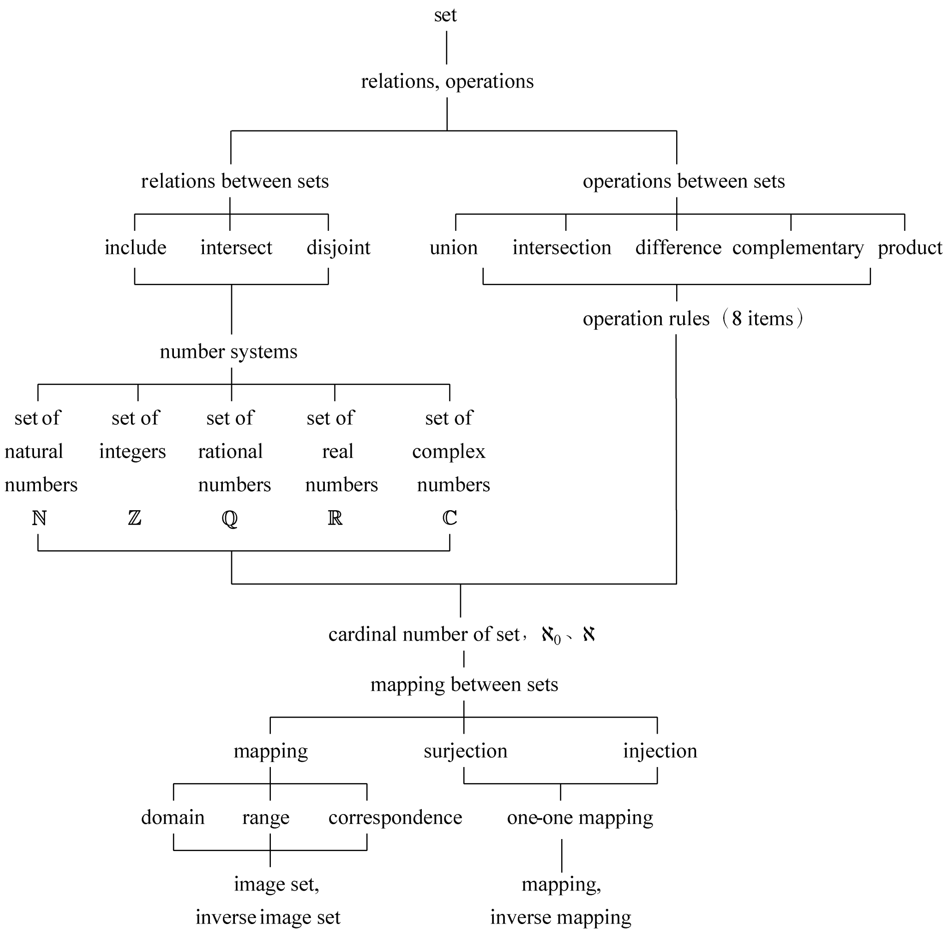
Chapter 1

Set,Structure of Operation on Set

Set theory is the foundation of modern mathematics. We start from its basic knowledge showing the following frame, firstly.



1.1 Sets, the Relations and Operations between Sets

Set theory was constructed at the later period of 19 century by German mathematician G. Cantor. It has developed as an important and fundamental branch of mathematics, rapidly, and permeated through lots of scientific fields as a mathematical tool. There are abundant bibliography and references. We introduce some basic knowledge of set theory in our course, and refer to [1], [2].

1.1.1 Relations between sets

An important thought of mathematics is: put observed objects those having certain properties together, called "a family", or "a collection", or "a set", then studies the properties of some representative elements in the set, instead of studing those individual objects, hence the essence and nature characters of original set can be revealed.

For example, put all rational numbers in one set, and call it **the set of rational numbers**, or simply, **the rational number set**, denoted by

$$\mathbb{Q}=\left\{x: x=\frac{q}{p}, q \in \mathbb{Z}, p \in \mathbb{Z}^{+}\right\}, \quad a \in A$$

with **the set of integers** $\mathbb{Z}=\{\cdots,-2,-1,0,1,2,\cdots\}$, and **the set of positive integers** $\mathbb{Z}^{+}=\{1,2,\cdots\}$.

Here notation "$\in$" means "belong to". That is "$a \in A \Leftrightarrow a$ belongs to A".

