MA1100 Tutorial

Xiang Sun[1][2]

Department of Mathematics

November 12, 2010

[1] Email: xiangsun@nus.edu.sg

[2] Corrections are always welcome.

Self-Introduction

Name Sun Xiang (English) and 孙祥 (Chinese)
Third-year Ph.D. student in Department of Mathematics

Email xiangsun@nus.edu.sg

Mobile 9169 7677

Office S17-06-14, map

Social xiangsun_sunny (twitter),
xiangsun.sunny@hotmail.com (Windows Live Messenger),
xiangsun.sunny@gmail.com (Google Talk, Buzz, Google Reader),
http://www.facebook.com/xiangsun.sunny (facebook),
402197754 (QQ)

Introduction

- 10 tutorials: 4 before mid-term test, and 6 after it.
- Take attendance:
  - 2 points for full attendance, and pro-rated for partial attendance;
  - Everyone need to print his/her signature, rather than a tick;
  - If you find some mistakes on the attendance sheet, please let me know.
- Presentation: call for volunteers.
- My tutorial style:
  - 5–10 mins for reviewing concepts;
  - 25–35 mins for tutorial questions;
  - 0–10 mins for additional material.
- Additional material: discuss questions in the past-year papers, some anecdotes and histories.
- Download: Tutorial slides and other material will be uploaded to my SkyDrive.

Schedule of Tutorial 1

- Review concepts:
  - Sets:
    - Set, sets relations, sets operations;
    - Partition of set;
    - Cartesian product of sets.
  - Logic:
    - Statement, open sentence;
    - Logic operators and their truth tables;
    - Necessary and sufficient condition.
- Tutorial
- Additional material:
  - Question 3 in Mid-term 2009–2010(I);
  - Resolve Russell's paradox.

Sets

Notations $\{x \in U \mid p(x)\}$, x is a general element, $p(x)$ is the condition in terms of x, U is the universal set.

Empty set the set containing no elements, $\emptyset$ or $\{\ \}$.

Relations

- Subsets: $A \subseteq B$ if every element of A is an element of B;
- Equality: $A = B$ if $A \subseteq B$ and $B \subseteq A$;
- Proper subsets: $A \subsetneq B$ if $A \subseteq B$ and $A \neq B$.

Operations

- Power set: the power set of A is the set of all subsets of A, $\mathcal{P}(A) = \{S \subseteq U \mid S \subseteq A\}$ (another notation: 2^A);
- Intersection: the intersection of A and B is the set of all elements that are in both A and B, $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$;
- Union: the union of A and B is the set of all elements that are in A or in B, $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$;
- Complement: the complement of A is the set of all elements of U that are not in A, $\bar{A} \equiv A^c = \{x \in U \mid x \notin A\}$;
- Relative complement: the relative complement of B w.r.t. A is the set of all elements that are in A but not in B, $A - B = \{x \in U \mid x \in A, x \notin B\}$.

Sets (Cont.)

Cardinality For a finite set S, we use $|S|$ to denote the number of elements in S, which is called cardinal number or cardinality[3].

Indexed Collection of Sets $A_1, A_2, A_3, \ldots$ are an indexed collection of sets, N (not $\mathbb{N}$) is index set

- Intersection: $\bigcap_{n\in N} A_n = A_1 \cap A_2 \cap A_3 \cap \cdots$;
- Union: $\bigcup_{n\in N} A_n = A_1 \cup A_2 \cup A_3 \cup \cdots$.

Partitions of Sets A is a non-empty set, and S is a collection of subsets of A. S is a partition of A if

- For each $X \in S$, $X \neq \emptyset$, i.e. each part has at least one element;
- For every $X, Y \in S$, if $X \neq Y$, then $X \cap Y = \emptyset$;
- The union of all elements in the collection S is equal to A.

Cartesian Products of Sets The Cartesian product[4] of A and B:
$A \times B = \{(a, b) \mid a \in A, b \in B\}$, where (a, b) is an ordered pair.

[3] We will redefine "cardinality" in chapter 10, Chartrand's book.

[4] The Cartesian product is named after René Descartes whose adjectival form is "Cartesian".

Logic

Statements A statement is a sentence that is either true or false (but not both); We denote a statement by capital letters, usually $P, Q, R, \ldots$;

Open Sentences An open sentence is a (mathematical) sentence that involves variables; We denote an open sentence by capital letters with the variables involved, such as $P(n)$, $Q(x, y)$;

Logic operators Let P and Q be two statements,

Conjunction $P \wedge Q$, it is true only when both P and Q are true;
Disjunction $P \vee Q$, it is false only when both P and Q are false;
Negating $\sim P$, if P is true, then $\sim P$ is false, and vice versa;
Implication $P \Rightarrow Q$, the rule is false only when the rule is violated.

Truth tables

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

Some forms of Implication The following sentences are equivalent:

- $S \Rightarrow T$;
- If S then T;
- T if S;
- S only if T;
- S implies T;
- T whenever S;
- S is sufficient for T;
- T is necessary for S.

Exercise (1-1)

The set of even numbers can be described by means of set builder notation $\{x \in \mathbb{Z} \mid x = 2n \text{ where } n \in \mathbb{Z}\}$ *and alternative set notation* $\{2n \mid n \in \mathbb{Z}\}$. *Describe the following sets in a similar manner.*

(a) $A = \{\ldots, -18, -13, -8, -3, 2, 7, 12, 17, \ldots\}$;

(b) $B = \{2, 5, 10, 17, 26, \ldots\}$;

(c) $C = \{1, 3, 6, 10, 15, 21, 28, \ldots\}$.

Method

Find the general form of the elements by "Observing" and "Experience".

Solution of (a).

The sequence "$\ldots, -18, -13, -8, -3, 2, 7, 12, 17, \ldots$" is an arithmetic sequence and the common difference of successive members is 5, then

$$\begin{aligned} A &= \{x \in \mathbb{Z} \mid x = 5n - 3 \text{ where } n \in \mathbb{Z}\} = \{5n - 3 \mid n \in \mathbb{Z}\} \\ &= \{x \in \mathbb{Z} \mid x = 5n + 2 \text{ where } n \in \mathbb{Z}\} = \{5n + 2 \mid n \in \mathbb{Z}\}. \end{aligned}$$

Solution of (b,c).

(b) In the sequence "$2, 5, 10, 17, 26, \ldots$", the difference of the $(n+1)$-th term and the n-th term is $2n+1$, hence the n-th term is

$$2 + \underbrace{3 + 5 + 7 + \cdots + (2n-1)}_{(n-1) \text{ terms}} = 2 + \frac{3 + (2n-1)}{2}(n-1) = n^2 + 1.$$

Therefore, $B = \{x \in \mathbb{Z} \mid x = n^2 + 1 \text{ where } n \in \mathbb{N}\} = \{n^2 + 1 \mid n \in \mathbb{N}\}$;

(c) In the sequence "$1, 3, 6, 10, 15, 21, 28, \ldots$", the difference of the $(n+1)$-th term and the n-th term is n, hence the n-th term is

$$\underbrace{1 + 2 + 3 + 4 + \cdots + n}_{n \text{ terms}} = \frac{(1+n)n}{2}.$$

Therefore, $C = \left\{x \in \mathbb{Z} \mid x = \frac{n(n+1)}{2} \text{ where } n \in \mathbb{N}\right\} = \left\{\frac{n(n+1)}{2} \mid n \in \mathbb{N}\right\}$.

□

Exercise (1-2)

Determine the following power sets and their cardinalities:

(a) $\mathcal{P}(\mathcal{P}(\emptyset))$; (b) $\mathcal{P}(\mathcal{P}(\{1\}))$.

Recall

- Power set: the set of all subsets of A, $\mathcal{P}(A) = \{S \subseteq U \mid S \subseteq A\}$;
- Cardinality: the number of elements of set S, denoted as $|S|$;
- $|\mathcal{P}(S)| = 2^{|S|}$.

Method

Apply definition.

Solution.

(a) For $\emptyset$, there is only one subset, $\emptyset$, i.e., $\mathcal{P}(\emptyset) = \{\emptyset\}$.
For $\{\emptyset\}$, its all subsets are $\emptyset$ and $\{\emptyset\}$, i.e., $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Therefore,

$$\mathcal{P}\big(\mathcal{P}(\emptyset)\big) = \big\{\emptyset, \{\emptyset\}\big\}, \quad \big|\mathcal{P}\big(\mathcal{P}(\emptyset)\big)\big| = 2 (= 2^{2^{|\emptyset|}}).$$

(b) For $\{1\}$, its all subsets are $\emptyset$ and $\{1\}$, then $\mathcal{P}(\{1\}) = \big\{\emptyset, \{1\}\big\}$;
For $\big\{\emptyset, \{1\}\big\}$, its all subsets are $\emptyset$, $\{\emptyset\}$, $\{\{1\}\}$, and $\big\{\emptyset, \{1\}\big\}$, therefore

$$\mathcal{P}\big(\mathcal{P}(\{1\})\big) = \big\{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\big\}, \quad \big|\mathcal{P}\big(\mathcal{P}(\{1\})\big)\big| = 4 (= 2^{2^{|\{1\}|}}).$$

Exercise (1-3)

Let (a, b) be an open interval of real numbers and $c \in (a, b)$.

(i) *Write down the largest possible open interval I centered at c such that $I \subset (a, b)$. (Give your answer in terms of a, b, c.)*

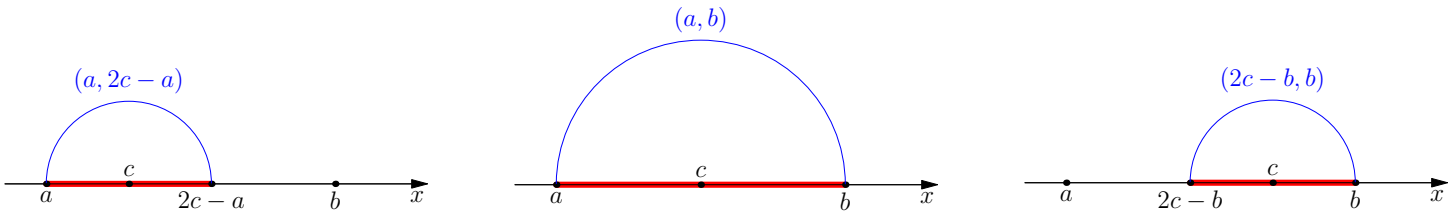
(ii) *For the interval I in (i), write down the relative complement $(a, b) - I$.*

(iii) *Is it possible to find a partition of (a, b) consisting of exactly two open intervals? Why?*

Recall

Open interval (a, b) is the set $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$.

Solution.



(i–ii) (1) If $c < \frac{b+a}{2}$, then $I = (a, 2c - a)$ and $(a, b) - I = [2c - a, b)$;
(2) If $c = \frac{b+a}{2}$, then $I = (a, b)$ and $(a, b) - I = \emptyset$;
(3) If $c > \frac{b+a}{2}$, then $I = (2c - b, b)$ and $(a, b) - I = (a, 2c - b]$.

(iii) No. Let $\{A, B\}$ be a partition of (a, b). If A is an open interval, then $B = (a, b) - A$ will be (union of) half-open interval(s).

□

Exercise (1-4)

Give an example of a partition of $\mathbb{N}$ into 3 subsets S_1, S_2, S_3 that satisfy each of the following conditions (if possible)

(a) S_1, S_2, S_3 *finite;*

(b) S_1, S_2 *finite,* S_3 *infinite;*

(c) S_1 *finite,* S_2, S_3 *infinite;*

(d) S_1, S_2, S_3 *infinite.*

Solution.

(a) Impossible: if $\mathbb{N} = S_1 \cup S_2 \cup S_3$, then $\mathbb{N}$ is a finite set which is not correct;

(b) $S_1 = \{1\}$, $S_2 = \{2\}$, $S_3 = \{3, 4, \ldots\}$;

(c) $S_1 = \{1\}$, $S_2 = \{3, 5, 7, \ldots\}$ (all odd numbers greater than 1), $S_3 = \{2, 4, 6, \ldots\}$ (all even numbers greater than 1);

(d) $S_1 = \{3n \mid n \geq 1\}$, $S_2 = \{3n + 1 \mid n \geq 0\}$, and $S_3 = \{3n + 2 \mid n \geq 0\}$.

□

Exercise (1-5)

For each $n \in \mathbb{N}$, define

$$A_n = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 \leq n\}, \quad B_n = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 \geq n\}.$$

By interpreting each of the A_n and B_n as a geometrical object in the Cartesian plane $\mathbb{R}^2$, determine

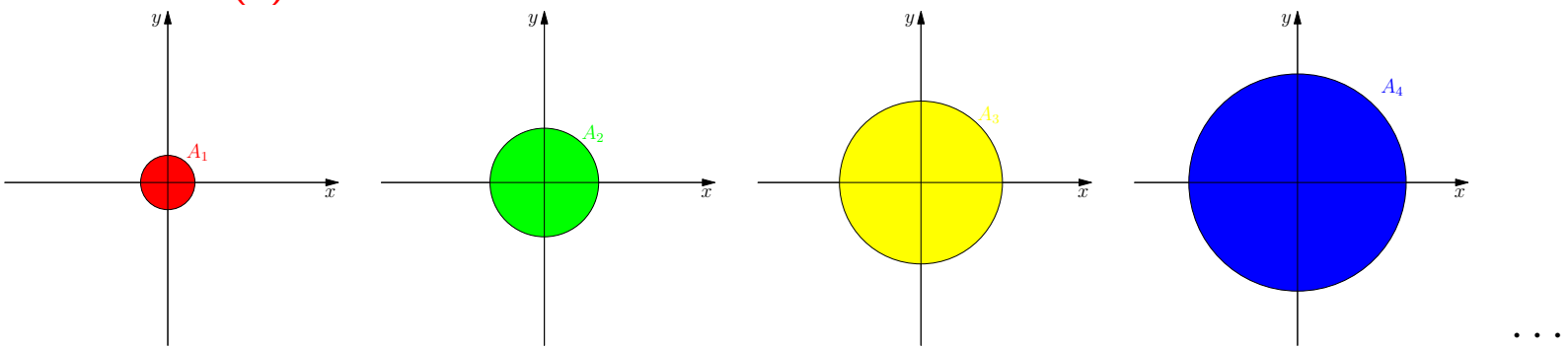
(a) $\cup_{n=1}^{k} A_n$, $\cap_{n=1}^{k} A_n$, $\cup_{n\in\mathbb{N}} A_n$ *and* $\cap_{n\in\mathbb{N}} A_n$;

(b) $\cup_{n=1}^{k} B_n$, $\cap_{n=1}^{k} B_n$, $\cup_{n\in\mathbb{N}} B_n$ *and* $\cap_{n\in\mathbb{N}} B_n$.

Recall

- $A \cap B$ is the set of all elements that are in both A and B;
- $A \cup B$ is the set of all elements that are in A or in B;
- $\bigcap_{n\in\mathbb{N}} A_n = A_1 \cap A_2 \cap A_3 \cap \cdots$;
- $\bigcup_{n\in\mathbb{N}} A_n = A_1 \cup A_2 \cup A_3 \cup \cdots$.

Solution of (a).



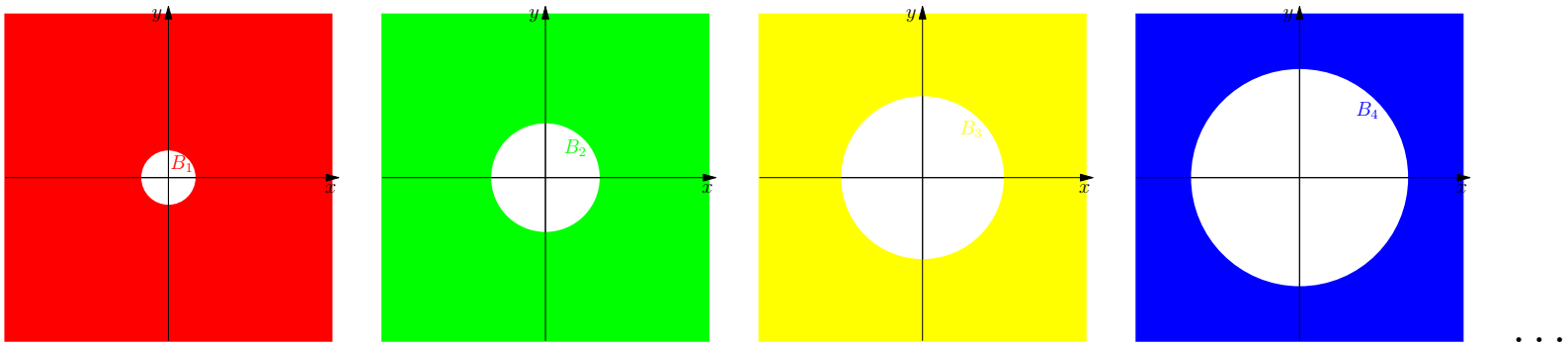
(1) It is obvious that $A_n \subset A_{n+1}$. Hence $\cup_{n=1}^{k} A_n = A_k$, $\cap_{n=1}^{k} A_n = A_1$.

(2) For any point $p \in \mathbb{R}^2$, we can find a circle containing p, say A_n, hence $\cup_{n\in\mathbb{N}} A_n = \mathbb{R}^2$.

(3) Since $A_1 \subset A_2 \subset A_3 \subset \cdots \subset A_n \subset A_{n+1} \subset \cdots$, we have $\cap_{n\in\mathbb{N}} A_n = A_1$.

□

Solution of (b).



(1) It is obvious that $B_n \supset B_{n+1}$. Hence $\cup_{n=1}^{k} B_n = B_1$, $\cap_{n=1}^{k} B_n = B_k$.

(2) Since $B_1 \supset B_2 \supset B_3 \supset \cdots \supset B_n \supset B_{n+1} \supset \cdots$, we have $\cup_{n\in\mathbb{N}} B_n = B_1$.

(3) For any point $p \in \mathbb{R}^2$, we can find a circle $x^2 + y^2 = n$ whose interior contains p, then B_n does not contain p. Hence $\cap_{n\in\mathbb{N}} B_n = \emptyset$.

□

Exercise (1-6)

For the open sentence $Q(A)$: A is a proper subset of $\{1,2,3,4\}$ over the domain $S = \mathcal{P}(\{2,3,4,5\})$, determine

(a) *all $A \in S$ for which $Q(A)$ is true.*

(b) *all $A \in S$ for which $Q(A)$ is false.*

(c) *How will the answers above change if we remove the word "proper" from the sequence $Q(A)$?*

Method

Substitute A with every possible subset of $\{2,3,4,5\}$, and see whether it is a (proper) subset of $\{1,2,3,4\}$.

Solution.

(a–b)

$$S = \left\{ \begin{array}{l} \emptyset, \{2\}, \{3\}, \{4\}, \{5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}, \\ \{4,5\}, \{2,3,4\}, \{2,3,5\}, \{2,4,5\}, \{3,4,5\}, \{2,3,4,5\} \end{array} \right\},$$

where the red elements of S are the solutions of (a), other elements are the solutions of (b);

(c) For any subset of $\{2,3,4,5\}$, it does not contain $\{1\}$. Hence, the answer will still be the same.

□

Exercise (1-7)

Let $P(x)$ stand for "x is an even integer" and let $Q(x)$ stand for "x^2 is an even integer". Express the implication $P \Rightarrow Q$ in English using

(a) *The "if then" form of the implication;*

(b) *The word "implies";*

(c) *The "only if" form of the implication;*

(d) *The phrase "is necessary for";*

(e) *The phrase "is sufficient for".*

Recall

Refer to page 40 of Chartrand's book.

Solution.

(a) If the integer x is even, then x^2 is even;

(b) The integer x is even implies that x^2 is even;

(c) The integer x is even only if x^2 is even;

(d) The integer x^2 is even is necessary for x to be even;

(e) The integer x is even is sufficient for x^2 to be even.

Exercise (1-8)

Suppose that P and Q are statements for which $P \Rightarrow Q$ is false. What conclusion (if any) can be made about the truth value of each of the following statements?

(a) $(\sim P) \Rightarrow Q$; (b) $Q \Rightarrow P$; (c) $P \vee Q$; (d) $P \wedge Q$.

Recall

Truth tables: figure 2.2, 2.3, 2.4, 2.5 of Chartrand's book.

Solution.

Using truth table, from $P \Rightarrow Q$ being false, we know that P is true and Q is false. So we have

(a) $(\sim P) \Rightarrow Q$ is true;

(b) $Q \Rightarrow P$ is true;

(c) $P \vee Q$ is true;

(d) $P \wedge Q$ is false.

□

Additional material

Exercise (Question 3 in Mid-term 2009–2010(I))

Let $A_n = \left\{ k \in \mathbb{N} \mid \frac{(n-1)n}{2} + 1 \leq k \leq \frac{n(n+1)}{2} \right\}$ *for every* $n \in \mathbb{N}$. *Answer the following questions:*

(i) *What is the cardinality* $|A_n|$*?*

(ii) *What are* $\cup_{n\in\mathbb{N}} A_n$ *and* $\cap_{n\in\mathbb{N}} A_n$*?*

(iii) *Give an example of a set* B *such that* $|B \cap A_n| = 1$ *for every* $n \in \mathbb{N}$. *Express your answer using set notation.*

(iv) *Give a partition* S *of* $\mathbb{N}$ *such that* S *is an infinite set and every element of* S *has a different cardinality from each other.*

Additional material: Russell's paradox

Exercise

Usually, for any formal criterion, a set exists whose members are those objects (and only those objects) that satisfy the criterion, i.e. $\{x \in U \mid p(x)\}$ *is a set. Whether does there exist an object with the form* $\{x \in U \mid p(x)\}$*, which is not a set?*

Solution.

This question is disproved by a set containing exactly the sets that are not members of themselves. If such a set qualifies as a member of itself, it would contradict its own definition as a set containing sets that are not members of themselves. On the other hand, if such a set is not a member of itself, it would qualify as a member of itself by the same definition. This contradiction is Russell[5]'s paradox.
Let $A = \{X \in U \mid X \notin X\}$, U is the collection of all sets.

- If $A \in A$, then A does not satisfy $X \notin X$, i.e. $A \notin A$, contradiction;
- If $A \notin A$, then A satisfies $X \notin X$, i.e. $A \in A$, contradiction.

Therefore, the definition is not well-defined, and this error is from U (implies that U is not a set). □

[5] Bertrand Arthur William Russell (May 18, 1872–February 2, 1970), a British philosopher, logician, mathematician, historian, atheist, socialist, pacifist, and social critic.

Additional material: Russell's paradox (Cont.)

Exercise

How to resolve this problem?

Solution.

- Roughly speaking, the method is giving some restrictions on the definition of set.
- Russell's paradox (also known as Russell's antinomy), discovered by Russell in 1901.
- In 1908, two ways of avoiding the paradox were proposed, Russell's type theory and Ernst Zermelo[6]'s axiomatic set theory, the first constructed axiomatic set theory.
- Zermelo's axioms evolved into the now-canonical Zermelo-Fraenkel[7] set theory (ZF).
- For more information, please wiki: Russell's paradox.

□

[6] Ernst Friedrich Ferdinand Zermelo (July 27, 1871–May 21, 1953), a German mathematician.

[7] Abraham Halevi (Adolf) Fraenkel (February 17, 1891–October 15, 1965), an Israeli mathematician.

Change log

- Page 7: Add a item "some forms of implication";
- Page 8: Revise typos: "$5n+3$" to "$5n-3$", "$5n-2$" to "$5n+2$";
- Page 11: Revise a typo: "$\frac{b-a}{2}$" to "$\frac{b+a}{2}$";
- Page 16: Give more interpretation for part (c).

Last modified: 20:39, August 26, 2010.

Schedule of Tutorial 2

- Review concepts: Logic
  - Converse, contrapositive, inverse, biconditional;
  - Logical equivalence, operations of logic operators;
  - Universal quantifier, existential quantifier, 2 quantifiers, negation with quantifier.
- Tutorial
- Additional material: Relation between 5 logic operators.

Logic: Concepts

Hypothesis, conclusion In the implication $P \Rightarrow Q$, P is called hypothesis or premise, and Q is called conclusion.

Converse The implication $Q \Rightarrow P$ is called the converse of $P \Rightarrow Q$.

Contrapositive $(\sim Q) \Rightarrow (\sim P)$ is called the contrapositive of $P \Rightarrow Q$.

Inverse The implication $(\sim P) \Rightarrow (\sim Q)$ is called the inverse of $P \Rightarrow Q$. (Exercise 2.34)

Tautology A logical expression that is always true is called a tautology.

Contradiction A logical expression that is always false is called a contradiction.

Logical Equivalence Two logical expressions are said to be logically equivalent to each other if they have the same truth value. Notation: $\equiv$.

Converse vs Contrapositive vs Inverse

$$\begin{array}{ccc} P \Rightarrow Q & \xrightarrow[\text{converse}]{\text{not logically equivalent}} & Q \Rightarrow P \\ \| & & \| \\ & \text{contrapositive, logically equivalent} & \\ \| & & \| \\ \sim Q \Rightarrow \sim P & \xrightarrow[\text{converse}]{\text{not logically equivalent}} & \sim P \Rightarrow \sim Q \end{array}$$

Biconditional P if and only if Q, that is $P \Leftrightarrow Q$.

Logic: Properties

- Commutative Laws: $P \vee Q \equiv Q \vee P$, and $P \wedge Q \equiv Q \wedge P$;
- Associative Laws:

$$P \vee Q \vee R \equiv P \vee (Q \vee R) \equiv (P \vee Q) \vee R, \quad P \wedge Q \wedge R \equiv P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R;$$

- Distributive Laws:

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R), \quad P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R);$$

- De Morgan[8]'s Laws:

$$\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q), \quad \sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q);$$

- Implication as disjunction (Thm 2.17): $P \Rightarrow Q \equiv (\sim P) \vee Q$;
- Negation of implication (Thm 2.21): $\sim (P \Rightarrow Q) \equiv P \wedge (\sim Q)$;
- Implication with disjunction: $P \Rightarrow (Q \vee R) \equiv (P \wedge (\sim Q)) \Rightarrow R$.

[8] Augustus De Morgan (June 27, 1806–March 18, 1871), a British mathematician and logician.

Logic: Quantifiers

- The phrase "for each", "for every", "for all", ...is called a universal quantifier. Notation: $\forall$, say "for all".
- The phrase "there exists", "there is", ...is called a existential quantifier. Notation: $\exists$, say "there exist".
- $\forall$ vs $\exists$:

$P(x)$ true for	$(\forall x)P(x)$	$(\exists x)P(x)$
all the x	True	True
only some x	False	True
none of the x	False	False

Logic: Quantifiers (Cont.)

- Two quantifiers:

	True	False
$(\forall x)(\forall y)P(x,y)$	$P(x,y)$ is true for all x and all y	$P(x,y)$ is false for some x or some y
$(\exists x)(\exists y)P(x,y)$	$P(x,y)$ is true for some x and some y	$P(x,y)$ is false for all x and y
$(\forall x)(\exists y)P(x,y)$	For any x, $P(x,y)$ is true for some y	For some x, $P(x,y)$ is false for all y
$(\exists x)(\forall y)P(x,y)$	For some x, $P(x,y)$ is true for all y	For any x, $P(x,y)$ is false for some y
$(\forall y)(\exists x)P(x,y)$	For any y, $P(x,y)$ is true for some x	For some y, $P(x,y)$ is false for all x
$(\exists y)(\forall x)P(x,y)$	For some y, $P(x,y)$ is true for all x	For any y, $P(x,y)$ is false for some x

- Negation with quantifier:

$$\begin{aligned}
\sim (\forall x)P(x) &\equiv (\exists x)(\sim P(x)),\\
\sim (\exists x)P(x) &\equiv (\forall x)(\sim P(x)),\\
\sim (\forall x)(\exists y)P(x,y) &\equiv (\exists x)(\forall y)(\sim P(x,y)),\\
\sim (\exists x)(\forall y)P(x,y) &\equiv (\forall x)(\exists y)(\sim P(x,y)),\\
\sim (\forall x)(\forall y)P(x,y) &\equiv (\exists x)(\exists y)(\sim P(x,y)),\\
\sim (\exists x)(\exists y)P(x,y) &\equiv (\forall x)(\forall y)(\sim P(x,y)).
\end{aligned}$$

Exercise (2-1)

Consider the implication: For all integers x, if $x = 2$, then $x^2 = 4$ (S).

(a) *Write down the hypothesis $P(x)$ and conclusion $Q(x)$ of S.*

(b) *Substitute x by 2, -2 and 3. Determine the truth value of $P(x) \Rightarrow Q(x)$*[9] *respectively.*

(c) *Is the universal implication S true? Explain your answer briefly.*

(d) *Write down the converse of S and determine whether it is true or false.*

(e) *Write down the contrapositive of S and determine whether it is true or false.*

Solution of (a).

