Sets

June 23, 2021 7:45 PM

Definition: as set is a collection of objects. These objects are called the elements of the set
Notation: $\mathbb{N} = \{1,2,3, \ldots\}$, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, $\mathbb{R}$ =all real number.
Remark: two sets are equal if they have the same elements

Empty set: $\emptyset = \{\square\}$.

Set builder notation

- Set of all even natural numbers= $\{2n: n \; is \; a \; number \; of \; \mathbb{N}\} = \{2n: n \in \mathbb{N}\}$
- For A a set and x an element of A, write $x \in A$.

Special kind of sets: intervals in $\mathbb{R}$

- $\{x \in \mathbb{R}, 0 \leq x \leq 8\} = [0,8]$.
- $\{x \in \mathbb{R}, 0 < x < 8\} = (0,8)$.
- $\{x \in \mathbb{R}, 0 < x \leq 8\} = (0,8] =]0,8]$.
- $\{x \in \mathbb{R}, 0 \leq x < 8\} = [0,8) = [0,8[$
- $\emptyset$ is also an interval of $\mathbb{R}$.

Subset

- Let X, Y be sets, we say X is a subset of Y and write $X \subset Y$ when $\forall x \in Y$, we have $x \in Y$.
- For any set Y, $\emptyset \subset Y$.

Well ordering principle

- Definition: Let S be a set of numbers, let $a \in S$, a is the smallest element of S if $\forall s \in S$, we have $s \geq a$.
  - $\mathbb{Z}$ does not have a smallest element.
  - $\mathbb{N}$ does not have a smallest element.
- A set S of real number is well ordered if any non-empty subset of S has a smallest element.
  - $\mathbb{N}$ is well ordered.
  - $[0,1]$ is not well ordered.
  - Any non empty subset of $\mathbb{Z}$ which is bounded below is well ordered

Power set

- Let X be a set, the power set of X denoted by $P(X)$ is $P(X) = \{Y: Y \subset X\}$
- It is a set of sets
- Lemma: $|X| = n \Rightarrow |P(X)| = 2^n$.

Set operations

- Union: $A \cup B = \{x: x \in A \; or \; x \in B\}$
- Intersection: $A \cap B = \{x: x \in A \; and \; x \in B\}$
- Difference: $A \backslash \mathrm{B} = A - B = \{x: x \in A \; and \; x \notin B\}$
- Complement:
  - Fix a universe U or Ω.
  - For $A \subset \Omega$, we call complement of A and denote by $\overline{A}$ the set $\overline{A} = \{x \in \Omega: x \notin A\}$.
- Cartesian product
  - Let A and B be 2 sets, the cartesian product of A and B is $A \times B = \{(a, b): a \in A, b \in B\}$.

Proofs involving sets

- Let A and B be two sets
- To prove $A \subset B$, we have to prove if $a \in A$, then $a \in B$.
- To prove $A = B$, we have to prove $A \subset B$ and $B \subset A$, i.e. $a \in A$ if and only if $a \in B$.

Identities

- $\overline{\overline{A}} = A$.
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Statements and proves

June 24, 2021 8:53 AM

Statements: a statement is a claim that is either true or false
Direct proof: proof of conditional statement in direct style

Modify, combine statements (logic operations)

- Negation
  - Notation: $\neg P$, $\sim P$.
  - $\neg P$ is true, if P is false.
  - $\neg(\neg P)$ and P have the same truth values, they are logically equivalent.
  - not all= at least one
- And
  - Notation: $P \wedge Q$.
  - $P \wedge Q = Q \wedge P$.
  - $P \wedge Q$ is true if and only if both P and Q are true.
- Or
  - Notation: $P \vee Q$.
  - $\neg(P \vee Q) = \neg P \wedge \neg Q$.
  - $\neg(P \wedge Q) = \neg P \vee \neg Q$.

Conditional statement

- Given statements P and Q, consider the statement if P then Q.
- Notation: $P \Rightarrow Q$.
- It is equivalent to $\neg P \vee Q$.
- $\neg(P \Rightarrow Q) = P \wedge \neg Q$.

Biconditional statements ($\Leftrightarrow$)

- Let P and Q be 2 statements, we consider the statement $P \Rightarrow Q$ and $Q \Rightarrow P$.
- Notation: $P \Leftrightarrow Q$ (P if and only if Q)
- To prove biconditional statements, need to prove both $P \Rightarrow Q$ and $Q \Rightarrow P$.
- To prove $A \Leftrightarrow B \Leftrightarrow C$, it is equivalent to prove $A \Rightarrow B \Rightarrow C \Rightarrow A$.

