Number

Min Yan

February 5, 2014

Contents

1 Algebraic **3**
- 1.1 Natural Number . . . 3
- 1.2 Integer . . . 7
- 1.3 $\mathbb{N} \subset \mathbb{Z}$ and Order of Integers . . . 10
- 1.4 Multiplication . . . 12
- 1.5 Rational Number . . . 16

2 Analytical **21**
- 2.1 Real Number . . . 21
- 2.2 Addition . . . 23
- 2.3 Order . . . 25
- 2.4 Multiplication . . . 28
- 2.5 Exponential . . . 32

If you ask anybody what the numbers are, the answer is most likely a list: $1, 2, 3, \ldots$, and perhaps with the additional comment that $-1, 0.5, \sqrt{2}$, etc. can also be numbers. An immediate problem with such an answer is whether the following are also numbers

- (Spanish) dos, tres, cuato, $\cdots$.
- (Chinese) yi, er, san, $\cdots$.
- (Cave men) |, ||, |||, $\cdots$.

One may argue that this is just a language issue. However, even if the languages can be perfectly translated by dictionaries, there is still the question whether there are numbers before human civilization, or even before there is any life.

We often define concepts in everyday life by describing them. This is also the way most mathematical concepts are defined. The circle, the polynomial, the matrix, the limit, and the derivative are such examples. These definitions often build upon more basic definitions. When it comes to the most basic concepts such as numbers, however, we cannot define the concepts by describing in terms of more basic concepts.

The proper way of defining *numbers* is by considering how the numbers are used. The simplest numbers are the *natural numbers*, which are used primarily for *counting*. A counting system can be built around the simple operation of "one more". Then two more sophisticated operations, addition and multiplication, can be introduced. (In this note, for the efficiency of presentation, the multiplication is introduced after integers.)

Natural numbers are sufficient for very primitive civilizations. The Pirahã people in the Amazon jungle count only "one", "two" and "many". On the other hand, the development of civilization eventually found the natural number system to be inadequate. (Positive) *rational numbers* appeared as early as the 12th Dynasty of Egypt (1990-1800 BC). The concept was introduced for fractions and the division operation. *Integers* (especially negative numbers) first appeared in the Chinese arithmetic book "Shuan Shu Shu" (Writings on Reckoning, 202-186 BC, Western Han Dynasty), discovered in 1984 in Hubei province. The concept was introduced for subtraction. The modern concept of rational numbers, which also include negative numbers, carries the four arithmetic operations. The development so far are therefore *algebraic*.

Irrational numbers first appeared in the Indian text Sulbha Sutras (600 BC), for the construction of altar. The first proof of the irrationality of $\sqrt{2}$ is generally attributed to the Greeks (500 BC). Arabic mathematicians introduced the *real numbers* around 900. The modern rigorous definition of real numbers was introduced in 1872 by Karl Weierstrass, Eduard Heine, Georg Cantor (using infinite series), and Richard Dedekind (using cuts). Real numbers also carries the four arithmetic operations, and can only be distinguished from rational numbers by the limit operation. Therefore real numbers is an *analytical* concept.

The theory of numbers is the logical foundation of mathematical analysis. In this note, we start from natural numbers and build more and more sophisticated number systems. Eventually we have the real number system, with four arithmetic operations, the order, and the exponential operation.

1 Algebraic

1.1 Natural Number

The *natural numbers* are used for counting. For example, there are 4 alphabets in the set $\{a, b, c, d\}$. The number 4 is the *cardinality* of the set $\{a, b, c, d\}$. The natural numbers are also used to indicate the location in an ordered sequence. For example, the alphabet c is the 3rd in the sequence a, b, c, d. The number 3 is the *ordinality* of c in the sequence.

The natural numbers can be described by the following properties, called the Peano's axioms[1].

Definition 1.1. The *natural numbers* is a set $\mathbb{N}$ satisfying the following properties.

1. There is a special element $1 \in \mathbb{N}$.
2. For any $n \in \mathbb{N}$, there is assigned a unique $n' \in \mathbb{N}$.
3. For any $n \in \mathbb{N}$, we have $n' \neq 1$.
4. If $m' = n'$, then $m = n$.
5. If a subset $S \subset \mathbb{N}$ contains 1 and has the property that $n \in S$ implies $n' \in S$, then $S = \mathbb{N}$.

The first axiom gives us the initial number. In the second axiom, n' is meant to be $n + 1$, called the *successor* of n. For example, 2 is the successor of 1, 3 is the successor of 2, and 4 is the successor of 3, etc. The reason for using the notation n' instead of $n + 1$ is because the addition is yet to be defined. The first two axioms is intended to "build up" all the natural numbers by starting with the initial number 1 and creating the others by repeatedly applying the "successor operation".

The third axiom says that the special number 1 is not a successor. Thus 1 is the "beginning", with no other natural number "prior" to it. The fourth axiom says that if two natural numbers have the same successors, then the two numbers are the same. Thus we can talk about the *predecessor* of a natural number unambiguously (provided the number itself is the successor). For example, 1 is the predecessor of 2, and 2 is the predecessor of 3, etc.

The fifth axiom is called the *induction axiom*. Recall that the induction for a sequence of statements $A(1)$, $A(2)$, $A(3)$, ... involves verifying the truth of $A(1)$ and proving that the truth of $A(n)$ implies the truth of $A(n')$. To see how the fifth axiom implies the induction process, we denote

$$S = \{n \in \mathbb{N} \colon A(n) \text{ is true}\}.$$

[1]Giuseppe Peano: born 27 Aug 1858 in Cuneo, Piemonte, Italy; died 20 April 1932 in Turin, Italy. The famous axioms were published in *Arithmetices principia, nova methodo exposita* in 1889. Another stunning invention of his was the "space-filling" curves in 1890.

The two induction steps tell us that $1 \in S$ and $n \in S \implies n' \in S$. Then the fifth axiom implies that $S = \mathbb{N}$, which means that $A(n)$ is true for all n.

Proposition 1.2. *Any natural number other than* 1 *is a successor.*

Proof. Let

$$S = \{1\} \cup \{n' \colon n \in \mathbb{N}\}.$$

Then $1 \in S$ and for any n (in S or not, as long as it is in $\mathbb{N}$), we have $n' \in S$. Therefore we may apply the fifth axiom to S and get $S = \mathbb{N}$.

□

Definition 1.3. The *sum* $m+n$ of two natural numbers is the operation $\mathbb{N}\times\mathbb{N} \to \mathbb{N}$ characterized by

- $m + 1 = m'$.
- $m + n' = (m + n)'$.

The definition is consistent with our intuition and makes use of only the materials from the Peano's axioms. Moreover, it is a typical *inductive definition*, in which the first number m is fixed and the induction is applied to the second number n. The fifth axiom implies that for any fixed number m, $m + n$ is defined for all n. As a result, $m + n$ is defined for all m and n.

Strictly speaking, we need to verify that the sum map $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is *well*-defined by the inductive process. To see the subtle issue involved, all the possible ambiguities in the inductive process need to be examined.

The first ambiguity is the hypothetical possibility that the two requirements in the definition may overlap. Since this happens only if $1 = n'$, which is excluded by the third axiom, we know there is no overlap between the two requirements.

The second ambiguity is the possibility that the equality in the second requirement may overlap itself. Note that the second requirement really means that, for fixed m, $m+n'$ is defined as $(m + n)'$. Since $(m + n)'$ is determined by $m + n$, the ambiguity lies in the choice of the predecessor n of n'. By the fourth axiom, the choice of n is unique for the given n'. Therefore there is no overlap within the second requirement.

In summary, the addition is well-defined, thanks to all the axioms.

Proposition 1.4. *The sum in* $\mathbb{N}$ *has the following properties.*

1. *Cancelation law:* $m + k = n + k \implies m = n$.
2. *Associativity:* $k + (m + n) = (k + m) + n$.
3. *Commutativity:* $m + n = n + m$.

Proof. The following verifies the cancelation law for $n = 1$.

$$\begin{aligned} m+1 = n+1 &\implies m' = n' && \text{[1st in Definition 1.3]} \\ &\implies m = n. && \text{[fourth Peano axiom]} \end{aligned}$$

Under the inductive assumption $m + k = n + k \implies m = n$, we have

$$\begin{aligned} m+k' = n+k' &\implies (m+k)' = (n+k)' && \text{[2nd in Definition 1.3]} \\ &\implies m+k = n+k && \text{[fourth Peano axiom]} \\ &\implies m = n. && \text{[inductive assumption]} \end{aligned}$$

This completes the inductive proof of the cancelation law. To prove the associativity, we fix k, m and induct on n. The following verifies the associativity for $n = 1$.

$$\begin{aligned} k+(m+1) &= k+m' && \text{[1st in Definition 1.3]} \\ &= (k+m)' && \text{[2nd in Definition 1.3]} \\ &= (k+m)+1. && \text{[1st in Definition 1.3]} \end{aligned}$$

Under the inductive assumption $k + (m + n) = (k + m) + n$, we have

$$\begin{aligned} k+(m+n') &= k+(m+n)' && \text{[2nd in Definition 1.3]} \\ &= (k+(m+n))' && \text{[2nd in Definition 1.3]} \\ &= ((k+m)+n)' && \text{[inductive assumption]} \\ &= (k+m)+n'. && \text{[2nd in Definition 1.3]} \end{aligned}$$

This completes the inductive proof of the associativity. The proof of the commutativity is left as an exercise. □

The associativity tells us that the sums $(m+n)+(k+l)$, $(m+(n+k))+l$, $m+(n+(k+l))$ of natural numbers are all equal, so that we may write $m + n + k + l$ without any ambiguity. Moreover, the commutativity allows us to freely exchange orders of numbers in a sum, such as $k + n + l + m = m + n + k + l$.

Exercise 1.1. Prove that $n \neq n'$.

Exercise 1.2. The equality $m + 1 = 1 + m$ may be proved by inducting on m. For $m = 1$, the equality holds trivially. Next assume $m + 1 = 1 + m$. Then

$$\begin{aligned} m'+1 &= (m+1)+1 && \text{[1st in Definition 1.3]} \\ &= (m+1)' \\ &= (1+m)' \\ &= 1+m'. \end{aligned}$$

Fill in the reason for each step.

Exercise 1.3. The equality $m + n = n + m$ may be proved by inducting on m. The case $n = 1$ has been verified in Exercise 1.2. Next assume $m + n = n + m$. Then

$$\begin{aligned} m + n' &= m + (n + 1) \\ &= (m + n) + 1 && \text{[associativity]} \\ &= 1 + (m + n) \\ &= 1 + (n + m) \\ &= (1 + n) + m \\ &= (n + 1) + m \\ &= n' + m. \end{aligned}$$

Fill in the reason for each step.

Exercise 1.4. Using Proposition 1.4, the following proves $(m + n) + (k + l) = (m + k) + (n + l)$.

$$\begin{aligned} (m + n) + (k + l) &= ((m + n) + k) + l && \text{[associativity]} \\ &= (m + (n + k)) + l \\ &= (m + (k + n)) + l \\ &= ((m + k) + n) + l \\ &= (m + k) + (n + l). \end{aligned}$$

Fill in the reason for each step.

Exercise 1.5. The product mn of two natural numbers is characterized by $m1 = m$ and $mn' = mn + m$. Show that there is no ambiguity in the definition.

Exercise 1.6. Prove that the product of natural numbers have the following properties.

1. Distributivity: $(m + n)k = mk + nk$.
2. Commutativity: $mn = nm$.
3. Associativity: $k(mn) = (km)n$.

Exercise 1.7. Define the order $m \leq n$ between natural numbers by $1 \leq n$ for any n and $m \leq n \implies m' \leq n'$. Show that there is no ambiguity in the definition.