(a) Hypothesis $P(x) : x = 2$ and conclusion $Q(x) : x^2 = 4$.

□

[9] $Q(y)$ should be $Q(x)$ in tutorial set 2.

Solution of (b–e).

(b)
- When $x = 2$, $P(2)$ and $Q(2)$ are true, hence $P(2) \Rightarrow Q(2)$ is true;
- When $x = -2$, $P(-2)$ is false, and $Q(-2)$ is true, hence $P(-2) \Rightarrow Q(-2)$ is true;
- When $x = 3$, $P(3)$ and $Q(3)$ are false, hence $P(3) \Rightarrow Q(3)$ is true.

(c) Yes.
- By part (b), for $x = 2$, we have $P(2) \Rightarrow Q(2)$ is true;
- For all other value of x, the hypothesis $P(x)$ is false. Whatever the truth value of the conclusion $Q(x)$ is, we have $P(x) \Rightarrow Q(x)$ is true.

Hence the universal statement $\forall x \in \mathbb{Z}, P(x) \Rightarrow Q(x)$ is true.

(d) Converse of S is "For all integers x, if $x^2 = 4$, then $x = 2$". This is false. Counterexample: $x = -2$.

(e) Contrapositive of S is "For all integers x, if $x^2 \neq 4$, then $x \neq 2$". This is true, since contrapositive is equivalent to the original conditional statement S.

Remark

For parts (d) and (e), we do not switch quantifiers when we take the converse or contrapositive of a quantified implication.

□

Exercise (2-2)

Let x be a real number. Consider the following implication:

$$\textit{If } x^3 - x = 2x^2 + 6, \textit{ then } x = -2 \textit{ or } x = 3 \quad (T).$$

Which of the following statements have the same meaning as T and which ones are negations of T. Explain your answers briefly.

(a) *If $x \neq -2$ and $x \neq 3$, then $x^3 - x \neq 2x^2 + 6$.*

(b) *If $x = -2$ or $x = 3$ then $x^3 - x = 2x^2 + 6$.*

(c) *If $x \neq -2$ or $x \neq 3$, then $x^3 - x \neq 2x^2 + 6$.*

(d) *If $x^3 - x = 2x^2 + 6$ and $x \neq -2$, then $x = 3$.*

(e) $x^3 - x = 2x^2 + 6$, $x \neq -2$ *and* $x \neq 3$.

(f) $x^3 - x \neq 2x^2 + 6$ *or* $x = -2$ *or* $x = 3$.

Solution (Using truth table).

Let $P : x^3 - x = 2x^2 + 6$, $Q : x = -2$, and $R : x = 3$, then the given statement T is $P \Rightarrow (Q \vee R)$.

(a) This statement is $((\sim Q) \wedge (\sim R)) \Rightarrow (\sim P) = \sim (Q \vee R) \Rightarrow (\sim P)$. It is the contrapositive of the given statement T and hence is equivalent to it.

(b) This statement is $(Q \vee R) \Rightarrow P$. It is the converse of the given statement T, and hence is not equivalent to the given statement and not the negation of it.

(c–f) The statements in part (c–f) are $((\sim Q) \vee (\sim R)) \Rightarrow (\sim P)$, $(P \wedge (\sim Q)) \Rightarrow R$, $P \wedge (\sim Q) \wedge (\sim R)$, and $(\sim P) \vee Q \vee R$, respectively.

P	T	T	T	T	F	F	F	F
Q	T	T	F	F	T	T	F	F
R	T	F	T	F	T	F	T	F
$T : P \Rightarrow (Q \vee R)$	T	T	T	F	T	T	T	T
(c): $((\sim Q) \vee (\sim R)) \Rightarrow (\sim P)$	T	T	T	T	F	T	T	T
(d): $(P \wedge (\sim Q)) \Rightarrow R$	T	T	T	F	T	T	T	T
(e): $P \wedge (\sim Q) \wedge (\sim R)$	F	F	F	T	F	F	F	F
(f): $(\sim P) \vee Q \vee R$	T	T	T	F	T	T	T	T

To summarize: The statements in parts (a), (d) and (f) are equivalent to the given statement T, and the statement in part (e) is the negation of T. □

Solution (Using algebra).

Let $P : x^3 - x = 2x^2 + 6$, $Q : x = -2$, and $R : x = 3$, then the given statement T is $P \Rightarrow (Q \vee R)$.

(a) This statement is $((\sim Q) \wedge (\sim R)) \Rightarrow (\sim P) = \sim (Q \vee R) \Rightarrow (\sim P)$. It is the contrapositive of the given statement T and hence is equivalent to it.

(d)

$$P \Rightarrow (Q \vee R) \equiv (P \wedge (\sim Q)) \Rightarrow R \qquad \text{Implication with disjunction}$$

(e)

$$\begin{aligned} \sim (P \Rightarrow (Q \vee R)) &\equiv P \wedge (\sim (Q \vee R)) && \text{Negation of implication} \\ &\equiv P \wedge (\sim Q \wedge \sim R) && \text{De Morgan's law} \\ &\equiv P \wedge (\sim Q) \wedge (\sim R) && \text{Associative law} \end{aligned}$$

(f)

$$P \Rightarrow (Q \vee R) \equiv (\sim P) \vee Q \vee R \qquad \text{Implication as disjunction}$$

Exercise (2-3)

Write in words a meaningful negation of each of the following statements.

(a) *If we do not win the first game, then we will not play a second game.*

(b) *If you graduate from college, then you will get a job or you will go to graduate school.*

(c) *If you clean your room or wash the dishes, then you can go to see a movie.*

Recall

- Negation of implication: $\sim (P \Rightarrow Q) \equiv P \wedge (\sim Q)$;
- De Morgan's Laws: $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$, $\sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$.

Solution.

(a) The negation is "We do not win the first game and we will play a second game".

(b) The negation is "You graduate from college, and you will not get a job and you will not go to graduate school".

(c) The negation is "Clean your room or wash the dishes, and you cannot go to see a movie".

Exercise (2-4)

Lord Hazelton was murdered. A detective was called in to solve the murder mystery. He determines some facts (true statements) listed below. Is it possible for the detective to deduce the identity of the murderer from the facts? Explain your reasoning.

(i) *Lord Hazelton was killed by a blow on the head with a brass candlestick.*

(ii) *Either Lady Hazelton or a maid, Sara, was in the dining room at the time of the murder.*

(iii) *If the cook was in the kitchen at the time of the murder, then the butler killed Lord Hazelton with a fatal dose of strychnine.*

(iv) *If Lady Hazelton was in the dining room at the time of the murder, then the Chauffer killed Lord Hazelton.*

(v) *If the cook was not in the kitchen at the time of the murder, then Sara was not in the dining room when the murder was committed.*

(vi) *If Sara was in the dining room at the time the murder was committed, then the wine steward killed Lord Hazelton.*

(vii) *There was only one cause of death.*

Solution.

First we represent the following (simple) statements by alphabetical letters:

A Lord Hazelton was killed by a blow on the head with a brass candlestick.

B Lady Hazelton was in the dining room at the time of the murder.

C Maid Sara was in the dining room at the time of the murder.

D The cook was in the kitchen at the time of the murder.

E The butler killed Lord Hazelton with a fatal dose of strychnine.

F The Chauffer killed Lord Hazelton.

G The wine steward killed Lord Hazelton.

H There was only one cause of death.

Then the facts (i) to (vii) can be represented by:

(i) A; (ii) $B \vee C$; (iii) $D \Rightarrow E$; (iv) $B \Rightarrow F$; (v) $\sim D \Rightarrow \sim C$; (vi) $C \Rightarrow G$; (vii) H.

- Since (i) and (vii) are true, we deduce that E is false.
- Then by (iii), we deduce that D is false.
- Then by (v), we deduce that C is false.
- Then by (ii), we deduce that B is true.
- Then by (iv), we deduce that F is true.

Hence the Chauffer killed Lord Hazelton. □

Exercise (2-5)

Express each of the following statements in symbolic form using quantifiers $\forall$ or $\exists$.

(a) *Every real number is positive, negative or zero.*

(b) *The integer 13 is not a square.*

(c) *There is at least one real number whose square is 13.*

(d) *No even numbers are prime.*

(e) *Not all odd numbers are prime.*

Solution.

(a) $(\forall x \in \mathbb{R})((x > 0) \vee (x < 0) \vee (x = 0))$;

(b) $(\forall x \in \mathbb{Z})(13 \neq x^2)$;

(c) $(\exists x \in \mathbb{R})(13 = x^2)$;

(d) $\sim (\exists x \in \mathbb{Z})((x \text{ is even}) \wedge (x \text{ is a prime}))$.
Alternative solutions: $(\forall x \in \mathbb{Z})((x \text{ is even}) \Rightarrow (x \text{ is not a prime}))$, or
$(\forall x \in \{2n \mid n \in \mathbb{Z}\})(x \text{ is not a prime})$;

(e) $(\exists x \in \mathbb{Z})((x \text{ is odd}) \wedge (x \text{ is not a prime}))$.

Exercise (2-6)

Write the negation of each of the following quantified statements in symbolic form without using the negation symbol.

(a) $(\forall a \in \mathbb{Z})(a$ *is even or* a *is odd*$)$

(b) $(\exists x \in \mathbb{Q})(\sqrt{2} < x < \sqrt{3})$

(c) $(\forall a \in \mathbb{Z})($*If* a^2 *is odd, then* a *is odd*$)$

(d) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x^2 + y^2 = 1)$

Recall

- Roughly speaking, $\sim$ changes $\forall$ to $\exists$, and $\exists$ to $\forall$;
- Negation of implication: $\sim (P \Rightarrow Q) \equiv P \wedge (\sim Q)$;
- De Morgan's Laws: $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$, $\sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$.

Solution.

(a) $(\exists a \in \mathbb{Z})((a$ is odd$) \wedge (a$ is even$))$;

(b) $(\forall x \in \mathbb{Q})((x \leq \sqrt{2}) \vee (x \geq \sqrt{3}))$;

(c) $(\exists a \in \mathbb{Z})((a^2$ is odd$) \wedge (a$ is even$))$;

(d) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x^2 + y^2 \neq 1)$.

Exercise (2-7)

Consider the open sentence $P(x, y) : x = 2y$ where the variables represent integers. There are six different ways to quantify $P(x, y)$ into a statement. Write down all the six statements and determine whether each is true or false. Give brief explanations for your answers.

Recall

Truth tables of 2-quantifier implications.

Solution.

The 6 statements are as follows:

- $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x = 2y)$: False. Counterexample $x = 1$, $y = 2$;
- $(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x = 2y)$: True. Take $x = 2$, $y = 1$;
- $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x = 2y)$: False. Counterexample $x = 3$. Then $3 \neq 2y$ for any integer y;
- $(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x = 2y)$: False. We cannot find any fixed integer x that is twice of every integer y;
- $(\forall y \in \mathbb{Z})(\exists x \in \mathbb{Z})(x = 2y)$: True. For any integer y, simple let $x = 2y$, which is an integer;
- $(\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z})(x = 2y)$: False. We cannot find any fixed integer y that is half of every integer x.

Exercise (2-8)

Determine whether each of the following biconditional statements is true or false. If it is false, "weaken" it to an implication which is true.

(a) *An integer is an even square if and only if it is divisible by 4.*

(b) *A square integer is even if and only if it is divisible by 4.*

Solution.

(a) False.

- For the "if" part, it is false, and 8 is a counterexample;
- For the "only if" part, since x is in the form $(2n)^2$, it will be divisible by 4.

We will weaken the biconditional statement to the "only if" part: An integer is an even square only if it is divisible by 4.

(b) True.

- For the "if" part, it is trivial that a integer is even if it is divisible by 4;
- For the "only if" part, since square integer x is even, x will be an even square, and hence x will be divisible by 4.

□

Additional material

Exercise (Question 3 in Mid-term 2009–2010(I))

Let $A_n = \left\{k \in \mathbb{N} \mid \frac{(n-1)n}{2} + 1 \leq k \leq \frac{n(n+1)}{2}\right\}$ *for every* $n \in \mathbb{N}$. *Answer the following questions:*

(i) *What is the cardinality* $|A_n|$*?*

(ii) *What are* $\cup_{n\in\mathbb{N}} A_n$ *and* $\cap_{n\in\mathbb{N}} A_n$*?*

(iii) *Give an example of a set* B *such that* $|B \cap A_n| = 1$ *for every* $n \in \mathbb{N}$. *Express your answer using set notation.*

(iv) *Give a partition* S *of* $\mathbb{N}$ *such that* S *is an infinite set and every element of* S *has a different cardinality from each other.*

Solution.

(i) $|A_n| = \frac{n(n+1)}{2} - \left(\frac{(n-1)n}{2} + 1\right) + 1 = n$;

(ii) Since there is no common element in A_n and A_{n+1}, $\cap_{n\in\mathbb{N}} A_n = \emptyset$; For any positive integer x, we can find an integer n, such that $\frac{(n-1)n}{2} + 1 \leq x \leq \frac{n(n+1)}{2}$, i.e. $x \in A_n$. Hence $\cup_{n\in\mathbb{N}} A_n = \mathbb{N}$;

(iii) $B = \left\{\frac{n(n+1)}{2} \mid n \in \mathbb{N}\right\}$;

(iv) $S = \{A_n \mid n \in \mathbb{N}\}$.

Additional material: Relation between logic operators

Exercise

(a) *Could you use* $\sim$ *and* $\wedge$ *to equivalently represent* $\vee$, $\Rightarrow$ *and* $\Leftrightarrow$*?*

(b) *Could you use* $\sim$ *and* $\vee$ *to equivalently represent* $\wedge$, $\Rightarrow$ *and* $\Leftrightarrow$*?*

(c) *Could you use* $\sim$ *and* $\Rightarrow$ *to equivalently represent* $\wedge$, $\vee$ *and* $\Leftrightarrow$*?*

(d) *Could you use* $\sim$ *and* $\Leftrightarrow$ *to equivalently represent* $\wedge$, $\vee$ *and* $\Rightarrow$*?*

(e) *Could you use* $\vee$, $\wedge$, $\Rightarrow$ *and* $\Leftrightarrow$ *to equivalently represent* $\sim$*?*

Additional material: Relation between logic operators (Cont.)

Solution.

(a) Yes.

- $P \vee Q \equiv \sim((\sim P) \wedge (\sim Q))$;
- $P \Rightarrow Q \equiv (\sim P) \vee Q \equiv \sim(P \wedge (\sim Q))$;
- $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \equiv \sim(P \wedge (\sim Q)) \wedge \sim(Q \wedge (\sim P))$;

(b) Yes.

- $P \wedge Q \equiv \sim((\sim P) \vee (\sim Q))$;
- $P \Rightarrow Q \equiv (\sim P) \vee Q$;
- $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \equiv ((\sim P) \vee Q) \wedge ((\sim Q) \vee P)$;

(c) Yes.

- $P \wedge Q \equiv \sim(P \Rightarrow (\sim Q))$;
- $P \vee Q \equiv (\sim P) \Rightarrow Q$;
- $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \equiv \sim((P \Rightarrow Q) \Rightarrow (\sim(Q \Rightarrow P)))$;

(d) No.

(e) No.

□

Remark

See Section 1.3.7 in 数理逻辑（汪芳庭，中国科学技术大学出版社，1990）.

Change log

- Page 31: Revise a typo: "the statements in parts (b) and (e) are the negation of T" to "the statement in part (e) is the negation of T";
- Page 32: Add another solution based on algebra method;
- Page 36: Revise the solution for part (d);
- Page 39: Give more details for the solutions.

Last modified: 20:39, August 30, 2010.

Schedule of Tutorial 3

- Review concepts: Proof
  - Definition, axiom, theorem, proposition;
  - Direct proof, proof by contrapositive, proof by cases, disjunction in conclusion;
  - Parity, divisibility, congruence;
  - Abstract value, triangle inequality.
- Tutorial
- Additional material:
  - Question 2(a) in Mid-term 2007–2008(I);
  - Question 4 in Mid-term 2008–2009(I);
  - Properties of $(\mathbb{Z}, +, \cdot)$.

Proof: True statements and Proof methods

True statements

- Definition: Giving the precise meaning of a word or phase that represents some object, property or other concepts.
- Axiom: Basic properties that are regarded as true statement without needing a proof is called an axiom.
- Theorem, lemma, corollary, proposition (need proofs).
- Axioms, Definitions $\Rightarrow$ Theorems, Lemmas, Propositions.

Proof methods

- Direct proof: Starting from hypothesis P, using some true statements to get conclusion Q.
- Proof by contrapositive: $P \Rightarrow Q \equiv (\sim Q) \Rightarrow (\sim P)$.
- Proof by cases: for convenience, we usually split the assumption to several cases, and then prove every case.
- Disjunction in conclusion:
  $(P \Rightarrow (Q \vee R)) \equiv ((P \wedge (\sim Q)) \Rightarrow R)$.
  Advantage: more conditions.
- Proving biconditionals: $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Integers (Closure, Parity)

- Basic properties of $(\mathbb{Z}, +, \cdot)$:
  - Identity: $n + 0 = n$ and $n \cdot 1 = n$;
  - Inverse: $n + (-n) = 0$, but the inverse for multiplication does not exist except $n = \pm 1$;
  - Commutative: $n + m = m + n$ and $m \cdot n = n \cdot m$;
  - Associative: $(l + m) + n = l + (m + n)$ and $(l \cdot m) \cdot n = l \cdot (m \cdot n)$;
  - Distributive: $l \cdot (m + n) = l \cdot m + l \cdot n$, and $(l + m) \cdot n = l \cdot n + m \cdot n$.
- Closure: $\mathbb{Z}$ is closed under $\begin{cases} \text{addition} & m + n \\ \text{multiplication} & m \cdot n \end{cases} \in \mathbb{Z}$ for any $m, n \in \mathbb{Z}$.
- Parity: n is $\begin{cases} \text{odd} \\ \text{even} \end{cases}$, iff there exists an integer m, such that $n = \begin{cases} 2m + 1 \\ 2m \end{cases}$.

  There are some facts:
  - odd $\pm$ odd $=$ even, odd $\pm$ even $=$ odd, even $\pm$ even $=$ even (By definition);
  - n is even iff n^2 is even (Theorem 3.12);
  - n is odd iff n^2 is odd (Contrapositive of Theorem 3.12);
  - ab is even iff a is even or b is even (Theorem 3.17);
  - ab is odd iff a is odd and b is odd (Contrapositive of Theorem 3.17).

Integers (Divisibility)

- Divisibility: m divides n if there exists an integer q, such that $n = mq$. Notation: $m \mid n$, and we say that m is divisor.
  Negation: m does not divide n if for any integer q, $n \neq mq$. Notation: $m \nmid n$.
- Congruence: Let a, b and n be integers with $n \geq 2$. If n divides $a - b$, we say that a is congruent to b modulo n. Notation: $a \equiv b \bmod n$.
- Relation:
  - $a \equiv b \bmod n$, iff $n \mid (a - b)$, iff $a - b = nk$ for some integer k.
  - Let a and n be integers with $n \geq 2$, then $a \equiv 0 \bmod n$ iff $n \mid a$.
- Division Algorithm[10]: Given two integers a and d, with $d \neq 0$. There exist unique integers q and r such that $a = qd + r$ and $0 \leq r < |d|$, where $|d|$ denotes the absolute value of d. q is called the quotient, r is called the remainder, d is called the divisor, and a is called the dividend.
  That is, for any integers a and d (here we assume that d is positive), we have that a can be expressed as $a = qd$, or $a = qd + 1, \ldots,$ or $a = qd + (d - 1)$ for some integer q.
  For example, let $d = 3$, then every integer x can be expressed as $x = 3q$, or $x = 3q + 1$, or $x = 3q + 2$ for some integer q.

[10] See Theorem 11.4 on page 247, Chartrand's textbook.

Real Numbers

- Absolute value: $|x| = \begin{cases} x, & \text{if } x \geq 0; \\ -x, & \text{if } x < 0. \end{cases}$
- Triangle inequality: $|x+y| \leq |x| + |y|$.

  Proof.
  - By definition, we have $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$.
  - Combining these inequalities, we obtain $-(|x| + |y|) \leq x + y \leq |x| + |y|$
  - Also by definition, we have $|x+y| \leq |x| + |y|$.
- Triangle inequality: $|x-y| \geq |x| - |y|$.

Exercise (3-1)

Let n be an integer. Use the definitions of even and odd integers to prove that following statements:

(a) *If n is even, then n^3 is even.*

(b) *If n^3 is even, then n is even.*

(c) *The integer n is even if and only if n^3 is even.*

(d) *The integer n is odd if and only if n^3 is odd.*

Proof.

(a) Let n be even. So there exists an integer k such that $n = 2k$. Then $n^3 = (2k)^3 = 8k^3 = 2(4k^3)$. Since $4k^3$ is an integer, we obtain that n^3 is even.

(b)
- It suffices to show the contrapositive: If n is odd, then n^3 is odd.
- Let n be odd. So there exists an integer k such that $n = 2k + 1$. Then $n^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$. This means that n^3 is odd.
- Therefore we have that n is even if n^3 is even.

(c) This biconditional statement is the conjunction of the two implications in parts (a) and (b), which have been proven.

(d) This biconditional statement is the conjunction of the contrapositives of the two implications in parts (a) and (b), which have been proven.

□

Exercise (3-2)

Let a, b and c be nonzero integers. Prove the following statements.

(a) *If a divides b and b divides c, then a divides c.*

(b) *If a divides b, then ac divides bc.*

(c) *If a divides b, then a^2 divides b^2.*

(d) *If a divides b and b divides a, then $a = \pm b$.*

Recall

By definition, $m \mid n$ iff there exists an integer q such that $n = mq$.

Proof.

(a) Since $a \mid b$, there exists an integer p such that $b = ap$. Since $b \mid c$, there exists an integer q such that $c = bq$. So $c = (ap)q = a(pq)$. This means $a \mid c$ since pq is an integer.

(b) Since $a \mid b$, there exists an integer q such that $b = aq$. So $bc = (aq)c = q(ac)$. This means $ac \mid bc$.

(c) Since $a \mid b$, there exists an integer q such that $b = aq$. So $b^2 = (aq)^2 = a^2q^2$. This means $a^2 \mid b^2$.

(d) Since $a \mid b$ and $b \mid a$, there exist integers p and q such that $b = ap$ and $a = bq$. So $b = ap = (bq)p = b(pq)$ and thus $pq = 1$ which implies $p = \pm 1$ since p and q are integers. This means $a = \pm b$.

□

Exercise (3-3)

Is each of the following statements true or false? Give a proof if it is true, and give a counter-example if it is false.

(a) *For all integers a, b, c, if a divides $b + c$, then a divides b or a divides c.*

(b) *For all integers a, b, c, if a divides bc, then a divides b or a divides c.*

(c) *For all integers a, b, if a divides b^2 and $a \leq b$, then a divides b.*

(d) *For all integers a, b, c, if ab divides c, then a divides c and b divides c.*

Solution.

(a) False. Counterexample: $a = 2, b = 1, c = 3$. Then $2 \mid (1 + 3)$ but $2 \nmid 1$ and $2 \nmid 3$.

(b) False. Counterexample: $a = 4, b = 2, c = 6$. Then $4 \mid (2 \times 6)$ but $4 \nmid 2$ and $4 \nmid 6$.

(c) False. Counterexample: $a = 4, b = 6$. Then $4 \mid 6^2$ and $4 \leq 6$ but $4 \nmid 6$.

(d) True. Since $ab \mid c$, there exists an integer q such that $c = abq$. So $c = a(bq)$ and $c = b(aq)$. Since bq and aq are both integers. This means $a \mid c$ and $b \mid c$.

Exercise (3-4)

Let a, b be integers and n a positive integer. Prove the following propositions:

(a) *If $a \equiv b \bmod n$, then $ka \equiv kb \bmod kn$ for any positive integer k.*

(b) *If m is a divisor of n, and $a \equiv b \bmod n$, then $a \equiv b \bmod m$.*

Recall

$a \equiv b \bmod n$ iff $n \mid (a-b)$ iff $a - b = nk$ for some integer k, where $n \geq 2$.

Proof.

(a)
1. Given $a \equiv b \bmod n$. Let k be a positive integer. We want to prove that $ka \equiv kb \bmod kn$.
2. By definition of congruence, we have $n \mid (a-b)$. This means there exists an integer q such that $a - b = nq$.
3. Multiply this equation by k, we get $k(a-b) = k(nq)$ which gives $ka - kb = (kn)q$. This implies $kn \mid (ka - kb)$.
4. By definition of congruence, we have $ka \equiv kb \bmod kn$.

(b)
1. Given $m \mid n$ and $a \equiv b \bmod n$. We want to prove that $a \equiv b \bmod m$.
2. By definition of congruence, we have $n \mid (a-b)$.
3. Since we have $m \mid n$ and $n \mid (a-b)$, we conclude that $m \mid (a-b)$ (by Exercise 3-2(a)).
4. By definition of congruence, we have $a \equiv b \bmod m$.

□

Exercise (3-5)

Show that 3 divides $n(n+1)(2n+1)$ for any integer n.

Proof.

We consider three cases:

- If $n \equiv 0 \mod 3$: then $n = 3k$ for some integer k, and $n(n+1)(2n+1) = 3k(n+1)(2n+1)$, which is divisible by 3.
- If $n \equiv 1 \mod 3$: then $n = 3k+1$ for some integer k, and $n(n+1)(2n+1) = n(n+1)(2[3k+1]+1) = n(n+1)(6k+3) = 3n(n+1)(2k+1)$, which is divisible by 3.
- If $n \equiv 2 \mod 3$: then $n = 3k+2$ for some integer k, and $n(n+1)(2n+1) = n([3k+2]+1)(2n+1) = n(3k+3)(2n+1) = 3n(k+1)(2n+1)$, which is divisible by 3.

We see that, for all the three cases, $n(n+1)(2n+1)$ is divisible by 3. □

Exercise (3-6)

Prove the following statement by proving its contrapositive. For all integers a, b, if $ab \equiv 0 \bmod 3$, then $a \equiv 0 \bmod 3$ or $b \equiv 0 \bmod 3$.

Proof.

1. The contrapositive is: For all integers a, b, if $a \not\equiv 0 \bmod 3$ and $b \not\equiv 0 \bmod 3$, then $ab \not\equiv 0 \bmod 3$.
2. So from the hypothesis, for any integers a, b, we will have the following four cases:
   - If $a \equiv 1 \bmod 3$ and $b \equiv 1 \bmod 3$; so $ab \equiv 1 \times 1 \equiv 1 \bmod 3$.
   - If $a \equiv 1 \bmod 3$ and $b \equiv 2 \bmod 3$; so $ab \equiv 1 \times 2 \equiv 2 \bmod 3$.
   - If $a \equiv 2 \bmod 3$ and $b \equiv 1 \bmod 3$; so $ab \equiv 2 \times 1 \equiv 2 \bmod 3$.
   - If $a \equiv 2 \bmod 3$ and $b \equiv 2 \bmod 3$; so $ab \equiv 2 \times 2 \equiv 1 \bmod 3$.
3. In all cases, we have $ab \not\equiv 0 \bmod 3$.
4. Therefore, for all integers a, b, if $ab \equiv 0 \bmod 3$, then $a \equiv 0 \bmod 3$ or $b \equiv 0 \bmod 3$.

□

Exercise (3-7)

Use definition of absolute value to prove the following biconditional: For all real number x and a with $a > 0$, $|x| < a$ if and only if $-a < x < a$.

Recall

Absolute value: $|x| = \begin{cases} x, & \text{if } x \geq 0; \\ -x, & \text{if } x < 0. \end{cases}$

Proof.

"If" Given $-a < x < a$ (1). From the definition of abstract value, we will consider two cases: $x \geq 0$ and $x < 0$.

- $x \geq 0$. Then from (1), $|x| = x < a$.
- $x < 0$. Then from (1), $-a < x$ implies $a > -x = |x|$.

Combining the two cases, we conclude that $|x| < a$.

"Only if" Given $|x| < a$ (2). From the definition of abstract value, we will consider two cases: $x \geq 0$ and $x < 0$.

- $x \geq 0$. Then from (2), $x < a$. Also $-a < 0 \leq x$. So we have $-a < x < a$.
- $x < 0$. Then from (2), $-x < a$ which implies $x > -a$. Also $x < 0 < a$. So we have $-a < x < a$.

Combining the two cases, we conclude that $-a < x < a$.

□

Exercise (3-8)

Let a and b be positive integers such that $a^2 = b^3$. Prove that, if a is even, then 4 divides both a and b.

Proof.

