Chapter 1

The Real Numbers

1.1. Some Preliminaries

Discussion: The Irrationality of $\sqrt{2}$. We begin with the **natural numbers**

$$\mathbf{N} = \{1, 2, 3, \cdots\}.$$

In **N** we can do addition, but in order to do subtraction we need to extend **N** to the **integers**

$$\mathbf{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

In **Z** we can do addition, subtraction and multiplication, but in order to perform division we need to extend **Z** to the **rational numbers**

$$\mathbf{Q} = \{\text{all fractions } \tfrac{p}{q} \text{ where } p \text{ and } q \text{ are integers with } q \neq 0\}.$$

In **Q** we have a *field* structure: addition and multiplication are defined with commutative, associative and distributive properties and the existence of additive and multiplicative inverses.

Also **Q** has a natural *order* structure defined on it (based on the ordering in **N**). Given any two rational numbers r and s, exactly one of the following is true:

$$r < s; \quad r = s; \quad r > s.$$

However, can we measure all lengths with rational numbers? If we have a square with each side length 1, can we measure the length of its diagonal with a rational number? The answer is No.

Theorem 1.1. *There is no rational number whose square is 2.*

This course is a course primarily focusing on the theory developments and the proofs. To get an earlier flavor what it looks like, let us see how to write a rigorous proof of the previous theorem.

Proof. The theorem asserts that no rational numbers r exist such that $r^2 = 2$; that is, if r is any rational number then $r^2 \neq 2$. Since any rational number r is given by $r = \frac{p}{q}$ for some integers p and q with $q \neq 0$. Therefore, what we need to show is that no matter what such p and q are chosen it is never the case $(p/q)^2 = 2$. The line of attack is indirect, using a method of proof by contradiction; the idea is to show the opposite cannot be true.

That is, assume there *exist* some integers p and q with $q \neq 0$ such that $(p/q)^2 = 2$ and we want to reach a conclusion that is unacceptable (absurd). We can also assume p and q have no common factors since any common factor can be canceled out, leaving the fraction $\frac{p}{q}$ unchanged. Since

$$p^2 = 2q^2,$$

we know p^2 is an *even* number, and hence p itself must be even (otherwise p is odd and p^2 would be odd). So write $p = 2k$ where k is an integer. Then $p^2 = 4k^2 = 2q^2$. Hence we have $q^2 = 2k^2$, which again implies q must be an even number. However, in the beginning, we assumed p and q have no common factors, but we have reached a conclusion saying p and q have a common factor 2 (since both are even). The contradicting conclusions show that our opposite assumption that *there exist some integers p and q with $q \neq 0$ such that* $(p/q)^2 = 2$ must be false. This proves the original statement of the theorem. □

Sets and Functions.

Definition 1.1. A **set** is any collection of objects. These objects are referred to as the **elements** of the set. A set containing no elements is called the **empty set** and is denoted by $\emptyset$.

Given a set A, if x is an element of A then we write $x \in A$ (and say x is in A or belongs to A or, simply, x is an element of A). If x is not an element of A then we write $x \notin A$.

Given two sets A and B, if every element of A is an element of B, then we write $A \subseteq B$ or $B \supseteq A$; in this case, we say A is a **subset** of B. Note that two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

Given two sets A and B (or a family of sets $\{A_\alpha\}_{\alpha \in I}$), the **union** $A \cup B$ (or the **union** $\bigcup\limits_{\alpha \in I} A_\alpha$) is defined to be the set consisting of all x such that either $x \in A$ or $x \in B$ (or such that $x \in A_\alpha$ for *some* $\alpha \in I$).

Similarly, given two sets A and B (or a family of sets $\{A_\alpha\}_{\alpha \in I}$), the **intersection** $A \cap B$ (or the **intersection** $\bigcap\limits_{\alpha \in I} A_\alpha$) is defined to be the set consisting of all x such that $x \in A$ and $x \in B$ (or such that $x \in A_\alpha$ for *all* $\alpha \in I$).

