游戏开发工程师数学基础

木头骨头石头

2025 年 9 月 27 日

目录

Chapter 1

集合论简介

1.1 朴素集合论

集合（Set）是由一些事物汇集一起组成的整体，这些事物称为集合的**元素（Element）**。集合通常用大写英文字母表示，集合中的元素用小写字母表示。不含任何元素的集合称为空集，记为 $\varnothing$。集合有如下三个特性：

1. **无序性**：集合中每个元素的地位是相同的，元素之间是无序的。当然，我们可以在集合上定义偏序关系之后，元素之间可以依次排序。但就集合本身，元素之间是没有必然的序的。
2. **互异性**：集合中的元素是互不相同的，每个元素只出现一次。
3. **确定性**：给定一个集合 A，任何一个对象要么属于集合 A，要么不属于集合 A，二者必居其一，不允许有模棱两可的情况出现。

公理 1.1.1 (概括公理模式 Axiom Schema of Comprehension)**.** *假设任意属性 $P(x)$，存在一个集合 A，使得对于任意对象 x，$x \in A$ 当且仅当 $P(x)$ 为真。集合 A 记为 $\{x|P(x)\}$ 或 $\{x : P(A)\}$。*

> 注解
>
> 公理（Axiom）是一条命题。公理模式（Axiom Schema）中的谓词 P 是可变的，公理模式实际上包含无穷多条公理。选择具体的一个谓词，就得到一条命题。

概括公理模式是朴素集合论中构造集合的基本方法，换句话说，存在一个包含万事万物的集合，任选一条属性，都能从中筛选元素建构新的集合。概括公理模式限制太少，所以蕴含一个经典的悖论——**罗素悖论（Russell's Paradox）**，若存在一个集合 R，它是由“所有不包括自身的集合”所组成，也即

$$R = \{x : x \notin x, \text{x is a set}\}$$

那么，R 是否包含自身呢？如果 $R \in R$，那么根据 R 的定义，$R \notin R$；反之，如果 $R \notin R$，那么根据 R 的定义，$R \in R$。无论哪种情况，都会导致矛盾。消解罗素悖论需要提出新的公理。**ZFC 公理系统**是通过限制概括公理模式来规避罗素悖论。在 **NBG 公理系统**中，引入比集合更高阶的“类（Class）”，从而避免讨论“包含所有集合的集合”，而是“包含所有集合的类”。下面主要介绍 ZFC 公理系统。

1.2 ZFC 公理集合论

为了消解罗素悖论，需要限制概括公理模式。为此，数理学家 Zermelo 和 Fraenkel 提出了一套公理定义集合，称为 **ZF 公理集合论（ZF Axiomatic Set Theory）**，在 ZF 公理集合论的基础上加上**选择公理（Axiom of Choice）**就是 **ZFC 公理集合论**。ZFC 公理集合论一共有九条公理：

1. **外延公理 Axiom of extensionality**：设 A, B 是集合，说 A 和 B 是相等的，记作 $A = B$，当且仅当，两个集合有相同的元素。
2. **配对公理 Axiom of pairing**：对于任意集合（或元素）a, b，存在一个集合 $\{a, b\}$ 包含 a, b。
3. **分类公理模式 Axiom schema of specification**：设 A 是一个集合，并对于每个 $x \in A$，设 $P(x)$ 是一个关于 x 的性质。那么存在一个集合 $\{x \in A : P(x)\}$，它的元素是 A 中使 $P(x)$ 成立的所有 x。
4. **并集公理 Axiom of union**：对于集合 A，存在集合 $\cup A$。$\forall u \in \cup A$，存在集合 $B \in A$，使得 $u \in B$。
5. **幂集公理 Axiom of power set**：对于集合 A，存在集合 $\mathcal{P}(A)$ 是所有 A 的子集的集合，称为幂集。
6. **无穷公理 Axiom of infinity**：存在集合 A，使得$\varnothing \in A$，且任意对象 $a \in A$ 都有 $a \cup \{a\} \in A$。
7. **替代公理模式 Axiom schema of replacement**：设属性 $P(x, y)$，对于每个 x 唯一确定一个 y 使得 $P(x, y)$ 成立。则对于任意集合 A，存在集合 B，任意 $b \in B$，存在 $a \in A$ 使得 $P(a, b)$ 成立。
8. **正则公理 Axiom of regularity**：任意非空集合 A 包含一个元素 x，使得 $x \cap A = \varnothing$。
9. **选择公理 Axiom of choic**：任意由非空集合组成的集族 $\mathcal{F}$，存在一个选择函数 f，使得对每个 $A \in \mathcal{F}$，有 $f(A) \in A$。

1.2.1 外延公理

公理 1.2.1 (外延公理 Axiom of extensionality)**.** *设 A, B 是集合，说 A 和 B 是相等的，记作 $A = B$，当且仅当，两个集合有相同的元素。*

注解

外延公理说明一个集合完全由它的元素决定。通过外延公理，可以定义子集。

子集

定义 1.2.1 (子集 Subset)**.** *设 A, B 是集合，说 A 是 B 的子集，记作 $A \subseteq B$，当且仅当，A 的每个元素都是 B 中的元素。*

定理 1.2.1. *若两个集合互为对方的子集，两集合相等。也即，设 A, B 是集合，如果 $A \subseteq B$ 且 $B \subseteq A$，则 $A = B$。*

1.2.2 配对公理

公理 1.2.2 (配对公理 Axiom of pairing)**.** 对于任意集合（或元素） a, b，存在一个集合 $\{a, b\}$ 包含 a, b。

注解

外延公理和配对公理说明，集合中的元素都是独一无二的，且没有顺序，比如：

$$\{1, 2\} = \{2, 1\},\ \{1, 1\} = \{1\}$$

通过配对公理，可以定义有序对。

有序对

定义 1.2.2 (有序对 Ordered Pair)**.** 由两个元素 x 和 y 按一定顺序排列成的二元组称为一个有序对或序偶，记为：(x, y)，其中 x 是它的第一个元素，y 是第二个，那么

$$(x, y) := \{x, \{x, y\}\}$$

命题 1.2.1 (有序对的性质)**.** 设 x, y 是元素，(x, y) 是有序对，那么

1. 当 $x = y$ 时，$(x, y) = (y, x)$；当 $x \neq y$ 时，$(x, y) \neq (y, x)$
2. $(x, y) = (u, v)$ 当且仅当 $x = u,\ y = v$

定义 1.2.3 (有序数组 Ordered n-Tuple)**.** 由 n 个元素 $x_1, x_2, \cdots, x_n$ 按一定顺序排列成的 n 元组称为一个有序数组，记为：$(x_1, x_2, \cdots, x_n)$，其中 x_1 是它的第一个元素，x_2 是第二个，依此类推，那么

$$(x_1, x_2, \cdots, x_n) := ((x_1, x_2, \cdots, x_{n-1}), x_n)$$

命题 1.2.2. 两个 n 元有序数组 $(a_1, \cdots, a_n) = (b_1, \cdots, b_n)$ 相等，当且仅当，$a_1 = a_1, \cdots, a_n = b_n$

1.2.3 分类公理模式

公理 1.2.3 (分类公理模式 Axiom schema of specification)**.** 设 A 是一个集合，并对于每个 $x \in A$，设 $P(x)$ 是一个关于 x 的性质。那么存在一个集合 $\{x \in A : P(x)\}$，它的元素是 A 中使 $P(x)$ 成立的所有 x。

注解

分类公理模式是 ZFC 公理集合论中构造集合的方式，与朴素集合论的概括公理模式相比，它是从一个已知集合中挑选元素构造一个子集，而不是直接构造所有满足性质 P 的集合。因此通过分类公理模式可以定义空集、交集、差集、补集…… 但不能定义并集。并集需要从已知集合构造一个更大的，包含已知集合的集合，这需要并集公理。

空集

定义 1.2.4 (空集 Empty). 对于任意集合 A，集合：

$$\{x \in A : x \neq x\}$$

称为空集，记为 $\varnothing$

> 注解
>
> 因为满足性质 $x \neq x$ 的元素并不存在，所以 $\varnothing$ 中不包含任何元素。根据定义，空集是任意集合的子集。

交集

定义 1.2.5 (交集 Intersection). 两个集合 A 和 B 的交是一个集合，记为 $A \cap B$，那么

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

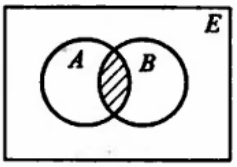


图 1.1: 交集

定义 1.2.6 (分离 Disjoint). 两个集合 A 和 B 是分离的，当且仅当：$A \cap B = \varnothing$

差集

定义 1.2.7 (差集 Difference). 两个集合 A 和 B 的差是一个集合，记为 $A - B$ 或 $A \setminus B$，那么

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

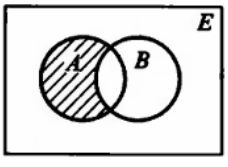


图 1.2: 差集

补集

定义 1.2.8 (补集). 设集合 E 和 A，$A \subseteq E$，A 的补集记为 $\complement_E A$，那么

$$\complement_E A := E \setminus A = \{x \in E : x \notin A\}$$

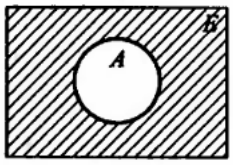


图 1.3: 补集

1.2.4 并集公理

定义 1.2.9 (并集 Union). 两个集合 A 和 B 的并是一个集合，记为 $A \cup B$，那么

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

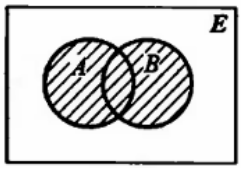


图 1.4: 并集

定义 1.2.10 (对称差 Symmetric Difference). 两个集合 A 和 B 的对称差是一个集合，记为 $A \oplus B$，那么：

$$A \oplus B := (A - B) \cup (B - A)$$

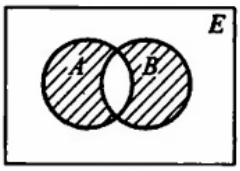


图 1.5: 并集

定理 1.2.2 (集合常用算律). 设 A, B, C 是集合

1. 幂等律： $A \cup A = A,\ A \cap A = A$
2. 结合律：$A \cup (B \cup C) = (A \cup B) \cup C,\ A \cap (B \cap C) = (A \cap B) \cap C$
3. 交换律：$A \cup B = B \cup A,\ A \cap B = B \cap A$
4. 分配律：$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

5. 排中律：$A \cup \complement_E A = E$
6. 矛盾律：$A \cap \complement_E A = \varnothing$
7. 德摩根律：
   (a) $A - (B \cup C) = (A - B) \cap (A - C)$
   (b) $A - (B \cap C) = (A - B) \cup (A - C)$
   (c) $\complement_E(B \cup C) = \complement_E B \cap \complement_E C$
   (d) $\complement_E(B \cap C) = \complement_E B \cup \complement_E C$
8. 双重否定率：$\complement_E(\complement_E A) = A$

1.2.5 幂集公理

公理 1.2.4 (幂集公理 Axiom of power set)**.** *对于集合 A，存在集合 $\mathcal{P}(A)$ 是所有 A 的子集的集合，称为幂集。*

注解

换句话说，集合 A 的幂集是 A 全体子集构成的集合。通过幂集公理，同样可以从已知集合构造更大的集合。有序对的定义：

$$(a, b) := \{a, \{a, b\}\}$$

如果 $a \in A, b \in B$，那么：

$$(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$$

通过并集公理和幂集公理，构造集合 $\mathcal{P}(\mathcal{P}(A \cup B))$，通过分离公理模式，分离出有序对的集合，从而可以定义两个集合的**笛卡尔积**。

笛卡尔积

定义 1.2.11 (笛卡尔积 Cartesian Product)**.** *设 A, B 为集合，A, B 的笛卡尔积记为 $A \times B$，那么*

$$A \times B := \{(x, y) \in \mathcal{P}(\mathcal{P}(A \cup B)) : x \in A, y \in B\}$$

递归地，可以定义 n 个集合 $S_1, S_2, \cdots, S_n$ 的笛卡尔积，记为 $\prod_{i=1}^{n} S_i$，那么

$$(x_1, x_2, \cdots, x_n) \in \prod_{i=1}^{n} S_i$$

特别地，当 $S_i = S$ 时，$\prod_{i=1}^{n} S_i$ 记为 S^n。

注解

笛卡尔积是构造有序对集合的基本方法。有了有序对的集合，再通过分离公理模式，从中分离出我们感兴趣的有序对，从而构建起集合元素之间的关系，比如，等价关系、偏序关系、函数关系等。集合+关系构成现代数学的基础。布尔巴基学派认为，现代数学的理论大多是集合与某种关系的组合的研究，比如，代数结构（群、环、域等）是集合与代数运算关系的组合，序结构（偏序集、全序集等）是集合与序关系的组合，拓扑结构（拓扑空间、度量空间等）是集合与邻近关系的组合。

命题 1.2.3 (笛卡尔积的性质). 设 A, B, C 为集合，

1. 笛卡尔积不满足结合律
   (a) $(A \times B) \times C \neq A \times (B \times C)$
2. 笛卡尔积通常不满足交换律
   (a) $A \times B \neq B \times A$
3. 笛卡尔积对集合交并满足分配律
   (a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
   (b) $(B \cup C) \times A = (B \times A) \cup (C \times A)$
   (c) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
   (d) $(B \cap C) \times A = (B \times A) \cap (C \times A)$

1.2.6 无穷公理

公理 1.2.5 (无穷公理 Axiom of Infinity). 存在集合 A，使得 $\varnothing \in A$，且任意对象 $a \in A$ 都有 $a \cup \{a\} \in A$

> 注解
>
> 无穷公理断言了无穷集的存在，但这种“无穷”并不是像朴素集合论那样不加限制的无穷，而是对后继（successor）操作 $a \cup \{a\}$ 封闭的无穷，也即 $\forall a \in A$ 都存在其后继 $a \cup \{a\} \in A$。满足这一性质的集合，也称为**归纳集（Inductive Set）**。自然数的递归定义依赖于无穷公理。数学归纳法的有效性依赖于自然数集的无限性。若没有无穷公理，归纳法只能应用于有限步骤。

自然数

定义 1.2.12 (自然数 Natural numbers). 通过无穷公理，我们可以无限递归地定义每一个自然数：

1. 令 $0 := \varnothing$
2. 任意自然数 n 的后继 $S(n)$，那么 $S(n) := n \cup \{n\}$

无穷公理说明，集合 $n \cup \{n\}$ 的存在，记所有自然数的集合记为 $\mathbb{N}$。

定义 1.2.13 (自然数的序). 设 $\forall m, n \in \mathbb{N}$ 是自然数，我们说 n 大于等于 m，记作 $n \geq m$ 或 $m \leq n$，当且仅当 $m \subseteq n$。

注解

根据自然数的定义，

$$
\begin{aligned}
0 &= \{\} = \varnothing \\
1 &= 0 \cup \{0\} = \{0\} = \{\varnothing\} \\
2 &= 1 \cup \{1\} = \{0,1\} = \{\varnothing, \{\varnothing\}\} \\
3 &= 2 \cup \{2\} = \{0,1,2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \\
&\vdots
\end{aligned}
$$

1.2.7 替代公理模式

公理 1.2.6 (替代公理模式 Axiom Schema of Replacement). 设属性 $P(x,y)$，对于每个 x 唯一确定一个 y 使得 $P(x,y)$ 成立。则对于任意集合 A，存在集合 B，任意 $b \in B$，存在 $a \in A$ 使得 $P(a,b)$ 成立。

注解

属性 $P(x,y)$ 类似于“函数”（因为函数是通过集合公理定义的，所以在集合公理中避免谈及“函数”），也即 x 对应唯一的 y。通过替代公理模式，可以将已知集合 A 中的元素 x 替换为 y 生成一个新的集合 B。通过替代公理模式，可以递归地定义自然数的加法与乘法。

自然数的加法与乘法

定义 1.2.14 (自然数的加法). 设 m 是自然数，

1. $m + 0 := m$
2. 任意自然数 n 的后继为 $S(n)$，$m + S(n) := S(m+n)$

注解

替代公理模式断言了属性，$P(m,0) = m + 0$ 和 $P(m,n) = m + S(n)$ 的存在，再根据无穷公理，可以递归的定义任意自然数 m 与 n 的加法：

$$
\begin{aligned}
m + 0 &= m \\
m + 1 &= m + S(0) = S(m+0) = S(m) \\
m + 2 &= m + S(1) = S(m+1) = S(S(m+0)) = S(S(m)) \\
m + 3 &= m + S(2) = S(m+2) = S(S(S(m+0))) = S(S(S(m))) \\
&\vdots
\end{aligned}
$$