1. We start with the given condition $a^2 = b^3$ (1);
2. Suppose a is even. Then $a = 2k$ (2) for some integer k. Substitute (2) into (1), we get $b^3 = 4k^2 = 2(2k^2)$ (3);
3. So b^3 is even, and hence b is even (by Exercise 3-1(d)) and we can write $b = 2h$ (4) for some integer h;
4. By substituting (4) into (3), we get $8h^3 = 4k^2$ which simplifies as $2h^3 = k^2$ (5);
5. This implies k^2 is even and hence k is even. So we can write $k = 2t$ (6) for some integer t;
6. Substituting (6) into (2), we get $a = 4t$. This proves 4 divides a.
7. Now substituting (6) into (5), we get $2h^3 = 4t^2$. This simplifies as $h^3 = 2t^2$ which implies h^3 is even.
8. Hence h is even, and we can write $h = 2s$ (7) for some integer s. Substituting (7) into (4), we get $b = 4s$. This proves 4 divides b.

□

Additional material

Exercise (Question 2(a) in Mid-term 2007–2008(I))

Prove that, for every integer n, if $n^2 - 4n + 1$ is odd, then n is even.

Direct proof.

1. For any integer n, assume that $n^2 - 4n + 1$ is odd;
2. Since $-4n + 1 = 2(-2n) + 1$ is odd, we obtain that n^2 is even;
3. Since n^2 and n have the same parity, we obtain that n is even.

□

Proof by contrapositive.

1. Contrapositive: Suppose that n is odd, we want to show that $n^2 - 4n + 1$ is even;
2. Since n is odd, we obtain that n^2 is odd. On the other hand, $4n = 2(2n)$ is even;
3. So $n^2 - 4n$ is odd, and therefore $n^2 - 4n + 1$ is even.

□

Additional material

Exercise (Question 4 in Mid-term 2008–2009(I))

Let $A_1 = \{m \in \mathbb{Z}^+ \mid 2 \nmid m\}$, $A_2 = \{m \in \mathbb{Z}^+ \mid 3 \nmid m\}$, ... *In general,* $A_n = \{m \in \mathbb{Z}^+ \mid (n+1) \nmid m\}$ *for every* $n \in \mathbb{Z}^+$.

(a) *Write down the set builders notation of* $A_1 \cap A_2$ *in terms of congruence modulo 6. Briefly justify your answer.*

(b) *Show that* $A_1 \cap A_3 = A_1$.

(c) *What is* $\cap_{n \in \mathbb{N}} A_n$*? Justify your answer.*

Change log

Last modified: 20:39, September 6, 2010.

Information of Mid-term test

- Time: October 1st (Friday), 12:00–14:00;
- Venue: MPSH 2;
- Close book with 1 a4-size helpsheet;
- Consultation:
  - Time:
    - Sept 27th, Monday, 09:00–11:00, 13:00–17:00, 19:00–21:00;
    - Sept 28th, Tuesday, 09:00–11:00, 13:00–17:00, 19:00–21:00;
    - Sept 29th, Wednesday, 09:00–11:00;
    - Sept 30th, Thursday, 09:00–11:00;
    - Oct 1st, Friday, 09:00–11:00.
  - Venue: S17-06-14
  - Email: xiangsun@nus.edu.sg
  - Mobile: 9169 7677

Schedule of Tutorial 4

- Review concepts: Proof
  - proof by contradiction, existence proof;
  - rational number, irrational number.
- Tutorial
- Additional material:
  - relation between rational numbers and decimal;
  - Question 4 in Mid-term 2008–2009(I);
  - Question 4 in Mid-term 2009–2010(I).

Proof: Proof by Contradiction

- Direct Proof, Proof by Contrapositive, Proof by contradiction;
- - Prove that R is true:
    Assume that $\sim R$ is true, and try to get a contradiction;
  - Prove that $(\forall x)R(x)$ is true:
    Assume that $(\exists x)(\sim R(x))$ is true, and try to get a contradiction;
  - Prove that $(\forall x)(P(x) \Rightarrow Q(x))$ is true:
    Assume that $(\exists x)(P(x) \wedge (\sim Q(x)))$ is true, and try to get a contradiction.
- When to use:
  - When there is no direct proof: "there do not exist...", "A is an emptyset...", and "p is an irrational number..."....
  - When it is easy to work with the $\sim R$.
- Notice: to prove (quantified) implication, "proof by contradiction" and "proof by contrapositive" have the same power.
- Advantage: For implication $P \Rightarrow Q$, we have more assumption[11] to work with:
  - For direct proof, we have one assumption P;
  - For proof by contradiction, we have more assumption $\sim Q$.

[11] Compare with disjunction in conclusion.

Proof: Existence Proof

- Existence statements are those that involve existential quantifiers.
- Three types:
  - $(\exists x)\, P(x)$.
  - $(\exists x)(\forall y)\, P(x, y)$.
  - $(\forall x)(\exists y)\, P(x, y)$.
- Two approaches:
  - Constructive proof:
    (1) Give a specific example of such objects;
    (2) Justify that the given examples satisfy the stated conditions.
  - Non-constructive proof:
    (1) Use when specific examples are not easy or not possible to find;
    (2) Make arguments why such objects have to exist;
    (3) Use definitions, axioms or results that involves existence statements.

Rational numbers and irrational numbers

- A rational number is a real number that can be written as a quotient $\frac{m}{n}$ where m and n are integers, with $n > 0$.
- An irrational number is a real number that is not a rational number.
- A rational number $\frac{m}{n}$ with $n > 0$ is in lowest term if m and n have no common factor which is greater than 1. This property is very useful for proof by contradiction.
- (1)

$$\begin{aligned} \text{Rational} \pm \text{Rational} &= \text{Rational}, \\ \text{Rational} \pm \text{Irrational} &= \text{Irrational}, \\ \text{Irrational} \pm \text{Irrational} &= ? \text{ (it depends)}. \end{aligned}$$

(2)

$$\begin{aligned} \text{Rational} \cdot \text{Rational} &= \text{Rational}, \\ \text{Zero} \cdot \text{Irrational} &= \text{Zero (Rational)}, \\ \text{Non-zero Rational} \cdot \text{Irrational} &= \text{Irrational}, \\ \text{Irrational} \cdot \text{Irrational} &= ? \text{ (it depends)}. \end{aligned}$$

Rational numbers and irrational numbers (Cont.)

- (1) Every rational number is either a terminating or non-terminating repeating decimal;
  (2) Every irrational number is a non-terminating non-repeating decimal.

  Proof for part(1) We will apply long division for rational numbers. Only finitely many different remainders can occur.
  - If at any point in the division the remainder is 0, the expansion terminates at that point;
  - If 0 never occurs as a remainder, then the division process continues forever, and eventually a remainder must occur that has occurred before. The next step in the division will yield the same new digit in the quotient, and the same new remainder, as the previous time the remainder was the same. Therefore the following division will repeat the same results.

  Proof for part(2) We will apply proof by contrapositive: every terminating or non-terminating repeating decimal is rational.
  - It is trivial that every terminating decimal is a rational number;
  - For any non-terminating repeating decimal x, let n be the length of the repetend. Then $10^n x - x$ is a terminating decimal, and hence x is a rational number.

- (1) There is a rational number between any two distinct real numbers;
  (2) There are infinitely many rational numbers in $[0, 1]$ (any interval).

- (1) There is an irrational number between any two distinct real numbers;
  (2) There are infinitely many irrational numbers in $[0, 1]$ (any interval).

Exercise (4-1)

Let a, b, c be integers. Prove that, if 3 divides a, 3 divides b, and $c \equiv 1 \bmod 3$, then the equation $ax + by = c$ has no integer solutions in x and y.

Proof.

1. A proof by contradiction will be used. We assume that the statement is false. That is, we assume that there exist integers a, b and c such that $3 \mid a$, $3 \mid b$ and $c \equiv 1 \bmod 3$, and that the equation $ax + by = c$ has a solution in which both x and y are integers.
2. Let $x = m$ and $y = n$ be the solution for the equation $ax + by = c$, where m, n are integers. Then m and n satisfy the equation
$$am + bn = c.$$
3. Notice that $3 \mid a$ and $3 \mid b$, and thus $3 \mid am$ and $3 \mid bn$ which implies $3 \mid (am + bn)$, and so $3 \mid c$. But that contradicts $c \equiv 1 \bmod 3$.
4. Consequently, our assumption cannot be true, and we have proven that: If $3 \mid a$, $3 \mid b$ and $c \equiv 1 \bmod 3$, then the equation $ax + by = c$ has no integer solutions in x and y.

□

Remark

We can also apply a proof by contrapositive.

Exercise (4-2(a))

Is the following statement true or false? Give a proof if it is true, and give a counterexample if it is false.
(a) *For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.*

Recall

Irrational numbers are difficult to represent, so generally we consider its contradiction in terms of rational numbers.

Solution.

1. Assume that the original statement is true first, and try to prove it.
2. Proof by contradiction: assume that there exists a positive real number x, such that x is irrational and $\sqrt{x}$ is rational. We want to find a contradiction.
3. Since $\sqrt{x}$ is rational, there exist integers $m \geq 0$ and $n > 0$ (since $\sqrt{x} \geq 0$) such that $\sqrt{x} = \frac{m}{n}$.
4. Squaring both sides, we have $x = \frac{m^2}{n^2}$ which is rational (Contradiction).
5. Hence, the original statement is true.

□

Exercise (4-2(b))

Is the following statement true or false? Give a proof if it is true, and give a counterexample if it is false.
(b) *For each pair of real numbers x and y, if $x+y$ is irrational, then x is irrational and y is irrational.*

Recall

Rational $\pm$ Irrational $=$ Irrational, Irrational $\pm$ Irrational $=$? (It depends).

Solution.

False. A counterexample is $x=\sqrt{2}$ and $y=0$. Then $x+y=\sqrt{2}$ is irrational but not both x and y are irrational. $\square$

Exercise (4-2(c))

Is the following statement true or false? Give a proof if it is true, and give a counterexample if it is false.
(c) *For each pair of real numbers x and y, if $x+y$ is irrational, then x is irrational or y is irrational.*

Recall

Rational $\pm$ Rational $=$ Rational.

Solution.

1. We consider its contrapositive: for each pair of real numbers x and y, if x is rational and y is rational, then $x+y$ is rational.
2. This statement is true by closure property of rational numbers under addition: let $x=\frac{m}{n}$ and $y=\frac{p}{q}$, then $x+y=\frac{mq+np}{nq}$.
3. Hence, the original statement is true.

□

Exercise (4-2(d))

Is the following statement true or false? Give a proof if it is true, and give a counterexample if it is false.
(d) *For each pair of nonzero real numbers x and y, if x is rational and y is irrational, then xy is irrational.*

Recall

Non-zero Rational $\cdot$ Irrational $=$ Irrational, Zero $\cdot$ Irrational $=$ Zero (Rational).

Solution.

1. Apply a proof by contradiction. So, we assume that there exist nonzero real numbers x and y such that x is rational, y is irrational, and xy is rational.
2. Since the rational numbers are closed under division by nonzero rational numbers, this implies that $\frac{xy}{x}$ is a rational number.
3. Since $\frac{xy}{x} = y$, we conclude that y is a rational number and this contradicts the assumption that y is irrational.
4. Hence, the original statement is true.

□

Exercise (4-3(a))

Prove that $\sqrt{3}$ is an irrational number. (You may assume the fact that $3 \mid n$ if and only if $3 \mid n^2$.)

Recall

$3 \mid n$ if and only if $3 \mid n^2$.

Proof of Recall.

"Only if" Trivial.

"If" Prove by contrapositive: if $3 \nmid n$, then $3 \nmid n^2$. Consider the following two cases:

- If $n \equiv 1 \bmod 3$, i.e. $n = 3k + 1$ for some integer k. Then $n^2 = 3(3k^2 + 2k) + 1$, and hence $3 \nmid n^2$;
- If $n \equiv 2 \bmod 3$, i.e. $n = 3k + 2$ for some integer k. Then $n^2 = 3(3k^2 + 4k + 1) + 1$, and hence $3 \nmid n^2$.

□

Remark

In the proof of the question, we do not need to prove the hint.

Proof of 4-3(a).

1. Proof by contradiction: If we assume that $\sqrt{3}$ is rational, then we can write $\sqrt{3} = \frac{m}{n}$ in lowest term, i.e. m, n are integers with no common factor greater than 1.
2. By squaring, we have $3n^2 = m^2$ (1).
3. So $3 \mid m^2$, which implies $3 \mid m$. Hence we can write $m = 3k$ for some integer k.
4. Substituting m in terms of k in (1), we have $3n^2 = (3k)^2 = 9k^2$ and hence $n^2 = 3k^2$.
5. So $3 \mid n^2$, which implies $3 \mid n$.
6. We have shown that m and n have a common factor of 3, which contradicts our choice of m and n.
7. Hence we conclude that $\sqrt{3}$ is irrational.

□

Exercise (4-3(b))

Prove that there are infinitely many irrational numbers.

Non-constructive proof[12].

1. Assume that there are only finite irrational numbers.
2. Then we can choose the largest one among them, say r.
3. Then $r+1$ is an irrational number, and $r+1 > r$, which contradicts that r is the largest irrational number.
4. Hence, there are infinitely many irrational numbers.

□

[12] This proof is provided by Mr. Cui Wei.

Recall

Rational + Irrational = Irrational, nonzero Rational · Irrational = Irrational.

1st construction.

1. Since $\sqrt{2}$ is irrational, and any integer n is rational, so $\sqrt{2}+n$ is irrational.
2. For any two integers $m \neq n$, we have $\sqrt{2}+m \neq \sqrt{2}+n$.
3. Since there are infinitely many different choices of integers n, this gives us infinitely many different irrational numbers $\sqrt{2}+n$.

□

2nd construction.

1. Since $\sqrt{2}$ is irrational, and any positive integer n is rational, so $\frac{\sqrt{2}}{n}$ is irrational.
2. For any two integers $m \neq n$, we have $\frac{\sqrt{2}}{m} \neq \frac{\sqrt{2}}{n}$.
3. Since there are infinitely many different choices of positive integers n, this gives us infinitely many different irrational numbers $\frac{\sqrt{2}}{n}$.

□

Remark

There are many methods to construct infinitely many irrational numbers.

Exercise (4-4)

Prove that there are no integers a and n with $n \geq 2$ and $a^2 + 1 = 2^n$.

Proof.

Use a proof by contradiction. Assume there exist integers a and n with $n \geq 2$ and $a^2 + 1 = 2^n$. Consider two cases: a is even and a is odd.

- If a is even. Then $a^2 + 1$ is odd, which is a contradiction since 2^n is even when $n \geq 2$.
- If a is odd. Then there exists an integer k such that $a = 2k + 1$. Since $a^2 + 1 = 2^n$, we then see that

$$(2k+1)^2 + 1 = 4k^2 + 4k + 2 = 2^n. \tag{1}$$

We now use the assumption that $n \geq 2$ and write $2^n = 4 \cdot 2^{n-2}$, using this and equation (1), we have

$$2 = 2^n - 4k^2 - 4k = 4 \cdot 2^{n-2} - 4k^2 - 4k = 4(2^{n-2} - k^2 - k)$$

and this implies that 4 divides 2, which is a contradiction.

In view of the two cases, our assumption is false and there are no integers a and n with $n \geq 2$ and $a^2 + 1 = 2^n$. □

Exercise (4-5)

Let y_1, y_2, y_3, y_4 be real numbers. The mean (average) y of these four numbers is defined to be the sum of the four numbers divided by 4. That is

$$\bar{y} = \frac{y_1 + y_2 + y_3 + y_4}{4}.$$

Prove that there exists a y_i with $1 \leq i \leq 4$ such that $y_i \geq \bar{y}$.

Non-constructive proof.

Proof by contradiction: Suppose all the four numbers are smaller than $\bar{y}$. Then

$$\bar{y} = \frac{y_1 + y_2 + y_3 + y_4}{4} < \frac{\bar{y} + \bar{y} + \bar{y} + \bar{y}}{4} = \bar{y}.$$

This is a contradiction. So there must be some y_i which is greater than or equal to $\bar{y}$. □

Constructive proof.

Suppose y_1 is the largest of y_1, y_2, y_3 and y_4. Hence,

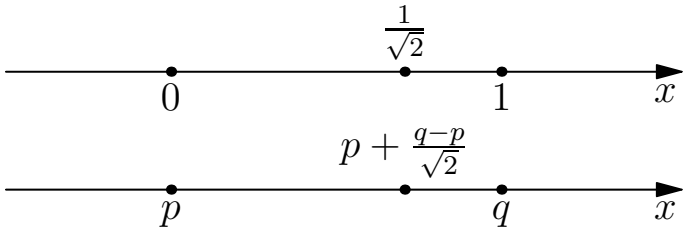
$$\bar{y} = \frac{y_1 + y_2 + y_3 + y_4}{4} \leq \frac{y_1 + y_1 + y_1 + y_1}{4} = y_1.$$

This proves the existence statement. □

Exercise (4-6)

Prove that for every pair of rational numbers p and q with $p < q$, there is an irrational number r such that $p < r < q$.

Proof.



1. Take $r = p + \frac{q-p}{\sqrt{2}}$ $\left(\frac{q-p}{\sqrt{2}}\right.$ is $\left.\frac{1}{\sqrt{2}}\right.$ of the length of the interval $[p, q]\big)$.
2. We need to show $p < r < q$. Since $q > p$, so $\frac{q-p}{\sqrt{2}} > 0$ and hence $r > p$. On the other hand, $\frac{q-p}{\sqrt{2}} < q - p$. So $r < p + (q - p) = q$.
3. We need to show that r is irrational. Suppose r is rational. Then $\sqrt{2} = \frac{q-p}{r-p}$. Since p, q, r are all rational, this implies $\sqrt{2}$ is rational, which gives a contradiction.

□

Alternative proof[13].

1. Let $\epsilon = q - p > 0$.
2. We can choose an integer n which is large enough, so that $\epsilon > \frac{\sqrt{2}}{2^n}$.
3. Then $r = p + \frac{\sqrt{2}}{2^n}$ is an irrational number and $p < r < q$.

□

Remark

We have additional result in Question 4 in Mid-term 2009–2010(I), please see additional material.

[13] This proof is provided by Mr. Dong Yongsen.

Exercise (4-7)

Determine whether the following statements are true or false. Justify your answers.

(a) *For some positive integer n, both n and $n^2 + n + 1$ are prime numbers.*

(b) *For every irrational number a, there is an irrational number b such that ab is an integer.*

(c) *There exists nonzero real numbers a and b such that $(a + b)^2 = a^2 + b^2$.*

Solution.

(a) True. Constructive proof: Take $n = 2$, a prime. Then $n^2 + n + 1 = 7$ which is also a prime.

(b) True. Constructive proof: For any irrational number a, take $b = \frac{1}{a}$. Then $ab = 1$ which is an integer. It remains to show that this b is irrational. Suppose b is rational, then $\frac{1}{b} = a$ is also rational, which is a contradiction.

(c) False. Suppose there exists $a, b \neq 0$ such that $(a + b)^2 = a^2 + b^2$. Then $a^2 + 2ab + b^2 = a^2 + b^2$, which implies $2ab = 0$. This means either a or b is 0, which is a contradiction.

□

Exercise (4-8)

Prove that the equation $x^5 + 2x - 5 = 0$ *has a unique solution between* $x = 1$ *and* $x = 2$.

Method

For existence of these questions, we will use Intermediate Value Theorem if we can not solve the equation directly.

Recall

Intermediate Value Theorem: If the function $y = f(x)$ is continuous on the interval $[a, b]$, and $f(a)f(b) < 0$, then there is a $c \in [a, b]$ such that $f(c) = 0$.

Proof of existence part.

Let $f(x) = x^5 + 2x - 5$, which is a continuous function (since $f(x)$ is a polynomial). Then $f(1) = -2$ and $f(2) = 31$. So, there exists a real number c with $1 < c < 2$ such that $f(c) = 0$. i.e.

$$c^5 + 2c - 5 = 0. \tag{2}$$

This c is a solution of the equation $x^5 + 2x - 5$. □

Method

For uniqueness, in general, let c and d be the numbers each of which satisfies the condition, and then prove $c = d$.

Proof of uniqueness part.

To show that this solution is unique. Suppose d is another solution of the equation and $1 < d < 2$. We may assume $c < d$. Then

$$d^5 + 2d - 5 = 0. \tag{3}$$

Since c and d are greater than 1, so $c^5 < d^5$. Hence

$$c^5 + 2c - 5 < d^5 + 2d - 5.$$

By (2) and (3), we have $0 < 0$ which gives a contradiction. □

Additional material

Exercise (Question 4 in Mid-term 2008–2009(I))

Let $A_1 = \{m \in \mathbb{Z}^+ \mid 2 \nmid m\}$, $A_2 = \{m \in \mathbb{Z}^+ \mid 3 \nmid m\}$, ... *In general,* $A_n = \{m \in \mathbb{Z}^+ \mid (n+1) \nmid m\}$ *for every* $n \in \mathbb{Z}^+$.

(a) *Write down the set builders notation of* $A_1 \cap A_2$ *in terms of congruence modulo 6. Briefly justify your answer.*

(b) *Show that* $A_1 \cap A_3 = A_1$.

(c) *What is* $\cap_{n\in\mathbb{N}} A_n$*? Justify your answer.*

Solution of part(a).

For any positive integer m, since $2 \nmid m$ iff $m \equiv 0 \bmod 2$ iff $m \equiv 1, 3$ or $5 \bmod 6$, we have

$$A_1 = \{m \in \mathbb{Z}^+ \mid m \equiv 1, 3, 5 \bmod 6\}.$$

Similarly, we have

$$A_2 = \{m \in \mathbb{Z}^+ \mid m \equiv 1, 2, 4 \text{ or } 5 \bmod 6\}.$$

Hence

$$A_1 \cap A_2 = \{m \in \mathbb{Z}^+ \mid m \equiv 1 \text{ or } 5 \bmod 6\}.$$

□

Additional material

Solution and proof of part(b) and part(c).

(b) It is equivalent to show $A_1 \cap A_3 \subset A_1$ and $A_1 \cap A_3 \supset A_1$.

- For any sets A and B, it is trivial $A \cap B \subset A$. Hence $A_1 \cap A_3 \subset A_1$;
- It is equivalent to show $A_1 \subset A_3$: for any element $n \in A_1$, $2 \nmid n$. Then $4 \nmid n$, i.e., $n \in A_3 = \{m \in \mathbb{Z}^+ \mid 4 \nmid m\}$.

Therefore, $A_1 \cap A_3 = A_1$.

(c) By observing, we have the following fact:
for any integer $n \geq 2$, $n \notin A_{n-1} = \{m \in \mathbb{Z}^+ \mid n \nmid m\}$.
Hence there is only one common element 1 among $\{A_n\}_{n=1}^{\infty}$.
Claim: $\cap_{n=1}^{\infty} A_n = \{1\}$. We need to show $\cap_{n=1}^{\infty} A_n \subset \{1\}$ and $\cap_{n=1}^{\infty} A_n \supset \{1\}$:

- For any positive integer n, since $(n+1) \nmid 1$, we have $1 \in A_n$. Hence $1 \in \cap_{n=1}^{\infty} A_n$;
- Let $m \in \cap_{n=1}^{\infty} A_n$. Then $m \in A_n$ for all $n \in \mathbb{Z}^+$. In particular, if $m \geq 2$, then $m \in A_{m-1}$ which means $m \nmid m$ (Contradiction). So $m \leq 1$. Hence $\cap_{n=1}^{\infty} A_n \subset \{1\}$.

Therefore we have proven the claim: $\cap_{n=1}^{\infty} A_n = \{1\}$.

□

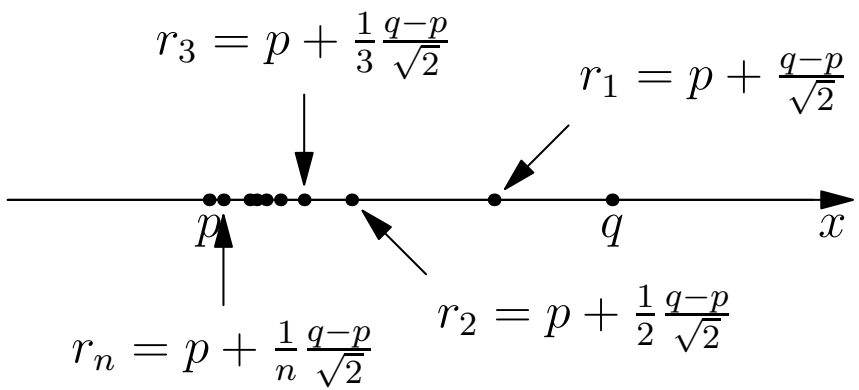
Additional material

Exercise (Question 4 in Mid-term 2009–2010(I))

Prove that for any two rational numbers p and q with $p < q$, there are infinitely many irrational numbers r such that $p < r < q$.

Proof.

1. In Exercise 4-6, we have found an irrational number $r = p + \frac{q-p}{\sqrt{2}}$ with $p < r < q$.
2. Since the multiplication of a non-zero rational number and an irrational number is an irrational number, we have that $r_n = p + \frac{1}{n}\frac{q-p}{\sqrt{2}}$ is an irrational number for every positive integer n. It is trivial that $p < r_n < q$, and $r_n \neq r_m$ if $n \neq m$.
3. Since there are infinitely many different choices of positive integers n, this gives us infinitely many different irrational numbers $r_n = p + \frac{1}{n}\frac{q-p}{\sqrt{2}}$.



□

Additional material

Alternative proof[14].

- Let $\epsilon = q - p > 0$.
- We can choose an integer n which is large enough, so that $\epsilon > \frac{\sqrt{2}}{2^n}$.
- Then $r_1 = p + \frac{\sqrt{2}}{2^n}$ is an irrational number and $p < r_1 < q$.
- Let $r_n = \frac{p+r_{n-1}}{2}$ be the mean of p and r_{n-1}, then $r_1, r_2, r_3, \ldots$ is a sequence of irrational numbers in (p, q).

□

[14] This proof is provided by Mr. Dong Yongsen.

Change log

- Page 62: Add a notice: “to prove (quantified) implication, ‘proof by contradiction’ is equivalent to ‘proof by contrapositive’.”;
- Page 65: Revise a mistake: “an integer” to “a terminating decimal”;
- Page 65: Add “(any interval)”;
- Page 65: Revise a typo: “There is a irrational number” to “There is an irrational number”;
- Page 66: Add a remark “We can also apply a proof by contrapositive.”;
- Page 67: Revise the solution;
- Page 73: Add a non-constructive proof (Thanks Mr. Cui Wei);
- Page 74: Add a remark;
- Page 78: Add an alternative proof (Thanks Mr. Dong Yongsen);
- Page 85: Add an alternative proof (Thanks Mr. Dong Yongsen).

Last modified: 13:10, September 28, 2010.

Schedule of Tutorial 5

- Review concepts:
  - Proof
    - Element-chasing method;
    - Set operations and algebra of sets;
  - Mathematical Induction
    - The Axiom of induction, and the Well-ordering principle;
    - The (strong) Principle of Mathematical Induction, and its generalization.
- Tutorial
- Additional material:
  - The Well-ordering theorem;
  - Fibonacci sequence;
  - Euclid's Theorem;
  - Upper bounds on the nth prime.

Proof: Element-chasing method

- Procedure of element-chasing method:
  (1) Choose an arbitrary element;
  (2) Show that the element satisfies the given property.
- Using this method, we can prove some relations between two sets: $A \subseteq B$, $A \nsubseteq B$, $A = B$, $A \neq B$, etc.
- For example, to prove $A \subseteq B$, where $A = \{x \in U :| (x)\}$, and $B = \{x \in U \mid q(x)\}$, we will apply the element-chasing method as follows:
  (1) Choose an arbitrary element $x_0 \in A$, then $p(x_0)$ holds;
  (2) Based on some results we have, try to prove $q(x_0)$ holds;
  (3) Since $q(x_0)$ holds, we will have $x_0 \in B$;
  (4) Hence we obtain $A \subseteq B$.

Proof: Algebra of sets

- Set operations: $P : x \in A,\ Q : x \in B$,

Set	Meaning	Logic
$A \cap B$	$x \in A$ and $x \in B$	$P \wedge Q$
$A \cup B$	$x \in A$ or $x \in B$	$P \vee Q$
A^c	$x \notin A$	$\sim P$
$A - B$	$a \in A$ and $x \notin B$	$P \wedge (\sim Q)$

- Algebra of Sets:

Idempotent $A \cap A = A,\ A \cup A = A$;
Commutative $A \cap B = B \cap A,\ A \cup B = B \cup A$;
Associative $A \cap B \cap C \equiv (A \cap B) \cap C = A \cap (B \cap C)$,
$A \cup B \cup C \equiv (A \cup B) \cup C = A \cup (B \cup C)$;
Distributive $A \cap (B \cup C) = (A \cap B) \cup (A \cap C),\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
Double Complement $(A^c)^c = A$;
De Morgan $(A \cap B)^c = A^c \cup B^c,\ (A \cup B)^c = A^c \cap B^c$.