If $A \cap B = \emptyset$, we say A and B are **disjoint**. We also define

$$B \setminus A = \{x \in B \,:\, x \notin A\}.$$

If B is a fixed underlying large set, we usually write $B \setminus A$ as A^c for all subsets A of B and call it the **complement** (in B) of the set A. Note that $(A^c)^c = A$; this is to say, *x is an element of A (or A^c) if and only if x is not an element of A^c (or A).*

We have the following

Theorem 1.2 (**De Morgan's Laws**). *Let $A_\alpha \subseteq B$ for each index $\alpha \in I$. Then*

$$\left(\bigcup_{\alpha \in I} A_\alpha\right)^c = \bigcap_{\alpha \in I} A_\alpha^c; \quad \left(\bigcap_{\alpha \in I} A_\alpha\right)^c = \bigcup_{\alpha \in I} A_\alpha^c.$$

Proof. Let's only show that first equality. Equality of two sets $C = D$ means that: if $x \in C$ then $x \in D$, and if $x \in D$ then $x \in C$.

First, assume $x \in (\bigcup_{\alpha \in I} A_\alpha)^c$ and prove $x \in \bigcap_{\alpha \in I} A_\alpha^c$. Since x is not an element of $\bigcup_{\alpha \in I} A_\alpha$, by definition (of union set), x is not element of any of sets A_α; hence $x \in A_\alpha^c$ for all $\alpha \in I$. By definition of intersection set, $x \in \bigcap_{\alpha \in I} A_\alpha^c$.

Second, assume $x \in \bigcap_{\alpha\in I} A_\alpha^c$ and prove $x \in (\bigcup_{\alpha\in I} A_\alpha)^c$. Suppose, for contradiction, x is an element of $\bigcup_{\alpha\in I} A_\alpha$. Then $x \in A_\alpha$ for some $\alpha \in I$ (maybe more such α's). Hence, by definition of complement set, x is not in A_α^c and hence x is not in the intersection set $\bigcap_{\alpha\in I} A_\alpha^c$, a contradiction. □

Definition 1.2. Given two sets A and B, a **function** from A to B is a rule f that associates each element x in A a single element y in B.

In this case, we write $f\colon A \to B$ with $x \mapsto y$, and write $y = f(x)$. The set A is called the **domain** of the function and B the **target** of the function. $y = f(x)$ is called the **image** of x. The set of all images $f(x)$ of elements x in A is called the **range** of the function and sometimes is denoted by $f(A)$. Note that $f(A)$ is always a subset of the target B.

Some functions cannot be given by formulas.

Example 1.1. (i) **Dirichlet's function**:

$$g(x) = \begin{cases} 1 & x \in \mathbf{Q} \\ 0 & x \notin \mathbf{Q}. \end{cases}$$

(ii) **Absolute value function**:

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

This function satisfies the following properties: $|x| \geq 0$ for all x, and $|x| = 0$ if and only if $x = 0$; moreover,

$$|ab| = |a||b|; \quad |a+b| \leq |a| + |b| \ (\textbf{Triangle Inequality}).$$

Logic and Proofs. A rigorous proof in mathematics follows logical steps, relies on certain known true facts and uses some accepted hypotheses to show a statement (a theorem, proposition or lemma) is valid.

A proof can follow a *direct* approach by deriving the validity of the statement directly or can use an *indirect* method by showing the opposite of the statement will never hold.

An indirect method is often called the **proof by contradiction**, where, under the assumption that the original statement be false or under the negation of the original statement, an absurd conclusion (a desired contradiction) would be reached after logical reasonings based on known results, definitions and facts, along with the *assumption of the negation of the original statement*. Therefore, it is often important to know how to formulate the negation of a statement in a logical way (see some Exercises in later sections).

Example 1.2. Show that two numbers a, b are equal if and only if for every number $\epsilon > 0$ it follows that $|a - b| < \epsilon$.

