmetic

Arithmetic

Definition

A *partial ordering relation* on a set X is a relation that is reflexive ($x \leq x$ for all $s \in S$), antisymmetric ($x \leq y$ and $y \leq x$ implies $x = y$), and transitive ($x \leq y$ and $y \leq z$ implies $x \leq z$). A ordered pair (X, R) is called a *partial ordered set* if X is a set and R is a partial order relation on X.

Example

The binary relation $\leq$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are partial ordering relation. It is not an equivalent relation since $x \leq y$, but $y \not\leq x$.

-

Arithmetic

Example

The binary relation R on $\mathbb{Z}$ given by xRy if and only if $|x| \leq |y|, x, y \in \mathbb{Z}$ is reflexive, transitive, it is neither symmetric nor antisymmetric. Since if $|x| \leq |y|$ and $|y| \leq |x|$, then $|x| = |y|$. We can not have $x = y$.

-

Arithmetic

Definition

Let (X, R) be a partial ordering set. If for all $x, y \in X$, either xRy or yRx, that is whenever any two elements are comparable. In this case, (X, R) is called a *totally ordering set*

Example

The binary relation $\leq$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are totally ordering relation.

Arithmetic

- Let X be a nonempty set. Let R be a binary relation on $P(X)$ given by ARB if and only if $A \subseteq B$.

Arithmetic

- Let X be a nonempty set. Let R be a binary relation on $P(X)$ given by ARB if and only if $A \subseteq B$.
- Then relation R is reflexive, transitive, antisymmetric.

Arithmetic

- Let X be a nonempty set. Let R be a binary relation on $P(X)$ given by ARB if and only if $A \subseteq B$.
- Then relation R is reflexive, transitive, antisymmetric.
- R is partial ordering relation on $P(X)$. Denoted by $(P(X), \leq)$.

Arithmetic

- Let X be a nonempty set. Let R be a binary relation on $P(X)$ given by ARB if and only if $A \subseteq B$.
- Then relation R is reflexive, transitive, antisymmetric.
- R is partial ordering relation on $P(X)$. Denoted by $(P(X), \leq)$.
- It is a total ordering if and only if $X = \{a\}$.

Arithmetic

- Let X be a nonempty set. Let R be a binary relation on $P(X)$ given by ARB if and only if $A \subseteq B$.
- Then relation R is reflexive, transitive, antisymmetric.
- R is partial ordering relation on $P(X)$. Denoted by $(P(X), \leq)$.
- It is a total ordering if and only if $X = \{a\}$.
- If $X = \{a, b\}$, then $P(X) = \{\emptyset, \{a\}, \{b\}, X\}$. Then there is no relation $\{a\}$ and $\{b\}$. X is not a totally ordering set.

Arithmetic

Definition

A nonempty subset S of $\mathbb{Z}$ is *well-ordered* if S contains a least element.

- $\mathbb{N}$, $\mathbb{Z}^+$ are well-ordered sets. But $\mathbb{Z}$ is not a well-ordered set since $\mathbb{Z}$ has not a least element.

Arithmetic

Definition

A nonempty subset S of $\mathbb{Z}$ is *well-ordered* if S contains a least element.

- $\mathbb{N}$, $\mathbb{Z}^+$ are well-ordered sets. But $\mathbb{Z}$ is not a well-ordered set since $\mathbb{Z}$ has not a least element.

Theorem (Principle of well-ordering)

Every nonempty subset of the natural numbers $\mathbb{N}$ is well-ordered.

-

Lemma

Zorn's Lemma: If S is a nonempty partially ordered set such that every chain of S has an upper bound in S, then S has a maximal element.

-

Arithmetic

Theorem (Division Algorithm)

Let a and b be integers, with $b > 0$. Then there exists an unique integer q and r such that $a = bq + r$, where $0 \leqslant r < b$.

Arithmetic

- Proof: Let $S = \{a - bk \mid k \in \mathbb{Z} \text{ and } \; a - bk \geqslant 0\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$.

Arithmetic

- Proof: Let $S = \{a - bk \mid k \in \mathbb{Z} \text{ and } \ a - bk \geqslant 0\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$.
- If $0 \in S$, $\exists k' \in \mathbb{Z}$, such that $0 = a - bk'$, i.e. $a = bk'$. Let $q = \dfrac{a}{b}$ and $r = 0$, then $a = b \cdot \dfrac{a}{b} + 0$.