定义 1.2.15 (自然数的乘法). 设 m 是自然数，

1. $m \times 0 := 0$
2. 任意自然数 n 的后继为 $S(n)$， $m \times S(n) := m \times n + m$

注解

替代公理模式断言了属性，$P(m,0) = m \times 0$ 和 $P(m,n) = m \times S(n)$ 的存在，再根据无穷公理，可以递归的定义任意自然数 m 与 n 的乘法：

$$
\begin{aligned}
&m \times 0 = 0 \\
&m \times 1 = m \times S(0) = m \times 0 + m = m \\
&m \times 2 = m \times S(1) = m \times 1 + m = m \times 0 + m + m = m + m \\
&m \times 3 = m \times S(2) = m \times 2 + m = m \times 0 + m + m + m = m + m + m \\
&\quad \vdots
\end{aligned}
$$

命题 1.2.4 (自然数的性质). 设任意 $a, b, c \in \mathbb{N}$ 是自然数，有：

1. 加法交换律：$a + b = b + a$
2. 加法结合律：$(a + b) + c = a + (b + c)$
3. 乘法交换律：$a \times b = b \times a$
4. 乘法结合律：$(a \times b) \times c = a \times (b \times c)$
5. 乘法对加法的分配律：$a \times (b + c) = a \times b + a \times c$
6. 加法单位元：0
7. 乘法的零元：0
8. 乘法的单位元：1

1.2.8 正则公理

公理 1.2.7 (正则公理 Axiom of Regularity). 任意非空集合 A 包含一个元素 x，使得 $x \cap A = \varnothing$。

注解

换句话说，如果 A 是一个非空集合，其中至少包含一个元素 x，它要么不是集合，要么是与 A 完全不同的集合。正则公理也称为**基础公理（Foundation Axiom）**，它断言了不存在以自身为元素的集合，从而避免罗素悖论。

1.2.9 选择公理

定义 1.2.16 (集族 Family of Sets)**.** 以集合为元素的集合称为集族。集族常用大写的花体字母 $\mathcal{A}, \mathcal{B}, \mathcal{C}$ 表示。比如，集合 A 的幂集 $\mathcal{P}(A)$；集合 A 的拓扑 $\mathcal{T}(A)$。集合 A 的 σ 代数 $\mathcal{M}(A)$

公理 1.2.8 (选择公理 Axiom of Choice)**.** 任意由非空集合组成的集族 $\mathcal{F}$，存在一个选择函数 f，使得对每个 $A \in \mathcal{F}$，有 $f(A) \in A$

注解

选择公理说明，无论集合族的结构如何复杂，总能为每个集合选出一个代表元素。选择公理仅断言选择函数存在，但不提供具体构造方法。这与构造主义数学的哲学相冲突，但被经典数学广泛接受。

Chapter 2

关系与结构

任意两事物之间存在某种关系（Relation），比如数之间的大小关系、相等关系，相似关系、正交关系、共线关系等。这些关系可以用关系谓词来叙述，比如 a 大于 b、点 A 与点 B 共线、整数 x 整除整数 y 等。在没有定义元素之间的关系前，集合只是一堆元素的“堆砌”，我们只能讨论集合与集合的包含关系，集合与元素的从属关系。当定义了元素之间的关系时，集合就会表现出某些性质，就称这个集合具备了某种结构（Structure）。

受结构主义（Structuralism）思潮的影响，在二十世纪初，布尔巴基学派（Bourbaki）的数学家主张在集合论的基础上，通过元素之间的关系定义数学对象。集合限定了讨论对象的范围；关系是集合的笛卡尔积，通过分类公理模式筛选出来的子集；集合与关系一起构成了数学对象的结构。布尔巴基学派提出三种基本数学结构：

1. 代数结构 Algebraic Structure：群、环、域、向量空间等，研究运算与代数性质，作为代数学的基础
2. 序结构 Order Structure：偏序集、全序集等，研究元素之间的顺序关系，作为分析学的基础
3. 拓扑结构 Topological Structure：拓扑空间、度量空间等，研究元素之间的邻近关系，作为几何学的基础

布尔巴基学派认为，现代数学的理论大多是这些结构或其组合的研究，比如，如拓扑群、赋范向量空间、序拓扑等。布尔巴基学派深刻的影响了 20 世纪的数学以及数学教育的发展，现代主流的数学教材大多遵循布尔巴基学派的思想编写。

布尔巴基学派活跃于 20 世纪上半叶。到了二十世纪下半叶，范畴论（Category Theory）继承与发展了结构主义思想，提出一种更为抽象和统一的视角来研究数学对象及其关系。结构主义是在集合公理的基础上，利用关系定义数学对象。而在范畴论中，数学对象被视为范畴中的对象（Objects），对象之间的关系被视为态射（Morphisms）。范畴论强调对象之间的关系和变换，而不是对象本身的内部结构。

2.1 二元关系

2.1.1 二元关系的定义

定义 2.1.1 (关系 Relation)**.** 设 $X_1, X_2, \cdots, X_n$ 为集合，存在属性 P，使得有序数组 $(x_1, x_2, \cdots, x_n)$ 满足该属性，则称 P 为 $X_1, X_2, \cdots, X_n$ 上的一个 n 元关系（*n-ary Relation*），记为 R，那么

$$R = \{(x_1, x_2, \cdots, x_n) \in \prod_{i=1}^{n} X_i : P(x_1, x_2, \cdots, x_n)\}$$

特别的，当 $n = 2$，称为**二元关系（*Binary Relation*）**。若 $(a, b) \in R$，记为 aRb。二元关系 R 中所有有序对的第一个元素构成的集合称为 R 的**定义域（*Domain*）**，记为 $\mathrm{dom}R$；二元关系 R 中所有有序对的第二个元素构成的集合称为 R 的**值域（*Range*）**，记为 $\mathrm{ran}R$。

定义 2.1.2 (二元关系的逆 Inverse)**.** 设 R 为集合 X, Y 上的二元关系，则 R 的**逆（*Inverse*）**，记为 R^{-1}，定义为

$$R^{-1} = \{(y, x) \in Y \times X : (x, y) \in R\}$$

定义 2.1.3 (二元关系的复合 Composition)**.** 设 R 为集合 X, Y 上的二元关系，S 为集合 Y, Z 上的二元关系，则 R, S 的**复合（*Composition*）**，记为 $S \circ R$，定义为

$$S \circ R = \{(x, z) \in X \times Z : \exists y \in Y[(x, y) \in R \wedge (y, z) \in S]\}$$

定义 2.1.4 (恒等关系 Identity Relation)**.** 设 X 为集合，则 X 上的**恒等关系（*Identity Relation*）**，记为 I_X，定义为

$$I_X = \{(x, x) : x \in X\}$$

命题 2.1.1. 设 R, S, T 为适当集合上的二元关系，则有

1. $(R^{-1})^{-1} = R$
2. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$
3. $T \circ (S \circ R) = (T \circ S) \circ R$
4. $F \circ (S \cup R) = (F \circ S) \cup (F \circ R)$
5. $(S \cup R) \circ F = (S \circ F) \cup (R \circ F)$
6. $F \circ (S \cap R) \subseteq (F \circ S) \cap (F \circ R)$
7. $(S \cap R) \circ F \subseteq (S \circ F) \cap (R \circ F)$

2.1.2 关系矩阵与关系图

定义 2.1.5 (关系矩阵). 设 R 为有限集 X,Y 上的二元关系，则 R 的**关系矩阵（*Relation Matrix*）**记为 M_R，其中每一个分量定义为：

$$m_{i,j} = \begin{cases} 1, & if\,(x_i, y_j) \in R \\ 0, & if\,(x_i, y_j) \notin R \end{cases}$$

其中 $X = \{x_1, x_2, \ldots, x_n\}$，$Y = \{y_1, y_2, \ldots, y_m\}$。

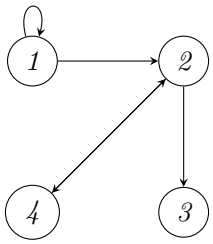
例 2.1.1. 设一个二元关系 $R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 2,4\rangle, \langle 4,2\rangle\}$，其关系矩阵为

$$M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

定义 2.1.6 (关系图). 设 R 为有限集 X,Y 上的二元关系，则 R 的**关系图（*Relation Graph*）**为一个有向图 $G_R = (V, E)$，其中

- 顶点集 $V = X$；
- 边集 $E = \{(x_i, x_j) : (x_i, x_j) \in R\}$。

例 2.1.2. 在例 *2.1.1* 中，关系 R 的关系图为：



2.1.3 自反性与反自反性

定义 2.1.7. 设 R 为集合 X 上的二元关系，

1. 自反性 *Reflexivity*：若对任意 $x \in X$，$(x,x) \in R$，则称 R 具有自反性。
2. 反自反性 *Irreflexivity*：若对任意 $x \in X$，$(x,x) \notin R$，则称 R 具有反自反性。

命题 2.1.2. 设 R 为集合 X 上的二元关系，则有

1. R 是自反的，当且仅当，$I_X \subseteq R$
2. R 是反自反的，当且仅当，$I_X \cap R = \varnothing$

注解

如果 X 是有穷集合，通过关系矩阵或关系图可以更直观的判断该二元关系是否具有自反性或反自反性：

1. 关系矩阵：自反性对应矩阵的主对角线全为 1；反自反性对应矩阵的主对角线全为 0
2. 关系图：自反性对应每个节点都有一个指向自身的环；反自反性对应没有节点有指向自身的环

自反性说明该集合中任意一个元素与其自身的都有关系，比如实数集上的等于关系，自然数集上的整除关系等；反之，如果如果集合中任意一个元素与其自身没有关系，那么这种二元关系具有反自反性，比如实数集上的大于关系。不具有自反关系的二元关系不一定是反自反的，比如一个二元关系：a 与 a 的乘积是偶数，这个二元关系在偶数集上是自反的、在奇数集上是反自反的、在自然数集上既不是自反的，也不是反自反的。

2.1.4 对称性与反对称性

定义 2.1.8. 设 R 为集合 X 上的二元关系，

1. 对称性 *Symmetry*：任意 $x, y \in X$，如果 $(x, y) \in R$ 那么 $(y, x) \in R$，则称 R 具有对称性。
2. 反对称性 *Antisymmetry*：任意 $x, y \in X$ 如果 $(x, y) \in R$ 且 $(y, x) \in R$ 那么 $x = y$，则称 R 具有反对称性。

命题 2.1.3. 设 R 为集合 X 上的二元关系，则有

1. R 是对称的，当且仅当，$R = R^{-1}$
2. R 是反对称的，当且仅当，$R \cap R^{-1} \subseteq I_X$

注解

如果 X 是有穷集合，通过关系矩阵或关系图可以更直观的判断该二元关系是否具有对称性或反对称性：

1. 关系矩阵：对称性对应矩阵关于主对角线对称；反对称性对应矩阵关于主对角线对称的位置上不同时为 1
2. 关系图：对称性对应每一条有向边 (x, y) 都有一条与之反向的边 (y, x)；反对称性对应没有两个不同的节点之间有相互指向的边

对称性说明二元关系与其逆关系是同一个集合，比如实数集上的相等关系是对称的；整数集上模 n 同余是对称的；一个二元关系：a 和 b 在 C 公司是同事也是对称的。另一方面，整数集上的整除关系是反对称的，实数集上的大于等于关系也是反对称的。对称关系和反对称关系并不是互斥的，比如集合 A 上的恒等关系既是对称的，也是反对称的。

2.1.5 传递性

定义 2.1.9. 设 R 为集合 X 上的二元关系，若对任意 $x, y, z \in X$，如果 $(x, y) \in R$ 且 $(y, z) \in R$ 那么 $(x, z) \in R$，则称 R 具有**传递性（*Transitivity*）**。

命题 2.1.4. 设 R 为集合 X 上的二元关系，则有 R 是传递的，当且仅当，$R \circ R \subseteq R$

注解

如果 X 是有穷集合，通过关系矩阵或关系图可以更直观的判断该二元关系是否具有传递性：

1. 关系矩阵：传递性对应矩阵的平方中非零元素对应的位置在原矩阵中也为非零
2. 关系图：传递性对应如果存在从节点 x 到节点 y 的路径，且存在从节点 y 到节点 z 的路径，那么必然存在从节点 x 到节点 z 的路径

实数集上的小于等于关系；整数集上的整除关系；集合的包含关系都具有传递性。集合 A 上的全域，恒等关系也是传递关系。

2.2 函数

定义 2.2.1 (函数 Function)**.** 设 X, Y 为集合，f 为 X, Y 上的二元关系，f 称为 X 到 Y 的一个**函数（*Function*）**，当且仅当，f 满足：

1. 唯一性：$\forall x \in \mathrm{dom} f$，如果 $(x, y_1) \in f$ 且 $(x, y_2) \in f$，则 $y_1 = y_2$

记作 $f : X \to Y$，记 xfy 为 $y = f(x)$。定义域 $\mathrm{dom} f$ 也称为函数的原像（*Preimage*），值域 $\mathrm{ran} f$ 也称为函数的像（*Image*），也常记为 $\mathrm{im} f$ 或 $f(X)$。

注解

函数是一种特殊的二元关系，其唯一性说明，若对任意 $x \in X$，在 f 中存在唯一的 $y \in Y$，使得 $(x, y) \in f$。不存在一个 $x \in X$，对应多个 $y \in Y$ 的情况。函数的复合的复合也即二元关系的复合。函数的逆不一定是函数，因为可能存在 $y \in Y$，对应多个 $x \in X$ 的情况，不满足唯一性。

定义 2.2.2. 设 $f : X \to Y$ 为函数，若

1. **满射（*Surjection*）**：如果 $\mathrm{ran} f = Y$，则称 f 为满射。
2. **单射（*Injection*）**：如果 $\forall y \in \mathrm{ran} f$，$(x_1, y) \in f$ 且 $(x_2, y) \in f$，$x_1 = x_2$，则称 f 为单射。
3. **双射（*Bijection*）**：如果 f 同时为单射与满射，则称 f 为双射。

2.2.1 集合的势

对于一个有穷集合，我们可以用一个自然数表示集合的大小，并根据自然数的大小比较集合的大小。这是对集合“大小”非常朴素的认识，并没有严格定义，而且推广到无穷集时，这一方法就失效了。为了使无穷集之间也能比“大小”，通过函数定义集合的势（Cardinality）。

定义 2.2.3 (集合的势 Cardinality)**.** 设 X, Y 为集合，

1. X 与 Y **等势**，当且仅当，存在 X 到 Y 的双射，记为 $|X| = |Y|$；
2. Y **优势于** X，当且仅当，存在 X 到 Y 的单射，记为 $|X| \leq |Y|$；
3. Y **严格优势于** X，当且仅当，存在 X 到 Y 的单射，但不存在 X 到 Y 的双射，记为 $|Y| < |X|$。

命题 2.2.1. 等势具有自反性、对称性和传递性：

1. 自反性：对于任意集合 X，有 $|X| = |X|$。
2. 对称性：如果 $|X| = |Y|$，则 $|Y| = |X|$。
3. 传递性：如果 $|X| = |Y|$ 且 $|Y| = |Z|$，则 $|X| = |Z|$。

命题 2.2.2. 优势关系具有自反性、反对称性和传递性：

1. 自反性：对于任意集合 X，有 $|X| \leq |X|$。
2. 反对称性：如果 $|X| \leq |Y|$ 且 $|Y| \leq |X|$，则 $|X| = |Y|$。
3. 传递性：如果 $|X| \leq |Y|$ 且 $|Y| \leq |Z|$，则 $|X| \leq |Z|$。

定义 2.2.4 (有限集与无限集). 设 X 为集合，

1. 如果 X 与某个自然数 n 等势，则称 X 为**有限集（*Finite Set*）**，记为 $|X| = n$；
2. 如果 X 为空集，则称 X 为**空集（*Empty Set*）**，记为 $|X| = 0$；
3. 如果 X 既不是空集也不是有限集，则称 X 为**无限集（*Infinite Set*）**。
4. 如果 X 与自然数集 $\mathbb{N}$ 等势，则称 X 为**可数无限集（*Countably Infinite Set*）**

例 2.2.1. 对于常见的数集，$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ 都是可数无限集，$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$，因为可以找到双射函数

1. 设 $f : \mathbb{N} \to \mathbb{Z}$，将 $\mathbb{Z}$ 中的整数按如下方式排列：

$$0, 1, -1, 2, -2, 3, -3, \cdots$$

   这样就可以定义双射 $f(n)$ 为上述排列中第 n 个整数

2. 设 $g : \mathbb{N} \to \mathbb{Q}$，将 $\mathbb{Q}$ 中的有理数按如下方式排列：

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, \frac{1}{3}, -\frac{1}{3}, \frac{2}{3}, -\frac{2}{3}, 3, -3, \cdots$$

