Peano Axioms, Integers, Rationals

Parasar Mohanty, 2022

[1]

1 Peano Axioms

Axiom 1: 1 is a natural number.

Axiom 2: If n is a natural number then n has a *successor* denote it by $(n+)$.

Axiom 3: 1 is not a successor of any natural number.

Axiom 4: Different natural numbers must have different successors.

Axiom 5: (Mathematical Induction) Let $P(n)$ be any property pertaining to natural number. Suppose $P(1)$ is true and suppose whenever $P(n)$ is true then $P(n+)$ is also true. Then $P(n)$ is true for every natural number n.

Through Peano axioms we define Natural numbers. We also have addition in $\mathbb{N}$. If $m, n \in \mathbb{N}$ then $m + n = ((((((m+)+)+)\dots)+$, i.e. n^{th} successor of n.

Proposition 1.1. *If $A \subset \mathbb{N}$ then it has an element which is not a successor of any element in A.*

Exercise 1.1.

1. *Prove that* $111\dots111$ (729 *ones) is divisible by* 729.
2. *A set of n points is taken on a circle and each pair is connected by a segment. It happens that no three of these segments meet at the same point. Into how many parts do they divide the interior of the circle?*
3. *Show that* $1 + 3 + \cdots + (2n-1) = n^2$.
4. *Show that* $1.2 + 2.3 + \cdots + (n-1).n = (n-1)n(n+1)/3$.
5. *Show that* $\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{(n-1)n}{=}\frac{n-1}{n}$.
6. *Let $l, k \in \mathbb{N}$. Show that* $\frac{1}{l(l+k)} + \frac{1}{l(+k)(l+2k)} + \cdots + \frac{1}{(l+(n-1)k)(l+nk)} = \frac{n}{l(l+nk)}$.

[1]Part of this note is based on materials from Analysis I by Terrence Tao

2 Integers

Define a relation on $\mathbb{N} \times \mathbb{N}$ as $(m, n) \sim (p, q)$ if $m + q = n + p$. This is an equivalence relation. Denote $m - n = (m, n)$. An integer is an expression of the form $m - n$ where m and n belongs to $\mathbb{N}$. Two integers are considered to be equal, $m_1 - n_1 = m_2 - n_2$, if and only if $m_1 + n_2 = m_2 + n_1$.

Let us denote $\mathbb{Z}$ to be the set of all integers. We have the following well defined addition and multiplications in $\mathbb{Z}$.

Add: $(m - n) + (p - q) = (m + p) - (n + q)$.

Mult: $(m - n) \times (p - q) = (mp + nq) - (np + mq)$.

Exercise 2.1. *Show that addition and multiplication are well defined.*

Definition 2.2. *If $m - n$ is an integer then define* **negation** *of $m - n$ to be the pair (n, m).*

Lemma 2.3. *Let x be an integer. Then exactly one of the following statement is true.*

1. $x = (m, m)$
2. $x = (m, n)$ *where* $m > n$
3. $x = (m, n)$ *where* $m < n$.

Proposition 2.1 (No zero divisors)**.** *Let $m, n \in \mathbb{Z}$ such that $mn = 0$. Then either $m = 0$ or $n = 0$.*

Proof. Let us assume both are not zero. Then considering signs of m and n one can conclude $mn \neq 0$, by using the fact integers are of three types. □

3 Rational Number

Define a relation on $\mathbb{Z} \times \mathbb{Z} \cup \{0\}$ as $(m, n) \sim (p, q)$ if $mq = np$. This is an equivalence relation. Denote $\frac{p}{q} = (p, q)$. A rational number is an expression of the form $\frac{p}{q}$ where p and q are integers and $q \neq 0$. Let us denote $\mathbb{Q}$ to be the set of rationals. We have addition, multiplication and division for rationals.

Add: $\frac{m}{n} + \frac{p}{q} = \frac{mq+pn}{nq}$.

Mult: $\frac{m}{n} \times \frac{p}{q} = \frac{mp}{nq}$.

Div: $\frac{m}{n} / \frac{p}{q} = \frac{mq}{np}, \;\; p \neq 0$.

Let $x, y \in \mathbb{Q}$ we say that $x > y$ if $x - y > 0$ and $x < y$ if $y > x$. Also, $x \geq y$ iff either $x > y$ or $x = y$, similarly we can define $x \leq y$.

Proposition 3.1. *Let $x, y \in \mathbb{Q}$ then exactly one of the three statements is true: (i) $x > y$ (ii) $x = y$ (iii) $x < y$.*

Definition 3.1 (Absolute Value)**.** *Let $x \in \mathbb{Q}$ define*

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

(Distance) Let $x, y \in \mathbb{Q}$ define $d(x, y) = |x - y|$.

Proposition 3.2.

