MATH 415

Modern Algebra I

Lecture 2:
Cardinality of a set (continued).
Binary operations.

Countable and uncountable sets

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: $|A| = |B|$.

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

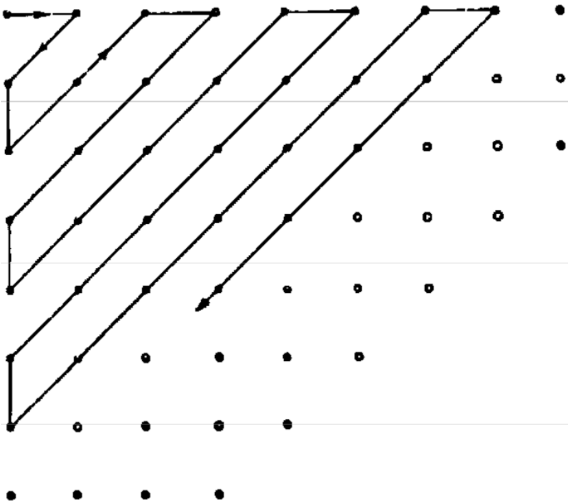
- Infinite set $E_1 \cup E_2 \cup \dots$, where each E_n is finite.

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).



Enumeration of $\mathbb{N} \times \mathbb{N}$

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 $0.d_1 d_2 d_3 \dots$, where each $d_i \in \{0, 1, \dots, 9\}$. In particular,

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

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.

How to compare cardinalities?

Definition. Given two sets A and B, we say that the cardinality of A is **less than or equal to** the cardinality of B (and write $|A| \preceq |B|$) if the set A is of the same cardinality as some subset of B. An equivalent condition is that there exists an injective function $f : A \to B$.

We say that the cardinality of A is **less than** the cardinality of B (and write $|A| \prec |B|$) if $|A| \preceq |B|$ and $|A| \neq |B|$.

Proposition (i) If $|A| \preceq |B|$ and $|B| \preceq |C|$, then $|A| \preceq |C|$.
(ii) If $|A| \prec |B|$ and $|B| \prec |C|$, then $|A| \prec |C|$.

Theorem (Schröder-Bernstein) If $|A| \preceq |B|$ and $|B| \preceq |A|$, then $|A| = |B|$.

Hence $\preceq$ (or $\prec$) is an ordering of cardinalities. Moreover, this ordering is **total**, i.e., any two cardinalities are comparable.

Theorem For any two sets A and B, we have either $|A| \prec |B|$ or $|B| \prec |A|$ or $|A| = |B|$.

Binary operations

Definition. A **binary operation** $*$ on a nonempty set S is simply a function $*: S \times S \to S$.

The usual notation for the element $*(x, y)$ is $x * y$.

The pair $(S, *)$ is called a **binary algebraic structure**.

"Structures are the weapons of the mathematician."

Nicholas Bourbaki

Examples: arithmetic operations

Addition $+$ of:

natural numbers, integers, rationals, real numbers, complex numbers, vectors, matrices of fixed dimensions, real-valued functions with fixed domain.

Subtraction $-$ of:

all above examples with addition except for natural numbers.

Multiplication $\times$ of:

natural numbers, integers, rationals, real numbers, complex numbers, square matrices of fixed dimensions, real-valued functions with fixed domain.

Division $/$ of:

positive rationals, nonzero rationals, positive real numbers, nonzero real numbers, nonzero complex numbers, nonzero rational functions.

Examples: addition modulo n

Given a natural number n, let $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.

A binary operation $+_n$ (**addition modulo** n) on $\mathbb{Z}_n$ is defined for any $x, y \in \mathbb{Z}_n$ by

$$x +_n y = \begin{cases} x + y & \text{if } x + y < n, \\ x + y - n & \text{if } x + y \geq n. \end{cases}$$

Now let n be a positive real number and $\mathbb{R}_n = [0, n)$. The binary operation $+_n$ on $\mathbb{R}_n$ is defined by the same formula as above.

