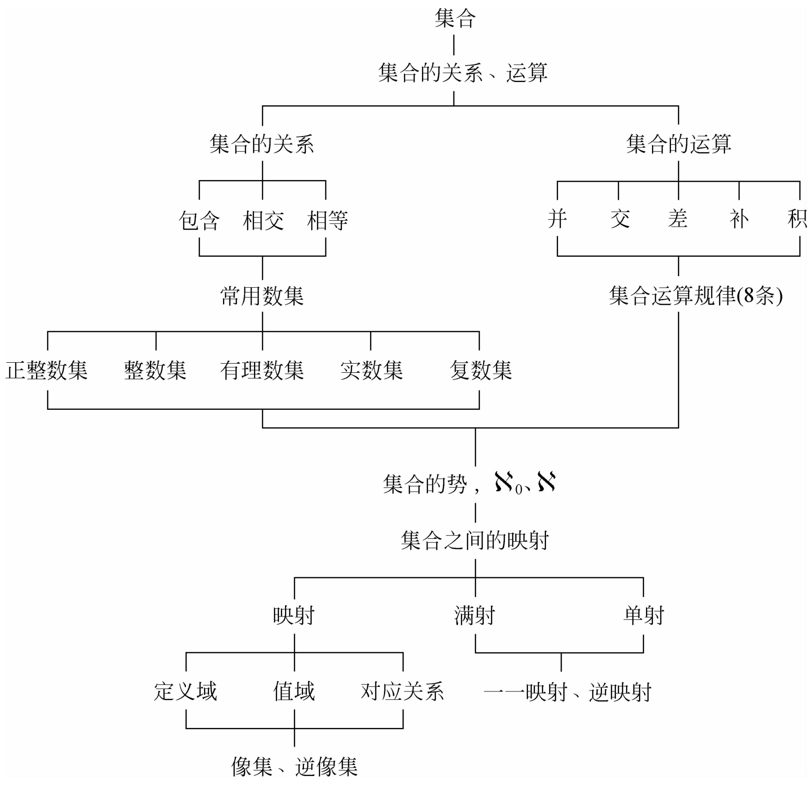
第1章 集合与集合的运算结构

集合论是近代数学的基础,我们从学习集合论的基本知识开始. 首先列出一张框图.



1.1 集合及其运算

集合论是 19 世纪后期由德国数学家 G. Cantor 创立的,经过一个多世纪,已经发展成为一个重要的数学分支; 同时,也已经渗透到数学科学的各个领域,有大量的学术论文与专

著可供参考. 这里仅介绍集合论的基本知识. 本章主要参考文献为[1],[2].

1.1.1 集合

一个重要的数学思维方法是:把研究对象按照一定的性质分成各种类型进行研究,分在同一类型中的对象具有共同的性质,因此不需一个一个地考虑,而是按类集中,这样更能使我们了解一类事物的本质. 例如,把全体有理数归为一类,称为**有理数集**,记为

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

其中$\mathbb{Z}=\{\cdots,-2,-1,0,1,2,\cdots\}$为整数的全体,$\mathbb{Z}^{+}=\{1,2,\cdots\}$为正整数的全体.

又如,在区间$[a,b]$上连续函数的全体,称为**$[a,b]$上的连续函数集**,记为

$$C([a,b])=\{f:[a,b] \rightarrow \mathbb{R}, f(x) \text{ 是}[a,b] \text{ 上的连续函数}\};$$

$[a,b]$上具有一阶连续导数的连续函数的全体,称为**$[a,b]$上一阶连续可导函数集**,记为

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

一般地,把**具有一定性质的对象的全体称为一个集合(set)**(也简称**集**). 集合通常用大写英文字母 $A,B,\cdots$或 $X,Y,\cdots$表示. 集中的对象称为**元素(element)**(也简称**元**),一般用小写英文字母 $a,b,\cdots$或 $x,y,\cdots$表示.

若 a 是 A 的元,便记为 $a\in A$; 若 a 不是 A 的元,记为 $a\notin A$.