Arithmetic

- Proof: Let $S = \{a - bk \mid k \in \mathbb{Z} \text{ and } \ a - bk \geqslant 0\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$.
- If $0 \in S$, $\exists k' \in \mathbb{Z}$, such that $0 = a - bk'$, i.e. $a = bk'$. Let $q = \dfrac{a}{b}$ and $r = 0$, then $a = b \cdot \dfrac{a}{b} + 0$.
- If $0 \notin S$, we will show that S is nonempty. If $a > 0$, then $a - b \cdot 0 \in S$. If $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$.

Arithmetic

- Proof: Let $S = \{a - bk \mid k \in \mathbb{Z} \text{ and } \ a - bk \geqslant 0\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$.
- If $0 \in S$, $\exists k' \in \mathbb{Z}$, such that $0 = a - bk'$, i.e. $a = bk'$. Let $q = \dfrac{a}{b}$ and $r = 0$, then $a = b \cdot \dfrac{a}{b} + 0$.
- If $0 \notin S$, we will show that S is nonempty. If $a > 0$, then $a - b \cdot 0 \in S$. If $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$.
- In either case, S is nonempty. S is a nonempty subset of $\mathbb{N}$, there exists a smallest number in S. Let $r = a - bq \in S$ be the smallest number in S. Therefore, $a = bq + r, r \geqslant 0$. We now show that $r < b$. Suppose that $r > b$. Then $a - b(q + 1) = a - bq - b = r - b > 0$. We have $a - b(q + 1) \in S$. But $a - b(q + 1) < a - bq$, which contradict the fact that $r = a - bq$ is the smallest number in S. So $r \leq b$. Since $0 \notin S, r \neq b$ and so $r < b$.

Arithmetic

- Uniqueness of q and r. Suppose that there exist integers r, r', q, q', such that

$$a = bq + r, \quad 0 \leqslant r < b.$$
$$a = bq' + r', \quad 0 \leqslant r' < b.$$

Arithmetic

- Uniqueness of q and r. Suppose that there exist integers r, r', q, q', such that

$$a = bq + r, \quad 0 \leqslant r < b.$$
$$a = bq' + r', \quad 0 \leqslant r' < b.$$

- Assume that $r' > r$. From the last equation we have

$$bq - bq' = b(q - q') = r' - r.$$

Arithmetic

- Uniqueness of q and r. Suppose that there exist integers r, r', q, q', such that

$$a = bq + r, \quad 0 \leqslant r < b.$$
$$a = bq' + r', \quad 0 \leqslant r' < b.$$

- Assume that $r' > r$. From the last equation we have

$$bq - bq' = b(q - q') = r' - r.$$

- Therefore $b \mid r' - r$ and $0 \leqslant r' - r < r' < b$. This is possible only if $r' - r = 0$. Hence $r = r'$ and $q = q'$.

Arithmetic

Definition

The *greatest common divisor* of integers a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and d, then $d'|d$. We write $d = gcd(a, b)$.

Theorem

Let a and b be nonzero integers. Then there exist integers r and s such that $gcd(a, b) = ar + bs$. Furthermore, the greatest common divisor of a and b is unique.

-

Arithmetic

- Proof: Let $S = \{am + bn | m, n \in \mathbb{Z}, am + bn > 0\}$. Clearly, S is nonempty, hence, S must have a smallest member $d = ar + bs$ by well-ordering principle. We claim that $d = gcd(a, b)$. Write
$$a = dq + r', 0 \leq r' < d.$$

Arithmetic

- Proof: Let $S = \{am + bn | m, n \in \mathbb{Z}, am + bn > 0\}$. Clearly, S is nonempty, hence, S must have a smallest member $d = ar + bs$ by well-ordering principle. We claim that $d = gcd(a, b)$. Write
$$a = dq + r', 0 \leq r' < d.$$
- If $r' > 0$, then $r' = a - dq = a - (ar + bs)q = a - arq - bsq = a(1 - rq) + b(-sq) \in S$. It is contradict the fact that d is the smallest member of S. Hence, $r' = 0$ and d divides a. A similar argument shows that d divides b. Therefore, d is a common divisor of a and b.

