

1 Tue 8/25 Discussion

A quick recall:

- (1) union, intersection, complement, subset
- (2) Proper subset: if $A \subsetneq B$ then $\exists x \in B$ such that $x \notin A$.
- (3) Cardinality: number of element in the set, $|\mathcal{S}|$.
- (4) A map $f : A(\text{domain}) \rightarrow B(\text{codomain})$ is called **injective** (one to one) if $x \neq y \implies f(x) \neq f(y)$. Contrapositive: $f(x) = f(y) \implies x = y$. In other words, each element in B correspond to at most one element in A .
- (5) If $f : A \rightarrow B$ is injective then $|A| \leq |B|$.
- (6) A map $f : A \rightarrow B$ is called **surjective** (onto) if $\forall y \in B, \exists x \in A$ such that $f(x) = y$. In other words, each element in B correspond to at least one element in A .
- (7) If $f : A \rightarrow B$ is surjective then $|A| \geq |B|$.
- (8) If a function $A \rightarrow B$ is both injective and surjective then it is **bijective**. In other words, there is a one-to-one *correspondence* (different from the one-to-one adjective for injectivity) between elements in A and B .

Time to play with cardinality: $|\{\text{Even integers}\}| = |\mathbb{Z}|$ because $f(x) := x/2$ is a bijective function with the set of even integers as domain and \mathbb{Z} as codomain. Obviously $\{\text{Even integers}\} \subsetneq \mathbb{Z}$ but they have the same cardinality.

Consider the function $f : \mathbb{N} \rightarrow \mathbb{Z}$ defined by

$$f(x) = \begin{cases} \frac{x}{2}, & x \text{ is even} \\ -\frac{x-1}{2}, & x \text{ is odd} \end{cases}$$

which is a bijection. Therefore $|\mathbb{N}| = |\mathbb{Z}|$.

[†] $\mathbb{N} = \{1, 2, \dots\}$ and it does not include 0.

Definition 1

A **binary relation** \sim is a subset of $\mathcal{S} \times \mathcal{S}$ that may or may not have the following properties:

- (1) **Reflexive:** $x \sim x, \forall x \in \mathcal{S}$.
- (2) **Symmetric:** if $x \sim y$, then $y \sim x, \forall x, y \in \mathcal{S}$.
- (3) **Transitive:** if $x \sim y$ and $y \sim z$, then $x \sim z, \forall x, y, z \in \mathcal{S}$.

If all three are met, then \sim is called an **equivalence relation**.

Example 1.1

Let \sim be $<$. It is not an equivalence relation on \mathbb{Z} : $x < x$ and $x < y \implies y < x$ are both false. It is transitive though: $x < y \wedge y < z \implies x < z$.

Let \sim be congruent modulo 5. This time \sim is indeed an equivalence relation on \mathbb{Z} : $x \sim x$, $x \sim y \implies y \sim x$, and $x \sim y \wedge y \sim z \implies x \sim z$.

Definition 2

Given a set S , its **power set** is defined $\mathbb{P}(S) = \{E \mid E \subset S\}$.

Example 1.2

$$\mathbb{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Remark

$|\mathbb{P}(S)| = 2^{|S|}$. Obvious when S is a finite set: choose or not choose each element; beyond the scope when S is an infinite set.

Problem 1

Suppose that A and B are two subsets of S . Prove that $A \subset B$ if and only if $B^c \subset A^c$.

Solution

Note that $A \subset B$ is the same as the statement $(x \in A \implies x \in B)$, whereas $B^c \subset A^c$ is the same as the statement $x \in B^c \implies x \in A^c$, which is in turn the same as $(x \notin B) \implies (x \notin A)$. Now we've got a pair of contrapositive (in parentheses). One is true if and only if the other is true. Therefore $A \subset B$ if and only if $B^c \subset A^c$.

Problem 2

Prove that there does not exist a surjection f with domain \mathcal{S} and codomain $\mathbb{P}(\mathcal{S})$.

Proof

Suppose f is surjective and consider the set $Y = \{x \in \mathcal{S} : x \notin f(x)\}$. Clearly Y is a subset of \mathcal{S} so it is an element of $\mathbb{P}(\mathcal{S})$. Since f is assumed to be surjective, there must be some $y \in \mathcal{S}$ such that $f(y) = Y$. Now where can y be?

- (1) If $y \in Y$, then by the definition of Y we have $y \notin f(y)$. Since $y \in Y$ but $y \notin f(y)$, we know $Y \neq f(y)$ since they do not have the identical elements.
- (2) On the other hand, if $y \notin Y$, then by the definition of Y we have $y \in f(y)$, which, again, implies $Y \neq f(y)$.

Therefore there is no $y \in \mathcal{S}$ satisfying $f(y) = Y$, namely an element in $\mathbb{P}(\mathcal{S})$ does *NOT* have a pre-image. Hence f is not surjective. Contradiction. \square

2 Wed 8/26

A bunch of stuff about Dedekind cuts and the L.U.B. today:

- (1) The set of all real numbers, \mathbb{R} , is the set of all **Dedekind cuts** in \mathbb{Q} .
- (2) By definition, a Dedekind cut refers to two subsets $A, B \in \mathbb{Q}$ satisfying
 - (1) A has no largest element
 - (2) Every element of A is smaller than any element of B
 - (3) $A \neq \emptyset, B \neq \emptyset$, but $A \cap B = \emptyset$
 - (4) $A \cup B = \mathbb{Q}$

and we may denote a real number as $x = A|B$.

- (3) Any subset $\mathcal{S} \subset \mathbb{R}$ which is nonempty and bounded from above has a least upper bound (L.U.B).
- (4) \mathbb{Z} satisfy the L.U.B property.
- (5) \mathbb{Q} does not satisfy the L.U.B property: consider $\mathcal{S} = \{x \in \mathbb{Q} : x < 0 \text{ or } x^2 < 2\}$. There is no “closest rational number” to $\sqrt{2}$.

(6) Let \mathcal{S} to be such a set. We defined a Dedekind $C|D$ where

$$C := \{x \in \mathbb{Q} : x \in A \text{ for some } A|B \in \mathcal{S}\} \text{ and } D := \mathbb{Q} \setminus C$$

Claim: $C|D$ is a L.U.B. for \mathcal{S} .

