Some properties of Natural numbers and Real numbers

1 Preliminaries

Definition 1.1. A binary relation ρ on a nonempty set S is called a *partial order relation* if

1. $a\rho a$ for all $a \in S$ (reflexivity),
2. $a, b \in S$, $a\rho b$ and $b\rho a$ imply $a = b$ (antisymmetry),
3. $a, b, c \in S$, $a\rho b$ and $b\rho c$ imply $a\rho c$ (transitivity).

Definition 1.2. A nonempty set S together with a partial ordering ρ is called a *partially ordered* set. A partially ordered set (S, ρ) is called *totally ordered* if for any $a, b \in S$, either $a\rho b$ or $b\rho a$ or both (in which case $a = b$). A totally ordered set (S, ρ) is called *well-ordered* if every nonempty subset of S has a smallest element.

Definition 1.3. Let $(S, \leq)$ be a partially ordered set (please do not confuse $\leq$ with its usual meaning in $\mathbb{R}$, here $\leq$ is just a replacement for ρ above for convenience). Let A be a nonempty subset of S. An element $x \in S$ is called an *upper bound* of A if $a \leq x$ for all $a \in A$. An upper bound s of A is called the *least upper bound* (in brief, *lub*) or *supremum* (in brief, *sup*) if $s \leq x$ for any upper bound x of A. An element $y \in S$ is called a *lower bound* of A if $y \leq a$ for all $a \in A$. A lower bound t of A is called the *greatest lower bound* (in brief, *glb*) or *infimum* (in brief, *inf*) if $y \leq t$ for any lower bound y of A. An lub (or glb), if it exists, is unique by definition. In this context, we just mention, a partially ordered set is called a *lattice* if there exist lub and glb for every pair of elements in the set. Let A be a nonempty subset of S. If A has an upper bound in S, then A called *bounded above* and if A has a lower bound in S, then A is called *bounded below*. A is called *bounded* if it is both bounded above and bounded below. A totally ordered set $(S, \leq)$ is said to have the *lub property* if every subset A of S which is bounded above has an lub (in S). Similarly, a totally ordered set $(S, \leq)$ is said to have the *glb property* if every subset A of S which is bounded below has a glb (in S).

Definition 1.4. A nonempty set F together with two binary operation $+$ and $\cdot$ is called a *field* if the following conditions are satisfied ($+$ and $\cdot$ are binary operations on F imply that $a+b, a\cdot b \in F$ for all $a, b \in F$):

1. $a + b = b + a$ for all $a, b \in F$,
2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in F$,
3. there exists $0 \in F$ such that $a + 0 = a$ for all $a \in F$,

4. for each $a \in F$, there exists $-a \in F$ such that $a + (-a) = 0$,

5. $a \cdot b = b \cdot a$ for all $a, b \in F$,

6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in F$,

7. there exists $1 \in F$ such that $a \cdot 1 = a$ for all $a \in F$,

8. for each $0 \neq a \in F$, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$,

9. $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Notations: We denote the sets of natural numbers, integers, rational numbers and real numbers by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ respectively.

Here we assume the constructions of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ and the following properties:

1. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are totally ordered with usual $\leq$.

2. $(\mathbb{N}, +, \cdot)$ is a totally ordered additively and multiplicatively commutative *semiring* with multiplicative identity (satisfying 1,2,5,6,7,9 of Definition 1.4).

3. $(\mathbb{Z}, +, \cdot)$ is a totally ordered commutative *ring* with identity (satisfying 1,2,3,4,5,6,7,9 of Definition 1.4).

4. $(\mathbb{Q}, +, \cdot)$ a totally ordered field.

5. $(\mathbb{R}, +, \cdot)$ is a totally ordered field with lub property.