   这样就可以定义双射 $g(n)$ 为上述排列中第 n 个有理数

实数集 $\mathbb{R}$ 是不可数无限集，$|\mathbb{R}| > |\mathbb{N}|$，可以通过 *Cantor* 对角线论证法证明。

2.3 等价关系

定义 2.3.1 (等价关系 Equivalence Relation)**.** 设 X 为非空集合，$R \subseteq X \times X$ 是 X 上的二元关系。称 R 为 X 上的等价关系，当且仅当，对任意 $x, y, z \in X$，R 满足：

1. 自反性 *Reflexivity*：$(x, x) \in R$
2. 对称性 *Symmetry*：若 $(x, y) \in R$，则 $(y, x) \in R$
3. 传递性 *Transitivity*：若 $(x, y) \in R$ 且 $(y, z) \in R$，则 $(x, z) \in R$

对于任意 $x, y \in X$，若 $(x, y) \in R$，则称 x 与 y 关于关系 R 等价，记为 $x \sim y$。可以根据等价关系，将集合划分为若干个互不相交的子集，每个子集称为一个等价类。

注解

等价关系是一种特殊的二元关系，需要满足自反性、对称性和传递性。

例 2.3.1. 定义在有限集 $X = \{1, 2, \cdots, 8\}$ 上的关系 R：

$$R = \{(x, y) : x, y \in X \wedge x \equiv y (\mathrm{mod}\ 3)\}$$

$x \equiv y (\mathrm{mod}\ 3)$ 称为 x, y 模 3 相等，不难验证该关系是自反的、对称的和传递的。其中 1、4、7 模 3 等于 1；2、5、8 模 3 等于 2；3、6 模 3 等于 0

定义 2.3.2 (等价类 Equivalence Class)**.** 设 R 为集合 X 上的等价关系。对于任意 $x \in X$，定义 x 的等价类为

$$[x]_R = \{y \in X : (x, y) \in R\}$$

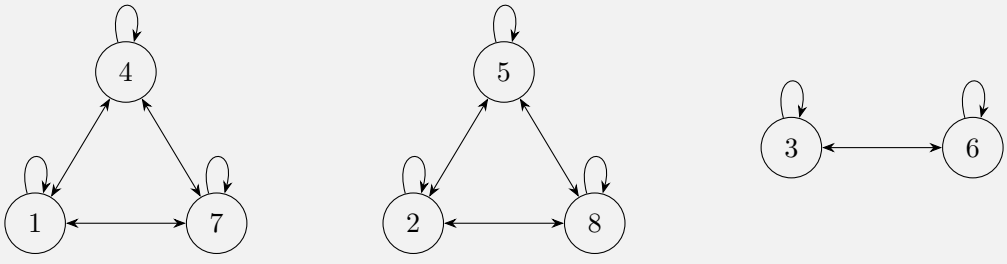
或简记为

$$[x] = \{y \in X : y \sim x\}$$

称 $[x]$ 为包含元素 x 的等价类。

注解

x 的等价类是A中所有与 x 等价的元素构成的集合。在例 2.3.1 中，1 的等价类为 $[1] = \{1, 4, 7\}$；2 的等价类为 $[2] = \{2, 5, 8\}$；3 的等价类为 $[3] = \{3, 6\}$。这三个等价类，互相没有交集，用关系图表示为：



定义 2.3.3 (商集 Quotient Set)**.** 设 R 为集合 X 上的等价关系。X 关于 R 的商集定义为

$$X/R = \{[x] : x \in X\}$$

称 X/R 为集合 X 关于等价关系 R 的商集。

注解

在例 2.3.1 中，商集为

$$X/R = \{[1], [2], [3]\} = \{\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6\}\}$$

2.3.1 划分

定义 2.3.4 (划分 Partition)**.** 设 X 为非空集合，$\mathcal{P}$ 是 X 的幂集。子集族 $\mathcal{S} \subseteq \mathcal{P}$ 称为 X 的一个划分，当且仅当，$\mathcal{S}$ 满足：

1. 非空性 *Non-emptiness*：对任意 $\varnothing \notin \mathcal{S}$
2. 覆盖性 *Coverage*：$\bigcup_{A \in \mathcal{S}} A = X$
3. 互斥性 *Mutual Exclusion*：对任意 $A, B \in \mathcal{S}$，若 $A \neq B$，则 $A \cap B = \varnothing$

注解

划分中，每一个元素是都是一个非空子集，这些子集是互不相交的，且它们的并集为整个集合。商集是根据等价关系得到的对集合的划分，不同的等价关系会得到不同的划分。

2.4 代数结构

定义 2.4.1 (代数运算 Algebraic Operation)**.** 设 X 为集合，$n \in \mathbb{N}^+$，函数 $f : X^n \to X$ 称为 X 上的 n 元运算，当且仅当，f 满足：

1. 封闭性：$\mathrm{dom} f = X^n$

特别地，当 $n = 1$ 时，称 f 为一元运算；当 $n = 2$ 时，称 f 为二元运算。二元运算常用符号 $*, \circ, \cdot$ 等表示，$f(x, y)$ 简记为 $x * y$。

定义 2.4.2 (代数结构 Algebraic Structure)**.** 设 X 为集合，O 为 X 上的运算集，则二元组 (X, O) 称为代数结构。

定义 2.4.3 (子代数 Subalgebra)**.** 设 (X, O) 为代数结构，$Y \subseteq X$。二元组 (Y, O) 称为代数结构 (X, O) 的子代数，当且仅当，对于任意 n 元运算 $f \in O$，满足封闭性 $\mathrm{dom} f = Y^n$。

> 注解
>
> 代数运算要求函数满足封闭性，也即集合中任意 n 个元素经过运算后仍然属于该集合。代数结构是集合与运算的结合体，在某些代数结构中存在特殊元素，比如单位元、零元，它们属于该代数系统的性质，称为代数常数。集合、运算和代数常数是构成一个代数结构的三要素，它们的性质是代数学研究的主要对象。子代数会从原始结构中继承相关的运算性质，且含有相同的代数常数，因此具有相同的代数结构。

2.4.1 代数常数

定义 2.4.4 (单位元 Identity Element)**.** 设 $(X, *)$ 为代数结构。如果存在 $e_l \in X$，当对任意 $x \in X$，均有

$$e_l * x = x$$

时，称 e_l 为 $(X, *)$ 的左单位元。如果存在 $e_r \in X$，当对任意 $x \in X$，均有

$$x * e_r = x$$

时，称 e_r 为 $(X, *)$ 的右单位元。如果 $e_l = e_r$，则称 e_l（或 e_r）为 $(X, *)$ 的单位元，记为 e。

定义 2.4.5 (零元 Zero Element)**.** 设 $(X, *)$ 为代数结构。如果存在 $z_l \in X$，当对任意 $x \in X$，均有

$$z_l * x = z_l$$

时，称 z_l 为 $(X, *)$ 的左零元。如果存在 $z_r \in X$，当对任意 $x \in X$，均有

$$x * z_r = z_r$$

时，称 z_r 为 $(X, *)$ 的右零元。如果 $z_l = z_r$，则称 z_l（或 z_r）为 $(X, *)$ 的零元，记为 z。

定义 2.4.6 (逆元 Inverse Element). 设 $(X,*)$ 为代数结构，e 为 $(X,*)$ 的单位元。如果对任意 $x\in X$，均存在 $y\in X$，使得

$$x*y=e$$

则称 y 为 x 关于运算 $*$ 的右逆元，记为 x_r^{-1}。如果对任意 $x\in X$，均存在 $y\in X$，使得

$$y*x=e$$

则称 y 为 x 关于运算 $*$ 的左逆元，记为 x_l^{-1}。如果对任意 $x\in X$，均存在 $y\in X$，使得

$$x*y=y*x=e$$

则称 y 为 x 关于运算 $*$ 的逆元，记为 x^{-1}。

定义 2.4.7 (反元 Additive Inverse). 设 $(X,+)$ 为代数结构，z 为 $(X,+)$ 的零元。如果对任意 $x\in X$，均存在 $y\in X$，使得

$$x+y=z$$

则称 y 为 x 关于加法的反元，记为 $-x$。

2.4.2 代数算律

定义 2.4.8 (交换律 Commutative Law). 设 $(X,*)$ 为代数结构。如果对任意 $x,y\in X$，均有

$$x*y=y*x$$

则称运算 $*$ 满足交换律。

定义 2.4.9 (结合律 Associative Law). 设 $(X,*)$ 为代数结构。如果对任意 $x,y,z\in X$，均有

$$(x*y)*z=x*(y*z)$$

则称运算 $*$ 满足结合律。

定义 2.4.10 (分配律 Distributive Law). 设 $(X,+,\cdot)$ 为代数结构。如果对任意 $x,y,z\in X$，均有

$$x\cdot(y+z)=x\cdot y+x\cdot z$$

则称运算 $\cdot$ 对运算 $+$ 满足左分配律；如果对任意 $x,y,z\in X$，均有

$$(y+z)\cdot x=y\cdot x+z\cdot x$$

则称运算 $\cdot$ 对运算 $+$ 满足右分配律；如果运算 $\cdot$ 对运算 $+$ 同时满足左、右分配律，则称运算 $\cdot$ 对运算 $+$ 满足分配律。

定义 2.4.11 (消去律 Cancellation Law). 设 $(X,*)$ 为代数结构。如果对任意 $a,b,c\in X$，$a\neq z$ 不是零元。当 $a*b=a*c$ 时，必有 $b=c$，则称运算 $*$ 满足左消去律；如果对任意 $a,b,c\in X$，当 $b*a=c*a$ 时，必有 $b=c$，则称运算 $*$ 满足右消去律；如果运算 $*$ 同时满足左、右消去律，则称运算 $*$ 满足消去律。

2.4.3 同态与同构

定义 2.4.12 (同态 Homomorphism). 设 $(X,*)$ 和 $(Y,\circ)$ 为代数结构。如果映射 $f:X\to Y$ 满足对任意 $x_1,x_2\in X$，均有

$$f(x_1*x_2)=f(x_1)\circ f(x_2)$$

则称映射 f 为从代数结构 $(X,*)$ 到代数结构 $(Y,\circ)$ 的同态。另外，

1. 如果 f 是单射，则称 f 为**单同态 *Monomorphism***;
2. 如果 f 是满射，则称 f 为**满同态 *Epimorphism***;
3. 如果 f 是双射，则称 f 为**同构 *Isomorphism***。

注解

同态映射反应了两个同类型代数结构的“相似性”，它可以将一个代数结构里的运算与另一个同类型代数结构的对应运算相关联。如果是同构映射，那么这两个代数结构是等价的，比如，三维空间中全体有向箭头与三维实向量集合同构，那么三维空间中有向箭头的相加和缩放可以归结为三维实向量的相加和数乘，这是解析几何的重要基础。

2.4.4 群

定义 2.4.13 (半群 Semigroup). 设 $(G,*)$ 为代数结构。如果运算 $*$ 满足结合律，则称 $(G,*)$ 为半群。也即，$(G,*)$ 是半群，当且仅当，二元运算 $*$ 满足：

1. 封闭性：对任意 $a,b\in G$，有 $a*b\in G$;
2. 结合律：对任意 $a,b,c\in G$，有 $(a*b)*c=a*(b*c)$。

定义 2.4.14 (幺半群 Monoid). 设 $(M,*)$ 为半群。如果存在单位元，则称 $(M,*)$ 为幺半群。也即，$(M,*)$ 是幺半群，当且仅当，二元运算 $*$ 满足：

1. 封闭性：对任意 $a,b\in M$，有 $a*b\in M$;
2. 结合律：对任意 $a,b,c\in M$，有 $(a*b)*c=a*(b*c)$;
3. 存在单位元：存在 $e\in M$，使得对任意 $a\in M$，有 $e*a=a*e=a$。

定义 2.4.15 (群 Group). 设 $(G,*)$ 为幺半群。如果每个元素均有逆元，则称 $(G,*)$ 为群。也即，$(G,*)$ 是群，当且仅当，二元运算 $*$ 满足：

1. 封闭性：对任意 $a,b\in G$，有 $a*b\in G$;
2. 结合律：对任意 $a,b,c\in G$，有 $(a*b)*c=a*(b*c)$;
3. 存在单位元：存在 $e\in G$，使得对任意 $a\in G$，有 $e*a=a*e=a$;
4. 存在逆元：对任意 $a\in G$，存在 $b\in G$，使得 $a*b=b*a=e$。

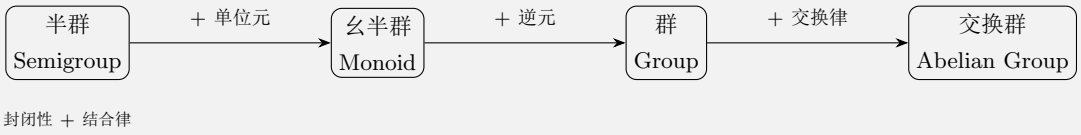
只含有单位元的群称为**平凡群 *Trivial Group***，记为 $\{e\}$；反之，含有除单位元外其他元素的群称为**非平凡群 *Non-Trivial Group***。

定义 2.4.16 (阿贝尔群 Abelian Group)**.** 设 $(G,*)$ 为群。如果运算 $*$ 满足交换律，则称 $(G,*)$ 为阿贝尔群或交换群。也即，$(G,*)$ 是交换群，当且仅当，二元运算 $*$ 满足：

1. 封闭性：对任意 $a,b\in G$，有 $a*b\in G$；
2. 结合律：对任意 $a,b,c\in G$，有 $(a*b)*c=a*(b*c)$；
3. 存在单位元：存在 $e\in G$，使得对任意 $a\in G$，有 $e*a=a*e=a$；
4. 存在逆元：对任意 $a\in G$，存在 $b\in G$，使得 $a*b=b*a=e$；
5. 交换律：对任意 $a,b\in G$，有 $a*b=b*a$。

注解

用一幅图展示各种群之间的关系：



例 2.4.1. 正整数集上定义普通加法的代数结构 $(\mathbb{Z}^+,+)$ 是半群；自然数集上定义普通加法的代数结构 $(\mathbb{N},+)$ 是幺半群；整数集上定义普通加法的代数结构 $(\mathbb{Z},+)$ 是群（交换群），称为整数加群。

2.4.5 环与域

定义 2.4.17 (环 Ring)**.** 设 $(R,+,\cdot)$ 为代数结构。如果

1. $(R,+)$ 是交换群；
2. $(R,\cdot)$ 是半群；
3. 乘法对加法满足分配律；

则称 $(R,+,\cdot)$ 为环。群 $(R,+)$ 中的单位元记为 0，称为加法零元。如果环只有一个元素，则称为***零环 Zero Ring***，记为 $\{0\}$；反之，含有两个及以上元素的环称为***非零环 Non-Zero Ring***。

定义 2.4.18 (无零因子环 Ring without Zero Divisors)**.** 设 $(R,+,\cdot)$ 为环。如果对任意 $a,b\in R$，$a\neq 0$，$b\neq 0$，均有 $a\cdot b\neq 0$，则称环 $(R,+,\cdot)$ 为无零因子环。

定义 2.4.19 (含幺环 Ring with identity)**.** 设 $(R,+,\cdot)$ 为环。如果存在乘法单位元，则称环 $(R,+,\cdot)$ 为含幺环。也即 $(R,\cdot)$ 是幺半群，$(R,+,\cdot)$ 为含幺环。其中，乘法单位元记为 e 或 1，且 $e\neq 0$。

定义 2.4.20 (整环 Integral Domain)**.** 设 $(R,+,\cdot)$ 为含幺环。如果 $(R,+,\cdot)$ 是无零因子环，则称 $(R,+,\cdot)$ 为整环。

定义 2.4.21 (交换环 Commutative Ring)**.** 设 $(R,+,\cdot)$ 为环。如果乘法 $\cdot$ 满足交换律，则称 $(R,+,\cdot)$ 为交换环。

定义 2.4.22 (除环 Division Ring)**.** 设 $(R,+,\cdot)$ 为含幺环。如果对任意 $a\in R$，$a\neq 0$，均存在 $a^{-1}\in R$，使得 $a\cdot a^{-1}=a^{-1}\cdot a=e$，则称 $(R,+,\cdot)$ 为除环。也即 $(R-\{0\},\cdot)$ 是群，$(R,+,\cdot)$ 为含幺环。

例 2.4.2. 常见的环有：整数环 $(\mathbb{Z},+,\cdot)$ 是含幺交换环和整环，但不是除环，因为除法不封闭；多项式环 $(P[x],+,\cdot)$ 是含幺交换环和整环，但不是除环，因为除法不封闭；矩阵环 $(M_n(\mathbb{R}),+,\cdot)$ 是含幺环，但不是交换环，因为矩阵乘法不满足交换律，也不是整环，因为存在零因子（非零矩阵相乘可能得零矩阵），但它是除环当且仅当 $n=1$；四元数环 $(\mathbb{H},+,\cdot)$ 是含幺环和除环，但不是交换环，因为四元数乘法不满足交换律。