Proof. The meaning of "if and only if" is to show that the two statements are the same despite of being in different forms. There are two statements involved here:

(A) $a = b$ (B) For every number $\epsilon > 0$ it follows that $|a - b| < \epsilon$.

Two things are to be proved here: (i) (the "if" part) (A) is true *if* (B) is true;
(ii) (the "only if" part) (A) is true *only if* (B) is true.

Statement (ii) is just to say that: (ii') If (A) is true then (B) is true. (This is also the same as: If (B) is not true then (A) is not true.) (ii') is easy to prove. For example, if

$a = b$ (that is, if (A) is true), then $|a - b| = 0$. Hence, for every number $\epsilon > 0$ it follows that $|a - b| = 0 < \epsilon$; this is exactly the statement (B). So (ii) (the "only if" part) is proved. This is a direct proof.

The proof of (i) (the "if" part) can be given by an indirect or contradiction proof. In logic, Statement (i) is the same as the statement that: (i') If (A) is not true then (B) is not true. We prove this indirect statement (i'). Suppose (A) is not true; that is, $a \neq b$. Then $|a - b| > 0$. The number $\epsilon_0 = |a - b|$ is a number > 0. However, for this number ϵ_0, it does not follow that $|a - b| < \epsilon_0$ since the two numbers are equal; this means Statement (B) is not true. (In logic, what is the negation of statement (B)? Work on Exercise 1.2.8.) This shows (i') and hence (i) is proved. □

A useful direct method is the **mathematical induction** based on the following fact:

Theorem 1.3 (**Induction Theorem**). *Let S be some subset of* $\mathbf{N}$. *Assume*

(i) $1 \in S$.

(ii) If $k \in S$ *then* $k + 1 \in S$.

Then $S = \mathbf{N}$.

EXAMPLE 1.3. Let $y_1 = 1$ and, for each $n \in \mathbf{N}$, define $y_{n+1} = (3y_n + 4)/4$.

(a) Show $y_n < 4$ for all $n \in \mathbf{N}$.

(b) Show that $y_n < y_{n+1}$ for all $n \in \mathbf{N}$.

Proof. Use induction for both parts.

(a) $y_1 = 1 < 4$. Assume $y_k < 4$ and prove $y_{k+1} < 4$. Since $y_k < 4$, $3y_k < 12$ and hence $3y_k + 4 < 16$. Therefore, $y_{k+1} = (3y_k + 4)/4 < 16/4 = 4$.

(b) $y_2 = (3 + 4)/4 = 7/4 > 1 = y_1$. Assume $y_k < y_{k+1}$ and prove $y_{k+1} < y_{k+2}$. Since $y_k < y_{k+1}$, it follows that

$$(3y_k + 4)/4 < (3y_{k+1} + 4)/4;$$

This is just saying $y_{k+1} < y_{k+2}$. □

1.2. The Axiom of Completeness

We shall not discuss how to construct the set of real numbers, denoted by $\mathbf{R}$, from the rational numbers $\mathbf{Q}$. We assume $\mathbf{R}$ is an extension of $\mathbf{Q}$ that keeps the order and operations of $\mathbf{Q}$ but satisfies an important property called the **Axiom of Completeness**, to be defined below. Suppose we have already defined the set $\mathbf{R}$.

Least Upper Bound and Greatest Lower Bound. A set $A \subseteq \mathbf{R}$ is called **bounded above** if there exists a number $b \in \mathbf{R}$ such that $a \leq b$ for all $a \in A$. Any such a number b is called an **upper-bound** for A.

Similarly, a set $A \subseteq \mathbf{R}$ is called **bounded below** if there exists a number $b \in \mathbf{R}$ such that $a \geq b$ for all $a \in A$. Any such a number b is called a **lower-bound** for A.