集合是一个非常有用的概念,更是很有用的数学工具,因为无论自然科学还是社会科学、人文科学,所研究的都是具有一定性质的对象,引进集合来描述这些对象,更便于用数学思维方法处理问题.

1. 常用的数集

正整数集(positive number set) $\mathbb{Z}^{+}=\{x: x=1,2,3,\cdots\}$,

自然数集(natural number set) $\mathbb{N}=\{x: x=0,1,2,3,\cdots\}$,

整数集(integer set) $\mathbb{Z}=\{x: x=0,\pm 1,\pm 2,\cdots\}$,

有理数集(rational number set) $\mathbb{Q}=\left\{x: x=\frac{q}{p}, q\in \mathbb{Z}, p\in \mathbb{Z}^{+}\right\}$,

实数集(real number set) $\mathbb{R}=\{x: x \text{ 为实数}\}$,

复数集(complex number set) $\mathbb{C}=\{z: z=a+\mathrm{i}b, a, b\in \mathbb{R}\}, \mathrm{i}=\sqrt{-1}$.

2. 集合之间的关系

包含(include) 设 A 与 B 为两个集合. 若 A 中任一个元 $a\in A$ 同时也属于 B,即 $x\in B$,则称 A **含于** B,记为 $A\subseteq B$,或称 B **包含** A,记为 $B\supseteq A$,并称 A **为** B **的子集(subset)**.

若 A 含于 B,但 $A\neq B$,则称 A 为 B 的**真子集(proper subset)**,记为 $A\subset B$.

例如，$\mathbb{Z}^+ \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

相等(equal)　若 $A \subseteq B$，且 $B \subseteq A$，则称 A **与** B **相等**，记为 $A=B$.

例如，$\{x \in \mathbb{N}: x^2=1\}=\{1\} \subset \{x \in \mathbb{Z}: x^2=1\}=\{1,-1\}$.

1.1.2　集合的运算

1. 集合的并、交、差、补、积

空集(empty set)　不含任何元素的集合称为空集，记为$\varnothing$.

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

集合的并集(union set)　设 A 与 B 为两个集合. A 与 B 的并集(图 1.1.1(a))定义为一个集合，其中的元素或者属于 A，或者属于 B. 记为

$$A \cup B = \{x: x \in A \text{ 或 } x \in B\}.$$

集合的交集(intersection set)　设 A 与 B 为两个集合. A 与 B 的交集(图 1.1.1(b))定义为一个集合，其中的元素既属于 A，又属于 B. 记为

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

集合的差集(difference set)　设 A 与 B 为两个集合. A 与 B 的差集(图 1.1.1(c))定义为一个集合，其中的元素属于 A，但不属于 B. 记为

$$A \backslash B = \{x: x \in A \text{ 且 } x \notin B\}.$$

集合的补集(complementary set)　设 X 是基本集合，$A \subset X$ 为其子集. 称差集 $X \backslash A$ 为 A 关于基本集合 X 的补集(图 1.1.2(a)). 记为 $A^C = X \backslash A$，或 CA.

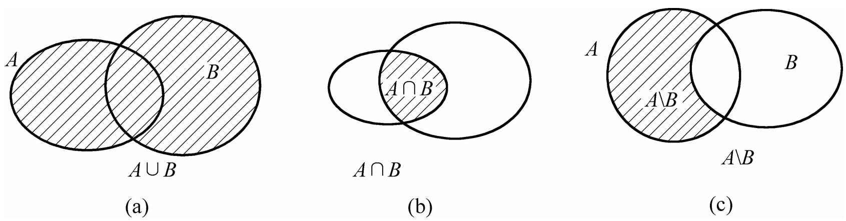


图 1.1.1　集合的并、交、差

集合的积集(product set)　设 A 与 B 为两个集合. A 与 B 的积集(图 1.1.2(b))定义为一个集合，记为

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

n 个集合的积集记为

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

无限多个集合的积集 $\prod\limits_{\lambda\in\Lambda}A_\lambda$，这里指标集 Λ 可以是可数集，如 $\prod\limits_{j\in\mathbb{N}}A_j$，也可以是任意集.