定义 2.4.23 (域 Field)**.** 设 $(F,+,\cdot)$ 为代数结构。如果

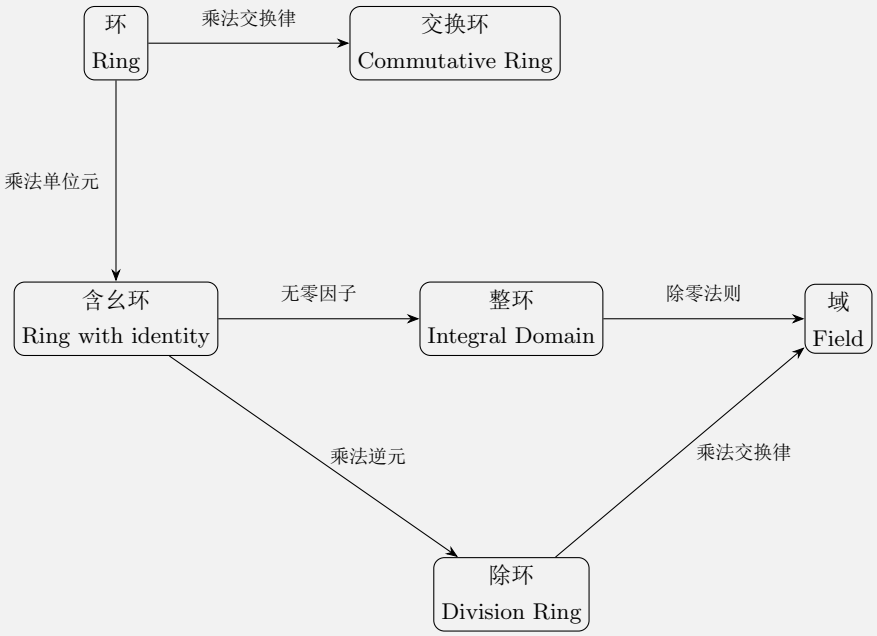
1. $(F,+)$ 是交换群；
2. $(F,\cdot)$ 是交换群；
3. 乘法对加法满足分配律；
4. 除零法则：对任意 $a\in F$，$a\neq 0$，存在 $b\in F$，使得 $a\cdot b=1$。

则称 $(F,+,\cdot)$ 为域。也即，域 $(F,+,\cdot)$ 是含幺交换环且是除环。

例 2.4.3. 常见的域有：有理数域 $(\mathbb{Q},+,\cdot)$、实数域 $(\mathbb{R},+,\cdot)$ 和复数域 $(\mathbb{C},+,\cdot)$

注解

用一幅图展示各种环之间的关系：



2.4.6 模与线性空间

定义 2.4.24 (模 Module). 设 $(R,+,\cdot)$ 为含幺环，$(G,+)$ 为阿贝尔群。如果存在一个标量乘法 $*:R\times G\to G$，满足以下条件：

1. 对任意 $r,s\in R$，$g\in G$，有 $(r+s)*g=r*g+s*g$；
2. 对任意 $r\in R$，$g,h\in G$，有 $r*(g+h)=r*g+r*h$；
3. 对任意 $r,s\in R$，$g\in G$，有 $(r*s)*g=r*(s*g)$；
4. 对任意 $g\in G$，有 $1*g=g$。

则称 $(G,+)$ 为**左R-模**。如果存在一个标量乘法 $*:G\times R\to G$，满足以下条件：

1. 对任意 $r,s\in R$，$g\in G$，有 $g*(r+s)=g*r+g*s$；
2. 对任意 $r\in R$，$g,h\in G$，有 $(g+h)*r=g*r+h*r$；
3. 对任意 $r,s\in R$，$g\in G$，有 $g*(r*s)=(g*r)*s$；
4. 对任意 $g\in G$，有 $g*1=g$。

则称 $(G,+)$ 为**右R-模**。如果 $(R,+,\cdot)$ 是含幺交换环，左、右 R-模没有区别，对任意 $r\in R$，$g\in G$，均有 $r*g=g*r$，则称 $(G,+)$ 为**双边R-模**，或 **R-模**。

定义 2.4.25 (线性空间 Linear Space). 设 $(F,+,\cdot)$ 为域，$(V,+)$ 为阿贝尔群。如果存在一个标量乘法 $\cdot:F\times V\to V$，满足以下条件：

1. 对任意 $r,s\in F$，$\mathbf{v}\in V$，有 $(r+s)\cdot\mathbf{v}=r\cdot\mathbf{v}+s\cdot\mathbf{v}$；
2. 对任意 $r\in F$，$\mathbf{u},\mathbf{v}\in V$，有 $r\cdot(\mathbf{u}+\mathbf{v})=r\cdot\mathbf{u}+r\cdot\mathbf{v}$；
3. 对任意 $r,s\in F$，$\mathbf{v}\in V$，有 $(r\cdot s)\cdot\mathbf{v}=r\cdot(s\cdot\mathbf{v})$；
4. 对任意 $\mathbf{v}\in V$，有 $1\cdot\mathbf{v}=\mathbf{v}$。

则称 $(V,+,\cdot)$ 为 F-线性空间，或向量空间 *Vector Space*。V 中的元素称为向量 *Vector*，F 中的元素称为标量 *Scalar*。

注解

线性空间是模的特例，线性空间是定义在域上的模，而模是定义在环上的。线性空间是非常重要的代数结构，是线性代数研究的对象。线性空间中“空间”二字，强调了线性空间的几何意义，解析几何中常用向量表示空间中的点、线、面等几何对象。在线性空间上定义度量结构后，称为赋范线性空间，是泛函分析的研究对象。可以说线性空间是现代数学的基础。

2.5 序结构

定义 2.5.1 (偏序关系 Partial Order Relation). 设 R 为非空集合 X 上的二元关系。称 R 为 X 上的偏序关系，当且仅当，R 满足：对 $x, y, z \in X$

1. 自反性（*Reflexivity*）：$(x, x) \in R$;
2. 反对称性（*Antisymmetry*）：若 $(x, y) \in R$ 且 $(y, x) \in R$，则 $x = y$;
3. 传递性（*Transitivity*）：若 $(x, y) \in R$ 且 $(y, z) \in R$，则 $(x, z) \in R$。

偏序关系常用符号 $\preceq$ 表示，$(x, y) \in R$ 简记为 $x \preceq y$。二元组 $(X, \preceq)$ 称为偏序集。

定义 2.5.2 (严格偏序关系 Strict Partial Order Relation). 设 R 为非空集合 X 上的二元关系。称 R 为 X 上的严格偏序关系，当且仅当，R 满足：对 $x, y, z \in X$

1. 反自反性（*Irreflexivity*）：$(x, x) \notin R$;
2. 反对称性（*Antisymmetry*）：若 $(x, y) \in R$ 且 $(y, x) \in R$，则 $x = y$;
3. 传递性（*Transitivity*）：若 $(x, y) \in R$ 且 $(y, z) \in R$，则 $(x, z) \in R$。

严格偏序关系常用符号 $\prec$ 表示，$(x, y) \in R$ 简记为 $x \prec y$。

定义 2.5.3 (全序关系 Total Order Relation). 设 $\preceq$ 为非空集合 X 上的偏序关系。称 $\preceq$ 为 X 上的全序关系，当且仅当，$\preceq$ 满足：

1. 全序性（*Totality*）：对任意 $x, y \in X$，要么 $x \preceq y$，要么 $y \preceq x$。

全序关系也称为线序关系，全序关系常用符号 $\leq$ 表示，二元组 $(X, \leq)$ 称为全序集或线序集。

> 注解
>
> 在集合论中，集合中的元素是没有顺序的概念的，当定义了集合中元素之间的某种顺序关系后，集合才具有了序结构。如果是全序关系，那么这个集合中任意两个元素都是可比的。序关系强调集合元素之间的可比性，如果集合中的元素是也是一些集合，那么集合之间的包含关系是一种偏序关系，集合之间的优势关系也是一种偏序关系。

2.5.1 上下界

定义 2.5.4 (上界 Upper Bound). 设 $(X, \preceq)$ 为偏序集，$Y \subseteq X$。若存在 $b \in X$，使得对任意 $y \in Y$，均有 $y \preceq b$，则称 b 为子集 Y 的上界。

定义 2.5.5 (下界 Lower Bound). 设 $(X, \preceq)$ 为偏序集，$Y \subseteq X$。若存在 $a \in X$，使得对任意 $y \in Y$，均有 $a \preceq y$，则称 a 为子集 Y 的下界。

注解

如果子集 Y 存在上界（下界），但不唯一，且不一定属于子集 Y；如果 Y 没有上界（下界），则称 Y 无界。

定义 2.5.6 (下确界 Infimum). 设 $(X, \preceq)$ 为偏序集，$Y \subseteq X$。若 Y 存在下界，且存在 $i \in X$，使得对任意 $y \in Y$，均有 $i \preceq y$，且对任意 $a \in X$，若 $a \preceq y$，则有 $a \preceq i$，则称 i 为子集 Y 的下确界，记为 $i = \inf Y$。

定义 2.5.7 (上确界 Supremum). 设 $(X, \preceq)$ 为偏序集，$Y \subseteq X$。若 Y 存在上界，且存在 $s \in X$，使得对任意 $y \in Y$，均有 $y \preceq s$，且对任意 $b \in X$，若 $y \preceq b$，则有 $s \preceq b$，则称 s 为子集 Y 的上确界，记为 $s = \sup Y$。

注解

如果 Y 存在上界，那么上确界是所有上界中最小的一个；如果 Y 存在下界，那么下确界是所有下界中最大的一个。

定理 2.5.1 (确界唯一性). 设 $(X, \preceq)$ 为偏序集，$Y \subseteq X$。若 Y 存在上确界（下确界），则上确界（下确界）唯一。

证明. 假设 $s_1, s_2 \in X$ 均为子集 Y 的上确界，且 $s_1 \neq s_2$。由上确界定义可知，对任意 $y \in Y$，均有 $y \preceq s_1$ 且 $y \preceq s_2$，且对任意 $b \in X$，若 $y \preceq b$，则有 $s_1 \preceq b$ 且 $s_2 \preceq b$。取 $b = s_2$，则有 $s_1 \preceq s_2$；取 $b = s_1$，则有 $s_2 \preceq s_1$。由反对称性可知，$s_1 = s_2$，与假设矛盾，因此上确界唯一。下确界唯一的证明类似。 □

定义 2.5.8 (最小元 Minimal Element). 设 $(X, \preceq)$ 为偏序集，$Y \subseteq X$。若存在 $m \in Y$，使得对任意 $y \in Y$，均有 $m \preceq y$，则称 m 为子集 Y 的最小元。

定义 2.5.9 (最大元 Maximal Element). 设 $(X, \preceq)$ 为偏序集，$Y \subseteq X$。若存在 $M \in Y$，使得对任意 $y \in Y$，均有 $y \preceq M$，则称 M 为子集 Y 的最大元。

2.6 拓扑结构

定义 2.6.1 (拓扑空间 Topological Space). 设X是一个集合，$\mathcal{T}(X) \subseteq \mathcal{P}(X)$ 是 X 的子集族，二元组 $(X, \mathcal{T}(X))$ 称为拓扑空间，当且仅当，$\mathcal{T}(X)$ 满足：

1. 空集与全集：$\varnothing \in \mathcal{T}(X)$ 且 $X \in \mathcal{T}(X)$；
2. 对任意并封闭：任意 $\{U_i : i \in I\} \subseteq \mathcal{T}(X)$，有 $\bigcup_{i\in I} U_i \in \mathcal{T}(X)$；
3. 对有限交封闭：有限个 $U_1, U_2, \ldots, U_n \in \mathcal{T}(X)$，有 $U_1 \cap U_2 \cap \cdots \cap U_n \in \mathcal{T}(X)$。

子集族 $\mathcal{T}(X)$ 称为 X 上的**拓扑 *Topology***，$\mathcal{T}(X)$ 中的元素称为**开集 *Open Set***。

注解

根据拓扑空间的的定义，幂集 $\mathcal{P}(X)$ 和 $\{\varnothing, X\}$ 都是 X 上的拓扑，分别称为**离散拓扑 Discrete Topology**和**平凡拓扑 Trivial Topology**。给定集合 X，X 的任意子集族并非都是 X 上的拓扑，X 的拓扑也非唯一。比如，设 $X = \{a, b, c\}$，那么下面的子集族都是 X 上的拓扑：

$$\begin{aligned}
\mathcal{T}_1(X) &= \{\varnothing, X\},\\
\mathcal{T}_2(X) &= \mathcal{P}(X),\\
\mathcal{T}_3(X) &= \{\varnothing, X, \{a\}\},\\
\mathcal{T}_4(X) &= \{\varnothing, X, \{a, b\}\},\\
\mathcal{T}_5(X) &= \{\varnothing, X, \{a\}, \{a, b\}\},\\
\mathcal{T}_6(X) &= \{\varnothing, X, \{a, b\}, \{b\}, \{b, c\}\}.
\end{aligned}$$

下面的子集族不是 X 上的拓扑：

$$\begin{aligned}
\mathcal{T}_7(X) &= \{\varnothing, X, \{a\}, \{b\}\},\\
\mathcal{T}_8(X) &= \{\varnothing, X, \{a, b\}, \{b, c\}\}.
\end{aligned}$$

定义 2.6.2 (闭集 Closed Set). 设 $(X, \mathcal{T}(X))$ 为拓扑空间，称 $A \subseteq X$ 为闭集，当且仅当，$\complement_X A \in \mathcal{T}(X)$。

命题 2.6.1 (闭集的性质). 设 $(X, \mathcal{T}(X))$ 为拓扑空间，则有：

1. 空集与全集：$\varnothing$ 与 X 是闭集；
2. 对任意交封闭：$\bigcap_{i\in I} A_i$ 是闭集，其中 $\{A_i : i \in I\}$ 是闭集；
3. 对有限并封闭：$A_1 \cup A_2 \cup \cdots \cup A_n$ 是闭集，其中 $A_1, A_2, \ldots, A_n$ 是闭集。

注解

闭集是对几何空间中闭区间、闭球等概念的抽象。闭集与开集的关系是互补的，即一个集合是闭集，当且仅当它的补集是开集。拓扑空间中的闭集可以用来定义点的极限、闭包等概念。

2.6.1 连续函数

定义 2.6.3 (连续函数 Continuous Function). 设 $(X,\mathcal{T}(X))$ 和 $(Y,\mathcal{T}(Y))$ 是拓扑空间，映射 $f: X\to Y$ 称为连续函数，当且仅当，$\forall V\in\mathcal{T}(Y)$，有 $f^{-1}(V)\in\mathcal{T}(X)$。

定义 2.6.4 (同胚 Homeomorphism). 设 $(X,\mathcal{T}(X))$ 和 $(Y,\mathcal{T}(Y))$ 是拓扑空间，映射 $f: X\to Y$ 称为同胚，当且仅当，f 是双射且 f 与 f^{-1} 都是连续函数，记为 $X\cong Y$。

注解

连续函数是对几何空间中连续变化概念的抽象。连续函数保持了拓扑结构，即开集的原像仍然是开集。同胚是拓扑空间之间的一种等价关系，表示两个拓扑空间在拓扑意义下是相同的。拓扑空间的同胚类似于代数结构的同构。

2.6.2 度量空间

定义 2.6.5 (度量空间 Metric Space). 设 X 是一个非空集合，映射 $d: X\times X\to\mathbb{R}$ 称为度量，当且仅当，$\forall x,y,z\in X$，有：

1. 非负性：$d(x,y)\geq 0$，且当且仅当 $x=y$ 时取等号；
2. 对称性：$d(x,y)=d(y,x)$；
3. 三角不等式：$d(x,z)\leq d(x,y)+d(y,z)$。

二元组 (X,d) 称为度量空间，函数 d 称为 X 上的度量。

定义 2.6.6 (开球 Open Ball). 设 (X,d) 为度量空间，$x\in X$ 且 $r>0$，集合 $B(x,r)=\{y\in X: d(x,y)<r\}$ 称为以 x 为中心、r 为半径的开球。

命题 2.6.2 (度量空间诱导的拓扑). 设 (X,d) 为度量空间，定义 $\mathcal{T}(X)=\{U\subseteq X: \forall x\in U, \exists r>0, B(x,r)\subseteq U\}$，则 $(X,\mathcal{T}(X))$ 为拓扑空间。