Arithmetic

- Proof: Let $S = \{am + bn | m, n \in \mathbb{Z}, am + bn > 0\}$. Clearly, S is nonempty, hence, S must have a smallest member $d = ar + bs$ by well-ordering principle. We claim that $d = gcd(a, b)$. Write
$$a = dq + r', 0 \leq r' < d.$$
- If $r' > 0$, then $r' = a - dq = a - (ar + bs)q = a - arq - bsq = a(1 - rq) + b(-sq) \in S$. It is contradict the fact that d is the smallest member of S. Hence, $r' = 0$ and d divides a. A similar argument shows that d divides b. Therefore, d is a common divisor of a and b.
- Suppose that d' is another common divisor of a and b, and we want to show that $d'|d$. If we let $a = d'h$ and $b = d'k$, then $d = ar + bs = d'hr + d'ks = d'(hr + ks)$. So d' must divide d. Hence, d must be the unique greatest common divisor of a and b.

Arithmetic

Definition

p is a prime number if the positive numbers that divide p are 1 and p itself. An integer $n > 1$ that is not prime is said to be composite.

Arithmetic

Lemma

Let a and b be integers and p be a prime number. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.

- Proof: Suppose that $p \nmid a$, then we will show that p must divide b.
  Since $\gcd(a, p) = 1$, there exists integers r and s such that $ar + ps = 1$.
  Then $b = b(ar + ps) = (ab)r + p(bs)$. Since $p \mid ab$ and $p|ps$, p must divide b.

Equivalence

Theorem

There exist infinite numbers of primes.

- Proof: Suppose that there are only finite number of primes, say $p_1, \cdots, p_n$. Let $p = p_1 \cdots p_n + 1$. Next we will show that p is a prime number, or p has other prime divisor. If p is a prime, it is contradict to there are n primes. If p is not a prime, then p can be divided by some prime q.

Equivalence

Theorem

There exist infinite numbers of primes.

- Proof: Suppose that there are only finite number of primes, say $p_1, \cdots, p_n$. Let $p = p_1 \cdots p_n + 1$. Next we will show that p is a prime number, or p has other prime divisor. If p is a prime, it is contradict to there are n primes. If p is not a prime, then p can be divided by some prime q.
- If $q = p_i$ for some $1 \leq i \leq n$. In this case, p_i must divide $p_1 \cdots p_n + 1$. $p_i \mid p_1 \cdots p_n$. Thus $p_i \mid 1$. This is a contradiction to p_i a prime number. If $q \neq p_j$ for all $1 \leq j \leq n$, then q is a prime different from $p_1, \cdots, p_n$. It is contradiction to there are finite primes.

Equivalence

Theorem

Fundamental theorem of Arithmetic: Let n be an integer, such that $n > 1$. Then $n = p_1 p_2 \cdots p_k$, where $p_1, p_2, \cdot, p_k$ are primes(not necessary distinct). Furthermore, this factorization is unique, that is if $n = q_1 q_2 \cdots q_l$, then $k = l$, and the q_i's are just the p_i's rearranged.

-

Equivalence

- Proof: Uniqueness we will use induction on n. It is true for $n = 2$. Assume that the result holds for all integers m, $1 \leq m < n$ and $n = p_1 p_2 \cdots\ p_k = q_1 q_2 \cdots q_l$, where $p_1 \leq p_2 \leq \cdots \leq p_k$, and $q_1 \leq q_2 \leq \cdots \leq q_k$.

Equivalence

- Proof: Uniqueness we will use induction on n. It is true for $n = 2$. Assume that the result holds for all integers m, $1 \leq m < n$ and $n = p_1 p_2 \cdots \ p_k = q_1 q_2 \cdots q_l$, where $p_1 \leq p_2 \leq \cdots \leq p_k$, and $q_1 \leq q_2 \leq \cdots \leq q_k$.
- By lemma of prime, $p_1 | q_i$ for some i and $q_1 | p_j$ for some j. Because $q_i' s$ and $P_j' s$ are primes. So $p_1 = q_i$, $q_1 = p_j$. Hence, $p_1 = q_1$, since $p_1 \leq p_j = q_1 \leq q_i = p_1$.