Contrapositive

- The contrapositive of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$.
- They are logically equivalent

Quantifiers

- There exists $\exists$
- For all $\forall$
- Such that :
- Negation of $\forall x \in A, P(x)$ is $\exists x \in A, \neg P(x)$.
- Negation of $\exists x \in A, P(x)$ is $\forall x \in A, \neg P(x)$.

Disproof

- if I have a statement of the form $\forall x \in X$, $P(x)$, I can disprove it if I prove the negation is true, namely, $\exists x \in X$, $\neg P(x)$.
- if I have a statement of the form $\exists x \in X$, $P(x)$, I can disprove it if I prove the negation is true, namely, $\forall x \in X$, $\neg P(x)$.

Induction

- Questions are in the form: Prove the statement for all $n \in \mathbb{N}$, or all $n \in \mathbb{Z}$, $n \geq b$.
- Base step: prove that $P(b)$ or $P(1)$ is true.
- Induction step: prove that $\forall n \geq b$ or $n \geq 1$, $P(n) \Rightarrow P(n+1)$.

Double induction

- Prove $P(n)$ for all $n \in \mathbb{N}$.
- Base step: prove $P(1)$ and $P(2)$.
- Induction step: $\forall n \in \mathbb{N}$, prove $P(n) \wedge P(n+1) \Rightarrow P(n+2)$.

Definition (even, odd, divisors, prime/composite numbers):

- Let $x \in \mathbb{Z}$, x is called even if there exists $y \in \mathbb{Z}$ such that $x = 2y$
- Let $x \in \mathbb{Z}$, x is called odd if there exists $y \in \mathbb{Z}$ such that $x = 2y + 1$
- Let $a, b \in \mathbb{Z}$, we say a divides b and write $a|b$ if there exists $c \in \mathbb{Z}$ such that $b = ac$.
    - In this case, we say that b is a multiple of a, a is a divisor of b
- Let $m \in \mathbb{N}$, we say m is a prime number if it has exactly 2 divisors in $\mathbb{N}$, 4 divisors in $\mathbb{Z}$
- Let $n \in \mathbb{N}$, if $n \neq 1$ and is not prime, then it is a composite number.

Fact:

- if $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$, $ab \in \mathbb{Z}$.
- if $a, b \in \mathbb{R}$, then $a + b \in \mathbb{R}$, $a - b \in \mathbb{R}$, $ab \in \mathbb{R}$.
    - If $b \neq 0, \frac{a}{b} \in \mathbb{R}$.

Theorem(Euclidean division algorithm): Let $a, b \in \mathbb{Z}$, such that $b \neq 0$, there exists a unique $q \in \mathbb{Z}$ (quotient) and a unique $r \in \mathbb{Z}$ (remainder), such that $0 \leq r < b$ and $a = bq + r$.

- q and r are unique.
- Let $n \in \mathbb{Z}$, if the remainder of the Euclidean division of n by 2 is 0, then n is even.
- Let $n \in \mathbb{Z}$, if the remainder of the Euclidean division of n by 2 is 1, then n is odd.

Definition:

- GCD(greatest common divisor): let $a, b \in \mathbb{Z}$, suppose they are not both zero, we call the greatest common divisor of a and b and we denote by $\gcd(a, b)$ the greatest integer that divides both a and b.
    - $\gcd(a, b) \geq 1$.
- Let $a, b \in \mathbb{Z}$, with $a \neq 0$ and $b \neq 0$, we call the lowest common multiple of a and b, and we denote by $lcm(a, b)$ the smallest natural number that is a multiple of both a and b.

Congruences

- Definition: Let $a, b, n \in \mathbb{Z}$, suppose $n \neq 0$, we say a and b are congruent mod n, or a is congruent to b mod n, and write $a \equiv b \ mod\ n$ or $b \equiv a \ mod\ n$ when $n|(a - b)$.
- Note: $a \equiv 0 \ mod\ n \Leftrightarrow n|a$.
- Proposition: let $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{Z}$ with $n \neq 0$.
    - If $a \equiv b \ mod\ n$ and $b \equiv c \ mod\ n$, then $a \equiv c \ mod\ n$.
    - If $a \equiv b \ mod\ n$ and $c \equiv d \ mod\ n$, then $a + c \equiv b + d \ mod\ n$.
    - If $a \equiv b \ mod\ n$ and $c \equiv d \ mod\ n$, then $ac \equiv bd \ mod\ n$.
- Let $a \in \mathbb{Z}$, $n \in \mathbb{Z}$, $n \neq 0$ Euclidean division of a by n: $a = nq + r$ where $q, r \in \mathbb{Z}$, $0 \leq r < n$, then $a \equiv r \ mod\ n$
- Congruence do not behave well with divisions.
- Remarks
    - $\forall a \in \mathbb{Z}$, $a^2 \equiv 0 \ or\ 1 \ mod\ 3$.
    - $\forall a \in \mathbb{Z}$, $a^2 \equiv 0 \ or\ 1 \ mod\ 4$.