Theorem 1.5. $\mathbb{N}$ *is well-ordered, i.e., every nonempty subset of natural numbers contains a smallest element.*

Proof. Let $\emptyset \neq A \subseteq \mathbb{N}$. If $A = \mathbb{N}$, then 1 is the smallest element of A. Let $A \subsetneq \mathbb{N}$. Let $P = \{x \in \mathbb{N} \mid x \leq n \text{ for all } n \in A\}$. Now $P \neq \emptyset$ as $1 \in P$. Then if $x \in P \implies x + 1 \in P$, then by induction $P = \mathbb{N}$ which implies $A = \emptyset$, for otherwise, if $n \in A$, then $n + 1 \notin P = \mathbb{N}$ which is a contradiction. Thus there exists $x_0 \in P$ such that $x_0 + 1 \notin P$. Then there exists $n_0 \in A$ such that $x_0 + 1 > n_0$. Then $x_0 + 1 \geq n_0 + 1$, i.e., $x_0 \geq n_0$. Again $x_0 \leq n_0$ as $x_0 \in P$ and $n_0 \in A$. So $x_0 = n_0 \in A$ and $x_0 \leq n$ for all $n \in A$ as $x_0 \in P$. Therefore x_0 is the least element of A. □

2 Cardinal numbers

Definition 2.1. Let $\mathscr{C}$ be a collection of sets. Define a binary relation $\sim$ on $\mathscr{C}$ by $A \sim B$ if and only if there exists a bijective map from A onto B. It is easy to see that $\sim$ is an equivalence relation on $\mathscr{C}$. For any $A \in \mathscr{C}$, the equivalence class, $\{B \in \mathscr{C} \mid B \sim A\}$ of A under the equivalence relation $\sim$ is said to be the *cardinal number* of A and is denoted by $|A|$. Two sets A and B are said to be

numerically equivalent if $A \sim B$, i.e., $|A| = |B|$. For convenience, we write $n = |\{1, 2, \ldots, n\}|$ for any $n \in \mathbb{N}$ and $|\emptyset| = 0$. A set A is called *finite* if $|A| = 0$ or $|A| = n$, i.e., if there exists a bijective map from A onto $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. A set is *infinite* if it is not finite, i.e., if there does not exist a bijective map from A onto $\{1, 2, \ldots, n\}$ for any $n \in \mathbb{N}$. A cardinal number is said to be *infinite* (resp. *finite*) if it is the cardinal number of an infinite set (resp. finite set). The cardinal number of $\mathbb{N}$ is denoted by $\aleph_0$.

Theorem 2.2. (Schroeder-Bernstein Theorem) *Let X and Y be two nonempty sets such that there exist injective maps $f : X \longrightarrow Y$ and $g : Y \longrightarrow X$. Then there exists a bijective map from X onto Y* (for proof, see Simmons Pg 29–30).

Definition 2.3. Let $\mathscr{C}$ be a collection of sets. Define $|A| \leq |B|$ if and only if there exists an injective map from A into B. Then by Schroeder-Bernstein Theorem, we have $\leq$ is a partial order relation on $\mathscr{C}$. We write $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$, i.e., if there exists an injective map from A into B, but there does not exist any bijective map from A onto B or, equivalently, there does not exist any injective map from B into A. For example, $|A| < |\mathscr{P}(A)|$ for any set A, where $\mathscr{P}(A)$ denotes the set of all subsets of A. We denote $|\mathscr{P}(A)| = 2^{|A|}$.

Theorem 2.4. (Cardinal Arithmatics) *Let A, B be two sets such that $A \cap B = \emptyset$. Let $\alpha = |A|$ and $\beta = |B|$. Define $\alpha + \beta = |A \cup B|$, $\alpha\beta = |A \times B|$ and $\alpha^\beta = |A^B|$, where A^B denotes the set of all maps from B into A. Then*

1. $\alpha + \beta = \beta + \alpha$, $\alpha\beta = \beta\alpha$
2. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.
3. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.
4. $\alpha^{(\beta+\gamma)} = \alpha^\beta \cdot \alpha^\gamma$.
5. $(\alpha\beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$.
6. $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.
7. $\alpha \leq \beta \Longrightarrow \alpha + \gamma \leq \beta + \gamma$, $\alpha\gamma \leq \beta\gamma$, $\alpha^\gamma \leq \beta^\gamma$, $\gamma^\alpha \leq \gamma^\beta$.
8. $\alpha \leq \alpha + \beta$, $\alpha \leq \alpha\beta$ *(for $\beta \neq 0$)*.
9. $\alpha < 2^\alpha$.