Foundation for the Principle of Mathematical Induction

- Axiom of Induction: If T is a subset of $\mathbb{N}$, such that:
  - $1 \in T$;
  - For every $k \in \mathbb{N}$, if $k \in T$, then $k+1 \in T$.

  Then $T = \mathbb{N}$.
- We may rewrite the "Axiom of induction" in logical symbols:

$$(\forall P)\Big[\big[\underbrace{P(1)}_{\text{Base case}} \wedge \underbrace{(\forall k \in \mathbb{N})[P(k) \Rightarrow P(k+1)]}_{\text{Inductive step}}\big] \Rightarrow (\forall n \in \mathbb{N})[P(n)]\Big].$$

- Let $\emptyset \neq S \subset \mathbb{R}$, S is well-ordered if every nonempty subset of S has smallest element.
- The Well-ordering principle: The set $\mathbb{N}$ is well-ordered.
  It is a theorem and hence can be proven.
- The Well-ordering theorem: Every set can be well-ordered.
  It is an axiom, which is equivalent to "the Axiom of Choice" and "Zorn's lemma", and a foundation for generalization from $\mathbb{N}$ to any universal set U (which is always well-ordered.).

The Principle of Mathematical Induction

- PMI: Let $P(n)$ be an open sentence, such that
  - If $P(1)$ is true;
  - For all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

  Then $P(n)$ is true for all $n \in \mathbb{N}$.
- SPMI: Let $P(n)$ be an open sentence, such that
  - If $P(1)$ is true;
  - For all $k \in \mathbb{N}$, if $P(1), P(2), \ldots, P(k)$ are true, then $P(k+1)$ is true.

  Then $P(n)$ is true for all $n \in \mathbb{N}$.
- The procedure of using (S)PMI to prove that $(\forall n \in \mathbb{N})P(n)$ is true:
  (1) Identify the open sentence $P(n)$ (For general universal set, we need to identify it at first.);
  (2) Base case: prove that $P(1)$ is true;
  (3) Inductive step: for all $k \in \mathbb{N}$, assume that $P(k)$ (or $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$) is true, and prove that $P(k+1)$ is true;
  (4) Summarize the conclusion you get.

Generalizations

(S)PMI can be generalized from $\mathbb{N}$ to general universal sets (well-ordered sets).

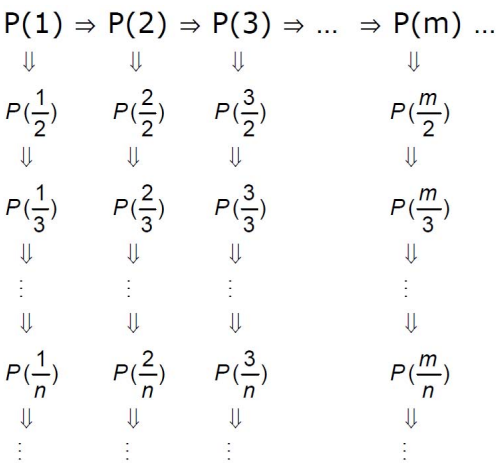
- $\{n \mid n \in \mathbb{Z}, n \geq M\}$ (M is an integer) with the order:

$$P(M) \to P(M+1) \to P(M+2) \to \cdots \to P(M+n) \to P(M+n+1) \to \cdots;$$

- $\mathbb{Z}$ with the order:

$$\cdots \leftarrow P(-n) \leftarrow \cdots \leftarrow P(-2) \leftarrow P(-1) \leftarrow P(0) \to P(1) \to P(2) \to \cdots \to P(n) \to \cdots;$$

- $\mathbb{Q}^+$:



- $\{n \in \mathbb{N} \mid n = 3p+1, p \in \mathbb{Z}, p \geq 0\}$ with the natural order:

$$P(1) \to P(4) \to P(7) \to \cdots \to P(3p+1) \to P(3p+4) \to \cdots.$$

Exercise (5-1(a))

Use Element-Chasing Method to prove
(a) *For all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cup B = B$.*

Proof of part(a).

We want to show that

$$\text{the quantified biconditional } (\forall A, B \subseteq U)\big[A \subseteq B \Leftrightarrow A \cup B = B\big] \text{ is true.}$$

For all subsets A and B of U,

"If" Given $A \cup B = B$, we want to prove $A \subseteq B$.
Let $x \in A$. It follows that $x \in A \cup B$. Since $A \cup B = B$, we have $x \in B$. This implies $A \subseteq B$.

"Only if" Given $A \subseteq B$, we want to prove $A \cup B = B$. We need to show the following two parts:

- $A \cup B \subseteq B$: Let $x \in A \cup B$, then either $x \in A$ or $x \in B$.
  - If $x \in B$, then we have done;
  - If $x \in A$, since $A \subseteq B$, we have $x \in B$.

  In either case, we have $x \in B$. Hence, $A \cup B \subseteq B$.
- $A \cup B \supseteq B$: Let $x \in B$, then $x \in A \cup B$. Hence $B \subseteq A \cup B$.

Combining these two parts, we have proven that for all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cup B = B$. □

Exercise (5-1(b))

Use Element-Chasing Method to prove
(b) *For all subsets* A, B *and* C *of some universal set* U, $A \subseteq B \cap C$ *if and only if* $A \subseteq B$ *and* $A \subseteq C$.

Proof of part(b).

We want to show that

the quantified biconditional $(\forall A, B, C \subseteq U)\big[A \subseteq B \cap C \Leftrightarrow A \subseteq B \text{ and } A \subseteq C\big]$ is true.

For all subsets A, B and C of U,

"If" Given $A \subseteq B$ and $A \subseteq C$, we want to prove $A \subseteq B \cap C$.

(1) Let $x \in A$.
(2) Since $A \subseteq B$ and $A \subseteq C$, we have $x \in B$ and $x \in C$.
(3) Then $x \in B \cap C$, and hence $A \subseteq B \cap C$.

"Only if" Given $A \subseteq B \cap C$, we want to prove $A \subseteq B$ and $A \subseteq C$.

(1) Let $x \in A$.
(2) Since $A \subseteq B \cap C$, we have $x \in B \cap C$.
(3) Then $x \in B$ and $x \in C$, and hence $A \subseteq B$ and $A \subseteq C$.

Combining these two parts, we have proven that for all subsets A, B and C of some universal set U, $A \subseteq B \cap C$ if and only if $A \subseteq B$ and $A \subseteq C$. □

Exercise (5-2(a))

Let A, B, C be subsets of some universal set U. Use Algebra of Sets to establish the following equality:
(a) $(A \cap B) - C = (A - C) \cap (B - C)$;

Method

When applying the algebra of sets to establish some equalities, we may start from the more complicated side, because simplification is always easier.

Proof.

$$
\begin{aligned}
\text{RHS} &= (A - C) \cap (B - C) \\
&= (A \cap C^c) \cap (B \cap C^c) && \text{Def of complimentary} \\
&= A \cap C^c \cap B \cap C^c && \text{Associative law} \\
&= A \cap B \cap (C^c \cap C^c) && \text{Commutative law} \\
&= A \cap B \cap C^c && \text{Idempotent law} \\
&= (A \cap B) \cap C^c && \text{Associative law} \\
&= (A \cap B) - C = \text{LHS} && \text{Def of complimentary}
\end{aligned}
$$

□

Exercise (5-2(b))

Let A, B, C be subsets of some universal set U. Use Algebra of Sets to establish the following equality:
(b) $(A \cup B) - (A \cap B) = (A - B) \cup (B - A)$;

Proof.

$$
\begin{aligned}
\text{LHS} &= (A \cup B) - (A \cap B) \\
&= (A \cup B) \cap (A \cap B)^c && \text{Def of complimentary} \\
&= (A \cup B) \cap (A^c \cup B^c) && \text{De Morgan's law} \\
&= [A \cap (A^c \cup B^c)] \cup [B \cap (A^c \cap B^c)] && \text{Distributive law} \\
&= [(A \cap A^c) \cup (A \cap B^c)] \cup [(B \cap A^c) \cup (B \cap B^c)] && \text{Distributive law} \\
&= [A \cap B^c] \cup [B \cap A^c] \\
&= (A - B) \cup (B - A) = \text{RHS} && \text{Def of complimentary}
\end{aligned}
$$

□

Exercise (5-2(c))

Let A, B, C be subsets of some universal set U. Use Algebra of Sets to establish the following equality:
(c) $(A \cup B) - B = A - (A \cap B)$.

Proof.

$$
\begin{aligned}
\text{LHS} &= (A \cup B) - B \\
&= (A \cup B) \cap B^c && \text{Def of complimentary} \\
&= (A \cap B^c) \cup (B \cap B^c) && \text{Distributive law} \\
&= A - B && \text{Def of complimentary}
\end{aligned}
$$

$$
\begin{aligned}
\text{RHS} &= A - (A \cap B) \\
&= A \cap (A \cap B)^c && \text{Def of complimentary} \\
&= A \cap (A^c \cup B^c) && \text{De Morgan's law} \\
&= (A \cap A^c) \cup (A \cap B^c) && \text{Distributive law} \\
&= A - B && \text{Def of complimentary}
\end{aligned}
$$

□

Exercise (5-3)

Let A, B, C, D be subsets of some universal set U. Are the following statements true or false? Justify your answers.

(a) *If $A \subseteq B$, $C \subseteq D$ and $A \cap C = \emptyset$, then $B \cap D = \emptyset$.*

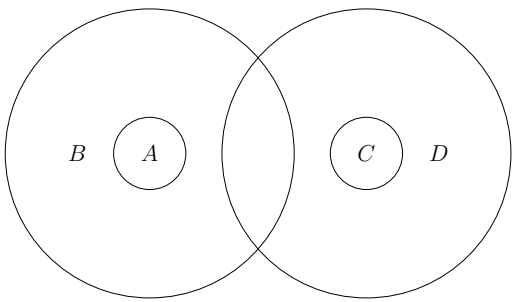
(b) *If $A \subseteq B$, $C \subseteq D$ and $B \cap D = \emptyset$, then $A \cap C = \emptyset$.*

Method

We may apply Venn diagrams for such questions.

Solution.

(a) False. Idea:



Let U be a nonempty set, $A = C = \emptyset$, and $B = D = U$. Then $A \cap C = \emptyset$, but $B \cap D = U \neq \emptyset$.

(b) True.

(1) Assume that there exist $A, B, C, D \subseteq U$, such that $A \subseteq B$, $C \subseteq D$, $B \cap D = \emptyset$, and $A \cap C \neq \emptyset$.
(2) Then let $x \in A \cap C$. So $x \in A$ and $x \in C$.
(3) Since $A \subseteq B$, we have $x \in B$. Since $C \subseteq D$, we have $x \in D$.
(4) So $x \in B \cap D$. This contradict that $B \cap D = \emptyset$.

Exercise (5-4)

Let A and B be subsets of some universal set U.

(a) *Prove that $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$.*

(b) *Give a counterexample to show that it is not necessarily true that $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$.*

Recall

The power set of A is the set of all subsets of A.

Proof and Solution.

(a) Apply element-chasing method:

(1) Let $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Then $X \in \mathcal{P}(A)$ or $X \in \mathcal{P}(B)$.
(2) This means $X \subseteq A$ or $X \subseteq B$. So $X \subseteq A \cup B$.
(3) That is, $X \in \mathcal{P}(A \cup B)$.
(4) This proves $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

(b) Take $U = \{1, 2\}$, $A = \{1\}$ and $B = \{2\}$. So $A \cup B = \{1, 2\}$, $\mathcal{P}(A) = \{\emptyset, A\}$, $\mathcal{P}(B) = \{\emptyset, B\}$, and $\mathcal{P}(A \cup B) = \{\emptyset, A, B, A \cup B\}$. So $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

□

Remark

The equation $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$ holds only when $A \subseteq B$ or $B \subseteq A$.

Exercise (5-5)

Let $A_n = \left\{x \in \mathbb{R} \mid -\frac{1}{n} < x < \frac{1}{n}\right\}$ *for* $n \in \mathbb{N}$. *Show that* $\cap_n A_n = \{0\}$.

Proof.

To show $\cap_n A_n = \{0\}$, we need to prove two parts:

- $\{0\} \subseteq \cap_n A_n$:
  (1) This is the same as showing $0 \in \cap_n A_n$.
  (2) Since $-\frac{1}{n} < 0 < \frac{1}{n}$ for every positive integer n, we have $0 \in A_n$ for every $n \in \mathbb{N}$, and hence $0 \in \cap_n A_n$.
  (3) This proves $\{0\} \subseteq \cap_n A_n$.
- $\{0\} \supseteq \cap_n A_n$:
  (1) It suffices to show that every nonzero number does not belong to $\cap_n A_n$.
  (2) Prove by contradiction: Suppose that there exists a nonzero number $x \in \cap_n A_n$. Then $-\frac{1}{n} < x < \frac{1}{n}$ for every positive integer n.
  (3) So $|x| < \frac{1}{n}$ for every positive integer n. Since $x \neq 0$, we have $\frac{1}{|x|} > n$ for every positive integer n.
  (4) This is impossible: $\left[\frac{1}{|x|}\right] + 1$ is an integer which is greater than $\frac{1}{|x|}$, where $[y]$ denotes the integer part of the real number y.
  (5) Therefore $\{0\} \supseteq \cap_n A_n$.

Combining these two parts, we have $\cup_n A_n = \{0\}$. □

Exercise (5-6(a))

Use Mathematical Induction to prove

(a) *For each positive integer* n, $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$.

Proof.

(1) The universal set is $\mathbb{N}$. Let $P(n) : 1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$.

(2) Base case: Let $n = 1$. LHS $= 1^3 = 1 = \left[\frac{1(1+1)}{2}\right]^2 =$ RHS, so $P(1)$ is true.

(3) Inductive step: For all $k \in \mathbb{N}$, assume that $P(k)$ is true, i.e. $1^3 + 2^3 + \cdots + k^3 = \left[\frac{k(k+1)}{2}\right]^2$ $(*)$. We want to show that $P(k+1)$ is true:

$$\underbrace{1^3 + 2^3 + \cdots + k^3}_{\text{Apply the Equation } (*)} + (k+1)^3 = \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 = (k+1)^2\left[\frac{k^2}{4} + (k+1)\right]$$

$$= (k+1)^2 \frac{k^2 + 4k + 4}{4} = \left[\frac{(k+1)(k+2)}{2}\right]^2$$

(4) Hence by the Principle of Mathematical Induction, we have proven: For each positive integer n, $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$.

□

Exercise (5-6(b))

Use Mathematical Induction to prove

(b) *For each positive integer* n, $\frac{n^3}{3}+\frac{n^2}{2}+\frac{7n}{6}$ *is a positive integer.*

Proof.

(1) The universal set is $\mathbb{N}$. Let $P(n):\ \frac{n^3}{3}+\frac{n^2}{2}+\frac{7n}{6}$ is a positive integer.

(2) Base case: Let $n=1$. $\frac{n^3}{3}+\frac{n^2}{2}+\frac{7n}{6}=2$ is a positive integer, so $P(1)$ is true.

(3) Inductive step: For all $k\in\mathbb{N}$, assume that $P(k)$ is true, i.e. $\frac{k^3}{3}+\frac{k^2}{2}+\frac{7k}{6}$ is a positive integer $(*)$. We want to show $P(k+1)$ is true:

$$\begin{aligned}\frac{(k+1)^3}{3}+\frac{(k+1)^2}{2}+\frac{7(k+1)}{6} &= \frac{k^3+3k^3+3k+1}{3}+\frac{k^2+2k+1}{2}+\frac{7k+7}{6}\\ &= \underbrace{\left[\frac{k^3}{3}+\frac{k^2}{2}+\frac{7k}{6}\right]}_{\text{Apply the Statement }(*)}+(k^2+k+k)+2\end{aligned}$$

is a positive integer.

(4) Hence by the Principle of Mathematical Induction, we have proven: For each positive integer n, $\frac{n^3}{3}+\frac{n^2}{2}+\frac{7n}{6}$ is a positive integer.

□

Exercise (5-6(c))

Use Mathematical Induction to prove
(c) *For each positive integer* n *with* $n \geq 3$, $\left(1+\frac{1}{n}\right)^n < n$.

Proof.

(1) The universal set U is $\{n \in \mathbb{N} \mid n \geq 3\}$. Let $P(n) : \left(1+\frac{1}{n}\right)^n < n$.

(2) Base case: Let $n = 3$. $\left(1+\frac{1}{3}\right)^3 = \frac{64}{27} < 3$, so $P(3)$ is true.

(3) Inductive step: For all $k \in U$, assume that $P(k)$ is true, i.e. $\left(1+\frac{1}{k}\right)^k < k$ $(*)$. We want to show that $P(k+1)$ is true:

$$\left(1+\frac{1}{k+1}\right)^{k+1} < \left(1+\frac{1}{k}\right)^{k+1} = \underbrace{\left(1+\frac{1}{k}\right)^k}_{\text{Apply the Inequality } (*)} \left(1+\frac{1}{k}\right)$$

$$< k\left(1+\frac{1}{k}\right) = k+1$$

(4) Hence by the Principle of Mathematical Induction, we have proven: For each positive integer n with $n \geq 3$, $\left(1+\frac{1}{n}\right)^n < n$.

□

Exercise (5-7(a))

Let $f_1, f_2, \ldots, f_n$ be the Fibonacci sequence. i.e. The sequence is defined recursively by

$$f_1 = 1 \text{ and } f_2 = 1, \quad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 3.$$

(a) *Prove that for each positive integer n, f_{5n} is a multiple of 5.*

Proof.

(1) The universal set is $\mathbb{N}$. Let $P(n) : f_{5n}$ is a multiple of 5.

(2) Base case: Let $n = 1$. $f_5 = f_4 + f_3 = (f_3 + f_2) + (f_2 + f_1) = f_2 + f_1 + 3 = 5$, so $P(1)$ is true.

(3) Inductive step: For all $k \in \mathbb{N}$, assume that $P(k)$ is true, i.e. f_{5k} is a multiple of 5. We want to show that $P(k+1)$ is true:

$$\begin{aligned} f_{5(k+1)} &= f_{5k+4} + f_{5k+3} = (f_{5k+3} + f_{5k+2}) + (f_{5k+2} + f_{5k+1}) \\ &= (f_{5k+2} + f_{5k+1}) + 2(f_{5k+1} + f_{5k}) + f_{5k+1} \\ &= (f_{5k+1} + f_{5k}) + 4f_{5k+1} + 2f_{5k} = 5f_{5k+1} + 3f_{5k} \end{aligned}$$

is a multiple of 5, since f_{5k} is a multiple of 5.

(4) Hence by the Principle of Mathematical Induction, we have proven: For each positive integer n, f_{5n} is a multiple of 5.

□

Exercise (5-7(b))

Let $f_1, f_2, \ldots, f_n$ be the Fibonacci sequence. i.e. The sequence is defined recursively by

$$f_1 = 1 \text{ and } f_2 = 1, \quad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 3.$$

(b) *Prove that for each positive integer n, $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$.*

Proof.

(1) The universal set is $\mathbb{N}$. Let $P(n) : f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$.

(2) Base case: Let $n = 1$. LHS $= f_1 = f_2 =$ RHS, so $P(1)$ is true.

(3) Inductive step: For all $k \in \mathbb{N}$, assume that $P(k)$ is true, i.e. $f_1 + f_3 + \cdots + f_{2k-1} = f_{2k}$ $(*)$. We want to show that $P(k+1)$ is true:

$$\underbrace{f_1 + \cdots + f_{2k-1}}_{\text{Apply the Equation } (*)} + f_{2(k+1)-1} = f_{2k} + f_{2k+1} = f_{2(k+1)}.$$

(4) Hence by the Principle of Mathematical Induction, we have proven: For each positive integer n, $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$.

□

Exercise (5-7(c))

Let $f_1, f_2, \ldots, f_n$ be the Fibonacci sequence. i.e. The sequence is defined recursively by

$$f_1 = 1 \text{ and } f_2 = 1, \quad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 3.$$

(c) *Prove that for each positive integer n such that $n \not\equiv 0 \bmod 3$, f_n is an odd number.*

Proof.

We have the following subquestions:

- For each positive integer n such that $n \equiv 1 \bmod 3$, f_n is an odd number.
  (1) It suffices to show that for all nonnegative integer n, f_{3n+1} is an odd number.
  (2) The universal set U is $\{n \in \mathbb{Z} \mid n \geq 0\}$. Let $P(n) : f_{3n+1}$ is an odd number.
  (3) Base case: Let $n = 0$. Then $f_1 = 1$ which is odd, so $P(0)$ is true.
  (4) Inductive step: For all $k \in U$, assume that $P(k)$ is true, i.e. f_{3k+1} is odd. We want to show that $P(k+1)$ is true:

  $$f_{3(k+1)+1} = f_{3k+4} = f_{3k+3} + f_{3k+2} = f_{3k+2} + f_{3k+1} + f_{3k+2} = 2f_{3k+2} + f_{3k+1}$$

  is odd, since f_{3k+1} is odd.
  (5) Hence by the Principle of Mathematical Induction, we have proven: For each positive integer n such that $n \equiv 1 \bmod 3$, f_n is an odd number.
- For each positive integer n such that $n \equiv 2 \bmod 3$, f_n is an odd number. We will prove it similarly.

Combine these two parts, we have that for each positive integer n such that $n \not\equiv 0 \bmod 3$, f_n is an odd number. □

Fibonacci sequence

- The sequence was studied by Leonardo of Pisa[15], known as Fibonacci, in his "*Liber Abaci*" (1202).
- He considers the growth of an idealised rabbit population, assuming that:
  - a newly-born pair of rabbits, one male, one female, are put in a field;
  - rabbits are able to mate at the age of one month so that at the end of its second month a female can produce another pair of rabbits;
  - rabbits never die and a mating pair always produces one new pair (one male, one female) every month from the second month on.
- The puzzle that Fibonacci posed was: how many pairs will there be in one year?
  - At the end of the 1st month, they mate, but there is still only 1 pair.
  - At the end of the 2nd month the female produces a new pair, so now there are 2 pairs of rabbits in the field.
  - At the end of the 3rd month, the original female produces a second pair, making 3 pairs in all in the field.
  - At the end of the 4th month, the original female has produced yet another new pair, the female born two months ago produces her first pair also, making 5 pairs.
  - At the end of the nth month, the number of pairs of rabbits is equal to the number of new pairs (which is the number of pairs in month $n-2$) plus the number of pairs alive last month. This is the nth Fibonacci number.

[15] Leonardo Pisano Bigollo (c. 1170–c. 1250), an Italian mathematician.

Fibonacci sequence (Cont.)

Actually, we can get the explicit expression of f_n via matrices diagonalization in Linear Algebra:

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Exercise (5-8)

Let p_n be the nth prime number, i.e. $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ etc. Show that $p_n < 2^{2^n}$ for all $n \in \mathbb{N}$.

Proof.

(1) The universal set is $\mathbb{N}$. Let $P(n) : p_n < 2^{2^n}$.

(2) Base case: Let $n = 1$. We have $p_1 = 2 < 4 = 2^{2^1}$. So $P(1)$ is true.

(3) Inductive step: For all $k \in \mathbb{N}$, assume that $P(1), P(2), \ldots, P(k)$ are true. That is, $p_i < 2^{2^i}$ for all $i = 1, 2, \ldots, k$. We want to prove that $P(k+1)$ is true: Let $N = p_1 p_2 \cdots p_k + 1$, then we have

$$\begin{aligned} N = p_1 p_2 \cdots p_k + 1 &< (p_1 + 1)(p_2 + 1) \cdots (p_k + 1) \\ &\leq 2^{2^1} 2^{2^2} \cdots 2^{2^k} = 2^{2^1 + 2^2 + \cdots + 2^k} = 2^{2^{k+1} - 2} < 2^{2^{k+1}}. \end{aligned}$$

- If N is prime then $p_{k+1} \leq N < 2^{2^{k+1}}$.
- If N is not prime then some prime factor p divides N. Then $p \neq p_i$ for $i = 1, 2, \ldots, k$. Otherwise, $p \mid N$ and $p \mid (N - 1)$. This implies $p \mid 1$ which is impossible. So p is a prime bigger than p_k. i.e. $p_{k+1} \leq p < N < 2^{2^{k+1}}$.

(4) Hence by the Strong Principle of Mathematical Induction, we have proven that $p_n < 2^{2^n}$ for all positive integers n.

□

Euclid's Theorem

The idea of considering the number $N = p_1 p_2 \cdots p_k + 1$ comes from the proof of Euclid[16]'s Theorem: There are infinitely many prime numbers.

Proof.
Take any finite list of prime numbers $p_1, p_2, \ldots, p_n$. It will be shown that some additional prime numbers not in this list exist. Let $N = p_1 p_2 \cdots p_n + 1$. Then, N is either prime or not:

- If N is prime then there is at least one more prime than is listed.
- If N is not prime then some prime factor p divides N. This factor p is not on our list: if it were, then it would divide $N - 1$ (since $N - 1$ is the product of every number on the list); but as we know, p divides N. Then p would have to divide the difference of the two numbers, which is $N - (N - 1) = 1$. But no prime number divides 1 so there would be a contradiction, and therefore p cannot be on the list. This means at least one more prime number exists beyond those in the list.

□

[16] Euclid (fl. 300 BC), a Greek mathematician, often referred to as the "Father of Geometry".

Upper bounds on the nth prime

- Bertrand's postulate (actually a theorem) states that if $n > 3$ is an integer, then there always exists at least one prime number p with $n < p < 2n - 2$. This statement was first conjectured in 1845 by Joseph Bertrand[17]. Bertrand himself verified his statement for all numbers in the interval $[2, 3 \times 10^6]$. His conjecture was completely proved by Chebyshev[18] in 1850.
- If we let p_n denote the nth prime, then it is not difficult to show by Bertrand's postulate and mathematical induction that $p_n < 2^n$ for $n \geq 2$.
- There exists at least one prime number between n and $\frac{6}{5}n$ for $n \geq 25$. This theorem was proven by J. Nagura[19] at 1952.
- $p_n \leq n \log n + n(\log \log n - 0.9385)$ for $n \geq 7022$. This theorem was proven by G. Robin[20] at 1983.

---

[17] Joseph Louis Frano is Bertrand (March 11, 1822–April 5, 1900), a French mathematician.

[18] Pafnuty Lvovich Chebyshev (May 16, 1821–December 8, 1894), a Russian mathematician.

[19] Refer to: J. Nagura, On the interval containing at least one prime number, *Proc. Japan Acad.*, **28** (1952) 177–181.

[20] Refer to: G. Robin, Estimation de la fonction de Tschebychef θ sue le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs de n, *Acta Arith.*, **42** (1983) 367–389.

Additional material

Change log

- Page 92: Revise a typo: "$p \in \mathbb{N}$" to "$p \in \mathbb{Z}, p \geq 0$";
- Page 109: Revise a typo: "$p \leq N$" to "$p < N$".

Last modified: 13:20, October 11, 2010.

Schedule of Tutorial 6

- Review concepts: Relations
  - Representation of relation, domain and range of relation;
  - Equivalence relations;
  - Equivalence classes, partitions.
- Tutorial

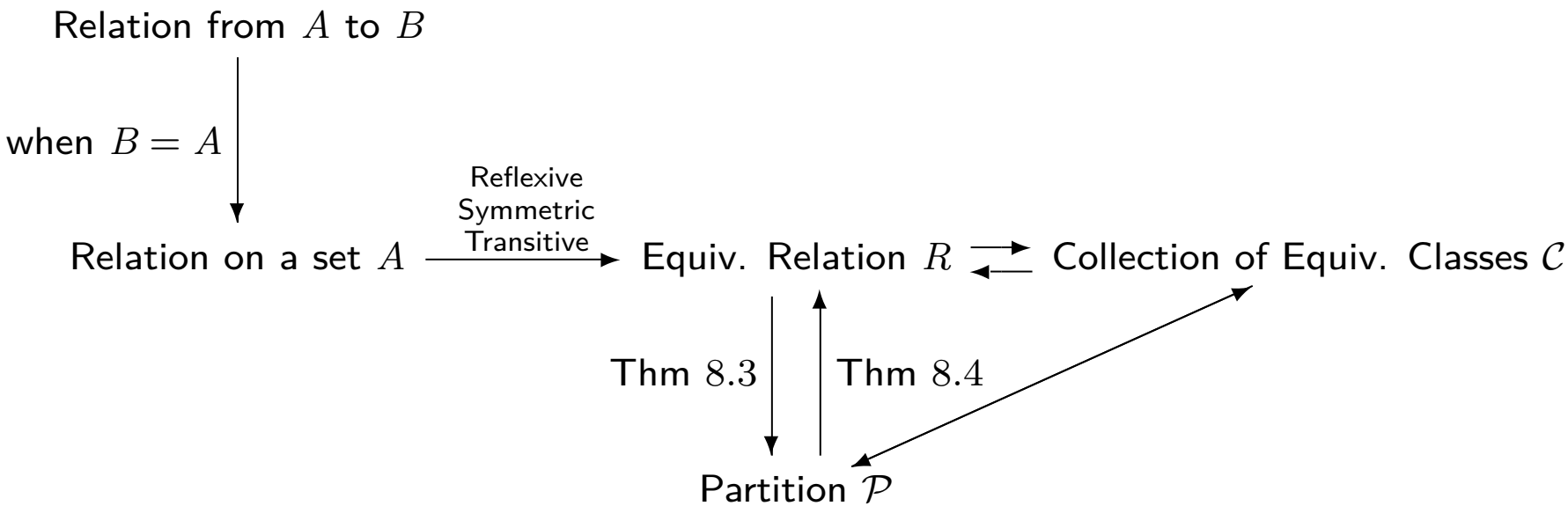
Relations

- Let A, B be sets. A relation R from A to B is a subset of $A \times B$, i.e. $R = \{(a, b) \in A \times B \mid \text{conditions on } a \text{ and } b\}$.
- Let R be a relation from A to B. If $(x, y) \in R$, then x is related to y. Notation: $(x, y) \in R$, $x \sim y$, $x \sim_R y$, xRy.
- Let R be a relation from A to B. The domain of R $(\mathrm{domain}(R))$ is the collection of all the first coordinates of the ordered pairs in R. The range of R $(\mathrm{range}(R))$ is the collection of all the second coordinates of the ordered pairs in R.

