# Introduction to Sets and Logic (MATH 1190)

Instructor: Lili Shen
Email: shenlili@yorku.ca

Department of Mathematics and Statistics
York University

Dec 4, 2014

# Outline

# Relations



## Definition

A relation $R$ from a set $A$ to a set $B$ is a subset

$$R \subseteq A \times B.$$

$a$ is related to $b$ if $(a, b) \in R$, and is also denoted by $aRb$.

In order to distinguish from $n$-ary relations, a subset $R \subseteq A \times B$ is also called a binary relation.

# Examples of relations



## Example

Let $A$ be the set of students in a university, and $B$ the set of courses. Then a relation

$$R \subseteq A \times B$$

can be used to represent the enrollments of students at the university. That is to say,

$$(a, b) \in R \quad \text{or} \quad aRb$$

means the student $a$ is enrolled in the course $b$.

# Relations on a set



**Definition**

A relation on a set $A$ is a relation $R$ from $A$ to $A$.

In other words, a relation on a set $A$ is a subset of $A \times A$.

# Examples of relations



**Example (Divisibility relation)**

Let $A$ be the set $\{1, 2, 3, 4\}$, then the relation

$$R = \{(a, b) \mid a \text{ divides } b\}$$

is exactly

$$R = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}.$$

In general, this relation can be defined on the set $\mathbf{Z}^+$ of positive integers.

# Examples of relations

**Example (Congruence relation modulo $m$)**

Let $m$ be an integer with $m > 1$. Then

$$R = \{(a, b) \mid a \equiv b \pmod{m}\}$$

is a relation on the set $\mathbf{Z}$ of integers.

# Reflexive relations

## Definition

A relation $R$ on a set $A$ is reflexive if

$$\forall a \in A((a, a) \in R).$$

Both the divisibility relation on $\mathbf{Z}^+$ and the congruence relation modulo $m$ on $\mathbf{Z}$ are reflexive.

# Symmetric and antisymmetric relations



**Definition**

A relation $R$ on a set $A$ is symmetric if

$$\forall a, b \in A((a, b) \in R \to (b, a) \in R).$$

A relation $R$ on a set $A$ is antisymmetric if

$$\forall a, b \in A(((a, b) \in R \wedge (b, a) \in R) \to (a = b)).$$

The divisibility relation on $\mathbf{Z}^+$ is antisymmetric but not symmetric, and the congruence relation modulo $m$ on $\mathbf{Z}$ is symmetric but not antisymmetric.

# Transitive relations



**Definition**

A relation $R$ on a set $A$ is transitive if

$$\forall a, b, c \in A(((a, b) \in R \wedge (b, c) \in R) \to (a, c) \in R).$$

Both the divisibility relation on $\mathbf{Z}^+$ and the congruence relation modulo $m$ on $\mathbf{Z}$ are transitive.

# Outline

# Equivalence relations



## Definition

A relation $R$ on a set $A$ is called an equivalence relation if it is reflexive, symmetric, and transitive. Explicitly, for all $a, b, c \in A$,

- (reflexivity) $(a, a) \in R$;
- (symmetry) $(a, b) \in R \to (b, a) \in R$;
- (transitivity) $((a, b) \in R \wedge (b, c) \in R) \to (a, c) \in R$.

Two elements $a$ and $b$ are related by an equivalence relation are called equivalent, and we denote it by $a \sim b$.

# Examples of relations

**Example (Congruence modulo $m$)**

Let $m$ be an integer with $m > 1$. Show that the relation

$$R = \{(a, b) \mid a \equiv b \pmod{m}\}$$

is an equivalence relation on the set **Z** of integers.

# Examples of relations



**Proof.**

- Reflexivity: $a \equiv a \pmod{m}$ since $a - a = 0$ is divisible by $m$.
- Symmetry: if $a \equiv b \pmod{m}$, then $a - b = km$ for some integer $k$, and consequently $b - a = -km$. Thus $b \equiv a \pmod{m}$.
- Transitivity: if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $b = a + km$ and $c = b + lm$ for some integers $k, l$. It follows that

  $$c = a + km + lm = a + (k + l)m.$$

  Thus $a \equiv c \pmod{m}$.