Equivalence

- Proof: Uniqueness we will use induction on n. It is true for $n = 2$. Assume that the result holds for all integers m, $1 \leq m < n$ and $n = p_1 p_2 \cdots\ p_k = q_1 q_2 \cdots q_l$, where $p_1 \leq p_2 \leq \cdots \leq p_k$, and $q_1 \leq q_2 \leq \cdots \leq q_k$.
- By lemma of prime, $p_1 | q_i$ for some i and $q_1 | p_j$ for some j. Because $q_i' s$ and $P_j' s$ are primes. So $p_1 = q_i$, $q_1 = p_j$. Hence, $p_1 = q_1$, since $p_1 \leq p_j = q_1 \leq q_i = p_1$.
- By the induction hypothesis, $n' = p_2 \cdots\ p_k = q_2 \cdots\ q_l < n$ and n' has a unique factorization. Hence $k = l$ and $q_i = p_i$ for $i = 1, \cdots, k$.

Equivalence

- Existence: Suppose that there is some integers that cannot be written as the product of primes. Let S be the set of all such numbers. $S \subseteq \mathbb{N}$, S has a smallest number, say a.

Equivalence

- Existence: Suppose that there is some integers that cannot be written as the product of primes. Let S be the set of all such numbers. $S \subseteq \mathbb{N}$, S has a smallest number, say a.
- If the only positive factors of a are a and 1, then a is prime, which is a contradiction. Hence $a = a_1 a_2$, where $1 < a_1 < a$ and $1 < a_2 < a$.

Equivalence

- Existence: Suppose that there is some integers that cannot be written as the product of primes. Let S be the set of all such numbers. $S \subseteq \mathbb{N}$, S has a smallest number, say a.
- If the only positive factors of a are a and 1, then a is prime, which is a contradiction. Hence $a = a_1 a_2$, where $1 < a_1 < a$ and $1 < a_2 < a$.
- Neither $a_1 \in S$ nor $a_2 \in S$, since a is the smallest number of S. So $a_1 = p_1 \cdots p_s$ and $a_2 = q_1 \cdots q_l$.
- Therefore $a = p_1 \cdots p_s q_1 \cdots q_l$. So $a \notin S$. It's contradiction to the definition of S.

1.5 The Chinese Remainder Theorem

The Chinese Remainder Theorem

Proposition

Let a, b, n be integers with $n > 0$, $gcd(a, n)$ be the greatest common divisor of a and n. Then there is a solution x of the congruence equation $ax \equiv b(\mod n)$ if and only if $gcd(a, n)|b$.

-

The Chinese Remainder Theorem

Proposition

Let a, b, n be integers with $n > 0$, $gcd(a, n)$ be the greatest common divisor of a and n. Then there is a solution x of the congruence equation $ax \equiv b(\mod n)$ if and only if $gcd(a, n)|b$.

-
- Proof: Let $d = gcd(a, n)$. If x is a solution of $ax \equiv b(\mod n)$, then $ax = b + nq$ for some $q \in \mathbb{Z}$; it follows that d must divide b.

The Chinese Remainder Theorem

Proposition

Let a, b, n be integers with $n > 0$, $gcd(a, n)$ be the greatest common divisor of a and n. Then there is a solution x of the congruence equation $ax \equiv b(\mod n)$ if and only if $gcd(a, n)|b$.

-
- Proof: Let $d = gcd(a, n)$. If x is a solution of $ax \equiv b(\mod n)$, then $ax = b + nq$ for some $q \in \mathbb{Z}$; it follows that d must divide b.
- Conversely, assume that $d|b$. There are integers u, v such that $d = au + nv$. Multiplying integer $\frac{b}{d}$, we obtain $b = a(\frac{ub}{d}) + n(\frac{vb}{d})$. Put $x = \frac{ub}{d}$; then $ax \equiv b(\mod n)$ and x is a solution of the congruence.

The Chinese Remainder Theorem

Corollary

Let a, n be integers with $n > 0$. Then the congruence equation $ax \equiv 1 (\mod n)$ has a solution x if and only if a is relatively prime to n.

-

The Chinese Remainder Theorem

Theorem

The Chinese Remainder Theorem: *Let* $a_1, a_2, \cdots, a_k$ *and* $m_1, m_2, \cdots, m_k$ *be integers with* $m_i > 0$*; assume that* $gcd(m_i, m_j) = 1$ *if* $i \neq j$*. Then there is a common solution* x *of the system of congruences*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

-

The Chinese Remainder Theorem

- Proof: Put $m = m_1 m_2 \cdots m_k$ and $\widehat{m_i} = \frac{m}{m_i}$. Then m_i and $\widehat{m_i}$ are relatively prime, so there exist an integer l_i such that $\widehat{m_i} l_i \equiv 1 (\mod m_i)$. Now put $x = a_1 \widehat{m_1} l_1 + \cdots + a_k \widehat{m_k} l_k$. Then

$$\begin{aligned}
x &= a_i \widehat{m_i} l_i + \sum_{j \neq i} a_j \widehat{m_j} l_j \\
&\equiv a_i (\mod m_i) + \sum_{j \neq i} 0 \\
&= a_i (\mod m_i).
\end{aligned}$$

The Chinese Remainder Theorem

- Example: Let us determine what day of the week January 1 in the year 2030 will be.