Exercise 1.8. Prove that the order of natural numbers have the following properties.

1. Reflexivity: $m \leq n$ and $n \leq m$ imply $n \leq n$.
2. Transitivity: $l \leq m$ and $m \leq n$ implies $l \leq n$.
3. Compatible with addition: $m \leq n$ if and only if $m + l \leq n + l$.

1.2 Integer

The *integers* are the natural numbers, their negatives, and zero. This enables the subtraction operation among integers, while the system of natural numbers do not have the subtraction. The need to subtract numbers may be considered as the motivation for defining the integers. So we may define integers as subtractions of natural numbers. For examples, we have $-\mathbf{2} = 3-5$, $\mathbf{0} = 2-2$, $-\mathbf{5} = 1-6$, $\mathbf{3} = 5-2$, where the bold faced numbers are the integers to be constructed, and the normal faced numbers are the natural numbers already given by Peano's axioms.

For the moment, we will use the ordered pairs (m,n), $m,n \in \mathbb{N}$, to denote integers (so $(3,5)$, $(2,2)$, $(1,6)$, $(5,2)$ are the temporary notations for $-\mathbf{2}$, $\mathbf{0}$, $-\mathbf{5}$, $\mathbf{3}$). We cannot yet use the subtraction notation $m-n$ (which is the real meaning of (m,n)) because strictly speaking, the subtraction operation is yet to be defined. The subtraction can only be defined *after* the whole set $\mathbb{Z}$ of integers is constructed.

There is just one problem with the idea above. The same integer can be expressed as the subtractions of different pairs of natural numbers. For example, -2 can be represented by $(3,5)$, by $(4,6)$, or by $(5,7)$. Therefore the pairs $(3,5)$, $(4,6)$, $(5,7)$, etc, should be considered as equal. This leads to the following definition.

Definition 1.5. The *integers* is the set $\mathbb{Z}$ of the equivalence ordered classes of pairs (m,n) of natural numbers $m,n \in \mathbb{N}$, subject to the equivalence relation

$$(m,n) \sim (k,l) \iff m+l = n+k.$$

An integer is then an equivalence class $[(m,n)]$, which we will simply denote by $[m,n]$. For example, $-2 = [3,5] = [4,6] = [5,7]$, $0 = [2,2]$, $-5 = [1,6]$, $3 = [5,2]$. The following verifies that the relation in the definition is indeed an equivalence relation.

1. The symmetry "$(m,n) \sim (k,l) \implies (k,l) \sim (m,n)$" means $m+l = n+k \implies k+n = l+m$. This follows from the commutativity in Proposition 1.4.

2. The reflexivity "$(m,n) \sim (m,n)$" means $m+n = n+m$. This is exactly the commutativity in Proposition 1.4.

3. The transitivity "$(m,n) \sim (k,l)$, $(k,l) \sim (p,q) \implies (m,n) \sim (p,q)$" is verified below.

$$\begin{aligned}
& (m,n) \sim (k,l),\ (k,l) \sim (p,q) \\
\iff & m+l = n+k, k+q = l+p \\
\implies & (m+l)+(k+q) = (n+k)+(l+p) && \text{[associativity and commutativity]} \\
\implies & (m+q)+(k+l) = (n+p)+(k+l) && \text{[cancelation law]} \\
\implies & m+q = n+p \\
\iff & (m,n) \sim (p,q).
\end{aligned}$$

After constructing $\mathbb{Z}$, we define the *sum* of integers by

$$[m,n]+[k,l]=[m+k,n+l].$$

The formula is based on the expectation $(m-n)+(k-l)=(m+k)-(n+l)$. The formula means that the sum is a map $\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ given by the following process: Express integers $a,b\in\mathbb{Z}$ as $a=[m,n]$ and $b=[k,l]$ for some $m,n,k,l\in\mathbb{N}$. Then $a+b=[m+k,n+l]\in\mathbb{Z}$. The following verifies that the process is well defined.

$$\begin{aligned}
&[m_1,n_1]=[m_2,n_2],\ [k_1,l_1]=[k_2,l_2] && \\
\iff & m_1+n_2=n_1+m_2,\ k_1+l_2=l_1+k_2 && \text{[definition of equivalence class]}\\
\implies & m_1+k_1+n_2+k_2=n_1+k_1+m_2+k_2 && \text{[associativity and commutativity]}\\
\iff & [m_1+k_1,n_1+k_1]=[m_2+k_2,n_2+k_2]. && \text{[definition of equivalence class]}
\end{aligned}$$

Proposition 1.6. *The sum in $\mathbb{Z}$ has the following properties.*

1. *Associativity: $a+(b+c)=(a+b)+c$.*
2. *Commutativity: $a+b=b+c$.*
3. *Zero: There is a unique integer 0 satisfying $a+0=0+a=a$.*
4. *Negative: For any $a\in\mathbb{Z}$, there is unique $-a\in\mathbb{Z}$ satisfying $a+(-a)=(-a)+a=0$.*

Similar to the remarks made after the proof of Proposition 1.4, the associativity and the commutativity imply that the expressions such as $a+b+c+d$ is unambiguous, and the order of terms may be exchanged.

Proof. The first two properties follow directly from the corresponding properties in Proposition 1.4 and the definition of the sum of integers.

Let $a=[m,n]$, $z=[k,l]$, $m,n,k,l\in\mathbb{N}$. Then $a+z=[m+k,n+l]$, and

$$\begin{aligned}
a+z=a &\iff m+k+n=n+l+m && \text{[definition of equivalence class]}\\
&\iff k=l. && \text{[commutativity and cancelation law]}
\end{aligned}$$

The argument shows that 0 exists and must be of the form $[k,k]$. Since $[k,k]=[l,l]$ for any $k,l\in\mathbb{N}$, the special number 0 is unique.

Let $a=[m,n]$, $b=[k,l]$, $m,n,k,l\in\mathbb{N}$. Then $a+b=[m+k,n+l]$, and by using $0=[1,1]$,

$$\begin{aligned}
a+b=0 &\iff m+k+1=n+l+1 && \text{[definition of equivalence class]}\\
&\iff m+k=n+l && \text{[fourth Peano axiom]}\\
&\iff b=[n,m]. && \text{[definition of equivalence class]}
\end{aligned}$$

Therefore $-a$ exists and must be of the unique form $[n,m]$. □

The negative allows us to define the *subtraction* of integers as

$$a - b = a + (-b).$$

Then the expressions such as $a-b+c-d$ make sense for integers. Moreover, the fourth property in Proposition 1.6 becomes $a - a = 0$, and we also have the *cancelation law* by subtracting c

$$a + c = b + c \implies a = b.$$

Exercises 1.11 through 1.15 confirm some familiar properties of subtraction.

Exercise 1.9. Here is the alternative way of proving the zero property in Proposition 1.6.

1. Show the existence by verifying that $a + [1, 1] = a$ for any integer a.
2. For the uniqueness, suppose 0 and $\bar{0}$ are two candidate integers for zero. Then we have $a + 0 = 0 + a = a$ and $a + \bar{0} = \bar{0} + a = a$. By taking $a = 0$ and $a = \bar{0}$ in these equalities, prove that $0 = \bar{0}$.

Exercise 1.10. Proving the existence of the negative in Proposition 1.6 by verifying $[m, n] + [n, m] = [1, 1]$ for any $m, n \in \mathbb{N}$. This shows the existence of the nagative. Then prove the uniqueness by explaining that, if $a + b = b + a = 0$ and $a + c = c + a = 0$, then

$$b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c.$$

Exercise 1.11. Explain that $a - b = 0$ if and only if $a = b$.

Exercise 1.12. Prove $[m, n] = m - n$. In other words, $[m, n] = [m + 1, 1] - [n + 1, 1]$.

Exercise 1.13. For $a, b \in \mathbb{Z}$, explain each step in the following computation by properties in Proposition 1.6, and then conclude that $-(a + b) = -a - b$.

$$\begin{aligned}(a + b) + ((-a) + (-b)) &= (b + a) + ((-a) + (-b)) = ((b + a) + (-a)) + (-b) \\ &= (b + (a + (-a))) + (-b) = (b + 0) + (-b) = b + (-b) = 0.\end{aligned}$$

Exercise 1.14. Explain why $-(-a) = a$.

Exercise 1.15. Provide reason for each step of the following proof of $-(a - b) = b - a$.

$$-(a - b) = -(a + (-b)) = -((-b) + a) = -(-b) - a = b - a.$$

1.3 $\mathbb{N} \subset \mathbb{Z}$ and Order of Integers

Natural numbers are integers. This means that the set $\mathbb{N}$ may be identified with a subset of $\mathbb{Z}$. Specifically, the formula $n = (n+1) - 1$ suggests a map

$$f(n) = [n+1, 1] \colon \mathbb{N} \to \mathbb{Z}.$$

The map is one-to-one because (provide reason for each step)

$$f(m) = f(n) \iff m+1+1 = 1+n+1 \implies m = n.$$

Then f identifies the natural numbers with the subset $f(\mathbb{N})$ of $\mathbb{Z}$. Therefore we may simply write $n = [n+1, 1]$ and call integers of the form $[n+1, 1]$ natural numbers.

Proposition 1.7. *Any integer $a \in \mathbb{Z}$ has three mutually exclusive possibilities: $a \in \mathbb{N}$, $a \in -\mathbb{N}$, $a = 0$.*

The set $-\mathbb{N} = \{-n \colon n \in \mathbb{N}\}$ is the negatives of all the natural numbers. By $-(-a) = a$, we know $a \in -\mathbb{N}$ is the same as $-a \in \mathbb{N}$. We call the integers in $\mathbb{N}$ *positive* and call integers in $-\mathbb{N}$ *negative*. The proposition gives a disjoint union $\mathbb{Z} = \mathbb{N} \sqcup -\mathbb{N} \sqcup \{0\}$, or any integer is either positive, negative, or zero.

Proof. First we prove that any integer can be written as either $[r, 1]$ or $[1, r]$ for some $r \in \mathbb{N}$. For each $n \in \mathbb{N}$, consider the statement

$$A(n) \colon \text{For any } m \in \mathbb{N}, \text{ there is } r \in \mathbb{N}, \text{ such that either } [m, n] = [r, 1] \text{ or } [m, n] = [1, r].$$

Clearly, $A(1)$ is true for the trivial reason. Next, we assume $A(n)$ is true and try to prove that $A(n+1)$ is also true. For any $m \in \mathbb{N}$, there are two possibilities by Proposition 1.2.

- $m = 1$. In this case, $[m, n+1] = [1, r]$ for $r = n+1$.
- $m = k+1$ for some $k \in \mathbb{N}$. In this case,

$$\begin{aligned} [m, n+1] &= [k, n] && \text{[definition of equivalence class in } \mathbb{Z}\text{]} \\ &= [r, 1] \text{ or } [1, r]. && \text{[assumption that } A(n) \text{ is true]} \end{aligned}$$

This completes the inductive proof of $A(n)$.

By Proposition 1.2, the natural number r in $A(n)$ must be either 1 or $s+1$ for some $s \in \mathbb{N}$. Therefore there are three possibilities for any $a \in \mathbb{Z}$.

- $a = [1, 1] = 0$, where the second equality appeared in the proof of Proposition 1.6.
- $a = [s+1, 1] = f(s)$ is a natural number.

- $a = [1, s+1] = -[s+1, 1] = -f(s)$, where the second equality appeared in the proof of Proposition 1.4. Thus a is the negative of a natural number.