For all infinite cardinal numbers α, β, the following results hold:

10. $\aleph_0 \leq \alpha$, $n < \alpha$ *for all* $n \in \mathbb{N}$.
11. $\alpha + \alpha = \alpha$, $\alpha\alpha = \alpha$, $n\alpha = \alpha$, $\alpha^n = \alpha$ *for all* $n \in \mathbb{N}$.

12. $\alpha \leq \beta \Longrightarrow \alpha + \beta = \beta$, $\alpha\beta = \beta$. *In particular,* $\aleph_0 + \alpha = \alpha$, $\aleph_0\alpha = \alpha$.

Proof. Below we prove (6). Others are left as exercises.

Let A, B, C be three sets such that $\alpha = |A|$, $\beta = |B|$ and $\gamma = |C|$.
Define the map $\phi : (A^B)^C \longrightarrow A^{B\times C}$ by $\phi(f)(b,c) = f(c)(b)$ for all $b \in B$ and $c \in C$. Note that the maps have the following domains and co-domains: $\phi(f) : B \times C \longrightarrow A$, $f : C \longrightarrow A^B$, $f(c) : B \longrightarrow A$ for all $c \in C$. Now

$$\begin{aligned} & \phi(f_1) = \phi(f_2) \\ \Longrightarrow\ & \phi(f_1)(b,c) = \phi(f_2)(b,c) \ \text{ for all } b \in B, c \in C \\ \Longrightarrow\ & f_1(c)(b) = f_2(c)(b) \ \text{ for all } b \in B, c \in C \\ \Longrightarrow\ & f_1(c) = f_2(c) \ \text{ for all } c \in C \\ \Longrightarrow\ & f_1 = f_2. \end{aligned}$$

Therefore ϕ is injective.

Let $F \in A^{B\times C}$. Define $f : C \longrightarrow A^B$ by $f(c)(b) = F(b,c)$ for all $b \in B$, $c \in C$. Then

$$\begin{aligned} & c_1 = c_2 \\ \Longrightarrow\ & (b, c_1) = (b, c_2) \ \text{ for all } b \in B \\ \Longrightarrow\ & F(b, c_1) = F(b, c_2) \quad \text{for all } b \in B \\ \Longrightarrow\ & f(c_1)(b) = f(c_2)(b) \quad \text{for all } b \in B \\ \Longrightarrow\ & f(c_1) = f(c_2). \end{aligned}$$

So f is well-defined. Also $\phi(f)(b,c) = f(c)(b) = F(b,c)$ for all $b \in B$, $c \in C$. Thus $\phi(f) = F$. Therefore ϕ is surjective and hence bijective. So we have $|(A^B)^C| = |A^{B\times C}|$, i.e., $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$. □

Definition 2.5. A set is A called *countable* if $|A| \leq \aleph_0$. All finite sets are countable. A countable infinite set is called *countably infinite*. A set A is called *uncountable* if it is not countable ($|A| > \aleph_0$), i.e., if there does not exist any injective map from A into $\mathbb{N}$. The set $\mathbb{R}$ of all real numbers is uncountable. The cardinal number of $\mathbb{R}$ is denoted by c.