Definition 1.3. A number s is called a **least upper-bound** for a set $A \subseteq \mathbf{R}$ if s satisfies the following two criteria:

(i) s is an upper-bound for A;

(ii) if b is any upper-bound for A, then $s \leq b$.

Remark 1.4. (i) If s_1 and s_2 are both a least upper-bound for A then, by the criteria (i) and (ii) of the definition, we must have that $s_1 \le s_2$ and $s_2 \le s_1$; hence $s_1 = s_2$. Therefore, if A has a least upper-bound s, then it must be *unique* and, in this case, we denote it by $s = \sup A$ (the **supremum** of A).

(ii) If $\sup A \in A$, then we say $\sup A$ is the **maximum** of A and denote it also by $\max A$. Note that every nonempty finite set of **R** has the maximum.

(iii) Similarly, we can define the **greatest lower-bound** for a set A and denote it by $\inf A$ (the **infimum** of A). Again if $\inf A \in A$ then we say $\inf A$ is the **minimum** of A and denote it by $\min A$. Note that every nonempty finite set of **R** has the minimum.

The supremum can also been characterized by the following equivalent criterion.

Lemma 1.4. *Let s be an upper-bound for a set $A \subseteq \mathbf{R}$. Then $s = \sup A$ if and only if, for each $\epsilon > 0$, there exists an element $a \in A$ such that $s - \epsilon < a$.*

Proof. 1. Assume $s = \sup A$. We show that, for each $\epsilon > 0$, there exists an element $a \in A$ such that $s - \epsilon < a$. Suppose not; then $\exists \epsilon > 0\ \forall a \in A\ (a \le s - \epsilon)$. This implies that $s - \epsilon$ is an upper-bound of A; hence, by the definition of $s = \sup A$, we have that $s - \epsilon \ge s$, a contradiction.

2. Assume $s \ne \sup A$. Then, the negation of (ii) in the definition is true; that is, there exists an upper bound b of A such that $s > b$. Let $\epsilon_0 = s - b > 0$; then $s - \epsilon_0 = b$ is an upper bound of A. Hence $\forall a \in A\ (a \le s - \epsilon_0)$; so, for this $\epsilon_0 > 0$, there is no $a \in A$ such that $s - \epsilon_0 < a$. □

We now state the **Axiom of Completeness**, which defines the set of real numbers **R**.

The Axiom of Completeness (AoC). *Every nonempty subset of **R** that is bounded above has a least upper-bound in **R**.*

1.3. Consequences of Completeness

Density of Q in R. First of all, we prove the following property of the set **N**.

Theorem 1.5 (Archimedean Property (AP)). *(i) Given any number $x \in \mathbf{R}$, there exists a number $n \in \mathbf{N}$ such that $n > x$.*

(ii) Given any number $y > 0$, there exists a number $n \in \mathbf{N}$ such that $\frac{1}{n} < y$.

Proof. We first prove (i) by contradiction. Suppose the statement (i) fails; that is, for some number $x_0 \in \mathbf{R}$ and for every $n \in \mathbf{N}$, one has $n \le x_0$. This would imply that x_0 is an upper-bound for the set **N**. Therefore **N** becomes a nonempty set of real numbers that is bounded above. Hence the Axiom of Completeness (AoC) would assert that $\alpha = \sup \mathbf{N}$ exists in **R**. Now the number $\alpha - 1$ will not be an upper-bound for **N** because it is less than α. So there exists a number $n_0 \in \mathbf{N}$ such that $n_0 > \alpha - 1$. Hence $n_0 + 1 > \alpha$. Since $n_0 + 1 \in \mathbf{N}$, this last conclusion conflicts with the fact that α is an upper-bound. This contradiction proves the statement (i).

For (ii) we apply (i) with $x = 1/y$. □

Example 1.4. Let $A = \{\frac{n}{n+1} \mid n \in \mathbf{N}\} = \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \cdots\}$. Show that $\sup A = 1$.