(7) Let $S \subset \mathbb{R}$ is a subset. A real number $M \in \mathbb{R}$ is an upper bound for \mathcal{S} if $\forall x \in \mathcal{S}$ we have $x \leq M$. M is a L.U.B. if for any other upper bound M' of \mathcal{S} , we always have $M \leq M'$.

(8) A set with a largest element has the largest element as the L.U.B. A set without a largest element may or may not have a L.U.B: $\mathcal{S}_1 = \{x \in \mathbb{R} \mid x < \sqrt{2}\}$ has L.U.B $\sqrt{2}$ because any real number $< \sqrt{2}$ is smaller than some element in \mathcal{S} . However, $\mathcal{S}_2 = \{x \in \mathbb{Q} \mid x < \sqrt{2}\}$ does not as previously said.

(9) Proving $C|D$ is a L.U.B.:

(1) Show that $C|D$ is an upper bound for \mathcal{S} : for any $A|B \in \mathcal{S}$, we always have $A \subseteq C$. Hence $A|B \leq C|D$ (by definition), and $C|D$ is an upper bound, though probably not the least.

(2) Show that $C|D$ is the least cut satisfying the property in (1). Suppose $C'|D'$ is another upper bound for \mathcal{S} . Try to prove that we always have $C \subseteq C'$. Then it follows that $C|D$ is the least element in the set $\{C'|D'\}$ (the set of *all* upper bounds).

In other words, we break down the word L.U.B. into upper bound and least, and we prove them separately.

(10) Addition of cuts: suppose $x = A|B$ and $y = C|D$, then

$$x + y := E|F \text{ where } E = \{r \in \mathbb{Q} \mid r = a + c, a \in A, c \in C\} \text{ and } F = \mathbb{Q} \setminus E$$

(11) Additive inverse / negation:

$$-x := A'|B' \text{ where } A' = \{b \in B \mid \text{for some } b \in B, \text{ not the smallest element of } B, r = -b\} \text{ and } B' = \mathbb{Q} \setminus A'$$

note that A has no largest element, so $b \in B$ must not be chosen as the smallest element of B .

(12) Positivity: $A|B$ is positive if $A|B > 0^*$.

(13) Multiplication: suppose $x = A|B, y = C|D$, then the product $x \cdot y := E|F$ where

$$E = \{r \in \mathbb{Q} \mid r \leq 0 \text{ or } \exists a \in A \text{ and } c \in C \text{ such that } a > 0, c > 0, \text{ and } r = ac\} \text{ and } F = \mathbb{Q} \setminus E$$

we do this because we have to avoid the product of two negative numbers which produce arbitrarily large numbers.

(14) if x is positive and y is negative, then

$$x \cdot y := -(x \cdot (-y)), \text{ etc.}$$

3 Fri 8/28

More properties of \mathbb{R} and Dedekind cuts:

- (1) Associativity of addition: $x + (y + z) = (x + y) + z$.
- (2) Associativity of multiplication: $x(yz) = (xy)z$.
- (3) Ordering property: $x < y \iff y - x > 0$.
- (4) Transitivity: $x < y \wedge y < z \implies x < z$.
- (5) Trichotomy: exactly one of the following is true: $x < y, x > y, x = y$.
- (6) **Archimedean property**: $\forall x \in \mathbb{R}, \exists$ an integer n such that $n > x$.
- (7) **The ε -principle**: if $a, b \in \mathbb{R}$ and if $a \leq b + \varepsilon$ for any positive real number ε , then $a \leq b$.

Proof

By trichotomy, either $a \leq b$ or $a > b$. Suppose by contradiction that $a > b$. Then pick $0 < \varepsilon < a - b$, and we have $a \leq b + \varepsilon < b + (a - b) = a \implies a < a$ by transitivity. \square

- (8) Absolute value: for $x \in \mathbb{R}$,

$$|x| = \begin{cases} x & \text{if } x \geq 0^* \\ -x & \text{if } x < 0^* \end{cases}$$

- (9) **Triangle inequality** : for $x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$.

Theorem 3

\mathbb{R} is a **complete ordered field** containing \mathbb{Q} as an ordered **subfield**.

Remark

Some informal and formal definitions:

- (1) Field: a set, together with notions of addition and multiplication, with *lots of* compatibilities between these.
- (2) *Field: a nontrivial commutative ring with 1 in which every nonzero element has a multiplicative inverse.
- (3) Complete: has the L.U.B. property.

(4) *Complete(-ness of a metric space): each Cauchy sequence in the metric space converges to a limit inside the same metric space.

Corollary 4

Any other complete ordered field containing \mathbb{Q} as an ordered subfield is **isomorphic** to \mathbb{R} .

Theorem 5

Any Cauchy sequence in \mathbb{R} converges to a limit in \mathbb{R} . (So \mathbb{R} is complete.)

Remark

Not every Cauchy sequence in \mathbb{Q} converges to a limit in \mathbb{Q} . (So \mathbb{Q} is not complete)

Example 3.1

Let $a_1 = 3, a_2 = 3.1, a_3 = 3.14, a_4 = 3.141, \dots$ where the sequence (a_n) represent the decimal expansion of π . It converges to $\pi \in \mathbb{R}$ but it does not converge to any limit in \mathbb{Q} .

Definition 6

A sequence (a_n) of real numbers converges to a limit $L \in \mathbb{R}$ if $\forall \varepsilon > 0, \exists N \in \mathbb{Z}^+$ such that $\forall n > N$, we always have $|a_n - L| < \varepsilon$.

Definition 7

A sequence (a_n) of real numbers is **Cauchy** $\forall \varepsilon > 0, \exists N \in \mathbb{Z}^+$ such that $\forall n, m \geq N$, we have $|a_n - a_m| < \varepsilon$.

Example 3.2

The sequence $(a_n) = \frac{1}{n}$ is Cauchy.

Proof

Take $N > 2/\epsilon$, then $m, n \geq N \implies \frac{1}{m} + \frac{1}{n} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$. □

Remark

A Cauchy sequence in \mathbb{R} may not converge to a limit. See the example of π above.