Put all continuous functions on the interval $[a,b]$ together, denoted by

$$C([a,b])=\{f: [a,b] \to \mathbb{R}, f(x) \text{ is continuous on } [a,b]\};$$

Then $C([a,b])$ is called **the set of continuous functions on** $[a,b]$.

All functions possessed continuous one order derivatives on $[a,b]$, denoted by

$$C^1([a,b])=\{f(x): [a,b] \to \mathbb{R}, f(x), f'(x) \in C[a,b]\};$$

Then $C^1([a,b])$ is called **the set of first order continuous derivable functions on** $[a,b]$. Moreover, **the set of k-order continuous derivable functions on** $[a,b]$, denoted by

$$C^k([a,b])=\{f(x): [a,b] \to \mathbb{R}, f(x), \cdots, f^{(k)}(x) \in C[a,b]\}, \quad k \in \mathbb{N}.$$

Set In general, a collection of all considered objects possessed certain properties is said to be **a set**, denoted by $A, B, \cdots$, or $X, Y, \cdots$. A member, or an object in a set, is said to be an **element** of the set; A member, or object, is denoted by a、$b\cdots$, or x、y, $\cdots$.

Notation $\in$ and $\notin$ If a is an element of set A, or a member of A, then it is said that a **belongs to** A, denoted by $a \in A$; otherwise, if a is not in A, then it is denoted by $a \notin A$.

"Set" is not only an abstract and profound mathematical idea, but also a very useful and exquisite mathematical tool; It plays role not only in the natural science and social science field, but also in the medical science and humanities science field. It is a main concept、important thought idea, as well as main tool in our book too.

1. Number Systems

positive integer number set $\mathbb{Z}^{+}=\{x: x=1,2,3,\cdots\}$;
natural number set $\mathbb{N}=\{x: x=0,1,2,3,\cdots\}$;
integer number set $\mathbb{Z}=\{x: x=0,\pm 1,\pm 2,\cdots\}$;
rational number set $\mathbb{Q}=\left\{x: x=\frac{q}{p}, q\in\mathbb{Z}, p\in\mathbb{Z}^{+}\right\}$;
real number set $\mathbb{R}=\{x: x \text{ is real}\}$;
complex number set $\mathbb{C}=\{z: z=a+\mathrm{i}b,\quad a,b\in\mathbb{R}\}$, $\mathrm{i}=\sqrt{-1}$.

2. Relations between sets

We consider the position relations between sets.

Include Let A and B be two sets. If each element a in A is also in B, i. e., "$a\in A$ implies $a\in B$", then A is said to be **included in** B, denoted by $A\subseteq B$, or B **includes** A, denoted by $B\supseteq A$; and we say that A **is a subset of** B.

If A is included in B, but $A\neq B$, then A is said to be a **proper subset of** B, denoted by $A\subset B$.

For example, $\mathbb{Z}^{+}\subset\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$; $\{x\in\mathbb{N}: x^2=1\}=\{1\}\subset\{x\in\mathbb{Z}: x^2=1\}=\{1,-1\}$.

Equal If $A\subseteq B$, and $B\subseteq A$, then we say that A **equals** B, denoted by $A=B$.

Intersect Let A and B be two sets. If there are common elements of A and B, then we say that A **intersects** B (in weak sense). It is clear that "include" and "equal" are special cases of "intersect (in weak sense)".

In general, A **intersects** B (in strong sense) means: A and B have common elements, and there is at least one element $a\in A$, but $a\notin B$; also there is at least one element $b\in B$, but $b\notin A$. For example, $A=\{1,2,3,4\}$ intersects $B=\{1,3,5,7\}$ (in strong sense).

Empty set If a set A does not contain any element, then it is called **empty set**, or, A is **empty**, denoted by $A=\varnothing$.

For example, $\{x\in\mathbb{N}: x^2=-1\}=\varnothing$, and $\{z\in\mathbb{C}: z^2=-1\}\neq\varnothing$.

Disjoint Let A and B be two sets. If A and B do not have common element, i. e., their common part is an empty set $\varnothing$, then we say that A **disjoints** B, or A **and** B **disjoint each other**.

For example, the odd number set $A=\{1,3,5,\cdots\}$ and the even number set $B=\{2,4,6,\cdots\}$ disjoint each other.