Proof. By definition and the lemma above, we need to show that the following two statements are true:

(i) 1 is an upper-bound of A; that is, $\forall a \in A \ (a \leq 1)$;

(ii) $\forall \epsilon > 0 \ \exists a \in A \ (1 - \epsilon < a)$.

To prove (i), let $a \in A$; then $a = \frac{n}{n+1}$ for some $n \in \mathbf{N}$. Hence $1 - a = 1 - \frac{n}{n+1} = \frac{1}{n+1} > 0$. Hence $a < 1$ and so (i) is true.

To prove (ii), let $\epsilon > 0$; then, by the (AP)(ii), there exists a number $n \in \mathbf{N}$ such that $\frac{1}{n} < \epsilon$; hence $\frac{1}{n+1} < \epsilon$. So

$$1 - \frac{n}{n+1} > 1 - \epsilon; \quad \text{taht is,} \quad \frac{n}{n+1} > 1 - \epsilon.$$

Therefore, $a = \frac{n}{n+1} \in A$ satisfies $a > 1 - \epsilon$, which proves (ii). □

Theorem 1.6 (Density of $\mathbf{Q}$ in $\mathbf{R}$). *For any two real numbers $a < b$, there exists a rational number r such that $a < r < b$; that is, $\mathbf{Q} \cap (a, b) \neq \emptyset$ for all intervals $(a, b) \subseteq \mathbf{R}$.*

Proof. Let $y = b - a > 0$. By the Archimedean Property (ii) above, we find an $n \in \mathbf{N}$ such that $\frac{1}{n} < y = b - a$; hence, $na + 1 < nb$. Let m be the smallest integer greater than na. (Think about **why such an m exists?**) Then

$$m - 1 \leq na < m.$$

From $m \leq na + 1 < nb$ we have $\frac{m}{n} < b$. From $na < m$ we have $a < \frac{m}{n}$, and hence $\frac{m}{n} \in \mathbf{Q}$ is such that $a < \frac{m}{n} < b$. □

Corollary 1.7. *For any two real numbers $a < b$, there exists an irrational number t such that $a < t < b$.*

Proof. Exercise. □

Theorem 1.8 (Existence of $\sqrt{2}$). *There exists a real number $\alpha > 0$ such that $\alpha^2 = 2$.*

Proof. Let $T = \{r \in \mathbf{Q} \ : \ r^2 < 2\}$. Then T is nonempty as $1 \in T$. Also, T is bounded above by 2 (if not, there exists a $r \in T$ such that $r > 2$ but then $r^2 > 4$). By the (AoC), $\alpha = \sup T$ exists in $\mathbf{R}$. Certainly $\alpha \geq 1$ since $1 \in T$. We now prove

$$\alpha^2 = 2. \tag{1.1}$$

We use the contradiction method to prove this. Assume $\alpha^2 \neq 2$. Then we have two cases: $\alpha^2 < 2$ or $\alpha^2 > 2$. We show either case will lead to a contradiction.

Case 1: $\alpha^2 < 2$. Let $y = \dfrac{2 - \alpha^2}{2\alpha + 1} > 0$. By the Archimedean Property (ii), there is an $n \in \mathbf{N}$ such that $\frac{1}{n} < y$. This inequality implies

$$\alpha^2 + \frac{2\alpha + 1}{n} < 2.$$

Hence $(\alpha + \frac{1}{n})^2 < 2$. Now that, by the density of $\mathbf{Q}$, there exists a number $t \in \mathbf{Q}$ such that $\alpha < t < \alpha + \frac{1}{n}$. Hence $t^2 < (\alpha + \frac{1}{n})^2 < 2$; so $t \in T$, which leads to $t \leq \alpha$, a desired contradiction.