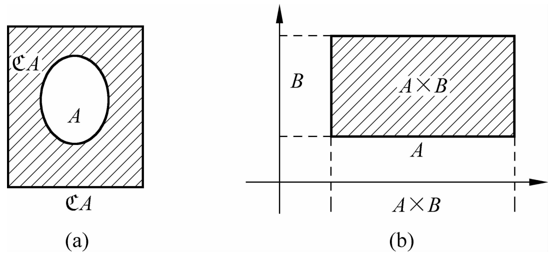


图 1.1.2　集合的补、积

2. 集合的运算律

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

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

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

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

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

(6) $\complement(\complement A)=A$，$\complement(A\cap B)=\complement A\cup\complement B$，$\complement(A\cup B)=\complement A\cap\complement B$.　　(对合律)

还可以考虑有限多个集合或无限多个集合的并集与交集：

$$\bigcup_{j\in\Lambda}A_j,\quad \bigcap_{j\in\Lambda}A_j,$$

这里指标集 Λ 可以是有限集或无限集，并且有以下性质：

(7) $A\cap\left(\bigcup\limits_{j\in\Lambda}A_j\right)=\bigcup\limits_{j\in\Lambda}(A\cap A_j)$，　$A\cup\left(\bigcap\limits_{j\in\Lambda}A_j\right)=\bigcap\limits_{j\in\Lambda}(A\cup A_j)$；

(8) $\complement\left(\bigcup\limits_{j\in\Lambda}A_j\right)=\bigcap\limits_{j\in\Lambda}\complement A_j$，　$\complement\left(\bigcap\limits_{j\in\Lambda}A_j\right)=\bigcup\limits_{j\in\Lambda}\complement A_j$.　　(de Morgan 公式)

1.1.3　集合之间的映射

函数是高等数学中的重要概念之一，高等数学中函数 f 的定义域 D_f 是实数集$\mathbb{R}$中的集合(一元函数)，或是$\mathbb{R}^n$中的集合(多元函数)；值域 R_f 总是在$\mathbb{R}$中. 然而，近代科学技术中所遇到的量的变化范围、量与量的关系远远超出了欧氏空间$\mathbb{R}$与$\mathbb{R}^n$. 因此，在集合上引进"对应关系"，以刻画变量之间的关系，也就是必然的了.

1. 映射

定义 1.1.1(对应关系)　设 X,Y 为两个集合(可以相同，也可不同). 对于给定的两个子集 $A\subseteq X,B\subseteq Y$，如果有一个**对应关系(corresponding relation)**，记为 $f:A\to B$，使得对每

一个 $x\in A$,有**惟一的**(**unique**)$y\in B$ 与之对应,记为 $y=f(x)$,则称 $f:A\to B$ 为 A 到 B 的**映射**(**mapping**),或**变换**(**transform**),或**算子**(**operator**). 称 A 为 f 的**定义域**(**domain**),记为 D_f;称 B 为 f 的**值域**(**range**),记为 R_f. 称 $f(A)=\{f(x):x\in A\}\subseteq B$ 为 f 的**像集**(**image set**),记为 $\mathrm{im}(f)=f(A)$;对子集 $C\subseteq B$,称集 $f^{-1}(C)=\{x\in A:f(x)\in C\}\subseteq A$ 为 f 的**逆像集**(**inverse image set**).

易见,$f(A)\subseteq B$ 有可能是 $f(A)=B$,也有可能是 $f(A)\subset B$,$f(A)\neq B$.

满射(**surjective**) 当 $f(A)=B$ 时,称 f 为 A 到 B 的满射. 亦即,对每个 $y\in B$,至少存在一个 $x\in A$,满足 $f(x)=y\in Y$. 此时,f 的像集 $f(A)$ 充满整个 B,即 $\mathrm{im}(f)=B$.