1.1.2 Operations between sets

1. Union, intersection, difference, complimentary and product of sets

Union of sets Let A and B be two sets. The union set $A\cup B$ of A and B, or union of A and B is defined by(Fig. 1.1.1(a).)

$$A\cup B=\{x: x\in A \text{ or } x\in B\},$$

Intersection of sets Let A and B be two sets. The intersection $A\cap B$ of A and B, or simply intersection of A and B, is defined by(Fig. 1.1.1(b).)

$$A\cap B=\{x: x\in A \text{ and } x\in B\},$$

Usually, it is more general and useful to consider the union $\bigcup\limits_{\lambda\in\Lambda} A_\lambda$ and intersection $\bigcap\limits_{\lambda\in\Lambda} A_\lambda$ of set family $\{A_\lambda: \lambda\in\Lambda\}$ with index set Λ. For example, if $\Lambda=\{1,2,\cdots,n\}$, $n\in\mathbb{N}$, then they are $\bigcup\limits_{j=1}^{n} A_j$ and $\bigcap\limits_{j=1}^{n} A_j$; and if $\Lambda=\mathbb{N}$, they are $\bigcup\limits_{j\in\mathbf{N}} A_j$ and $\bigcap\limits_{j\in\mathbf{N}} A_j$ $\left(\text{or } \bigcup\limits_{j=1}^{\infty} A_j, \bigcap\limits_{j=1}^{\infty} A_j\right)$ respectively.

Difference of sets Let A and B be two sets. The difference $A\setminus B$ of A and B, or for simply, difference of A and B is defined by(Fig. 1.1.1(c).)

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

Symmetric difference For two sets A and B, the symmetric difference $A\triangle B$ is defined by

$$A\triangle B=(A\setminus B)\cup(B\setminus A).$$

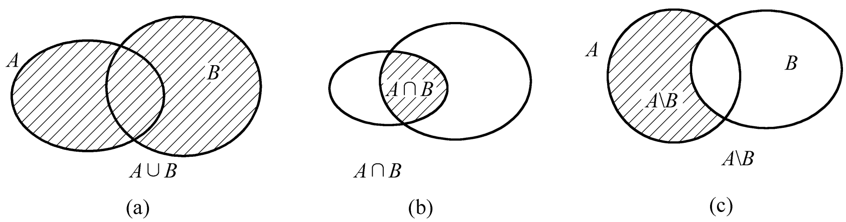
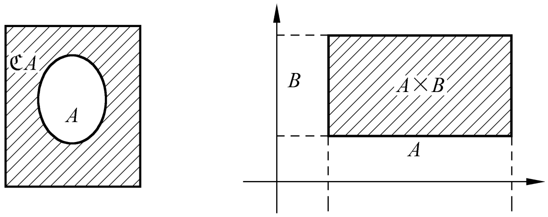


Fig. 1.1.1 Union, intersection and difference

Complementary of sets Let X be a basic set, $A\subset X$ a subset of X. The difference set $X\setminus A$ is said to be **the complementary** of A about X(Fig. 1.1.2(a)), denoted by $A^{C}=X\setminus A$, or by $\complement A$.

Product of sets Let A and B be two sets. The product set $A\times B$ of A and B is defined by(Fig. 1. 1. 2(b).)

$$A\times B=\{(x,y): x\in A, y\in B\}.$$



(a) $\mathfrak{C}A$ (b) $A\times B$

Fig. 1. 1. 2 Complementary and product

The product of n sets is denoted by

$$\prod_{j=1}^{n} A_j \equiv A_1\times A_2\times\cdots\times A_n=\{(x_1,x_2,\cdots,x_n): x_j\in A_j, j=1,2,\cdots,n\}.$$

2. Laws of operations

(1) $A\cap B\subset A\subset A\cup B, A\cap B\subset B\subset A\cup B$;

(2) $A\cap B=B\cap A, A\cup B=B\cup A$;

(3) $A\cap(B\cap C)=A\cap(B\cap C), A\cup(B\cup C)=A\cup(B\cup C)$;

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

(5) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$, $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$;

(6) $\mathfrak{C}(\mathfrak{C}A)=A, \mathfrak{C}(A\cap B)=\mathfrak{C}A\cup\mathfrak{C}B, \mathfrak{C}(A\cup B)=\mathfrak{C}A\cap\mathfrak{C}B$;