Finally, we prove the three cases are mutually exclusive. First,

$$\begin{aligned} [s+1,1] = [1,1] &\implies (s+1)+1 = 1+1 && \text{[definition of equivalence class in } \mathbb{Z}\text{]} \\ &\implies s+1 = 1. && \text{[fourth Peano axiom]} \end{aligned}$$

Since the conclusion contradicts with the third Peano axiom, we find the first and the second cases are mutually exclusive. By the similar reason, the second and the third cases are mutually exclusive. Finally, if $[s+1, 1] = [1, r+1]$, then $(s+1)+(r+1) = 1+1$, which also leads to a contradiction in a similar way, so that the first and the third cases are mutually exclusive. □

Given that the notations 1, 2, 3, 4, ... are used for natural (positive) numbers in $\mathbb{Z}$, the proposition enables us to use the notations ..., −4, −3, −2, −1, 0, 1, 2, 3, 4, ... for integers, without any ambiguity. Moreover, we may also use the proposition to define the order in $\mathbb{Z}$.

Definition 1.8. An integer a is *bigger* than another integer b, denoted $a > b$, if $a - b \in \mathbb{N}$. In this case, b is also *smaller* than a and denoted $b < a$.

Applying the definition to Proposition 1.7, we find that $a \in \mathbb{N}$ is the same as $a > 0$, and $a \in -\mathbb{N}$ is the same as $a < 0$. Therefore the three mutually exclusive possibilities are $a > 0$, $a < 0$, $a = 0$.

Proposition 1.9. *The order in $\mathbb{Z}$ has the following properties.*

1. *For $a, b \in \mathbb{Z}$, one and only one of following happens: $a > b$, $a < b$, $a = b$.*
2. *Transitivity: $a > b$, $b > c \implies a > c$.*
3. *Compatible with sum: $a > b \implies a + c > b + c$.*
4. *Compatible with negative: $a > b \implies -a < -b$.*
5. *1 is the smallest natural number.*

Proof. By Proposition 1.7, there are three mutually exclusive possibilities for the integer $a - b$.

- $a - b \in \mathbb{N}$. This means $a > b$.
- $a - b \in -\mathbb{N}$. By Exercises 1.14 and 1.15, this implies $b - a = -(a - b) \in \mathbb{N}$, so that $a < b$.
- $a - b = 0$. This means $a = b$.

This proves the first property. For the last property, note that any natural number other than 1 is of the form $n+1$ by Proposition 1.2, and $n+1>1$ by $(n+1)-1=n\in\mathbb{N}$. The proof of the middle three properties are left as exercises. □

Exercise 1.16. Verify that the map $f\colon \mathbb{N}\to\mathbb{Z}$ preserves the sum

$$f(m+n)=f(m)+f(n).$$

Then use this to prove the second property of Proposition 1.9.

Exercise 1.17. Prove the third property of Proposition 1.9.

Exercise 1.18. Prove the fourth property of Proposition 1.9.

Exercise 1.19. Prove that $a<b$ if and only if $a-b<0$.

Exercise 1.20. Prove $a>0 \iff -a<0$.

Exercise 1.21. Prove $a>b,\ c>d \implies a+c>b+d$.

Exercise 1.22. In Exercise 1.7, a relation $m\le n$ is defined in $\mathbb{N}$. Prove that $m\le n$ if and only if $m<n$ or $m=n$, where the order in $\mathbb{Z}$ is used in $m<n$.

1.4 Multiplication

The product of natural numbers may be defined inductively, similar to the sum.

Definition 1.10. The *product* mn of two natural numbers is the operation $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ characterized by

- $m1=m$.
- $mn'=mn+m$.

Similar argument as the sum tells us that the product is well-defined.

Proposition 1.11. *The product in* $\mathbb{N}$ *has the following properties.*

1. *Distributivity:* $(m+n)k=mk+nk$.
2. *Commutativity:* $mn=nm$.
3. *Associativity:* $k(mn)=(km)n$.

Proof. To prove the distributivity, we fix m, n and induct on k. The case $k = 1$ follows from the first requirement in Definition 1.10.

$$(m + n)1 = m + n = m1 + n1.$$

Under the inductive assumption that $(m + n)k = mk + nk$, we have

$$\begin{aligned}
(m + n)k' &= (m + n)k + (m + n) && \text{[2nd in Definition 1.10]} \\
&= (mk + nk) + (m + n) && \text{[inductive assumption]} \\
&= (mk + m) + (nk + n) && \text{[Proposition 1.4]} \\
&= mk' + nk'. && \text{[2nd in Definition 1.10]}
\end{aligned}$$

This completes the inductive proof of the distributivity.

The proof of the commutativity is a double induction. We first prove $m1 = 1m$ by inducting on m. For $m = 1$, the equality holds trivially. Under the assumption $m1 = 1m$, we have

$$\begin{aligned}
m'1 &= m' && \text{[1st in Definition 1.10]} \\
&= m + 1 && \text{[definition of sum]} \\
&= m1 + 1 && \text{[1st in Definition 1.10]} \\
&= 1m + 1 && \text{[inductive assumption]} \\
&= 1m'. && \text{[2nd in Definition 1.10]}
\end{aligned}$$

This completes the inductive proof of $m1 = 1m$.

Next assume $mn = nm$. Then

$$\begin{aligned}
mn' &= mn + m && \text{[2nd in Definition 1.10]} \\
&= nm + m && \text{[inductive assumption]} \\
&= nm + m1 && \text{[1st in Definition 1.10]} \\
&= nm + 1m && \text{[}m1 = 1m\text{, just proved]} \\
&= (n + 1)m && \text{[distributivity, just proved]} \\
&= n'm. && \text{[1st in Definition 1.10]}
\end{aligned}$$

This completes the inductive proof of the commutativity.

The proof of the associativity is left as an exercise. □

Note that the commutativity and the distributivity imply the other distributivity

$$k(m + n) = km + kn.$$

Moreover, the associativity tells us $(mn)(kl) = (m(nk))l = m(n(kl))$, so that the expressions such as $mnkl$ are unambiguous. The commutativity further allows us to change the order of the numbers in a product, such as $knlm = nmkl$.

Based on the expectation $(m-n)(k-l) = (mk+nl) - (ml+nk)$, we define the product of two integers by

$$[m,n][k,l] = [mk+nl, ml+nk].$$

The verification that the product is well-defined is left as an exercise.

Proposition 1.12. *The product in $\mathbb{Z}$ has the following properties.*

1. *The map $f\colon \mathbb{N} \to \mathbb{Z}$ preserves the product: $f(mn) = f(m)f(n)$.*
2. *Distributivity: $(a+b)c = ac+bc$.*
3. *Commutativity: $ab = ba$.*
4. *Associativity: $a(bc) = (ab)c$.*
5. *One: $a1 = 1a = 1$.*
6. *Zero: $ab = 0 \iff a = 0$ or $b = 0$.*
7. *Negative: $(-a)b = -ab$, $(-1)a = -a$.*
8. *Order: If $c > 0$, then $a > b \iff ac > bc$.*

Proof. The first property

$$[mn+1, 1] = [m+1, 1][n+1, 1] = [(m+1)(n+1)+1, (m+1)1 + 1(n+1)]$$

is the verification of

$$mn + 1 + (m+1)1 + 1(n+1) = 1 + (m+1)(n+1) + 1.$$

This can be easily done by the definition of the product and Propositions 1.4 and 1.11.

The proofs of the second, third and fourth properties are left as exercises.

For the fifth property, we use $a = [m,n] = m-n$ (see Exercise 1.12), the distributivity and the first requirement in Definition 1.10

$$a1 = (m-n)1 = m1 - n1 = m - n = a.$$

Next we prove $0a = 0$, which by the commutativity is the $\Longleftarrow$ direction of the zero property. By $0+0=0$ and the distributivity, we have $0a + 0a = (0+0)a = 0a$. Then by the cancelation law, we get $0a = 0$.

For the negative property, we have

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{[distributivity]} \\ &= 0b && \text{[negative property in Proposition 1.6]} \\ &= 0. && \text{[just proved]} \end{aligned}$$

Then by the uniqueness of the negative of ab, we get $(-a)b = -ab$. The formula further implies that $(-1)a = -(1a) = -a$.

For the order property, we note that

$$(a-b)c = (a+(-b))c = ac + (-b)c = ac + (-bc) = ac - bc.$$

We also note that $a > b$ is defined as $a-b \in \mathbb{N}$, which is the same as $a-b > 0$. Therefore the order property is the same as that under the assumption $c > 0$, we have $a - b > 0 \iff (a-b)c > 0$. Using a in place of $a - b$, we consider three possibilities for a in Proposition 1.7 (also see the discussion after Definition 1.8).

- $a > 0$. Then by the first property, $a, c \in \mathbb{N}$ implies $ac \in \mathbb{N}$, or $ac > 0$.
- $a < 0$. Then $-a > 0$, and by the first case, we get $-ac = (-a)c \in \mathbb{N}$, or $ac < 0$.
- $a = 0$. Then by the $\Longleftarrow$ direction of the zero property, we have $ac = 0$.

Thus the three mutually exclusive possibilities for a correspond to the same mutually exclusive possibilities for ac. As a consequence, we have $a > 0 \iff ac > 0$.

Finally, we prove the $\Longrightarrow$ direction of the zero property. This is the same as $a \neq 0$ and $b \neq 0 \implies ab \neq 0$. By Proposition 1.7, we have $a > 0$ or $a < 0$, and the same for b. If $a > 0, b > 0$, then the order property says $ab > 0b = 0$. If $a < 0$ and $b < 0$, then $-a > 0$ and $-b > 0$, and the order property says $ab = (-a)(-b) > 0$. Similar argument can be carried out for $a > 0, b < 0$, and $a < 0, b > 0$. We always conclude $ab \neq 0$. □

The development so far justifies all of our usual operations of integers, particularly the sum, the product, and the order (which includes the sign). From now on, we will get rid of those provisional notations such as $[m, n]$ and $f(n)$. We can safely use notations in our everyday life for the integers and manipulate them in our usual way. For example, we may freely apply the formulae such as $(a-b)c = ac - bc$ and $(a+b)(a-b) = a^2 - b^2$ to integers.

Exercise 1.23. Prove the associativity in Proposition 1.11 by using the distributivity, the commutativity, and the induction on n (while fixing k and m).

Exercise 1.24. Verify that the product of integers is well defined. In other words, prove that $m_1 + n_2 = n_1 + m_2$ and $k_1 + l_2 = l_1 + k_2$ imply

$$(m_1k_1 + n_1l_1) + (m_2l_2 + n_2k_2) = (m_1l_1 + n_1k_1) + (m_2k_2 + n_2l_2).$$

Exercise 1.25. Use Proposition 1.11 to verify the distributivity, the commutativity and the associativity in Proposition 1.12.

Exercise 1.26. Prove the equality $a0 = 0$ by verifying $[m, n][1, 1] = [1, 1]$ for $m, n \in \mathbb{N}$.

Exercise 1.27. Prove the equality $a1 = a$ by verifying $[m, n][1 + 1, 1] = [m, n]$ for $m, n \in \mathbb{N}$.

Exercise 1.28. Prove that if $c < 0$, then $a > b \iff ac < bc$.

Exercise 1.29. Prove the *cancelation law*: If $c \neq 0$, then $a = b \iff ac = bc$.

1.5 Rational Number

Rational numbers are quotients of integers with nonzero denominators. However, the same rational number can be expressed as the quotients with different numerators and denominators, such as $\frac{2}{3} = \frac{4}{6}$. Similar to the definition of integers, the problem can be dealt with by equivalence classes.

Definition 1.13. The *rational numebrs* is the set $\mathbb{Q}$ of the equivalence classes of pairs (a, b) of integers $a, b \in \mathbb{Z}$, $b \neq 0$, subject to the equivalence relation

$$(a, b) \sim (c, d) \iff ad = bc.$$

The pair (a, b) in the definition is meant to represent the quotient $\frac{a}{b}$, and the definition of the equivalence relation comes from $\frac{a}{b} = \frac{c}{d}$. We will simply denote the equivalence class by $\frac{a}{b}$ instead of $[a, b]$, so that

$$\mathbb{Q} = \left\{ \frac{a}{b} \colon a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

The important thing to remember here is that we cannot yet think of $\frac{a}{b}$ as a divided by b, because the division operation is yet to be defined. At the moment, $\frac{a}{b}$ is simply a *unified notation* for the equivalence class.