单射(**injective**) 若映射 $f:A\to B$ 是 A 到 B 的一一对应映射,即"$f(x_1)=f(x_2)$ 蕴含 $x_1=x_2$",就称映射 f 为单射,或称**一一**(**one to one**)**映射**.

注意,一一映射 $f:A\to B$ 未必是满射.

逆映射(**inverse**) 对于一一映射(单射)$f:A\to B$,定义其**逆映射** $f^{-1}:B\to A$ 为满足"$f(x)=y$ 蕴含 $f^{-1}(y)=x$"的映射 f^{-1}.(请读者区分逆映射 $f^{-1}:B\to A$ 与逆像集 $f^{-1}(B)\subset X$.)

例 1.1.1 设 $A=\{a,b,c\}$,$B=\{1,2,3,4\}$. 映射 $f:A\to B$ 满足

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

则 f 是 A 到 B 的一一映射,但不是满射.

例 1.1.2 取 $A=B=\mathbb{Z}=\{0,\pm1,\pm2,\pm3,\cdots\}$,映射 $f:A\to B$ 满足

$$f(n)=n+1,$$

则 f 是$\mathbb{Z}$到$\mathbb{Z}$的一一映射,并且是满射.

定义 1.1.2(**映射的复合**) 设 A,B,C 是三个给定的集合,映射 $f:A\to B$,$g:B\to C$,则由映射 f 与 g 确定的、$x\in A$ 到 $z\in C$ 的、满足

$$z=h(x)=g(f(x))$$

的映射 $h:A\to C$,称为**映射 f 与 g 的复合**(**compound**),记为 $h=g\circ f$.

注意,在考虑映射的复合时,像集 $f(A)$必须包含在映射 $g:B\to C$ 的定义域 B 中,但未必一定等于 B.

例 1.1.3 设 $A=C[a,b]$. 令 $J:C[a,b]\to\mathbb{R}$ 是由下面的积分确定的映射:

$$J(f)=\int_a^b f(x)\mathrm{d}x,$$

这里 $J(f)$为 f 的黎曼积分. 当 $f\in C[a,b]$时,$J(f)$视为 f 的函数,称 $J(f)$为集合 $C[a,b]$上的一个泛函. 下一节引入空间概念后,对于泛函还要给出更确切的定义.

2. 集合的势

"集合中元素个数"表示集合中元素的多少. 在自然科学问题的研究中,集合所含元素

的个数往往反映集合的许多方面的性质,因此非常重要. 但是,“多少”这个概念,对于“有限多个”而言才是有意义的,对于“无限多个”,就失去了意义.

有限集(finite set) 若集合 A 中含有限多个元素,即

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

这里 $n\in\mathbb{Z}^+$ 是一个确定的、有限的正整数,则称 n 是 A 的**个数**,并称 A 为**有限集**.

无限集(infinite set) 若 A 的个数不是有限的,即 A 不是有限集,则称 A 为**无限集**,也称**无穷集**.

例如,$\{1,2,3,4\}$,$\mathbb{Z}_2=\{0,1\}$都是有限集,而$\mathbb{Z}^+$,$\mathbb{N}$,$\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$都是无限集.

显然,对无限集谈“个数”是没有实际意义的. 例如,自然数集$\mathbb{N}=\{0,1,2,\cdots\}$与偶数集$\mathbb{O}=\{2,4,6,\cdots\}$都含有无限多个元素,都是无限集,看似自然数集中的元比偶数集的元多出一倍,但偶数也是非常非常多的,因此说哪个集合中的元素更多,没有实际意义.

为了比较两个无限集元素的“多少”,我们注意到两个相等的有限集 A 与 B 有一个重要的**特征性质**,那就是,两者的元素之间可以建立一一对应关系. 正是这种特征性质的启发,使得我们用下面的方法来研究无限集中含元素的多少.