Theorem 2.6. *The following results hold:*

1. *Let A be an infinite subset of $\mathbb{N}$. Then $|A| = \aleph_0$.*
2. *Let A be an infinite set and B be a finite set. Then $|A \cup B| = |A|$. If C is a finite subset of A, then $|A \setminus C| = |A|$.*
3. *Let A be an infinite set. Then there exists a subset B of A such that $|B| = |\mathbb{N}|$. That is, every infinite set contains a copy of $\mathbb{N}$.*
4. *A set is infinite if and only if it has a bijection with a proper subset of itself.*

5. *Let* $\{A_i \mid i \in I\}$ *be a collection of sets such that* $|A_i| \leq \aleph_0$*, where* $I \subseteq \mathbb{N}$*. Then* $|\bigcup_{i\in I} A_i| \leq \aleph_0$*. That is, countable union of countable sets is countable.*

6. $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$*, i.e.,* $\aleph_0^2 = \aleph_0$*. In general,* $\aleph_0^n = \aleph_0$ *for all* $n \in \mathbb{N}$*.*

7. *The set* $\mathbb{Z}$ *of all integers and the set* $\mathbb{Q}$ *of all rational numbers are countable, i.e.,* $|\mathbb{Z}| = \aleph_0$ *and* $|\mathbb{Q}| = \aleph_0$*.*

8. *Let* A *be an infinite subset of* $\mathbb{Q}$*, then* $|A| = \aleph_0$*.*

9. $|\mathbb{Q}^n| = \aleph_0$ *for all* $n \in \mathbb{N}$*.* $|\bigcup_{i\in I} A_i| \leq \aleph_0$ *where* $A_i \subseteq \mathbb{Q}$ *for all* $i \in I \subseteq \mathbb{N}$*.*

10. *Let* A, B *be two non-empty sets,* $f : A \longrightarrow B$ *be a surjective map and* A *is countable. Then* B *is also countable, i.e., image of a countable set is countable.*

11. $c > \aleph_0$*, i.e., the set of real numbers is uncountable.*

12. $2^{\aleph_0} = c$*, i.e.,* $|\mathbb{R}| = |\mathscr{P}(\mathbb{N})|$*.*

13. *For any* $a < b$ *in* $\mathbb{R}$*,* $c = |\mathbb{R}| = |(a, b)| = |[a, b]| = |[a, b)| = |(a, b]| = |(0, 1)| = |[0, 1]| = |[0, 1)| = |(0, 1]|$*.*

14. $|\mathbb{N} \times \mathbb{R}| = |\mathbb{Q} \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}^n| = |\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}| = c$ *for all* $n \in \mathbb{N}$*. Note that* $c^{\aleph_0} = c$*.*

15. $|\mathbb{N}^{\mathbb{R}}| = |\mathbb{Q}^{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}| = 2^c$*. Note that,* ${\aleph_0}^c = c^c = 2^c$*.*

3 Properties of rational numbers

Theorem 3.1. $\mathbb{Q}$ *is* densely ordered*, i.e., between any two rational numbers, there exist infinite number of rational numbers.*

Hint: $a < \frac{a+b}{2} < b$, $a < \frac{a+\frac{a+b}{2}}{2} < \frac{a+b}{2}$ and so on.

Theorem 3.2. $\mathbb{Q}$ *is* archimedian ordered*, i.e., for any* $a, b \in \mathbb{Q}$ *with* $a, b > 0$*, there exists* $n \in \mathbb{N}$ *such that* $nb > a$*.*

Proof. Suppose $nb \leq a$ for all $n \in \mathbb{N}$. Then $\frac{nb}{a} \leq 1 \leq m$ for all $m, n \in \mathbb{N} \Longrightarrow \frac{n}{m} \leq \frac{a}{b}$ for all $m, n \in \mathbb{N}$ $\Longrightarrow x \leq \frac{a}{b}$ for all $x \in \mathbb{Q}^+$, which is a contradiction (as $\frac{a}{b} + 1 > \frac{a}{b}$). □