Similar to the inclusion $\mathbb{N} \subset \mathbb{Z}$, we introduce a map

$$g(a) = \frac{a}{1} \colon \mathbb{Z} \to \mathbb{Q}.$$

We emphasis again that $\frac{a}{1}$ means the equivalence class of $(a, 1)$ and not yet the division of a by 1. The following verifies that the map is one-to-one.

$$g(a) = g(b) \iff (a, 1) \sim (b, 1) \iff a1 \sim 1b \iff a = b.$$

Therefore the integers are identified with the subset $g(\mathbb{Z})$ of $\mathbb{Q}$ by writing $a = \frac{a}{1}$ for $a \in \mathbb{Z}$.

Next we define the sum and the product of rational numbers in the expected ways.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b}\,\frac{c}{d} = \frac{ac}{bd}.$$

Proposition 1.14. *The sum and the product in $\mathbb{Q}$ have the following properties.*

1. *The map $g\colon \mathbb{Z} \to \mathbb{Q}$ preserves the sum and the product: $g(a+b) = g(a) + g(b)$, $g(ab) = g(a)g(b)$.*
2. *Associativity: $(r+s)+t = r+(s+t)$, $(rs)t = r(st)$.*
3. *Commutativity: $r+s = s+r$, $rs = sr$.*
4. *Distributivity: $(r+s)t = rt + st$.*
5. *Zero: The integer 0 is the unique rational number such that $r + 0 = 0 + r = r$.*
6. *Negative: For any rational number r, there is a unique rational number $-r$ satisfying $r + (-r) = (-r) + r = 0$.*
7. *One: The integer 1 is the unique rational number such that $r1 = 1r = r$.*
8. *Reciprocal: For any rational number $r \neq 0$, there is a unique rational number r^{-1} satisfying $rr^{-1} = r^{-1}r = 1$.*

Proof. The following verifies the first property.

$$\frac{a}{1} + \frac{b}{1} = \frac{a1 + 1b}{1 \cdot 1} = \frac{a+b}{1}, \quad \frac{a}{1}\frac{b}{1} = \frac{ab}{1 \cdot 1} = \frac{ab}{1}.$$

The associativity, the commutativity and the distributivity are left as exercises. The properties will be used in subsequent argument.

The following verifies that the integers 0 and 1 have the expected properties.

$$\frac{a}{b} + \frac{0}{1} = \frac{a1 + b0}{b1} = \frac{a+0}{b} = \frac{a}{b}, \quad \frac{1}{1}\frac{a}{b} = \frac{1a}{1b} = \frac{a}{b}.$$

The following shows the existence of the negative.

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{bb} = \frac{ab - ab}{bb} = \frac{0}{bb} = \frac{0}{1}.$$

For $r = \dfrac{a}{b} \neq 0 = \dfrac{0}{1}$, by the definition of equivalence classes, we have $a = a1 \neq 0b = 0$. Threfore a can be used as a denominator and $\dfrac{b}{a}$ is also a rational number. The following shows that $\dfrac{b}{a}$ is a reciprocal of r.

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}.$$

Now we prove the uniqueness. Suppose both rational numbers 0 and $\bar{0}$ satisfy

$$r + 0 = r = 0 + r, \quad r + \bar{0} = r = \bar{0} + r.$$

Then by taking $r = \bar{0}$ in the first equality and $r = 0$ in the second equality, we get

$$\bar{0} = 0 + \bar{0} = 0.$$

Similar argument shows the uniqueness of 1.

Suppose both s and $\bar{s}$ satisfy

$$rs = 1 = sr, \quad \bar{s}r = 1 = r\bar{s}.$$

Then by the property of 1 and the associativity, we get

$$s = s1 = s(r\bar{s}) = (sr)\bar{s} = \bar{s}.$$

Similar argument shows the uniqueness of the negative. □

The existence of the negative allows us to define the subtraction of rational numbers

$$r - s = r + (-s).$$

Similarly, the existence of reciprocal allows us to define the division of rational numbers

$$r \div s = rs^{-1}.$$

For integers $a, b \in \mathbb{Z}$, the following computation

$$\begin{aligned} a \div b &= \frac{a}{1}\left(\frac{b}{1}\right)^{-1} && \text{[definition of division and } \mathbb{Z} \subset \mathbb{Q}\text{]} \\ &= \frac{a}{1}\frac{1}{b} && \text{[proof of Proposition 1.14]} \\ &= \frac{a1}{1b} && \text{[definition of product]} \\ &= \frac{a}{b}. \end{aligned}$$

shows that the rational number $\dfrac{a}{b}$ is indeed the division of a by b. Therefore we will also write $\dfrac{r}{s}$ for the division $r \div s$ of rational numbers. Proposition 1.14 implies the usual properties about the subtraction and the division, such as

$$\frac{r-s}{t} = \frac{r}{t} - \frac{s}{t}, \quad \frac{-r}{t} = -\frac{r}{t}, \quad \frac{rt}{st} = \frac{r}{s}, \quad \left(\frac{r}{s}\right)^{-1} = \frac{s}{r}.$$

So we established the four arithmetic operations for the rational numbers satisfying the usual properties.

Definition 1.15. A rational number r is *bigger* than another rational number s, denoted $r > s$, if $r - s = \dfrac{a}{b}$ with $a > 0$ and $b > 0$. In this case, s is also *smaller* than r and denoted $s < r$.

The order extends the order in $\mathbb{Z}$. First, if integers a and b satisfy $a > b$, then $a - b = \dfrac{a-b}{1}$ fits the definition above. Conversely, if $a - b = \dfrac{c}{d}$ for integers $c, d > 0$, then by the order property in Proposition 1.12, we have $ad - bd = (a-b)d = c > 0$ implying $a > b$.

Proposition 1.16. *The order in $\mathbb{Q}$ has the following properties.*

1. *For $r, s \in \mathbb{Q}$, one and only one of following happens: $r > s$, $r < s$, $r = s$.*
2. *Transitivity: $r > s$, $s > t \implies r > t$.*
3. *Compatible with sum: $r > s \implies r + t > s + t$.*
4. *Compatible with negative: $r > s \implies -r < -s$.*
5. *Compatible with product: If $t > 0$, then $r > s \iff rt > st$.*
6. *Compatible with reciprocal: If $r, s > 0$, then $r > s \iff r^{-1} < s^{-1}$.*
7. *For any $r > s$, there is t satisfying $r > t > s$.*
8. *For any $r > 0$, there is a natural number n satisfying $n > r > \dfrac{1}{n}$.*

Proof. By $\dfrac{a}{b} = \dfrac{-a}{-b}$, any rational number can be expressed as a quotient with positive denominator. Let $r - s = \dfrac{a}{b}$ with $b > 0$. We consider three mutually exclusive possibilities for a.

- $a > 0$. By $b > 0$ and Definition 1.15, this means $r > s$.
- $a < 0$. Then $s - r = -\dfrac{a}{b} = \dfrac{-a}{b}$. By $-a > 0$, $b > 0$ and Definition 1.15, this means $r < s$.
- $a = 0$. This is the same as $r - s = 0$, or $r = s$.

This proves the first property.

For the transitivity, the assumption means $r - s = \dfrac{a}{b}$, $s - t = \dfrac{c}{d}$, with $a, b, c, d > 0$. Then $r - t = (r - s) + (s - t) = \dfrac{ad + bc}{bd}$. By Proposition 1.12, $a, b, c, d > 0$ implies $ad + bc > 0$ and $bd > 0$. Then we get $r > t$.

The proofs of the third through the sixth properties are rather routine and are left as exercises.

The seventh property may be proved by choosing $t = \dfrac{r+s}{2}$.

$$r - t = (r-s)\frac{1}{2} > 0, \quad t - s = (r-s)\frac{1}{2} > 0 \implies r > t > s.$$

For the last property, write $r = \dfrac{a}{b}$ with $a, b \in \mathbb{N}$. Pick $n \in \mathbb{N}$ satisfying $n > a$, $n > b$ ($n = a + b$, for example). Then by $a, b \geq 1$ and the compatibility of the order with the product and reciprocal, we have

$$n > a \geq ab^{-1} \geq b^{-1} > n^{-1}. \qquad \square$$

We may use the order in $\mathbb{Q}$ to define the *absolute value*, the *maximum* and the *maximum*

$$|r| = \begin{cases} r, & \text{if } r \geq 0, \\ -r, & \text{if } r < 0; \end{cases} \quad \max\{r,s\} = \begin{cases} r, & \text{if } r \geq s, \\ s, & \text{if } r < s; \end{cases} \quad \min\{r,s\} = \begin{cases} s, & \text{if } r \geq s, \\ r, & \text{if } r < s. \end{cases}$$

Exercises 1.33 through 1.35 provide some properties.

We have established the four arithmetic operations and the order for the rational numbers. We also proved all the usual properties. From now on, we may freely manipulate rational numbers just as we do in everyday life.

Exercise 1.30. Prove the associativity, the commutativity and the distributivity in Proposition 1.14.

Exercise 1.31. Use Proposition 1.14 to prove the *cancelation laws* for rational numbers.

1. $r + t = s + t \implies r = s$.
2. $rt = st$ and $t \neq 0 \implies r = s$.

Exercise 1.32. Prove the third, fourth, fifth and six properties of Proposition 1.16.

Exercise 1.33. Prove $|r + s| \leq |r| + |s|$, $|rs| = |r||s|$ and $|r| < s \iff -s < r < s$.

Exercise 1.34. Prove that for any rational number r, there is an integer n satisfying $|r| < n$.

Exercise 1.35. Prove $\max\{r,s\} \geq r$, $\min\{r,s\} \leq r$, $\max\{r,s\} + \min\{r,s\} = r + s$, $\max\{r,s\} - \min\{r,s\} = |r - s|$.

2 Analytical

2.1 Real Number

Our usual knowledge about real numbers is that they can be expressed as infinite decimal expansions

$$\begin{aligned}\frac{1}{3} &= 0.33333333\cdots,\\ \sqrt{2} &= 1.41421356\cdots,\\ \pi &= 3.14158265\cdots.\end{aligned}$$

Moreover, the rational numbers are supposed to be the "periodic" expansions. While it is possible to use decimal expansions to define real numbers, it would be rather complicated to use the definition to define the sum and the product of real numbers. Moreover, how to explain that $\sqrt{2}$, as the number whose square is 2, can be expressed by a decimal expansion?

A better idea is to consider the actual meaning of the decimal expansion. By including more and more decimal digits, we are getting closer and closer to the number. For example, $\sqrt{2} = 1.41421356\cdots$ means that $\sqrt{2}$ is the *limit* of the sequence of *rational* numbers

$$1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142,\ 1.41421,\ 1.414213,\ 1.4142135,\ 1.41421356,\ \ldots.$$

This suggests that it might be possible to define real numbers as the limits of *convergent* sequences of rational numbers. Such sequences are called *Cauchy sequences*, and it is indeed possible to construct real numbers in this way. This is the Cauchy[2] method.