The Chinese Remainder Theorem

- Example: Let us determine what day of the week January 1 in the year 2030 will be.
- Labeling a week as

$$
\begin{aligned}
&Sunday = \bar{0},\ \text{Monday} = \bar{1},\ Tuesday = \bar{2},\\
&Wednesday = \bar{3},\ Thursday = \bar{4},\ Friday = \bar{5},\\
&Saturday = \bar{6}.
\end{aligned}
$$

The Chinese Remainder Theorem

- Example: Let us determine what day of the week January 1 in the year 2030 will be.
- Labeling a week as

$$\begin{aligned} &Sunday = \bar{0},\ \text{Monday} = \bar{1},\ Tuesday = \bar{2},\\ &Wednesday = \bar{3},\ Thursday = \bar{4},\ Friday = \bar{5},\\ &Saturday = \bar{6}. \end{aligned}$$

- Suppose that today is January 1, 2023, Sunday. There are 2557 days from January 1, 2030. Now $2557 \equiv 2(\mod 7)$. We conclude that January 1, 2030 will be Tuesday.

The Chinese Remainder Theorem

- It is well know that an integer is divisible by 3 if and only if the sum of its digits is a multiple of 3.
  Let $m = m_k m_{k-1} \cdots m_1 m_0$ be the decimal representation of an integer m, where $0 \leq m_i \leq 9$. Then $m = m_k 10^k + m_{k-1} 10^{k-1} + \cdots m_1 10 + m_0$. Note that $10 \equiv 1 (\mod 3)$, i.e. $\bar{10} = \bar{1}$. Then $\bar{10}^i = \bar{1}^i = \bar{1}$ for $i \geq 0$. It follows that $m \equiv m_k + m_{k-1} + \cdots + m_1 + m_0 (\mod 3)$.

The Chinese Remainder Theorem

- There is an ancient problem in an Indian manuscript of the 7th Century. There are some eggs in a basket. When eggs are removed $k = 2, 3, 4, 5, 6$ times, there is 1 eggs left, and when $k = 7$, there is no eggs left. What is the smallest number of eggs in the basket.
  Let x be the number of eggs in the basket. The conditions require that $x \equiv 1(\mod k)$ for $k = 2, 3, 4, 5, 6$ and $x \equiv 0(\mod k)$ for $k = 7$. Clearly this amounts to x satisfying the four congruences

$$\begin{aligned} x &\equiv 1(\mod 3), \\ x &\equiv 1(\mod 4), \\ x &\equiv 1(\mod 5), \\ x &\equiv 0(\mod 7). \end{aligned}$$

The Chinese Remainder Theorem

- Furthermore, the equations are equivalent to

$$x \equiv 1 \pmod{60},$$
$$x \equiv 0 \pmod{7}.$$

By the Chinese Remainder Theorem, there is a solution to the congruences equations. Applying Theorem 49, we have $m = 420, m_1 = 60, m_2 = 7$, so that $\widehat{m_1} = 7, \widehat{m_2} = 60$; also $l_1 = 43, l_2 = 2$.

The Chinese Remainder Theorem

- Furthermore, the equations are equivalent to

$$x \equiv 1 \pmod{60},$$
$$x \equiv 0 \pmod{7}.$$

  By the Chinese Remainder Theorem, there is a solution to the congruences equations. Applying Theorem 49, we have $m = 420, m_1 = 60, m_2 = 7$, so that $\widehat{m_1} = 7, \widehat{m_2} = 60$; also $l_1 = 43, l_2 = 2$.

- Therefore one solution is given by $x = 1 \cdot 7 \cdot 43 + 0 \cdot 60 \cdot 2 = 301$. If y is any other solution, note that $y - x$ must be divisible by $60 \times 7 = 420$. Thus the general solution is $x = 301 + 420q, q \in \mathbb{Z}$. So the smallest positive solution is 301.