Limits and sequences of real numbers

- Notation: sequence $(u_n)_{n \in \mathbb{N}}$.
- We say $(u_n)_{n \in \mathbb{N}}$ is bounded if $\exists m, M \in \mathbb{R}$ such that $\forall n \in \mathbb{N}$, $m \leq u_n \leq M$.
    - We say $(u_n)_{n \in \mathbb{N}}$ is bounded above if $\exists M \in \mathbb{R}$ such that $\forall n \in \mathbb{N}$, $u_n \leq M$.
    - We say $(u_n)_{n \in \mathbb{N}}$ is bounded below if $\exists m \in \mathbb{R}$ such that $\forall n \in \mathbb{N}$, $u_n \geq m$.
- We say $(u_n)_{n \in \mathbb{N}}$ converges to a real number l when $\forall \epsilon > 0$, $\exists m \in \mathbb{N}$ such that $\forall n \in \mathbb{N}$, $n \geq m \Rightarrow |u_n - l| < \epsilon$.

- We say $\left(u_n\right)_{n\in\mathbb{N}}$ converges towards ∞ when $\forall A > 0$, $\exists m \in \mathbb{N}$ such that $\forall n \in \mathbb{N}, n \geq m \Rightarrow u_n > A$.
- We say $\left(u_n\right)_{n\in\mathbb{N}}$ converges towards $-\infty$ when $\forall B < 0$, $\exists m \in \mathbb{N}$ such that $\forall n \in \mathbb{N}, n \geq m \Rightarrow u_n < B$.

Lemma: $\forall n \in \mathbb{N}$, $\exists x \in \mathbb{N}$ such that $\frac{n}{2^{x-1}}$ is odd.

Rational numbers:

- A rational number is a real number x that can be written as $x = \frac{a}{b}$, for $a \in \mathbb{Z}, b \in \mathbb{N}$.
- Simplify the fraction: can always pick a and b such that $\gcd(a, b) = 1$.

Relations and functions

June 24, 2021 9:10 AM

Relations

- Let X be a non-empty, a relation on X is a non-empty subset of $X \times X$.
- Notation: given a relation $R \subset X \times X$, we usually write xRy instead of $(x, y) \in R$.
- Properties
  - Reflexivity: a relation R on a set X is reflexive when $\forall x \in X$, xRx
    - To prove R is not reflexive, give an example $x \in X$, such that x is not related to x.
  - Symmetry: a relation R on a set X is symmetric when $\forall x, y \in X$, $xRy \Rightarrow yRx$
    - To prove R is not symmetric, give an example $x, y \in X$, such that xRy but y is not related to x
  - Transitivity: a relation R on a set X is reflexive when $\forall x, y, z \in X$, $xRy \wedge yRz \Rightarrow xRz$

Equivalence relation

- Given a relation R on a set X, we say R is an equivalence relation when R is reflexive, symmetric and transitive
- Given an equivalence relation R on a set X and $x \in X$, we call equivalence class of x the subset of X by $cl(x)$ or $[x]_R$ or $cl_R(x) = \{y \in X: xRy\} = \{y \in X: yRx\}$
- Let C be a subset of X and suppose it is an equivalence class ($\exists x \in X$ such that $C = cl(x)$), then any $y \in C$ is called a representative of the class C, and $C = cl(x) = cl(y)$
- Remark: Given $n \in \mathbb{N}$, the relation on $\mathbb{Z}$, xRy, when $x \equiv y \ mod \ n$ is an equivalence relation with equivalence classes:
  - $[0] = [n] = [-n] = [2n] = \cdots.$
  - $[1] = [n+1] = [-2n+1] = \cdots.$
  - $[n-1] = [2n-1] = [-1] = \cdots.$

Partitions and equivalence relations

- Let X be a non empty set and P is a set of subsets of X, $P = \{X_\alpha: \alpha \in A\}$, where A is a set of α, such that $X_\alpha \subset X$.
- P is a partition of X where
  - $X_\alpha \neq \emptyset, \forall \alpha \in A.$
  - $X_\alpha \cap X_\beta \neq \emptyset \Rightarrow X_\alpha = X_\beta, \alpha = \beta.$
  - $X = \cup_{\alpha \in A} X_\alpha.$
- If R is an equivalence relation on X, the collection of all equivalence classes give a partition on X

