MATH 415
Modern Algebra I

Lecture 1:
Preliminaries.

Cartesian product

Definition. The **Cartesian product** $X \times Y$ of two sets X and Y is the set 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.

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"

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

- "divides"

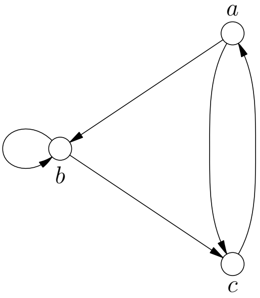
$X = \mathbb{P}, \;\; xRy \iff x|y$

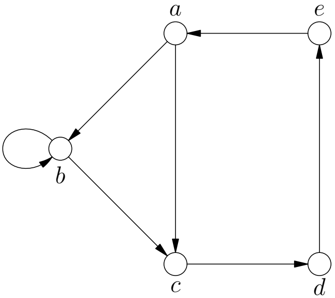
A relation R on a finite set X can be represented by a **directed graph**.

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:

- $xRy \implies$ 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**) $f : X \to Y$ is an assignment: to each $x \in X$ we assign an element $f(x) \in Y$.

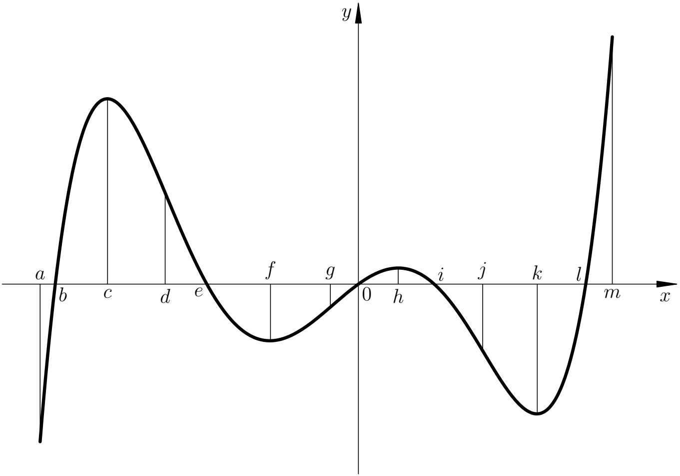
Definition. A function $f : X \to Y$ is **injective** (or **one-to-one**) if $f(x') = f(x) \implies x' = x$.

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 $f : X \to Y$ 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.



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

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 $f \circ g = \mathrm{id}_Y$.

Cardinality of a set

Definition. Given two sets A and B, we say that A is of the same **cardinality** as B if there exists a bijective function $f : A \to B$. Notation: $|A| = |B|$.

Theorem The relation "is of the same cardinality as" is an equivalence relation, i.e., it is reflexive ($|A| = |A|$ for any set A), symmetric ($|A| = |B|$ implies $|B| = |A|$), and transitive ($|A| = |B|$ and $|B| = |C|$ imply $|A| = |C|$).

Proof: The identity map $\mathrm{id}_A : A \to A$ is bijective. If f is a bijection of A onto B, then the inverse map f^{-1} is a bijection of B onto A. If $f : A \to B$ and $g : B \to C$ are bijections then the composition $g \circ f$ is a bijection of A onto C.

Countable and uncountable sets

A nonempty set is **finite** if it is of the same cardinality as $\{1, 2, \dots, n\} = [1, n] \cap \mathbb{N}$ for some $n \in \mathbb{N}$. Otherwise it is **infinite**.

An infinite set is called **countable** (or **countably infinite**) if it is of the same cardinality as $\mathbb{N}$. Otherwise it is **uncountable** (or **uncountably infinite**).

An infinite set E is countable if it is possible to arrange all elements of E into a single sequence (an infinite list) $x_1, x_2, x_3, \dots$ The sequence is referred to as an **enumeration** of E.

Countable sets

- $2\mathbb{N}$: even natural numbers.

Bijection $f : \mathbb{N} \to 2\mathbb{N}$ is given by $f(n) = 2n$.

- $\mathbb{N} \cup \{0\}$: nonnegative integers.

Bijection $f : \mathbb{N} \to \mathbb{N} \cup \{0\}$ is given by $f(n) = n - 1$.

- $\mathbb{Z}$: integers.