Let $x, y, z \in \mathbb{Q}$. Then following statements holds.

1. (Non-degenracy) $d(x, y) \geq 0$. Also $d(x, y) = 0 \iff x = y$.
2. (Symmetry) $d(x, y) = d(y, x)$.
3. (Traingle Inequality) $d(x, y) \leq d(x, z) + d(y, z)$.

3.1 Differences between $\mathbb{Z}$ and $\mathbb{Q}$

1. Each integer has a *successor*. However, this is not true in $\mathbb{Q}$. As let $x, y \in \mathbb{Q}$ and $x < y$ then there exists a $z \in \mathbb{Q}$ such that $x < z < y$.
2. $\mathbb{Q}$ is a field but $\mathbb{Z}$ is not.
3. For $x \in Q$ and $0 < \epsilon \in \mathbb{Q}$ define $B_\epsilon(x) = \{y \in \mathbb{Q} : \ d(y, x) < \epsilon\}$. If $0 < \epsilon < 1$ and $x \in \mathbb{Z}$ then then the set $B_\epsilon(x) \cap \mathbb{Z} = \emptyset$. However, for $x \in \mathbb{Q}$ we have $B_\epsilon(x) \cap \mathbb{Q} \neq \emptyset$.
4.

   Definition 3.2. *Let $A \subset \mathbb{Q}$. We say that A is* **bounded above** *if there exists a $M \in \mathbb{Q}$ such that $x \leq M$ for all $x \in A$. Similarly, A is* **bounded below** *if there exists a $N \in \mathbb{Q}$ such that $x \geq N$ for all $x \in A$. A is said to be bounded if it is both bounded above as well as bounded below.*

   M is called an **upper bound** *for A. Similarly N is called a* **lower bound.**

   Proposition 3.3. *Let $A \subset \mathbb{Z}$ and bounded above. There exists $N \in A$ such that $N \leq M$ for any upper bound of A.*

   Similarly, for $A \subset \mathbb{Z}$ and bounded below. There exists $N \in A$ such that $N \geq M$ for any other lower bound of A.

   We do not have this property in Q!!

   Proposition 3.4. *There exists a set $A \subset \mathbb{Q}$ which is bounded above with the property that any $\alpha \in A$ of A there is a $\beta \in A$ such that $\beta > \alpha$.*

   Proof. Consider $A = \{x \in \mathbb{Q} : x^2 < 2\}$. Clearly 2 is an upper bound of A, so A is bounded above. Let $\alpha \in \ A$. Let $\beta = \alpha + \frac{2-\alpha^2}{\alpha+2}$. Clearly, $\beta > \alpha$ and $\beta \in \mathbb{Q}$. Also, $\beta^2 - 2 = \frac{2(\alpha^2-2)}{(\alpha+2)^2} < 0$. $\square$

3.2 Striking Similarity between $\mathbb{Z}$ and $\mathbb{Q}$

There exists a bijection from $\mathbb{Z}$ to $\mathbb{Q}$.

3.2.1 Cardinality

Cardinality of a set A is the number of elements of A, we denote it by $|A|$. It can be finite and it can be infinite. If there exists a bijection $f : A \to B$ then we say that $|A| = |B|$.

Definition 3.3. *We say that a set A is countable if there exists a bijection $f : N \to A$ where $N \subsetneq \mathbb{N}$ is finite or $N = \mathbb{N}$. In the first case we say that A is finite and in the later case we say A is countably infinite.*

Example 3.4. *$\mathbb{Z}$ is countable. Define $f : \mathbb{N} \to \mathbb{Z}$ as*

$$f(n) = \begin{cases} \frac{n}{2} & if\ n\ is\ even \\ -\frac{n-1}{2} & if\ n\ is\ odd. \end{cases}$$

Example 3.5. *Suppose $A \subsetneq \mathbb{N}$ and infinite then $|A| = |\mathbb{N}|$.*

Proof. Let a_1 is the smallest element of A, a_2 be the smallest element of $A \setminus \{a_1\}$, a_3 be the smallest element of $A \setminus \{a_1, a_2\}$ and so on. So we have $a_1 < a_2 < a_3 < \dots$ If $a \in A$ consider $\{n \in A : n \leq a\}$ this set is finite say k elements then $a = a_k$. So the map $f(l) = a_l,\ l \in \mathbb{N}$ will give us the required bijection. □

Example 3.6. *Finite union of countable sets is countable.*

Proof. If all of them are finite then nothing to prove. Let A_1 and A_2 be two countably infinite set. Then there exists bijections $\phi_1 : 2\mathbb{N} \to A_1$ and $\phi_2 : (2\mathbb{N} + 1) \to A_2$. Combining these two bijections we easily get bijection from $\mathbb{N}$ onto $A_1 \cup A_2$. □

What about countable union? Let $A_1, A_2, \dots$ be countable sets. To avoid repetition let $B_1 = A_1$ and $B_i = A_i \setminus \cup_{k=1}^{i-1} A_k$. Each B_i is countable so list its elements as $b_{i,1}, b_{i,2}, \dots$ and $A = \cup_{i \geq 1} A_i = \cup_{i \geq 1} B_i$. Consider the map $f : A \to \mathbb{N} \times \mathbb{N}$ as $f(b_{i,j}) = (i, j)$ is one-one. Thus $|A| \leq |\mathbb{N} \times \mathbb{N}|$. Following proposition will tell us it is countable.