Another approach is based on the observation that the a real number can be described as the *supremum* (i.e., least upper bound) of some set of rational numbers (i.e., subsets of $\mathbb{Q}$). For example, $\sqrt{2}$ is the smallest real number that is bigger than all the numbers (i.e., an upper bound) in

$$X = \{1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, 1.41421356, \ldots\} \subset \mathbb{Q}.$$

However, $\sqrt{2}$ is also the supremum of a smaller set

$$Y = \{1, 1.41, 1.4142, 1.414213, 1.41421356, \ldots\} \subset \mathbb{Q}.$$

The problem can be dealt with either by introducing some equivalence relation, or by choosing the biggest set of rational numbers for which $\sqrt{2}$ is a supremum

$$Z = \{r \in \mathbb{Q} \colon r < \sqrt{2}\} \subset \mathbb{Q}.$$

[2]Augustin Louis Cauchy: born 21 Aug 1789 in Paris, France; died 23 May 1857 in Sceaux (near Paris), France. Many fundamental results in real and complex analysis are due to Cauchy and bear his name: Cauchy integral theorem, Cauchy-Kovalevskaya theorem, the Cauchy-Riemann equations, Cauchy sequences.

Alternatively, we may use the biggest set of rational numbers for which $\sqrt{2}$ is the infimum (i.e., greatest lower bound)

$$Z' = \{r \in \mathbb{Q} \colon r > \sqrt{2}\} = \{r \in \mathbb{Q} \colon r^2 > 2\} \subset \mathbb{Q}.$$

This supremum/infimum approach is called the Dedekind[3] cut. We choose to use sets similar to Z' to define real numbers.

Definition 2.1. A *real number* is a nonempty set $X \subset \mathbb{Q}$ of rational numbers satisfying the following conditions.

1. $s > r$ and $r \in X \implies s \in X$.
2. $r \in X \implies$ There is $s \in X$ satisfying $r > s$.
3. X is bounded below: There is $p \in \mathbb{Q}$ such that $r > p$ for any $r \in X$.

The collection of all real numbers is denoted $\mathbb{R}$.

Here is the motivation behind the definition. The first condition says that X is an interval of rational numbers with $+\infty$ as the right side. There are three possibilities for such an interval.

- $X = (x, +\infty) \cap \mathbb{Q} = \{r \in \mathbb{Q} \colon r > x\}$ for some real number x.
- $X = [x, +\infty) \cap \mathbb{Q} = \{r \in \mathbb{Q} \colon r \geq x\}$ for some real number x.
- $X = (-\infty, +\infty) \cap \mathbb{Q} = \mathbb{Q}$.

The third condition says that only the first two happens. If x is irrational, then $(x, \infty) \cap \mathbb{Q} = [x, \infty) \cap \mathbb{Q}$, so that the two possibilities are the same, and the real number x corresponds to the unique set. If x is rational, however, $(x, \infty) \cap \mathbb{Q}$ and $[x, \infty) \cap \mathbb{Q}$ are different, yet correspond to the same x. To avoid the ambiguity, the second condition choses the subset $(x, \infty) \cap \mathbb{Q}$.

The definition simply identifies the real numbers x with the sets $(x, \infty) \cap \mathbb{Q}$ of rational numbers. So we are entitled to write equalities such as $2 = (2, \infty) \cap \mathbb{Q}$. After all, $\sqrt{2}$, $1.41421356 \cdots$, and $\{r \in \mathbb{Q} \colon r^2 > 2\}$ are equally good notations for the real number x satisfying $x^2 = 2$.

We will use the capital letters $X, Y, Z, \ldots$, when we think of real numbers as sets. We will also use lower case letters $x, y, z, \ldots$, when we think of real numbers not as sets (say, as points on the real line). We will use both lower case and capital letters according to the context, and will keep in mind that $x = X, y = Y, z = Z, \ldots$.

Rational numbers can be considered as real numbers via the map

$$h(r) = \{s \in \mathbb{Q} \colon s > r\} \colon \mathbb{Q} \to \mathbb{R}.$$

[3]Julius Wihelm Richard Dedekind: born 6 October 1831 in Braunschweig, Germany; died 12 Feb 1916 in Braunschweig, Germany. Dedekind made a number of highly significant contributions to mathematics, particularly in algebraic number theory. Dedekind came up with the idea of cut on 24 November 1858.

For rational numbers $r > r'$, we have $h(r') \neq h(r)$ by $r \in h(r')$ and $r \notin h(r)$. Therefore h is one-to-one.

To establish the theory of real numbers, we need to know how the real and rational numbers interact. The following technical result essentially says that any real number is sandwiched between rational numbers that are very close to each other.

Lemma 2.2. *For any real number X and any rational number $\epsilon > 0$, there are rational numbers $r \in X$ and $s \notin X$, such that $r - s = \epsilon$.*

Proof. Since X is not empty and bounded below, we have rational $q \in X$ and rational lower bound p as in the third condition in Definition 2.1. Then for the rational numbers $\frac{p}{\epsilon}$ and $\frac{q}{\epsilon}$, by the eighth property in Proposition 1.16, there are $m, n \in \mathbb{N}$ satisfying $\frac{p}{\epsilon} > -m$ and $n > \frac{q}{\epsilon}$.

By $-m\epsilon < p \notin X$, $n\epsilon > q \in X$ and the first condition in Definition 2.1, we get $-m\epsilon \notin X$ and $n\epsilon \in X$. By adding ϵ repeatedly to $-m\epsilon$, we get an increase sequence of rational numbers

$$-m\epsilon,\ (-m+1)\epsilon,\ (-m+2)\epsilon,\ \ldots,\ (n-1)\epsilon,\ n\epsilon.$$

Since sequence starts with $-m\epsilon \notin X$ and ends with $n\epsilon \in X$, there are two adjacent terms in the sequence, say $s = k\epsilon$ and $r = (k+1)\epsilon$, such that $s \notin X$ and $r \in X$, and the difference $r - s = \epsilon$. □

Exercise 2.1. For any real number X, explain that $r \in X, s \notin X \implies r > s$. Also explain that $r \notin X, s < r \implies s \notin X$.

Exercise 2.2. For any real number X and any rational number $\epsilon > 0$, prove that there are rational numbers $r \in X$ and $s \notin X$, such that $r - s < \epsilon$.

Exercise 2.3. If we try to use sets similar to Z to define real numbers, how would you modify Definition 2.1? Moreover, does $\{r \in \mathbb{Q} \colon r^2 < 2\} \subset \mathbb{Q}$ satisfy the modified definition?

2.2 Addition

The sum of two real numbers is naturally defined as

$$X + Y = \{r + s \colon r \in X, s \in Y\}.$$

The following verifies that $X + Y$ satisfy the three conditions in Definition 2.1.

1. Suppose a rational number $t > r + s$ for some $r \in X$ and $s \in Y$. By $t - r > s$ and the first condition for Y, we get $t - r \in Y$ and $t = r + (t - r) \in X + Y$.

2. Suppose $t = r + s \in X + Y$ for some $r \in X$ and $s \in Y$. By the second condition for X, there is $r' \in X$ satisfying $r > r'$, so that $t' = r' + s \in X + Y$ satisfies $t > t'$.

3. If p and q are lower bounds for X and Y, then $p + q$ is a lower bound for $X + Y$.

The sum of real numbers is consistent with the sum of rational numbers. This means that for $r, s \in \mathbb{Q}$, the following are equivalent for any $t \in \mathbb{Q}$ (the left side means $t \in h(r + s)$, the right side means $t \in h(r) + h(s)$).

$$t > r + s \iff t = r' + s' \text{ for some } r', s' \in \mathbb{Q} \text{ satisfying } r' > r \text{ and } s' > s.$$

The $\Longleftarrow$ direction is obvious. For the $\Longrightarrow$ direction, we note that $t > r + s$ implies $t - r > s$. By the seventh property in Proposition 1.16, there is $s' \in \mathbb{Q}$ satisfying $t - r > s' > s$. Then we have $t = r' + s'$ for $r' = t - s' > r$ and $s' > s$.

Proposition 2.3. *The sum in $\mathbb{R}$ has the following properties.*

1. *Associativity:* $(x + y) + z = x + (y + z)$.

2. *Commutativity:* $x + y = y + x$.

3. *Zero: There is a unique real number* 0 *satisfying* $x + 0 = 0 + x = x$.

4. *Negative: For any real number x, there is a unique real number $-x$ satisfying* $x + (-x) = (-x) + x = 0$.

Proof. The associativity follows from

$$(X + Y) + Z = \{(r + s) + t \colon r \in X, s \in Y, t \in Z\},$$
$$X + (Y + Z) = \{r + (s + t) \colon r \in X, s \in Y, t \in Z\},$$

and the associativity for the sum in $\mathbb{Q}$. The commutativity can be proved similarly.

For $h(0) = \{s \in \mathbb{Q} \colon s > 0\}$ (the rational number 0 considered as a real number), we have

$$X + h(0) = \{r + s \colon r \in X,\ s \in h(0)\} = \{r + s \colon r \in X,\ s \in \mathbb{Q},\ s > 0\}.$$

By $r + s > r \in X$ and the first condition in Definition 2.1, we get $r + s \in X$. This proves $X + h(0) \subset X$. On the other hand, for $r \in X$, by the second condition in Definition 2.1, there is $s \in X$ satisfying $r > s$. Then $r = s + (r - s)$ with $s \in X$ and $r - s > 0$ implies that $r \in X + h(0)$. This proves $X \subset X + h(0)$. We conclude that $X + h(0) = X$.

The negative Y of a real number X satisfies $X + Y = \{r + t \colon r \in X, t \in Y\} = h(0)$. So it is tempting to construct the negative as

$$Y = \{t \in \mathbb{Q} \colon r + t > 0 \text{ for any } r \in X\}.$$

However, for $X = (x, +\infty) \cap \mathbb{Q}$, the construction gives $Y = [-x, +\infty) \cap \mathbb{Q}$. On the other hand, what we really want is $(-x, +\infty) \cap \mathbb{Q}$, which is different from Y in case x is a rational number. So we further modify Y to get $(-x, +\infty) \cap \mathbb{Q}$

$$\begin{aligned} Z &= \{s \in \mathbb{Q} \colon s > t \text{ for some } t \in Y\} \\ &= \{s \in \mathbb{Q} \colon \text{There is } t \in \mathbb{Q} \text{ satisfying } s > t \text{ and } r + t > 0 \text{ for any } r \in X\}. \end{aligned}$$

The following verifies that Z satisfies the three conditions in Definition 2.1, so that Z is indeed a real number.

1. Suppose $s \in Z$ and $s' > s$. Then by the transitivity in Proposition 1.16, $s > t$ for some $t \in Y$ implies $s' > t$ for the same $t \in Y$. This implies $s' \in Z$.

2. Suppose $s \in Z$. Then $s > t$ for some $t \in Y$. By the seventh property in Proposition 1.16, there is $s' \in \mathbb{Q}$ satisfying $s > s' > t$. Then $s' > t$ implies $s' \in Z$, and we find $s' \in Z$ satisfying $s' < s$.

3. Fix any $r \in X$. For any $s \in Z$, we have $s > t$ for some $t \in Y$. Then we further have $r \in X$ satisfying $r + t > 0$. Therefore $r + s > r + t > 0$. This implies $s > -r$, so that $-r$ is a lower bound of Z.

Next we prove $X + Z = h(0)$. For $r \in X$ and $s \in Z$, we have $s > t$ for some $t \in Y$. Then $r + s > r + t > 0$. This proves $X + Z \subset h(0)$. For the other inclusion $h(0) \subset X + (-X)$, we need to show that any $\epsilon \in h(0)$ can be expressed as $r + s$ for some $r \in X$ and $s \in Z$. Note that $\epsilon \in h(0)$ means $\epsilon > 0$. By Lemma 2.2, there are rational numbers $r \in X$ and $r' \notin X$, such that $r - r' = \dfrac{\epsilon}{2} < \epsilon$. Then $\epsilon = r + s$ with $s = \epsilon - r$. We know $r \in X$, and only need to show $s \in Z$. We also know $s = \epsilon - r > -r'$, and the problem is reduced to showing $-r' \in Y$. This means that for any $s \in X$, we need to show $s + (-r') > 0$, or $s > r'$. By the first condition in Definition 2.1, $s \in X$ and $r' \notin X$ indeed imply $s > r'$.