Functions

- Let A, B be two non-empty sets, a function f is a subset of $A \times B$ such that $\forall a \in A$, there is a unique ($\exists!$) $b \in B$, such that $(a, b) \in f$, this b is usually called $f(a)$.
- Write $f: A \to B$, $f(a) = b$
  - A is the domain/source space of f.
  - B is the codomain/target space of f.
- Define: $Range(f) = \{b \in B: \exists a \in A \ such \ that \ f(a) = b\} = \{f(a): a \in A\} \subset B.$
- f is surjective or onto if $Range(f) = B$, i.e. $\forall b \in B, \exists a \in A: f(a) = b.$
- f is injective or one-to-one if $\forall a, a' \in A$, $f(a) = f(a') \Rightarrow a = a'.$
  - Or $\forall a, a' \in A$, $a \neq a' \Rightarrow f(a) \neq f(a').$
- If f is injective and surjective, then it is bijective, we call it a bijection

Cardinality of finite sets and functions

- Suppose A and B are finite sets, $f: A \to B$.
- If f is injective, then $|A| \leq |B|$
- If f is surjective, then $|A| \geq |B|$
- If f is bijective, then $|A| = |B|$
  - Remark: we say 2 sets A and B have the same cardinality if $\exists f: A \to B$ which is bijective.

Composing functions

- Let $g: A \to B$, $f: B \to C$, consider the function $f \circ g: A \to C$, $\forall a \in A, f \circ g(a) = f\big(g(a)\big)$.
- Lemma:
  - If $f \circ g$ is injective, then g is injective.
  - If $f \circ g$ is surjective, then f is surjective.

Image and preimage

- Let $f: A \to B$ and $a \in A$, we call $f(a)$ the image of a by f
- Let $X \subset A$, we call image of X by f the subset $f(x)$ of B defined by $f(X) = \{f(x): x \in X\}$.
  - $Range(f) = f(A)$.
- Let $Y \subset B$, we call preimage of Y by f the subset $f^{-1}(Y) \subset A$.
- For any $f: A \to B$, any $X \subset A$, $X \subset f^{-1}\big(f(X)\big)$.
  - If f is injective, then $\forall X \subset A, X = f^{-1}\big(f(X)\big)$.

Inverse function

- Let A, B be sets, the function $f: A \to A$ $f(a) = a$ is called the identity function of A. It is denoted by id_A or simply id when there is no ambiguity
- Let $f: A \to A$, then f is bijective $\Leftrightarrow \exists \tilde{f}: A \to A$, such that $f \circ \tilde{f} = \tilde{f} \circ f = id_A$.

Let $f: A \to B$ be a function

- Let $X \subset A$, $y \in f(X)$ means $\exists x \in X, y = f(x)$.
- Let $Y \subset B$, $x \in f^{-1}(Y)$ means $f(x) \in Y$.

Counting

- Given A, B two sets, we say that A and B have the same cardinality and we write $|A| = |B|$ when $\exists f: A \to B$ a bijection
  - $\exists f: A \to B$ a bijection $\Leftrightarrow \exists g: B \to A$ a bijection ($g = f^{-1}$).
- Let A be a set
  - A is finite, if $A = \emptyset$ or $\exists n \in \mathbb{N}$ such that $|A| = \big|\{1,2,3, \dots, n\}\big|$, in this case, A has cardinality n, we write $|A| = n$.
    - If A and B are finite, then $A \times B$ is finite, $C \subset A$ is finite and $A \cup B$ is finite
  - A is countably infinite if $|A| = |\mathbb{N}|$, namely $\exists f: \mathbb{N} \to A$ a bijection.
    - It means $A = \{f(1), f(2), \dots\}$.
    - $|\mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.
    - Since $\mathbb{Q} \subset \mathbb{N} \times \mathbb{Z}$, Q is countably infinite.
    - If A and B are countably infinite, then $A \times B$ and $A \cup B$ countably infinite, $C \subset A$ can be finite or countably infinite.
    - If $|A| = |B| = |\mathbb{N}|$ then $|A \cup B| = |A \times B| = |\mathbb{N}|$, $|C| = |\mathbb{N}|$ if C is an infinite subset of A.
  - A set A is countable if A is finite or countably infinite.
    - Equivalently $\exists f: A \to \mathbb{N}$, injective.
    - Equivalently $\exists f: \mathbb{N} \to A$, surjective.

Comparing cardinalities

- A, B are sets, $|A| \leq |B|$ if $\exists f: A \to B$ injective.
- If $A \subset B$, then $|A| \leq |B|$.
- If $|A| = |B|$, then $|A| \leq |B|$.
- If $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$ (if f and g are injective, then $f \circ g$ is injective).
- If $|A| \leq |B|$ and $|A| \neq |B|$, then $|A| < |B|$ ($f: A \to B$ injective but not bijective).
- $|A| < \big|P(A)\big|$.
  - If $|A| = n$ (finite), then $|A| < |P(A)| \Rightarrow n < 2^n$.
  - Set $U = \big\{\big(a_1, a_2, a_3, \dots\big), a_i \in (0,1)\big\}$ is not countable.
- If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.