Corollary 8

A convergent sequence is always Cauchy, but the converse is not necessarily true. (They are both true in \mathbb{R} because \mathbb{R} is complete.)

Proof

We will show that convergent \implies Cauchy using triangle inequality: By the definition of convergence, for a convergent sequence (a_n) with a limit L , given $\epsilon/2$, there always exists $N \in \mathbb{Z}^+$ such that $n, m \geq N$, we have $|a_n - L| < \epsilon/2$ and $|a_m - L| < \epsilon/2$. Then by triangle inequality,

$$|a_n - a_m| \leq |a_n - L| + |a_m - L| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

which is exactly the definition of Cauchy. □

Proof

(Cauchy in $\mathbb{R} \implies$ converges to a limit in \mathbb{R})

Step one: let (a_n) be a Cauchy sequence in \mathbb{R} . Claim: each Cauchy sequence is bounded, i.e., $\exists M \in \mathbb{R}^+$

such that $-M \leq a_i \leq M$. To prove this, define set \mathcal{X} as

$$\mathcal{X} = \{x \in \mathbb{R} \mid \text{there are infinitely many } a_n \text{'s greater than } x\}$$

(we'll use this later, but not now.)

First we show that there's "cluster" in this sequence: take $\epsilon = 1$ and there exists $N \in \mathbb{Z}^+$ such that $n, k \geq N \implies |a_n - a_k| < 1$. Then all terms after a_N is within the "cluster" of $(a_N - 1, a_N + 1)$, and we only have a finite number of terms that's outside this cluster: a_1, a_2, \dots, a_{N-1} . Then it's easy to see that the set of all these first $N - 1$ terms, along with that "cluster", is bounded, since the set is *finite*. Then set

$$M = |\max(a_1, a_2, \dots, a_{N-1}, (a_N + 1))| + 1$$

and we see that *no* term of the sequence (a_n) is great than M , so M is an upper bound of \mathcal{X} . It's also clear that $-M$ is a lower bound of \mathcal{X} since there are *infinitely many* points in the cluster greater than $-M$. Clearly \mathcal{X} is not empty. Therefore \mathcal{X} is a nonempty and bounded subset of \mathbb{R} , and it has a L.U.B., which we call L .

Now we will try to show $\lim_{n \rightarrow \infty} a_n = L$.

Fix $\epsilon > 0$, and we will focus on $\epsilon/2$ for now, but remember that what we are trying to show is that given $\epsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that if $n \geq N$ we have $|a_n - L| < \epsilon$.

Clearly $L - \epsilon/2$ is not an upper bound for \mathcal{X} since L is the L.U.B. Therefore there exist infinitely many a_n 's greater than $L - \epsilon$. Therefore there exists some $x \in \mathcal{X}$ such that $x \geq L - \epsilon/2$. Hence infinitely many a_i 's are greater than x . However, since $L + \epsilon/2$ does not belong to \mathcal{X} , only finitely many a_i 's are greater than $L + \epsilon/2$. Therefore, there are infinitely many a_i 's greater than a_i and between $L - \epsilon/2$ and $L + \epsilon/2$ (or more specifically, between x and $L + \epsilon/2$):

$$L - \frac{\epsilon}{2} < x < a_i < L + \frac{\epsilon}{2}$$

Since infinitely many a_i 's satisfy $x < a_i < L + \epsilon$, infinitely many a_i 's with $i \geq N$ satisfy this. Pick one which we call a_k . Now we have $k \geq N$.

Since (a_n) is cauchy, there exists $N \in \mathbb{Z}^+$ such that if $n, m \geq N$ then $|a_n - a_m| < \epsilon/2$. (Again, we set it to $\epsilon/2$ here for a better result later on.) Then, if for another term a_n , if we have both $k \geq N$ (which we already know from previous construction of a_i) and $n \geq N$, then

$$|a_n - L| \leq \underbrace{|a_n - a_k|}_{\text{Sequence is Cauchy, } n, k \geq N} + \overbrace{|a_k - L|}^{a_k \text{ within } (L-\epsilon/2, L+\epsilon/2)} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

□

4 Tue 9/1 Discussion

Quick review:

- (1) Dedekind cuts.

- (2) Addition of Dedekind cuts.
 (3) Additive inverse of Dedekind cuts.

Example 4.1

Suppose $x = A | B$ is a cut. Show that $\frac{A}{2} | \frac{B}{2}$ is also a cut where

$$A = \left\{ \frac{a}{2} \mid a \in A \right\}, B = \left\{ \frac{b}{2} \mid b \in B \right\}.$$

Solution

We simply need to verify all three properties of a cut.

- (1) To show the union of these two sets is \mathbb{Q} and they are disjoint:

$\forall r \in \mathbb{Q}$, we always have $2r \in \mathbb{Q}$. Therefore since $A \cup B = \mathbb{Q}$, $2r$ is either in A or in B .

If $2r \in A$, then $r \in \frac{A}{2}$; if $2r \in B$, then $r \in \frac{B}{2}$. Therefore $r \in \frac{A}{2} \cup \frac{B}{2}$. Therefore $\mathbb{Q} \subset \frac{A}{2} \cup \frac{B}{2}$.

Also, since \mathbb{Q} is closed under addition, we have $\frac{A}{2} \cup \frac{B}{2} \subset \mathbb{Q}$.

Therefore $\frac{A}{2} \cup \frac{B}{2} = \mathbb{Q}$.

Now we show that they are disjoint: suppose $r \in \frac{A}{2}$ and $r \in \frac{B}{2}$. Then $r = a/2$ for some $a \in A$ and also $r = b/2$ for some $b \in B$. Therefore $2r$ is both in A and B , contradicting A and B being disjoint.

Hence such r does not exist, i.e., $\frac{A}{2}$ and $\frac{B}{2}$ are disjoint.

- (2) To show that $\forall a/2 \in \frac{A}{2}$ and $\forall b/2 \in \frac{B}{2}$ we have $a/2 < b/2$:

Since $a \in A$ and $b \in B$ we have $a < b$. Therefore $a/2 < b/2$.