Therefore, $R$ is an equivalence relation. $\square$

# Equivalence classes

**Definition**

Let $R$ be an equivalence relation on a set $A$. The set of all elements that are related to an element $a$ of $A$

$$\{s \mid (a, s) \in R\}$$

is called the equivalence class of $a$, and is denoted by $[a]_R$. $[a]_R$ can be abbreviated as $[a]$ if there is no confusion.

# Equivalence classes



## Remark

- Each $b \in [a]_R$ is called a representative of this equivalence class.
- Any element in a equivalence class can be used as a representative of this class. In other words, if $b \in [a]_R$ and $b' \in [a]_R$, then

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

# Examples of relations

## Example (Congruence classes modulo $m$)

The equivalence classes of the relation congruence modulo $m$ are called congruence classes modulo $m$. The congruence class of an integer $a$ modulo $m$ is denoted by $[a]_m$, and

$$[a]_m = \{\dots, a-2m, a-m, a, a+m, a+2m, \dots\}.$$

For example,

$$\begin{aligned}
[0]_4 &= \{\dots, -8, -4, 0, 4, 8, \dots\},\\
[1]_4 &= \{\dots, -7, -3, 1, 5, 9, \dots\},\\
[2]_4 &= \{\dots, -6, -2, 2, 6, 10, \dots\},\\
[3]_4 &= \{\dots, -5, -1, 3, 7, 11, \dots\}.
\end{aligned}$$

# Equivalence classes and partitions



**Theorem**

*Let $R$ be an equivalence relation on a set $A$. The following statements are equivalent for $a, b \in A$:*

(i) $(a, b) \in R$;

(ii) $[a] = [b]$;

(iii) $[a] \cap [b] \neq \varnothing$.

# Equivalence classes and partitions

**Proof.**

(i)$\to$(ii): Suppose $c \in [a]$, then $(c, a) \in R$.
Since $R$ is an equivalence relation and $(a, b) \in R$, by the transitivity of $R$ we have $(c, b) \in R$, and consequently $c \in [b]$.
Similarly one can show that $c \in [b]$ implies $c \in [a]$.
Therefore $[a] = [b]$.

(ii)$\to$(iii): Since $[a] = [b]$, it follows that $a \in [a] \cap [b]$. Hence $[a] \cap [b] \neq \varnothing$.

(iii)$\to$(i): Since $[a] \cap [b] \neq \varnothing$, then there exists $c \in [a] \cap [b]$, and consequently $(a, c) \in R$ and $(c, b) \in R$. Therefore $(a, b) \in R$ by the transitivity of $R$. $\square$

# Equivalence classes and partitions

From this theorem we know that

$$[a] \neq [b] \longleftrightarrow [a] \cap [b] = \varnothing.$$

Therefore, Given any $a, b \in A$, there are only two cases:

- $[a] = [b]$;
- $[a] \cap [b] = \varnothing$.

Note also that

$$\bigcup_{a \in A} [a] = A.$$

Therefore, the equivalence classes form a partition of $A$, because they split $A$ into disjoint subsets.

# Partitions

## Definition

A partition of a set $S$ is a collection of disjoint nonempty subsets of $S$ that have $S$ as their union.

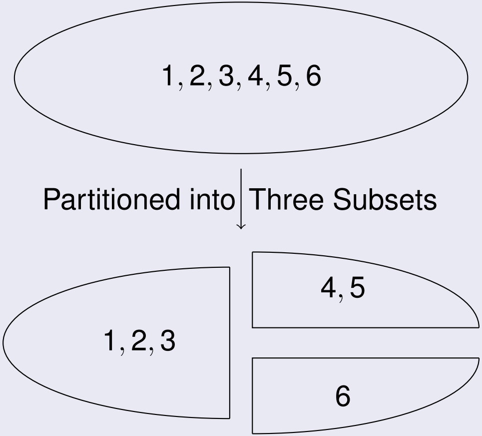
In other words, the collection of subsets $A_i$, where $i \in I$ ($I$ is an index set), forms a partition of $S$ if and only if

- $A_i \neq \varnothing$ for $i \in I$,
- $A_i \cap A_j = \varnothing$ when $i \neq j$, and
- $\bigcup\limits_{i \in I} A_i = S$.

# Examples of partitions



## Example



# Equivalence classes and partitions



**Theorem**

*Let $R$ be an equivalence relation on a set $S$. Then the equivalence classes of $R$ form a partition of $S$. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set $S$, there is an equivalence relation $R$ that has the sets $A_i$, $i \in I$, as its equivalence classes.*

# Equivalence classes and partitions

**Proof.**

We have already shown the first part of the theorem.