Proposition 3.3. $\mathbb{Q}$ *does not have the lub property.*

Proof. Let $A = \{x \in \mathbb{Q} \mid x > 0,\ x^2 < 2\}$. Now A is bounded above as $x < 2$ for all $x \in A$. Let $x \in A$. Define $y = \frac{2x+2}{x+2} = x + \frac{2-x^2}{x+2}$. Since $x^2 < 2$, $y > x$. Also $2 - y^2 = \frac{2(2-x^2)}{(x+2)^2} > 0$. Thus $y^2 < 2$ and so $y \in A$. Therefore for each $x \in A$, there is a y in A such that $y > x$, i.e., A has no greatest element. Again let $B = \{x \in \mathbb{Q} \mid x > 0,\ x^2 > 2\}$. Let $x \in B$. Define $y = x - \frac{x^2-2}{x+2} = \frac{2x+2}{x+2}$. Then $0 < y < x$ and $y^2 > 2$. So B has no least element. Finally, there is no rational number y such that $y^2 = 2$ (surely, its proof is known to you). Thus A has no lub. □

4 Properties of $\mathbb{R}$

Theorem 4.1. *$\mathbb{R}$ is archimedean ordered, i.e., for any $x, y \in \mathbb{R}$ with $x > 0$, there exists $n \in \mathbb{N}$ such that $nx > y$.*

Proof. Let $A = \{nx \mid n \in \mathbb{N}\}$. If the result is not true, then y is an upper bound of A. But then A has a lub in $\mathbb{R}$. Let $\alpha = \sup(A)$. Since $x > 0$, $\alpha - x < \alpha$ and $\alpha - x$ is not an upper bound of A. Then $\alpha - x < mx$ for some $m \in \mathbb{N}$. But then $\alpha < (m+1)x \in A$ which is impossible as $\alpha = \sup(A)$. □

Theorem 4.2. *$\mathbb{Q}$ is dense in $\mathbb{R}$, i.e., if $x, y \in \mathbb{R}$ with $x < y$, then there exists $p \in \mathbb{Q}$ such that $x < p < y$.*

Proof. We have $y - x > 0$. So there exists $n \in \mathbb{N}$ such that $n(y-x) > 1$, i.e., $ny > 1 + nx$ Also $m_1, m_2 \in \mathbb{N}$ such that $m_1 \cdot 1 > nx$ and $m_2 \cdot 1 > -nx$. Then $-m_2 < nx < m_1$. This implies there exists $m \in \mathbb{Z}$ such that $m - 1 \leq nx < m$. Therefore $nx < m \leq 1 + nx < ny$ which imples $x < \frac{m}{n} < y$. This proves the result for $p = \frac{m}{n}$. □

Definition 4.3. (Limit points of a subset of $\mathbb{R}$): Let $S \subseteq \mathbb{R}$ and $x \in \mathbb{R}$. Then x is called a *limit point* of S if for every $\delta > 0$, $(x-\delta, x+\delta) \cap (S \setminus \{x\}) \neq \emptyset$. In other words, every *neighborhood* of x contains at least one point of S different from x itself, where $N \subseteq \mathbb{R}$ is a neighborhood of x if there exists $\delta > 0$, $\delta \in \mathbb{R}$ such that $(x-\delta, x+\delta) \subseteq N$. It is important to understand that δ in the definition of a limit point is arbitrary, i.e., the condition holds for ANY δ (i.e., δ can be as small as you please. But do not romanticize δ to be the length of a very small nano particle! It is simply, arbitrary). Another important thing to note in the definition of a limit point is that $(x-\delta, x+\delta) \cap (S \setminus \{x\}) \neq \emptyset \iff (x-\delta, x+\delta) \cap S$ is infinite (prove!). Finally, note that the limit of a sequence of real numbers is not the same as limit points. For example, the limit of the constant sequence $\{1, 1, 1, \ldots\}$ is 1. But as a set, $\{1, 1, 1, \ldots\} = \{1\}$ and it has no limit points (prove!).