- (3) To show $\frac{A}{2}$ does not have a largest element:

Suppose $\frac{A}{2}$ had a largest element $a/2$. Then $a/2 \geq a'/2$ for all $a'/2 \in \frac{A}{2}$. Multiplying this inequality by 2 we find that A is the largest element in A , contradicting A not having a largest element.

- (4) The L.U.B. property of real numbers: if $\mathcal{S} \subset \mathbb{R}$ is bounded from above and is nonempty, then \mathcal{S} has a L.U.B.

Worksheet for Today

Problem 3

Show that for any $a < b$, $a, b \in \mathbb{R}$ with $a < b$, there exists some rational number $r \in \mathbb{Q}$ such that $a < r < b$. In formal terms, \mathbb{Q} is dense in \mathbb{R} .

Solution

Alternate solution: write $r = p/q$ where $p, q \in \mathbb{Z}$ with $q \neq 0$. Then we pick $\frac{1}{q}$ sufficiently small that $\frac{1}{q} < b - a$. We claim that there exists $m \in \mathbb{Z}$ such that $\frac{m}{q} \in (a, b)$. Suppose not, then for all $m \in \mathbb{Z}$ we have $\frac{m}{q} \leq a$ or $\frac{m}{q} \geq b$. Now we take the largest integer not exceeding aq , i.e., $m \leq aq$ but $m + 1 > aq$. It follows that $(m + 1)/q$ must be $\geq b$.

Now we have $\frac{m}{q} \leq a \implies -\frac{m}{q} \geq -a$. Adding this with $(m + 1)/q \geq b$ we have $\frac{1}{q} \geq b - a$, contradicting our construction of $\frac{1}{q}$.

Problem 4

Consider two rational numbers s, t . Show that

- (1) $s \leq t$ if and only if $s^* \leq t^*$.
- (2) $s = t$ if and only if $s^* = t^*$.
- (3) $(s + t)^* = s^* + t^*$. Note that $s^* + t^*$ is the sum of two Dedekind cuts.

Solution

Since $s, t \in \mathbb{Q}$, we know $s^* = \{r \in \mathbb{Q} \mid r < s\} \mid \text{rest of } \mathbb{Q}$ and $t^* = \{r \in \mathbb{Q} \mid r < t\} \mid \text{rest of } \mathbb{Q}$.

- (1) If $s \leq t$, then $\{r \in \mathbb{Q} \mid r < s\} \subset \{r \in \mathbb{Q} \mid r < t\}$. By definition of two cuts, $s^* \leq t^*$.

To show the other direction, if $s^* \leq t^*$, by definition we have $\{r \in \mathbb{Q} \mid r < s\} \subset \{r \in \mathbb{Q} \mid r < t\}$. Suppose $s \geq t$, then we also have $\{r \in \mathbb{Q} \mid r < t\} \subsetneq \{r \in \mathbb{Q} \mid r < s\}$, an impossibility. Therefore $s \leq t$.

- (2) If $s = t$ then $s \leq t$ and $s \geq t$ both holds. Therefore the two sets are mutual subsets of each other and $s^* \leq t^*$ and $s^* \geq t^*$. Therefore $s^* = t^*$. Likewise for converse.
- (3) Note that the LHS and RHS are both cuts. We have to show mutual inclusion for the “left” part of the cuts.

First we have $(s+t)^* = \{r \in \mathbb{Q} \mid r < s+t\} \mid \text{rest of } \mathbb{Q} = A \mid B$ and $s^* + t^* = E \mid F$ where

$$E = \{a+b \mid a < s, b < t, a, b \in \mathbb{Q}\} \text{ and } F = \mathbb{Q} \setminus E$$

To show $E \subset A$, $\forall a+b \in E$, it always holds that $a < s, b < t$ and so $a+b < s+t$. Therefore $E \subset A$.

To show $A \subset E$, for all $r \in A$ we have $r < s+t$, and we want to show that $r = a+b$ for some $a < s, b < t$.

Let $a = s - \frac{s+t-r}{2}$ and $b = t - \frac{s+t-r}{2}$. It follows that $a < s, b < t$, and $a+b = s+t - (s+t-r) = r$. So $A \subset E$.

Problem 5

- (1) Prove that if $\mathcal{S} \subset \mathbb{R}$ is non-empty and bounded from below, then it has a greatest lower bound, $\inf(\mathcal{S})$.
- (2) Prove that if $\mathcal{S} \subset \mathbb{R}$ is non-empty and bounded from below, then

$$\inf(\mathcal{S}) = -\sup(-\mathcal{S})$$

Solution

- (1) Since \mathcal{S} is nonempty and bounded from below, we know $(-\mathcal{S})$ is nonempty and bounded from above. Therefore $(-\mathcal{S})$ has a L.U.B. Suppose $\sup(-\mathcal{S}) = b$. Claim: $-b = \inf(\mathcal{S})$.
 First show that $-b$ is a lower bound. Since $b \geq -s, \forall s \in \mathcal{S}$, we know $-b \leq s, \forall s \in \mathcal{S}$. Therefore $-b$ is a lower bound for \mathcal{S} .
 Now we show that it's the greatest among all lower bounds. Let $-b'$ be another lower bound. By the same argument b' is also an upper bound for $(-\mathcal{S})$. Since $-b = \sup(-\mathcal{S})$, it follows that $b \leq b'$, and $-b \geq -b'$. Therefore $-b$ is indeed $\inf(\mathcal{S})$.
- (2) Already shown.

Problem 6

Let $b = \sup(\mathcal{S})$, where \mathcal{S} is a bounded nonempty subset of \mathbb{R} .

- (1) Given $\epsilon > 0$ show that there exists an $s \in \mathcal{S}$ with

$$b - \epsilon \leq s \leq b.$$

- (2) Can $s \in \mathcal{S}$ always be found so that $b - \epsilon < s < b$?

Solution

- (1) Suppose for some $\epsilon > 0$ we cannot find any $s \in \mathcal{S}$ satisfying $s \in [b - \epsilon, b]$. Therefore $b - \epsilon$ is another upper bound for \mathcal{S} and it's smaller than b . (All $s \in \mathcal{S}$ are smaller than b , but since no $s \in \mathcal{S}$ is between $[b - \epsilon, b]$ we also know all elements $\leq b - \epsilon$.) Therefore $b \neq \sup(\mathcal{S})$. Contradiction.
- (2) A set containing discrete elements, for example the singleton $\mathcal{S} = \{1\}$.