定义 1.1.3(对等) 若集合 A 与 B 之间存在对应关系 $\varphi:A\to B$,使得 φ 是 A 到 B 的单射,同时也是满射,亦即,φ 是 A 到 B 上的一一映射,且 $B=\varphi(A)$,则称集合 A 与 B **对等(equivalence)**,记为 $A\sim B$,称 φ 为 A 到 B 上的**对等关系(equivalence relation)**.

根据定义,**两个有限集是对等的,当且仅当它们的个数相等.**

但是,无限集就完全不同了.

正整数集$\mathbb{Z}^+=\{1,2,\cdots\}$与偶数集$\mathbb{O}=\{2,4,6,\cdots\}$中元素相比较,正整数要比偶数多一倍,但是,它们却是对等的(请读者给出对等关系 φ). 又如,有理数集$\mathbb{Q}$与正整数集$\mathbb{Z}^+$,都含有无限多个元素,而有理数集中所含的元素,要比正整数集中的元素多得多,但$\mathbb{Q}$与$\mathbb{Z}^+$也是对等的(请读者给出对等关系 φ).

定义 1.1.4(无限集的势) 若两个无限集合 A 与 B 是对等的,则称它们具有相同的**势(cardinal number)**,集合 A 的势记为 $\overline{\overline{A}}$. 故对等集 A 与 B 满足 $\overline{\overline{A}}=\overline{\overline{B}}$.

有限集的个数、无限集的势,统称为集合的**基数(cardinality)**,记为 $\mathrm{card}(A)=\overline{\overline{A}}$.

无限集与它的子集的势,是可以比较大小的.

势的比较 对于无限集 B 的一个真子集 $A\subset B$,$A\neq B$,有

(1) 若 A 为有限集,则 $\overline{\overline{A}}<\overline{\overline{B}}$;

(2) 若 A 为无限集,且 $A\sim B$,则 A 的势等于 B 的势,即 $\overline{\overline{A}}=\overline{\overline{B}}$;

(3) 若 A 为无限集,且 A 与 B 不对等,则 A 的势小于 B 的势,$\overline{\overline{A}}<\overline{\overline{B}}$;或说 B 的势大于 A 的势,记为 $\overline{\overline{B}}>\overline{\overline{A}}$.

在数的集合中，正整数集$\mathbb{Z}^+$是最小的无限集，称它的势为$\aleph_0$，读作**阿列夫零**. 势为$\aleph_0$的集称为**可数集**. 凡与$\mathbb{Z}^+$对等的无限集的势，都是$\aleph_0$. 显然，$\mathbb{Z}^+\sim\mathbb{N}\sim\mathbb{Z}\sim\mathbb{Q}$，因此$\mathbb{N}$，$\mathbb{Z}$与$\mathbb{Q}$的势都是$\aleph_0$.

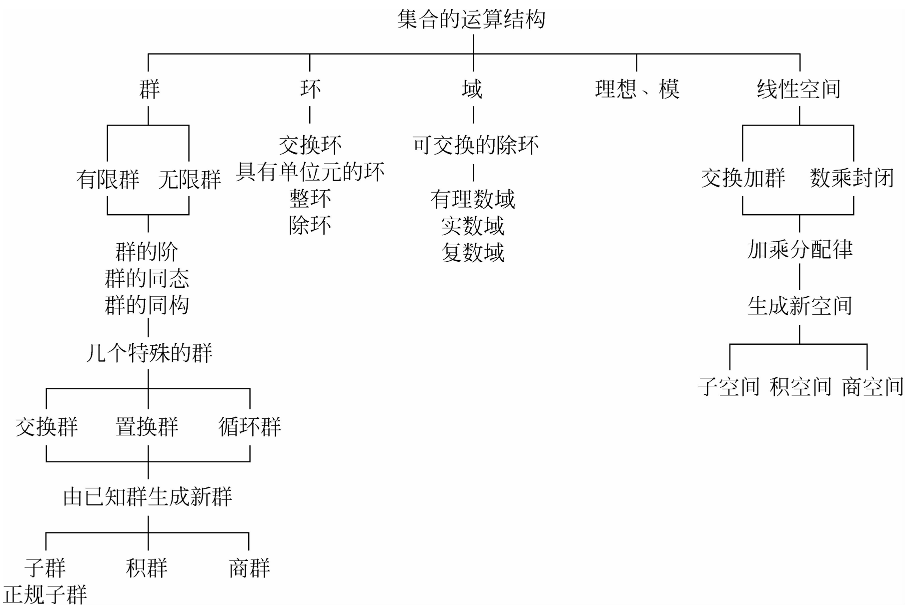
$[0,1]$中含有无限多个数，包括有理数与无理数，它不可能与$\mathbb{Z}^+$建立一一对应（这在实变函数教程中有详细证明，参考[6]、[14]），称$[0,1]$的势为$\aleph$，读作**阿列夫**. 于是，$\aleph_0<\aleph$.