例 2.6.1. 实数集 $\mathbb{R}$ 和绝对值距离 $d(x,y)=|x-y|$ 构成一个度量空间，其中，

1. 任意开区间 (a,b) 是开集；$(a,+\infty)$ 和 $(-\infty,b)$ 也是开集;
2. 任意闭区间 $[a,b]$ 是闭集，它是开区间 $(-\infty,b)\cap(a,+\infty)$ 的补集；有限集也是闭集；
3. $\mathbb{R}$ 和 $\varnothing$ 既是开集也是闭集
4. 任意半开半闭区间 $[a,b)$ 和 $(a,b]$ 既不是开集也不是闭集。

注解

度量空间是对几何空间中距离概念的抽象。度量函数 d 用来衡量集合中任意两个元素之间的距离。常见的度量包括欧氏距离、曼哈顿距离和切比雪夫距离等。度量空间可以诱导出拓扑结构，开球的集合构成了 X 上的一个拓扑，称为由度量 d 诱导的拓扑。

2.6.3 赋范线性空间

定义 2.6.7 (赋范线性空间 Normed Linear Space)**.** 设 V 是域 $\mathbb{F}$ 上的线性空间，映射 $\|\cdot\|: V \to \mathbb{R}$ 称为范数，当且仅当，$\forall x, y \in V$ 且 $\forall \alpha \in \mathbb{F}$，有：

1. 非负性：$\|x\| \geq 0$，且当且仅当 $x = 0$ 时取等号；
2. 齐次性：$\|\alpha x\| = |\alpha| \|x\|$；
3. 三角不等式：$\|x + y\| \leq \|x\| + \|y\|$。

二元组 $(V, \|\cdot\|)$ 称为赋范线性空间，函数 $\|\cdot\|$ 称为 V 上的范数。

命题 2.6.3 (赋范线性空间诱导的度量)**.** 设 $(V, \|\cdot\|)$ 为赋范线性空间，定义 $d : V \times V \to \mathbb{R}$，$d(x, y) = \|x - y\|$，则 (V, d) 为度量空间。

2.6.4 内积空间

定义 2.6.8 (内积空间 Inner Product Space)**.** 设 V 是域 $\mathbb{F}$ 上的线性空间，映射 $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{F}$ 称为内积，当且仅当，$\forall x, y, z \in V$ 且 $\forall \alpha \in \mathbb{F}$，有：

1. 共轭对称性：$\langle x, y\rangle = \overline{\langle y, x\rangle}$；
2. 线性性：$\langle \alpha x + y, z\rangle = \alpha\langle x, z\rangle + \langle y, z\rangle$；
3. 正定性：$\langle x, x\rangle \geq 0$，且当且仅当 $x = 0$ 时取等号。

二元组 $(V, \langle\cdot,\cdot\rangle)$ 称为内积空间，函数 $\langle\cdot,\cdot\rangle$ 称为 V 上的内积。

命题 2.6.4 (内积空间诱导的赋范线性空间)**.** 设 $(V, \langle\cdot,\cdot\rangle)$ 为内积空间，定义 $\|\cdot\| : V \to \mathbb{R}$，$\|x\| = \sqrt{\langle x, x\rangle}$，则 $(V, \|\cdot\|)$ 为赋范线性空间。

注解

赋范线性空间既是线性空间又是度量空间。范数 $\|\cdot\|$ 用来衡量向量的长度或大小。内积空间既是线性空间又是赋范线性空间。内积 $\langle\cdot,\cdot\rangle$ 用来衡量向量之间的夹角和正交性。

Chapter 3

数系的扩充

在第一章中，利用无穷公理定义了自然数 1.2.12，根据集合的包含关系，定义了自然数的序 1.2.13，$(\mathbb{N}, \leq)$ 是一个全序集。然后利用替代公理模式，定义了自然数的加法 1.2.14 和乘法 1.2.15，$(\mathbb{N}, +)$ 和 $(\mathbb{N}, \times)$ 都是是一个交换幺半群；乘法对加法分配，$(\mathbb{N}, +, \times)$ 是一个含幺交换半环。在本章中，将介绍如何从自然数出发，扩充出整数、有理数、实数等数系。数系的每一次扩充，都希望它能使更多的运算封闭，并且已有的运算性质能“向下兼容”。

定义 3.0.1 (等于关系 Equality Relation)**.** *R 为集合 X 上的一个等价关系。称 R 为 X 上的等于关系，当且仅当，R 满足：*

1. *替代性：对于任意 $(x, y) \in R$，对于一切函数 $f : X \to X$，均有 $(f(x), f(y)) \in R$*

记 $(x, y) \in R$ 为 $x = y$。

> 注解
>
> 等于关系是更严格的等价关系。满足替代性说明，集合中等价的两元素，经过任意函数映射后的像也是等价的。在定义新的数系的时候，不仅需要验证新的运算是否对集合封闭，还需要给出一个等于关系。

3.1 整数

定义 3.1.1 (整数 Integer)**.** *有序对 $(a, b) \in \mathbb{N}^2$ 记为 $a - b$，其中，*

1. *等于关系：$a - b = c - d \iff a + d = b + c$*
2. *等价类：任意 $a - b \in \mathbb{N}^2$ 的等价类为*

$$[a - b]_= = \{(c, d) \in \mathbb{N}^2 : a + d = b + c\}$$

称 $\mathbb{N}^2$ 关于 $=$ 关系的商集 $\mathbb{N}^2/_= = \{[a - b]_= : a - b \in \mathbb{N}^2\} =$ 为整数集，记为 $\mathbb{Z}$。整数集中的元素称为整数。

注解

在 $a-b$ 中，$-$ 不是减号，而是一个符号，此时还没有定义减法，仅表示这是一个有序对 (a,b)。整数也不是有序对，而是有序对关于等于关系的等价类，比如，$3-5$ 和 $1-3$ 是不同的有序对，但它们属于同一个等价类 $[3-5]_= = [1-3]_=$，表示同一个整数。全体自然数可以嵌入到整数集中，即 $\forall n \in \mathbb{N}$，有 $n = [n-0]_= \in \mathbb{Z}$。例如，$0 = [0-0]_=$，$1 = [1-0]_=$，$2 = [2-0]_=$，$3 = [3-0]_=$，$\cdots$。$\complement_{\mathbb{Z}}\mathbb{N}$ 中的元素称为负整数。

定义 3.1.2 (整数的加法 Addition of Integers)**.** 设 $[a-b]_=, [c-d]_= \in \mathbb{Z}$，定义加法为

$$[a-b]_= + [c-d]_= = [(a+c)-(b+d)]_=$$

定义 3.1.3 (整数的乘法 Multiplication of Integers)**.** 设 $[a-b]_=, [c-d]_= \in \mathbb{Z}$，定义乘法为

$$[a-b]_= \cdot [c-d]_= = [(ac+bd)-(ad+bc)]_=$$

注解

整数的加法和乘法都是良定义（Well-defined）的，即不依赖于代表元的选取，而且是封闭的。证明略。自然数的加法和乘法在整数集中保持不变。例如，$[2-0]_= + [3-0]_= = [(2+3)-(0+0)]_= = [5-0]_=$，即 $2+3=5$。

定义 3.1.4 (整数加法的逆元 Additive Inverse of Integers)**.** 设 $[a-b]_= \in \mathbb{Z}$，定义其加法逆元为

$$-[a-b]_= = [b-a]_=$$

使得，$[a-b]_= + [-[a-b]_= = [0-0]_=$。

定义 3.1.5 (整数的减法 Subtraction of Integers)**.** 设 $[a-b]_=, [c-d]_= \in \mathbb{Z}$，定义减法为

$$[a-b]_= - [c-d]_= = [a-b]_= + (-[c-d]_=) = [(a+d)-(b+c)]_=$$

注解

可以证明，任何一个整数都有唯一的加法逆元。因此，整数的减法也是良定义的，即不依赖于代表元的选取，而且是封闭的。自然数集中，不存在加法逆元，因此也不存在减法。整数集相比自然数集，扩充了加法逆元，使得加法和减法都能良定义。

定理 3.1.1 (整数代数运算的性质)**.** 设 $x, y, z \in \mathbb{Z}$，则

1. 交换律：$x+y = y+x$，$xy = yx$
2. 结合律：$(x+y)+z = x+(y+z)$，$(xy)z = x(yz)$
3. 分配律：$x(y+z) = xy+xz$
4. 存在加法单位元 0，使得 $\forall x \in \mathbb{Z}$，有 $x+0 = 0+x = x$

5. 存在乘法单位元 1，使得 $\forall x \in \mathbb{Z}$，有 $x \cdot 1 = 1 \cdot x = x$
6. 存在加法逆元 $-x$，使得 $\forall x \in \mathbb{Z}$，有 $x + (-x) = (-x) + x = 0$
7. 乘法对加法的零因子：$\forall x, y \in \mathbb{Z}$，若 $xy = 0$，则 $x = 0$ 或 $y = 0$

定义 3.1.6 (整数的序关系 Order Relation on Integers). 设 $[a-b]_=, [c-d]_= \in \mathbb{Z}$，定义序关系为

$$[a-b]_= \leq [c-d]_= \iff a + d \leq b + c$$

定义 3.1.7 (整数的绝对值 Absolute Value of Integers). 设 $[a-b]_= \in \mathbb{Z}$，定义其绝对值为

$$|[a-b]_=| = \begin{cases} [a-b]_= & a \geq b \\ -[a-b]_= & a < b \end{cases}$$

定义 3.1.8 (整数的绝对值距离 Distance of Absolute Value of Integers). 设 $x, y \in \mathbb{Z}$，定义它们的绝对值距离为

$$d(x, y) = |x - y|$$

定理 3.1.2 (整数绝对值的性质 Properties of Absolute Value of Integers). 设 $x, y \in \mathbb{Z}$，则

1. 非负性：$|x| \geq 0$，且 $|x| = 0 \iff x = 0$
2. 积的绝对值：$|xy| = |x||y|$
3. 三角不等式：$|x + y| \leq |x| + |y|$
4. 反三角不等式：$||x| - |y|| \leq |x - y|$
5. 距离的非负性：$d(x, y) \geq 0$，且 $d(x, y) = 0 \iff x = y$
6. 距离的三角不等式：$d(x, z) \leq d(x, y) + d(y, z)$
7. 距离的对称性：$d(x, y) = d(y, x)$

注解

三元组 $(\mathbb{Z}, +, \cdot)$ 是一个交换整环。二元组 $(\mathbb{Z}, \leq)$ 是一个全序集。二元组 $(\mathbb{Z}, d)$ 是一个度量空间。

3.2 有理数

定义 3.2.1 (有理数 Rational Number). 有序对 $(a,b)\in\mathbb{Z}^2$ 记为 a/b，其中，

1. 约定 $b\neq 0$。
2. 等于关系：$a/b=c/d \iff ad=bc$
3. 等价类：任意 $a/b\in\mathbb{Z}^2$ 的等价类为

$$[a/b]_{=}=\{(c,d)\in\mathbb{Z}^2 : ad=bc\}$$

称 $\mathbb{Z}^2$ 关于 $=$ 关系的商集 $\mathbb{Z}^2/_{=}=\{[a/b]_{=} : a/b\in\mathbb{Z}^2\}$ 为有理数集，记为 $\mathbb{Q}$。有理数集中的元素称为有理数。

注解

在 a/b 中，/ 不是除号，而是一个符号，此时还没有定义除法，仅表示这是一个有序对 (a,b)。有理数也不是有序对，而是有序对关于等于关系的等价类，比如，$1/2$ 和 $2/4$ 是不同的有序对，但它们属于同一个等价类 $[1/2]_{=}=[2/4]_{=}$，表示同一个有理数。全体整数可以嵌入到有理数集中，即 $\forall n\in\mathbb{Z}$，有 $n=[n/1]_{=}\in\mathbb{Q}$。例如，$0=[0/1]_{=}$，$1=[1/1]_{=}$，$2=[2/1]_{=}$，$3=[3/1]_{=}$，$\cdots$。$\complement_{\mathbb{Q}}\mathbb{Z}$ 中的元素称为真分数。

注解

有序对中要求第二个元素不为零，即 $b\neq 0$，这是因为如果 $b=0$，则等于关系将变得不合理，比如，$1/0=2/0$ 将导致 $1\cdot 0=2\cdot 0$，即 $0=0$，这对任何 $a/0$ 和 $c/0$ 都成立，违背了等于关系的自反性，从而使得所有形如 $a/0$ 的有序对都属于同一个等价类，我们不希望这样的情况出现。

定义 3.2.2 (有理数的加法 Addition of Rational Numbers). 设 $[a/b]_{=},[c/d]_{=}\in\mathbb{Q}$，定义加法为

$$[a/b]_{=}+[c/d]_{=}=[(ad+bc)/(bd)]_{=}$$

定义 3.2.3 (有理数的乘法 Multiplication of Rational Numbers). 设 $[a/b]_{=},[c/d]_{=}\in\mathbb{Q}$，定义乘法为

$$[a/b]_{=}\cdot[c/d]_{=}=[(ac)/(bd)]_{=}$$

定义 3.2.4 (有理数的加法逆元 Additive Inverse of Rational Numbers). 设 $[a/b]_{=}\in\mathbb{Q}$，定义其加法逆元为

$$-[a/b]_{=}=[-a/b]_{=}$$

使得，$[a/b]_{=}+-[a/b]_{=}=[0/b^2]_{=}$。

定义 3.2.5 (有理数的减法 Subtraction of Rational Numbers). 设 $[a/b]_{=},[c/d]_{=}\in\mathbb{Q}$，定义减法为

$$[a/b]_{=}-[c/d]_{=}=[a/b]_{=}+(-[c/d]_{=})=[(ad-bc)/(bd)]_{=}$$

注解

有理数的加法、减法和乘法都是良定义（Well-defined）的，即不依赖于代表元的选取，而且是封闭的。证明略。整数的加法和乘法在有理数集中保持不变。例如，$[2/1]_= + [3/1]_= = [(2\cdot 1+3\cdot 1)/(1\cdot 1)]_= = [5/1]_=$，即 $2+3=5$。

定义 3.2.6 (有理数的乘法逆元 Multiplicative Inverse of Rational Numbers)**.** 设 $[a/b]_= \in \mathbb{Q}$，且 $a \neq 0$，定义其乘法逆元为

$$[a/b]_=^{-1} = [b/a]_=$$

使得，$[a/b]_= \cdot [a/b]_=^{-1} = [ab/ab]_= = [1/1]_=$。

定义 3.2.7 (有理数的除法 Division of Rational Numbers)**.** 设 $[a/b]_=, [c/d]_= \in \mathbb{Q}$，且 $c \neq [0/1]_=$，定义除法为

$$[a/b]_= / [c/d]_= = [a/b]_= \cdot [c/d]_=^{-1} = [(ad)/(bc)]_=$$

注解

可以证明，任何一个非零有理数都有唯一的乘法逆元。因此，有理数的除法也是良定义的，即不依赖于代表元的选取，而且是封闭的。整数集中，不存在乘法逆元，因此也不存在除法。相比整数集，有理数集扩充了乘法逆元，使得加法、减法、乘法和除法都能良定义。

定理 3.2.1 (有理数代数运算的性质)**.** 设 $x, y, z \in \mathbb{Z}$，则

1. 交换律：$x+y = y+x$，$xy = yx$
2. 结合律：$(x+y)+z = x+(y+z)$，$(xy)z = x(yz)$
3. 分配律：$x(y+z) = xy + xz$
4. 加法的单位元：存在唯一的 $0 \in \mathbb{Q}$，使得 $\forall x \in \mathbb{Q}$，有 $x + [0/1]_= = x$
5. 乘法的单位元：存在唯一的 $1 \in \mathbb{Q}$，使得 $\forall x \in \mathbb{Q}$，有 $x \cdot [1/1]_= = x$
6. 乘法对加法的零因子：$\forall x, y \in \mathbb{Q}$，若 $xy = [0/1]_=$，则 $x = [0/1]_=$ 或 $y = [0/1]_=$
7. 加法的逆元：$\forall x \in \mathbb{Q}$，存在唯一的 $-x \in \mathbb{Q}$，使得 $x + (-x) = [0/1]_=$
8. 乘法的逆元：$\forall x \in \mathbb{Q}, x \neq [0/1]_=$，存在唯一的 $x^{-1} \in \mathbb{Q}$，使得 $x \cdot x^{-1} = [1/1]_=$

注解

三元组 $(\mathbb{Q}, +, \cdot)$ 构成一个有理数域。

定义 3.2.8 (有理数的序关系 Order Relation of Rational Numbers)**.** 设 $[a/b]_=, [c/d]_= \in \mathbb{Q}$，为了避免符号歧义，约定 $b>0,\ d>0$，定义序关系为：

$$[a/b]_= \leq [c/d]_= \iff ad \leq bc$$

定义 3.2.9 (有理数的绝对值 Absolute Value of Rational Numbers). 设 $[a/b]_= \in \mathbb{Q}$，定义其绝对值为

$$|[a/b]_=| = \begin{cases} [a/b]_=, & a/b \geq [0/1]_= \\ -[a/b]_=, & a/b < [0/1]_= \end{cases}$$