5 Wed 9/2

More properties of real numbers:

- (1) For $a, b \in \mathbb{R}$ and $a < b$, the interval (a, b) denotes the set of all Dedekind cuts $c \in \mathbb{R}$ such that $a < c < b$.

Proposition 9

Every interval (a, b) contains infinitely many rational cuts and also infinitely many [!] irrational cuts.

Proof

Suppose $a = A \mid B$ and $b = C \mid D$. Since $a < b$ we know $A \not\subseteq C$. Therefore we can find some $c \in C \setminus A$. We claim that we can find another $d \in \mathbb{Q}$ such that $c^* < d^* < b$. Reason: C has no largest element by the definition of Dedekind cuts. Therefore c is not the largest element in C and we can find $d \in C$ satisfying $c^* < d^*$.

For the irrational number proof, play around with something like $\sqrt{2}$ and then start adding $\sqrt{2}/n$ to a until we reach b . n can be arbitrary large. \square

- (2) From now on we may take cuts and real numbers for granted... Finally.

Euclidean Space \mathbb{R}^n

Definition 10

For $n \in \mathbb{N}$, $\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ times}}$. That is, $\mathbb{R}^n = \{(x_1, x_2, \dots, x_n) \mid x_1, x_2, \dots, x_n \in \mathbb{R}\}$.

- (1) Addition: if $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n)$ then $\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$.
- (2) Scalar multiplication: if $c \in \mathbb{R}$, then $c\mathbf{x} = (cx_1, cx_2, \dots, cx_n)$.
- (3) Zero vector: $\vec{0} = \mathbf{0} = (0, 0, \dots, 0)$.
- (4) Commutativity and associativity of addition; existence of additive inverse and identity.
- (5) Associativity of scalar multiplication; existence of inverse and identity.
- (6) Distributivity of scalar multiplication.
- (7) A **vector space** is a set closed under addition and scalar multiplication (along with the ten axioms). \mathbb{R}^n is an example of a real vector space. More examples: the set of all polynomials with real coefficients; the set of all functions $[0, 1] \rightarrow \mathbb{R}$ (with $(f + g)(x) = f(x) + g(x)$ and $(cf)(x) = cf(x)$); the set of all continuous functions.

Inner Products

Definition 11

If \mathcal{V} is a real vector space, an inner product is a map $\langle -, - \rangle : \mathcal{V} \times \mathcal{V} \rightarrow \mathbb{R}$ (- as placeholders) such that

- (1) $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$,
- (2) $\langle c\mathbf{x}, \mathbf{y} \rangle = c\langle \mathbf{x}, \mathbf{y} \rangle$ and $\langle \mathbf{x} + \mathbf{x}', \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}', \mathbf{y} \rangle$.
- (3) **Positive definiteness:** $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$ and $\langle \mathbf{x}, \mathbf{x} \rangle = 0$ if and only if $\mathbf{x} = \mathbf{0}$.

Example 5.1

On \mathbb{R}^n , the dot product of $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n)$ is $x_1y_1 + x_2y_2 + \cdots + x_ny_n = \sum_{i=1}^n x_iy_i$.

Definition 12

A vector space with the inner product property is an **inner product space**.

Remark

Even for \mathbb{R}^n , inner product doesn't necessarily have to be dot products. For example, if we define $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + 2x_2y_2 + 3x_3y_3$, all three criteria are met.

Definition 13

(See below) If \mathcal{V} is an inner product space, we say $\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$ is the **norm** induced by the inner product $\langle -, - \rangle$.

6 Fri 9/4**Definition 14**

(Following the last definition from above) Let \mathcal{V} be a real vector space. A **norm** is a function $\|-\| : \mathcal{V} \rightarrow \mathbb{R}$ such that

- (1) $\|\mathbf{v}\| \geq 0$ and $\|\mathbf{v}\| = 0$ if and only if $\mathbf{v} = \mathbf{0}$ for all $\mathbf{v} \in \mathcal{V}$.
- (2) $\|\lambda\mathbf{v}\| = |\lambda|\|\mathbf{v}\|$ where $\mathbf{v} \in \mathcal{V}$ and $\lambda \in \mathbb{R}$. (Scalar multiplication)
- (3) $\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$ for all $\mathbf{v}, \mathbf{u} \in \mathcal{V}$. (Addition and triangle inequality)

Lemma 6.1

If $(\mathcal{V}, \langle -, - \rangle)$ is an inner product space, then $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$ is the norm of \mathbf{v} .

Remark

The fact that inner product \implies norm comes from

- (1) Inner products are positive definite, so $\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$ is always meaningful.
- (2) Inner products are linear for scalar multiplications.
- (3) For triangle inequality: see below.

Remark

When thinking about inner products, we can always think about the quintessential example of dot products in \mathbb{R}^n . Of course there are other kinds of inner products in other vector spaces though.

Theorem 15

Two key properties of inner products:

- (1) **Triangle inequality:** $\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$.
- (2) **Cauchy-Schwarz inequality:** $\langle \mathbf{v}, \mathbf{w} \rangle \leq \|\mathbf{v}\| \cdot \|\mathbf{w}\|$.

Proof of Cauchy-Schwarz inequality

Let \mathcal{V} be a vector space and $\langle -, - \rangle$ an inner product. Given two vectors $\mathbf{x}, \mathbf{y} \in \mathcal{V}$, define a function $f : \mathbb{R} \rightarrow \mathbb{R}$ by

$$f(t) = \langle t\mathbf{x} + \mathbf{y}, t\mathbf{x} + \mathbf{y} \rangle.$$

Since $t\mathbf{x} + \mathbf{y}$ is a vector, this function is meaningful. Observe that $f(t)$ is positive definite, i.e., $f(t) \geq 0$, since inner products are positive definite. Now expand $\langle t\mathbf{x} + \mathbf{y}, t\mathbf{x} + \mathbf{y} \rangle$:

$$\begin{aligned} f(t) &= \langle t\mathbf{x} + \mathbf{y}, t\mathbf{x} + \mathbf{y} \rangle \\ &= t^2 \langle \mathbf{x}, \mathbf{x} \rangle + 2t \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle, \end{aligned}$$

a quadratic function of t . By the positive definiteness of $f(t)$, there is no solution to $f(t) < 0$, so the graph of $f(t)$ touches the x -axis at most once, i.e., $\sqrt{\delta} \leq 0$. Therefore

$$4 \langle \mathbf{x}, \mathbf{y} \rangle^2 - 4 \langle \mathbf{x}, \mathbf{x} \rangle \langle \mathbf{y}, \mathbf{y} \rangle \leq 0 \implies \langle \mathbf{x}, \mathbf{y} \rangle \leq \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle \langle \mathbf{y}, \mathbf{y} \rangle}$$

from which $\langle \mathbf{x}, \mathbf{y} \rangle \leq \|\mathbf{x}\| \cdot \|\mathbf{y}\|$, the Cauchy-Schwarz inequality, follows. \square