Finally, the uniqueness of the zero and the negative are the consequences of their properties and the associativity (see the proof of Proposition 1.14). □

Exercise 2.4. Suppose Y is a non-empty set of rational numbers with lower bound. Prove that $Z = \{s \in \mathbb{Q} \colon s > t \text{ for some } t \in Y\}$ satisfies the three conditions in Definition 2.1. The fact is used in the proof of Proposition 2.3. In fact, the real number Z is the *infimum* of the set Y.

Exercise 2.5. What are the rational numbers in $-\sqrt{2}$? What are the rational numbers in $1-\sqrt{2}$?

2.3 Order

The order of real numbers is naturally defined by

$$X > Y \iff X \subset Y \text{ and } X \neq Y.$$

The definition is the same as

$$X \geq Y \iff X \subset Y.$$

The first thing we need to verify is the consistency with the order for rational numbers. This means that for $r, s \in \mathbb{Q}$, the following are equivalent (the right side is $h(r) > h(s)$ in $\mathbb{R}$, all $>$ happens in $\mathbb{Q}$)

$$r > s \iff t > r \text{ implies } t > s, \text{ and } r \neq s.$$

The $\implies$ direction follows from the transitivity in Proposition 1.16. The $\impliedby$ direction is equivalent to

$$r \leq s \implies t > r \text{ does not imply } t > s, \text{ or } r = s.$$

This is further equivalent to

$$r < s \implies t > r \text{ and } t \leq s \text{ for some } t.$$

By the seventh property in Proposition 1.16, the implication holds.

The following provides the criterion for comparing rational numbers and real numbers.

Lemma 2.4. *Suppose $r \in \mathbb{Q}$ and $X \in \mathbb{R}$. Then $r > X$ if and only if $r \in X$. In other words, $X = \{r : r \in \mathbb{Q},\ r > X\}$.*

Proof. By the definition, $r > X$ means the following.

1. $h(r) \subset X$: $s > r$ implies $s \in X$.
2. $h(r) \neq X$: There is $t \in X$ satisfying $t \leq r$.

By the first condition in Definition 2.1 and the second statement, we have $r \in X$. Conversely, if $r \in X$, then the first statement holds by the first condition in Definition 2.1, and the second statement holds with $t = r$. □

Proposition 2.5. *The order in $\mathbb{R}$ has the following properties.*

1. *For $x, y \in \mathbb{R}$, one and only one of following happens: $x > y$, $x < y$, $x = y$.*
2. *Transitivity: $x > y$, $y > z \implies x > z$.*
3. *Compatible with sum: $x > y \implies x + z > y + z$.*
4. *Compatible with negative: $x > y \implies -x < -y$.*
5. *For any $x > y$, there is a rational number r satisfying $x > r > y$.*

Proof. The first property is the consequence of the claim that there must be an inclusion relation between any two real numbers X and Y. So we assume $Y \not\subset X$ and try to prove $X \subset Y$.

By $Y \not\subset X$, there is $r \in \mathbb{Q}$ satisfying $r \notin X$ and $r \in Y$. By the first condition in Definition 2.1 and $r \notin X$, we have $s > r$ for any $s \in X$. By the first condition again and $r \in Y$, we have $s \in Y$. This proves $X \subset Y$.

The transitivity follows directly from the transitivity of the inclusion. It is also easy to see the compatibility with the sum. By using $-(x+y)$ in place of z, we also get $x > y \implies -y = x - (x+y) > y - (x+y) = -x$, which is the compatibility with the negative.

Now we turn to the last property. If $X > Y$, then $X \subset Y$ and $X \neq Y$, so that there is $s \in \mathbb{Q}$ satisfying $s \notin X$ and $s \in Y$. By Lemma 2.4, we have $s > Y$. By Lemma 2.4 and $s \notin X$, we have $s \not> X$. Since s and X can be compared by the first property, we conclude that $X \geq s > Y$. By the second condition in Definition 2.1, there is another rational number $r \in Y$ satisfying $s > r$. Then we get $X > r > Y$. □

The definition of real numbers is motivated by the supremum and the infimum. Naturally one would like to ask whether the motivation is fulfilled.

Theorem 2.6. *Any set of real numbers bounded above has a real number as the supremum. Any set of real numbers bound below has a real number as has the infimum.*

Proof. Let A be a set of real numbers with a lower bound p. Define

$$Z = \{r \in \mathbb{Q} \colon r > x \text{ for some } x \in A\}.$$

First we need to verify the three conditions in Definition 2.1. By the transitivity in Proposition 2.5, Z satisfies the first condition. By the last property in Proposition 2.5, Z satisfies the second condition. By choosing a rational number smaller than p in case p is not rational, Z satisfies the third condition. Therefore Z is a real number.

If Z is not a lower bound of A, then we have $X \in A$ satisfying $X < Z$. This means there is $r \in \mathbb{Q}$ satisfying $r \in X$ and $r \notin Z$. By Lemma 2.4, $r \in X$ implies $r > X$, so that $r \in Z$ and we have a contradiction.

To show that Z is the biggest lower bound, we consider another real number $W > Z$. We have $r \in \mathbb{Q}$ satisfying $r \in Z$ and $r \notin W$. Note that $r \in Z$ means $r > X$ for some $X \in A$, which by Lemma 2.4 further means $r \in X$. Then $r \in X$ and $r \notin W$ imply $X \not\subset W$, which means $X \not\geq W$. Therefore W is not a lower bound of A.

The existence of the supremum can be proved by applying the negative to everything and changing to the existence of infimum. □

Exercise 2.6. For any $x \in \mathbb{R}$, prove that $x = \inf\{r \colon r \in \mathbb{Q},\ r > x\}$. This recovers the original idea of constructing real numbers as the infima of rational numbers.

Exercise 2.7. Give an alternative proof of Proposition 2.6 by using $Z = \cup\{X \colon X \in A\}$.

2.4 Multiplication

Real numbers are defined with the help of order in $\mathbb{Q}$. We also expect good and clean compatibility between the order and the product in $\mathbb{R}$. Since such compatibility happens only for the product of positive numbers, some preparation on positive numbers is needed.

We remark that $X \geq 0$ means $X \subset h(0)$, or all the rational numbers in X are positive.

Lemma 2.7. *Suppose X is a positive real number.*

1. *There is a natural number n satisfying $n > X > \dfrac{1}{n}$.*
2. *For any rational number $\epsilon > 0$, there are rational numbers $r \in X$ and $s \notin X$, such that $s > 0$ and $\dfrac{r}{s} < 1 + \epsilon$.*

The first statement is similar to the last property in Proposition 1.16. The second statement is the multiplicative version of Lemma 2.2. Note that $r \in X$ and $s \notin X$ already imply $r > s$.

Proof. By Lemma 2.4, any $r \in X$ satisfies $r > X$. By $X > 0$ and the last property in Proposition 2.5, there is another $t \in \mathbb{Q}$ satisfying $X > t > 0$. By the last property in Proposition 1.16, we have $n_1, n_2 \in \mathbb{N}$ satisfying $n_1 > r > \dfrac{1}{n_1}$ and $n_2 > t > \dfrac{1}{n_2}$. Then $n = \max\{n_1, n_2\} \in \mathbb{N}$ satisfies $n > r$ and $t > \dfrac{1}{n}$. By the transitivity in Proposition 2.5, we have $n > X > \dfrac{1}{n}$.

For the second statement, take $t \in \mathbb{Q}$ above satisfying $X > t > 0$. By Lemma 2.2, there are $r \in X$ and $u \notin X$ satisfying $r - u < \epsilon t$. By Lemma 2.4 and $t < X$, we have $t \notin X$. Then $s = \max\{u, t\} \notin X$. By $s \geq u$, $s \geq t$ and $\epsilon > 0$, we have $r - s \leq r - u < \epsilon t < \epsilon s$. By $s \geq t > 0$ and the fifth property in Proposition 1.16, we may divide s and get $\dfrac{r}{s} - 1 < \epsilon$. □

Define the product of *non-negative* real numbers $X, Y \geq 0$ by

$$XY = \{rs \colon r \in X,\ s \in Y\}.$$

We note that all rational numbers in X and Y are positive. The following verifies the three conditions in Definition 2.1.

1. Suppose a rational number $t > rs$ for some $r \in X$ and $s \in Y$. Then $r > 0$ and we have $\dfrac{t}{r} > s$. By $s \in Y$, this implies $\dfrac{t}{r} \in Y$, so that $t = r\dfrac{t}{r} \in XY$.
2. Suppose $t = rs \in XY$ with $r \in X$ and $s \in Y$. Then there are $r' \in X$ and $s' \in Y$ satisfying $r > r'$ and $s > r'$. Since $r', s' > 0$, we have $t' = r's' \in XY$ satisfying $t > t'$.
3. 0 is a lower bound of XY.

The product is consistent with the product of non-negative rational numbers. Specifically, we need to show that for any given rational numbers $r, s \geq 0$, the following are equivalent for any $t \in \mathbb{Q}$.

$$t > rs \iff t = r's' \text{ for some rational } r', s' \in \mathbb{Q} \text{ satisfying } r' > r \text{ and } s' > s.$$

The $\Longleftarrow$ direction is obvious. For the $\Longrightarrow$ direction, we note that $t > rs$ implies $\dfrac{t}{r} > s$. By the seventh property in Proposition 1.16, there is s' satisfying $\dfrac{t}{r} > s' > s$. Then $r' = \dfrac{t}{s'} > r$ and we have $t = r's'$.

Proposition 2.8. *The product of non-negative real numbers has the following properties.*

1. *Associativity:* $(xy)z = x(yz)$.
2. *Commutativity:* $xy = yx$.
3. *Distributivity:* $(x + y)z = xz + yz$.
4. *Zero:* $x0 = 0x = 0$.
5. *One: There is a unique real number* 1 *satisfying* $x1 = 1x = x$.
6. *Reciprocal: For any real number* $x > 0$*, there is a unique real number* x^{-1} *satisfying* $xx^{-1} = x^{-1}x = 1$.
7. *Compatible with positivity:* $x > 0,\ y > 0 \implies xy > 0$.

Proof. The associativity follows from

$$(XY)Z = \{(rs)t \colon r \in X, s \in Y, t \in Z\},$$
$$X(YZ) = \{r(st) \colon r \in X, s \in Y, t \in Z\}.$$

and the associativity in Proposition 1.14. The commutativity can be proved similarly.

A rational number in $(X + Y)Z$ is of the form $(r + s)t$ with $r \in X$, $s \in Y$, $t \in Z$. By the distributivity in Proposition 1.14, we have $(r + s)t = rt + st \in XZ + YZ$. This proves $(X + Y)Z \subset XZ + YZ$. Conversely, a rational number in $XZ + YZ$ is of the form $rt_1 + st_2$ with $r \in X$, $s \in Y$, $t_1 \in Z$, $t_2 \in Z$. Then for $t = \min\{t_1, t_2\}$, we have $rt_1 + st_2 \geq (r + s)t \in (X + Y)Z$. By the first condition in Definition 2.1 for the real number $(X + Y)Z$, we have $rt_1 + st_2 \in (X + Y)Z$. This shows $XZ + YZ \subset (X + Y)Z$ and completes the proof of the distributivity.

A rational number in $Xh(0)$ is of the form rs with $r \in X$ and $s > 0$. Since $X \geq 0$ implies $r > 0$, we have $rs > 0$, which means $rs \in h(0)$. This proves $Xh(0) \subset h(0)$. Conversely, fix $r \in X$, which must satisfy $r > 0$. Then any $s \in h(0)$ also satisfies $s > 0$ and can be written

as $s = r\dfrac{s}{r}$ with $\dfrac{s}{r} > 0$. Therefore $\dfrac{s}{r} \in h(0)$ and $s \in Xh(0)$. This shows $h(0) \subset Xh(0)$ and completes the proof of $x0 = 0$.