(7) $A\cap\left(\bigcap_{j\in I}A_j\right)=\bigcup_{j\in I}(A\cap A_j)$, $A\cup\left(\bigcap_{j\in I}A_j\right)=\bigcap_{j\in I}(A\cup A_j)$;

(8) $\mathfrak{C}\left(\bigcup_{j\in I}A_j\right)=\bigcap_{j\in I}\mathfrak{C}A_j$, $\mathfrak{C}\left(\bigcap_{j\in I}A_j\right)=\bigcup_{j\in I}\mathfrak{C}A_j$. (de Morgan formulas)

1.1.3 Mappings between sets

"Function" is the most important concept and plays crucial role in advanced mathematics, recall that: the domain D_f of a function f is contained in the real number set $\mathbb{R}$ for one variable, or contained in $\mathbb{R}^n$ for several variables; The range R_f is always contained in $\mathbb{R}$. However, variables appearing in modern science and technology are differing, the corresponding relations between two variables, as well as their domains and ranges, all overstep far from Euclidean spaces $\mathbb{R}$ and $\mathbb{R}^n$. Thus, we will consider more general sets instead to be domains and ranges, and give new ideas and methods to describe the concepts of corresponding relations in the place of classical functions.

1. Mappings

Definition 1.1.1 (corresponding relation) Let X and Y be two sets (may be the same, or different).

For **given subsets** $A \subseteq X$, $B \subseteq Y$, if there exists a **corresponding relationship**, denoted by $f: A \to B$, such that for each $x \in A$, there is the **unique** $y \in B$, denoted by $y = f(x)$, then $f: A \to B$ is said to be a **mapping**, or a **transformation**, or an **operator** from A to B. Set A is said to be the **domain** of f, denoted by $\mathfrak{D}_f$; set B is said to be the **range** of f, denoted by $\mathfrak{R}_f$; the set $f(A) = \{f(x): x \in A\} \subseteq B$ is said to be **the image set** of f, denoted by $\mathrm{im}(f) = f(A)$.

For a subset $C \subseteq B$, the set $f^{-1}(C) = \{x \in A: f(x) \in C\} \subseteq A$ is said to be the **inverse image set** of f.

Surjection If $f(A) = B$, then f is said to be a surjection from A onto B, i.e., for each $y \in B$, there is at least one $x \in A$ satisfying $f(x) = y \in Y$. Then, the image set $f(A)$ of f is B, that is, $\mathrm{im}(f) = B$.

Injection If a mapping $f: A \to B$ is one-one corresponding from A into B, i.e.

$$f(x_1) = f(x_2) \quad \text{implies} \quad x_1 = x_2,$$

then f is said to be an infection, or an **one-one mapping** (from A to B).

Note 1 a one-one mapping $f: A \to B$ may not be necessarily a surjection.

Inverse mapping For an injective mapping $f: A \to B$, its inverse mapping $f^{-1}: B \to A$ defined by "$f(x) = y$ implies $f^{-1}(y) = x$"

Note 2 Distinguishing an inverse mapping $f^{-1}: B \to A$ of f with an inverse image set $f^{-1}(B) \subset X$ of f.

Example 1.1.1 Let $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$. Then the mapping $f: A \to B$ with

$$f(a) = 1, \quad f(b) = 2, \quad f(c) = 3$$

is one-one from A into B, but it is not surjective.

Example 1.1.2 Take $A = B = \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$, then the mapping $f: A \to B$ with $f(n) = n + 1$ is one-one from $\mathbb{Z}$ onto $\mathbb{Z}$, and it is a surjective too.

Definition 1.1.2 (compound mapping) Let A, B, C be given sets. For given mappings $f: A \to B$ and $g: B \to C$, if the mapping $h: A \to C$ satisfies

$$z = h(x) = g(f(x)), \quad x \in A,$$

then h is said to be **a compound mapping of f and g**, or **a composition mapping of f and g**, denoted by $h = g \circ f$; and $h = g \circ f: A \to C$.

Note 3 in this definition the image set $f(A)$ must be contained in B which is the domain of mapping $g: B \to C$, but is not necessarily equal to B.

