

MATH 415
Modern Algebra I

Lecture 1:
Preliminaries from set theory.

Set theory

The primary notions of **set theory** are an **element** (an object that we can work with), a **set** (a collection of objects that we can work with), and **membership**. Namely, given an element x and a set S , we have either $x \in S$ (x is a member of S) or $x \notin S$ (x is not a member of S).

Any set is determined uniquely by its members (**axiom of extensionality**). Given sets S_1 and S_2 , we say that S_1 is a **subset** of S_2 (and write $S_1 \subset S_2$) if every member of S_1 is also a member of S_2 . The axiom of extensionality can be rephrased as follows: for any sets S_1 and S_2 ,

$$S_1 = S_2 \iff S_1 \subset S_2 \text{ and } S_2 \subset S_1.$$

Set theory

Set theory can provide the foundation for all of mathematics (though there are other ways as well).

The general idea is that every mathematical object is modeled as a set so that objects of the same kind are the same if and only if the corresponding sets are the same (but the same set can serve as a model for many objects of different kinds).

For example, one way to model nonnegative integers is as follows: 0 is the empty set \emptyset , 1 is $\{\emptyset\}$, 2 is $\{\emptyset, \{\emptyset\}\}$, 3 is $\{\emptyset, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}$, and so on...

Cartesian product

Definition. The **Cartesian product** $X \times Y$ of two sets X and Y is the set consisting of all ordered pairs (x, y) such that $x \in X$ and $y \in Y$.

The Cartesian square $X \times X$ is also denoted X^2 .

If the sets X and Y are finite, then

$\#(X \times Y) = (\#X)(\#Y)$, where $\#S$ denote the number of elements in a set S .

Remark. An ordered pair (x, y) can be modeled as a set $S_{x,y}$, where $S_{x,y} = \{x, \{x, y\}\}$ if $x \neq y$ and $S_{x,y} = \{x, \{x\}\}$ if $x = y$.

Relations

Definition. Let X and Y be sets. A **relation** R from X to Y is given by specifying a subset of the Cartesian product: $S_R \subset X \times Y$.

If $(x, y) \in S_R$, then we say that x **is related to** y (in the sense of R or by R) and write xRy .

Remarks. • Usually the relation R is identified with the set S_R .

• In the case $X = Y$, the relation R is called a **relation on** X .

Examples. • “is equal to”

$$xRy \iff x = y$$

Equivalently, $R = \{(x, x) \mid x \in X \cap Y\}$.

• “is not equal to”

$$xRy \iff x \neq y$$

• “is mapped by f to”

$xRy \iff y = f(x)$, where $f : X \rightarrow Y$ is a function.

Equivalently, R is the graph of the function f .

• “is the image under f of”

(from Y to X) $yRx \iff y = f(x)$, where $f : X \rightarrow Y$ is a function. If f is invertible, then R is the graph of f^{-1} .

• reversed R'

$xRy \iff yR'x$, where R' is a relation from Y to X .

• not R'

$xRy \iff \text{not } xR'y$, where R' is a relation from X to Y .

Equivalently, $R = (X \times Y) \setminus R'$ (set difference).

Relations on a set

- “is equal to”

$$xRy \iff x = y$$

- “is not equal to”

$$xRy \iff x \neq y$$

- “is less than”

$$X = \mathbb{R}, \quad xRy \iff x < y$$

- “is less than or equal to”

$$X = \mathbb{R}, \quad xRy \iff x \leq y$$

- “is contained in”

$X =$ the set of all subsets of some set Y ,

$$xRy \iff x \subset y$$

- “is congruent modulo n to”

$$X = \mathbb{Z}, \quad xRy \iff x \equiv y \pmod{n}$$

- “divides”

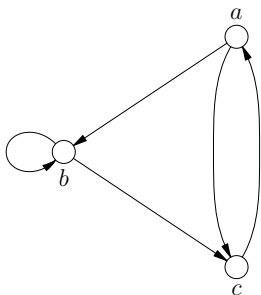
$$X = \mathbb{N}, \quad xRy \iff x|y$$

A relation R on a finite set X can be represented by a **directed graph**.

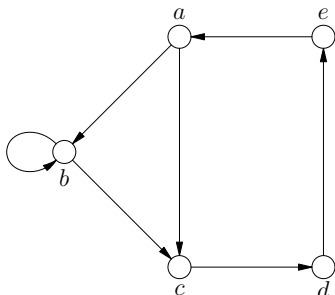
Vertices of the graph are elements of X , and we have a directed edge from x to y if and only if xRy .

Another way to represent the relation R is the **adjacency table**.