Proposition 3.5. *The set $\mathbb{N} \times \mathbb{N}$ is countable.*

In particular, countable union of countable sets is countable.

Proof. Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as $f(m, n) = 2^{m-1}(2n - 1)$. Observe $2^{m-1}(2n - 1) = 2^{p-1}(2q - 1)$ if and only if $m = p$ and $n = q$. For onto consider $l \in \mathbb{N}$ then either l is odd or even. If it is odd then $l = 2p - 1$ for some $p \in \mathbb{N}$ consider $m = 1$ and $n = p$. If even the it can be factorized into powers of 2 and an odd number. □

Corollary 3.7. $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$.

Does there exists an uncountable set? i.e does there exists an infinity bigger than the countable infinity.

Consider $T(\mathbb{N}) = \{f : \mathbb{N} \to \{0, 1\}\}$. What is the cardinality of $T(\mathbb{N})$?

Proposition 3.6. *No bijection from $\mathbb{N}$ to $T(\mathbb{N})$*

Proof. Let $\phi : \mathbb{N} \to T(\mathbb{N})$ be a one-one map. Denote $\phi(n) = f_n$. Define $h(n) = \begin{cases} 1 & \text{if } f_n(n) = 0 \\ 0 & \text{if } f_n(n) = 1. \end{cases}$.
Certainly $h \in T(\mathbb{N})$. If ϕ is onto then there exists a $l \in \mathbb{N}$ such that $\phi(l) = h$. Then, $h(l) = 1 \Rightarrow f_l(l) = 0 \Rightarrow \phi(l) = 0$. Similarly if $h(l) = 0 \Rightarrow f_l(l) = 1 \Rightarrow \phi(l) = 1$. Hence a contradiction. □

Corollary 3.8. $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$ *and* $\mathcal{P}(\mathbb{N})$ *is not countable.*

Proof. Considering the map $x \mapsto \{x\}$ we get $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$. Now consider the bijection $\psi : \mathcal{P}(\mathbb{N}) \to T(\mathbb{N})$ by $\psi(B) = \chi_B$. To show it is onto, let $f \in T(\mathbb{N})$ define $B = \{n \in \mathbb{N} : f(n) = 1\}$. □

In fact the following more general statement is true.

Theorem 3.9. *Let* A *be any set then* $|A| < |\mathcal{P}(A)|$.

Proof. If $|A| < \infty$ then $|\mathcal{P}(A)| = 2^{|A|}$. Assume A is an infinite set. Suppose there exists a bijection $f : A \to \mathcal{P}(A)$. Consider $B = \{x : x \notin f(x)\}$. Clearly $B \in \mathcal{P}(A)$. If f is bijection then there exists a $y \in A$ such that $f(y) = B$. Now either $y \in B$ or $y \notin B$. If $y \in B$ then $y \in f(y)$ a contradict. If $y \notin B$ then $y \in f(y) = B$. Hence f cannot be a bijection. So, $|A| < |\mathcal{P}(A)|$. □

3.3 Cantor-Schröeder-Bernstein

Theorem 3.10. *Let* X *and* Y *be two sets. If* $|X| \leq |Y|$ *and* $|Y| \leq |X|$ *then* $|X| = |Y|$.

Proof. (Sketch) Let $M \subset Y$ and $N \subset X$ such that there exist bijections $f : X \to M$ and $g : Y \to N$. Let $x \in X$. If $x \in g(Y)$ we consider $g^{-1}(x)$ call it *first ancestor* of x. If $g^{-1}(x) \in M$ then we consider $(f^{-1}g^{-1})(x)$. Call it *second ancestor*. Continue the process of identifying ancestry of every x. Now there are three cases

1. x has infinitely many ancestors. Denote those x as X_i.
2. x has even number of ancestor(s) (0 is an even number!) Denote those x as X_e.
3. x has odd numbers of ancestors. Denote those x as X_o.

Clearly, $X = X_i \cup X_e \cup X_o$. Define $F : X \to Y$ as $F(x) = \begin{cases} f(x) & if\ x \in X_i \cup X_e \\ g^{-1}(x) & if\ x \in X_o. \end{cases}$

F is a bijection □