Proof of triangle inequality

$$\begin{aligned}
\|\mathbf{v} + \mathbf{w}\|^2 &= \langle \mathbf{v} + \mathbf{w}, \mathbf{v} + \mathbf{w} \rangle \\
&= \langle \mathbf{v}, \mathbf{v} + \mathbf{w} \rangle + \langle \mathbf{w}, \mathbf{v} + \mathbf{w} \rangle && \text{(linearity)} \\
&= \langle \mathbf{v}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle + \langle \mathbf{w}, \mathbf{v} \rangle + \langle \mathbf{w}, \mathbf{w} \rangle && \text{(more linearity)} \\
&= \|\mathbf{v}\|^2 + \|\mathbf{w}\|^2 + 2\langle \mathbf{v}, \mathbf{w} \rangle && \text{(symmetry and def of norm)} \\
&\leq \|\mathbf{v}\|^2 + \|\mathbf{w}\|^2 + 2\|\mathbf{v}\| \cdot \|\mathbf{w}\| && \text{(assuming Cauchy-Schwarz[!])} \\
&= \underbrace{(\|\mathbf{v}\| + \|\mathbf{w}\|)^2}_{>0}
\end{aligned}$$

Since $\|\mathbf{v} + \mathbf{w}\| \geq 0$ and $\|\mathbf{v}\| + \|\mathbf{w}\| \geq 0$, we have

$$\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|.$$

□

Example 6.1

Suppose we are in \mathbb{R}^5 . With dot product, Cauchy-Schwarz says for any real numbers x_1, \dots, x_5 and y_1, \dots, y_5 , we always have

$$x_1y_1 + \dots + x_5y_5 \leq \sqrt{(x_1^2 + \dots + x_5^2)(y_1^2 + \dots + y_5^2)}.$$

Example 6.2

Let $C([0, 1], \mathbb{R})$ denote the set of *continuous* (we'll get to this very soon) functions from $[0, 1] \rightarrow \mathbb{R}$. This is a vector space[!]. Define an inner product by

$$\langle f(x), g(x) \rangle = \int_0^1 f(x)g(x)dx \quad \text{[why?]}$$

Then Cauchy-Schwarz states that for any $f(x), g(x) \in C([0, 1], \mathbb{R})$, we have

$$\int_0^1 f(x)g(x)dx \leq \sqrt{\left(\int_0^1 f(x)^2dx\right)\left(\int_0^1 g(x)^2dx\right)}$$

Note that the norm of $f(x)$ is $\sqrt{\langle f(x), f(x) \rangle} = \sqrt{\int_0^1 f(x) dx}$. A quick application of this:

$$\int_0^1 e^x \sin(x) dx \leq \left(\sqrt{\int_0^1 e^{2x} dx} \right) \left(\sqrt{\int_0^1 \sin^2(x) dx} \right).$$

Remark

Suppose we took $C((0,1), \mathbb{R})$ with the same inner product. This will not be a valid inner product space. Reason: $f : (0,1) \rightarrow \mathbb{R}$ being continuous does not necessarily guarantee that $\int_0^1 f(x) dx$ is defined. Consider $\int_0^1 (1/x) dx$ for example.

Cardinality

Definition 16

Give sets A, B , we say A and B have the same **cardinality** if there exists a bijection $f : A \rightarrow B$, (Remember that bijections are invertible, so there also exists $f^{-1} : B \rightarrow A$.)

Notations: $A \sim B$, $|A| = |B|$, $\text{card}(A) = \text{card}(B)$, $\#A = \#B$. Lots of notations.

Remark

Having equal cardinality is an equivalence relation on sets.

Definition 17

A set \mathcal{S} is:

- (1) **finite** if either $\mathcal{S} = \emptyset$ or $\mathcal{S} \sim \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$.
- (2) **denumerable / countably infinite / enumerable** if $\mathcal{S} \sim \mathbb{N}$.
- (3) **countable** if \mathcal{S} is either finite or denumerable, and
- (4) **uncountable** if \mathcal{S} is not countable.

7 Tue 9/8 Discussion

Review:

- (1) \mathbb{R} has the L.U.B. property: if $\mathcal{S} \subset \mathbb{R}$ is nonempty and bounded above, then \mathcal{S} has a L.U.B.
- (2) Q: if $c = \sup(\mathcal{S})$, is $c \in \mathcal{S}$ necessarily true?
A: No. The π example again (in \mathbb{Q}), or consider the set $\{a \in \mathbb{R} \mid a < 2\}$ with $\sup = 2$.
- (3) Definition of Cauchy sequence.
- (4) Definition of convergent sequence.
- (5) Convergent \implies Cauchy always holds, but Cauchy may not \implies convergence, depending on whether the metric space is complete or not.
- (6) Definition of completeness of a metric space: whether every Cauchy sequence converges or not (whether the limits of every Cauchy sequence lie within the same metric space).
- (7) A quick example:

Example 7.1

Let (a_n) be an increasing sequence in \mathbb{R} and let it be bounded above. Show that (a_n) is convergent.

Proof. Let $\mathcal{S} = \{a_n\}$. Clearly \mathcal{S} is nonempty and bounded above. Therefore \mathcal{S} has a supremum, which we denote as $b = \sup(\mathcal{S})$.