For the second part, assume that $\{A_i \mid i \in I\}$ is a partition of $S$. Let $R$ be the relation on $S$ consisting of the pairs $(x, y)$ where $x$ and $y$ belong to the same subset $A_i$ in the partition. We must show that $R$ satisfies the properties of an equivalence relation.

# Equivalence classes and partitions



- Reflexivity: For every $a \in S$, $(a, a) \in R$, because $a$ is in the same subset as itself.
- Symmetry: If $(a, b) \in R$, then $b$ and $a$ are in the same subset of the partition, so $(b, a) \in R$.
- Transitivity: If $(a, b) \in R$ and $(b, c) \in R$, then $a$ and $b$ are in the same subset of the partition, as are $b$ and $c$. Since the subsets are disjoint and $b$ belongs to both, the two subsets of the partition must be identical. Therefore, $(a, c) \in R$ since $a$ and $c$ belong to the same subset of the partition.

$\square$

# Examples of partitions



## Example

The partition in the example of Page 23 gives rise to an equivalence relation on $\{1, 2, 3, 4, 5, 6\}$, which consists of the following ordered pairs:

$$(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2),$$
$$(4, 4), (5, 5), (4, 5), (5, 4),$$
$$(6, 6).$$

# Examples of partitions



## Example

We already know that

$$\begin{aligned}
[0]_4 &= \{\ldots, -8, -4, 0, 4, 8, \ldots\},\\
[1]_4 &= \{\ldots, -7, -3, 1, 5, 9, \ldots\},\\
[2]_4 &= \{\ldots, -6, -2, 2, 6, 10, \ldots\},\\
[3]_4 &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}.
\end{aligned}$$

These congruence classes modulo 4 form a partition of the set **Z** of integers.

In general, congruence classes module $m$ ($m > 1$ is an integer) form a partition of **Z**, and split **Z** into $m$ disjoint subsets.

# Outline

# Partial ordering



## Definition

A relation $R$ on a set $S$ is called a partial ordering (or partial order) if it is reflexive, antisymmetric, and transitive. Explicitly, for all $a, b, c \in S$,

- (reflexivity) $(a, a) \in R$;
- (antisymmetry) $((a, b) \in R \wedge (b, a) \in R) \to (a = b)$;
- (transitivity) $((a, b) \in R \wedge (b, c) \in R) \to (a, c) \in R$.

A set $S$ equipped with a partial ordering $R$ is called a partially ordered set, or abbreviated as a poset, and is denoted by $(S, R)$.
Usually we write a poset as $(S, \preceq)$, if $\preceq$ is a partial ordering on $S$.

# Examples of posets



## Example

- $(\mathbf{Z}, \leq)$ is a poset, where $\leq$ is the usual "less than or equal to" relation.
- $(\mathbf{Z}, \geq)$ is a poset, where $\geq$ is the usual "greater than or equal to" relation.
- $(\mathbf{Z}, =)$ is a poset, where $=$ is the usual "equal to" relation. Note that $=$ is also an equivalence relation on $\mathbf{Z}$.
- $(\mathbf{Z}, <)$ and $(\mathbf{Z}, >)$ are not posets due to the lack of reflexivity and antisymmetry.
- $(\mathbf{Z}, \neq)$ is not a poset due to the lack of reflexivity, antisymmetry and transitivity.

# Examples of posets



**Example (Divisibility relation)**

Show that $(\mathbf{Z}^{+}, |)$ is a partially ordered set.

# Examples of posets

**Proof.**

- Reflexivity: $a \mid a$ is trivial.
- Antisymmetry: if $a \mid b$ and $b \mid a$, then $a = kb$ and $b = la$ for some positive integers $k$ and $l$. Since all these integers are positive, it follows that $a = kla$ and consequently $kl = 1$, which implies $k = l = 1$. Hence $a = b$.
- Transitivity: if $a \mid b$ and $b \mid c$, then $b = ka$ and $c = lb$ for some integers $k, l$. It follows that $c = (kl)a$, and thus $a \mid c$.

Therefore, $(\mathbf{Z}^+, |)$ is a partially ordered set. □

# Comparable elements in posets

## Definition

The elements $a$ and $b$ in a poset $(S, \preceq)$ are called comparable if $a \preceq b$ or $b \preceq a$.
If neither $a \preceq b$ nor $b \preceq a$, $a$ and $b$ are called incomparable.