定义 3.2.10 (有理数的距离 Distance of Rational Numbers). 设 $[a/b]_=, [c/d]_= \in \mathbb{Q}$，定义它们之间的距离为

$$d([a/b]_=, [c/d]_=) = |[a/b]_= - [c/d]_=|$$

定理 3.2.2 (有理数绝对值的性质). 设 $x, y \in \mathbb{Q}$，则

1. 非负性：$|x| \geq [0/1]_=$，且 $|x| = [0/1]_= \iff x = [0/1]_=$
2. 乘积的绝对值：$|xy| = |x||y|$
3. 幂的绝对值：$|x^n| = |x|^n,\ n \in \mathbb{Z}$
4. 商的绝对值：$|x/y| = |x|/|y|,\ y \neq [0/1]_=$
5. 三角不等式：$|x + y| \leq |x| + |y|$
6. 反三角不等式：$||x| - |y|| \leq |x - y|$
7. 距离的非负性：$d(x, y) \geq [0/1]_=$，且 $d(x, y) = [0/1]_= \iff x = y$
8. 距离的三角不等式：$d(x, z) \leq d(x, y) + d(y, z)$
9. 距离的对称性：$d(x, y) = d(y, x)$

注解

二元组 $(\mathbb{Q}, \leq)$ 是一个全序集，二元组 $(\mathbb{Q}, d)$ 是一个度量空间。

命题 3.2.1 (有理数的稠密性 Density of Rational Numbers). 设 $x, y \in \mathbb{Q}$，且 $x < y$，则存在 $z \in \mathbb{Q}$，使得 $x < z < y$。例如，取 $z = (x + y)/2$。

注解

有理数的稠密性说明任意两个有理数之间，都有无数个有理数。尽管有理数是稠密的，但在有理数之间依然存在无限多的“空隙”，比如, 在 1 和 2 之间，不存在有理数 x 使得 $x^2 = 2$，因此有理数集存在“空隙”，是“不连续的”。

3.3 实数

从自然数到有理数的扩充都非常的自然，然而有理数并不能满足我们的所有需求。比如在上一节的末尾介绍有理数稠密性时提到，不存在有理数 x 使得 $x^2 = 2$。为了满足这样的需求，我们需要对数系进行进一步的扩充，得到实数系。

例 3.3.1. 通过迭代法，我们可以找到一个有理数序列 a_n，使得 $(a_n)^2$ 趋近于 2：

$$a_{n+1} = \frac{1}{2}(a_n + \frac{2}{a_n}),\ n \geq 0 \tag{3.1}$$

令 $a_0 = 1$，得到一个有理数序列：

$$\begin{aligned}
a_1 &= \frac{1}{2}(1+2) = \frac{3}{2} = 1.5 \\
a_2 &= \frac{1}{2}(\frac{3}{2} + \frac{4}{3}) = \frac{17}{12} = 1.41666666666\cdots \\
a_3 &= \frac{1}{2}(\frac{17}{12} + \frac{24}{17}) = \frac{577}{408} = 1.414215686274\cdots \\
a_4 &= \frac{1}{2}(\frac{577}{408} + \frac{816}{577}) = \frac{665857}{470832} = 1.414213562374\cdots \\
&\vdots
\end{aligned}$$

无限递归执行下去，会得到一个有理数的数列。随着 n 的增大，a_n 之间的间隔会越来越小。换一个首项，令 $a'_0 = 1.4$，同样使用迭代式 *3.1*，得到另一个有理数数列：

$$\begin{aligned}
a'_1 &= \frac{1}{2}(\frac{7}{5} + \frac{10}{7}) = \frac{99}{70} = 1.4142857142857\cdots \\
a'_2 &= \frac{1}{2}(\frac{99}{70} + \frac{140}{99}) = \frac{19601}{13860} = 1.4142135642135642\cdots \\
a'_3 &= \frac{1}{2}(\frac{19601}{13860} + \frac{27720}{19601}) = \frac{768398401}{543339720} = 1.41421356237309504\cdots \\
a'_4 &= \frac{1}{2}(\frac{768398401}{543339720} + \frac{1086679440}{768398401}) = \frac{1180872205318713601}{835002744095575440} = 1.414213562373095048801\cdots \\
&\vdots
\end{aligned}$$

无限递归执行下去，会得到另一个有理数的数列。随着 n 的增加，数列中项与项之间的间隔会也会越来越小。同时，随着序号 n 的增加，数列 a_n 和数列 a'_n 中项的差 $|a_n - a'_n|$ 也会越来越小。

> 注解
>
> 我们知道，这两个序列最终都会收敛到无理数 $\sqrt{2}$，但是 $\sqrt{2} \notin \mathbb{Q}$。我们称数列 $\{a_n \in \mathbb{Q}\}$ 和数列 $\{a'_n \in \mathbb{Q}\}$ 为**柯西序列**，$\sqrt{2}$ 为这两个**柯西序列的极限**。在有理数集中，柯西序列的极限不一定是有理数。因此我们需要对有理数集打上补丁，让这些序列的极限也在这个新集合中。

3.3.1 柯西序列与实数

定义 3.3.1 (有理数序列 sequence of rational numbers)**.** 函数 $f : \mathbb{N} \to \mathbb{Q}$ 为有理数序列，记为 $\{a_n\}$，其中 $a_n = f(n),\ n \geq m, \cdots$。

注解

有理数序列说明，对于每个大于等于 m 的自然数，都有唯一一个确定的有理数与之对应。例如：

1. 等比数列：$a_n = a_1 q^{n-1},\ a_1 \neq 0,\ q \neq 0,\ n = 1, 2, 3, \cdots$
2. 等差数列：$a_n = a_1 + (n-1)d,\ n = 1, 2, 3 \cdots$
3. 斐波那契数列：$a_1 = 1,\ a_2 = 1,\ a_n = a_{n-1} + a_{n-2},\ n \geq 3$
4. 素数数列：$a_1 = 2,\ a_2 = 3,\ a_3 = 5,\ a_4 = 7,\ a_5 = 11,\ a_6 = 13, \cdots$

定义 3.3.2 (柯西序列 Cauchy sequence)**.** 设 $\{a_n\}$ 是有理数序列。$\{a_n\}$ 是柯西序列，当且仅当，对于任意给定的有理数 $\epsilon > 0$，都存在一个正整数 N，使得当 $i, j > N$ 时，有

$$|a_i - a_j| \leq \epsilon$$

柯西序列也称为**基本序列**。

注解

柯西序列是一种特殊的有理数序列，它要求随着序号 n 的增大，序列中项与项之间的间隔越来越小。例如，数列 $a_n = \frac{1}{n},\ n \geq 1$ 和 $a_{n+1} = \frac{1}{2}(a_n + \frac{2}{a_n}),\ n \geq 0$ 都是柯西序列，

定义 3.3.3 (有界序列 bounded sequence)**.** 设 $\{a_n\}$ 是有理数序列。如果存在有理数 $M > 0$，使得对任意的 n 都有 $|a_n| \leq M$，则称 $\{a_n\}$ 是有界序列。

定理 3.3.1. 柯西序列都是有界序列；有界序列不一定是柯西序列。

注解

一个序列是柯西序列蕴含该序列是有界序列，但有界序列不一定是柯西序列，比如，$a_n = (-1)^n,\ n \geq 1$ 是有界序列，但不是柯西序列。

定义 3.3.4 (实数 Real Number)**.** 设 S 是所有有理柯西序列的集合

1. 等于关系：对任意有理柯西序列 $\{a_n\}, \{b_n\} \in S$，$\{a_n\} = \{b_n\}$ 当且仅当，对于任意有理数 $\epsilon > 0$，都存在一个正整数 N，使得当 $n > N$ 时，有

$$|a_n - b_n| \leq \epsilon$$

2. 等价类：任意 $\{a_n\} \in S$ 的等价类为

$$[\{a_n\}]_= = \{\{b_n\} \in S : \{a_n\} = \{b_n\}\}$$

称 S 关于 $=$ 关系的商集 $S/_= = \{[\{a_n\}]_= : \{a_n\} \in S\}$ 为实数集，记为 $\mathbb{R}$。实数集中的元素称为实数。

注解

实数是柯西序列关于等于关系的等价类，比如，数列 $a_n = \frac{1}{n},\ n \geq 1$ 和数列 $b_n = \frac{1}{n^2},\ n \geq 1$ 是不同的柯西序列，但它们满足等于关系，属于同一个等价类 $[\{a_n\}]_= = [\{b_n\}]_=$，表示同一个实数 0。再比如，在例 3.3.1 中，数列 a_n 和数列 a'_n 是不同的柯西序列，但它们满足等于关系，属于同一个等价类 $[\{a_n\}]_= = [\{a'_n\}]_=$，表示同一个实数 $\sqrt{2}$。全体有理数可以嵌入到实数集中，即 $\forall q \in \mathbb{Q}$，有 $q = [\{q, q, q, \cdots\}]_= \in \mathbb{R}$。例如，$a_0 = 1, a_2 = 1, a_3 = 1, \cdots$ 和 $b_0 = 0, b_2 = 0.9, b_3 = 0.999, \cdots$ 都表示同一个实数 1。

定义 3.3.5 (实数加法 Addition of Real Numbers)**.** 设 $[\{a_n\}]_=, [\{b_n\}]_= \in \mathbb{R}$，定义加法为

$$[\{a_n\}]_= + [\{b_n\}]_= = [\{a_n + b_n\}]_=$$

命题 3.3.1. 实数加法的定义是良定义（*Well-defined*）的，即不依赖于代表元的选取，而且是封闭的。

证明. 先证明实数加法的封闭性，任意两个实数相加依然是实数。因为 $\{a_n\}, \{b_n\}$ 是柯西序列，根据柯西序列的定义，任意有理数 $\epsilon > 0$，都存在一个正整数 N_a，使得当 $m, n > N_a$ 时，有 $|a_m - a_n| \leq \epsilon/2$；同理，存在一个正整数 N_b，使得当 $m, n > N_b$ 时，有 $|b_m - b_n| \leq \epsilon/2$；设序列 $\{c_n\} = \{a_n + b_n\}$，令 $N = \max(N_a, N_b)$，则当 $m, n > N$ 时，有

$$\begin{aligned} |c_m - c_n| &= |a_m + b_m - (a_n + b_n)| \\ &= |(a_m - a_n) + (b_m - b_n)| \\ &\leq |a_m - a_n| + |b_m - b_n| \\ &\leq \varepsilon/2 + \varepsilon/2 = \varepsilon \end{aligned}$$

所以 $\{c_n\}$ 是柯西序列。
再证明实数加法与实数代表元的选择无关。设任意与 $\{a_n\}, \{b_n\}$ 等价的柯西序列分别为 $\{a'_n\}, \{b'_n\}$。那么，对于任意有理数 $\epsilon > 0$，都存在一个正整数 N_a，使得当 $i > N_a$ 时，有 $|a_i - a'_i| \leq \epsilon/2$；同理，存在一个正整数 N_b，使得当 $j > N_b$ 时，有 $|b_j - b'_j| \leq \epsilon/2$。设序列 $\{c'_n\} = \{a'_n + b'_n\}$，令 $N = \max(N_a, N_b)$，则当 $n > N$ 时，有

$$\begin{aligned} |c'_n - c_n| &= |a'_n + b'_n - (a_n + b_n)| \\ &= |(a'_n - a_n) + (b'_n - b_n)| \\ &\leq |a'_n - a_n| + |b'_n - b_n| \\ &\leq \varepsilon/2 + \varepsilon/2 = \varepsilon \end{aligned}$$

所以 $\{c'_n\}$ 与 $\{c_n\}$ 等价，表示同一个实数。 □

定义 3.3.6 (实数乘法 Multiplication of Real Numbers)**.** 设 $[\{a_n\}]_=, [\{b_n\}]_= \in \mathbb{R}$，定义乘法为

$$[\{a_n\}]_= \cdot [\{b_n\}]_= = [\{a_n b_n\}]_=$$

命题 3.3.2. 实数乘法的定义是良定义（*Well-defined*）的，即不依赖于代表元的选取，而且是封闭的。

证明. 先证明实数乘法的封闭性，任意两个实数实数相乘依然是实数。因为 $\{a_n\},\{b_n\}$ 是柯西序列，也是有界序列，存在有理数 M，使得对任意的 n 都有 $|a_n| \leq M$ 和 $|b_n| \leq M$。根据柯西序列的定义，任意有理数 $\epsilon > 0$，都存在一个正整数 N_a，使得当 $m,n > N_a$ 时，有 $|a_m - a_n| \leq \epsilon/2M$；同理，存在一个正整数 N_b，使得当 $m,n > N_b$ 时，有 $|b_m - b_n| \leq \epsilon/2M$；设序列 $\{c_n\} = \{a_n b_n\}$，令 $N = \max(N_a, N_b)$，则当 $m,n > N$ 时，有：

$$\begin{aligned}
|c_m - c_n| &= |a_m * b_m - a_n * b_n| \\
&= |a_m * b_m - a_m * b_n + a_m * b_n - a_n * b_n| \\
&\leq |a_m * b_m - a_m * b_n| + |a_m * b_n - a_n * b_n| \\
&= |a_m||b_m - b_n| + |b_n||a_m - b_n| \\
&\leq M\frac{\varepsilon}{2M} + M\frac{\varepsilon}{2M} \\
&= \varepsilon
\end{aligned}$$

所以 $\{c_n\}$ 是柯西序列。

再证明实数乘法与实数代表元的选择无关。设任意与 $\{a_n\},\{b_n\}$ 等价的柯西序列分别为 $\{a'_n\},\{b'_n\}$。那么，对于任意有理数 $\epsilon > 0$，都存在一个正整数 N_a，使得当 $i > N_a$ 时，有 $|a_i - a'_i| \leq \epsilon/2M$；同理，存在一个正整数 N_b，使得当 $j > N_b$ 时，有 $|b_j - b'_j| \leq \epsilon/2M$。设序列 $\{c'_n\} = \{a'_n b'_n\}$，令 $N = \max(N_a, N_b)$，则当 $n > N$ 时，有

$$\begin{aligned}
|c'_m - c_m| &= |a'_m * b'_m - a_m * b_m| \\
&= |a'_m * b'_m - a'_m * b_m + a'_m * b_m - a_m * b_m| \\
&\leq |a'_m * b'_m - a'_m * b_m| + |a'_m * b_m - a_m * b_m| \\
&= |a'_m||b'_m - b_m| + |b_m||a'_m - a_m| \\
&\leq M\frac{\varepsilon}{2M} + M\frac{\varepsilon}{2M} \\
&= \varepsilon
\end{aligned}$$

所以 $\{c'_n\}$ 与 $\{c_n\}$ 等价，表示同一个实数。 □

定义 3.3.7 (实数加法逆元与减法). 设 $a = [\{a_n\}]_= \in \mathbb{R}$，加法逆元记为 $-a$，使得

$$a + (-a) = [\{0\}]_=$$

那么：

$$-a := [\{-a_n\}]_=$$

设 $a_1, a_2 \in \mathbb{R}$, 实数的减法定义为：

$$a_1 - a_2 = a_1 + (-a_2)$$

定义 3.3.8 (实数乘法逆元与除法). 设 $a = [\{a_n\}]_= \in \mathbb{R}$，且 $a \neq 0$，乘法逆元记为 a^{-1}，使得

$$a \cdot a^{-1} = [\{1\}]_=$$

那么：

$$a^{-1} := [\{a_n^{-1}\}]_=$$

设 $a_1, a_2 \in \mathbb{R}$, $a_2 \neq 0$, 实数的除法定义为：

$$a_1/a_2 = a_1 \cdot a_2^{-1}$$

命题 3.3.3 (实数代数运算的性质). 设 $a,b,c\in\mathbb{R}$，则实数的代数运算具有以下性质：

1. 交换律：$a+b=b+a$
2. 加法结合律：$(a+b)+c=a+(b+c)$;
3. 加法单位元：存在唯一的实数 0，使得 $a+0=a$;
4. 加法逆元：任意实数 a 存在唯一的实数 $-a$，使得 $a+(-a)=0$;
5. 乘法交换律：$ab=ba$;
6. 乘法结合律：$(ab)c=a(bc)$;
7. 乘法单位元：存在唯一的实数 1，使得 $a\cdot 1=a$;
8. 乘法逆元：任意非零实数 a 存在唯一的实数 a^{-1}，使得 $a\cdot a^{-1}=1$;
9. 乘法对加法的分配律：$a(b+c)=ab+ac$.
10. 乘法零元：$a\cdot 0=0$.