Remark. The binary structure $(\mathbb{R}_{2\pi}, +_{2\pi})$ is an abstract model for rotations of a circle.

Examples: composition of functions

Let $F(X,X)$ denote the set of all functions $f : X \to X$. Given two functions $f, g \in F(X,X)$, the composition $f \circ g$ is another function in $F(X,X)$ defined by $(f \circ g)(x) = f(g(x))$, $x \in X$.

Then $\circ$ is a binary operation on the following subsets of $F(X,X)$:

- all functions,
- all invertible functions,
- all injective functions,
- all surjective functions.

Examples: set theory

$\mathcal{P}(X)$ = the set of all subsets of some set X.

Binary operations on $\mathcal{P}(X)$:

- union $A \cup B$,
- intersection $A \cap B$,
- set difference $A \setminus B$,
- symmetric difference $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Examples: logic

Binary logic $\mathcal{L} = \{\text{“true”}, \text{“false”}\}$.

Binary operations on $\mathcal{L}$:

- logical AND,
- logical OR,
- XOR (eXclusive OR),
- $\Longrightarrow$,
- $\Longleftarrow$,
- $\Longleftrightarrow$.

Overall, there are $2^{2 \cdot 2} = 16$ distinct binary operations on any set consisting of two elements.

Counterexamples

- Reciprocal of a positive number.

$S = \mathbb{R}^+,\ *(x) = x^{-1}.$

This operation is unary, not binary.

- Mean arithmetic value of three numbers.

$$S = \mathbb{R},\ *(x, y, z) = \frac{x + y + z}{3}.$$

This operation is ternary, not binary.

- Division of real numbers.

$S = \mathbb{R},\ x * y = x/y.$

The operation is only partially defined as one cannot divide by 0.

Counterexamples

- Division of natural numbers.

$S = \mathbb{N},\ x * y = x/y.$

The operation is not well defined as $x * y$ is not always an integer.

- Solution of a quadratic equation.

$S = \mathbb{C},\ (x * y)^2 + x(x * y) + y = 0.$

The operation is not defined uniquely as the equation can have two solutions. In other words, this is not a function.

Restriction

Suppose $(S, *)$ is a binary structure. If S_0 is a nonempty subset of S then we can restrict $*$, as a function, from $S \times S$ to $S_0 \times S_0$.

If the restricted function is a binary operation on S_0 then we call it the **restriction** of the operation to S_0 and use the same notation $*$.

The restricted function is a binary operation on S_0 if and only if the subset S_0 is **closed under the operation** $*$ which means that $x, y \in S_0$ implies $x * y \in S_0$. Otherwise the restricted operation is not well defined.

Useful properties of binary operations

Suppose $(S, *)$ is a binary structure.

- Commutativity:

$g * h = h * g$ for all $g, h \in S$.

- Associativity:

$(g * h) * k = g * (h * k)$ for all $g, h, k \in S$.

- Existence of the identity element:

there exists an element $e \in S$ such that $e * g = g * e = g$ for all $g \in S$.

- Existence of the inverse element:

for any $g \in S$ there exists an element $h \in S$ such that $g * h = h * g = e$ (where e is the identity element).

- Cancellation:

$g * h_1 = g * h_2$ implies $h_1 = h_2$ and $h_1 * g = h_2 * g$ implies $h_1 = h_2$ for all $g, h_1, h_2 \in S$.

Cayley table

A binary operation on a finite set can be given by a **Cayley table** (i.e., “multiplication” table):

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The Cayley table is convenient to check commutativity of the operation (the table should be symmetric relative to the diagonal), cancellation properties (left cancellation holds if each row contains all elements, right cancellation holds if each column contains all elements), existence of the identity element, and existence of the inverse.

However this table is not convenient to check associativity of the operation.

Problem. The following is a partially completed Cayley table for a certain commutative operation with cancellation:

$*$	a	b	c	d
a	b			c
b			c	
c				a
d		d		

Complete the table.

Solution:

$*$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b