A rational number in $Xh(1)$ is of the form rs with $r \in X$ and $s > 1$. Then $rs > r$, and by $r \in X$, we have $rs \in X$. This proves $Xh(1) \subset X$. Conversely, for any $r \in X$ there is $s \in X$ satisfying $r > s$. Then $\dfrac{r}{s} > 1$ means $\dfrac{r}{s} \in h(1)$, and we have $r = s\dfrac{r}{s} \in Xh(1)$. This shows $X \subset Xh(1)$ and completes the proof of $x1 = x$.

For positive X, construct the reciprocal by

$$X^{-1} = \{s \in \mathbb{Q} \text{: There is } t \in \mathbb{Q} \text{ satisfying } s > t \text{ and } rt > 1 \text{ for any } r \in X\}.$$

The construction is similar to the construction of the negative in the proof of Proposition 2.3. It can be similarly verified that X^{-1} satisfies the three conditions in Definition 2.1. In particular, we note that 0 is a lower bound of X^{-1}.

The inclusion $XX^{-1} \subset h(1)$ follows from

$$r \in X,\ s \in X^{-1} \implies rs > rt > 1.$$

Conversely, consider $u \in h(1)$, which means $u > 1$. By Lemma 2.7, there are $r \in X$ and $s \notin X$ satisfying $\dfrac{r}{s} < u$. We have $u = r\dfrac{u}{r}$ with $r \in X$. So to prove $u \in XX^{-1}$, it is sufficient to verify $\dfrac{u}{r} \in X^{-1}$. We note that $\dfrac{r}{s} < u$ implies $\dfrac{u}{r} > \dfrac{1}{s}$, and the following shows that $\dfrac{1}{s}$ can be used as t in the construction of X^{-1} (v is r in the construction of X^{-1}, and the first $\implies$ is due to $s \notin X$)

$$v \in X \implies v > s \implies v\frac{1}{s} > 1.$$

This shows $h(1) \subset XX^{-1}$ and completes the proof of $XX^{-1} = h(1)$.

The uniqueness of 1 and the reciprocal can be proved similar to the proof in Proposition 1.14.

Finally, suppose $x > 0$, $y > 0$. Then $xy \geq 0$ by the definition of the product. If $xy = 0$, then by multiplying the reciprocal of y (which exists because $y > 0$), we get $x = x(yy^{-1}) = (xy)y^{-1} = 0y^{-1} = 0$. The contradiction implies $xy > 0$. □

The product can be extended to all real numbers by

$$xy = \begin{cases} xy, & \text{if } x \geq 0,\ y \geq 0, \\ -(-x)y, & \text{if } x \leq 0,\ y \geq 0, \\ -x(-y), & \text{if } x \geq 0,\ y \leq 0, \\ (-x)(-y), & \text{if } x \leq 0,\ y \leq 0. \end{cases}$$

It can be easily verifies that the overlapping cases always give 0 as the product. Then we have the properties of the sum, the product, and the order for the real numbers.

Proposition 2.9. *The product in $\mathbb{R}$ has the following properties.*

1. *The map $h\colon \mathbb{Q} \to \mathbb{R}$ preserves the product.*
2. *Associativity: $(xy)z = x(yz)$.*
3. *Commutativity: $xy = yx$.*
4. *Distributivity: $(x+y)z = xz + yz$.*
5. *Zero: $x0 = 0x = 0$.*
6. *One: There is a unique real number 1 satisfying $x1 = 1x = x$.*
7. *Reciprocal: For any real number $x \neq 0$, there is a unique real number x^{-1} satisfying $xx^{-1} = x^{-1}x = 1$.*
8. *Compatible with order: If $x > 0$, then $y > z \iff xy > xz$.*

Proof. We need to consider various possibilities of signs. We illustrate the idea by proving some cases of the distributivity. We already know the distributivity in case $x, y, z \geq 0$ from Proposition 2.8. For the case $x+y \geq 0$, $y \leq 0$ and $z \geq 0$, we have $x \geq -y \geq 0$. By Proposition 2.8, we have

$$(x+y)z + (-y)z = [(x+y) + (-y)]z = xz.$$

Adding $-(-y)z = yz$ (the equality is the definition of yz) to both sides, we get $(x+y)z = xz+yz$. For the case $x+y \leq 0$, $x \geq 0$, $y \leq 0$ and $z \geq 0$, we have $-(x+y) \geq 0$, $-y \geq 0$. By Proposition 2.8, we have

$$xz + (-(x+y))z = [x - (x+y)]z = (-y)z.$$

By the definition of product in $\mathbb{R}$, we have $-(-(x+y))z = (x+y)z$ and $-(-y)z = yz$. Adding the three equalities together, we get $xz + yz = (x+y)z$.

The rest of the proof are left as an exercise. □

Exercise 2.8. Complete the proof of Proposition 2.9.

Exercise 2.9. Prove the product is compatible with the order: If $z > 0$, then $x > y \iff xz > yz$. If $x, y > 0$, then $x > y \iff x^{-1} < y^{-1}$.

Exercise 2.10. Another way of extending the product from non-negative real numbers to all real numbers is to show that any real number is a difference between two positive real numbers and define the product of $x = x_1 - x_2$ and $y = y_1 - y_2$ with $x_1, x_2, y_1, y_2 \geq 0$ by

$$xy = x_1y_1 + x_2y_2 - x_1y_2 - x_2y_1.$$

Carry out the details of this approach.

2.5 Exponential

For a real number x and a natural number n, define x^n to be the product of n copies of x. Strictly speaking, the definition is given by the following inductive process.

- $x^1 = x$.
- $x^{n+1} = x^n x$.

Proposition 2.10. *The natural number exponent x^n has the following properties.*

$$(xy)^n = x^n y^n, \quad x^{m+n} = x^m x^n, \quad x^{mn} = (x^m)^n, \quad x > y > 0 \implies x^n > y^n.$$

Proof. We prove $x^{m+n} = x^m x^n$ by fixing m and inducting on n. The other properties can be similarly proved by induction.

For $n = 1$, we have $x^{m+1} = x^m x = x^m x^1$ by the two equalities in the inductive definition. Now assume $x^{m+n} = x^m x^n$. Then $x^{m+n+1} = x^{m+n}x = (x^m x^n)x = x^m(x^n x) = x^m x^{n+1}$. Therefore the equality $x^{m+n} = x^m x^n$ is proved by induction on n. □

For $x \neq 0$ and $a \in \mathbb{Z}$, write $a = m - n$ with $m, n \in \mathbb{N}$ and define $x^a = \dfrac{x^m}{x^n}$. If $a = m_1 - n_1 = m_2 - n_2$, then $m_1 + n_2 = m_2 + n_1$. By Proposition 2.10, we have

$$x^{m_1} x^{n_2} = x^{m_1+n_2} = x^{m_2+n_1} = x^{m_2} x^{n_1}.$$

This implies $\dfrac{x^{m_1}}{x^{n_1}} = \dfrac{x^{m_2}}{x^{n_2}}$, so that x^a is well defined. The following are the properties of the integer exponent, and can be proved easily from Proposition 2.10.

Proposition 2.11. *The integer exponent x^a has the following properties.*

$$(xy)^a = x^a y^a, \quad x^{a+b} = x^a x^b, \quad x^{ab} = (x^a)^b, \quad x > y > 0 \implies \begin{cases} x^a > y^a, & \text{if } a > 0, \\ x^a < y^a, & \text{if } a < 0. \end{cases}$$

The next result defines the n-th root for natural numbers n.

Proposition 2.12. *For any $x > 0$ and $n \in \mathbb{N}$, there is a unique $x^{\frac{1}{n}} > 0$ satisfying $(x^{\frac{1}{n}})^n = x$. Moreover, $x^{\frac{1}{n}} > y^{\frac{1}{n}}$ if and only if $x > y$, so that the n-th root is unique.*

Proof. Construct the expected n-th root $w = \inf\{z : z > 0,\ z^n > x\}$ by using Theorem 2.6. We need to verify that $w^n = x$.

First we note that $y = \min\{1, x\}$ satisfies $y^n \leq x 1^{n-1} = x$. This implies $w \geq y > 0$.

Under the assumption $w^n > x$, we try to find $w > \delta > 0$, such that $(w-\delta)^n > x$. This contradicts the definition of w as the infimum. By the binomial expansion, we have

$$(w-\delta)^n = w^n - \delta\left(\binom{n}{1}w^{n-1} - \binom{n}{2}w^{n-2}\delta + \binom{n}{3}w^{n-3}\delta^2 - \cdots\right) = w^n - \delta A_\delta.$$

For $\delta < 1$, we have

$$\begin{aligned}|A_\delta| &\le \binom{n}{1}w^{n-1} + \binom{n}{2}w^{n-2}\delta + \binom{n}{3}w^{n-3}\delta^2 + \cdots \\ &< w^n + \binom{n}{1}w^{n-1} + \binom{n}{2}w^{n-2} + \binom{n}{3}w^{n-3} + \cdots = (w+1)^n.\end{aligned}$$

Therefore $(w-\delta)^n > w^n - \delta(w+1)^n$, and we can achieve $(w-\delta)^n > x$ by choosing $\delta = \min\left\{w, 1, \dfrac{w^n - x}{(w+1)^n}\right\}$. Here the assumption $w^n > x$ is used to make sure that $\delta > 0$.

Under the assumption $w^n < x$, we try to find $\delta > 0$, such that $(w+\delta)^n < x$. Again this contradicts the definition of w as the infimum. We have

$$(w+\delta)^n = w^n + \delta\left(\binom{n}{1}w^{n-1} + \binom{n}{2}w^{n-2}\delta + \binom{n}{3}w^{n-3}\delta^2 + \cdots\right) = w^n + \delta B_\delta.$$

By the similar reason as before, we have $|B_\delta| < (w+1)^n$ for $\delta < 1$. Therefore we can achieve $(w+\delta)^n < x$ by choosing $\delta = \min\left\{1, \dfrac{x - w^n}{(w+1)^n}\right\}$.

Since both $w^n > x$ and $w^n < x$ lead to contradictions, we conclude that $w^n = x$.

Finally, $x^{\frac{1}{n}} > y^{\frac{1}{n}}$ implies $x = (x^{\frac{1}{n}})^n > (y^{\frac{1}{n}})^n = y$. The converse also holds because $x^{\frac{1}{n}} \le y^{\frac{1}{n}}$ would imply $x = (x^{\frac{1}{n}})^n \le (y^{\frac{1}{n}})^n = y$. □

For $x > 0$ and $r \in \mathbb{Q}$, write $r = \dfrac{b}{n}$ with $b \in \mathbb{Z}$, $n \in \mathbb{N}$ and define $x^r = (x^{\frac{1}{n}})^b$. If $r = \dfrac{a}{m} = \dfrac{b}{n}$, then by Proposition 2.11,

$$[(x^{\frac{1}{m}})^a]^{mn} = (x^{\frac{1}{m}})^{mna} = [(x^{\frac{1}{m}})^m]^{na} = x^{na}, \quad [(x^{\frac{1}{n}})^b]^{mn} = (x^{\frac{1}{n}})^{mnb} = [(x^{\frac{1}{n}})^n]^{mb} = x^{mb}.$$

Therefore $(x^{\frac{1}{m}})^a = (x^{\frac{1}{n}})^b$ by the uniqueness of the mn-th root and $na = mb$. This shows that the rational exponent is well defined.