Example 1.1.3　Let $A=C[a,b]$, and mapping $J: C[a,b]\to\mathbb{R}$ be determined by Riemann integral: $J(f)=\int_a^b f(x)\mathrm{d}x$. If $f\in C[a,b]$, then $J(f)$ can be regarded as a function of f, called a **functional on** $C[a,b]$.

We will come back to this concept (i. e. functional) in the Chapter 4.

2. Cardinal numbers of sets

"Element number of a set" shows "how many elements in the set". However, it is just suitable for those sets in which there are finite elements. Still, how to measure "element number" is an important problem in many natural science field.

Finite set　If a set contains finite elements

$$A=\{a_1,a_2,\cdots,a_n\},\quad n\in\mathbb{Z}^+,$$

where $n\in\mathbb{Z}^+$ is a determined, finite positive integer, then n is said to be the element **number of** A, and A is said to be a **finite set.**

Infinite set　If element number of A is not finite, i. e., A is not a finite set, then A is said to be an **infinite set.**

For example, $\{1,2,3,4\}$ and $\mathbb{Z}_2=\{0,1\}$ are finite sets; $\mathbb{Z}^+$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are infinite sets.

It is clear that "element number" is no meaning for infinite sets. The positive integer set $\mathbb{Z}^+=\{1,2,\cdots\}$ and even number set $\mathbb{O}=\{2,4,6,\cdots\}$ contain infinite elements, both are infinite set. So, the word "element number" does not make sense for them.

To show "how many (or how much) elements" for the infinite set, we introduce an important concept by motivated by the essential property of the finite set: if the numbers of two finite sets A and B equal each other, then the elements of A and B can be established a one-one relationship.

Definition 1.1.3 (equivalence)　If there exists a corresponding relationship $\varphi: A\to B$ between sets A and B, such that φ is an injection from A onto B, and also a surjection, i. e., φ is one-one mapping from A onto B with $B=\varphi(A)$, then A and B are said to be **equivalent**, or, A is **equivalent** to B, denoted by $A\sim B$; and φ is said to be **equivalent relation** between A onto B.

By this definition, **we have: two finite sets are equivalent, if and only if they have same numbers of elements.**

For infinite sets, we have different phenomenon: $\mathbb{Z}^+=\{1,2,\cdots\}$ and $\mathbb{O}=\{2,4,6,\cdots\}$ do not have same "element number", the "element number" of $\mathbb{O}$ is just a half of that of $\mathbb{Z}^+$, but they are equivalent (give the equivalence relationship $\varphi: \mathbb{Z}^+\to\mathbb{O}$ by readers, please). So does the rational number set $\mathbb{Q}$ with positive integer set $\mathbb{Z}^+$.

Definition 1.1.4 (cardinality) If two infinite sets A and B are equivalent, then they are said to have same **cardinality**. The cardinality ("card", for short) of A is denoted by $\bar{\bar{A}}$, or card $A=\bar{\bar{A}}$.

The number of elements of a finite set is also said to be its **cardinality.**

The cardinality of a set can be compared with that of its subsets.

Comparison of cardinalities For a proper subset $A \subset B$ of infinite set B, with $A \neq B$.

(1) If A is a finite set, then $\bar{\bar{A}}<\bar{\bar{B}}$;

(2) If A is an infinite set, and $A \sim B$, then $\bar{\bar{A}}=\bar{\bar{B}}$;

(3) If A is an infinite set, and A is not equivalent to B, then $\bar{\bar{A}}<\bar{\bar{B}}$, or say $\bar{\bar{B}}>\bar{\bar{A}}$.

For number sets, **we agree on**: the positive integer set $\mathbb{Z}^+$ has a minimum cardinality, denoted by $\aleph_0$. A set is said to be **countable** if its cardinality is $\aleph_0$. All sets which are equivalent to $\mathbb{Z}^+$ have the cardinality $\aleph_0$. Clearly, $\mathbb{Z}^+ \sim \mathbb{N} \sim \mathbb{Z} \sim \mathbb{Q}$, thus, we have

$$\text{card } \mathbb{Z}^+ = \text{card } \mathbb{N} = \text{card } \mathbb{Z} = \text{card } \mathbb{Q} = \aleph_0.$$