注解

实数的四则运算的定义都是良定义的，即不依赖于代表元的选取，而且是封闭的。实数集和加法乘法一起，构成一个数域，称为实数域，记为 $(\mathbb{R},+,\cdot)$。

定义 3.3.9 (实数的序 Order of Real Numbers). 设 $[\{a_n\}]_=,[\{b_n\}]_=\in\mathbb{R}$，定义序为

$$[\{a_n\}]_=\le[\{b_n\}]_=\iff\exists N,\ \forall n>N,\ a_n\le b_n$$

定义 3.3.10 (实数的绝对值 Absolute Value of Real Numbers). 设 $a\in\mathbb{R}$，定义其绝对值为

$$|a|=\begin{cases}a, & a\ge 0\\ -a, & a<0\end{cases}$$

定义 3.3.11 (实数的距离 Distance of Real Numbers). 设 $a,b\in\mathbb{R}$，定义它们之间的距离为

$$d(a,b)=|a-b|$$

命题 3.3.4 (实数绝对值的性质). 设 $a,b\in\mathbb{R}$，则有：

1. 非负性：$|a|\ge 0$，且 $|a|=0\iff a=0$;
2. 乘法：$|ab|=|a||b|$;
3. 三角不等式：$|a+b|\le|a|+|b|$.
4. 反三角不等式：$||a|-|b||\le|a-b|$.
5. 距离的非负性：$d(a,b)\ge 0$，且 $d(a,b)=0\iff a=b$;
6. 距离的对称性：$d(a,b)=d(b,a)$;
7. 距离的三角不等式：$d(a,c)\le d(a,b)+d(b,c)$.

注解

二元组 $(\mathbb{R}, \leq)$ 构成一个全序集，实数绝对值运算同样满足非负性、三角不等式、反三角不等式等，二元组 $(\mathbb{R}, d)$ 构成一个度量空间。

3.3.2 实数集的完备性

实数相比有理数最大的区别是“连续”，准确的说，实数集是完备的。实数的完备性使得极限运算在实数集上是良定义的。

定义 3.3.12 (实数序列 sequence of real numbers)**.** 函数 $f : \mathbb{N} \to \mathbb{R}$ 为实数序列，记为 $\{x_n\}$，其中 $x_n = f(n),\ n \geq m, \cdots$。

定义 3.3.13 (实数柯西序列 Cauchy sequence of real numbers)**.** 设 $\{x_n\}$ 是实数序列。$\{x_n\}$ 是柯西序列，当且仅当，对于任意给定的实数 $\epsilon > 0$，都存在一个正整数 N，使得当 $i, j > N$ 时，有

$$d(x_i, x_j) = |x_i - x_j| \leq \epsilon$$

定义 3.3.14 (有界序列 bounded sequence of real numbers)**.** 设 $\{x_n\}$ 是实数序列。如果存在实数 $M > 0$，使得对任意的 n 都有 $|x_n| \leq M$，则称 $\{x_n\}$ 是有界序列。

定理 3.3.2. 实数柯西序列都是有界序列；有界序列不一定是柯西序列。

注解

实数序列的定义同有理数序列，不过序列是由实数构成的。类似地可以定义实数柯西序列和有界序列。一个实数序列是柯西序列蕴含该序列是有界序列。

定义 3.3.15 (收敛序列与序列极限 Convergent Sequence and Limit of Sequence)**.** 设 $\{x_n\}$ 是实数序列。$\{x_n\}$ 收敛于实数 x，记为 $\lim_{n\to\infty} x_n = x$，当且仅当，对于任意给定的实数 $\epsilon > 0$，都存在一个正整数 N，使得当 $n > N$ 时，有

$$d(x_n, x) = |x_n - x| \leq \epsilon$$

此时，称 x 为序列 $\{x_n\}$ 的极限。

命题 3.3.5. 收敛序列的极限是唯一。

证明. 使用反证法，假设实数收敛序列 $\{x_n\}$ 收敛于极限 x 和 y。那么设 $\epsilon = \frac{|x-y|}{2} > 0$，根据收敛序列的定义，存在正整数 N_1，使得当 $n > N_1$ 时，有 $|x_n - x| < \epsilon$；同理，存在正整数 N_2，使得当 $n > N_2$ 时，有 $|x_n - y| < \epsilon$；令 $N = \max(N_1, N_2)$，则当 $n > N$ 时，有

$$\begin{aligned} |x - y| &= |x - x_n + x_n - y| \\ &\leq |x - x_n| + |x_n - y| \\ &< \epsilon + \epsilon = 2\epsilon = |x - y| \end{aligned}$$

这说明 $|x - y| < |x - y|$，矛盾，所以假设不成立，极限是唯一的。 □

下面不加证明的给出实数集完备性的两个等价定理。

定理 3.3.3 (实数集的完备性 Completeness of Real Numbers)**.** 实数集具有完备性，当且仅当，所有的实数柯西序列都是收敛实数序列。

定理 3.3.4 (柯西收敛准则 Cauchy Convergence Criterion)**.** 实数序列 $\{x_n\}$ 收敛的充分必要条件是：对于任给的实数 $\epsilon > 0$，都存在正整数 N，使得当 $i, j > N$ 时，有 $d(x_i, x_j) = |x_i - x_j| \leq \epsilon$。

注解

柯西收敛准则和实数完备性是两条条等价的定理，它们说明了实数集和有理数集的本质区别。稠密的有理数集对极限运算不封闭，一个有理数序柯西序列的极限可能不是有理数，例 3.3.1 中的两个柯西序列在有理数集上没有极限，但在实数集上都收敛于 $\sqrt{2}$。完备性保证了有理数柯西列一定能收敛到一个实数，而不会收敛到一个不属于实数集的元素。换句话说，在实数集中，柯西序列与收敛序列是等价的，实数集对极限运算封闭。

3.3.3 实数的幂运算

定义 3.3.16 (实数的自然数次幂)**.** 设 $x \in \mathbb{R}$ 是实数，$n \in \mathbb{N}$ 是自然数，x 的 n 次幂记为 x^n，递归地定义：

1. $x^0 = 1$
2. $x^n = x \cdot x^{n-1},\ n \geq 1$

定义 3.3.17 (实数的负整数次幂)**.** 设 $x \neq 0 \in \mathbb{R}$，$n \in \mathbb{N}^+$ 是正整数，x 的 $-n$ 次幂记为 x^{-n}，定义

$$x^{-n} = \frac{1}{x^n}$$

定义 3.3.18 (正实数的真分数次幂)**.** 设 $x > 0 \in \mathbb{R}$ 是正实数，$n \in \mathbb{N}^+$ 是正整数，x 的 $\frac{1}{n}$ 次幂记为 $x^{\frac{1}{n}}$，定义

$$x^{\frac{1}{n}} = \sup\{y \in \mathbb{R} : y \geq 0,\ y^n \leq x\}$$

$x^{\frac{1}{n}}$ 称为 x 的n **次方根**，也常记为 $\sqrt[n]{x}$。

命题 3.3.6 (n 次方根的存在性)**.** 设 $x > 0 \in \mathbb{R}$ 是正实数，$n \in \mathbb{N}^+$ 是正整数，则 x 的 n 次方根 $x^{\frac{1}{n}}$ 存在且唯一。

定义 3.3.19 (正实数的有理数次幂)**.** 设 $x > 0 \in \mathbb{R}$ 是正实数，$m \in \mathbb{Z}$ 是整数，$n \in \mathbb{N}^+$ 是正整数，x 的 $\frac{m}{n}$ 次幂记为 $x^{\frac{m}{n}}$，定义

$$x^{\frac{m}{n}} = (x^{\frac{1}{n}})^m$$

定理 3.3.5 (正实数的有理数次幂的性质)**.** 设 $x, y > 0 \in \mathbb{R}$，$m, n \in \mathbb{N}^+$，$p, q \in \mathbb{Q}$ 则

1. $(x^{\frac{1}{n}})^n = x$
2. $x^{\frac{1}{m}} = (x^{\frac{1}{n}})^{\frac{n}{m}}$

3. $(xy)^p = x^p y^p$
4. $(x^p)^q = x^{pq}$
5. $x^p \cdot x^q = x^{p+q}$
6. $x^p / x^q = x^{p-q}$
7. 如果 $y = x^{1/n}$，那么 $x = y^n$
8. 若 $x \leq y$，则 $x^{\frac{1}{n}} \leq y^{\frac{1}{n}}$

注解

实数的有理数次幂要求底数为正实数，指数可以是任意有理数。在实数集中，负实数的有理数次幂没有定义，比如 $(-1)^{\frac{1}{2}}$ 是无意义的，也即不存在实数 x，使得 $x^2 = -1$。这说明实数集对开方运算不封闭，需要再次扩充数集，得到复数集。

3.4 复数

复数的引入源自解三次代数方程的负数平方根问题。在实数集中，一元二次次方程 $x^2+1=0$ 无解。如果，令 $i^2=-1$，称为虚数单位（Imaginary Unit），定义一个全新的数集——复数集，那么任何一个代数方程在复数集中都有解，并且解的个数恰好等于方程的次数，该结论称为代数基本定理。

定理 3.4.1 (代数基本定理 Fundamental Theorem of Algebra)**.** 每一个次数为 n 的非零单变量复系数多项式 $P(z)=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0,\ a_n\neq 0$ 在复数域上恰有 n 个根（重根按重数计算）。

3.4.1 复数的定义

定义 3.4.1 (复数 Complex Number)**.** 有序对 $(a,b)\in\mathbb{R}^2$ 记为 $a+bi$，其中，

1. 约定：$i^2=-1$;
2. 等于关系：$a+bi=c+di\Leftrightarrow a=c\wedge b=d$;
3. 等价类：$[a+bi]_{=}=\{(c,d)\in\mathbb{R}^2:a+bi=c+di\}$;

称 $\mathbb{R}^2$ 关于 $=$ 关系的商集 $\mathbb{R}^2/_{=}=\{[a+bi]_{=}:a+bi\in\mathbb{R}^2\}$ 为复数集，记为 $\mathbb{C}$。复数集中的元素称为复数。

注解

复数同样是一个等价类，但集合中只有一个有序对 (a,b)，所以可以直接用 $a+bi$ 来表示复数。在复数中，实数 a 称为复数的实部（Real Part），记为 $\mathrm{Re}(a+bi)=a$；实数 b 称为复数的虚部（Imaginary Part），记为 $\mathrm{Im}(a+bi)=b$。全体实数可以嵌入到复数集中，即 $\forall a\in\mathbb{R}$，有 $a=a+0i\in\mathbb{C}$。

定义 3.4.2 (复数的加法与乘法 Addition and Multiplication of Complex Numbers)**.** 设 $z_1=a+bi,\ z_2=c+di\in\mathbb{C}$，定义复数的加法与乘法如下：

1. 加法：$z_1+z_2=(a+c)+(b+d)i$;
2. 乘法：$z_1\cdot z_2=(ac-bd)+(ad+bc)i$.

注解

复数加法和乘法是良定义的，即不依赖于代表元的选取，而且是封闭的。

定义 3.4.3 (复数的加法逆元与减法)**.** 设 $z=a+bi\in\mathbb{C}$，则复数的加法逆元记为 $-z$，使得：

$$z+(-z)=0+0i$$

那么

$$-z:=-a-bi$$

设 $z_1 = a_1 + b_1 i,\ z_2 = a_2 + b_2 i \in \mathbb{C}$，复数的减法定义为

$$z_1 - z_2 = z_1 + (-z_2) = (a_1 - a_2) + (b_1 - b_2)i$$

注解

复数的加法逆元是良定义的，任意复数都存在唯一的加法逆元。复数乘法的逆元需要先定义复数的共轭和模。

定义 3.4.4 (复数的共轭 Conjugate of Complex Number)**.** 设 $z = a + bi \in \mathbb{C}$，复数的共轭记为 $\bar{z}$ 或 z^*，定义为

$$\bar{z} = a - bi$$

定义 3.4.5 (复数的模 Modulus of Complex Number)**.** 设 $z = a + bi \in \mathbb{C}$，复数的模记为 $|z|$，定义为

$$|z| = \sqrt{a^2 + b^2}$$

命题 3.4.1 (复数的模与共轭的关系)**.** 设 $z = a + bi \in \mathbb{C}$，则

$$|z|^2 = a^2 + b^2 = z\bar{z}$$

定义 3.4.6 (复数的度量 Metric of Complex Number)**.** 设 $z_1 = a + bi,\ z_2 = c + di \in \mathbb{C}$，定义复数集上的度量为

$$d(z_1, z_2) = |z_1 - z_2| = \sqrt{(a-c)^2 + (b-d)^2}$$

命题 3.4.2 (复数的模的性质)**.** 设 $z_1, z_2, z \in \mathbb{C}$，则复数的模具有以下性质：

1. 非负性：$|z| \geq 0$，且 $|z| = 0 \Leftrightarrow z = 0$;
2. 乘积性：$|z_1 z_2| = |z_1||z_2|$;
3. 三角不等式：$|z_1 + z_2| \leq |z_1| + |z_2|$.
4. 反三角不等式：$||z_1| - |z_2|| \leq |z_1 - z_2|$.
5. 共轭不变性：$|z| = |\bar{z}|$.
6. 度量非负性：$d(z_1, z_2) \geq 0$，且 $d(z_1, z_2) = 0 \Leftrightarrow z_1 = z_2$;
7. 度量对称性：$d(z_1, z_2) = d(z_2, z_1)$;
8. 度量三角不等式：$d(z_1, z_2) \leq d(z_1, z) + d(z, z_2)$.

注解

复数的共轭是复数集上一个自反的双射，任何一个复数都有唯一的共轭复数。复数集没有定义序关系，所以任意两个复数之间没有大小关系。但是，复数定义了模运算，是实数集绝对值运算的推广。复数的度量同样满足非负性、对称性和三角不等式。所以 $(\mathbb{C}, d)$ 是一个度量空间。

定义 3.4.7 (复数的乘法逆元与除法). 设 $z = a + bi \in \mathbb{C},\ z \neq 0 + 0i$，则复数的乘法逆元记为 z^{-1}，使得：

$$zz^{-1} = 1 + 0i$$

那么

$$z^{-1} := \frac{\bar{z}}{|z|^2} = \frac{\bar{z}}{z\bar{z}} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i$$

设 $z_1 = a_1 + b_1 i,\ z_2 = a_2 + b_2 i \in \mathbb{C},\ z_2 \neq 0 + 0i$，复数的除法定义为

$$\begin{aligned}\frac{z_1}{z_2} = z_1 z_2^{-1} &= \frac{z_1 \cdot \bar{z_2}}{|z_2|^2} = \frac{z_1 \cdot \bar{z_2}}{z_2 \bar{z_2}} \\ &= \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + \frac{b_1 a_2 - a_1 b_2}{a_2^2 + b_2^2} i\end{aligned}$$

命题 3.4.3 (复数代数运算的性质). 设 $z_1, z_2, z_3, z \in \mathbb{C}$，则

1. 加法交换律：$z_1 + z_2 = z_2 + z_1$;
2. 加法结合律：$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$;
3. 加法单位元：$z + 0 = z$;
4. 加法逆元：任意复数 z 都有唯一的加法逆元 $-z$，使得 $z + (-z) = 0$;
5. 加法共轭：$\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2}$;
6. 乘法交换律：$z_1 z_2 = z_2 z_1$;
7. 乘法结合律：$(z_1 z_2) z_3 = z_1 (z_2 z_3)$;
8. 乘法单位元：$z \cdot 1 = z$;
9. 乘法零元：$z \cdot 0 = 0$;
10. 乘法逆元：任意非零复数 z 都有唯一的乘法逆元 z^{-1}，使得 $zz^{-1} = 1$;
11. 乘法对加法的分配律：$z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$.
12. 乘法共轭性：$\overline{z_1 z_2} = \bar{z_1}\bar{z_2}$.

