Lecture 3

Monday, September 11, 2023 9:59 AM

Theorem The following statements are logically equivalent:

a) S is a countable set

b) There exists a surjection of $\mathbb{N}$ onto S

c) There exists an injection of S into $\mathbb{N}$

* surjection is easiest to construct

Proof a) $\Rightarrow$ b)

By def. of countable, there exists a bijection from $\mathbb{N}_n = \{1, 2, \ldots, n\}$ onto S.

b) $\Rightarrow$ c)

Let f be the surjection from $\mathbb{N}$ onto S and let g be the mapping from S into $\mathbb{N}$.

$$\begin{tikzcd} \mathbb{N} \arrow[r, "f"] & S \arrow[l, bend left, "g"] \end{tikzcd}$$

$g(s)$ is the least element in the set $f^{-1}(\{s\}) = \{n \in \mathbb{N} : f(n) = s,\ s \in S\}$

inverse image

Claim: g is injective $(g(s_1) = g(s_2) \Rightarrow s_1 = s_2)$

Proof Suppose $g(s_1) = g(s_2)$

Then $s_1 = f(g(s_1)) = f(g(s_2)) = s_2$, so $s_1 = s_2$

So, g is injective from S into $\mathbb{N}$. ∎

c) $\Rightarrow$ a)

Let g be the injection of S into $\mathbb{N}$. Consider g as the mapping from S to $g(S) \subseteq \mathbb{N}$.

Since $\mathbb{N}$ is countable and $g(S)$ is a subset of $\mathbb{N}$, it follows that $g(S)$ is countable.

Consider the case when $g(S)$ is denumerable.

$$\begin{tikzcd} S \arrow[r, leftrightarrow, "g"] & g(S) \arrow[r, leftrightarrow, "h"] & \mathbb{N} \arrow[ll, bend left, "g^{-1} \circ h"] \end{tikzcd}$$

Then there exists a bijection h from $\mathbb{N}$ onto $g(S)$, then $g^{-1} \circ h$ is a bijection from $\mathbb{N}$ onto S. So, S is denumerable.

Theorem 1.3.8 The set $\mathbb{N} \times \mathbb{N}$ is denumerable.

Theorem The set of rational numbers $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$ is denumerable.

$\mathbb{Q} = \mathbb{Q}^+ \cup \{0\}\ \mathbb{Q}^-$

just focus on showing that this is countable

$\mathbb{Q}^+ = \{\frac{m}{n} : m, n \in \mathbb{N}\}$

$\mathbb{N} \to \mathbb{Q}^+$

matrices!

$$\begin{array}{ccccc} \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \cdots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \cdots \\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \cdots \\ \frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \cdots \end{array}$$

"a picture is worth more than 1000 words"

diagonal mapping

1 appears in every row and column

This is a surjection of $\mathbb{N}$ onto $\mathbb{Q}^+$

So $\mathbb{Q}^+$ is countable

It can also be shown in the same way that $\mathbb{Q}^-$ is countable, and since $\{0\}$ is finite, $\mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}$ is countable.

Theorem If A_n is a countable set for each $n \in \mathbb{N}$, then $A = \bigcup_{n=1}^{\infty} A_n$ is countable.

$A_1 = \ a_{11} \quad a_{12} \quad a_{13} \ \cdots$

$A_2 = \ a_{21} \quad a_{22} \quad a_{23} \ \cdots$

$\vdots$

$A_n = \ a_{n1} \quad a_{n2} \quad a_{n3} \ \cdots$

another diagonal mapping

Cantor's Theorem Let A be any set. There is no surjection of A onto its power set $P(A)$.

☆ Kang did not mention this, I just thought it was cool

Section 2.1 $\mathbb{R}$

The system of real numbers is a field with respect to addition & multiplication.