Relations (Cont.)

- Let A be a set. A relation R on A is the subset of $A \times A$, i.e. $R = \{(a, a') \in A \times A \mid \text{condition on } a \text{ and } a'\}$.
- Let R be a relation on A:
  - R is reflexive on A if "for every $x \in A$, xRx";
  - R is symmetric on A if "for every $x, y \in A$, if xRy, then yRx";
  - R is transitive on A if "for every $x, y, z \in A$, if xRy and yRz, then xRz".
- Let R be a relation on A. R is an equivalence relation if it is a reflexive, symmetric, transitive relation on A.
- Let R be an equivalence relation on A. For each $n \in A$, let $[n]_R = \{x \in A \mid (x, n) \in R\} = \{x \in A \mid (n, x) \in R\}$. We call this an equivalence class of n determined by the relation R.
- Theorem 8.3: Let R be an equivalence relation on A, then the collection C of all equivalence classes determined by R is a partition of the set A.
- Theorem 8.4: Let $\mathcal{P} = \{A_\alpha \mid \alpha \in I\}$ be a partition of a nonempty set A. Then there exists an equivalence relation R on A such that $\mathcal{P}$ is the set of equivalence classes determined by R.

Relations (Cont.)



Exercise (6-1)

Let $A = \{a, b, c\}$. Consider the following relations on A. Determine whether each relation is reflexive, symmetric or transitive? Justify your answers.

(a) $R_1 = \{(a, a), (a, b), (b, a)\}$

(b) $R_2 = \{(a, b), (b, c), (a, c), (c, b)\}$

(c) $R_3 = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$

Method

Check through the ordered pairs in each R_i.

- For reflexive, check (x, x) for every $x \in A$.
- For symmetric, only need to check the pairs (x, y) and (y, x) for every $x \neq y$.
- For transitive, only need to check the triplets $(x, y), (y, z)$ and (x, z) for every distinct x, y, z.

Remark

The definitions of reflexive, symmetric and transitive are given by some universal statements (refer to notes).

- To show each of these properties holds, we need to give a proof to the respective universal statement.
- To show that each of these properties does not hold, we need to give a counter-example.

Solution.

(a)
- Not reflexive: $(b, b), (c, c) \notin R_1$;
- Symmetric: for every $(x, y) \in R_1$, we have $(y, x) \in R_1$;
- Not transitive: $(b, a), (a, b) \in R_1$, but $(b, b) \notin R_1$.

(b)
- Not reflexive: $(a, a), (b, b), (c, c) \notin R_2$;
- Not symmetric: $(a, b) \in R_2$, but $(b, a) \notin R_2$;
- Not transitive: $(b, c), (c, b) \in R_2$, but $(b, b) \notin R_2$.

(c)
- Reflexive: $(a, a), (b, b), (c, c) \in R_3$;
- Symmetric: for every $(x, y) \in R_3$, we have $(y, x) \in R_3$;
- Transitive: for every $(x, y), (y, z) \in R_3$, we have $(x, z) \in R_3$.

□

Exercise (6-2)

For each of the following relations, determine whether it is an equivalence relation? If not, determine whether it is reflexive, symmetric or transitive. Justify your answers.

(a) *R is the relation on $\mathbb{R}$ given by $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| + |y| = 4\}$.*

(b) *S is the relation on $\mathbb{Z}$ given by $S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid |a - b| \leq 3\}$.*

Solution.

(a)
- Not reflexive: for example, $(0, 0) \notin R$;
- Symmetric: for every $(x, y) \in R$, then $|x| + |y| = 4$. Therefore $|y| + |x| = 4$, and hence $(y, x) \in R$;
- Not transitive: for example, $(4, 0), (0, 4) \in R$, but $(4, 4) \notin R$.

(b)
- Reflexive: for every $x \in \mathbb{Z}$, we have $|x - x| = 0 \leq 3$, hence $(x, x) \in S$;
- Symmetric: for every $(x, y) \in S$, then $|x - y| \leq 3$. Therefore $|y - x| \leq 3$, and hence $(y, x) \in S$;
- Not transitive: for example, $(0, 3), (3, 6) \in S$, but $(0, 6) \notin S$.

□

Exercise (6-3)

Let U be a finite, nonempty set and let $\mathcal{P}(U)$ be the power set of U. Define the relations R on $\mathcal{P}(U)$ as follows:
For $A, B \in \mathcal{P}(U)$, $A \sim B$ if and only if $|A| = |B|$ (i.e. A and B have the same cardinality).

(a) *Show that R is an equivalence relation on $\mathcal{P}(U)$.*

(b) *Describe the equivalence classes of R. (You may describe them using set builder notation or otherwise.)*

Proof and Solution.

(a)
- Reflexive: for every $X \in \mathcal{P}(U)$, since $|X| = |X|$, we have XRX;
- Symmetric: for every pair $(X, Y) \in R$, then $|X| = |Y|$. Therefore $|Y| = |X|$, and hence $(Y, X) \in R$;
- Transitive: for every pairs $(X, Y), (Y, Z) \in R$, then $|X| = |Y|$ and $|Y| = |Z|$. Therefore $|X| = |Z|$, and hence $(X, Z) \in R$.

(b) For every $A \in \mathcal{P}(U)$, we have $[A]_R = \{S \in \mathcal{P}(U) \mid |S| = |A|\}$, that is, $[A]_R$ is the set of all subsets of U that has the same cardinality as A.
Suppose $|U| = n$, then all the distinct equivalence classes of R are:

$$\{\emptyset\}, S_1, S_2, \ldots, S_n,$$

where $S_k = \{A \in \mathcal{P}(U) \mid |A| = k\}$ for $k = 1, 2, \ldots, n$.

□

Exercise (6-4)

Let R be the relation on $\mathbb{R}$ defined by

$$x \sim y \text{ if and only if, either } xy > 0 \text{ or } (x = 0 \text{ and } y = 0).$$

(a) *Show that R is an equivalence relation on $\mathbb{R}$.*

(b) *Determine all the equivalence classes of this equivalence relation.*

Proof and Solution.

(a)
- Reflexive: for every $x \in \mathbb{R}$,
  - if $x = 0$, then xRx by definition of the relation R;
  - if $x \neq 0$, then $x^2 > 0$, and hence xRx.
- Symmetric: for every $(x, y) \in R$, then either $xy > 0$ or $(x = 0$ and $y = 0)$. Therefore either $yx > 0$ or $(y = 0$ and $x = 0)$, and hence $(y, x) \in R$;
- Transitive: for every $(x, y), (y, z) \in R$, then we have the following cases:
  - $xy > 0$ and $yz > 0$: then x, y have the same parity, y, z also have the same parity. Therefore x, z have the same parity, i.e. $xz > 0$ and $(x, z) \in R$;
  - $x = y = z = 0$: then $(x, z) \in R$ by the definition of R.

(b) There are 3 distinct equivalence classes of R:

$$[0]_R = \{0\}, \quad [1]_R = \{x \in \mathbb{R} \mid x > 0\}, \quad [-1]_R = \{x \in \mathbb{R} \mid x < 0\}.$$

Exercise (6-5)

Let A be a non-empty set and R a relation on A.

(a) *Show that if R is reflexive, then $\text{domain}(R) = A = \text{range}(R)$.*

(b) *Is the converse of (a) true? Justify your answer.*

Proof and Solution.

(a)
- To show $\text{domain}(R) = A$, we need $\text{domain}(R) \subseteq A$ (by default) and $A \subseteq \text{domain}(R)$: for every $a \in A$, given the reflexive condition, we have $(a, a) \in R$. This implies $a \in \text{domain}(R)$. By element-chasing, we have proven $A \subseteq \text{domain}(R)$;
- To show $\text{range}(R) = A$, we need $\text{range}(R) \subseteq A$ (by default) and $A \subseteq \text{range}(R)$: for every $a \in A$, given the reflexive condition, we have $(a, a) \in R$. This implies $a \in \text{range}(R)$. By element-chasing, we have proven $A \subseteq \text{range}(R)$;

(b) Converse: If $\text{domain}(R) = A = \text{range}(R)$, then R is reflexive.
It is false, and the counter-example is: take $A = \{1, 2\}$, and $R = \{(1, 2), (2, 1)\}$. Then $\text{domain}(R) = \text{range}(R) = \{1, 2\} = A$, but R is not reflexive since $(1, 1), (2, 2) \notin R$.

□

Exercise (6-6)

A relation R on a set A is a **circular relation** *provided that for all $a, b, c \in A$, if aRb and bRc, then cRa. Prove that:*
A relation R on a set A is an equivalence relation if and only if it is reflexive and circular.

Proof.

There are two directions to prove:

"Only if"
(1) Assume that R is an equivalence relation: it suffices to show that R is circular.
(2) For all $x, y, z \in A$ such that xRy and yRz, then xRz (by transitive condition).
(3) Then zRx (by symmetric condition), therefore R is circular.

"If" Assume that R is reflexive and circular: it suffices to show that R is symmetric and transitive.

- For all $x, y \in A$ such that xRy, since xRx, we have yRx (by circular condition), therefore R is symmetric;
- For all $x, y, z \in A$ such that xRy and yRz, then zRx (by circular condition), then xRz (by symmetric condition), therefore R is transitive.

□

Exercise (6-7)

Construct an equivalence relation R on $\mathbb{N}$ such that for any positive integer k, there is an equivalence class $[a]_R$ for some $a \in \mathbb{N}$ such that $[a]_R$ has exactly k elements.

Solution.

[21] Define

$$\mathcal{C} = \{\{1\}, \{2,3\}, \{4,5,6\}, \{7,8,9,10\}, \dots\},$$

which gives a partition of $\mathbb{N}$.
More rigourously, $\mathcal{C} = \{S_1, S_2, \dots, S_k, \dots\}$, where

$$S_k = \left\{ n \in \mathbb{N} \mid \frac{(k-1)k}{2} + 1 \leq n \leq \frac{k(k+1)}{2} \right\} \text{ for every } k \in \mathbb{N}.$$

Then $|S_k| = k$. We use this partition to construct an equivalence relation R on $\mathbb{N}$ with each element of $\mathcal{C}$ as an equivalence class.
That is, we have $[1]_R = S_1 = \{1\}$, $[2]_R = S_2 = \{2,3\}$, $[4]_R = S_3 = \{4,5,6\}$ and so on. In general, $\left[\frac{(k-1)k}{2} + 1\right]_R = S_k$ for every $k \in \mathbb{N}$. So there is an equivalence class with exactly k elements for every $k \in \mathbb{N}$. □

[21] Refer to "Question 3 in Mid-term 2009–2010(I)".

Change log

- Page 124: Revise typos: “If” to “Only if”, and “Only if” to “If”.

Last modified: 13:20, October 11, 2010.

Schedule of Tutorial 7

- Review concepts:
  - Relations:
    - Congruence modulo n relation, congruence classes modulo n, integers modulo n;
    - Modular arithmetic.
  - Functions:
    - Definitions and notations;
    - Representation of functions;
    - Composition of functions.
- Tutorial
- Additional material:
  - Well-defined;
  - Question 2(b) in Final 2009–2010(I);
  - Question 5 in Final 2008–2009(I);
  - Question 8(a) in Final 2009–2010(I).

Relations: congruence classes, integers modulo n

Let $n \geq 2$ be a positive integer.

- $a \equiv b \bmod n \Leftrightarrow n \mid (a-b) \Leftrightarrow n \mid (b-a) \Leftrightarrow a - b = nk$ for some integer k.
- Congruence modulo n relation:

  $$a \sim b \text{ if and only if } a \equiv b \bmod n$$

  is an equivalence relation on $\mathbb{Z}$.
- For each $a \in \mathbb{Z}$, we have an equivalence class $[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \bmod n\}$. We call $[a]_n$ the congruence class of a modulo n.
- The set of congruence classes modulo n

  $$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

  is called the integers modulo n.
- $|\mathbb{Z}_n| = n$.

Relations: modular arithmetic

Let $n \geq 2$ be a positive integer.

- For all integers a, b, c, and d. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then
  1. $a + c \equiv b + d \bmod n$
  2. $ac \equiv bd \bmod n$
  3. $a + k \equiv b + k \bmod n$ for every $k \in \mathbb{Z}$
  4. $ka \equiv kb \bmod n$ for every $k \in \mathbb{Z}$
  5. $a^m \equiv b^m \bmod n$ for every $m \in \mathbb{N}$
  6. $m^a \equiv m^b \bmod n$ may not hold for some a, b, m, n: $1 \equiv 4 \bmod 3$, but $2^1 = 2 \not\equiv 16 = 2^4 \bmod 3$.
- Arithmetic on $\mathbb{Z}_n$: For $[a]_n, [c]_n \in \mathbb{Z}_n$, define

$$[a]_n + [c]_n = [a + c]_n, \quad [a]_n \cdot [c]_n = [ac]_n.$$

- If $[a]_n = [b]_n$ and $[c]_n = [d]_n$, then
  1. $[a + c]_n = [b + d]_n$
  2. $[ac]_n = [bc]_n$
  3. $[a^m]_n = [b^m]_n$ for every $m \in \mathbb{N}$

Functions: definitions and notations

- A function from a set A to a set B is a rule that associate with every element x of A exactly one element of the set B. A function is also called a mapping. Notation: f: $A \to B$.
- The function f: $A \to B$ is a special type of relation from A to B. In this relation,
  1. every element x of A is associated with exactly one element of the set B;
  2. the domain of this relation is the whole of set A itself.
- If a function f satisfies the following condition, it is called well-defined:

$$\text{If } (a, b), (a, c) \in f, \text{ then } b = c.$$

- Maybe we are confused here since every function must be well-defined by the definition of function. However, there are some situations though when the definition of a function f may make it unclear whether f is well-defined or not. This can often occur when a function is defined on the set of equivalence classes of an equivalence relation.
- In conclusion, when a question ask us to prove that a function f is well-defined, it ask us to prove that this "rule" is well-defined. That is to say, we need to show "if $(a, b), (a, c) \in f$, then $b = c$", while we can not use the fact that every function is always well-defined here.

Functions: definitions and notations (Cont.)

- Let f: $A \to B$ be a function. The set A is called the domain of f, and the set B is called the codomain of f.
- Let f: $A \to B$ be a function. If $a \in A$, then the element of B that is associated with a is denoted $f(a)$. $f(a)$ is called the image of a under f, and a is called a preimage of $f(a)$ under f.
- Let f: $A \to B$ be a function. The set

  $$\text{range}(f) = \{b \in B \mid b \text{ is an image under } f \text{ of some element of } A\} = \{f(x) \mid x \in A\}$$

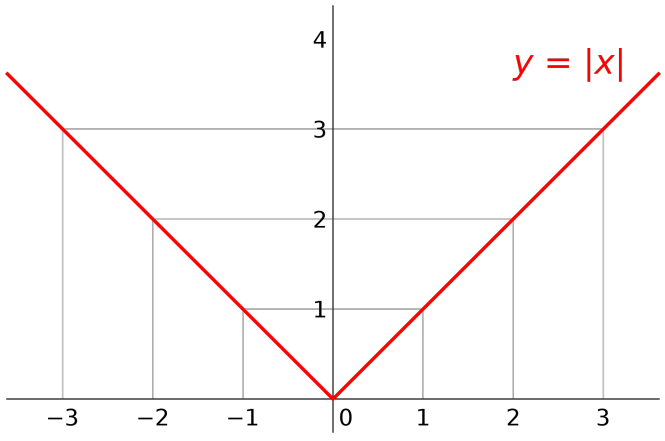
  is the range of f.
- Relation between codomain and range:
  - Codomain: what may possibly come out from the function;
  - Range: what actually comes out from the function;
  - For any function f, the range of f is always a subset of the codomain of f.
- The function f: $A \to B$ can be represented by arrow diagram or graph.

Functions: equality, composition

- Equality of functions: two functions f and g are equal provided
  1. The domain of f equals the domain of g;
  2. The codomain of f equals the codomain of g;
  3. For each x in the domain of f, $f(x) = g(x)$;

  Notation: $f = g$.
- Composition: Let $f : A \to B$ and $g : B \to C$ be functions. The composition of f and g is the function $g \circ f : A \xrightarrow{f} B \xrightarrow{g} C$ defined by $(g \circ f)(x) = g(f(x))$.
  - $f \circ g$ may not be defined if $A \neq C$.
  - $g \circ f$ may not be equal to $f \circ g$.
  - Associated law: $h \circ (g \circ f) = (h \circ g) \circ f$.
  - $f \circ \mathrm{I}_A = f$, $\mathrm{I}_B \circ f = f$.

Functions: examples



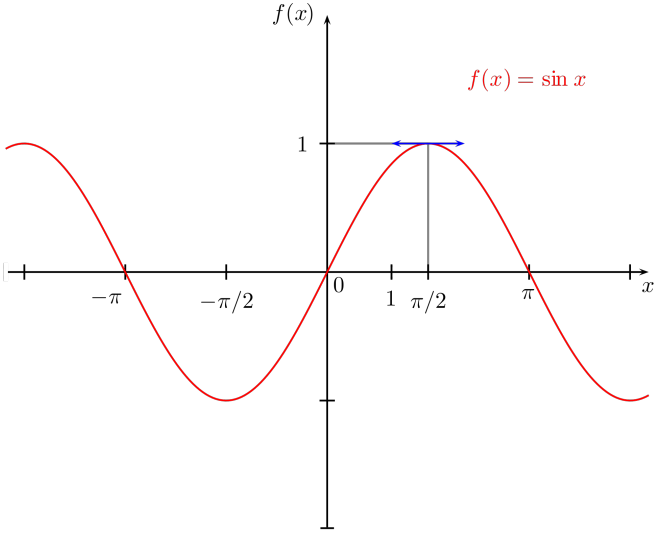


Figure: $|x|$ and $\sin x$.

Functions: examples (Cont.)

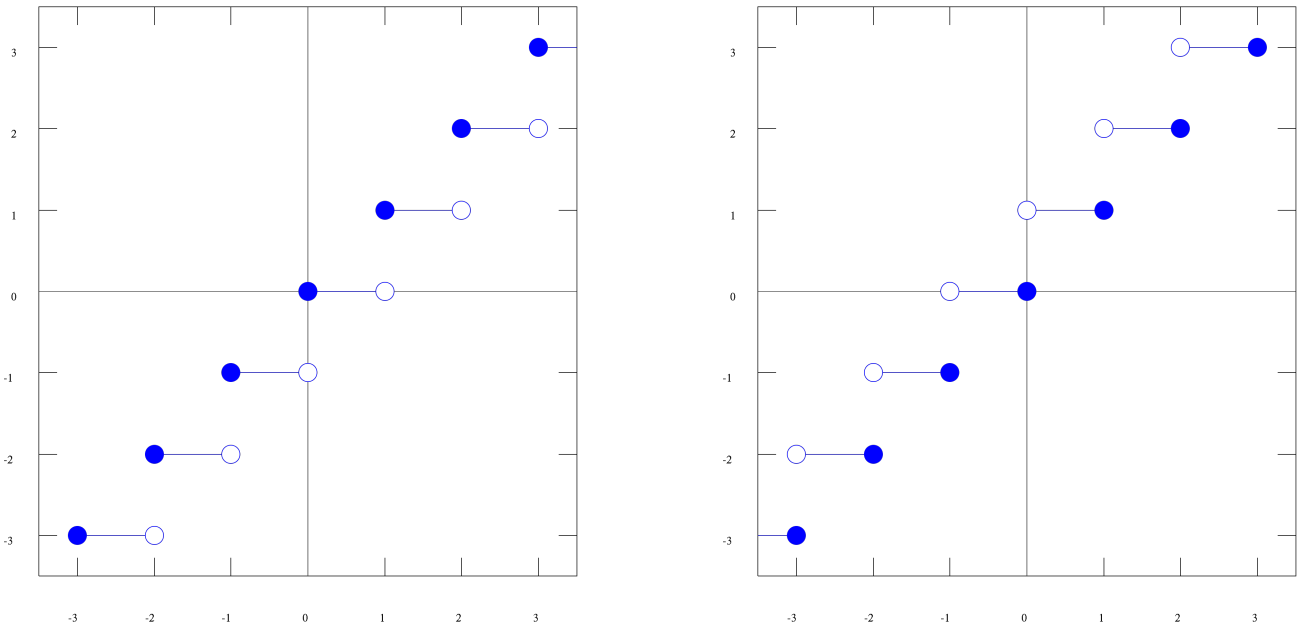


Figure: floor function $\lfloor x \rfloor$, and ceiling function $\lceil x \rceil$.

Since $3 < \pi \doteq 3.14 < 4$, we have

$$\lfloor \pi \rfloor = 3, \quad \lceil \pi \rceil = 4; \qquad \lfloor -\pi \rfloor = -4, \quad \lceil -\pi \rceil = -3.$$

Exercise (7-1)

(a) *Determine the congruence class in* $\mathbb{Z}_5$ *that is equal to* $[4]_5^3 \cdot [2]_5 + [3]_5$.

(b) *Determine the congruence class in* $\mathbb{Z}_6$ *that is equal to* $[4]_6^3 \cdot [2]_6 + [3]_6$.

(c) *Find all congruence classes* $[x]_5$ *in* $\mathbb{Z}_5$ *such that* $[3]_5 \cdot [x]_5 + [2]_5 = [0]_5$.

(d) *Find all congruence classes* $[x]_6$ *in* $\mathbb{Z}_6$ *such that* $[x]_6^2 + ([3]_6 \cdot [x]_6) = [3]_6$.

Recall

$[a]_n + [c]_n = [a + c]_n$, $[a]_n \cdot [c]_n = [ac]_n$.

Remark

Similar question: ▸ Question 2(b) in Final 2009–2010(I).

Solution of (a-b).

(a) $[4]_5^3 \cdot [2]_5 + [3]_5 = [4^3 \times 2 + 3]_5 = [131]_5 = [1]_5$.

(b) $[4]_6^3 \cdot [2]_6 + [3]_6 = [4^3 \times 2 + 3]_6 = [131]_6 = [5]_6$.

□

Solution of (c-d).

(c) It suffices to resolve the Equation

$$[3x+2]_5 = [0]_5.$$

By substituting every element in $\mathbb{Z}_5$ into the Equation, we find the only solution is $[x]_5 = [1]_5$:

$$[3\cdot 0+2]_5 = [2]_5 \neq [0]_5, \quad [3\cdot 1+2]_5 = [0]_5, \quad [3\cdot 2+2]_5 = [8]_5 = [3]_5 \neq [0]_5,$$
$$[3\cdot 3+2]_5 = [11]_5 = [1]_5 \neq [0]_5, \quad [3\cdot 4+2]_5 = [14]_5 = [4]_5 \neq [0]_5.$$

(d) It suffices to resolve the Equation

$$[x^2+3x]_6 = [3]_6.$$

By substituting every element in $\mathbb{Z}_6$ into the Equation, we find the Equation has no solution:

$$[0^2+3\cdot 0]_6 = [0]_6 \neq [3]_6, \qquad [1^2+3\cdot 1]_6 = [4]_6 \neq [3]_6,$$
$$[2^2+3\cdot 2]_6 = [10]_6 = [4]_6 \neq [3]_6, \qquad [3^2+3\cdot 3]_6 = [18]_6 = [0]_6 \neq [3]_6,$$
$$[4^2+3\cdot 4]_6 = [28]_6 = [4]_6 \neq [3]_6, \qquad [5^2+3\cdot 5]_6 = [40]_6 = [4]_6 \neq [3]_6.$$

□

Exercise (7-2)

Let R be the relation on $\mathbb{Z}$ defined by

$$\textit{For } a, b \in \mathbb{Z},\ a \sim b \textit{ if and only if } 2a + 3b \equiv 0 \bmod 5.$$

(a) *Is R an equivalence relation on $\mathbb{Z}$? If not, is it reflexive, symmetric, or transitive? Justify your answers.*

(b) *If R is an equivalence relation, describe its equivalence classes.*

Solution of (a).

- For any $a \in \mathbb{Z}$, since $2a + 3a = 5a$ is divisible by 5, we have $a \sim a$, and hence the relation R is reflexive.
- For any $a, b \in \mathbb{Z}$, if $a \sim b$, we want to check whether $b \sim a$ or not. By definition we have $2a + 3b \equiv 0 \bmod 5$. Then $3a + 2b = (5a + 5b) - (2a + 3b)$ is divisible by 5. That is, $b \sim a$, and hence the relation R is symmetric.
- For any $a, b, c \in \mathbb{Z}$, if $a \sim b$, $b \sim c$, we want to check whether $a \sim c$ or not. By definition we have $5 \mid (2a+3b)$, and $5 \mid (2b+3c)$, then $5 \mid [(2a+3b)+(2b+3c)]$, and hence $5 \mid (2a + 3c)$. That is, $a \sim c$, and hence the relation R is transitive.

Therefore, the relation R is an equivalence relation. □

Solution of (b).

1. First consider $a = 0$, we want to find all integers each of which is related with a. It suffices to resolve the Equation $2 \cdot 0 + 3b \equiv 0 \bmod 5$. Then $3b \equiv 0 \bmod 5$ iff $5 \mid 3b$, and iff $5 \mid b$, since 5 is a prime number. Hence $[0]_R = \{n \in \mathbb{Z} \mid n = 5k, k \in \mathbb{Z}\}$;
2. Then $\mathbb{Z} - [0]_R = \{\ldots, \cancel{0}, 1, 2, 3, 4, \cancel{5}, 6, 7, 8, 9, \ldots\}$. So next consider $a = 1$, we want to find all integers each of which is related with a. It suffices to resolve the Equation $2 \cdot 1 + 3b \equiv 0 \bmod 5$. Then $3(b-1) \equiv 0 \bmod 5$, and if and only if $5 \mid (b-1)$. Hence $[1]_R = \{n \in \mathbb{Z} \mid n = 5k+1, k \in \mathbb{Z}\}$;
3. Then $\mathbb{Z} - [0]_R - [1]_R = \{\ldots, \cancel{0}, \cancel{1}, 2, 3, 4, \cancel{5}, \cancel{6}, 7, 8, 9, \ldots\}$. So next consider $a = 2$. By similar method we obtain $[2]_R = \{n \in \mathbb{Z} \mid n = 5k+2, k \in \mathbb{Z}\}$;
4. Then $\mathbb{Z} - [0]_R - [1]_R - [2]_R = \{\ldots, \cancel{0}, \cancel{1}, \cancel{2}, 3, 4, \cancel{5}, \cancel{6}, \cancel{7}, 8, 9, \ldots\}$. So next consider $a = 3$. By similar method we obtain $[3]_R = \{n \in \mathbb{Z} \mid n = 5k+3, k \in \mathbb{Z}\}$;
5. Then $\mathbb{Z} - [0]_R - [1]_R - [2]_R - [3]_R = \{\ldots, \cancel{0}, \cancel{1}, \cancel{2}, \cancel{3}, 4, \cancel{5}, \cancel{6}, \cancel{7}, \cancel{8}, 9, \ldots\}$. So next consider $a = 4$. By similar method we obtain $[4]_R = \{n \in \mathbb{Z} \mid n = 5k+4, k \in \mathbb{Z}\}$, and $\mathbb{Z} - [0]_R - [1]_R - [2]_R - [3]_R - [4]_R = \{\ldots, \cancel{0}, \cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, \cancel{7}, \cancel{8}, \cancel{9}, \ldots\} = \emptyset$.