Case 2: $\alpha^2 > 2$. Let $y = \dfrac{\alpha^2 - 2}{2\alpha} > 0$. Take $n \in \mathbf{N}$ such that $\frac{1}{n} < y$. This will imply

$$(\alpha - \frac{1}{n})^2 > \alpha^2 - \frac{2\alpha}{n} > 2.$$

On the other hand, since $\alpha - \frac{1}{n}$ is not an upper-bound for T, there exists $t \in T$ such that $\alpha - \frac{1}{n} < t$. Both numbers are nonnegative, so taking squares will yield $(\alpha - \frac{1}{n})^2 < t^2 < 2$, which is another desired contradiction.

Therefore, $\alpha^2 = 2$; that is, $\alpha = \sqrt{2}$. $\square$

Remark 1.5. As we have already proved, $\sqrt{2} \notin \mathbf{Q}$. This shows that T as a nonempty bounded-above subset of $\mathbf{Q}$ does not have a least upper-bound in $\mathbf{Q}$; hence, *the set* $\mathbf{Q}$ *does not satisfy the (AoC).*

Nested Interval Property.

Theorem 1.9 (Nested Interval Property (**NIP**))**.** *Assume, for each* $n \in \mathbf{N}$, $I_n = [a_n, b_n] = \{x \in \mathbf{R} : a_n \le x \le b_n\}$ *is a nonempty closed interval. Assume* $I_{n+1} \subseteq I_n$ *for all* $n \in \mathbf{N}$*; that is,*

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots .$$

Then $\bigcap_{n=1}^{\infty} I_n \neq \emptyset$*; that is,* $\exists x \in \mathbf{R}\ \forall n \in \mathbf{N}\ (x \in I_n)$.

Proof. Let $A = \{a_1, a_2, a_3, \cdots\}$. Then A is nonempty. We show

$$a_n < b_k \quad \text{for all } n,\ k \in \mathbf{N}, \tag{1.2}$$

which implies that A is bounded above, with any b_k being an upper-bound for A. Note that the nested intervals imply $a_n \le a_{n+1} < b_{n+1} \le b_n$ for all $n \in \mathbf{N}$. In (1.2), if $n \le k$ then $a_n \le a_k < b_k$; if $n > k$ then $a_n < b_n \le b_k$. So in any case (1.2) is proved. Now, by the (AoC), $x = \sup A$ exists in $\mathbf{R}$. Since x is an upper-bound for A, it follows $a_n \le x$ for all $n \in \mathbf{N}$. Since, by (1.2), b_n is an upper-bound for A, and hence by the definition of $x = \sup A$, it follows $x \le b_n$. Therefore $a_n \le x \le b_n$ for all $n \in \mathbf{N}$; that is, $x \in I_n$ for all $n \in \mathbf{N}$ and hence $x \in \bigcap_{n=1}^{\infty} I_n$. This completes the proof. $\square$

1.4. Cardinality

Definition 1.6. A function $f\colon A \to B$ is **1-1** if $a_1 \neq a_2$ in A implies $f(a_1) \neq f(a_2)$ in B; f is **onto** if $B = f(A)$. If $f\colon A \to B$ is 1-1 and onto, then we say that f is a **1-1 correspondence** from A onto B.

Definition 1.7. Given two sets A and B, if there exists a 1-1 correspondence from A onto B, then we say that A has the same **cardinality** as B. In this case, we write $A \sim B$.

Remark 1.8. (i) We have that $A \sim A$, that $A \sim B \Longrightarrow B \sim A$, and that $(A \sim B) \wedge (B \sim C) \Longrightarrow A \sim C$. Therefore, the relation "$\sim$" is an *equivalence relation* on sets.

(ii) Two sets consisting of finitely many elements have the same cardinality if and only if they have exactly the same number of elements. The number of the elements of a finite set A is also called the **cardinality of finite set** A and denoted by $\#(A)$.

Example 1.5. Let $\mathbf{E} = \{2, 4, 6, 8, \cdots\} = \{2n : n \in \mathbf{N}\}$ be the set of all even numbers. This is a proper subset of $\mathbf{N}$. But the function $f\colon \mathbf{N} \to \mathbf{E}$ defined by $f(n) = 2n$ is 1-1 and onto; hence $\mathbf{E}$ and $\mathbf{N}$ have the same cardinality.