For interval $[0,1]$, it contains all rational and irrational numbers in $[0,1]$, in fact, there is no corresponding relation between $[0,1]$ and $\mathbb{Z}^+$ (see [6], [14]), **we agree on**: the cardinality of $[0,1]$ is $\aleph$. It holds $\aleph_0 < \aleph$. We have

$$\text{card}[a,b] = \text{card}[a,b) = \text{card}(a,b] = \text{card}(a,b) = \text{card } \mathbb{R} = \aleph.$$

1.2 Structures of Operations on Sets

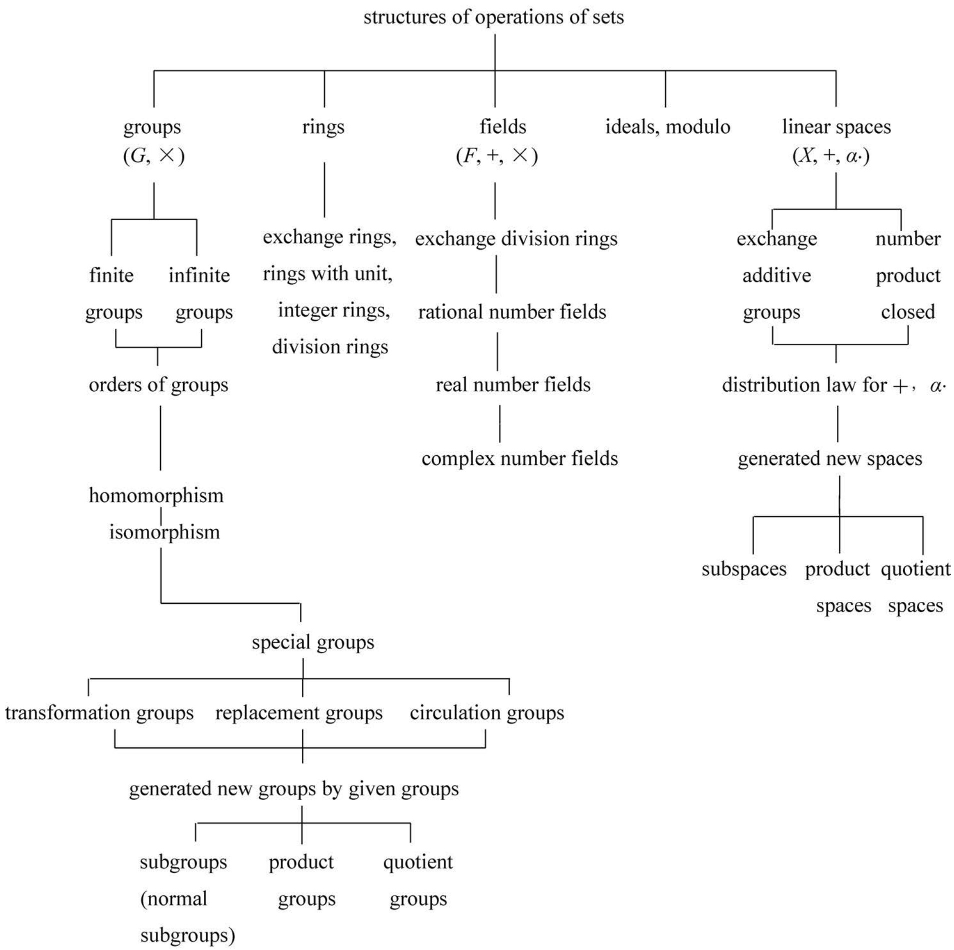
The position relations and the operation relations between two sets are discussed in the above section, whereas operations between elements in a set A are considered now, motivated by the familiar example $\mathbb{R}$, real number set, in which there are addition, subtraction, multiplication, division, … . What means "structure of operations of sets"? How to endow operations to a set? We discuss in this section, and introduce some quite new concepts compared with in Advanced Calculus, such as groups, rings, fields, ideals, modulo and linear spaces.

A set A endowed operations between its elements is said **to possess a structure of operations**, or **to have a structure of algebra**.