具有势$\aleph$的数集有$[a,b]$，$[a,b)$，$(a,b]$，(a,b)，$\mathbb{R}$等.

1.2　集合的运算结构

考虑集合中元素间的关系，有两个重要方面，一是元素之间的运算关系，如元素之间的加法、乘法等；二是元素间的位置关系，如两个元素间的距离，即远近的程度. 当然还有其他方面的关系，读者会在以后的学习或研究中遇到.

本节介绍集合中元素的一些运算关系，赋予代数运算的集合称其具有**运算结构**，也常称其具有代数结构. 本节内容见下图示意.



1.2.1　群、环、域、线性空间

1. 群

先从大家熟悉的实数集$\mathbb{R}$开始. 对于$x,y\in\mathbb{R}$，和式$x+y$可看作运算$+$的结果. 这种运算有以下熟知的性质：

封闭性 $x,y\in\mathbb{R}\Rightarrow x+y\in\mathbb{R}$；

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

单位元 存在单位元 $0\in\mathbb{R}$，使得 $\forall x\in\mathbb{R}\Rightarrow x+0=0+x=x$；

逆元 $\forall x\in\mathbb{R}$，存在逆元 $(-x)\in\mathbb{R}\Rightarrow x+(-x)=0$.

这时，称 $\mathbb{R}$ 在运算 $+$ 之下构成一个群.

把这个定义抽象化，得到群的概念.

定义 1.2.1（群） 如果在一个集合 G 上定义一个运算，记为 $\cdot$，满足

(1) $x,y\in G\Rightarrow x\cdot y\in G$； （封闭性）

(2) $x,y,z\in G\Rightarrow(x\cdot y)\cdot z=x\cdot(y\cdot z)$； （结合律）

(3) 存在单位元 $1\in G$，使得 $\forall x\in G\Rightarrow 1\cdot x=x\cdot 1=x$； （单位元）

(4) $\forall x\in G$，存在逆元 $x^{-1}\in G\Rightarrow x\cdot x^{-1}=x^{-1}\cdot x=1$， （逆元）

则称 G 在运算 $\cdot$ 之下构成一个**群**（**group**），1 称为群的**单位元**（**unit**）. 如果运算 $\cdot$ 还满足

(5) $x,y\in G\Rightarrow x\cdot y=y\cdot x$， （交换律）

则称 G 在运算 $\cdot$ 之下构成一个**交换群**（**exchange group**），也称为 **Abel 群**.

群 G 与其运算 $\cdot$，常记为 $(G,\cdot)$，或简记为 G.

若集合 G 上的运算 $\cdot$ 仅满足定义 1.2.1 中的(1)、(2)，则称 $(G,\cdot)$ 为一个**半群**（**semi-group**）.

定义 1.2.1 中定义的运算 $\cdot$ 的意义是很广泛的，可取作实数的加法、乘法，也可取作函数的复合等. 实数集 $\mathbb{R}=\{x:-\infty<x<+\infty\}$ 在数的加法 $+$ 之下构成一个交换群 $(\mathbb{R},+)$，其单位元就是数 0. 今后，在不发生混淆时，省去运算符号 $\cdot$.

