MATH 433

Applied Algebra

Lecture 14:
Sets and functions.
Relations.

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: paradoxes

Suppose $\mathcal{U}$ is the set of all sets. Let $\mathcal{U}_0 = \{X \in \mathcal{U} \mid X \notin X\}$, the subset of all sets that are not their own elements.

Question (Russell 1901) Is $\mathcal{U}_0$ an element of itself?

One way to resolve this paradox: not every collection of elements is a set!

Logical paradox behind Russell's paradox: "This statement is false." Less obvious paradox: "This statement is true."

Uncontrolled self-reference can be bad! A more general issue is chain-reference.

Statement on the right is true	Statement on the left is false

Axiom of foundation: Every non-empty set X contains an element Y that is disjoint from X.

Theorem For any two sets X and Y, if $X \in Y$ then $Y \notin X$.

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 $\varnothing$, 1 is $\{\varnothing\}$, 2 is $\{\varnothing, \{\varnothing\}\}$, 3 is $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, 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 $|X \times Y| = |X| \cdot |Y|$, where $|S|$ denotes 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 $x = y$.

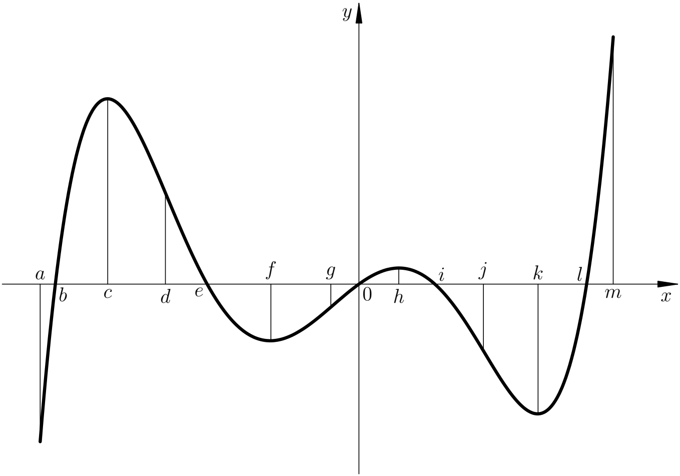
Functions

A **function** (or **map**) $f : X \to Y$ is an assignment: to each $x \in X$ we assign an element $f(x) \in Y$. The set X is called the **domain** of f. The set Y is called the **codomain** of f.

If $y = f(x)$ for some $x \in X$ and $y \in Y$, then y is the **image** of x under f while x is a **pre-image** of y under f. The **pre-image** of y under f can also refer to the set $\{x \in X \mid f(x) = y\}$, denoted $f^{-1}(y)$, which consists of all pre-images of y in the former sense.

Given $X_0 \subset X$, the set $\{f(x) \mid x \in X_0\}$, denoted $f(X_0)$, is called the **image** of the set X_0 under f. The image $f(X)$ of the entire domain is simply called the **image** of the function f. Given $Y_0 \subset Y$, the set $\{x \in X \mid f(x) \in Y_0\}$, denoted $f^{-1}(Y_0)$, is called the **pre-image** of the set Y_0 under f.

The **range** of the function f means either the codomain of f or the image of f (depending on an author).


y
x
a
b
c
d
e
f
g
0
h
i
j
k
l
m

Properties of functions

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

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 $f(x) = y$.

Theorem If X is a finite set and $f : X \to X$ is a function, then: f is injective $\iff$ f is surjective $\iff$ f is bijective.

Suppose we have two functions $f : X \to Y$ and $g : Y \to X$. 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 $f : X \to Y$ and $g : Y \to Z$ 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 $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f$ for any function $f : X \to Y$.
- For any functions $f : X \to Y$ and $g : Y \to X$, we have $g = f^{-1}$ if and only if $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.

Examples

- $f : \mathbb{N} \to \mathbb{N}, \;\; f(x) = x + 1$ for all $x \in \mathbb{N}$.

The function f is injective but not surjective. This is not possible for a map of a finite set to itself.

- $f : [0, \infty) \to \mathbb{R}, \;\; f(x) = \sqrt{x}$ for all $x \geq 0$;

$g : \mathbb{R} \to [0, \infty), \;\; g(x) = x^2$ for all $x \in \mathbb{R}$.

The function f is injective but not surjective. The function g is surjective but not injective. The composition $g \circ f$ is bijective since $g \circ f = \mathrm{id}_{[0,\infty)}$.

- $f : [0, \infty) \to [0, \infty), \;\; f(x) = \sqrt{x}$ for all $x \geq 0$;

$g : [0, \infty) \to [0, \infty), \;\; g(x) = x^2$ for all $x \geq 0$.

The only difference from the previous example is a change of domains and codomains. But this time both f and g are bijective functions, and so is $g \circ f$.

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 $f : X \to Y$ 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 $f : X \to Y$ 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'
$xRy \iff$ 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"

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

- "is less than or equal to"

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

- "is contained in"

$X =$ the set of all subsets of some set Y,
$xRy \iff x \subset y$

- "is congruent modulo n to"

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

- "divides"

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