Rows and columns are labeled by elements of X . We put 1 at the intersection of a row x with a column y if xRy . Otherwise we put 0.



	a	b	c
a	0	1	1
b	0	1	1
c	1	0	0



	a	b	c	d	e
a	0	1	1	0	0
b	0	1	1	0	0
c	0	0	0	1	0
d	0	0	0	0	1
e	1	0	0	0	0

Properties of relations

Definition. Let R be a relation on a set X . We say that R is

- **reflexive** if xRx for all $x \in X$,
- **symmetric** if, for all $x, y \in X$, xRy implies yRx ,
- **antisymmetric** if, for all $x, y \in X$, xRy and yRx cannot hold simultaneously,
- **weakly antisymmetric** if, for all $x, y \in X$, xRy and yRx imply that $x = y$,
- **transitive** if, for all $x, y, z \in X$, xRy and yRz imply that xRz .

Partial ordering

Definition. A relation R on a set X is a **partial ordering** (or **partial order**) if R is reflexive, weakly antisymmetric, and transitive:

- xRx ,
- xRy and $yRx \implies x = y$,
- xRy and $yRz \implies xRz$.

A relation R on a set X is a **strict partial order** if R is antisymmetric and transitive:

- $xRy \implies \text{not } yRx$,
- xRy and $yRz \implies xRz$.

Examples. “is less than or equal to”, “is contained in”, “is a divisor of” are partial orders. “is less than” is a strict order.

Equivalence relation

Definition. A relation R on a set X is an **equivalence relation** if R is reflexive, symmetric, and transitive:

- xRx ,
- $xRy \implies yRx$,
- xRy and $yRz \implies xRz$.

Examples. “is equal to”, “is congruent modulo n to” are equivalence relations.

Given an equivalence relation R on X , the **equivalence class** of an element $x \in X$ relative to R is the set of all elements $y \in X$ such that yRx .

Theorem The equivalence classes form a **partition** of the set X , which means that

- any two equivalence classes either coincide, or else they are disjoint,
- any element of X belongs to some equivalence class.

Functions

A **function** (or **map**) $f : X \rightarrow Y$ is an assignment: to each $x \in X$ we assign an element $f(x) \in Y$.

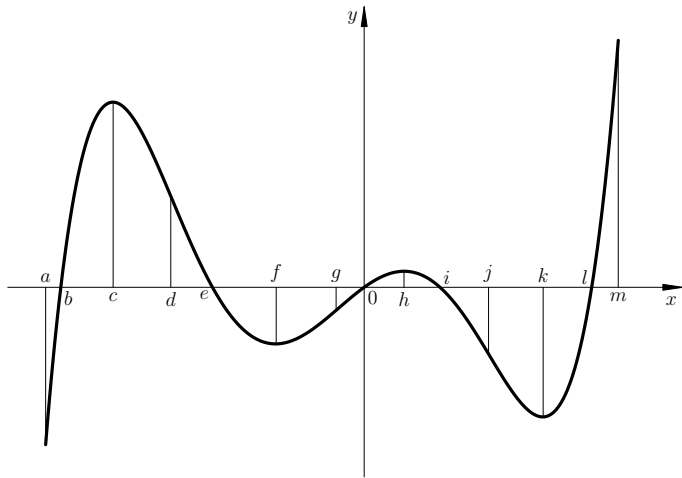
Definition. A function $f : X \rightarrow Y$ is **injective** (or **one-to-one**) if $f(x') = f(x) \implies x' = x$.

The function f is **surjective** (or **onto**) if for each $y \in Y$ there exists at least one $x \in X$ such that $f(x) = y$.

Finally, f is **bijective** if it is both surjective and injective. Equivalently, if for each $y \in Y$ there is exactly one $x \in X$ such that $f(x) = y$.

Suppose we have two functions $f : X \rightarrow Y$ and $g : Y \rightarrow X$. We say that g is the **inverse function** of f (denoted f^{-1}) if $y = f(x) \iff g(y) = x$ for all $x \in X$ and $y \in Y$.

Theorem The inverse function f^{-1} exists if and only if f is bijective.



Definition. The **composition** of functions $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ is a function from X to Z , denoted $g \circ f$, that is defined by $(g \circ f)(x) = g(f(x))$, $x \in X$.

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

Properties of compositions:

- If f and g are one-to-one, then $g \circ f$ is also one-to-one.
- If $g \circ f$ is one-to-one, then f is also one-to-one.
- If f and g are onto, then $g \circ f$ is also onto.
- If $g \circ f$ is onto, then g is also onto.
- If f and g are bijective, then $g \circ f$ is also bijective.
- If f and g are invertible, then $g \circ f$ is also invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
- If id_Z denotes the identity function on a set Z , then $f \circ \text{id}_X = f = \text{id}_Y \circ f$ for any function $f : X \rightarrow Y$.
- For any functions $f : X \rightarrow Y$ and $g : Y \rightarrow X$, we have $g = f^{-1}$ if and only if $g \circ f = \text{id}_X$ and $f \circ g = \text{id}_Y$.