1.2.1 Groups, rings, fields, and linear spaces

1. Groups

We begin with the familiar real number set $\mathbb{R}$. For any $x, y \in \mathbb{R}$, sum $x+y$ can be



regarded as a result of "operation + of x and y". This operation + has the following familiar properties:

Closed property $x, y \in \mathbb{R} \Rightarrow x+y \in \mathbb{R}$;

Combination law $x, y, z \in \mathbb{R} \Rightarrow (x+y)+z = x+(y+z)$;

unit element there exists "unit" element $0 \in \mathbb{R}$, such that $\forall x \in \mathbb{R} \Rightarrow x+0=0+x=x$;

inverse element $\forall x \in \mathbb{R}$, there exists an inverse element $(-x) \in \mathbb{R}$, such that $x+(-x)=0$.

Then $\mathbb{R}$ is called **a group** under operation $+$.

Abstractly, we introduce the concept of the group.

Definition 1.2.1 (**group**) If there is an **operation** on a given set G, denoted by $\cdot$, satisfying

(1) $x, y \in G \Rightarrow x \cdot y \in G$; (closed property)

(2) $x, y, z \in G \Rightarrow (x \cdot y) \cdot z = x \cdot (y \cdot z)$; (combination law)

(3) there exists an element $1 \in G$, such that $\forall x \in G \Rightarrow 1 \cdot x = x \cdot 1 = x$; (exists unit)

(4) $\forall x \in G$, there exists an element $x^{-1} \in G$, such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$, (exists inverse)

then G is said to be a **group** with operation $\cdot$; and 1 is said to be the **unit** of G; moreover, $x^{-1} \in G$ is said to be the **inverse of** x.

Further, if the operation $\cdot$ satisfies

(5) $x, y \in G \Rightarrow x \cdot y = y \cdot x$, (commutation law)

then G is said to be **a commutative group**, with operation $\cdot$, or **Abelian group**;

A group G with its operation $\cdot$ is denoted by $(G, \cdot)$, or simply, by G.

If the operation $\cdot$ of a set G only satisfies (1), (2), then $(G, \cdot)$ is said to be a **semi-group**.

For the sake of simplicity, we agree on: the sign $\cdot$ in $x \cdot y$ can be omitted, turning into xy, if there is no confusion.

Note An operation $\cdot$ in definition 1.2.1 can be taken very widely, it may be an addition, a multiplication, a compound, or any others. For example, the real number set $\mathbb{R} = \{x: -\infty < x < +\infty\}$ is a commutative group with $+$, denoted by $(\mathbb{R}, +)$, the unit element is number 0.

Example 1.2.1 Denoted by $\mathbb{R}^+ = \{x \in \mathbb{R}: x > 0\}$, the **positive real number set**, take operation $\cdot$ as **the multiplication** $\times$ **of real numbers**. It is easy to verify that $\mathbb{R}^+$ is an commutative group with $\times$, denoted by $(\mathbb{R}^+, \times)$, and unit is the number 1. However, $\mathbb{R}$ with $\times$ is not a group (why?). Do you think $(\mathbb{R} \setminus \{0\}, \times)$ is a group with operation $\times$?

Example 1.2.2 Take the set

$$C([a,b]) = \{f: [a,b] \to \mathbb{R}, \quad f(x) \text{ is continuous on } [a,b]\},$$

define operation $\cdot$ as **the addition** $+$ **of functions**, i.e., $(f+g)(x) = f(x) + g(x)$, then the set $(C([a,b]), +)$ is called **the continuous function set**, it is an Abelian group.

Example 1.2.3 The set

$$L(\mathbb{R}, \mathbb{R}) = \{T: T(x) = ax + b, a, b \in \mathbb{R}, a \neq 0\}$$

is that of all linear mappings from $\mathbb{R}$ onto $\mathbb{R}$, where $T(x)$ is called **affine transformation**. Define operation $\cdot$ as **the compound** $\circ$ **of functions**, then the set $(L(\mathbb{R}, \mathbb{R}), \circ)$ is a group.

In fact, for $S, T \in L(\mathbb{R}, \mathbb{R})$, let $S(x) = ax + b$, $T(x) = cx + d$, $a \neq 0$, $c \neq 0$. Then

$$(T \circ S)(x) = T(S(x)) = c(S(x)) + d = c(ax + b) + d = (ca)x + (cb + d),$$

thus $T \circ S \in L(\mathbb{R}, \mathbb{R})$ by $a, c \neq 0$. This shows that the closed property (1) in Definition 1.2.1 holds.

It is clear that the combination law (2) holds.

For (3), the identity mapping $I: x \to x$ with $I(x) = x$, is the unit element with $a = 1$