Proposition 2.13. *The rational exponent x^r has the following properties.*

$$(xy)^r = x^r y^r, \quad x^{r+s} = x^r x^s, \quad x^{rs} = (x^r)^s,$$

$$x > 1,\ r > s \implies x^r > x^s, \quad x > y > 0 \implies \begin{cases} x^r > y^r, & \text{if } r > 0, \\ x^r < y^r, & \text{if } r < 0. \end{cases}$$

Proof. The equalities follow from Proposition 2.11 and the uniqueness of the n-th root.

Assume $x > 1$ and $r > s$. Then $r - s = \dfrac{b}{n}$ with $b, n \in \mathbb{N}$. By the monotone property of n-th root in Proposition 2.12, we have $x^{\frac{1}{n}} > 1$, so that $x^{r-s} = (x^{\frac{1}{n}})^b > 1$. Then $x^r = x^{r-s}x^s > 1x^s = x^s$. This proves the first inequality. The second inequality follows from

$$x > y > 0,\ r > 0 \implies \frac{x}{y} > 1,\ r > 0 \implies x^r = \left(\frac{x}{y}\right)^r y^r > \left(\frac{x}{y}\right)^0 y^r = y^r. \qquad \square$$

For any $x > 1$ and $y \in \mathbb{R}$, define the exponent x^y by

$$x^y = \inf\{x^r : r \in \mathbb{Q},\ r > y\}.$$

By Lemma 2.4, if y is given by the set Y of rational numbers, then

$$x^y = \inf\{x^r : r \in Y\}.$$

We need to verify that the real exponent is consistent with the rational exponent. This means that for any rational $y = s \in \mathbb{Q}$, we have

1. x^s is a lower bound: $r > s \implies x^r > x^s$.
2. Any number bigger than x^s is not a lower bound: For any $\epsilon > 0$, there is $r > s$, such that $x^r \le x^s + \epsilon$.

The first statement follows from Proposition 2.13. The second statement can be established with the help of the following.

Lemma 2.14. *For any $x > 1$ and $\epsilon > 0$, there is $n \in \mathbb{N}$ satisfying $x^{\frac{1}{n}} - 1 < \epsilon$.*

Proof. Let $z_n = x^{\frac{1}{n}} - 1$. Then $x > 1$ implies $z_n > 0$. Moreover,

$$x = (1 + z_n)^n = 1 + \binom{n}{1} z_n + \binom{n}{2} z_n^2 + \cdots > \binom{n}{1} z_n = n z_n.$$

By Lemma 2.7, there is $n \in \mathbb{N}$ satisfying $\dfrac{x}{\epsilon} < n$. Then $x^{\frac{1}{n}} - 1 = z_n < \dfrac{x}{n} < \epsilon$. $\square$

In the second statement above, we are given $x > 1$, $s \in \mathbb{Q}$ and $\epsilon > 0$. Taking ϵ in the lemma to be ϵx^{-s}, we get $n \in \mathbb{N}$ satisfying $x^{\frac{1}{n}} - 1 < \epsilon x^{-s}$. Then $r = s + \dfrac{1}{n} > s$ satisfies $x^r = x^s x^{\frac{1}{n}} < x^s(1 + \epsilon x^{-s}) = x^s + \epsilon$.

Next we try to extend the exponent x^y from $x > 1$ to any positive x. Express any $x > 0$ as $x = \dfrac{x_1}{x_2}$ with $x_1, x_2 > 1$. This can be done, for example, by finding a rational number $r = \dfrac{m}{n}$ satisfying $x > r > 0$ and writing $x = \dfrac{nx}{n}$. Then we define

$$x^y = \frac{x_1^y}{x_2^y}, \quad x_1, x_2 > 1.$$

To show this is well defined, we make use of the properties of the infimum.

Lemma 2.15. *Suppose A and B are lower bounded sets of real numbers.*

1. *For $A+B=\{x+y\colon x\in A,\ y\in B\}$, we have $\inf(A+B)=\inf A+\inf B$.*
2. *If A and B contain only positive real numbers and $AB=\{xy\colon x\in A,\ y\in B\}$, then $\inf AB=\inf A\inf B$.*

Proof. For any $x+y\in A+B$, with $x\in A$ and $y\in B$, we have $x+y\geq \inf A+\inf B$. This shows that $\inf A+\inf B$ is a lower bound of $A+B$. On the other hand, if $z>\inf A+\inf B$, then $z=z_A+z_B$ for some $z_A>\inf A$ and $z_B>\inf B$ (take z_A to be any number satisfying $z-\inf B>z_A>\inf A$ and take $z_B=z-z_A$). Then we can find $z_A>x\in A$ and $z_B>y\in B$. This implies $z>x+y\in A+B$ and shows that any number bigger than $\inf A+\inf B$ is not a lower bound of $A+B$.

The proof for the product is the same, after replacing addition and subtraction by product and division. □

For $x,y>1$, by Lemma 2.15, we have (r,s are rational numbers)

$$\begin{aligned}(xy)^z&=\inf\{(xy)^r\colon r>z\}=\inf\{x^ry^r\colon r>z\},\\ x^zy^z&=\inf\{x^r\colon r>z\}\inf\{y^s\colon s>z\}=\inf\{x^ry^s\colon r,s>z\}.\end{aligned}$$

Since the first set is smaller than the second, we have $(xy)^z\geq x^zy^z$. On the other hand, since any number in the second set satisfies $x^ry^s\geq x^ty^t$ for $t=\min\{r,s\}>z$, we get $(xy)^z\leq x^zy^z$. This proves

$$(xy)^z=x^zy^z \text{ for } x,y>1.$$

Now suppose $x=\dfrac{x_1}{x_2}=\dfrac{x_1'}{x_2'}$ with $x_1,x_2,x_1',x_2'>1$. By what we just proved, we have

$$\frac{x_1}{x_2}=\frac{x_1'}{x_2'}\implies x_1x_2'=x_1'x_2\implies (x_1x_2')^y=(x_1'x_2)^y\implies x_1^yx_2'^y=x_1'^yx_2^y\implies \frac{x_1^y}{x_2^y}=\frac{x_1'^y}{x_2'^y}.$$

Therefore x^y is well defined for any $x>1$ and $y\in\mathbb{R}$.

Proposition 2.16. *The real exponent x^y has the following properties.*

$$(xy)^z=x^zy^z,\quad x^{y+z}=x^yx^z,\quad x^{yz}=(x^y)^z,$$

$$x>1,\ y>z\implies x^y>x^z,\quad x>y>0\implies \begin{cases}x^z>y^z, & \text{if } z>0,\\ x^z<y^z, & \text{if } z<0.\end{cases}$$

Proof. We already know $(xy)^z = x^z y^z$ for $x, y > 1$. To prove $(xy)^z = x^z y^z$ for general $x, y > 0$, we write $x = \dfrac{x_1}{x_2}$ and $y = \dfrac{y_1}{y_2}$ with $x_1, x_2, y_1, y_2 > 1$. Then $xy = \dfrac{x_1 y_1}{x_2 y_2}$ with $x_1 y_1, x_2 y_2 > 1$, and

$$(xy)^z = \frac{(x_1 y_1)^z}{(x_2 y_2)^z} = \frac{x_1^z y_1^z}{x_2^z y_2^z} = \frac{x_1^z}{x_2^z}\frac{y_1^z}{y_2^z} = x^z y^z.$$

For the equality $x^{y+z} = x^y x^z$, the following proves the case $x > 1$.

$$\begin{aligned}
x^{y+z} &= \inf\{x^r \colon r > y + z\} && \text{[definition of } x^{y+z}\text{]} \\
&= \inf\{x^{s+t} \colon s > y,\ t > z\} \\
&= \inf\{x^s x^t \colon s \in Y, t \in Z\} && \text{[Proposition 2.13]} \\
&= \inf\{x^s \colon s \in Y\} \inf\{x^t \colon t \in Z\} && \text{[Lemma 2.15]} \\
&= x^y x^z. && \text{[definition of } x^y, x^z\text{]}
\end{aligned}$$

Here the second equality follows from $y = \inf\{s \in \mathbb{Q} \colon s > y\}$, $z = \inf\{t \in \mathbb{Q} \colon t > z\}$ and Lemma 2.15. For the general $x > 0$, we have

$$x^{y+z} = \frac{x_1^{y+z}}{x_2^{y+z}} = \frac{x_1^y x_1^z}{x_2^y x_2^z} = \frac{x_1^y}{x_2^y}\frac{x_1^y}{x_2^y} = x^y x^z.$$

Next we prove that $x > 1$ and $y > z$ imply $x^y > x^z$. There is $r \in \mathbb{N}$ satisfying $y - z > r > 0$. Then $s > y - z$ implies $x^s > x^r$ by Proposition 2.13, so that

$$x^{y-z} = \inf\{x^s \colon s \in \mathbb{Q},\ s > y - z\} \geq x^r > 1.$$

Therefore $x^y = x^{y-z} x^z > x^z$.

Furthermore, for $x > y > 0$ and $z > 0$, we have

$$x > y > 0,\ z > 0 \implies \frac{x}{y} > 1,\ z > 0 \implies x^z = \left(\frac{x}{y}\right)^z y^z > \left(\frac{x}{y}\right)^0 y^z = y^z.$$

For the case $z < 0$, we note that $1 = x^0 = x^{z-z} = x^z x^{-z}$. Therefore we have $x^{-z} = \dfrac{1}{x^z}$, and the inequality follows from the case $z > 0$.

Finally, we prove the equality $x^{yz} = (x^y)^z$. For the case $z = n \in \mathbb{N}$, the equality $x^{yn} = (x^y)^n$ follows from the property $x^{y+z} = x^y x^z$ and the induction on n. Next, for the case $z = -n$, $n \in \mathbb{N}$, we have

$$x^{y(-n)} = x^{(-y)n} = (x^{-y})^n = \left(\frac{1}{x^y}\right)^n = \frac{1}{(x^y)^n} = (x^y)^{-n}.$$

The case $z = 0$ is trivial, and we conclude $x^{yz} = (x^y)^z$ for integers z.

For a rational number $z = r = \dfrac{a}{n}$, $n \in \mathbb{N}$, $a \in \mathbb{Z}$, we have

$$((x^y)^r)^n = (x^y)^{rn} = (x^y)^a = x^{ya} = x^{yrn} = (x^{yr})^n.$$

By the uniqueness of the n-th root in Proposition 2.12, we get $(x^y)^r = x^{yr}$.

Now assume $x > 1$ and $y > 0$. We have $x^y > 1$ by the inequality just proved. By the definition of exponential x^y in case $x > 1$, we have

$$(x^y)^z = \inf\{(x^y)^r : r \in \mathbb{Q},\ r > z\},$$
$$x^{yz} = \inf\{x^s : r \in \mathbb{Q},\ s > yz\}.$$

If $s > yz$, then we can find rational r satisfying $\dfrac{s}{y} > r > z$. Since $x > 1$, we get $(x^y)^r = x^{yr} < x^s$. This proves $x^{yz} \geq (x^y)^z$. On the other hand, if $r > z$, then we can find rational s satisfying $yr > s > yz$, and get $(x^y)^r = x^{yr} > x^s$. This proves $x^{yz} \leq (x^y)^z$. Thus we conclude $x^{yz} = (x^y)^z$ for the case $x > 1$ and $y > 0$.

Finally, for $x, y > 0$, we have

$$x^{yz} = \frac{x_1^{yz}}{x_2^{yz}} = \frac{(x_1^y)^z}{(x_2^y)^z} = \left(\frac{x_1^y}{x_2^y}\right)^z = (x^y)^z.$$

Here the third equality makes use of $x_1^y, x_2^y > 1$. The equality can be further extended to any $x > 0$ and all y by using $x^{-z} = \dfrac{1}{x^z}$. □

Exercise 2.11. Finish the proof of Proposition 2.10.