Algebraic Properties of $\mathbb{R}$

these are also called the field axioms of $\mathbb{R}$

Let $a, b, c \in \mathbb{R}$

(A1) $a + b = b + a$ (commutative property of addition)

(A2) $(a+b)+c = a+(b+c)$ (associative property of addition)

(A3) There exists an element $0 \in \mathbb{R}$ such that $0 + a = a + 0 = a$
(existence of a zero element)

(A4) $\forall a \in \mathbb{R}$, $\exists -a \in \mathbb{R}$ such that $a + (-a) = (-a) + a = 0$
(existence of negative elements)

(M1) $a \cdot b = b \cdot a$ (commutative property of multiplication)

(M2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associative property of multiplication)

(M3) There exists an element $1 \in \mathbb{R}$ distinct from 0 such that $1 \cdot a = a \cdot 1 = a$
(existence of a unit element)

(M4) $\forall a \neq 0$, there exists an element $\frac{1}{a} \in \mathbb{R}$ such that $a \cdot \left(\frac{1}{a}\right) = \left(\frac{1}{a}\right) \cdot a = 1$
(existence of reciprocals)

(D) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$
(distributive property of multiplication over addition)

Examples (These are theorems in 2.1)

a) If $z, a \in \mathbb{R}$ with $z + a = a$, then $z = 0$ (Rule of cancellation).

(A4) $\exists -a \in \mathbb{R}$ such that $a + (-a) = 0$

So, $z + a = a$ implies $(z + a) + (-a) = a + (-a) = 0$

(A2): $(z+a) + (-a) = z + (a + (-a)) = z + 0 = 0$

(A3): $z + 0 = z = 0$

so $z = 0$ ✓

b) If $u, b \in \mathbb{R}$ and $b \neq 0$ with $u \cdot b = b$, then $u = 1$.

(M3): $u = u \cdot 1$

(M4): $b \cdot \left(\frac{1}{b}\right) = 1$, so $u = u \cdot \left(b \cdot \frac{1}{b}\right)$

(M4): $b\cdot\left(\frac{1}{b}\right)=1$, so $u=u\cdot\left(b\cdot\frac{1}{b}\right)$

(M2): $u=\underbrace{(u\cdot b)}_{=b}\cdot\left(\frac{1}{b}\right)=\quad u=b\cdot\frac{1}{b}$

By M3 again, $u=1$

c) If $a\in\mathbb{R}$, $a\cdot 0=0$

(M3) $a+a\cdot 0 = a\cdot 1 + a\cdot 0$

(D): $a\cdot(1+0)$

(M3): $a\cdot(1+0) = a\cdot 1 = a$

So, $a+(a\cdot 0)=a$

By the rule of cancellation, $a\cdot 0$ must equal 0.

d) If $a\neq 0$ and $b\in\mathbb{R}$ with $a\cdot b=1$, then $b=\frac{1}{a}$. (Uniqueness of Reciprocals)

Proof By (M4), $\exists\ \frac{1}{a}\in\mathbb{R}$ such that $a\cdot\frac{1}{a}=\frac{1}{a}\cdot a=1$. Since $a\cdot b=1$, then $\frac{1}{a}\cdot ab=\frac{1}{a}\cdot 1=\frac{1}{a}$.

By (M2), $\frac{1}{a}\cdot(a\cdot b)=\left(\frac{1}{a}\cdot a\right)\cdot b$ which by M4 again is $1\cdot b$, which by (M3) is equal to b.

So, $b=\frac{1}{a}$.

e) If $a\cdot b=0$, then either $a=0$ or $b=0$.

Proof Case 1: $a=0$ done

Case 2: $a\neq 0$

By (M4), $\exists\ \frac{1}{a}\in\mathbb{R}$ such that $\frac{1}{a}\cdot a=1$. Multiplying $a\cdot b=0$ by $\frac{1}{a}$, we get $\frac{1}{a}(a\cdot b)=0\cdot\frac{1}{a}=0$.

By M2, $\frac{1}{a}\cdot(a\cdot b)=\left(\frac{1}{a}\cdot a\right)\cdot b$, which by M4, is $1\cdot b$.

So, we have $b\cdot 1=0$. By M3, $b\cdot 1=b$,

so we have $b=0$. ∎

The operation of subtraction is defined by addition: $a-b=a+(-b)$

Similarly, division is defined in terms of multiplication: For $a,b\in\mathbb{R}$ with $b\neq 0$, $a/b=a\cdot(1/b)$