Therefore there is no other equivalence class. That is, there are 5 distinct equivalence classes: $[0]_R, [1]_R, [2]_R, [3]_R, [4]_R$. □

Alternative Solution.

We shall prove that, given any $a, b \in \mathbb{Z}$,

$$2a + 3b \equiv 0 \bmod 5 \text{ if and only if } a \equiv b \bmod 5. \tag{4}$$

For any $a, b \in \mathbb{Z}$.

"If" Given $a \equiv b \bmod 5$. Then $2a + 3b \equiv 2a + 3a \equiv 5a \equiv 0 \bmod 5$.

"Only if" Given $2a + 3b \equiv 0 \bmod 5$. We have $2a + 3b + 2b \equiv 2b \bmod 5$, hence $2a \equiv 2b \bmod 5$. Then $6a \equiv 3(2a) \equiv 3(2b) \equiv 6b \bmod 5$, hence $a \equiv b \bmod 5$.

(a) The Claim (4) implies R is the regular congruence modulo 5 relation, and hence is an equivalence relation.

(b) The equivalence class $[a]_R$ is the same as the congruence class $[a]_5$. So the distinct equivalence classes of R are:

$$[0]_R = [0]_5, \quad [1]_R = [1]_5, \quad [2]_R = [2]_5, \quad [3]_R = [3]_5, \quad [4]_R = [4]_5.$$

□

Exercise (7-3)

Let R be the relation on $\mathbb{Z}$ defined by

$$\textit{For } a, b \in \mathbb{Z},\ a \sim b \textit{ if and only if } a^3 \equiv b^3 \bmod 9.$$

(a) *Show that R is an equivalence relation on $\mathbb{Z}$.*

(b) *Determine all the equivalence classes of this equivalence relation.*

Proof of (a).

- For any $a \in \mathbb{Z}$, since $a^3 \equiv a^3 \bmod 9$, we see that $a \sim a$ and R is reflexive.
- For any $a, b \in \mathbb{Z}$, if $a \sim b$, we want to prove $b \sim a$. Since $a \sim b$, then $a^3 \equiv b^3 \bmod 9$, and hence by the symmetric property of congruence, $b^3 \equiv a^3$. So $b \sim a$. This proves that R is symmetric.
- For any $a, b, c \in \mathbb{Z}$, if $a \sim b$, $b \sim c$, we want to prove $a \sim c$. Then $a^3 \equiv b^3 \bmod 9$ and $b^3 \equiv c^3 \bmod 9$. By the transitive property of congruence, we conclude that $a^3 \equiv c^3 \bmod 9$ and hence $a \sim c$. This proves that R is transitive.

By definition, R is an equivalence relation. □

Solution of (b).

Compute the cube of all elements in $\mathbb{Z}_9$:

$$[0]_9^3 = [0]_9, \quad [1]_9^3 = [1]_9, \quad [2]_9^3 = [8]_9,$$
$$[3]_9^3 = [0]_9, \quad [4]_9^3 = [1]_9, \quad [5]_9^3 = [8]_9,$$
$$[6]_9^3 = [0]_9, \quad [7]_9^3 = [1]_9, \quad [8]_9^3 = [8]_9.$$

This means

- $0^3 \equiv 3^3 \equiv 6^3 \bmod 9$, so $0 \sim 3$ and $0 \sim 6$.
- $1^3 \equiv 4^3 \equiv 7^3 \bmod 9$, so $1 \sim 4$ and $1 \sim 7$.
- $2^3 \equiv 5^3 \equiv 8^3 \bmod 9$, so $2 \sim 5$ and $2 \sim 8$.

Thus, the equivalence classes of R are:

$$[0]_R = [0]_9 \cup [3]_9 \cup [6]_9, \quad [1]_R = [1]_9 \cup [4]_9 \cup [7]_9, \quad [2]_R = [2]_9 \cup [5]_9 \cup [8]_9.$$

Exercise (7-4)

(a) *Complete the addition and multiplication tables for* $\mathbb{Z}_8$.

(b) *From the multiplication table, determine all possible congruence classes in* $\mathbb{Z}_8$ *that are squares of some congruence class* $[n]_8$ *in* $\mathbb{Z}_8$.

(c) *Use (b) to prove that, if* $n \equiv 7 \bmod 8$, *then* n *is not a sum of three squares.*

Solution of (a).

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[6]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[7]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[0]$	$[2]$	$[4]$	$[6]$
$[3]$	$[0]$	$[3]$	$[6]$	$[1]$	$[4]$	$[7]$	$[2]$	$[5]$
$[4]$	$[0]$	$[4]$	$[0]$	$[4]$	$[0]$	$[4]$	$[0]$	$[4]$
$[5]$	$[0]$	$[5]$	$[2]$	$[7]$	$[4]$	$[1]$	$[6]$	$[3]$
$[6]$	$[0]$	$[6]$	$[4]$	$[2]$	$[0]$	$[6]$	$[4]$	$[2]$
$[7]$	$[0]$	$[7]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Solution of (b) and Proof of (c).

(b) From the multiplication table, the possible values of the diagonal entries are $[0]_8$, $[1]_8$, $[4]_8$.

(c) Rephrase the statement in terms of congruence classes: if $[n]_8 = [7]_8$, then $[n]_8 \neq [a]_8^2 + [b]_8^2 + [c]_8^2$ for any $[a]_8, [b]_8, [c]_8 \in \mathbb{Z}_8$.

Prove by cases:

$[a]_8^2$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[1]_8$	$[1]_8$	$[1]_8$	$[4]_8$
$[b]_8^2$	$[0]_8$	$[0]_8$	$[0]_8$	$[1]_8$	$[1]_8$	$[4]_8$	$[1]_8$	$[1]_8$	$[4]_8$	$[4]_8$
$[c]_8^2$	$[0]_8$	$[1]_8$	$[4]_8$	$[1]_8$	$[4]_8$	$[4]_8$	$[1]_8$	$[4]_8$	$[4]_8$	$[4]_8$
Sum	$[0]_8$	$[1]_8$	$[4]_8$	$[2]_8$	$[5]_8$	$[0]_8$	$[3]_8$	$[6]_8$	$[1]_8$	$[4]_8$

Hence, we have proved that if $n \equiv 7 \bmod 8$, then n is not a sum of three squares.

□

Remark

Similar question: ▸ Question 5 in Final 2008–2009(I).

Exercise (7-5(a–c))

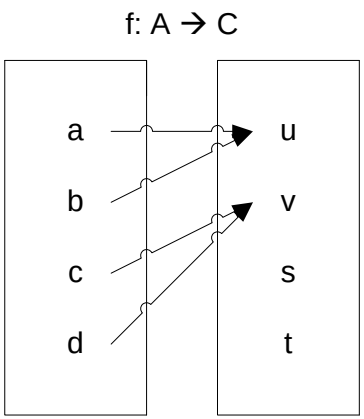
Let $A = \{a, b, c, d\}$, $B = \{a, b, c\}$ and $C = \{s, t, u, v\}$. In each of the following parts, construct a function with the required property if possible. You may draw an arrow diagram to represent your function. Give a brief explanation when it is not possible to construct such a function.

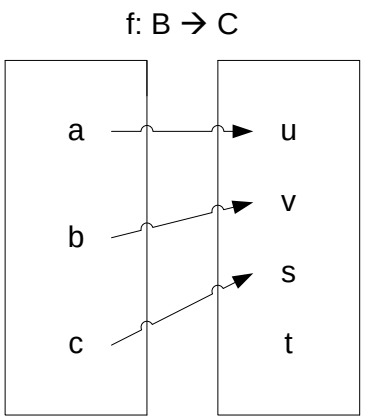
(a) f: $A \to C$ *with* $\text{range}(f) = \{u, v\}$.

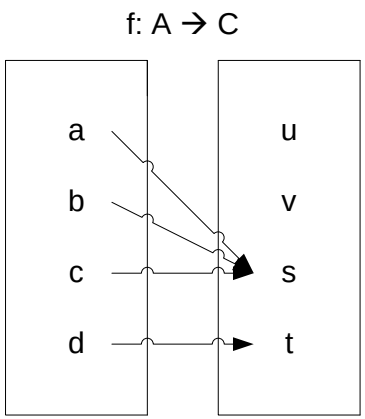
(b) f: $B \to C$ *with* $\text{range}(f) = C$.

(c) f: $A \to C$ *such that the set of preimage of s has cardinality equal to 3.*

Solution.







□

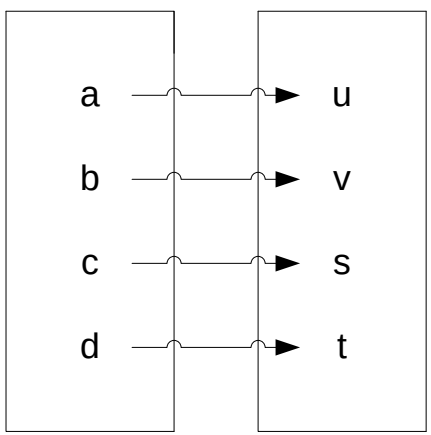
Exercise (7-5(d–e))

Let $A = \{a, b, c, d\}$, $B = \{a, b, c\}$ and $C = \{s, t, u, v\}$. In each of the following parts, construct a function with the required property if possible. You may draw an arrow diagram to represent your function. Give a brief explanation when it is not possible to construct such a function.

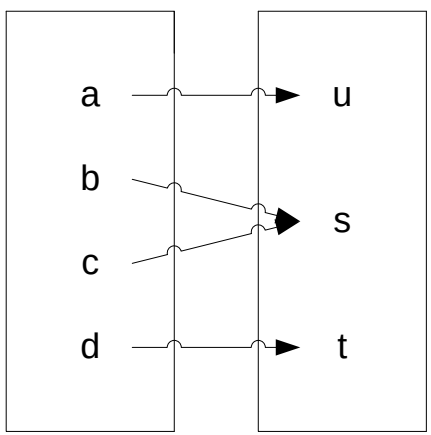
(d) f: $A \to C$ *such that, for all* $x, y \in A$, *if* $x \neq y$, *then* $f(x) \neq f(y)$.

(e) f: $A \to \{s, t, u\}$ *such that, for all* $x, y \in A$, *if* $x \neq y$, *then* $f(x) \neq f(y)$.

f: A → C



f: A → {s,t,u}



Exercise (7-6)

Let $g\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$ *be defined by* $g(m,n)=(2m,m-n)$.

(a) *Calculate* $g(3,5)$ *and* $g(-1,4)$.

(b) *Determine all the preimages of* $(0,0)$. *That is, find all* $(m,n)\in\mathbb{Z}\times\mathbb{Z}$ *such that* $g(m,n)=(0,0)$.

(c) *Determine all the preimages of* $(2,2)$.

(d) *Is the following statement true or false? Justify your answer. For each* $(s,t)\in\mathbb{Z}\times\mathbb{Z}$, *there exists an* $(m,n)\in\mathbb{Z}\times\mathbb{Z}$ *such that* $g(m,n)=(s,t)$.

Solution.

(a) $g(3,5)=(2\times 3,3-5)=(6,-2)$, and $g(-1,4)=(2\times(-1),-1-4)=(-2,-5)$.

(b) Let (m,n) be a preimage of $(0,0)$, then $(2m,m-n)=(0,0)$. Hence $m=n=0$. So $(0,0)$ is the only preimage.

(c) Let (m,n) be a preimage of $(2,2)$, then $(2m,m-n)=(2,2)$. Hence $m=1$, $n=-1$. So $(1,-1)$ is the only preimage.

(d) False. Consider $(2m,m-n)=(1,1)$ which has no integer solution for m and n. So there does not exist an $(m,n)\in\mathbb{Z}\times\mathbb{Z}$ such that $g(m,n)=(1,1)$.

□

Exercise (7-7)

Let $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$. *Define*

$$f\colon \mathbb{Z}_3 \to \mathbb{Z}_3 \text{ by } f([x]_3) = [x]_3^2 + [1]_3, \quad g\colon \mathbb{Z}_3 \to \mathbb{Z}_3 \text{ by } g([x]_3) = [x]_3^4 + [1]_3.$$

(a) *Calculate* $f([0]_3), f([1]_3), f([2]_3)$.

(b) *Calculate* $g([0]_3), g([1]_3), g([2]_3)$.

(c) *Is the function* f *equal to the function* g*?*

Solution.

(a,b)

$$f([0]_3) = [0]_3^2 + [1]_3 = [1]_3, \qquad g([0]_3) = [0]_3^4 + [1]_3 = [1]_3,$$
$$f([1]_3) = [1]_3^2 + [1]_3 = [2]_3, \qquad g([1]_3) = [1]_3^4 + [1]_3 = [2]_3,$$
$$f([2]_3) = [2]_3^2 + [1]_3 = [5]_3 = [2]_3. \qquad g([2]_3) = [2]_3^4 + [1]_3 = [17]_3 = [2]_3.$$

(c) Yes.

- The domain of f equals the domain of g, $\mathbb{Z}_3$.
- The codomain of f equals the codomain of g, $\mathbb{Z}_3$.
- Next from (a) and (b), we have $f([x]_3) = g([x]_3)$ for all $[x]_3 \in \mathbb{Z}_3$.

We conclude that f and g are equal.

Exercise (7-8(a-b))

Find the largest possible subset of $\mathbb{R}$ for the domain of each of the following functions. State the corresponding range of the function.

(a) $k(x) = \sqrt{x-3}$;

(b) $f(x) = 3\sin(2x)$;

Recall

To determine the domains, look for the values in $\mathbb{R}$ such that each function is not defined.

Solution of (a-b).

(a) Since $\sqrt{a}$ is defined only when $a \geq 0$, we have $\text{domain}(k) = \{x \in \mathbb{R} \mid x \geq 3\}$. As we known, every non-negative real number a has a unique non-negative square root, hence $\text{range}(k) = \{y \in \mathbb{R} \mid y \geq 0\}$.

(b) Since the domain of $\sin(x)$ is $\mathbb{R}$, we have $\text{domain}(f) = \mathbb{R}$. Since the range of $\sin(x)$ is $[-1, 1]$, we have $\text{range}(f) = \{y \in \mathbb{R} \mid -3 \leq y \leq 3\} = [-3, 3]$.

□

Exercise (7-8(c))

Find the largest possible subset of $\mathbb{R}$ *for the domain and the corresponding range of the function:* $g(x) = \frac{\lceil x \rceil}{\lfloor x \rfloor}$.

Solution of (c).

A fraction $\frac{a}{b}$ is defined only when $b \neq 0$. Hence

$$\text{domain}(g) = \mathbb{R} - \{x \in \mathbb{R} \mid \lfloor x \rfloor = 0\} = \mathbb{R} - [0, 1).$$

From the graphs of floor function and ceiling function, we obtain:

$$g(x) = \begin{cases} \cdots & \cdots \\ 1, & \text{when } x = -2; \\ \frac{-1}{-2} & \text{when } x \in (-2, -1); \\ 1, & \text{when } x = -1; \\ \frac{0}{-1} & \text{when } x \in (-1, 0); \end{cases} \qquad g(x) = \begin{cases} 1, & \text{when } x = 1; \\ \frac{2}{1} & \text{when } x \in (1, 2); \\ 1, & \text{when } x = 2; \\ \frac{3}{2} & \text{when } x \in (2, 3); \\ \cdots & \cdots \end{cases}$$

Hence we have

$$\begin{aligned} \text{range}(g) &= \left\{\ldots, \frac{-2}{-3}, \frac{-1}{-2}, \frac{0}{-1}, 1\right\} \cup \left\{1, \frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \ldots\right\} \\ &= \left\{y \in \mathbb{Q} \mid y = 1 \text{ or } y = \frac{n+1}{n} \text{ for some } n \in \mathbb{Z} - \{0\}\right\}. \end{aligned}$$

□

Additional material

Well-defined on the page 130.

Exercise (Question 2(b) in Final 2009–2010(I))

List all possible pairs of classes $[a]_{12}$ *and* $[b]_{12}$ *in* $\mathbb{Z}_{12}$ *such that* $[a]_{12} \cdot [b]_{12} = [0]_{12}$.

Solution.

$$[a]_{12} \cdot [b]_{12} = [0]_{12} \Leftrightarrow [ab]_{12} = [0]_{12} \Leftrightarrow 12 \mid (ab).$$

Hence all possible pairs of classes $[a]_{12}$ and $[b]_{12}$ are as follows:

$[a]_{12}$	$[b]_{12}$	$[a]_{12}$	$[b]_{12}$
$[0]_{12}$	every element in $\mathbb{Z}_{12}$	$[1]_{12}$	$[0]_{12}$
$[2]_{12}$	$[0]_{12}$, $[6]_{12}$	$[3]_{12}$	$[0]_{12}$, $[4]_{12}$, $[8]_{12}$
$[4]_{12}$	$[0]_{12}$, $[3]_{12}$, $[6]_{12}$, $[9]_{12}$	$[5]_{12}$	$[0]_{12}$
$[6]_{12}$	$[0]_{12}$, $[2]_{12}$, $[4]_{12}$, $[6]_{12}$, $[8]_{12}$, $[10]_{12}$	$[7]_{12}$	$[0]_{12}$
$[8]_{12}$	$[0]_{12}$, $[3]_{12}$, $[6]_{12}$, $[9]_{12}$	$[9]_{12}$	$[0]_{12}$
$[10]_{12}$	$[0]_{12}$, $[6]_{12}$	$[11]_{12}$	$[0]_{12}$

□

Exercise (Question 5 in Final 2008–2009(I))

(a) *Determine all possible congruence classes in $\mathbb{Z}_7$ that are squares $[n]_7^2$ of some congruence class $[n]_7$ in $\mathbb{Z}_7$.*

(b) *Use part (a) to prove that, for all $n, m \in \mathbb{Z}$, if $n^2 + m^2 \equiv 0 \bmod 7$, then n and m are both divisible by 7.*

(c) *Is it true that, for all $a, b, c \in \mathbb{Z}$, if $a^2 + b^2 + c^2 \equiv 0 \bmod 7$, then a, b, c are all divisible by 7? Justify your answer.*

Solution and Proof.

(a) $[0]_7^2 = [0]_7$, $[1]_7^2 = [1]_7$, $[2]_7^2 = [4]_7$, $[3]_7^2 = [2]_7$, $[4]_7^2 = [2]_7$, $[5]_7^2 = [4]_7$, $[6]_7^2 = [1]_7$. So the possible classes are $[0]_7, [1]_7, [2]_7$ and $[4]_7$.

(b) Let $n, m \in \mathbb{Z}$. If $n^2 + m^2 \equiv 0 \bmod 7$, so $[n]_7^2 + [m]_7^2 = [0]_7$. From part (a), we see that among the square classes, the only pair of $[n]_7^2$, $[m]_7^2$ that give a sum of $[0]_7$ is $[n]_7^2 = [0]_7$ and $[m]_7^2 = [0]_7$. This in turn means $[n]_7 = [0]_7$ and $[m]_7 = [0]_7$, which implies $7 \mid n$ and $7 \mid m$.

(c) False. From (a), we can find integers a, b, c such that

$$[a]_7^2 = [1]_7, [b]_7^2 = [2]_7, [c]_7^2 = [4]_7, \text{ and } [a]_7^2 + [b]_7^2 + [c]_7^2 = [0]_7.$$

That is, $7 \nmid a, b, c$ but $a^2 + b^2 + c^2 \equiv 0 \bmod 7$.

Exercise (Question 8(a) in Final 2009–2010(I))

Is it possible to find a partition C of $\mathbb{N}$ such that C is infinite and S is infinite for every $S \in C$? Justify your answer.

Change log

Last modified: 12:00, October 18, 2010.

Schedule of Tutorial 8

- Review concepts: Functions:
  - Injection, surjection;
  - Bijection, inverse functions.
- Tutorial
- Additional material:
  - Question 10 in Final 2007–2008(I);
  - Question 7 in Final 2008–2009(I).

Functions: injection

Let f: $A \to B$ be an injective function (or an injection, a one-to-one function).

- Original definition: $\forall x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.
- Working definition: $\forall x, y \in A$, if $f(x) = f(y)$, then $x = y$.
- For real functions ($A = B = \mathbb{R}$), we may apply "visualization":
  1. Plot the graph of the real function;
  2. Check whether every horizontal line intersects with the graph at most one point or not;
  3. If yes, this function is injective; otherwise, it is not.
- In additional, if A and B are finite sets, then $|A| \leq |B|$.
- Negation: $\exists x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

Functions: surjection

Let f: $A \to B$ be a surjective function (or a surjection, a onto function).

- Original definition: $\forall y \in B$, $\exists x \in A$ such that $y = f(x)$.
- Alternative definition: $\text{range}(f) = \text{codomain}(f)$. (In general, we only have $\text{range}(f) \subseteq \text{codomain}(f)$.)
- For real functions ($A = B = \mathbb{R}$), we may apply "visualization":
  1. Plot the graph of the real function and project the graph onto the y-axis;
  2. Check whether the projection is the whole of y-axis or not;
  3. If yes, this function is surjective; otherwise, it is not.
- In additional, if A and B are finite sets, then $|A| \geq |B|$.
- Negation: $\exists y \in B$ such that $\forall x \in A$, $y \neq f(x)$. Or $\text{range}(f) \neq \text{codomain}(f)$.

Functions: some results of injections and surjections

Let f: $A \to B$, g: $B \to C$ be two functions.

- If f and g are injective, then $g \circ f$ is injective.
- If f and g are surjective, then $g \circ f$ is surjective.
- If f and g are bijective, then $g \circ f$ is bijective.
- If $g \circ f$ is injective, then f is injective, and g may be not.
- If $g \circ f$ is surjective, then g is surjective, and f may be not.

Functions: bijection and inverse functions

- $f\colon A \to B$ is bijective, if f is both an injective and surjective function.
- Let $f\colon A \to B$ be a bijection. For $a \in A$ and $b \in B$, we define the inverse function by $f^{-1}(b) = a$ if $f(a) = b$. (bijection $\Rightarrow$ inverse functions)
- If the inverse function of f exists, then f is a bijection. (inverse functions $\Rightarrow$ bijection)
- If $f\colon A \to B$ is a bijection, then $f^{-1} \circ f = \mathrm{I}_A$ and $f \circ f^{-1} = \mathrm{I}_B$.
- If $f\colon A \to B$ and $g\colon B \to C$ are bijections, then $(g \circ f)^{-1} = (f^{-1}) \circ (g^{-1})$.

Exercise (8-1)

Show that the function below is an injection but not a surjection.

$$g\colon [0,1] \to (0,1) \text{ by } g(x) = \begin{cases} 0.8, & \text{if } x = 0 \\ 0.5x, & \text{if } 0 < x < 1 \\ 0.6, & \text{if } x = 1 \end{cases}$$

Method

Draw graph:

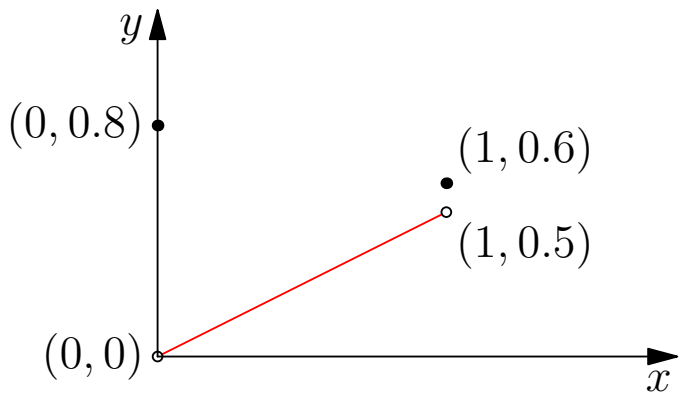


Figure: Graph of the function g.

Proof.

- To prove the function g is an injection, let $a, b \in [0, 1]$ and assume that $g(a) = g(b)$, we want to show $a = b$. Since g is a function by cases, we need consider the following three cases:
  - If $a = 0$, then $g(a) = 0.8$. If $b \neq 0$, which is not possible since $g(b) = g(a) = 0.8$. Therefore, $b = 0$ and hence, $a = b$.
  - If $a = 1$, then $g(a) = 0.6$. If $b \neq 1$, which is not possible since $g(b) = g(a) = 0.6$. Therefore, $b = 1$ and hence, $a = b$.
  - If $0 < a < 1$, then $0 < g(a) < 0.5$. Since $g(0) = 0.8$ and $g(1) = 0.6$, in order for $g(b)$ to equal $g(a)$, we must have $0 < b < 1$. Hence, $0.5a = 0.5b$ and hence, $a = b$.

  Therefore, g is an injection.
- To prove the function g is not a surjection: The function g is not a surjection since the range of g is $(0, 0.5) \cup \{0.6, 0.8\}$, which does not equal to $(0, 1)$, the codomain of g.

□

Exercise (8-2)

Let $A = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n \neq 0\}$. *Define* f: $A \to \mathbb{Q}$ *as follows: For each* $(m, n) \in A$, $f(m, n) = \frac{m+n}{n}$.
(i) Is f *an injection? (ii) Is* f *a surjection? Justify your answers.*

Solution.

(i)
1. Recall that there are many different fractions that represent the same rational number.
2. For example, 1 can be represented by $\frac{1}{1}$ and $\frac{2}{2}$, which are the images of $(0, 1)$ and $(0, 2)$, respectively.
3. Therefore, f is not an injection.

(ii)
1. We need to check whether it is possible to express every rational number in the form $\frac{m+n}{n}$.
2. Let x ba a rational number, then it can be rewritten as $\frac{a}{b}$, where $b \neq 0$. Then we need to check whether there exists $(m, n) \in A$ such that $f(m, n) = \frac{a}{b}$.
3. By observing, the equation $\frac{m+n}{n} = \frac{a}{b}$ has solution: $n = b$ and $m = a - b$.
4. This proves f is a surjection.

□

Exercise (8-3)

Let $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be a function. Is it possible that f is a surjection? Justify your answer.

Solution.

Yes.

1. In lecture, we have seen an example of injection $g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. By ordering all the integer ordered pairs on the Cartesian plane in an anticlockwise "spiralling" direction starting from the origin, we define the function g by

$$g(0,0) = 0,\ g(1,0) = 1,\ g(1,1) = 2,\ g(0,1) = 3,\ g(-1,1) = 4,$$
$$g(-1,0) = 5,\ g(-1,-1) = 6,\ g(0,-1) = 7,\ g(1,-1) = 8,\ \ldots.$$

   The range of g is $\mathbb{Z}^* = \{n \in \mathbb{Z} \mid n \geq 0\}$.
2. We have a bijection: $g' : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}^*$, where $g'(m,n) = g(m,n)$ when $m, n \in \mathbb{Z}$.
3. Then $(g')^{-1} : \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{Z}$ exists, denoted as f'.
4. Then we can extend $f' : \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{Z}$ to $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ in the following way:
   - For all non-negative integers n, we define $f(n) = f'(n)$.
   - For all negative integers $-n$, we define $f(-n) = (0,0)$.

We have a function f whose range is the whole of $\mathbb{Z} \times \mathbb{Z}$. i.e. f is a surjection. □

Alternative Solution.

Similar with the method in the lecture, by ordering all the integer ordered pairs on the Cartesian plane in an anticlockwise "spiralling" direction starting from the origin, we define the function f by

$$f(0,0)=0,\ f(1,0)=1,\ f(1,1)=-1,\ f(0,1)=2,\ f(-1,1)=-2,$$
$$f(-1,0)=3,\ f(-1,-1)=-3,\ f(0,-1)=4,\ f(1,-1)=-4,\ \ldots.$$

It is easy to see that $f\colon \mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$ is bijective. □

Remark

Actually, there is a nonconstructive proof for the existence of the bijection from $\mathbb{Z}\times\mathbb{Z}$ to $\mathbb{Z}$, using some results of "Cardinality".

Exercise (8-4)

The following functions are not bijections. In each case, replace the domain or codomain of the function by suitable subsets if necessary to make it a bijection.

(a) $f\colon \mathbb{R} \to \mathbb{R}$ *defined by* $f(x) = e^{-x^2}$.

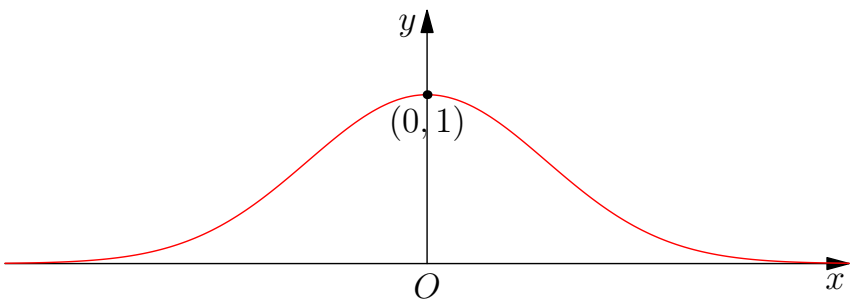
(b) $f\colon \mathbb{R} \to \mathbb{R}$ *defined by* $f(x) = \sin(x)$.