By definition, $\forall \epsilon/2 > 0$, there exists $s \in \mathcal{S}$ such that $b - \epsilon/2 \leq s \leq b$. (See the last problem on Tue 9/1 discussion above.) We may denote this s as a_N . Then, since the sequence is increasing, we see that since for any $k \geq N$, $a_k \geq a_N$, and thus $|b - a_k| \leq \epsilon/2 < \epsilon$. Hence convergence follows.

Note that after coming up with the a_N part, we can also use the definition of Cauchy sequence to complete this proof, but that requires the completeness of \mathbb{R} as the last step. \square

Worksheet for Today

Problem 7

Let \mathcal{S}, \mathcal{T} be two nonempty subsets of \mathbb{R} that are bounded above and define $\mathcal{S} + \mathcal{T} = \{s + t \mid s \in \mathcal{S}, t \in \mathcal{T}\}$.

(1) Show that the set $\mathcal{S} + \mathcal{T}$ has a least upper bound and

$$\sup(\mathcal{S} + \mathcal{T}) = \sup(\mathcal{S}) + \sup(\mathcal{T}).$$

(2) For all $x \in \mathbb{R}$, we define $\mathcal{S} + x = \{s + x \mid s \in \mathcal{S}\}$. Show that $\mathcal{S} + x$ has a least upper bound and

$$\sup(\mathcal{S} + x) = \sup(\mathcal{S}) + x.$$

Solution

(1) Clearly $\sup(\mathcal{S}) + \sup(\mathcal{T})$ is an upper bound for $\mathcal{S} + \mathcal{T}$. Therefore all that remains to show is that $\sup(\mathcal{S}) + \sup(\mathcal{T}) \leq \sup(\mathcal{S} + \mathcal{T})$.

Suppose not and set $\epsilon = \sup(\mathcal{S}) + \sup(\mathcal{T}) - \sup(\mathcal{S} + \mathcal{T})$. From the last problem of discussion on 9/1 we know there exists $s \in \mathcal{S}$ such that $\sup(\mathcal{S}) - \epsilon/4 \leq s \leq \sup(\mathcal{S})$. Likewise there exists $t \in \mathcal{T}$ such that $\sup(\mathcal{T}) - \epsilon/4 \leq t \leq \sup(\mathcal{T})$. Adding these gives

$$\sup(\mathcal{S}) + \sup(\mathcal{T}) - \epsilon < \sup(\mathcal{S}) + \sup(\mathcal{T}) - \frac{\epsilon}{2} \leq s + t \leq \sup(\mathcal{S}) + \sup(\mathcal{T}),$$

contradicting our assumption that $\sup(\mathcal{S}) + \sup(\mathcal{T}) > \sup(\mathcal{S} + \mathcal{T})$. Hence they are equal.

(2) Let $\mathcal{T} = \{x\}$ a singleton. Then this problem is immediate by the previous part.

Problem 8

Suppose $\mathcal{S} \subset \mathbb{R}$ is nonempty and bounded above. Assume $\sup(\mathcal{S}) = c$ and $c \notin \mathcal{S}$. Find a sequence (a_n) converging to c with $a_n \in \mathcal{S}$.

Solution

Recall that for all $\epsilon > 0$, there exists $s \in \mathcal{S}$ satisfying $c - \epsilon \leq s \leq c$. Therefore, there exists a_i satisfying

$$c - \frac{1}{i} \leq a_i \leq c \text{ with } a_i \in \mathcal{S}.$$

Therefore such sequence (a_n) with a_i defined above is a sequence satisfying the conditions. Proof of convergence: given $\epsilon > 0$ we simply need to set $N > 1/\epsilon$. Then by the construction above, $|a_k - c| < \epsilon$ for all $k \geq N$.

Problem 9

Let (a_n) be a Cauchy sequence in \mathbb{R} and all terms are integers. Show that there exists some N such that $a_n = C$ for all $n \geq N$ where C is an integer.

Solution

If the sequence is Cauchy and we set $\epsilon < 1$, then there exists $N \in \mathbb{Z}^+$ with all terms after a_N being the same integer because the difference between terms *must* be nonnegative integers. If we set this same integer to be C then we are done.

Problem 10

Let (a_n) and (b_n) be two Cauchy sequences in \mathbb{R} . Show that $(a_n + b_n)$ is also a Cauchy sequence. Note that similar arguments can be made for $(a_n - b_n)$.

Solution

Let (c_n) be a sequence with $c_i = a_i + b_i$. We want to show that (c_n) is Cauchy. By the triangle inequality,

$$|c_m - c_n| = |a_m + b_m - a_n - b_n| \leq |a_m - a_n| + |b_m - b_n|$$

Since (a_n) and (b_n) are both Cauchy, we can make m, n sufficiently large that the two absolute values on the right are both less than $\epsilon/2$. Then the LHS is less than ϵ and (c_n) is Cauchy. (Not quite formal; I'm getting tired).

8 Wed 9/9 Cardinality

Recall:

- (1) Definition of denumerable, countable, and uncountable sets.
- (2) $A \sim B$ means there exists a bijection between A and B .
- (3) Denumerable means $\sim \mathbb{N}$. Or countably infinite.

Problem 11

Is the set of integers \mathbb{Z} countable?

Solution

The function $f : \mathbb{N} \rightarrow \mathbb{Z}$ and $g : \mathbb{Z} \rightarrow \mathbb{N}$ defined by

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ -\frac{x-1}{2} & \text{if } x \text{ is odd} \end{cases} \quad \text{or } g(x) = \begin{cases} 1 + 2x & \text{if } x \geq 0 \\ -2x & \text{if } x < 0 \end{cases}$$

are two bijections. Hence $\mathbb{N} \sim \mathbb{Z}$ and \mathbb{Z} is countable. (We only need one bijection to show the equivalence though.)

Theorem 18

Any infinite subset of a denumerable set is denumerable.

Proof. Suppose B is denumerable and $A \subset B$. Then there exists a bijection between $f : \mathbb{N} \rightarrow B$. Now we need to show that there is a bijection $g : \mathbb{N} \rightarrow A$.