例 1.2.1 记

$$\mathbb{R}^+=\{x\in\mathbb{R}:x>0\}$$

为**正实数集合**，把运算 $\cdot$ 取作数的乘法 $\times$. 不难验证，$\mathbb{R}^+$ 在运算 $\times$ 之下成为一个交换群 $(\mathbb{R}^+,\times)$（请读者自行验证），它的单位元是 1. 也请读者考虑，$(\mathbb{R},\times)$ 是否能构成一个群？$(\mathbb{R}\setminus\{0\},\times)$ 是否能构成一个群？

例 1.2.2 取

$$C([a,b])=\{f:[a,b]\to\mathbb{R},f(x)\text{ 是}[a,b]\text{ 上的连续函数}\}.$$

把运算 $\cdot$ 取作函数的加法 $+$，即 $(f+g)(x)=f(x)+g(x)$，则 $(C([a,b]),+)$ 构成一个可交换的加群.

例 1.2.3 设

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

为 $\mathbb{R}$ 到 $\mathbb{R}$ 的线性映射的全体，$T(x)$ 称为**仿射变换**（**affine transformation**）. 把运算 $\cdot$ 取作函数的复合 $\circ$，则

$$(L(\mathbb{R},\mathbb{R}),\circ)$$

构成一个群.

事实上，对于 $S,T\in L(\mathbb{R},\mathbb{R})$，令

$$S(x)=ax+b,\quad T(x)=cx+d,\quad a\neq 0,c\neq 0.$$

则

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

因 $a,c\neq 0$，故 $T\circ S\in L(\mathbb{R},\mathbb{R})$，此即定义 1.2.1 中的封闭性(1).

定义 1.2.1 中的结合律(2)显然成立.

对于定义 1.2.1 中的(3)，单位元为恒同映射 $I:x\to x, I(x)=x$，亦即 $a=1,b=0$.

对于定义 1.2.1 中的(4)，$\forall S(x)=ax+b\in L(\mathbb{R},\mathbb{R}), a\neq 0$，其逆元 S^{-1} 为

$$S^{-1}(x)=\frac{x}{a}-\frac{b}{a}\in L(\mathbb{R},\mathbb{R}).$$

故 $L(\mathbb{R},\mathbb{R})$ 是一个群，但一般不满足定义 1.2.1 中的(5)，故它不是交换群.

例 1.2.4 $(\mathbb{R},+),(\mathbb{Q},+),(\mathbb{Z},+)$ 都是加群，这里加法运算 $+$ 就是实数的加法，它们都是加法交换群.

例 1.2.5 (1) $(\mathbb{R}\setminus\{0\},\times),(\mathbb{R}^+,\times)$ 都是乘法交换群，这里乘法运算 $\times$ 就是实数的乘法.

(2) 正整数乘法半群 $(\mathbb{Z}^+,\times)$.

(3) 正整数的 p 倍半群 $(\mathbb{Z}_p^+,\times)=(\{np:n\in\mathbb{Z}^+\},\times)$.

(4) p-adic 有限群 $(\{0,1,\cdots,p-1\},\oplus)$，$p\geqslant 2$ 为正整数，这里 $\oplus$ 是模 p 运算，$x\oplus y=x+y(\mathrm{mod}p)$.

(5) Cayley 有限群 $G=(\{1,\mathrm{i},-1,-\mathrm{i}\},\otimes)$，其中运算 $\otimes$ 由下面的 Cayley 表给出：

$\otimes$	1	i	−1	−i
1	1	i	−1	−i
i	i	−1	−i	1
−1	−1	−i	1	i
−i	−i	1	i	−1

(6) 非异 n 阶复方阵群(复完全线性群)

$$(GL(n,\mathbb{C}),\times)=(\{A=[\alpha_{jk}]_{n\times n}:\alpha_{jk}\in\mathbb{C},\det A\neq 0\},\times),$$

其中 $\times$ 为方阵乘法，$\det A$ 是方阵 A 的行列式；

非异 n 阶实方阵群(实完全线性群)

$$(GL(n,\mathbb{R}),\times)=(\{A=[\alpha_{jk}]_{n\times n}:\alpha_{jk}\in\mathbb{R},\det A\neq 0\},\times);$$

当 $n\geqslant 2$ 时，它们都是非交换群. 且 $(GL(n,\mathbb{R}),\times)\subset(GL(n,\mathbb{C}),\times)$.