If $(S, \preceq)$ is a poset in which every pair of elements are comparable, then $\preceq$ is called a total order or linear order on $S$, and $(S, \preceq)$ is called a totally ordered set or linearly ordered set or chain.

# Examples of posets



- $(\mathbf{Z}^+, |)$ is not totally ordered. For example, 3 and 9 are comparable, but 5 and 7 are incomparable.
- $(\mathbf{Z}, =)$ is not totally ordered. Indeed, two integers in this poset are comparable if and only if they are equal.
- $(\mathbf{Z}, \leq)$ and $(\mathbf{Z}, \geq)$ are both totally ordered.

# Recommended exercises



Section 9.1: 2.

Section 9.5: 37, 41, 47.

Section 9.6: 6, 14.

# Outline

# Coverage



The final exam will cover the contents in our lecture notes. Relevant sections in textbook are listed below (excluding those subsections that are not mentioned in the lecture notes):

- Chapter 1: 1.1, 1.3-1.7;
- Chapter 2: 2.1-2.5;
- Chapter 4: 4.1, 4.3, 4.4;
- Chapter 5: 5.1, 5.2;
- Chapter 9: 9.1, 9.5, 9.6.

# Requirements

Chapter 1:

- Constructing compound propositions using logic operators $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ and (nested) quantifiers $\forall, \exists$.
- Translating English sentences and mathematical statements into propositional or predicate logic, and vice versa.
- Understanding logical equivalences.
- The methods of direct proofs, proofs by contraposition and proofs by contradiction.
- The method of proving "if and only if" statements.

# Requirements



## Chapter 2:

- Understanding sets, (proper) subsets, empty set, power sets, Cartesian products of two sets.
- Set operations (intersection, union, complement, difference) and their relations to logic operators.
- The methods of proving one set is a (proper) subset of another set and two sets are equal.
- Understanding basic notions of functions, and some elementary real-valued functions (i.e., linear functions, quadratic functions and exponential functions).
- The methods of showing that a function is/is not injective/surjective/bijective.
- Compositions and inverses of functions.

# Requirements



Chapter 2 (continued):

- Solving some simple recurrence relations with given initial conditions.
- Calculating the sums of terms of arithmetic progressions and geometric progressions.
- Calculating some simple double summations.
- Understanding the difference between finite sets and infinite sets.
- Examples of countable sets and uncountable sets.
- The methods of showing that two sets have the same cardinality.

# Requirements

Chapter 4:

- Understanding the division algorithm and congruence relations.
- Finding prime factorizations of integers.
- Finding the greatest common divisor and least common multiple of integers.
- Using Euclidean Algorithm to express the greatest common divisor of integers as a linear combination.
- Solving linear congruences by finding inverses.
- Using Chinese remainder theorem or back substitution to solve a system of congruences.

# Requirements

## Chapter 5:

- Proofs by mathematical induction.
- Proofs by strong induction.

## Chapter 9:

- Understanding the connection between equivalence relations, congruence classes and partition, and related examples.
- Understanding partial orderings and comparability, and related examples.

# Instructions



- The final exam will be held on Saturday, Dec 13, 7-10 pm at TM East.
- Our final exam is different (in time, location, exam questions and coverage) from Section A. Please make sure that you are enrolled in Section B and take part in the right exam.
- Final exam is a must for the final grading of the course. Missing the final exam without a formal deferred standing due to force majeure will be considered as giving up the credits.
- Please contact me BEFORE the final exam if you think there is anything wrong with your quiz marks or homework records.
- Additional office hours next week: 9-11 am from Monday to Friday.

# Instructions

- The final exam is half-open-book. Everyone is allowed to take part in the exam with one A4 sheet of paper, and anything can be written or printed on both sides of this paper. No other aids are permitted, including (but not limited to) a second sheet of paper, textbooks, lecture notes, calculators and electronic devices.
- Reviewing tips: focus on lecture notes and recommended exercises.
- The difficulty of the final exam will be similar to the quizzes. However, it is not wise to guess the questions of final exam from the quizzes. In fact, the required knowledge and methods that are not covered by the quizzes will probably appear in the final exam.

# THE END



Thank you for enduring the pain of math for the whole term.

Hope everyone has this feeling after the final exam: