Chapter 1. Sets and Numbers

§1. Sets

A **set** is considered to be a collection of objects (elements). If A is a set and x is an element of the set A, we say x is a member of A or x belongs to A, and we write $x \in A$. If x does not belong to A, we write $x \notin A$. A set is thus determined by its elements.

Let A and B be sets. We say that A and B are **equal**, if they consist of the same elements; that is,

$$x \in A \quad \Longleftrightarrow \quad x \in B.$$

The set with no elements is called the **empty set** and is denoted by $\emptyset$. For any object x, there is a set whose only member is x. This set is denoted by $\{x\}$ and called a **singleton**. For any two objects x, y, there is a set whose only members are x and y. This set is denoted by $\{x, y\}$.

Let A and B be sets. The set A is called a subset of B if every element of A is also an element of B. If A is a subset of B, we write $A \subseteq B$. Further, if A is a subset of B, we also say that B is a superset of A and write $B \supseteq A$.

It follows immediately from the definition that A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$. Thus, every set is a subset of itself. Moreover, the empty set is a subset of every set.

If $A \subseteq B$ and $A \neq B$, then A is a **proper subset** of B and written as $A \subset B$.

Let A be a set. A condition P on the elements of A is **definite** if for each element x of A, it is unambiguously determined whether $P(x)$ is true or false. For each set A and each definite condition P on the elements of A, there exists a set B whose elements are those elements x of A for which $P(x)$ is true. We write

$$B = \{x \in A : P(x)\}.$$

Let A and B be sets. The **intersection** of A and B is the set

$$A \cap B := \{x \in A : x \in B\}.$$

The sets A and B are said to be **disjoint** if $A \cap B = \emptyset$. The **set difference** of B from A is the set

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

The set $A \setminus B$ is also called the **complement** of B relative to A.

Let A and B be sets. There exists a set C such that

$$x \in C \Longleftrightarrow x \in A \text{ or } x \in B.$$

We call C the union of A and B, and write $C = A \cup B$.

Theorem 1.1. *Let A, B, and C be sets. Then*

(1) $A \cup B = B \cup A$; $A \cap B = B \cap A$.

(2) $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$.

(3) *If* $A \subseteq B$, *then* $A \cap B = A$ *and* $A \cup B = B$.

(4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. We shall prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ only. Suppose $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Since $x \in B \cup C$, either $x \in B$ or $x \in C$. Consequently, either $x \in A \cap B$ or $x \in A \cap C$, that is, $x \in (A \cap B) \cup (A \cap C)$.

Conversely, suppose $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$. In both cases, $x \in A$ and $x \in B \cup C$. Hence, $x \in A \cap (B \cup C)$. □

Theorem 1.2. *(DeMorgan's Rules) Let A, B, and X be sets. Then*

(1) $X \setminus (X \setminus A) = X \cap A$.

(2) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$.

(3) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

Proof. (1) If $x \in X \setminus (X \setminus A)$, then $x \in X$ and $x \notin X \setminus A$. It follows that $x \in A$. Hence, $x \in X \cap A$. Conversely, if $x \in X \cap A$, then $x \in X$ and $x \notin X \setminus A$. Hence, $x \in X \setminus (X \setminus A)$.

(2) Suppose $x \in X \setminus (A \cup B)$. Then $x \in X$ and $x \notin A \cup B$. It follows that $x \notin A$ and $x \notin B$. Hence, $x \in X \setminus A$ and $x \in X \setminus B$, that is, $x \in (X \setminus A) \cap (X \setminus B)$. Conversely, suppose $x \in (X \setminus A) \cap (X \setminus B)$. Then $x \in X \setminus A$ and $x \in X \setminus B$. It follows that $x \in X$, $x \notin A$ and $x \notin B$. Hence, $x \notin A \cup B$, and thereby $x \in X \setminus (A \cup B)$.

(3) Its proof is similar to the proof of (2). □

In describing a set, the order in which the elements appear does not matter. Thus the set $\{a, b\}$ is the same as the set $\{b, a\}$. When we wish to indicate that a pair of elements a and b is ordered, we enclose the elements in parentheses: (a, b). Then a is called the first element and b is called the second. The important property of ordered pairs is that

$$(a, b) = (c, d) \quad \text{if and only if } \ a = c \text{ and } b = d.$$

If A and B are sets, then the **Cartesian product** of A and B, written $A \times B$, is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$.

Example 1. Let A be the set of three colors: red, blue, and yellow, and let B be the set of four fruits: apple, banana, orange, and peach. Then $A \times B$ is the set of the following twelve elements:

(red, apple)	(red, banana)	(red, orange)	(red, peach)
(blue, apple)	(blue, banana)	(blue, orange)	(blue, peach)
(yellow, apple)	(yellow, banana)	(yellow, orange)	(yellow, peach)

Let X be a set. The collection of all subsets of X is called the **power set** of X, written as $\mathcal{P}(X)$. The empty set has no elements. But it has exactly one subset. So the power set of $\emptyset$ is the singleton $\{\emptyset\}$.

Example 2. Let X be the set of three letters a, b, and c. List all the elements of $\mathcal{P}(X)$.

Solution. The elements of $\mathcal{P}(X)$ are $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a,b\}$, $\{a,c\}$, $\{b,c\}$, $\{a,b,c\} = A$. It has eight elements.

§2. The Natural Numbers

We denote the set $\{1,2,3,\ldots\}$ of all natural numbers by $\mathbb{N}$. Each natural number n has a successor, namely $n+1$. The set $\mathbb{N}$ of natural numbers has the following properties:

1. 1 belongs to $\mathbb{N}$;
2. If n belongs to $\mathbb{N}$, then its successor $n+1$ belongs to $\mathbb{N}$;
3. 1 is not the successor of any element in $\mathbb{N}$;
4. If m and n in $\mathbb{N}$ have the same successor, then $m = n$;
5. A subset of $\mathbb{N}$ which contains 1, and which contains $n+1$ whenever it contains n, must equal $\mathbb{N}$.

The above five properties are known as the Peano Axioms.

Addition and multiplication are defined in $\mathbb{N}$. For $m, n \in \mathbb{N}$, the sum $m+n$ is a natural number. The addition is commutative and associative:

$$m + n = n + m \quad \forall\, m, n \in \mathbb{N},$$
$$(m+n)+k = m+(n+k) \quad \forall\, m, n, k \in \mathbb{N}.$$

The product mn of two natural numbers m and n is a natural number. The multiplication is also commutative and associative:

$$mn = nm \quad \forall\, m, n \in \mathbb{N},$$
$$(mn)k = m(nk) \quad \forall\, m, n, k \in \mathbb{N}.$$

Moreover, the multiplication is distributive with respect to the addition:

$$m(n+k) = mn + mk \quad \forall\, m, n, k \in \mathbb{N}.$$

The last property in the Peano Axioms is the basis of mathematical induction. Let $P_1, P_2, \ldots$ be a list of statements or propositions that may or may not be true. The principle of mathematical induction asserts that all the statements $P_1, P_2, \ldots$ are true if

(I_1) P_1 is true, and

(I_2) P_{n+1} is true whenever P_n is true.

We will refer to (I_1) as the basis for induction and will refer to (I_2) as the induction step. For a sound proof based on mathematical induction, properties (I_1) and (I_2) must both be verified.

Example 1. Prove $1 + 2 + \cdots + n = n(n+1)/2$ for natural numbers n.

Proof. Our nth proposition is P_n : "$1 + 2 + \cdots + n = n(n+1)/2$". Thus P_1 asserts that $1 = 1(1+1)/2$. This is obviously true.

For the induction step, suppose that P_n is true, *i.e.*, $1 + 2 + \cdots + n = n(n+1)/2$. Since we wish to prove P_{n+1} from this, we add $n+1$ to both sides to obtain

$$1 + 2 + \cdots + n + (n+1) = \frac{1}{2}n(n+1) + (n+1)$$
$$= \frac{1}{2}(n+1)(n+2) = \frac{1}{2}(n+1)((n+1)+1).$$

Thus, P_{n+1} is true if P_n holds. By the principle of mathematical induction, we conclude that P_n is true for all n. □

Example 2. If a set X has n elements, then the power set $\mathcal{P}(X)$ has 2^n elements.

Proof. We proceed by mathematical induction on n. If $n = 1$ and X has one element, then X has exactly two subsets: $\emptyset$ and X itself. So $\mathcal{P}(X)$ has exactly two elements. This establishes the basis for induction.

For the induction step, suppose that the power set of any set with n elements has 2^n elements. Let X be a set having $n+1$ elements. Fix an element x in X. Then $A := X \setminus \{x\}$ has n elements. By the induction hypothesis, the power set $\mathcal{P}(A)$ has 2^n elements. Let B be a subset of X. Either $x \in B$ or $x \notin B$. If $x \notin B$, then B is a subset of A. If $x \in B$, then $B = (B \cap A) \cup \{x\}$. Thus any subset B of X is either a subset of A or is the union of a subset of A with $\{x\}$. The number of subsets of A is 2^n, and the number of subsets of the form $C \cup \{x\}$ with $C \subseteq A$ is also 2^n. Therefore the total number of subsets of X is $2^n + 2^n = 2^{n+1}$. This completes the induction procedure. □

§3. Relations

Let A and B be sets. A **relation from** A **to** B is any subset R of $A \times B$. We say that $a \in A$ and $b \in B$ are related by R if $(a, b) \in R$, and we often denote this by writing "aRb". If $B = A$, then we speak a relation $R \subseteq A \times A$ being a **relation on** A.

A relation R on a set S is called an **equivalence relation** if it has the following properties for all $x, y, z \in S$:

E1. (reflexivity) xRx;

E2. (symmetry) if xRy, then yRx;
E3. (transitivity) if xRy and yRz, then xRz.
Example 1. Let X be a set and let S be the power set $\mathcal{P}(X)$. An element of $S \times S$ has the form (A, B), where A and B are subsets of X. Let

$$R = \{(A, B) \in S \times S : \ A \text{ and } B \text{ have the same number of elements } \}.$$

Then R is an equivalence relation on S.

Given an equivalence relation R on a set S, we define the equivalence class (with respect to R) of $x \in S$ to be the set

$$E_x = \{y \in S : yRx\}.$$

Since R is reflexive, each element of S is in some equivalent class. Furthermore, two different equivalent classes must be disjoint.

In the above example, if $X = \{a, b, c\}$ is the set of three letters a, b, and c, then its power set $S = \mathcal{P}(X)$ has four equivalence classes with respect to R: $\{\emptyset\}$, $\{\{a\}, \{b\}, \{c\}\}$, $\{\{a, b\}, \{a, c\}, \{b, c\}\}$, $\{\{a, b, c\}\}$. They form a partition of S.

A relation R on a set S is called a **partial ordering** if it has the following properties for all $x, y, z \in S$:
O1. (reflexivity) xRx;
O2. (antisymmetry) if xRy and yRx, then $x = y$;
O3. (transitivity) if xRy and yRz, then xRz.
Example 2. Let X be a set and let S be the power set $\mathcal{P}(X)$. An element of $S \times S$ has the form (A, B), where A and B are subsets of X. Let

$$R = \{(A, B) \in S \times S : A \subseteq B\}.$$

Then R is a partial ordering on S.

Let $m, n \in \mathbb{N}$. If there exists some $k \in \mathbb{N}$ such that $n = m + k$, then we write $m < n$ or $n > m$. If $m < n$ or $m = n$, we write $m \le n$ or $n \ge m$. It is clear that $\le$ is a partial ordering on $\mathbb{N}$.

A partial ordering $\le$ on a set S is called a **linear** or **total ordering** if it has the additional property
O4. (comparability) For $x, y \in S$, either $x \le y$ or $y \le x$.

The partial ordering $\le$ on $\mathbb{N}$ is a total ordering. On the other hand, if a set X has more than one element, then the relation $\subseteq$ on $\mathcal{P}(X)$ is not a total ordering. Indeed, for any two distinct elements x and y in X, neither $\{x\} \subseteq \{y\}$ nor $\{y\} \subseteq \{x\}$.

Let $\leq$ be a partial ordering on a nonempty set X. For $x, y \in X$, $y \geq x$ has the same meaning as $x \leq y$. If $x \leq y$ and $x \neq y$, then we write $x < y$ or $y > x$. Let A be a nonempty subset of X. An element $a \in A$ is called the **smallest** (least) element of A if $a \leq x$ for all $x \in A$. Note that such an element is unique. Indeed, if a_1 and a_2 are two such elements of A, then $a_1 \leq a_2$ and $a_2 \leq a_1$. Since the relation $\leq$ is antisymmetric, it follows that $a_1 = a_2$. An element $b \in A$ is called the **largest** (greatest) element of A, if $b \geq x$ for all $x \in A$. An element $r \in A$ is said to be a **minimum** of A if there is no element $x \in A$ such that $x < r$. An element $s \in A$ is said to be a **maximum** of A if there is no element $y \in A$ such that $y > s$.

Theorem 3.1. *Let $\leq$ be a partial ordering on a nonempty set X, and let A be a nonempty subset of X.*

(1) *Suppose that a is the smallest element of A. Then a is also a minimal element of A, and a is the only minimal element of A.*
(2) *If $\leq$ is a total ordering on X and a is a minimal element of A, then a is the smallest element of A.*

Proof. (1) Let a be the smallest element of A. Then $a \leq x$ for all $x \in A$; hence there is no $x \in A$ such that $x < a$. This shows that a is a minimal element of A. Further, if $b \in A$ and $b \neq a$, then we have $b \geq a$ and $b \neq a$. Hence $b > a$. So b is not a minimal element of A. This shows that a is the only minimal element of A.

(2) Suppose that $\leq$ is a total ordering on X and a is a minimal element of A. Let x be an arbitrary element of A. Since $\leq$ is a total ordering, either $x \geq a$ or $x < a$. But a is a minimal element of A. So $x < a$ is false. Hence we must have $x \geq a$. This shows that a is the smallest element of A. $\square$

Theorem 3.2. *Every nonempty subset of $\mathbb{N}$ contains a least element.*

Proof. Let S_n be the set of all natural numbers less than or equal to n. Let P_n be the statement that every nonempty subset of S_n contains a least element. For $n = 1$, if A is a nonempty subset of $\{1\}$, then $A = \{1\}$ and 1 is the least element of A. For the induction step, suppose P_n is true. Let A be a nonempty subset of S_{n+1}. If $A \cap S_n$ is empty, then $A = \{n+1\}$ and $n+1$ is the least element of A. If $A \cap S_n$ is nonempty, then it has a least element a, by the induction hypothesis P_n. It is easily seen that a is the least element of A. This completes the induction step.

Now let A be an arbitrary nonempty subset of $\mathbb{N}$. Then A contains a natural number, say n. The intersection $A \cap S_n$ is a nonempty subset of S_n. By what has been proved, $A \cap S_n$ has a least element a. Clearly, a is the least element of A. $\square$

§4. Functions

Let A and B be sets. Suppose that F is a relation from A to B. Then F is called a **function from A to B** if for every $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in F$. Functions are also called **maps** or **mappings**.

Example 1. For each of the following relations from $A = \{a, b, c, d\}$ to $B = \{1, 2, 3, 4, 5\}$, determine whether or not it is a function from A to B.

(1) $\{(a, 1), (b, 2), (c, 3)\}$
(2) $\{(a, 1), (b, 2), (c, 3), (d, 4), (d, 5)\}$
(3) $\{(a, 1), (b, 2), (c, 3), (d, 5)\}$
(4) $\{(a, 5), (b, 5), (c, 5), (d, 5)\}$

Solution. (1) No, since $d \in A$, but there is no pair (d, x) in the relation. (2) No, since both $(d, 4)$ and $(d, 5)$ are in the relation. (3) Yes, since each element of A is related to exactly one element of B. (4) Yes, since each element of A is related to exactly one element of B, even though every element of A is related to the same element of B.

Suppose that f is a function from A to B. Then A is called the **domain** of the function f. If $a \in A$, then there is exactly one element b in B such that $(a, b) \in f$. This unique b is called the value of f at a or the image of a under f, and it is written $f(a)$. The set $\{f(a) : a \in A\}$ is called the **range** of f. It is a subset of B. Let f_1 be a function from A_1 to B_1, and let f_2 be a function from A_2 to B_2. Then $f_1 = f_2$ if and only if $A_1 = A_2$, $B_1 = B_2$, and $f_1(a) = f_2(a)$ for all $a \in A_1$.

Let A and B be sets and let f be a function from A to B. Then f is called **injective** or **one-to-one** if for all $x, y \in A$, $f(x) = f(y)$ implies that $x = y$. Moreover, f is called **surjective** or **onto** if for all $b \in B$ there is an $a \in A$ with $f(a) = b$. Finally, f is called **bijective** if f is both injective and surjective.

Example 2. (1) Let f be the function from $\mathbb{N}$ to $\mathbb{N}$ given by $f(n) = 2n$ for $n \in \mathbb{N}$. Then f is injective but not surjective. (2) Let g be the function from $\mathbb{N}$ to $\mathbb{N}$ that sends each $n \in \mathbb{N}$ to the least natural number m such that $2m \geq n$. Then g is surjective but not injective. (3) Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4, 5\}$. Let h be the relation $\{(a, 1), (b, 2), (c, 3), (d, 4), (e, 5)\}$. Then h is a bijective function.

Let A be a set, and let i_A be the relation $\{(a, a) : a \in A\}$. We call i_A the **identity function** on A. In other words, $i_A(a) = a$ for all $a \in A$. Clearly, i_A is bijective.

Let A, B, C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. Let h the function given by $h(a) = g(f(a))$, $a \in A$. Then h is called the **composition** of f and g and denoted by $g \circ f$.

Theorem 4.1. *Let A and B be sets and let f be a function from A to B. Then f is* *bijective if and only if there exists a function g from B to A such that $g \circ f = i_A$ and $f \circ g = i_B$.*

Proof. If there exists a function g from B to A such that $g \circ f = i_A$, then f is injective. Indeed, if $x, y \in A$ and $f(x) = f(y)$, then

$$x = i_A(x) = g(f(x)) = g(f(y)) = i_A(y) = y.$$

Moreover, suppose $f \circ g = i_B$. Then for $b \in B$ we have $f(g(b)) = (f \circ g)(b) = i_B(b) = b$. So f is surjective.

Conversely, suppose that f is bijective. Recall that f is considered as a relation from A to B. Let g be the relation from B to A given by $\{(b, a) \in B \times A : f(a) = b\}$. Since f is bijective, g is a function. Thus $g(b) = a$ if and only if $f(a) = b$. Hence, $g(f(a)) = a$ for all $a \in A$ and $f(g(b)) = b$ for all $b \in B$. This shows that $g \circ f = i_A$ and $f \circ g = i_B$. $\square$

Let f be a bijective function from A to B. From the above proof we see that there is a unique function g from B to A such that $g \circ f = i_A$ and $f \circ g = i_B$. The function g is called the **inverse** of f.

§5. Integers

Let $\mathbb{Z}$ denote the set of integers. We have

$$\mathbb{Z} := \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}.$$

In other words, the set $\mathbb{Z}$ consists of positive integers, 0, and negative integers. Let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

Addition and multiplication are defined in $\mathbb{Z}$. In particular, $m + 0 = m$ and $m \cdot 1 = m$ for all $m \in \mathbb{Z}$. We define $-0 := 0$ and $-(-n) := n$ for $n \in \mathbb{N}$. Consequently, $n + (-n) = 0$ for all $n \in \mathbb{Z}$. Both addition and multiplication are associative and commutative. Moreover, multiplication is distributive with respect to addition:

$$m(n + k) = mn + mk \quad \forall\, m, n, k \in \mathbb{Z}.$$

A system $(R, +, \cdot)$ is called a **commutative ring**, if R is a nonempty set and the addition and multiplication satisfy the following properties:

A1. The addition is associative: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

A2. The addition is commutative: $a + b = b + a$ for all $a, b \in R$.

A3. R has a zero element 0 such that $a + 0 = a$ for all $a \in R$.

A4. Each element $a \in R$ has a negative element $-a$ such that $a + (-a) = 0$.

M1. The multiplication is associative: $(ab)c = a(bc)$ for all $a, b, c \in R$.

M2. The multiplication is commutative: $ab = ba$ for all $a, b \in R$.

DL. The multiplication is distributive with respect to addition: $a(b + c) = ab + ac$ for all $a, b, c \in R$.

If R has an element $1 \neq 0$ such that $a \cdot 1 = a$ for all $a \in R$, then R is called the **identity** of R. Thus $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.

Theorem 5.1. *Let $(R, +, \cdot)$ be a commutative ring. The following statements are true for $a, b, c \in R$.*

(1) $a + c = b + c$ *implies* $a = b$*;*

(2) $-(-a) = a$*;*

(3) $a \cdot 0 = 0$*;*

(4) $(-a)b = -ab$*;*

(5) $(-a)(-b) = ab$*.*

Proof. (1) $a + c = b + c$ implies $(a + c) + (-c) = (b + c) + (-c)$ and so by A1 we have $a + [c + (-c)] = b + [c + (-c)]$. By A4 this reduces to $a + 0 = b + 0$ and so $a = b$ by A3.

(2) By A4 and A2 we have $[-(-a)] + (-a) = 0 = a + (-a)$ and so $-(-a) = a$ by (1).

(3) We use A3 and DL to obtain $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$. Hence, $0 + a \cdot 0 = a \cdot 0 + a \cdot 0$. By (1) we conclude that $a \cdot 0 = 0$.

(4) Since $a + (-a) = 0$, we have $ab + (-a)b = [a + (-a)]b = 0 \cdot b = 0 = ab + (-ab)$. From (1) we obtain $(-a)b = -ab$.

(5) By (4) and (2) we have $(-a)(-b) = -a(-b) = -(-ab) = ab$. □

For $a, b \in R$, we have $(a + (-b)) + b = a + ((-b) + b) = a + 0 = a$. Moreover, if $c + b = a$, then it follows from (1) in the above theorem that $c = a + (-b)$. We define the **difference** $a - b$ as $a + (-b)$. We have

$$(a + b)^2 = a^2 + 2ab + b^2, \quad (a - b)^2 = a^2 - 2ab + b^2, \quad \text{and} \quad (a + b)(a - b) = a^2 - b^2.$$

There is a natural order relation on $\mathbb{Z}$. For $m, n \in \mathbb{Z}$, if $n - m \in \mathbb{N}_0$, then we write $m \leq n$ or $n \geq m$. Evidently, $\leq$ is a total ordering on $\mathbb{Z}$. If $m, n \in \mathbb{Z}$ and $m \leq n$, then $m + k \leq n + k$ for all $k \in \mathbb{Z}$. Moreover, $mk \leq nk$ for all $k \geq 0$.

A commutative ring R is called an **ordered commutative ring** if it has a total ordering $\leq$ satisfying the following properties for all $a, b, c \in R$:

OA. If $a \leq b$, then $a + c \leq b + c$.

OM. If $a \leq b$ and $0 \leq c$, then $ac \leq bc$.

Thus, $(\mathbb{Z}, +, \cdot, \leq)$ is an ordered commutative ring with identity.

Theorem 5.2. *Let $(R, +, \cdot, \leq)$ be an ordered commutative ring with identity. The following statements are true for $a, b, c \in R$.*

(1) *if $a \leq b$. then $-b \leq -a$;*

(2) *if $a \leq b$ and $c \leq 0$, then $bc \leq ac$;*

(3) *$0 < a^2$ for all $a \neq 0$;*

(4) *$0 < 1$.*

Proof. (1) Suppose that $a \leq b$. By OA we have $a + [(-a) + (-b)] \leq b + [(-a) + (-b)]$. It follows that $-b \leq -a$.

(2) If $a \leq b$ and $c \leq 0$, then $0 \leq -c$ by (1). Now by OM we have $a(-c) \leq b(-c)$, *i.e.*, $-ac \leq -bc$. From (1) again, we see that $bc \leq ac$.

(3) Since $\leq$ is a total ordering, either $0 < a$ or $a < 0$. If $0 < a$, then $0 \cdot a < a \cdot a$. If $a < 0$, then $0 < -a$ and so $0(-a) < (-a)(-a)$. In both cases we obtain $0 < a^2$.

(4) Since $1 \neq 0$, by (3) we have $0 < 1^2 = 1$. $\square$

Let $(R, +, \cdot, \leq)$ be an ordered commutative ring. The **absolute value** $|a|$ of an element a in R is defined as follows:

$$|a| := \begin{cases} a & \text{if } a > 0, \\ 0 & \text{if } a = 0, \\ -a & \text{if } a < 0. \end{cases}$$

Theorem 5.3. *Let $(R, +, \cdot, \leq)$ be an ordered commutative ring. The following statements are true for $a, b \in R$.*

(1) *$|a| \geq 0$;*

(2) *$-|a| \leq a \leq |a|$;*

(3) *$|a| \leq b$ if and only if $-b \leq a \leq b$;*

(4) *$|a| \geq b$ if and only if $a \geq b$ or $a \leq -b$;*

(5) *$|a + b| \leq |a| + |b|$;*

(6) *$|ab| = |a| \cdot |b|$.*

Proof. (1) It follows from the definition at once.

(2) If $a \geq 0$, then $a = |a| \geq -|a|$. If $a < 0$, then $|a| = -a$, and hence $a = -|a| \leq |a|$.

(3) Suppose $|a| \leq b$. It follows that $-b \leq -|a|$. By (2) we have $-|a| \leq a \leq |a|$. Consequently, $-b \leq a \leq b$. Conversely, suppose $-b \leq a \leq b$. It follows that $-a \leq b$. We have $|a| = a$ or $|a| = -a$. In either case, $|a| \leq b$.

(4) Suppose $|a| \geq b$. It follows that $-|a| \leq -b$. If $a \geq 0$, then $a = |a| \geq b$; if $a < 0$, then $a = -|a| \leq -b$. Conversely, suppose $a \geq b$ or $a \leq -b$. Note that $a \leq -b$ implies $-a \geq b$. We have $|a| = a$ or $|a| = -a$. In either case, $|a| \geq b$.

(5) We use (2) to deduce that $-|a| \leq a \leq |a|$ and $-|b| \leq b \leq |b|$. It follows that $-(|a|+|b|) \leq a+b \leq |a|+|b|$. Then by (3) we have $|a+b| \leq |a|+|b|$.

(6) There are four cases. If $a \geq 0$ and $b \geq 0$, then $ab \geq 0$; hence $|ab| = ab = |a|{\cdot}|b|$. If $a \leq 0$ and $b \leq 0$, then $ab \geq 0$; hence, $|ab| = ab = (-a)(-b) = |a|{\cdot}|b|$. If $a \leq 0$ and $b \geq 0$, then $ab \leq 0$; hence, $|ab| = -ab = (-a)b = |a|{\cdot}|b|$. Finally, if $a \geq 0$ and $b \leq 0$, then $ab \leq 0$; hence, $|ab| = -ab = a(-b) = |a|{\cdot}|b|$. $\square$

An integer m is a **factor** or **divisor** of an integer n (or n is a **multiple** of m) if there exists an integer k such that $n = km$. We say that m divides n and write $m|n$.

Theorem 5.4 (division algorithm). *Let $m \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then there exist unique integers q and r such that*

$$m = kq + r, \quad 0 \leq r < k.$$

Proof. Let us prove existence of the desired q and r. If $k = 1$, then $q = m$ and $r = 0$ satisfy $m = kq + r$ and $0 \leq r < k$. So we may assume $k > 1$. Let m be a positive integer. We prove our assertion by induction on m. For the base case $m = 1$, $q = 0$ and $r = m$ satisfy $m = kq + r$ and $0 \leq r < k$. For the induction step, suppose that our assertion is true for m. We wish to prove it for $m+1$. Thus, $m = kq + r$ with $0 \leq r < k$. If $r < k-1$, then $m+1 = kq + (r+1)$ with $0 \leq r+1 < k$. If $r = k-1$, then $m+1 = kq + r + 1 = kq + k = k(q+1) + 0$. This completes the induction procedure.

If $m = 0$, then $q = 0$ and $r = 0$ satisfy $m = kq + r$. Now suppose that m is a negative integer. Then $-m$ is a positive integer. By what has been proved, $-m = kq + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < k$. It follows that $m = -kq - r$. If $r = 0$, we are done. If $0 < r < k$, then $m = k(-q-1) + (k-r)$ with $0 < k - r < k$.

For uniqueness of q and r, suppose that $m = kq + r = kq' + r'$ with $0 \leq r, r' < k$. It follows that $k(q - q') = r' - r$. If $q > q'$, then $q - q' \geq 1$ and $k(q - q') \geq k$. But $r' - r \leq r' < k$. So this is a contradiction. For the same reason, $q' > q$ will also lead to a contradiction. Thus we must have $q = q'$. Consequently, $r = r'$. $\square$

In the above division algorithm, q is called the **quotient**, and r the **remainder** of m modulo k.

An even number can be represented as $2k$ for some $k \in \mathbb{Z}$. An odd number can be represented as $2k+1$ for some $k \in \mathbb{Z}$. Note that $(2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. So the square of an odd number is an odd number.

§6. Sums and Products

A **binary operation** on a set S is a function from $S \times S$ to S. For example, addition and multiplication of natural numbers are binary operations on $\mathbb{N}$. Let $f : S \times S \to S$ be a binary operation, and let $x, y \in S$. In the additive notation, $f(x, y)$ is denoted by $x + y$. In the multiplicative notation, $f(x, y)$ is denoted by $x \cdot y$ or xy.

Let S be a set with a binary operation, written multiplicatively. The operation is said to be associative, if $(xy)z = x(yz)$ for all $x, y, z \in S$. The operation is said to be commutative, if $xy = yx$ for all $x, y \in S$. An element $e \in S$ is called an **identity element** if $ex = xe = x$ for all $x \in S$. An identity element, if it exists, is unique. In the multiplicative notation, the identity element is often denoted by 1. In the additive notation, the identity element is often denoted by 0.

A **semigroup** is a nonempty set together with one associative binary operation. A **monoid** is a semigroup with an identity element. A semigroup or monoid is commutative when its operation is commutative.

Example 1. (1) $(\mathbb{N}, +)$ is a semigroup, but not a monoid, since $m + n \neq n$ for all $m, n \in \mathbb{N}$. (2) $(\mathbb{N}_0, +)$ is a monoid. We have $0 + n = n + 0 = n$ for all $n \in \mathbb{N}_0$. (3) $(\mathbb{N}, \cdot)$ is a monoid. We have $1 \cdot n = n \cdot 1 = n$ for all $n \in \mathbb{N}$.

Let $(S, +)$ be a semigroup. For $a \in S$ and $n \in \mathbb{N}$, we define na recursively as follows: $1a := a$ and $(n + 1)a := na + a$. If $(S, +)$ is a monoid, then we define $0a := 0$.

Theorem 6.1. *Let $(S, +)$ be a semigroup. The following properties hold for all $a \in S$ and all $m, n \in \mathbb{N}$:*

(1) $ma + na = (m + n)a$;

(2) $m(na) = (mn)a$;

(3) *if $a, b \in S$ and $a + b = b + a$, then $n(a + b) = na + nb$.*

Proof. (1) We use induction on n. For $n = 1$, by definition we have $ma + a = (m + 1)a$. Let $n \in \mathbb{N}$ and assume that $ma + na = (m + n)a$. It follows that

$$ma + (n + 1)a = ma + (na + a) = (ma + na) + a = (m + n)a + a = (m + n + 1)a.$$

(2) We proceed by induction on n. For $n = 1$ we have $m(1a) = ma = (m \cdot 1)a$. Let $n \in \mathbb{N}$ and assume that $m(na) = (mn)a$. It follows that

$$m\big((n + 1)a\big) = m(na + a) = m(na) + ma = (mn)a + ma.$$

Then we use (1) to deduce that $(mn)a + ma = (mn + m)a = \big(m(n + 1)\big)a$. This completes the induction procedure.

(3) We proceed by induction on n. For $n = 1$ we have $1(a+b) = a+b = 1a+1b$. Let $n \in \mathbb{N}$ and assume that $n(a+b) = na+nb$. It follows that

$$(n+1)(a+b) = n(a+b) + (a+b) = (na+nb) + (a+b) = na + (nb+a) + b.$$

Since $a+b = b+a$, we may use induction to prove that $nb+a = a+nb$. Hence

$$na + (nb+a) + b = na + (a+nb) + b = (na+a) + (nb+b) = (n+1)a + (n+1)b.$$

This completes the proof. $\square$

Let $(S, \cdot)$ be a semigroup. For $a \in S$ and $n \in \mathbb{N}$, we define a^n recursively as follows: $a^1 := a$ and $a^{n+1} := a^n \cdot a$. If $(S, \cdot)$ is a monoid, then we define $a^0 := 1$. In this situation, Theorem 6.1 has the following form.

Theorem 6.1′. *Let $(S, \cdot)$ be a semigroup. The following properties hold for all $a \in S$ and all $m, n \in \mathbb{N}$:*
(1) $a^m \cdot a^n = a^{m+n}$;
(2) $(a^m)^n = a^{mn}$;
(3) *if $a, b \in S$ and $ab = ba$, then $(ab)^n = a^n b^n$.*

Let $(S, +)$ be a semigroup and for each $j \in \mathbb{N}$ let $a_j \in S$. Define the **sum**

$$\sum_{j=1}^{1} a_j = a_1$$

and for $n \in \mathbb{N}$ define the **sum**

$$\sum_{j=1}^{n+1} a_j := \sum_{j=1}^{n} a_j + a_{n+1}.$$

The parameter j is called the **summation index**.

Now let $(S, +)$ be a monoid. For each $j \in \mathbb{Z}$ let $a_j \in S$. Let m and n be arbitrary integers. The sum $\sum_{j=m}^{n} a_j$ is defined as follows. If $n < m$, then

$$\sum_{j=m}^{n} a_j := 0.$$

In other words, the empty sum is defined to be 0. If $n = m$, then

$$\sum_{j=m}^{n} a_j := a_m.$$

For $n \geq m$, define

$$\sum_{j=m}^{n+1} a_j := \sum_{j=m}^{n} a_j + a_{n+1}.$$

Theorem 6.2. *Let $(S, +)$ be a monoid. For each $j \in \mathbb{Z}$ let $a_j, b_j \in S$. Then the following hold.*

(1) *For $m, n, k \in \mathbb{Z}$ with $m \leq k \leq n$,*

$$\sum_{j=m}^{k} a_j + \sum_{j=k+1}^{n} a_j = \sum_{j=m}^{n} a_j.$$

(2) *For $m, n, k \in \mathbb{Z}$,*

$$\sum_{j=m+k}^{n+k} a_j = \sum_{i=m}^{n} a_{i+k}.$$

(3) *If $(S, +)$ is commutative, then for $m, n \in \mathbb{Z}$,*

$$\sum_{j=m}^{n} \big(a_j + b_j\big) = \sum_{j=m}^{n} a_j + \sum_{j=m}^{n} b_j.$$

Proof. (1) If $k = n$, then $\sum_{j=k+1}^{n} a_j = 0$. So our assertion is true for this case. For the general case we use induction on n. For the base case $n = m$, we must have $k = n$. Hence our assertion is valid. Now assume that our assertion is true for n and let $n + 1 \geq k \geq m$. The case $k = n + 1$ has been settled. So we may assume $m \leq k < n + 1$. Thus

$$\begin{aligned}\sum_{j=m}^{n+1} a_j &= \sum_{j=m}^{n} a_j + a_{n+1} = \left(\sum_{j=m}^{k} a_j + \sum_{j=k+1}^{n} a_j\right) + a_{n+1}\\ &= \sum_{j=m}^{k} a_j + \left(\sum_{j=k+1}^{n} a_j + a_{n+1}\right) = \sum_{j=m}^{k} a_j + \sum_{j=k+1}^{n+1} a_j.\end{aligned}$$

This completes the induction procedure.

(2) We proceed by induction on n. If $n = m$, then $\sum_{j=m+k}^{m+k} a_j = a_{m+k} = \sum_{i=m}^{m} a_{i+k}$. This establishes the base case. For the induction step, assume that our assertion is true for n. Then

$$\sum_{j=m+k}^{n+1+k} a_j = \sum_{j=m+k}^{n+k} a_j + a_{n+1+k} = \sum_{i=m}^{n} a_{i+k} + a_{n+1+k} = \sum_{i=m}^{n+1} a_{i+k}.$$

(3) We proceed by induction on n. If $n = m$, then

$$\sum_{j=m}^{m} \big(a_j + b_j\big) = a_m + b_m = \sum_{i=m}^{m} a_j + \sum_{i=m}^{m} a_j.$$

This establishes the base case. For the induction step, assume that our assertion is true for n. Then

$$\sum_{j=m}^{n+1}(a_j+b_j)=\sum_{j=m}^{n}(a_j+b_j)+(a_{n+1}+b_{n+1})=\left(\sum_{j=m}^{n}a_j+\sum_{j=m}^{n}b_j\right)+(a_{n+1}+b_{n+1}).$$

Since $(S,+)$ is commutative, we have

$$\left(\sum_{j=m}^{n}a_j+\sum_{j=m}^{n}b_j\right)+(a_{n+1}+b_{n+1})=\left(\sum_{j=m}^{n}a_j+a_{n+1}\right)+\left(\sum_{j=m}^{n}b_j+b_{n+1}\right)=\sum_{j=m}^{n+1}a_j+\sum_{j=m}^{n+1}b_j.$$

This completes the induction procedure. □

Now let $(S,\cdot)$ be a monoid. For each $j\in\mathbb{Z}$ let $a_j\in S$. Let m and n be arbitrary integers. The product $\prod_{j=m}^{n}a_j$ is defined as follows. If $n<m$, then

$$\prod_{j=m}^{n}a_j:=1.$$

In other words, the empty product is defined to be 1. If $n=m$, then

$$\prod_{j=m}^{n}a_j:=a_m.$$

For $n\geq m$, define

$$\prod_{j=m}^{n+1}a_j:=\prod_{j=m}^{n}a_j\cdot a_{n+1}.$$

The following theorem is a restatement of Theorem 6.2 in the multiplicative notation.

Theorem 6.2′. *Let $(S,\cdot)$ be a monoid. For each $j\in\mathbb{Z}$ let $a_j,b_j\in S$. Then the following hold.*

(1) *For $m,n,k\in\mathbb{Z}$ with $m\leq k\leq n$,*

$$\prod_{j=m}^{k}a_j\cdot\prod_{j=k+1}^{n}a_j=\prod_{j=m}^{n}a_j.$$

(2) *For $m,n,k\in\mathbb{Z}$,*

$$\prod_{j=m+k}^{n+k}a_j=\prod_{i=m}^{n}a_{i+k}.$$

(3) *If $(S,\cdot)$ is commutative, then for $m,n\in\mathbb{Z}$,*

$$\prod_{j=m}^{n}(a_j\cdot b_j)=\prod_{j=m}^{n}a_j\cdot\prod_{j=m}^{n}b_j.$$

The following theorem generalizes the distributive law.

Theorem 6.3. *Let $(R, +, \cdot)$ be a commutative ring with identity. For each $j \in \mathbb{Z}$ let $a_j \in R$. Then the following distributive property is valid for all $m, n \in \mathbb{Z}$ and all $c \in R$:*

$$c \cdot \left(\sum_{j=m}^{n} a_j \right) = \sum_{j=m}^{n} (c \cdot a_j).$$

Proof. If $n < m$, then both sides of the above equation are equal to 0. For $n \geq m$ we proceed by induction on n. For the base case $n = m$, both sides of the above equation are equal to $c \cdot a_m$. For the induction step, let $n \geq m$ and assume that our assertion is valid for n. Since $\sum_{j=m}^{n+1} a_j = \sum_{j=m}^{n} a_j + a_{n+1}$. By the distributive law we have

$$c \cdot \sum_{j=m}^{n+1} a_j = c \cdot \left(\sum_{j=m}^{n} a_j + a_{n+1} \right) = c \cdot \sum_{j=m}^{n} a_j + c \cdot a_{n+1}.$$

By the induction hypothesis, $c \cdot \sum_{j=m}^{n} a_j = \sum_{j=m}^{n} (c \cdot a_j)$. Therefore,

$$c \cdot \sum_{j=m}^{n+1} a_j = \sum_{j=m}^{n} (c \cdot a_j) + (c \cdot a_{n+1}) = \sum_{j=m}^{n+1} (c \cdot a_j).$$

This completes the induction procedure. □

Theorem 6.4. *Let $(R, +, \cdot)$ be a commutative ring with identity. The following property holds for all $a, b \in R$ and all $n \in \mathbb{N}$:*

$$a^n - b^n = (a - b)\left(\sum_{j=0}^{n-1} a^{n-1-j} b^j \right) = (a - b)\big(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}\big).$$

Proof. By the distributive law and Theorem 6.3 we have

$$(a-b)\left(\sum_{j=0}^{n-1} a^{n-1-j} b^j \right) = a \cdot \sum_{j=0}^{n-1} a^{n-1-j} b^j - b \cdot \sum_{j=0}^{n-1} a^{n-1-j} b^j = \sum_{j=0}^{n-1} a^{n-j} b^j - \sum_{j=0}^{n-1} a^{n-1-j} b^{j+1}.$$

By Theorem 6.2 we deduce that

$$\sum_{j=0}^{n-1} a^{n-j} b^j = a^n + \sum_{j=1}^{n-1} a^{n-j} b^j \quad \text{and} \quad \sum_{j=0}^{n-1} a^{n-1-j} b^{j+1} = \sum_{j=0}^{n-2} a^{n-1-j} b^{j+1} + b^n.$$

Applying Theorem 6.2 again we obtain

$$\sum_{j=0}^{n-2} a^{n-1-j} b^{j+1} = \sum_{j=1}^{n-1} a^{n-j} b^j.$$

Therefore,

$$(a - b)\left(\sum_{j=0}^{n-1} a^{n-1-j} b^j \right) = \left(a^n + \sum_{j=1}^{n-1} a^{n-j} b^j \right) - \left(\sum_{j=1}^{n-1} a^{n-j} b^j + b^n \right) = a^n - b^n.$$

This completes the proof of the theorem. □

§7. Rational Numbers

We use $\mathbb{Q}$ to denote the set of rational numbers:

$$\mathbb{Q} := \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

The addition in $\mathbb{Q}$ is defined by the rule

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

The multiplication in $\mathbb{Q}$ is defined by the rule

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

A system $(F, +, \cdot)$ is called a **field**, if it is a commutative ring with identity, and, in addition, each nonzero element a in F has an inverse a^{-1} such that $aa^{-1} = 1$. Clearly, each element a has only one inverse. It is easily seen that $(\mathbb{Q}, +, \cdot)$ is a field.

Let $(F, +, \cdot)$ be a field. If $a, b \in F$ and $b \neq 0$, we define a/b as ab^{-1}. In particular, $1/b = b^{-1}$. Note that a/b is the unique element such that $(a/b)b = a$. Thus, division is well defined in a field.

Theorem 7.1. *Let $(F, +, \cdot)$ be a field. The following properties hold for $a, b, c, d \in F$:*

(1) $a \neq 0$ *and* $b \neq 0$ *imply* $ab \neq 0$*;*

(2) $ac = bc$ *and* $c \neq 0$ *imply* $a = b$*;*

(3) *if* $b \neq 0$ *and* $d \neq 0$*, then* $a/b = c/d$ *if and only if* $ad = bc$*.*

(4) *if* $b \neq 0$ *and* $c \neq 0$*, then* $(ac)/(bc) = a/b$*.*

(5) *if* b, c, d *are nonzero, then*

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc}.$$

Proof. (1) If $ab = 0$ and $a \neq 0$, then $b = (a^{-1}a)b = a^{-1}(ab) = 0$. (2) $ac = bc$ and $c \neq 0$ imply $a = a(cc^{-1}) = (ac)c^{-1} = (bc)c^{-1} = b(cc^{-1}) = b$. (3) By (1) we have $bd \neq 0$. Moreover, by (2) we see that $a/b = c/d$ if and only if $(bd)(a/b) = (bd)(c/d)$, that is, $ad = bc$. (4) Since $b(ac) = a(bc)$, by (3) we obtain $(ac)/(bc) = a/b$. (5) In light of (3), this follows from $(a/b)(bc) = ac = (c/d)(ad)$. $\square$

A field F is called an **ordered field** if it has a total ordering $\leq$ satisfying the following properties:

OA. If $a \leq b$, then $a + c \leq b + c$.

OM. If $a \leq b$ and $0 \leq c$, then $ac \leq bc$.

Suppose that $m, p \in \mathbb{Z}$ and $n, q \in \mathbb{N}$. If $mq \le np$, we write $m/n \le p/q$. Then $\le$ is a total ordering in $\mathbb{Q}$. With this ordering, $\mathbb{Q}$ becomes an ordered field.

If $a \le b$ and $a \ne b$, we write $a < b$ or $b > a$. If $a < b$, then $a + c < b + c$ for $c \in F$ and $ac < bc$ for $c > 0$.

Theorem 7.2. *Let $(F, +, \cdot, \le)$ be an ordered field. The following statements are true for $a, b, c, d \in F$.*
(1) *if $a > 0$, then $a^{-1} > 0$;*
(2) *if $b > 0$ and $d > 0$, then $(a/b) \le (c/d) \Leftrightarrow ad \le bc$.*
(3) *if $0 < a < b$, then $0 < a^n < b^n$ for all $n \in \mathbb{N}$.*

Proof. (1) If $a > 0$, then $a^{-1} \ne 0$ and so $(a^{-1})^2 > 0$. Hence $a(a^{-1})^2 > 0$. It follows that $a^{-1} > 0$. (2) If $b > 0$ and $d > 0$, then $bd > 0$ and $(bd)^{-1} > 0$. Hence, $(a/b) \le (c/d)$ implies $(a/b)(bd) \le (c/d)(bd)$. It follows that $ad \le bc$. Conversely, if $ad \le bc$, then $(bd)^{-1}(ad) \le (bd)^{-1}(bc)$. Consequently, $a/b \le c/d$. (3) We proceed by induction on n. The proof for the base case $n = 1$ is trivial. Suppose that $0 < a^n < b^n$. Since $a > 0$, we have $0 < a \cdot a^n < a \cdot b^n$. Since $0 < a < b$, we have $a \cdot b^n < b \cdot b^n$. Consequently, $0 < a \cdot a^n < b \cdot b^n$. In other words, $0 < a^{n+1} < b^{n+1}$. This completes the induction procedure. $\square$

For $n \in \mathbb{N}_0$ we define

$$n! := \prod_{j=1}^{n} j.$$

In particular, $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, and $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$. We have $(n+1)! = n!(n+1)$ for all $n \in \mathbb{N}_0$. Further, for $n, k \in \mathbb{N}_0$ with $k \le n$, we define

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

Theorem 7.3. *For all $n, k \in \mathbb{N}$ with $k \le n$,*

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

Consequently, for all $n, k \in \mathbb{N}_0$, $\binom{n}{k}$ is a natural number.

Proof. We have

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!\big(n-(k-1)\big)!} + \frac{n!}{k!(n-k)!} = \frac{n!k}{k!(n-k+1)!} + \frac{n!(n-k+1)}{k!(n-k+1)!},$$

where we have used the fact that $k/k! = 1/(k-1)!$ and $(n-k+1)/(n-k+1)! = 1/(n-k)!$. It follows that

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!(k+n-k+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}.$$

To prove the second statement, we proceed by induction on n. For $n = 0$ we have $k = 0$, and so $\binom{n}{k} = 1 \in \mathbb{N}$. This establishes the base case. For the induction step, suppose that our assertion is valid for n. Consider $\binom{n+1}{k}$. If $k = 0$ or $k = n+1$, then $\binom{n+1}{k} = 1 \in \mathbb{N}$. If $0 < k < n+1$, then $\binom{n}{k-1}$ and $\binom{n}{k}$ are natural numbers, by the induction hypothesis. Therefore, $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \in \mathbb{N}$. This completes the induction procedure. $\square$

We are in a position to establish the following binomial theorem.

Theorem 7.4. *Let $(R, +, \cdot)$ be a commutative ring. Then for all $n \in \mathbb{N}$ and all $a, b \in R$,*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Proof. The proof proceeds by induction on n. For $n = 1$ we have

$$(a+b)^1 = a + b = \sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k}.$$

For the induction step, suppose that our assertion is valid for n. We wish to prove it for $n+1$. By the induction hypothesis we have

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Then we use the distributive law to obtain

$$(a+b)^{n+1} = a \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} + b \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}.$$

For the first sum we make the change of indices: $k = j - 1$. The range of k is from 0 to n, so the range of j is from 1 to $n+1$. Thus

$$\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} = \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n-j+1} = \sum_{j=1}^{n} \binom{n}{j-1} a^j b^{n-j+1} + a^{n+1}.$$

For the second sum we have

$$\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1} = \sum_{j=1}^{n}\binom{n}{j}a^j b^{n-j+1} + b^{n+1}.$$

Consequently,

$$(a+b)^{n+1} = a^{n+1} + \sum_{j=1}^{n}\left[\binom{n}{j-1} + \binom{n}{j}\right]a^j b^{n-j+1} + b^{n+1}.$$

Since $\binom{n}{j-1} + \binom{n}{j} = \binom{n+1}{j}$, we get

$$(a+b)^{n+1} = a^{n+1} + \sum_{j=1}^{n}\binom{n+1}{j}a^j b^{n+1-j} + b^{n+1} = \sum_{j=0}^{n+1}\binom{n+1}{j}a^j b^{n+1-j}.$$

This completes the induction procedure. $\square$

Although the rational numbers form a rich algebraic system, they are inadequate for the purpose of analysis because they are, in a sense, incomplete.

For example, there is no rational number r such that $r^2 = 2$. In order to prove this statement, consider the set S of all positive integers n such that $2n^2 = m^2$ for some $m \in \mathbb{N}$. If the set S is not empty, then we let n_0 be its least element. For this n_0, there exists some $m_0 \in \mathbb{N}$ such that $m_0^2 = 2n_0^2$. Since m_0^2 is an even number, m_0 must be an even number: $m_0 = 2m_1$ for some $m_1 \in \mathbb{N}$. Consequently, $(2m_1)^2 = 2n_0^2$, and so $2m_1^2 = n_0^2$. Thus n_0^2 is an even number, and hence n_0 is an even number: $n_0 = 2n_1$ for some $n_1 \in \mathbb{N}$. Now we have $m_1^2 = 2n_1^2$. Thus $n_1 \in S$ and $n_1 < n_0$. This contradicts the fact that n_0 is the least element of S. Therefore, there is no pair (m, n) of positive integers such that $m^2 = 2n^2$.

Suppose that $\leq$ is a partial ordering on a nonempty set X. Let A be a nonempty subset of X. An element $u \in X$ is called an **upper bound** of A if $u \geq a$ for all $a \in A$. If A has an upper bound, it is called **bounded above**. An element $v \in X$ is called a **lower bound** of A if $v \leq a$ for all $a \in A$. If A has a lower bound, it is called **bounded below**. A subset A of X is called **bounded** if it is bounded above and bounded below.