(c) $f\colon \mathbb{R} \to \mathbb{R}$ *defined by* $f(x) = |x - 1|$.

(d) $f\colon \mathbb{Z} \to \mathbb{Z}$ *defined by* $f(x) = 2x + 1$.

Solution of (a).

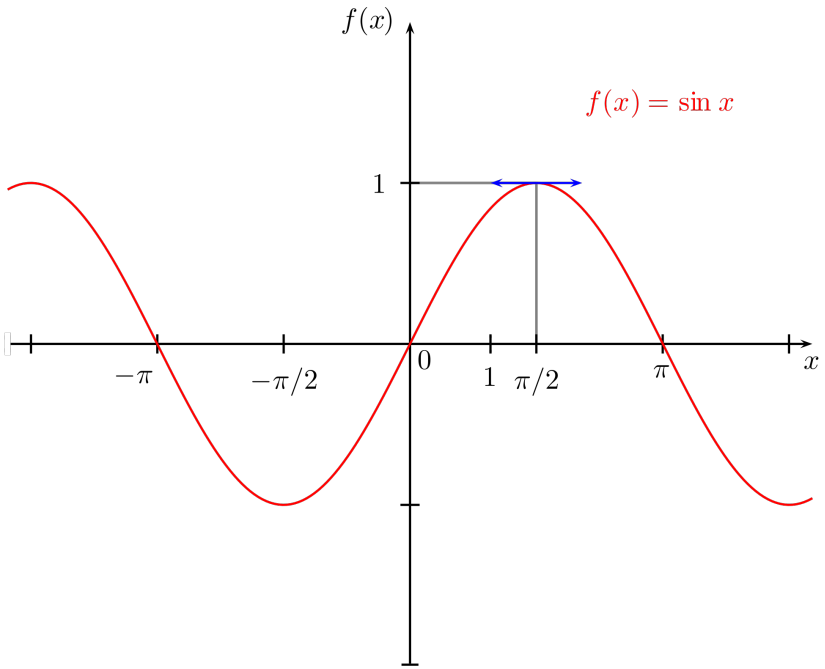
From the graph of $f(x) = e^{-x^2}$, we will see that f is not injective or surjective.



The graph of f is symmetric with respect to the y-axis, so the modified domain can not contain both x and $-x$ for every $x \in \mathbb{R}$. Then we may take the modified domain to be $[0, +\infty)$. From the graph, the range of f is $(0, 1]$, so we may take the modified codomain as $(0, 1]$. □

Solution of (b).

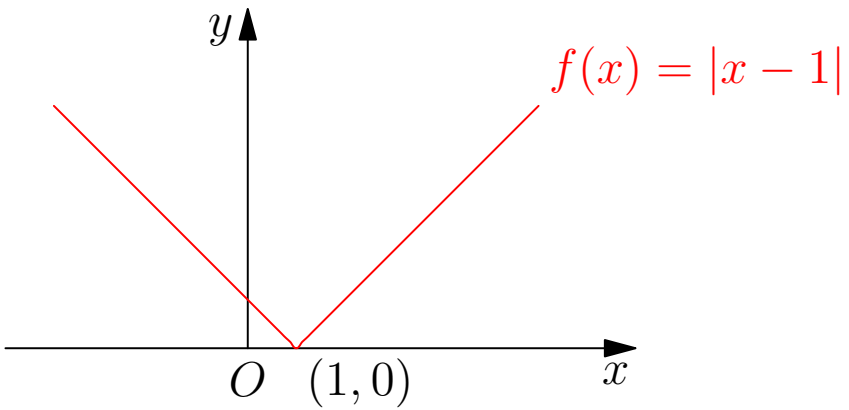
From the graph of $f(x) = \sin(x)$, we will see that f is not injective or surjective.



f is a periodic function with period 2π, so we may take the modified domain as $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ (half period). From the graph, the range of f is $[-1, 1]$, so we may take the modified codomain as $[-1, 1]$. □

Solution of (c).

From the graph of $f(x) = |x-1|$, we will see that f is not injective or surjective.



The graph of f is symmetric with respect to the line $x = 1$, so we may take right region of the point $(1,0)$: $[1,+\infty)$. From the graph, the range of f is $[0,\infty)$, so we may take the modified codomain as $[0,+\infty)$. □

Solution of (d).

1. For the function $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2x + 1$, note that the domain and codomain are $\mathbb{Z}$, we may not apply "visualization".
2. This function is injective but not surjective:
3. For any $x, y \in \mathbb{Z}$, if $f(x) = f(y)$, then $2x + 1 = 2y + 1$. Hence $x = y$. Therefore, f is injective, and hence we do not need modify the domain.
4. The range of f is the set of all odd integers. Hence we may take the modified codomain as the set of all odd integers.

□

Exercise (8-5)

(a) *Define* $f\colon \mathbb{R} \to \mathbb{R}$ *by* $f(x) = x^2 - 4$ *for all* $x \in \mathbb{R}$. *Explain why* f^{-1} *is not defined.*

(b) *Let* $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$ *and let* $T = \{y \in \mathbb{R} \mid y \geq -4\}$. *Define* $F\colon \mathbb{R}^* \to T$ *by* $F(x) = x^2 - 4$ *for all* $x \in \mathbb{R}^*$. *Explain why* F^{-1} *is defined and determine a formula for* $F^{-1}(y)$.

Method

To show the inverse exists is equivalent to show the function is bijection.

Solution.

(a) Since $f(-2) = 0 = f(2)$, we have that f is not an injection. So the inverse of f is not defined.

(b)
- We first prove that F is an injection. Let $a, b \in \mathbb{R}^*$ and assume that $F(a) = F(b)$. Then $a^2 - 4 = b^2 - 4$, which implies that $a^2 = b^2$. Since both a and b are nonnegative, we can take the square root of both sides of this equation to prove that $a = b$. Therefore, F is an injection.
- Now we prove that F is a surjection. Let $y \in T$. Then $y \in \mathbb{R}$ and $y \geq -4$. We can then conclude that $y + 4 \geq 0$ and hence, $\sqrt{y+4} \in \mathbb{R}^*$. So if $x = \sqrt{y+4}$, then $F(x) = x^2 - 4 = (y + 4) - 4 = y$. This shows that F is a surjection.
- Since F is a bijection, hence the inverse of F is a function. From the discussion above, we have for each $y \in T$, $x = \sqrt{y+4}$. Hence the formula for F^{-1} is given by $F^{-1}(y) = \sqrt{y+4}$.

Exercise (8-6)

(a) *Define* $g\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ *by* $g([x]_5) = [x]_5^3 + [4]_5$ *for all* $[x]_5 \in \mathbb{Z}_5$. *Explain why* g^{-1} *is defined.*

(b) *Use the fact that* $[x]_5^5 = [x]_5$ *for all* $[x]_5 \in \mathbb{Z}_5$ *to determine a formula for the inverse* g^{-1} *for* g *in part (a) in the form of* $g^{-1}(x) = [x+n]_5^k$ *for some* $k, n \in \mathbb{Z}^+$.

Solution.

(a) We check directly:

$$g([0]_4) = [4]_5,\ g([1]_5) = [0]_5,\ g([2]_5) = [2]_5,\ g([3]_5) = [1]_5,\ g([4]_5) = [3]_5.$$

So g is a bijection. Hence the inverse of g is defined.

(b) Let $[y]_5 = [x]_5^3 + [4]_5$. We want to solve $[x]_5$ in terms of $[y]_5$. At first, we have $[y+1]_5 = [x]_5^3$. Now, we need reduce the power 3 of $[x]_5$ to 1. We will use the result

$$[x]_5^5 = [x]_5 \text{ for all } [x]_5 \in \mathbb{Z}_5$$

twice in the following:

$$([y-4]_5)^3 = ([x]_5^3)^3 = [x]_5^4 \cdot [x]_5^5 = [x]_5^4 \cdot [x]_5 = [x]_5^5 = [x]_5.$$

Hence we get a formula $g^{-1}([y]_5) = [y-4]_5^3 = [y+1]_5^3$.

□

Exercise (8-7)

Let A, B and C be nonempty sets and let $f\colon A \to B$ and $g\colon B \to C$.

(a) *Prove: If $g \circ f\colon A \to C$ is a surjection, then g is a surjection.*

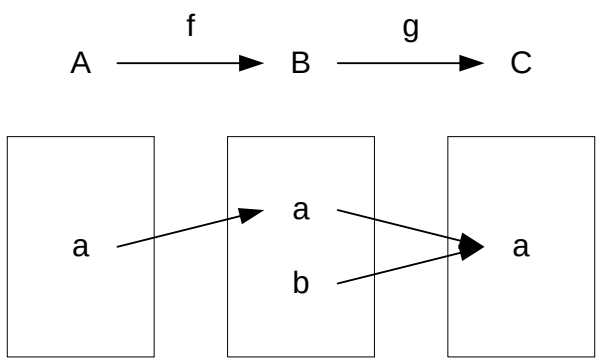
(b) *Disprove: If $g \circ f\colon A \to C$ is a surjection, then f is a surjection.*

Proof and solution.

(a)
1. To prove that g is a surjection, for any $z \in C$, we want to find $y \in B$, such that $g(y) = z$.
2. Now, since $g \circ f\colon A \to C$ is a surjection, there exists an $x \in A$ such that $g(f(x)) = (g \circ f)(x) = z$.
3. Take $y = f(x) \in B$, and this y satisfies the requirement.

We have proven that there exists an element $y \in B$ such that $g(y) = z$. Therefore, g is a surjection.

(b) From the following graph, we have a counterexample:



Exercise (8-8(a,b))

For each of the following, give examples of functions f: $A \to B$ and g: $B \to C$ that satisfy the stated conditions, or explain why no such examples exist.

(a) *f is an injection but $g \circ f$ is not an injection.*

(b) *f is not an injection but $g \circ f$ is a injection.*

Solution of (a,b).

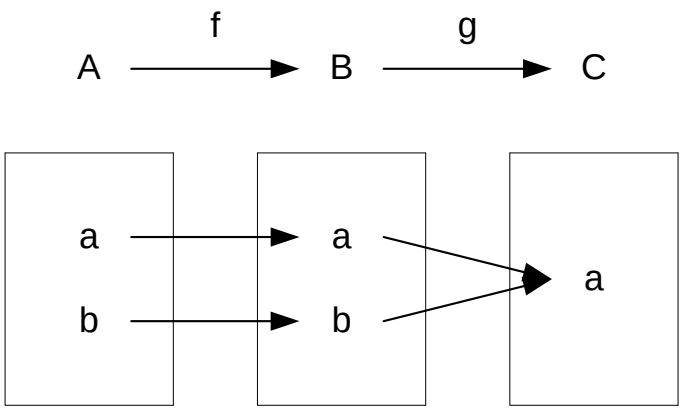


Figure: Example for (a).

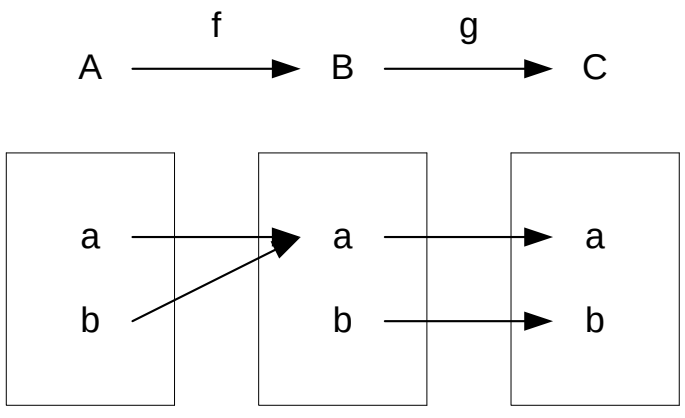


Figure: Counter-example for (b).

Statement in (b) is not possible. We have proven that if $g \circ f$ is a injection, then f has to be an injection. □

Exercise (8-8(c,d))

For each of the following, give examples of functions f: $A \to B$ and g: $B \to C$ that satisfy the stated conditions, or explain why no such examples exist.

(c) *g is an injection but $g \circ f$ is not an injection.*

(d) *g is not an injection but $g \circ f$ is an injection.*

Solution of (c,d).

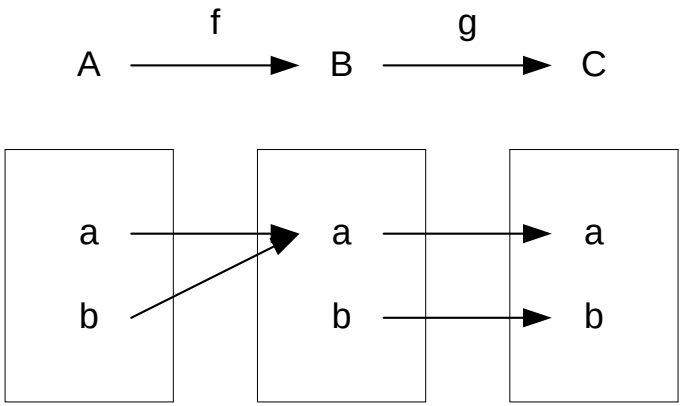


Figure: Example for (c)

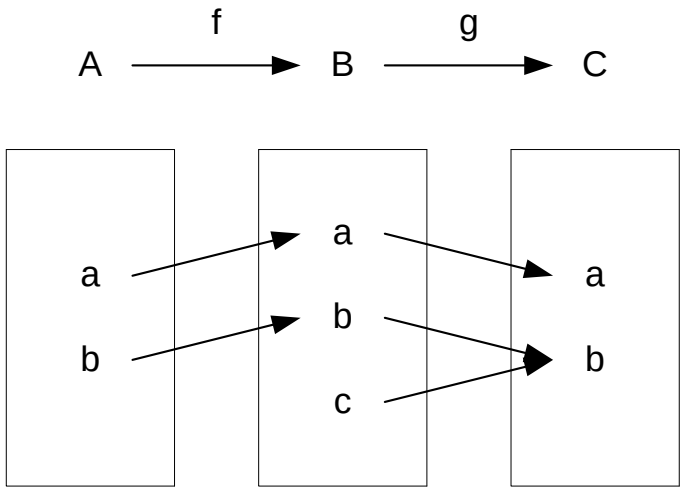


Figure: Example for (d)

Additional material

Exercise (Question 10 in Final 2007–2008(I))

(i) *Let $f\colon S \to T$ be a function such that $f^{-1}(f(A)) = A$ for all subsets A of S. Prove that f is an injection.*

(ii) *Let $g\colon S \to T$ be a surjection and P a partition of T. Show that the collection $\{g^{-1}(C) \mid C \in P\}$ is a partition of S.*

Proof.

(i) For any $a, b \in S$, if $f(a) = f(b)$. Then we have

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

Hence $a = b$. Therefore f is an injection.

(ii) Apply the definition of partition.

□

Additional material

Exercise (Question 7 in Final 2008–2009(I))

Let A and B be two non-empty subsets of some universal set U. Let $f\colon A \to A$ and $g\colon B \to B$ be two functions such that $f(x) = g(x)$ for all $x \in A \cap B$.
Define the function $h\colon (A \cup B) \to (A \cup B)$ by $h(a) = f(a)$ for all $a \in A$ and $h(b) = g(b)$ for all $b \in B$.

(a) *Suppose f and g are surjections. Is it necessary that h is a surjection?*

(b) *Suppose f and g are injections. Is it necessary that h is a injection?*

Solution.

(a)
1. For all $x \in A \cup B$, we have $x \in A$ or $x \in B$.
2. If $x \in A$, then there exists $a \in A$, such that $f(a) = x$ which implies that $h(a) = x$.
3. If $x \in B$, then there exists $b \in B$, such that $g(b) = x$ which implies that $h(b) = x$.
4. Hence, for all $x \in A \cup B$, there exists $c \in A \cup B$, such that $h(c) = x$.

(b) h is not necessarily injective: let

$$A = \{0, 1, 2, 3, \ldots\}, \qquad f(n) = n + 1 \text{ for all } n \in A;$$
$$B = \{-1, 1, 2, 3, \ldots\}, \qquad g(n) = n + 1 \text{ for all } n \in \mathbb{N},\ g(-1) = 1.$$

Then f and g are injective, but h is not since $h(0) = h(-1) = 1$.

Change log

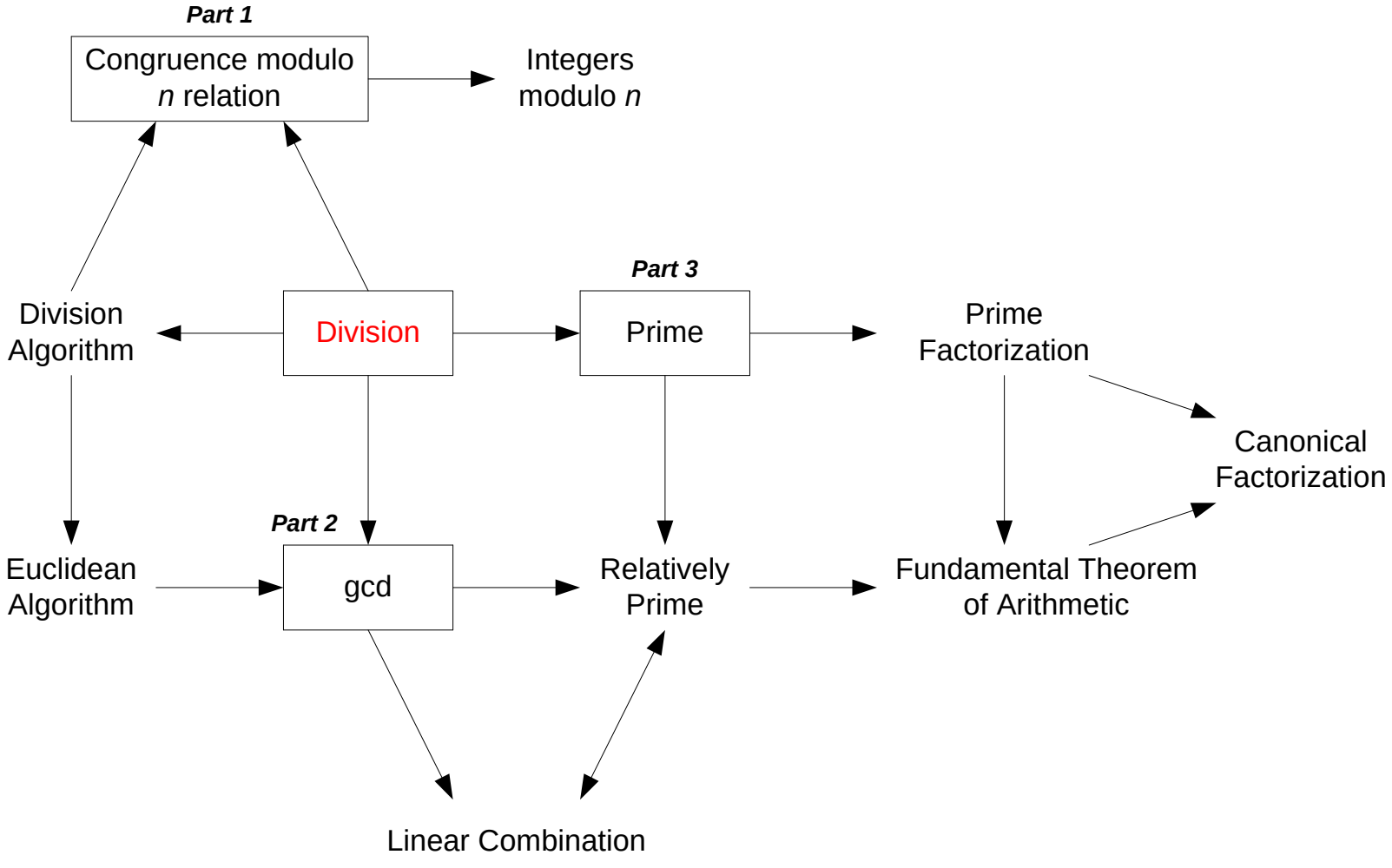
- Page 162: Revise the solution;
- Page 163: Add an alternative solution.

Last modified: 12:00, October 25, 2010.

Schedule of Tutorial 9

- Review concepts: Number Theory:
  - Common divisor, greatest common divisor;
  - Division Algorithm, Euclidean Algorithm;
  - Prime, composite number, Euclid's Theorem;
  - Relatively prime, Euclid's Lemma;
  - Prime factorization, Fundamental Theorem of Arithmetic, canonical factorization;
  - Perfect square.
- Tutorial
- Question 8(b) in Final 2008–2009(I);

Number Theory: Summary



Number Theory: Greatest Common Divisor

- Let a, b be integers and d a nonzero integer. d is a common divisor of a and b if $d \mid a$ and $d \mid b$. Notice: 0 can not be a common divisor of any a and b.
- Original definition: Let a, b be integers, not both 0. The largest integer that divides both a and b is called the greatest common divisor of a and b. Notation: $\gcd(a, b)$. Notice: $\gcd(0, 0)$ is not defined.
- Working definition: Let a, b be integers, not both 0, and $d \in \mathbb{N}$.

$$d = \gcd(a, b) \Leftrightarrow \begin{cases} d \mid a \text{ and } d \mid b; \\ \text{for all } k \in \mathbb{N}, \text{ if } k \mid a, k \mid b, \text{ then } k \leq d. \end{cases}$$

- Theorem 11.8: Let a, b be integers, not both 0, and $d \in \mathbb{N}$.

$$d = \gcd(a, b) \Leftrightarrow \begin{cases} d \mid a \text{ and } d \mid b; \\ \text{for all } k \in \mathbb{N}, \text{ if } k \mid a, k \mid b, \text{ then } k \mid d. \end{cases}$$

- An integer n is called a linear combination of a and b if n can be written in the form $ax + by$ by some integers x and y.
- Theorem 11.7: Let a, b be integers, not both 0, then $\gcd(a, b)$ is the smallest positive linear combination of a and b. Therefore, $\gcd(a, b) = ax + by$ for some integers x and y.

Number Theory: Greatest Common Divisor (Cont.)

Basic propositions:

- $0 \neq a \in \mathbb{Z}$, $\gcd(a, 0) = |a|$, $\gcd(a, a) = |a|$, $\gcd(a, an) = |a|$ for all $n \in \mathbb{Z}$.
- $\gcd(a, b) > 0$.
- $\gcd(a, b) = \gcd(b, a)$.
- $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.
- $\gcd(a, b) = \gcd(a, b + an)$ for all $n \in \mathbb{Z}$.
- p is a prime, $\gcd(p, a) = \begin{cases} p, & \text{if } p \mid a; \\ 1, & \text{if } p \nmid a. \end{cases}$
- If $0 < c \mid \gcd(a, b)$, then $\gcd(\frac{a}{c}, \frac{b}{c}) = \frac{\gcd(a,b)}{c}$. Specially, we have $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$.
- $\gcd(ca, cb) = c \gcd(a, b)$ if $c \in \mathbb{N}$.

Number Theory: Greatest Common Divisor (Cont.)

Theorems:

- - Theorem 11.7: $\gcd(a, b)$ is the smallest positive linear combination of a and b.
  - If $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.
- Theorem 11.8: $d = \gcd(a, b) \Leftrightarrow \begin{cases} d \mid a \text{ and } d \mid b; \\ \text{for all } k \in \mathbb{N}, \text{ if } k \mid a, k \mid b, \text{ then } k \mid d. \end{cases}$
- - If $\gcd(a, b) = 1$, then $\gcd(ac, b) = \gcd(c, b)$.
  - Theorem 11.13: If $\gcd(a, b) = 1$ and $a \mid (bc)$, then $a \mid c$.
  - Corollary 11.14: p a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
  - Corollary 11.15: p be a prime number. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some k $(1 \leq k \leq n)$.
- If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.
- Theorem 11.16: If $\gcd(a, b) = 1$, $a \mid c$, $b \mid c$, then $(ab) \mid c$.

Number Theory: Greatest Common Divisor (Cont.)

- Division Algorithm:
  - Original case: for all positive integers a and b, there exist unique integers q and r, such that $b = aq + r$, where $0 \leq r < a$.
  - Generalization: for all integers a and b, there exist unique integers q and r, such that $b = aq + r$, where $0 \leq r < |a|$. Here allow a and b to be negative.
  - Let a and b be positive integers. If $b = aq + r$ for some integers q and r, then $\gcd(b, a) = \gcd(a, r)$.
- Euclidean Algorithm: let a, b be integers, where $b \geq a > 0$.

$$
\begin{array}{rcl}
b = a \cdot q_1 + r_1 & \gcd(b, a) = \gcd(a, r_1) & 0 \leq r_1 < |a| \\
a = r_1 \cdot q_2 + r_2 & \gcd(a, r_1) = \gcd(r_1, r_2) & 0 \leq r_2 < r_1 \\
r_1 = r_2 \cdot q_3 + r_3 & \gcd(r_1, r_2) = \gcd(r_2, r_3) & 0 \leq r_3 < r_2 \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots \\
r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} & \gcd(r_{n-3}, r_{n-2}) = \gcd(r_{n-2}, r_{n-1}) & 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1} \cdot q_n + r_n & \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) & 0 \leq r_n < r_{n-1} \\
r_{n-1} = r_n \cdot q_{n+1} + 0 & \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n &
\end{array}
$$

  The sequence r_i will go to 0 eventually since $|a|$ is finite and $|a| > r_1 > r_2 > \cdots > r_{n-1} > r_n > r_{n+1} = 0$. Then $\gcd(a, b) = r_n$.
- Working backwards, we can find the integers x and y, so that $\gcd(a, b) = ax + by$.
- Notice: when a or b is negative, we can not apply Euclidean Algorithm to get $\gcd(a, b)$ directly. Apply $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$.

Number Theory: Prime

- A prime is an integer $p \geq 2$ whose only positive integer divisors are 1 and p. An integer $n \geq 2$ that is not prime is called a composite number.
- Let a and b be integers, not both 0.
  - If $\gcd(a, b) = 1$, then a and b are relatively prime.
  - Theorem 11.12: a and b are relatively prime iff 1 is a linear combination of a and b.
  - Theorem 11.16: Let $a, b, c \in \mathbb{Z}$, where a and b are relatively prime nonzero integers. If $a \mid c$ and $b \mid c$, then $ab \mid c$.
- Euclid's Lemma
  - Let a, b be integers, and p be a prime number. If $p \mid ab$, then $p \mid a$ or $p \mid b$.
  - Let $a_1, a_2, \ldots, a_n$ be integers, and p be a prime number. If $p \mid a_1 \cdots a_n$, then $p \mid a_k$ for some $1 \leq k \leq n$.
- If $n = p_1 p_2 \cdots p_r$ with primes $p_1 \leq p_2 \leq \ldots \leq p_r$, we will call this a prime factorization of n.
- Fundamental Theorem of Arithmetic:
  - Existence of prime factorization: Every integer greater than 1 is either a prime number or a product of prime numbers.
  - Uniqueness of prime factorization: For any integer greater than 1, the prime factorization is unique except possibly for the order in which the factors occur.
- Canonical factorization: Given any integer $n > 1$. Suppose $p_1 < p_2 < \cdots < p_r$ are the distinct prime divisors of n. Then we can write $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ for $k_i \geq 1$.

Number Theory: Misc

- Euclid's Theorem: There are infinitely many prime numbers.
- A positive integer n is a perfect square if there exists an integer m such that $n = m^2$.
- Let $n > 1$ be an integer. n is a perfect square iff every prime number in the canonical factorization of $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ appears an even number of time.
- Let n be a positive integer. If n is not a perfect square, then $\sqrt{n}$ is irrational.

Exercise (9-1)

Use the Euclidean Algorithm to find $\gcd(12628, 21361)$ *and find integers* m *and* n *such that* $\gcd(12628, 21361) = 12628m + 21361n$.

Solution.

By Euclidean Algorithm:

$$\begin{aligned}
21361 &= 12628 * 1 + 8733 \\
12628 &= 8733 * 1 + 3895 \\
8733 &= 3895 * 2 + 943 \\
3895 &= 943 * 4 + 123 \\
943 &= 123 * 7 + 82 \\
123 &= 82 * 1 + 41 \\
82 &= 41 * 2 + 0
\end{aligned}$$

Thus, $\gcd(12628, 21361) = 41$.