Definition 1.9. A set A is called **countable** if $\mathbf{N} \sim A$. An infinite set that is not countable is called an **uncountable set**.

Remark 1.10. (i) *Equivalently*, a set A is countable if and only if A can be listed as follows:

$$A = \{a_1, a_2, a_3, a_4, \cdots\}, \quad \text{where } a_i \neq a_j \text{ whenever } i \neq j.$$

This can be easily seen by setting $a_n = f(n)$ for all $n \in \mathbf{N}$, where f is a 1-1 correspondence from $\mathbf{N}$ onto A.

(ii) If $A \subseteq B$ and B is countable, then A is **at most countable** (meaning either finite or countable). If A_n is at most countable for each $n \in \mathbf{N}$, then $\cup_{n\in\mathbf{N}} A_n$ is at most countable.

The following result gives yet another significant difference between $\mathbf{Q}$ and $\mathbf{R}$.

Theorem 1.10. (i) $\mathbf{Q}$ *is countable.* (ii) $\mathbf{R}$ *is uncountable.*

Proof. (i) We try to list all the elements of $\mathbf{Q}$ by distinct groups of finite sets. For this purpose, for each $n \in \mathbf{N}$, let $A_1 = \{0\}$ and A_n $(n \geq 2)$ be the set given by

$$A_n = \left\{ \pm\frac{p}{q} \ : \ \text{where } p,\, q \in \mathbf{N} \text{ are in the lowest terms with } p + q = n \right\}.$$

The first few of these sets look like

$$A_2 = \left\{\frac{1}{1}, -\frac{1}{1}\right\}, \quad A_3 = \left\{\frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}\right\}, \quad A_4 = \left\{\frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1}\right\},$$

$$A_5 = \left\{\frac{1}{4}, -\frac{1}{4}, \frac{2}{3}, -\frac{2}{3}, \frac{3}{2}, -\frac{3}{2}, \frac{4}{1}, -\frac{4}{1}\right\}, \quad A_6 = \left\{\frac{1}{5}, -\frac{1}{5}, \frac{5}{1}, -\frac{5}{1}\right\}, \cdots.$$

(Note that $\pm\frac{2}{4}$ and $\pm\frac{3}{3}$ are not in A_6.) Then A_n is finite, $A_n \cap A_k = \emptyset$ $(\forall n \neq k)$, and $\mathbf{Q} = \bigcup_{n=1}^{\infty} A_n$ (**explain why?**). This shows that $\mathbf{Q}$ can be listed as

$$\mathbf{Q} = \{\{A_1\}, \{A_2\}, \{A_3\}, \cdots, \{A_n\}, \cdots\},$$

where the list in $\{A_n\}$ can be given in any certain way. Hence $\mathbf{Q}$ is countable.

(ii) We use the contradiction proof to show that $\mathbf{R}$ is uncountable. Note that $\mathbf{R}$ is infinite. Suppose, for the contrary, that $\mathbf{R}$ is countable; then we can list $\mathbf{R}$ as

$$\mathbf{R} = \{x_1, x_2, x_3, x_4, \cdots\}, \quad \text{where } x_i \neq x_j \text{ whenever } i \neq j. \tag{1.3}$$

Let I_1 be a closed interval that does not contain the number x_1; for example, let $I_1 = [x_1 + 1, x_1 + 2]$. Clearly I_1 contains two *disjoint* two smaller closed intervals and one of them must not contain x_2. Let I_2 be the one (or any one) such interval that does not contain x_2. In general, if a closed interval I_n is already defined, construct a closed interval I_{n+1} as above to satisfy

$$\text{(a)} \quad I_{n+1} \subseteq I_n \quad \text{and} \quad \text{(b)} \quad x_{n+1} \notin I_{n+1}.$$

In this way, we obtain a family of nested closed intervals I_n. By the (NIP), we conclude that there exists a real number $x \in \bigcap_{n=1}^{\infty} I_n$; that is, $x \in I_n$ for all $n \in \mathbf{N}$. However, since $x \in \mathbf{R}$, it must appear in the list (1.3), say, $x = x_m$ for some $m \in \mathbf{N}$; then, by (b), $x = x_m \notin I_m$, a contradiction.