If s is an upper bound of A and $s \leq u$ for every upper bound u of A, then s is unique. We say that s is the **least upper bound** or the **supermum** of A and write $s = \sup A$. Thus, s is the supremum of A if and only if s satisfies the following two properties: (1) $s \geq a$ for all $a \in A$ and (2) for any $s' < s$, there exists some $b \in A$ such that $s' < b$. If t is a lower bound of A and $t \geq v$ for every lower bound v of A, then we say that t is the **greatest lower bound** or the **infimum** of A and write $t = \inf A$.

Let $A := \{r \in \mathbb{Q} : r^2 \le 2\}$. We shall prove that the set A has no least upper bound in $\mathbb{Q}$. For this purpose we let $s \in \mathbb{Q}$ be an upper bound of A. Let us show $s^2 \ge 2$. Otherwise, $s^2 < 2$. We claim that there exists some $t > 0$ such that $(s+t)^2 < 2$. Indeed, we have $(s+t)^2 = s^2 + 2st + t^2 = s^2 + t(2s+t)$. Thus, if $t(2s+t) < 2 - s^2$, then $(s+t)^2 < 2$. Choose $t := (2-s^2)/(2s+1)$. Since $1 \in A$, we have $s \ge 1$, and so $t = (2-s^2)/(2s+1) < 1$. Hence $t(2s+t) < t(2s+1) = 2 - s^2$. This justifies our claim and shows that s would not be an upper bound of A. Since $s^2 \ne 2$, we must have $s^2 > 2$. Choose $r := (s^2-2)/(2s)$. Then $r > 0$ and

$$(s-r)^2 = s^2 - 2sr + r^2 > s^2 - 2sr = s^2 - 2s\frac{s^2-2}{2s} = 2.$$

This shows that $s - r$ is also an upper bound of A. Therefore s is not the least upper bound of A.

An ordered set $(X, \le)$ is said to be **complete** if every bounded subset of X has a supremum and an infimum. The above example demonstrates that $(\mathbb{Q}, \le)$ is incomplete.

§8. Real Numbers

A real number has a representation of the form

$$k + 0.d_1 d_2 d_3 \cdots,$$

where k is an integer and each digit d_j belongs to $\{0,1,2,3,4,5,6,7,8,9\}$. We use $\mathbb{R}$ to denote the set of all real numbers.

Let Q be the set $\{m/10^r : m \in \mathbb{Z}, r \in \mathbb{N}_0\}$. By using the division algorithm we can easily prove that each $q \in Q$ has a decimal expansion:

$$q = k + \sum_{j=1}^{r} \frac{d_j}{10^j} = k + 0.d_1 \cdots d_r,$$

where $k \in \mathbb{Z}$ and $d_1, \ldots, d_r \in \{0,1,2,3,4,5,6,7,8,9\}$. Thus, q can be identified with the real number

$$k + 0.d_1 \cdots d_r 000 \cdots,$$

which ends in a sequence of all 0's. If $d_r \ne 0$, then q has another representation

$$k + 0.d_1 \cdots (d_r - 1)999 \cdots,$$

which ends in a sequence of all 9's.

Suppose that $x = k + 0.d_1 d_2 d_3 \cdots$ and $x' = k' + 0.d_1' d_2' d_3' \cdots$ are two real numbers and neither decimal representation ends in a sequence of all 9's. We write $x < x'$ if $k < k'$, or if $k = k'$ and there exists some $r \in \mathbb{N}$ such that $d_j = d_j'$ for $1 \le j < r$ and $d_r < d_r'$. Given two real numbers x and y, we write $x \le y$ if $x = y$ or $x < y$. It can be easily proved that $\le$ is a total ordering on $\mathbb{R}$. Moreover, $(\mathbb{R}, \le)$ is complete as stated in the following theorem.

Theorem 8.1. *Every nonempty subset of* $\mathbb{R}$ *that is bounded above has a least upper bound.*

The following theorem establishes the denseness of Q in $\mathbb{R}$.

Theorem 8.2. *If* $x, x' \in \mathbb{R}$ *and* $x < x'$*, then there exists some* $q \in Q$ *such that* $x < q < x'$*.*

Proof. Suppose that $x = k + 0.d_1 d_2 d_3 \cdots$ and $x' = k' + 0.d'_1 d'_2 d'_3 \cdots$ and neither decimal representation ends in a sequence of all 9's. Consider the case $k < k'$ first. There exists some $s \in \mathbb{N}$ such that $d_s < 9$. Let $q := k + 0.d_1 \cdots d_{s-1}9$. Then $x < q < x'$. It remains to deal with the case $k = k'$. Since $x < x'$, there exists some $r \in \mathbb{N}$ such that $d_j = d'_j$ for $1 \le j < r$ and $d_r < d'_r$. There exists some $s > r$ such that $d_s < 9$. With $q := k + 0.d_1 \cdots d_{s-1}9$, we have $x < q < x'$. $\square$

The addition of two real numbers x and y is defined as

$$x + y := \sup\{p + q : p, q \in Q,\ p \le x,\ q \le y\}.$$

For each $x \in \mathbb{R}$, there exists a unique real number $-x$ such that $x + (-x) = 0$.

The multiplication of two real numbers x and y is defined as follows. If $x = 0$ or $y = 0$, we define $x \cdot y = 0$. If $x > 0$ and $y > 0$, we define

$$x \cdot y := \sup\{pq : p, q \in Q,\ 0 < p \le x,\ 0 < q \le y\}.$$

If $x > 0$ and $y < 0$, define $x \cdot y := -(x(-y))$; if $x < 0$ and $y > 0$, define $x \cdot y := -((-x)y)$; if $x < 0$ and $y < 0$, define $x \cdot y := (-x)(-y)$.

It can be proved that $(\mathbb{R}, +, \cdot, \le)$ is an ordered field. Moreover, $\mathbb{Q}$ is a subfield of $\mathbb{R}$. A number in $\mathbb{R} \setminus \mathbb{Q}$ is called an **irrational number**.

Although Theorem 8.1 only guarantees that nonempty subsets of $\mathbb{R}$ that are bounded above have suprema, existence of infima is a consequence.

Theorem 8.3. *Every nonempty subset of* $\mathbb{R}$ *that is bounded below has a greatest lower bound.*

Proof. Let S be a nonempty subset of $\mathbb{R}$ that is bounded below. We denote the set $\{-s : s \in S\}$ by $-S$. Then $-S$ is bounded above. By Theorem 8.1, $\sup(-S)$ exists as a real number. Let $s_0 := \sup(-S)$. We have $s_0 \ge -s$ for all $s \in S$. It follows that $-s_0 \le s$ for all $s \in S$. Hence, $-s_0$ is a lower bound of S. Furthermore, if t is a lower bound of S, then $t \le s$ for all $s \in S$. It follows that $-t \ge -s$ for all $s \in S$. Hence, $-t$ is an upper bound of $-S$. We have $-t \ge s_0$, since s_0 is the least upper bound of $-S$. Consequently, $t \le -s_0$. This shows that $-s_0$ is the greatest lower bound of S and $\inf S = -s_0 = -\sup(-S)$. $\square$

An ordered field F is said to have the **Archimedean property** if for every pair of positive elements a and b, there is a positive integer n such that $na > b$.

Theorem 8.4. *A complete ordered field F has the Archimedean property.*

Proof. We argue by contraposition. Suppose that the Archimedean property fails. Then there exist $a > 0$ and $b > 0$ such that $na \le b$ for all $n \in \mathbb{N}$. Let $S := \{na : n \in \mathbb{N}\}$. Then S is nonempty and b is an upper bound for S. Since the field F is complete, S has a supremum. Let $s_0 := \sup S$. Now $s_0 - a < s_0$, so it is not an upper bound for S. Hence, there exists some $n_0 \in \mathbb{N}$ such that $s_0 - a < n_0 a$. It follows that $s_0 < (n_0 + 1)a$. But $s_0 \ge na$ for all $n \in \mathbb{N}$. This contradiction shows that F has the Archimedean property. $\square$

We have shown that $(\mathbb{R}, +, \cdot, \le)$ is a complete ordered field. If $(F, +, \cdot, \le)$ is also a complete ordered field. Then there is a bijective function φ from F to $\mathbb{R}$ such that φ preserves addition, multiplication, and order. Such a function is called an isomorphism. Thus $\mathbb{R}$ is the unique complete ordered field (up to isomorphism).

For any real number x, there is a unique integer n such that $n \le x < n+1$. This integer n is called the **integer part** of x, and is denoted by $\lfloor x \rfloor$. For example, $\lfloor 5 \rfloor = 5$, $\lfloor 3.2 \rfloor = 3$, and $\lfloor -3.2 \rfloor = -4$.