Since $\mathbb{N} \sim B$, all elements of B appear somewhere in the set $\{f(1), f(2), \dots\}$. Now let $g(1)$ be the smallest k such that $f(k)$ is an element of A and let $g(i)$ be the i^{th} smallest element of A appearing in the list.

Claim: this is a bijection $g : \mathbb{N} \rightarrow A$.

Clearly it's a surjection since all elements in A gets mapped, and it's an injection because f is injective so $g(i) \neq g(j) \implies f(m) \neq f(n)$. \square

Theorem 19

$\mathbb{N} \times \mathbb{N}$ is countable. Furthermore it's denumerable.

Proof. Consider the $\infty \times \infty$ matrix

$$\begin{bmatrix} (1,1) & (1,2) & (1,3) & \dots \\ (2,1) & (2,2) & (2,3) & \dots \\ (3,1) & (3,2) & (3,3) & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

going along the diagonal gives a bijection:

$$(1, 1), (1, 2), (2, 1), (3, 1), (2, 2), (1, 3), \dots$$

□

Problem 12

Is $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ countable or uncountable?

Solution

$$\mathbb{N} \times \mathbb{N} \times \mathbb{N} \sim (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}.$$

Theorem 20

If $f : \mathbb{N} \rightarrow A$ is surjective, then A must be countable.

Proof.

Case 1: A is finite. Then it's countable.

Case 2: A is infinite. Consider $f(1), f(2), \dots$. This list exhausts A , but there might be redundancies. Then we need a bijection $g : \mathbb{N} \rightarrow A$. Let's start by defining $A \rightarrow \mathbb{N}$ by saying $h(a)$ is the smallest k such that $f(k) = a$. Clearly h is injective because there is only one smallest k . It may, however, not be surjective if f is not injective, i.e., one a corresponding to more than one k 's. Yet, h is bijective between A and the image of h . So $A \sim \text{image of } h \sim \mathbb{N}$. Hence $A \sim \mathbb{N}$. □

Theorem 21

\mathbb{Q} is denumerable.

Proof. First consider a map $\mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Q}$ defined by $(i, j) \mapsto i/j$. Clearly this map is well-defined and surjective. Since $\mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{Z} \times \mathbb{N}$, we know that we can find a surjective map $\mathbb{N} \rightarrow \mathbb{Q}$. Hence \mathbb{Q} is denumerable. □

9 Fri 9/11

Theorem 22

\mathbb{R} is uncountable.

Proof: Cantor's diagonalization trick. Suppose, by contradiction, we have a bijection $f : \mathbb{N} \rightarrow \mathbb{R}$. Then for each $i \in \mathbb{N}$, let $f(i) =$ the base 10 decimal expansion of a real number *without* an infinite string of 9's. It follows that, under such restriction, each real number corresponds to a unique decimal expansion.

$$\begin{array}{rcl}
 f(1) & = & N_1. \ x_{11} \ x_{12} \ x_{13} \ x_{14} \ x_{15} \ x_{16} \ x_{17} \\
 f(2) & = & N_2. \ x_{21} \ x_{22} \ x_{23} \ x_{24} \ x_{25} \ x_{26} \ x_{27} \\
 f(3) & = & N_3. \ x_{31} \ x_{32} \ x_{33} \ x_{34} \ x_{35} \ x_{36} \ x_{37} \\
 f(4) & = & N_4. \ x_{41} \ x_{42} \ x_{43} \ x_{44} \ x_{45} \ x_{46} \ x_{47} \\
 f(5) & = & N_5. \ x_{51} \ x_{52} \ x_{53} \ x_{54} \ x_{55} \ x_{56} \ x_{57} \\
 f(6) & = & N_6. \ x_{61} \ x_{62} \ x_{63} \ x_{64} \ x_{65} \ x_{66} \ x_{67} \\
 f(7) & = & N_7. \ x_{71} \ x_{72} \ x_{73} \ x_{74} \ x_{75} \ x_{76} \ x_{77} \\
 & \vdots & \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \ddots
 \end{array}$$

Now consider $y = 0.b_1b_2\dots$ such that $b_i \neq x_{ii}$ and $b_i \neq 9$ for each i . We know $y \neq f(1)$ because the first digit after the decimal point of the two numbers are different. Likewise, $b_n \neq x_n$ for all n . Therefore y does not appear as an image of f but clearly $y \in \mathbb{R}$. Hence no bijection exists from \mathbb{N} onto \mathbb{R} and \mathbb{R} is uncountable. \square

Remark

For sets A, B , we say $|A| \leq |B|$ if there is a surjection $B \rightarrow A$ and $|A| < |B|$ if, in addition, $A \sim B$ is false.

Problem 13

If $|A| \leq |B|$, is there an injection $A \rightarrow B$?

Solution

Yes. Let $f : B \rightarrow A$ be a surjection. Define an injection $g : A \rightarrow B$ as follows:

For $a \in A$, let $g(a)$ be a *chosen* element in B such that $f(b) = a$, i.e, $g(a) \in \{f^{-1}(a)\}$. (Note that there may be more than one element in the set $\{f^{-1}(a)\}$. Therefore we *choose* one following the *Axiom of Choice*.)

Then g is injective because if $g(a) = g(a')$ then a and a' have the same preimage under f and thus $a = a'$.

Schroeder-Bernstein

If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$. In other words, if A, B are sets and there exist injections $f : A \rightarrow B$ and $g : B \rightarrow A$, then there exists a bijection $h : A \rightarrow B$.

Proof. See Pugh's book, pg. 36. □

Definition 24

Let S be a set. The **power set** of A , $\mathbb{P}(S)$ (or 2^S), is the set of all subsets of A .

Remark

We know that $\mathcal{P}(\mathbb{N}) \sim$ the set of infinite binary expansions (see Ex. 1.38.(a)), therefore $\mathcal{P}(\mathbb{N}) \sim \mathbb{R} \sim [0, 1)$.

Problem Continuum Hypothesis

Is there any set A such that $|\mathbb{N}| < |A| < |\mathbb{R}|$?

10 Mon 9/14 Starting Ch.2

From last lecture:

More on Continuum Hypothesis: does there exist a set A such that $|\mathbb{N}| < |A| < |\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$?

Paul Cohen: the answer is independent of ZFC; not possible to prove or disprove the Continuum Hypothesis.