(7) 行列式为 1 的非异 n 阶复方阵群

$$(SL(n,\mathbb{C}),\times)=(\{A\in GL(n,\mathbb{C}):\det A=1\},\times);$$

行列式为1的非异 n 阶实方阵群

$$(SL(n,\mathbb{R}),\times)=(\{A\in GL(n,\mathbb{R}):\det A=1\},\times),$$

当 $n\geqslant 2$ 时，它们都是非交换群. 且 $(SL(n,\mathbb{R}),\times)\subset(SL(n,\mathbb{C}),\times)$.

(8) 正方形 $ABCD$ 绕其中心点将自身映射到自身的旋转群

$$R=\left\{\alpha:\alpha=0,\frac{1}{2}\pi,\pi,\frac{3}{2}\pi\right\},$$

其中 α 为旋转角，运算 $\circ$ 定义为：$\alpha_1\circ\alpha_2$ 表示先旋转 α_2，再旋转 α_1，则 $(R,\circ)$ 构成旋转群.

(9) 单位圆根群

$$\Omega_p=\left\{\exp\left(\frac{\mathrm{i}2k\pi}{p}\right):k=0,1,\cdots,p-1\right\},$$

运算定义为复数乘法 $\times$，$p\geqslant 2$ 为正整数，则 $(\Omega_p,\times)$ 构成单位圆根群.

例 1.2.6(子群) 给定群 $(G,\cdot)$ 的子集 $H\subset G$，若在 G 的运算 $\cdot$ 之下，H 也成为一个群，则称 H 为 G 的子群.

例如，$GL(n,\mathbb{R})$ 是 $GL(n,\mathbb{C})$ 的子群，$SL(n,\mathbb{R})$ 是 $SL(n,\mathbb{C})$ 的子群.

2. 环、域

定义 1.2.2(环、域) 若在集合 R 上定义两个运算，分别记为加法 $+$ 与乘法 $\times$.

1) **环** —— 若 R 上的运算满足

(1) R 关于加法 $+$ 构成一个交换群，其加法单位元记为 0，称为 R 的**零元**；

(2) R 关于乘法 $\times$ 构成一个半群，即满足封闭性与结合律，

$$x,y\in R\Rightarrow x\times y\in R;\qquad x,y,z\in R\Rightarrow(x\times y)\times z=x\times(y\times z);$$

(3) R 关于加法 $+$ 与乘法 $\times$ 满足加乘分配律，即

$$x,y,z\in R\Rightarrow x\times(y+z)=x\times y+x\times z,\quad (y+z)\times x=y\times x+z\times x;$$

则称 R 在运算 $+$ 与 $\times$ 之下构成一个**环(ring)**，记为 $(R,+,\times)$.

2) **交换环** —— 若环 $(R,+,\times)$ 还满足

(4) R 关于乘法 $\times$ 满足交换律，即

$$x,y\in R\Rightarrow x\times y=y\times x,$$

则称 $(R,+,\times)$ 为一个**交换环(exchange ring)**，亦即交换环满足(1)～(4).

3) **具有单位元的环** —— 若环 $(R,+,\times)$ 还满足

(5) R 对乘法 $\times$ 存在单位元，记为 1，即

$$\forall x\in R\Rightarrow 1\times x=x\times 1=x,$$

则称 $(R,+,\times)$ 为一个**具有单位元的环(ring with unit)**，亦即具有单位元的环满足(1)～(3)、(5).

注意，一个有单位元的环 $(R,+,\times)$ 中，每个元未必有关于乘法的逆元，例如整数环 $(\mathbb{Z},+,\times)$ 中，只有 $+1$ 与 -1 关于乘法有逆元，其余整数关于乘法都没有逆元.