Working backwards, we will obtain:

$$\begin{aligned}
41 &= 123 - 82 * 1 \\
&= 123 - (943 - 123 * 7) \\
&= 943 * (-1) + 123 * 8 \\
&= 943 * (-1) + (3895 - 943 * 4) * 8 \\
&= 3895 * 8 - 943 * 33 \\
&= 3895 * 8 - (8733 - 3895 * 2) * 33 \\
&= 12628 * 181 + 21361 * (-107)
\end{aligned}$$

Thus, $m = 181$, $n = -107$.

□

Exercise (9-2)

Let $a \in \mathbb{Z}$.

(a) *Show that the possible values of $\gcd(a, a+2)$ are 1 and 2.*

(b) *If p is a prime, find the possible values of $\gcd(a, a+p)$.*

(c) *Find a necessary and sufficient condition for $\gcd(a, a+p) = 1$ where p is a prime. Justify your answer.*

Recall

1. $\gcd(a, b) = \gcd(a, b + an)$ for all $n \in \mathbb{N}$.
2. p is a prime number, then $\gcd(p, a) = \begin{cases} p, & \text{if } p \mid a; \\ 1, & \text{if } p \nmid a. \end{cases}$

Solution.

(a) By Recall 1, we have $\gcd(a, a+2) = \gcd(a, 2)$. Then by Recall 2, since 2 is a prime number, the possible values of $\gcd(a, a+2)$ are 1 and 2.

(b) By Recall 1, we have $\gcd(a, a+p) = \gcd(a, p)$. Then by Recall 2, the possible values of $\gcd(a, a+p)$ are 1 and p.

(c) By Recall 1, we have $\gcd(a, a+p) = \gcd(a, p)$. Then by Recall 2, we have $\gcd(a, a+p) = 1$ if and only if $p \nmid a$.

□

Exercise (9-3)

Let $a, b, c \in \mathbb{Z}$, with a not zero. Show that:

(a) $\gcd(a, b) = \gcd(a, a + b)$;

(b) *If* $a \mid bc$, *then* $a \mid \gcd(a, b) \times c$;

(c) *If* $\gcd(a, b) = 1$ *and* $\gcd(a, c) = 1$, *then* $\gcd(a, bc) = 1$;

(d) *If* $\gcd(a, b) = d$, *then* $\gcd(a/d, b/d) = 1$;

(e) *If* $\gcd(a, b) = 1$, *then* $\gcd(a + b, a - b) = 1$ *or 2*;

(f) *If* $\gcd(a, b) = 1$, *then* $\gcd(ac, b) = \gcd(c, b)$.

Proof.

(a,c,d,f) For (a), (c), (d), and (f), please refer to Proposition 3.3 (3), Proposition 3.11 (1), Proposition 3.5 and Theorem 3.10 (1) in "Summary", respectively.

(b)
1. By Theorem 11.7, we have $\gcd(a, b) = ax + by$ for some integers x, y.
2. Multiply c, we obtain $\gcd(a, b) \times c = axc + byc$.
3. Since $a \mid bc$, we have $ak = bc$ for some integer k. Hence the Equation becomes $\gcd(a, b) \times c = axc + aky = a(xc + ky)$.
4. So we have $a \mid [\gcd(a, b) \times c]$.

(e)
1. Let $d = \gcd(a + b, a - b)$. Then $d \mid (a + b)$ and $d \mid (a - b)$. This implies $d \mid (2a)$ and $d \mid (2b)$. Hence $2a = dp$ and $2b = dq$ for some integers p, q.
2. Since $\gcd(a, b) = 1$, so $ax + by = 1$ for some integers x, y. Multiplying 2, we have $2ax + 2by = 2$.
3. Then we have $(dp)x + (dq)y = 2$ which gives $d(px + qy) = 2$. Hence $d \mid 2$. This implies $d = 1$ or 2.

Exercise (9-4)

(a) *Show that if the integers $r_1, r_2, \ldots, r_n$ are all of the form $4k+1$ for some integer k, then their product $r_1 r_2 \cdots r_n$ is also of the form $4k+1$.*

(b) *Prove that there are infinitely many primes that are congruent to 3 modulo 4.*

Proof of (a).

1. Since $r_i = 4k_i + 1$ for some integer k_i for all $i \in \{1, 2, \ldots, n\}$, we have
$$r_i \equiv 1 \bmod 4 \text{ for all } i = 1, 2, \ldots, n.$$
2. Then we have
$$r_1 r_2 \cdots r_n \equiv 1 \times 1 \times \cdots \times 1 \equiv 1 \bmod 4.$$
3. That is, $r_1 r_2 \cdots r_n = 4k + 1$ for some integer k.

□

Proof of (b).

The idea also comes from Euclid's proof for the existence of infinitely many prime numbers.

1. Prove by contradiction: Suppose there are only finitely many prime numbers that are congruent to 3 modulo 4.
2. Let $p_1, p_2, \ldots, p_m$ be all the primes that are congruent to 3 modulo 4. Construct the integer $M = 4p_1p_2 \cdots p_m - 1$.
3. Then we have the following facts:
   - (i) $M > p_i$ for all $i = 1, 2, \ldots, m$.
   - (ii) $M \equiv -1 \equiv 3 \bmod 4$.
   - (iii) M is not a prime number. Otherwise, by Fact (i) and (ii), we find another $4k+3$-form prime number M, which is a contradiction.
   - (iv) $p_i \nmid M$ for all i. Otherwise, we have $p_i \mid 1$ since $p_i \mid M + 1$, which is also a contradiction.
4. By Fact (iii), M is a composite number, and has a prime factorization $M = q_1 q_2 \cdots q_k$.
5. Since M is odd, q_j is odd for all j, and hence is congruent to 1 or 3 modulo 4.
6. By Fact (iv), q_j can not be any of the p_i. So all q_j must be congruent to 1 modulo 4.
7. Then by part (a), M is also congruent to 1 modulo 4, which is a contradiction.

□

Exercise (9-5)

(a) *Find the largest perfect square that divides* $25!$. *(You may present your answer as a prime factorization.)*

(b) *Find the largest square free integer that divides* $25!$.

(c) *Find the number of digits of 0 at the end of the* $25!$.

Solution.
We first express $25!$ as prime factorization:

$$\begin{aligned}25! =& 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 \times 13 \times 14 \times 15 \\ & \times 16 \times 17 \times 18 \times 19 \times 20 \times 21 \times 22 \times 23 \times 24 \times 25 \\ =& 2 \times 3 \times (2^2) \times 5 \times (2 \cdot 3) \times 7 \times (2^3) \times (3^2) \times (2 \cdot 5) \times 11 \times (2^2 \cdot 3) \times 13 \times (2 \cdot 7) \times (3 \cdot 5) \\ & \times (2^4) \times 17 \times (2 \cdot 3^2) \times 19 \times (2^2 \cdot 5) \times (3 \cdot 7) \times (2 \cdot 11) \times 23 \times (2^3 \cdot 3) \times (5^2) \\ =& 2^{22} \times 3^{10} \times 5^6 \times 7^3 \times 11^2 \times 13 \times 17 \times 19 \times 23\end{aligned}$$

(a) The largest perfect square that divides $25!$ is the product of all the prime factors of $25!$ to their largest possible even powers, i.e. $2^{22} \times 3^{10} \times 5^6 \times 7^2 \times 11^2$.

(b) The largest square-free number that divides $25!$ is the product of all the prime factors of $25!$ to the power 1, i.e. $2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \times 23$.

(c) Each pair of prime factor 2 and 5 will give a product of 10 and hence contributes to a 0 at the end of $25!$. Since there are twenty-two 2's and six 5's, so there are six 0's at the end of $25!$.

□

Exercise (9-6)

Show that every natural number n can be written as $n = mk^2$ where $m, k \in \mathbb{N}$ and m is square free.

Proof.

1. Let the canonical factorization of n be $p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$.
2. Rearrange the primes in n so that $p_1, \ldots, p_t$ have even powers $h_i = 2a_i$ and $p_{t+1}, \ldots, p_k$ have odd powers $h_i = 2a_i + 1$.
3. Then

$$\begin{aligned} n &= (p_1^{2a_1} \cdots p_t^{2a_t})(p_{t+1}^{2a_{t+1}+1} \cdots p_k^{2a_k+1}) \\ &= (p_1^{2a_1} \cdots p_t^{2a_t})(p_{t+1}^{2a_{t+1}} \cdots p_k^{2a_k})(p_{t+1} \cdots p_k) \\ &= (p_1^{2a_1} \cdots p_t^{2a_k} p_{t+1}^{2a_{t+1}} \cdots p_k^{2a_k})(p_{t+1} \cdots p_k) \\ &= (p_1^{a_1} \cdots p_k^{a_k})^2 (p_{t+1} \cdots p_k) \end{aligned}$$

4. By letting

$$k = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad m = p_{t+1} p_{t+2} \cdots p_k,$$

we have $n = mk^2$, where m is square free.

□

Additional material

Exercise (Question 8(b) in Final 2008–2009(I))

For any positive integer n, let $d(n)$ be the number of positive divisors of n. Show that $d(n) \leq 2\sqrt{n}$ for all $n \in \mathbb{Z}^+$.

Proof.

Let $d(n) = k$, and $1 = d_1 < d_2 < \cdots < d_k = n$ be all the positive divisors of n. Then

$$d_i d_{k+1-i} = n, \text{ for all } 1 \leq i \leq k.$$

- If n is a square, then k is odd and $d_{\frac{k+1}{2}} = \sqrt{n} \in \mathbb{N}$. Since

  $$1 = d_1 < d_2 < \cdots < d_{\frac{k+1}{2}} = \sqrt{n},$$

  we have $\frac{k+1}{2} \leq \sqrt{n}$. Hence $d(n) = k \leq 2\sqrt{n} - 1 < 2\sqrt{n}$.
- If n is not a square, then k is even and $d_{\frac{k}{2}} d_{\frac{k}{2}+1} = n$. Since $d_{\frac{k}{2}} < d_{\frac{k}{2}+1}$, we have $d_{\frac{k}{2}} < \sqrt{n}$. Now

  $$1 = d_1 < d_2 < \cdots < d_{\frac{k}{2}} < \sqrt{n},$$

  then we have $\frac{k}{2} < \sqrt{n}$. Hence $d(n) = k < 2\sqrt{n}$.

□

Change log

- Page 189: Revise a typo: "23" to "2×3".

Last modified: 12:00, October 31 2010.

Final Exam Information

- Time: November 23th (Tuesday), 09:00–11:00;
- Venue: MPSH 5;
- Results available in final exam (from VT, last year):
  - Short answer: you can use all of them (that we have discussed and proven)
  - Longer answer: you can use the results relative to the question asked. If an exam question can be answered in one or two lines by quoting a result, then you should know that you need to elaborate more.
- Consultation:
  - Time: Any time from November 15th to November 23th
  - Venue: S17-06-14
  - Email: xiangsun@nus.edu.sg
  - Mobile: 9169 7677
- Be careful, and do not make any stupid mistakes.
- Good Luck.

Schedule of Tutorial 10

- Review concepts: Cardinality:
  - Numerically equivalence;
  - Denumerable set, countable set, uncountable set.
- Tutorial
- Additional material:
  - Question 4(b) in Final 2006–2007(I);
  - Advanced results in cardinality;
  - Question 8(b) in Final 2009–2010(I).

Cardinality: Concepts

- A set A is finite, if $|A| = n$ for some nonnegative integer n.
  If A is a nonempty finite set, we can write $A = \{a_1, a_2, \ldots, a_n\}$ for some $n \in \mathbb{N}$.
- If there exists a bijection $f\colon A \to B$, we say that A is numerically equivalent to B.
  - If A and B finite, then A is numerically equivalent to B if and only if $|A| = |B|$.
  - If A and B infinite, we define $|A| = |B|$ if A is numerically equivalent to B.

  Therefore, for any sets A and B,

$$|A| = |B| \Leftrightarrow \text{ there is a bijection } f\colon A \to B.$$

- A set A is called a denumerable (or countably infinite) set, if $|A| = |\mathbb{N}|$.
  If A is a nonempty denumerable set, we can write $A = \{a_1, a_2, a_3, \ldots\}$.
- A set A is called a countable set, if it is either finite or a denumerable set.
- A set A is called an uncountable set, if it is not countable.

Cardinality: General Results

- Theorem 10.3: Every infinite subset of a denumerable set is denumerable.
- Result 10.5: If A and B are denumerable sets, then $A \times B$ is denumerable.
  Generalization: If A_i is denumerable for all $i \in \mathbb{N}$, then $\times_{i \in \mathbb{N}} A_i$ is also denumerable.
- If A and B are denumerable sets, then $A \cup B$ is denumerable. Refer to Exercise 10-3.
  Generalization: If A_i is denumerable for all $i \in \mathbb{N}$, then $\cup_{i \in \mathbb{N}} A_i$ is also denumerable.
- Theorem 10.9: Let A and B be sets, $A \subseteq B$. If A is uncountable, then B is uncountable.

Cardinality: Examples

- $\mathbb{Z}^*, \mathbb{Z}, \mathbb{Q}^+, \mathbb{Q}$ are denumerable.
- Theorem 10.8: $(0,1)$ is uncountable, i.e. $|(0,1)| \neq \mathbb{N}$: Cantor's diagonal argument.
- Theorem 10.13: $|(0,1)| = |\mathbb{R}|$: $f(x) = \tan\left((x - \frac{1}{2})\pi\right)$ is a bijection $(0,1) \to \mathbb{R}$.
- $|(0,1)| = |(0,1]| = |[0,1)| = |[0,1]|$. Refer to ▸ $|(0,1)| = |[0,1]|$
- sets
  - finite
  - infinite
    - denumerable $(\aleph_0)$: $\mathbb{N}, \mathbb{Z}^*, \mathbb{Z}, \mathbb{Q}^+, \mathbb{Q}$
    - uncountable
      - equivalent to $(0,1)$ $(\aleph_1, c)$: $(a,b), [0,1], [a,b], \mathbb{R}, \mathbb{I}$
      - not equivalent to $(0,1)$ $(\aleph_2, \aleph_3, \ldots)$: $\mathcal{P}(\mathbb{R}), \ldots$

Exercise (10-1)

State whether each of the following statements is true or false. Justify your answers.

(a) *If a set A is countable, then A is infinite.*

(b) *If a set A is denumerable, then A is countable.*

(c) *If a set A is uncountable, then A is infinite.*

(d) *If a set A is equivalent to a finite set, then A is not countable.*

(e) *If a set A is equivalent to an infinite set, then A is denumerable.*

Solution.

(a) False. By definition, a countable set is either finite or denumerable.

(b) True. This follows from definition of countable set.

(c) True. "Uncountable" means not countable. So an uncountable set cannot be finite.

(d) False. If A is equivalent to a finite set, then A itself is finite, and hence is countable.

(e) False. Counter-example: Take A to be $\mathbb{R}$, which is equivalent to the infinite set $(0, 1)$. But $\mathbb{R}$ is not denumerable.

□

Exercise (10-2(a))

Prove that the set of all positive integers that are multiples of 5 is denumerable by constructing a bijection from $\mathbb{N}$ to the set.

Proof.

1. Let $A = \{m \in \mathbb{N} \mid m = 5n \text{ for some } n \in \mathbb{Z}\} = \{5, 10, 15, 20, 25, \ldots\}$.
2. Define
$$f\colon \mathbb{N} \to A, \text{ by } f(n) = 5n.$$
3. f is an injection: Let $m, n \in \mathbb{N}$. If $f(m) = f(n)$, then $5m = 5n$. So $m = n$.
4. f is a surjection: Let $a \in A$. Then $a = 5n$ for some positive integer n. So $a = f(n)$ with $n \in \mathbb{N}$.
5. Thus f is a bijection, and hence A is denumerable.

□

Exercise (10-2(b))

Prove that $\{n \in \mathbb{Z} \mid n \geq -10\}$ *is denumerable by constructing a bijection from* $\mathbb{N}$ *to the set.*

Proof.

1. Let $B = \{n \in \mathbb{Z} \mid n \geq -10\} = \{-10, -9, -8, \ldots, 1, 2, 3, \ldots\}$.
2. Define
$$g\colon \mathbb{N} \to B, \text{ by } g(n) = n - 11.$$
3. g is an injection: Let $m, n \in \mathbb{N}$. If $g(m) = g(n)$, then $m - 11 = n - 11$. So $m = n$.
4. g is a surjection: Let $b \in B$. Then $b \geq -10$. So $b + 11 \geq 1$. That is, $b + 11 = n$ for some positive integer n. So $b = n - 11 = g(n)$ with $n \in \mathbb{N}$.
5. Thus g is a bijection, and hence B is denumerable.

□

Exercise (10-2(c))

Prove that $\mathbb{N} - \{4, 5, 6\}$ is denumerable by constructing a bijection from $\mathbb{N}$ to the set.

Proof.

1. Let $C = \mathbb{N} - \{4, 5, 6\} = \{1, 2, 3, 7, 8, 9, \ldots\}$.
2. Define $h\colon \mathbb{N} \to C$ by $h(n) = \begin{cases} n, & \text{if } n \leq 3; \\ n+3, & \text{if } n > 3. \end{cases}$
3. h is an injection: Let $m, n \in \mathbb{N}$. If $h(m) = h(n)$, we consider 4 cases:
   - $m, n \leq 3$. Then $h(m) = h(n) \Rightarrow m = n$.
   - $m, n > 3$. Then $h(m) = h(n) \Rightarrow m + 3 = n + 3 \Rightarrow m = n$.
   - $m \leq 3$, $n > 3$. Then $h(m) = m \leq 3$, $h(n) = n + 3 > 6$ which contradicts that $h(m) = h(n)$.
   - $m > 3$, $n \leq 3$. Similar to case 3, which is impossible.
4. h is a surjection: Let $c \in C$. Consider 2 cases:
   - $c = 1, 2$ or 3. Then $c = h(c)$ with $c \in \mathbb{N}$.
   - $c > 6$. Then $c - 3 > 3$. Then $c = (c - 3) + 3 = h(c - 3)$ with $c - 3 \in \mathbb{N}$.
5. Thus h is a bijection, and hence C is denumerable.

□

Exercise (10-3)

Let A and B be two disjoint denumerable sets. Show that $A \cup B$ is denumerable. (Note: The result still holds without the disjoint condition.)

Method

1. Since A and B are two denumerable sets, we can write

$$A = \{a_1, a_2, a_3, \ldots\}, \quad B = \{b_1, b_2, b_3, \ldots\}.$$

2. Then we can write $A \cup B$ as

$$\{a_1, b_1, a_2, b_2, a_3, b_3, \ldots, a_n, b_n, a_{n+1}, b_{n+1}, \ldots\}.$$

3. Then it is easy to construct the bijection from $\mathbb{N}$ to $A \cup B$.

Proof.

1. Since A and B are denumerable, there are bijections $f\colon \mathbb{N} \to A$ and $g\colon \mathbb{N} \to B$.
2. Define $h\colon \mathbb{N} \to A \cup B$, by $h(n) = \begin{cases} f(k), & \text{if } n = 2k-1 \text{ for some } k \in \mathbb{N}; \\ g(k), & \text{if } n = 2k \text{ for some } k \in \mathbb{N} \end{cases}$
3. h is injective: Let $m, n \in \mathbb{N}$. Suppose $h(m) = h(n)$.
   - If both m and n are odd, then $m = 2k-1$ and $n = 2l-1$. So $h(m) = f(k)$ and $h(n) = f(l)$. Now $f(k) = f(l)$ implies $k = l$ as f is injective. So $m = n$.
   - If both m and n are even, then $m = 2k$ and $n = 2l$. So $h(m) = g(k)$ and $h(n) = g(l)$. Now $g(k) = g(l)$ implies $k = l$ as g is injective. So $m = n$.
   - If m is even and n is odd, then $m = 2k$ and $n = 2l-1$. So $h(m) = g(k)$ and $h(n) = f(l)$. Now $g(k) \in B$ and $h(l) \in A$. So it is impossible that $g(k) = f(l)$.
4. h is surjective: Let $c \in A \cup B$.
   - If $c \in A$, then $c = f(k)$ for some $k \in \mathbb{N}$. So $c = h(2k-1)$.
   - If $c \in B$, then $c = g(k)$ for some $k \in \mathbb{N}$. So $c = h(2k)$.
5. Thus h is a bijection, and hence $A \cup B$ is denumerable.

□

Exercise (10-4)

State whether each of the following statements is true or false. Justify your answers.

(a) *If A is denumerable and B is finite, then $A - B$ is denumerable.*

(b) *If A and B are denumerable, then $A \cap B$ is denumerable.*

(c) *If A, B, C are sets such that $A \subseteq B \subseteq C$, and A and C are denumerable, then B is denumerable.*

Proof.

(a)
1. Since $A - B$ is a subset of A, $A - B$ is countable.
2. $A - B$ cannot be finite: Otherwise B and $A - B$ are finite will imply A is finite (contradiction).
3. Hence $A - B$ is denumerable. True.

(b) False. Take $A = \{n \in \mathbb{Z} \mid n \geq 0\}$ and $B = \{n \in \mathbb{Z} \mid n \leq 0\}$. Both are denumerable. But $A \cap B = \{0\}$ is finite, and hence not denumerable.

(c)
1. A is denumerable so it is infinite. Hence B is also infinite.
2. C is denumerable so it is countable. Hence B is also countable.
3. Since B is infinite and countable, it is denumerable. True.

Exercise (10-5)

Show that the set $\mathbb{I}$ of irrational numbers is uncountable.

Proof.

1. We have $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$, $\mathbb{Q}$ and $\mathbb{I}$ are disjoint.
2. If $\mathbb{I}$ is countable. Since $\mathbb{Q}$ is denumerable, by Question 10-3, we have that $\mathbb{R}$ would be denumerable, which is a contradiction.
3. Therefore, $\mathbb{I}$ is uncountable.

$\square$

Exercise (10-6)

(a) *Is it possible to find a denumerable subset of $\mathbb{R}$ that does not contain any rational number?*

(b) *Is it possible to find an uncountable subset of $\mathbb{R}$ that does not contain any irrational number?*

Justify your answers.

Solution.

(a) Possible. Example: $A = \{n + \sqrt{2} \mid n \in \mathbb{N}\}$. All the elements in A are irrational. The function $f\colon \mathbb{N} \to A$ defined by $f(n) = n + \sqrt{2}$ is a bijection.

(b) Impossible. A subset of $\mathbb{R}$ which does not contain any irrational number is a subset of $\mathbb{Q}$, which is countable. So such a subset must be countable.

□

Exercise (10-7(a))

Show that the cardinality of $(1, \infty)$ *is the same as* $|\mathbb{R}|$ *by constructing an appropriate bijection from* $\mathbb{R}$ *to the respective set.*

Proof.

1. Define
$$f\colon \mathbb{R} \to (1, \infty), \text{ by } f(x) = e^x + 1.$$
2. f is an injection: Let $x, y \in \mathbb{R}$. If $f(x) = f(y)$, then $e^x + 1 = e^y + 1$. So $e^x = e^y$. Since e^x is an injection, so $x = y$.
3. f is a surjection: Let $z \in (1, \infty)$. Then $z - 1 > 0$, which is in the range of the exponential function. So $z - 1 = e^x$ for some real number x. So $z = e^x + 1 = f(x)$ with $x \in \mathbb{R}$.
4. Hence $|(1, \infty)| = |\mathbb{R}|$.

□

Exercise (10-7(b))

Show that the cardinality of $\mathbb{R} - \{0\}$ is the same as $|\mathbb{R}|$ by constructing an appropriate bijection from $\mathbb{R}$ to the respective set.

Proof.

1. Define $g\colon \mathbb{R} \to \mathbb{R} - \{0\}$, by $g(x) = \begin{cases} x+1, & \text{if } x \in \mathbb{Z}^* \text{ (nonnegative integer)} \\ x, & \text{otherwise} \end{cases}$
2. Note that in this function, every real number will be mapped to itself, except for the nonnegative integers: $g(0) = 1,\ g(1) = 2,\ g(2) = 3$ etc. So no integer will map to 0, which makes g a well-defined function.
3. g is an injection: Let $x, y \in \mathbb{R}$. If $g(x) = g(y)$, we consider 4 cases:
   - $x, y \in \mathbb{Z}^*$. Then $g(x) = g(y) \Rightarrow x + 1 = y + 1 \Rightarrow x = y$.
   - $x, y \notin \mathbb{Z}^*$. Then $g(x) = g(y) \Rightarrow x = y$.
   - $x \in \mathbb{Z}^*$, $y \notin \mathbb{Z}^*$. Impossible.
   - $x \notin \mathbb{Z}^*$, $y \in \mathbb{Z}^*$. Impossible.
4. g is a surjection: Let $y \in \mathbb{R} - \{0\}$. Consider 2 cases:
   - $y \in \mathbb{N}$. Then $y - 1 \in \mathbb{Z}^*$. So $y = (y-1) + 1 = g(y-1)$ with $y - 1 \in \mathbb{R}$.
   - $y \notin \mathbb{Z}^*$. Then $y = g(y)$ with $y \in \mathbb{R}$.
5. Hence $|\mathbb{R} - \{0\}| = |\mathbb{R}|$.

□

Additional material

Exercise (Question 4(b) in Final 2006–2007(I))

Construct a bijection $f : [0, 1] \to (0, 1)$.

Solution.

1. To map $[0, 1]$ to $(0, 1)$, we realize that there are 2 extra points in $[0, 1]$ and we will need to find a way to squeeze them into $(0, 1)$.
2. So, the intuitive way to map $[0, 1]$ to $(0, 1)$ is to map $0 \mapsto \frac{1}{2}$, $1 \mapsto \frac{1}{3}$, $\frac{1}{2} \mapsto \frac{1}{4}$, $\cdots$, $\frac{1}{k} \mapsto \frac{1}{k+2}$, etc., and everything else remains the same.
3. $$f = \begin{cases} \frac{1}{2}, & \text{when } x = 0; \\ \frac{1}{n+2}, & \text{when } x = \frac{1}{n}, n \in \mathbb{N}; \\ x, & \text{when } x \neq 0 \text{ and is not reciprocal of some positive integer.} \end{cases}$$
4. It direct to check that f is bijective.

□

Additional material

- If $A \subseteq B \subseteq C$, and $|A| = |C|$, then $|A| = |B| = |C|$.
  Using this fact, it is easy to obtain $|(0,1)| = |[0,1]|$.
- Cantor[22]-Bernstein[23]-Schröder[24] Theorem (Theorem 10.18): If A and B are sets such that $|A| \leq |B|$ and $|A| \geq |B|$, then $|A| = |B|$.
  Using this fact, it is easy to obtain $|\mathbb{N}| = |\mathbb{Q}|$.
- Based $|(0,1)| = |[0,1]|$ and Cantor-Bernstein-Schröder Theorem, we have:

$$|[0,1]| = |(0,1)| = |[0,1)| = |(0,1]| = |[a,b]| = |(a,b)| = |[a,b)| = |(a,b]| = \mathbb{R}.$$

- Theorem 11.19: $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.
- $$\underbrace{|\mathbb{N}|}_{\aleph_0} < \underbrace{|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|}_{\aleph_1 = c} < \underbrace{|\mathcal{P}(\mathbb{R})|}_{\aleph_2} < \cdots .$$
- The Continuum Hypothesis[25]: There exist no set S such that

$$\aleph_0 < |S| < \aleph_1 = c.$$

[22] Georg Ferdinand Ludwig Philipp Cantor (March 3, 1845–January 6, 1918), a German mathematician.
[23] Felix Bernstein (February 24, 1978–December 3, 1956), a German mathematician.
[24] Ernst Schröder (November 25, 1941–June 16, 1902), a German mathematician.
[25] It is advanced by Georg Cantor in 1877.

Additional material

Exercise

1. *Question 8(b) in Final 2009–2010(I): Let $A = \{f \mid f\colon \{0,1\} \to \mathbb{N}\}$. Is A a countable set? Justify your answer.*
2. *Let $B = \{f \mid f\colon \mathbb{N} \to \{0,1\}\}$. Is B a countable set? Justify your answer.*

Solution.

(a) Yes.

1. Define a function $g\colon A \to \mathbb{N} \times \mathbb{N}$ by $g(f) = (a, b)$ if $f(0) = a$ and $f(1) = b$.
2. Let $f_1, f_2 \in A$. Suppose $g(f_1) = g(f_2) = (a, b)$, then $f_1(0) = a = f_2(a)$ and $f_1(1) = b = f_2(1)$. Therefore $f_1 = f_2$, and hence g is injective.
3. Let $(a, b) \in \mathbb{N} \times \mathbb{N}$. Define $f_0 \in A$ by $f_0(0) = a$ and $f_0(1) = b$. Then $g(f_0) = (a, b)$. Hence g is surjective.
4. Therefore $|A| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, and A is countable.

(b) No. $|2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$.

□

Change log

- Page 203: Revise typos: "$2k+1$" to "$2k-1$", and "$2l+1$" to "2l-1".

Last modified: 12:00, November 12, 2010.

Thank you