Enumeration of all integers: $0, 1, -1, 2, -2, 3, -3, \dots$
Equivalently, a bijection $f : \mathbb{N} \to \mathbb{Z}$ is given by $f(n) = n/2$ if n is even and $f(n) = (1-n)/2$ if n is odd.

- $E_1 \cup E_2$, where E_1 is finite and E_2 is countable.

First we list all elements of E_1. Then we append the list of all elements of E_2. If E_1 and E_2 are not disjoint, we also need to avoid repetitions in the joint list.

Countable sets

- $E_1 \cup E_2$, where E_1 and E_2 are countable.

Let $x_1, x_2, x_3 \ldots$ be an enumeration of E_1 and $y_1, y_2, y_3, \ldots$ be an enumeration of E_2. Then $x_1, y_1, x_2, y_2, \ldots$ enumerates the union (maybe with repetitions).

- Infinite set $E_1 \cup E_2 \cup \ldots$, where each E_n is finite.

First we list all elements of E_1. Then we append the list of all elements of E_2. Then we append the list of all elements of E_3, and so on... (and do not forget to avoid repetitions).

- $\mathbb{N} \times \mathbb{N}$: pairs of natural numbers

- $\mathbb{Q}$: rational numbers

- Algebraic numbers (roots of nonzero polynomials with integer coefficients).

Theorem (Cantor) The set $\mathbb{R}$ is uncountable.

Proof: It is enough to prove that the interval $(0,1)$ is uncountable. Assume the contrary. Then all numbers from $(0,1)$ can be arranged into an infinite list $x_1, x_2, x_3, \dots$ Any number $x \in (0,1)$ admits a decimal expansion of the form $0.d_1d_2d_3\dots$, where each $d_i \in \{0,1,\dots,9\}$. In particular,

$$x_1 = 0.d_{11}d_{12}d_{13}d_{14}d_{15}\dots$$
$$x_2 = 0.d_{21}d_{22}d_{23}d_{24}d_{25}\dots$$
$$x_3 = 0.d_{31}d_{32}d_{33}d_{34}d_{35}\dots$$

. . . .

Now for any $n \in \mathbb{N}$ choose a decimal digit $\tilde{d}_n$ such that $\tilde{d}_n \neq d_{nn}$ and $\tilde{d}_n \notin \{0,9\}$. Then $0.\tilde{d}_1\tilde{d}_2\tilde{d}_3\dots$ is the decimal expansion of some number $\tilde{x} \in (0,1)$. By construction, it is different from all expansions in the list. Although some real numbers admit two decimal expansions (e.g., $0.50000\dots$ and $0.49999\dots$), the condition $\tilde{d}_n \notin \{0,9\}$ ensures that $\tilde{x}$ is not such a number. Thus $\tilde{x}$ is not listed, a contradiction.

Uncountable sets

- Any interval (a, b) is of the same cardinality as $(0, 1)$.

Bijection $f : (0, 1) \to (a, b)$ is given by $f(x) = (b - a)x + a$.

- All intervals of the form (a, b) have the same cardinality.

Follows by transitivity since they are all of the same cardinality as $(0, 1)$.

- All intervals of the form (a, ∞) or $(-\infty, a)$ are of the same cardinality as $(0, \infty)$.

Bijection $f : (0, \infty) \to (a, \infty)$ is given by $f(x) = x + a$.
Bijection $f : (0, \infty) \to (-\infty, a)$ is given by $f(x) = -x + a$.

Uncountable sets

- $(0,1)$ is of the same cardinality as $(1,\infty)$.

Bijection $f:(0,1)\to(1,\infty)$ is given by $f(x)=x^{-1}$.

- $(0,\infty)$ is of the same cardinality as $\mathbb{R}$.

Bijection $f:\mathbb{R}\to(0,\infty)$ is given by $f(x)=e^x$.

- $[0,1]$ is of the same cardinality as $(0,1)$.

Let $x_1,x_2,x_3,\dots$ be a sequence of distinct points in $(0,1)$, say, $x_n=(n+1)^{-1}$ for all $n\in\mathbb{N}$. Then a bijection $f:[0,1]\to(0,1)$ is defined as follows: $f(0)=x_1$, $f(1)=x_2$, $f(x_n)=x_{n+2}$ for all $n\in\mathbb{N}$, and $f(x)=x$ otherwise.