For a pair of real numbers a and b, we define

$$(a, b) := \{x \in \mathbb{R} : a < x < b\}, \quad [a, b] := \{x \in \mathbb{R} : a \le x \le b\},$$
$$[a, b) := \{x \in \mathbb{R} : a \le x < b\}, \quad (a, b] := \{x \in \mathbb{R} : a < x \le b\}.$$

The set (a, b) is called an **open interval**, the set $[a, b]$ is called a **closed interval**, and the sets $[a, b)$ and $(a, b]$ are called **half-open** (or **half-closed**) **intervals**.

We introduce two symbols ∞ and $-\infty$. The ordering $\le$ in $\mathbb{R}$ can be extended to $\overline{\mathbb{R}} := \mathbb{R} \cup \{-\infty, \infty\}$ by defining

$$-\infty < a < \infty \quad \text{for all } a \in \mathbb{R}.$$

Then we have $(-\infty, \infty) = \mathbb{R}$ and

$$(a, \infty) = \{x \in \mathbb{R} : x > a\}, \quad [a, \infty) = \{x \in \mathbb{R} : x \ge a\},$$
$$(-\infty, b) = \{x \in \mathbb{R} : x < b\}, \quad (-\infty, b] = \{x \in \mathbb{R} : x \le b\}.$$

Let S be any nonempty subset of $\mathbb{R}$. The symbols $\sup S$ and $\inf S$ always make sense. If S is bounded above, then $\sup S$ is a real number; otherwise $\sup S = +\infty$. If S is bounded below, then $\inf S$ is a real number; otherwise $\inf S = -\infty$. Moreover, we have $\inf S \le \sup S$.

Example 2. Write the following sets in interval notation:
(a) $A := \{x \in \mathbb{R} : |x-3| \le 5\}$.
(b) $B := \{x \in \mathbb{R} : |x-3| > 5\}$.

Solution. (a) We see that $|x-3| \le 5$ if and only if $-5 \le x-3 \le 5$, that is, $3-5 \le x \le 3+5$. Hence, $A = [-2, 8]$.

(b) $|x-3| > 5$ if and only if $x-3 < -5$ or $x-3 > 5$. Hence, $B = (-\infty, -2) \cup (8, \infty)$.

§9. Powers and Roots

Given a real number a and a positive integer m, we want to solve the equation $x^m = a$ for x. For this purpose, we first establish the following Bernoulli inequality:

Theorem 9.1. *If $x \ge -1$, then for every positive integer n,*

$$(1+x)^n \ge 1 + nx.$$

Proof. The proof proceeds by induction on n. For $n = 1$, we have $(1+x)^1 = 1 + 1 \cdot x$. For the induction step, suppose that $(1+x)^n \ge 1+nx$ for $x \ge -1$. Since $x \ge -1$, we have $1 + x \ge 0$. Hence,

$$(1+x)^{n+1} = (1+x)(1+x)^n \ge (1+x)(1+nx) = 1 + x + nx + nx^2 \ge 1 + (n+1)x.$$

In the last step we have used the fact $x^2 \ge 0$. This completes the induction procedure. □

Theorem 9.2. *Let m be a positive integer. For every positive real number a, there exists a unique positive real number r such that $r^m = a$.*

Proof. We first prove the existence of r. Let $A := \{x \in \mathbb{R} : x \ge 0 \text{ and } x^m \le a\}$. Then $0 \in A$ and A is bounded above by $\max\{1, a\}$. Since $\mathbb{R}$ is a complete ordered field, A has a supremum. Let $r := \sup A$. If $a \ge 1$, then $1 \in A$; if $0 < a < 1$, then $a \in A$. Hence $r \ge \min\{1, a\} > 0$. We claim that $r^m = a$. To justify our claim, it suffices to show that $r^m \not< a$ and $r^m \not> a$. First, suppose that $r^m > a$. We wish to find some δ with $0 < \delta < r$ such that $(r-\delta)^m > a$. We have $(r-\delta)^m = r^m(1-\delta/r)^m$. So $(r-\delta)^m > a$ is true if $(1-\delta/r)^m > a/r^m$. By the Bernoulli inequality, $(1-\delta/r)^m \ge 1-m\delta/r$. So $1-m\delta/r > a/r^m$ implies $(r-\delta)^m > a$. But $1 - m\delta/r > a/r^m$ holds if and only if $\delta < r(1-a/r^m)/m$. Note that $1 - a/r^m > 0$. Thus, if δ is so chosen that $0 < \delta < r(1-a/r^m)/m$, then $\delta < r$ and $(r-\delta)^m > a$. This shows that r is not the *least* upper bound of A, a contradiction. Therefore $r^m \not> a$. Next. suppose that $r^m < a$. It follows that $(1/r)^m > 1/a$. By what has been proved, there exists some δ with $0 < \delta < 1/r$ such that $(1/r-\delta)^m > 1/a$. Note that $1/r - \delta = 1/r - (r\delta)/\delta = (1 - r\delta)/\delta$. Consequently, $\big(r/(1-\delta r)\big)^m < a$. Hence, $r/(1-\delta r) \in A$. But $r < r/(1-\delta r)$. Thus, r is not an upper bound of A, a contradiction. Therefore $r^m \not< a$. Since $r^m \not> a$ and $r^m \not< a$, we must have $r^m = a$.

For uniqueness, suppose that s is also a positive real number such that $s^m = a$. If $s < r$, then $s^m < r^m = a$; if $s > r$, then $s^m > r^m = a$. Hence we must have $s = r$. □

Let a be a positive real number and let m be a positive integer. Then the unique positive number r such that $r^m = a$ is called the mth **root** of a, denoted $\sqrt[m]{a}$. The second root of a is also called the **square root** of a, denoted $\sqrt{a}$. Note that $\sqrt{a^2} = |a|$.

If $a = 0$, then the equation $x^m = 0$ has a unique solution $\sqrt[m]{0} = 0$. If $a < 0$ and m is an even positive integer, then the equation $x^m = a$ is not solvable in $\mathbb{R}$. In particular, there is no real number r such that $r^2 = -1$. If $a < 0$ and m is an odd positive integer, then the equation $x^m = a$ has a unique solution in $\mathbb{R}$: $x = -\sqrt[m]{|a|}$.

If $a \in \mathbb{R} \setminus \{0\}$ and n is a negative integer, then we define $a^n := (a^{-1})^{-n}$. For $a, b \in \mathbb{R} \setminus \{0\}$ and $m, n \in \mathbb{Z}$, the following properties hold:

$$a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad (a \cdot b)^m = a^m \cdot b^m.$$

Now let a be a positive real number, and let $s \in \mathbb{Q}$. The rational number s has a representation $s = m/n$, where $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. We define

$$a^s := (\sqrt[n]{a})^m.$$

Suppose that $s = p/q$ is another representation with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. Then $qm = pn$. We have

$$\big((\sqrt[q]{a})^p\big)^n = (\sqrt[q]{a})^{pn} = (\sqrt[q]{a})^{qm} = \big((\sqrt[q]{a})^q\big)^m = a^m = \big(\sqrt[n]{a})^m\big)^n.$$

It follows that $(\sqrt[q]{a})^p = (\sqrt[n]{a})^m$. Thus the fractional power a^s is well defined.

Theorem 9.3. *Let a and b be positive real numbers, and let $s, t \in \mathbb{Q}$, then the following hold.*

(1) $a^s \cdot a^t = a^{s+t}$.

(2) $(a^s)^t = a^{st}$.

(3) $(a \cdot b)^s = a^s \cdot b^s$.

Proof. We may assume that $s = p/n$ and $t = q/n$, where $p, q \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then we have $(a^s)^n = a^p$ and $(a^t)^n = a^q$. Moreover, $s + t = (p+q)/n$, so $(a^{s+t})^n = a^{p+q}$. We have

$$(a^s \cdot a^t)^n = (a^s)^n \cdot (a^t)^n = a^p \cdot a^q = a^{p+q} = (a^{s+t})^n.$$

It follows that $a^s \cdot a^t = a^{s+t}$. This proves (1). For (2) we observe that $st = pq/n^2$ and

$$\big((a^s)^t\big)^{n^2} = (a^s)^{qn} = \big((a^s)^n\big)^q = (a^p)^q = a^{pq} = (a^{st})^{n^2}.$$

Consequently, $(a^s)^t = a^{st}$. Finally, we have

$$\big((a \cdot b)^s\big)^n = (a \cdot b)^p = a^p \cdot b^p = (a^s)^n \cdot (b^s)^n = (a^s \cdot b^s)^n.$$

It follows that $(a \cdot b)^s = a^s \cdot b^s$. This completes the proof. $\square$