Example 4.4. For example, 0 and 1 are limit points of the set $\{x \in \mathbb{R} \mid 0 < x < 1\}$, i.e., the open interval $(0, 1)$. Note that for any $\delta > 0$, $(-\delta, \delta) \cap (0, 1) \neq \emptyset$ as $0 < \frac{\delta}{2} < \delta < 1$ for $\delta < 1$ and $(0, 1) \subseteq (-\delta, \delta)$ for $\delta \geq 1$. Similarly, $(1-\delta, 1+\delta) \cap (0, 1) \neq \emptyset$ as $0 < 1 - \delta < 1 - \frac{\delta}{2} < 1$ for $\delta < 1$ and $(0, 1) \subseteq (1-\delta, 1+\delta)$ for $\delta \geq 1$. Another example is that 0 is a limit point of set $\left\{\frac{1}{n} \mid n \in \mathbb{N}\right\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots\right\}$ as for any $\delta > 0$, there exists $n \in \mathbb{N}$ such that $0 < \frac{1}{n} < \delta$.

Now which subsets of $\mathbb{R}$ always have limit points? Note that the set $\{1, 2, 3\}$ is finite and bounded, but it has no limits points (prove!). Also $\mathbb{N} = \{1, 2, 3, \ldots\}$ is infinite and not bounded. It has also no limit points (prove!).

Theorem 4.5. *(Bolzano-Weirstrass Theorem) Every bounded infinite subset of $\mathbb{R}$ has a limit point.*

Proof. Let S be a bounded infinite subset of $\mathbb{R}$. Since S is bounded, we have, $S \subseteq [a, b]$ for some $a, b \in \mathbb{R}$ with $a \leq b$. Let $A = \{x \in \mathbb{R} \mid x$ exceeds only a finite number of elements of $S\}$. Now

$A \neq \emptyset$ as $a \in A$. Also A is bounded above. In fact, for all $x \in A$, $x < b$ as for any $y \in \mathbb{R}$ with $y \geq b$ exceeds infinite number of elements of S (in fact, all elements of S and S is infinite). Thus by lub property, A has an lub, say, $r \in \mathbb{R}$.

We show that r is a limit point of S. Let $\delta > 0$. Then $r - \delta \in A$ and $r + \delta \notin A$. Thus $(r-\delta, r+\delta) \cap S$ contains infinite number of elements of S. This implies r is a limit point of S. □

4.1 Decimal expansion of Real numbers

Let $x > 0$, $x \in \mathbb{R}$. Let n_0 be the largest integer such that $n_0 \leq x$.

Having chosen $n_0, n_1, \ldots, n_{k-1}$, let n_k be the largest integer such that $n_0 + \frac{n_1}{10} + \cdots + \frac{n_k}{10^k} \leq x$.

Let $E = \left\{ n_0 + \frac{n_1}{10} + \cdots + \frac{n_k}{10^k} \mid k = 0, 1, 2, 3, \ldots \right\}$. Then $x = \sup(E)$. The decimal expansion of x is given by $n_0.n_1n_2 \ldots n_k \ldots$.

◊ **Exercise 4.1.** Prove that $\mathbb{R}$ has the glb property.

◊ **Exercise 4.2.** Find lub and glb of the following subsets of $\mathbb{R}$:

1. $S = \left\{ 1 + \frac{1}{n} \mid n \in \mathbb{N} \right\}$,
2. $S = \left\{ \frac{n}{n+2} \mid n \in \mathbb{N} \right\}$.

◊ **Exercise 4.3.** Let $\emptyset \neq S, T \subseteq \mathbb{R}$ be two bounded sets. Prove the following:

1. $S \subseteq T \Longrightarrow \inf(T) \leq \inf(S) \leq \sup(S) \leq \sup(T)$.
2. If $M = \{x \in \mathbb{R} \mid -x \in S\}$, then $\sup(M) = -\inf(S)$ and $\inf(M) = -\sup(S)$.
3. If $A = \{x + y \mid x \in S,\ y \in T\}$, then $\sup(A) = \sup(S) + \sup(T)$ and $\inf(A) = \inf(S) + \inf(T)$.
4. If $B = \{|x - y| \mid x, y \in S\}$, then $\sup(B) = \sup(S) - \inf(S)$ and $\inf(B) = 0$.