Hence $\mathbf{R}$ is uncountable. □

1.5. Cantor's Theorem

Cantor's Diagonalization Method. We discuss a different proof of the uncountability of $\mathbf{R}$. Since the interval $(0,1)$ is a subset of $\mathbf{R}$, the following result also proves that $\mathbf{R}$ is uncountable.

Theorem 1.11. *The open interval* $(0,1)$ *is uncountable.*

Proof. Clearly the interval $(0,1)$ is an infinite set. Suppose $(0,1)$ is countable. Then we can write

$$(0,1) = \{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_m, \cdots\},$$

where $\alpha_i \neq \alpha_j$ for $i \neq j$. Each $\alpha_m \in (0,1)$ has a decimal representation

$$\alpha_m = 0.a_{m1}a_{m2}a_{m3}\cdots,$$

where a_{mn} is a digit from the set $\{0,1,2,\cdots,9\}$. Some α_m may have two different decimal representations (e.g., $0.5 = 0.4999\cdots$, $0.45 = 0.44999\cdots$, etc), but this is fine if we simply select one of them. We define the number

$$b = 0.b_1b_2b_3b_4\cdots$$

where, for each $n \in \mathbf{N}$,

$$b_n = \begin{cases} 2 & \text{if } a_{nn} \neq 2 \\ 3 & \text{if } a_{nn} = 2. \end{cases}$$

(As long as $b_n \neq 0, 9$ and $b_n \neq a_{nn}$ for all $n \in \mathbf{N}$, the following argument is still valid.) Then $b \in (0,1)$; hence $b = \alpha_m$ for some $m \in \mathbf{N}$. This implies $b_k = a_{mk}$ for all $k \in \mathbf{N}$ (note that since $b_k \neq 0$ or 9 there is a unique decimal representation for b). In particular, $b_m = a_{mm}$, which contradicts the choice of b_m. □

Remark 1.11. The method used for defining the number b in the proof is generally called **Cantor's diagonalization method**, where the digits of b are chosen according to the property of the diagonal elements of the array $\{a_{mn}\}$. This method is also very useful in other problems. (See a homework problem.)

Power Sets*. Given a set A, the **power set** $P(A)$ (or sometime 2^A) is defined to be the set consisting of all subsets of A (always including the empty set $\emptyset$ and the set A itself).

For example, if $A = \{a_1, a_2, a_3\}$ then

$$P(A) = \{\emptyset, \{a_1\}, \{a_2\}, \{a_3\}, \{a_1,a_2\}, \{a_1,a_3\}, \{a_2,a_3\}, A\}.$$

A previous exercise says that if $\#(A) = n$ then $\#(2^A) = 2^n$.

The following result asserts that $P(A)$ always has a *larger* cardinality than A.

Theorem 1.12 (**Cantor's Theorem**). *Given any set* A*, there does not exist a function* $f\colon A \to P(A)$ *that is onto.*

Proof. Suppose, for the contrary, there exists a function $f\colon A \to P(A)$ that is onto. For each $a \in A$, the image $f(a)$ is a subset of A. Define the set

$$B = \{a \in A : a \notin f(a)\}.$$

Then $B \in P(A)$. Since f is onto, there exists an element $b \in A$ such that $B = f(b)$. If $b \in B$ then $b \notin f(b) = B$, a contradiction. If $b \notin B$ then, by the definition of B, $b \in f(b) = B$, again a contradiction. □