3.4.2 复数集的完备性

定义 3.4.8 (复数柯西序列 Cauchy Sequence of Complex Numbers). 设 $\{z_n = a_n + b_n i\}$ 是复数集 $\mathbb{C}$ 上的一个序列，如果对任意的 $\epsilon > 0$，都存在正整数 N，使得当 $m, n > N$ 时，有

$$d(z_n, z_m) < \epsilon$$

则称 $\{z_n\}$ 是复数集 $\mathbb{C}$ 上的一个柯西序列。

命题 3.4.4. 一个复数序列 $\{z_n = a_n + b_n i\}$ 是柯西序列，当且仅当，其实部序列 $\{a_n\}$ 和虚部序列 $\{b_n\}$ 都是柯西序列。

注解

复数柯西序列的定义与实数柯西序列的定义完全相同，都是随着序号的增大，序列中任意两项之间的距离可以任意小。

定义 3.4.9 (复数收敛序列与序列极限 Convergent Sequence and Limit of Sequence). 设 $\{x_n\}$ 是复数序列。$\{x_n\}$ 收敛于复数 x，记为 $\lim_{n\to\infty} x_n = x$，当且仅当，对于任意给定的实数 $\epsilon > 0$，都存在一个正整数 N，使得当 $n > N$ 时，有

$$d(x_n, x) = |x_n - x| \leq \epsilon$$

此时，称 x 为序列 $\{x_n\}$ 的极限。

命题 3.4.5. 一个复数序列 $\{z_n = a_n + b_n i\}$ 收敛于复数 $z = a + bi$，当且仅当，$\lim_{n\to\infty} a_n = a$ 且 $\lim_{n\to\infty} b_n = b$。

定理 3.4.2 (复数集的完备性 Completeness of Complex Numbers). 复数集具有完备性，当且仅当，所有的复数柯西序列都是收敛复数序列。

定理 3.4.3 (柯西收敛准则 Cauchy Convergence Criterion). 复数序列 $\{z_n\}$ 收敛的充分必要条件是：对于任给的实数 $\epsilon > 0$，都存在正整数 N，使得当 $i, j > N$ 时，有 $d(z_i, z_j) = |z_i - z_j| \leq \epsilon$。

注解

复数集关于度量 d 是完备的，即任意复数柯西序列在复数集中收敛。复数集的完备性来源于实数集的完备性。

3.4.3 复数的幂运算

定义 3.4.10 (复数的自然数次幂). 设 $z \in \mathbb{C}$ 是复数，$n \in \mathbb{N}$ 是自然数，z 的 n 次幂记为 z^n，递归地定义：

1. $z^0 = 1 + 0i$
2. $z^n = z \cdot z^{n-1},\ n \geq 1$

定义 3.4.11 (复数的负整数次幂). 设 $z \in \mathbb{C},\ z \neq 0$ 是非零复数，$n \in \mathbb{N}^+$ 是正整数，则

$$z^{-n} = (z^{-1})^n = \frac{1}{z^n}$$

定义 3.4.12 (复数的有理数次幂). 设 $z \in \mathbb{C},\ z \neq 0$ 是非零复数，$n \in \mathbb{N}^+$ 是正整数，z 的 $\frac{1}{n}$ 次幂记为 $z^{\frac{1}{n}}$，定义

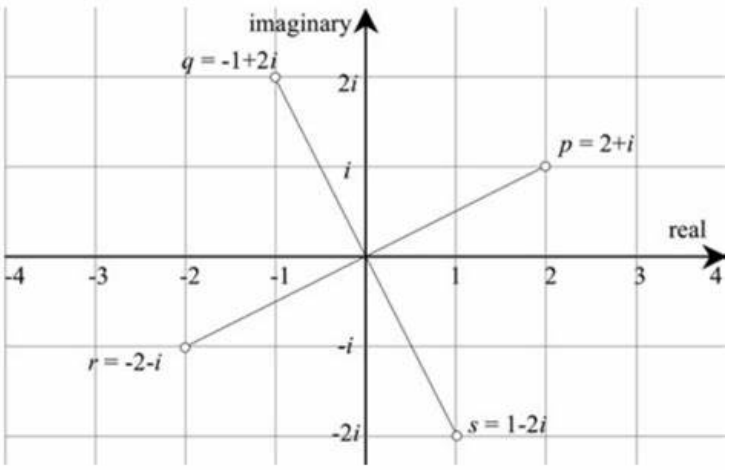


图 3.1: 复平面

3.4.4 复数的三角式

复数 $z = a + bi$ 可以表示为二维平面上的一个点 (a, b)，其中 a 是横坐标，b 是纵坐标。这个二维平面称为复平面（Complex Plane），横轴称为实轴（Real Axis），纵轴称为虚轴（Imaginary Axis）。

定义 3.4.13 (复数的三角式). 复平面上一点用极坐标表示：

$$\begin{cases} x = \rho\cos\varphi \\ y = \rho\sin\varphi \end{cases}$$

得到复数的三角式：

$$z = x + yi = \rho(\cos\varphi + i\sin\varphi) \tag{3.2}$$

其中，

1. $\rho = |z| = \sqrt{x^2 + y^2}$ 为复数的模（*Modulus*）；
2. $\varphi = \arg z$ 为复数的辐角（*Argument*），既正实轴到复数向量的逆时针夹角。一个复数的幅角值不能唯一确定，可以取无穷多个值，并且彼此相差 $2k\pi$, $k \in \mathbb{Z}$。

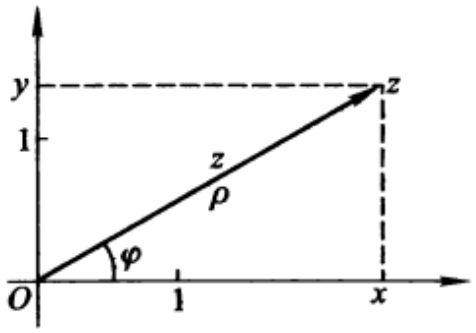


图 3.2: 复数的三角式

定理 3.4.4 (复数乘法的三角式). 设 $z_1 = \rho_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = \rho_2(\cos\varphi_2 + i\sin\varphi_2) \in \mathbb{C}$，则

$$z_1 z_2 = \rho_1\rho_2[\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)]$$

推论 3.4.1 (棣莫弗公式 De Moivre's Theorem). 设 $z = \rho(\cos\varphi + i\sin\varphi) \in \mathbb{C}$，$n \in \mathbb{Z}$，则

$$z^n = \rho^n[\cos(n\varphi) + i\sin(n\varphi)] \tag{3.3}$$

注解

通过复数的三角式，说明复数乘法的几何意义：两个复数相乘，模相乘，幅角相加。将 z_1 的长度拉伸 ρ_2 倍，并逆时针旋转 φ_2 角度，得到 $z_1 z_2$。

3.4.5 复数的指数式

定理 3.4.5 (欧拉公式 Euler's Formula). 设 $\theta \in \mathbb{R}$，则

$$e^{i\theta} = \cos\theta + i\sin\theta \tag{3.4}$$

定义 3.4.14 (复数的指数式). 将欧拉公式 *3.4* 代入复数的三角式 *3.2*，得到复数的指数式：

$$z = \rho e^{i\varphi} \tag{3.5}$$

其中，$\rho = |z|$ 为复数的模，$\varphi = \arg z$ 为复数的辐角。

定理 3.4.6 (复数乘法的指数式). 设 $z_1 = \rho_1 e^{i\varphi_1}$, $z_2 = \rho_2 e^{i\varphi_2} \in \mathbb{C}$，则

$$z_1 z_2 = \rho_1\rho_2 e^{i(\varphi_1+\varphi_2)}$$

定理 3.4.7 (复数除法的指数式). 设 $z_1 = \rho_1 e^{i\varphi_1}$, $z_2 = \rho_2 e^{i\varphi_2} \in \mathbb{C}$, $z_2 \neq 0$，则

$$\frac{z_1}{z_2} = \frac{\rho_1}{\rho_2} e^{i(\varphi_1-\varphi_2)}$$

3.5 四元数

从自然数到复数的扩充非常成功，整数的引入定义了减法，有理数的引入定义了除法，实数的引入定义了极限运算，复数的引入解决了多项式方程的根问题。复数的乘法可以表示二元平面内的旋转，为了表示更高维的旋转，需要引入更高维的数系，而四元数常用来表示三维空间内的旋转。

注解

之所以用四元数表示三维旋转，而不是用三元数，是因为三元数无法定义封闭的乘法运算，所以不能成为一个有用的数系。即便如此，四元数也不得不放弃乘法交换律。八元数甚至无法定义乘法结合律。

3.5.1 四元数的定义

定义 3.5.1 (四元数 Quaternion). 有序数组 $(a,b,c,d)\in\mathbb{R}^4$ 记为 $q=a+bi+cj+dk$，其中，

1. 约定：$i^2=j^2=k^2=ijk=-1$；
2. 等于关系：$a+bi+cj+dk=a'+b'i+c'j+d'k \iff a=a',b=b',c=c',d=d'$；
3. 等价类：$[a+bi+cj+dk]_=\{(e,f,g,h)\in\mathbb{R}^4 : a+bi+cj+dk=e+fi+gj+hk\}$。

称 $\mathbb{R}^4$ 关于 $=$ 关系的商集 $\mathbb{R}^4/_=\{[a+bi+cj+dk]_= : a+bi+cj+dk\in\mathbb{R}^4\}$ 为四元数集，记为 $\mathbb{H}$。四元数集中的元素称为四元数。

注解

四元数是一个等价类，但集合中只有一个有序数组作为代表元，所以可以直接用 $a+bi+cj+dk$ 来表示四元数。在四元数中，实数 a 称为四元数的实部，$bi+cj+dk$ 称为四元数的虚部。四元数可以用一个标量和一个三维向量来表示，即 $q=(a,\mathbf{v})$，其中 $\mathbf{v}=(b,c,d)$。观察四元数定义中的虚部的约定，可得下表：

$\times$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

定义 3.5.2 (四元数的加法). 设 $q_1=a_1+b_1i+c_1j+d_1k,\ q_2=a_2+b_2i+c_2j+d_2k\in\mathbb{H}$，定义四元数的加法：

$$q_1+q_2=(a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k$$

定义 3.5.3 (四元数加法逆元与减法). 设 $q=a+bi+cj+dk\in\mathbb{H}$，四元数的加法逆元记为 $-q$，满足：

$$q+(-q)=0+0i+0j+0k$$

那么

$$-q := -a - bi - cj - dk$$

四元数的减法定义为：

$$q_1 - q_2 = q_1 + (-q_2)$$

定义 3.5.4 (四元数的乘法). 设 $q_1 = a_1 + b_1 i + c_1 j + d_1 k,\ q_2 = a_2 + b_2 i + c_2 j + d_2 k \in \mathbb{H}$，定义四元数的乘法：

$$\begin{aligned} q_1 q_2 &= (a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) \\ &\quad + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\ &\quad + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j \\ &\quad + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k \end{aligned}$$

四元数的乘法还可以写成矩阵的形式：

$$q_1 q_2 = \begin{bmatrix} a_1 & -b_1 & -c_1 & -d_1 \\ b_1 & a_1 & -d_1 & c_1 \\ c_1 & d_1 & a_1 & -b_1 \\ d_1 & -c_1 & b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{bmatrix}$$

如果用 $q_1 = (a_1, \mathbf{v}_1),\ q_2 = (a_2, \mathbf{v}_2)$ 来表示四元数，则有：

$$q_1 q_2 = (a_1 a_2 - \mathbf{v}_1 \cdot \mathbf{v}_2, a_1 \mathbf{v}_2 + a_2 \mathbf{v}_1 + \mathbf{v}_1 \times \mathbf{v}_2)$$

其中， $\mathbf{v}_1 \cdot \mathbf{v}_2$ 是三维向量的点积，$\mathbf{v}_1 \times \mathbf{v}_2$ 是三维向量的叉积。

$$\mathbf{v}_1 \cdot \mathbf{v}_2 = b_1 b_2 + c_1 c_2 + d_1 d_2$$

$$\mathbf{v}_1 \times \mathbf{v}_2 = \begin{vmatrix} i & j & k \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{vmatrix} = (c_1 d_2 - d_1 c_2) i + (d_1 b_2 - b_1 d_2) j + (b_1 c_2 - c_1 b_2) k$$

注解

四元数的加法和乘法都是良定义的，即封闭，且与代表元的选择无关。四元数加法逆元是良定义的，任意一个四元数都有唯一的加法逆元。四元数的加法满足交换律和结合律，但乘法不满足交换律，只满足结合律。在定义四元数除法之前，需要先定义四元数的模和共轭。

定义 3.5.5 (四元数的共轭 Conjugate). 设 $q = a + bi + cj + dk \in \mathbb{H}$，四元数的共轭记为 $\bar{q}$ 或 q^*，那么：

$$\bar{q} = a - bi - cj - dk$$

定义 3.5.6 (四元数的模 Modulus). 设 $q = a + bi + cj + dk \in \mathbb{H}$，四元数的模记为 $|q|$，那么：

$$|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

命题 3.5.1 (四元数的共轭与模的关系). 设 $q = a + bi + cj + dk \in \mathbb{H}$，那么：

$$q\bar{q} = \bar{q}q = |q|^2$$

定义 3.5.7 (四元数的度量). 设 $q_1, q_2 \in \mathbb{H}$，定义四元数的度量：

$$d(q_1, q_2) = |q_1 - q_2|$$

定义 3.5.8 (四元数的逆元与除法). 设 $q = a + bi + cj + dk \in \mathbb{H},\ q \neq 0$，四元数的逆元记为 q^{-1}，满足：

$$qq^{-1} = q^{-1}q = 1$$

由此可得：

$$q^{-1} = \frac{\bar{q}}{|q|^2} = \frac{\bar{q}}{q\bar{q}} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

设 $q_1, q_2 \in \mathbb{H},\ q_2 \neq 0$，四元数的除法定义为：

$$q_1/q_2 = q_1 q_2^{-1} = \frac{q_1\bar{q_2}}{q_2\bar{q_2}}$$

3.5.2 四元数与旋转

定义 3.5.9 (单位四元数 Unit Quaternion). 设 $q = a + bi + cj + dk \in \mathbb{H}$，如果 $|q| = 1$，则称 q 为单位四元数。

3.5.3 对偶四元数

定义 3.5.10 (对偶四元数 Dual Quaternion). 有序数组 $(a, b, c, d, e, f, g, h) \in \mathbb{R}^8$ 记为 $Q = a + bi + cj + dk + \epsilon(e + fi + gj + hk)$，其中，

1. 约定：$i^2 = j^2 = k^2 = ijk = -1,\ \epsilon^2 = 0,\ \epsilon \neq 0$;
2. 等于关系：$a + bi + cj + dk + \epsilon(e + fi + gj + hk) = a' + b'i + c'j + d'k + \epsilon(e' + f'i + g'j + h'k)$

$$\iff a = a', b = b', c = c', d = d', e = e', f = f', g = g', h = h'$$

3. 等价类：$[a + bi + cj + dk + \epsilon(e + fi + gj + hk)]_= = \{(l, m, n, o, p, q, r, s) \in \mathbb{R}^8 : a + bi + cj + dk + \epsilon(e + fi + gj + hk) = l + mi + nj + ok + \epsilon(p + qi + rj + sk)\}$。

称 $\mathbb{R}^8$ 关于 $=$ 关系的商集 $\mathbb{R}^8/_= =$ 为对偶四元数集，记为 $\mathbb{DQ}$。对偶四元数集中的元素称为对偶四元数。

注解

对偶四元数可以表示三维空间中任何刚体变换，包括旋转和平移。根据四元数虚部的约定，可得下表：

$\times$	1	i	j	k	ϵ	ϵi	ϵj	ϵk
1	1	i	j	k	ϵ	ϵi	ϵj	ϵk
i	i	-1	k	$-j$	ϵi	$-\epsilon$	ϵk	$-\epsilon j$
j	j	$-k$	-1	i	ϵj	$-\epsilon k$	$-\epsilon$	ϵi
k	k	j	$-i$	-1	ϵk	ϵj	$-\epsilon i$	$-\epsilon$
ϵ	ϵ	ϵi	ϵj	ϵk	0	0	0	0
ϵi	ϵi	$-\epsilon$	ϵk	$-\epsilon j$	0	0	0	0
ϵj	ϵj	$-\epsilon k$	$-\epsilon$	ϵi	0	0	0	0
ϵk	ϵk	ϵj	$-\epsilon i$	$-\epsilon$	0	0	0	0

Chapter 4

抽象代数

4.1 群

4.1.1 群的定义

定义 4.1.1 (群 Group). 设 G 是一个非空集合，$*$ 是定义在 G 上的一个二元运算，如果对任意的 $a,b,c \in G$ 都满足以下四个条件：

1. 封闭性：$a*b \in G$;
2. 结合律：$(a*b)*c = a*(b*c)$;
3. 存在单位元：存在 $e \in G$，使得对任意的 $a \in G$ 都有 $e*a = a*e = a$;
4. 存在逆元：对任意的 $a \in G$，都存在 $b \in G$，使得 $a*b = b*a = e$，其中 e 是单位元。

那么称 $(G,*)$ 是一个群，简称群 G。

定义 4.1.2 (阿贝尔群 Abelian Group). 如果一个群 $(G,*)$，任意的 $a,b \in G$ 还满足：

1. 交换律：$a*b = b*a$,

那么称 $(G,*)$ 是一个阿贝尔群或交换群（*Commutative Group*）。

注解

群的四条性质称为群公理。如果只满足前两条性质，那么称为半群（Semigroup）。如果只满足前三条性质，那么称为幺半群（Monoid）。只含有单位元的群 $G = \{e\}$ 称为平凡群（Trivial Group），反之为非平凡群（Non-trivial Group）。比如，整数集 $\mathbb{Z}$ 关于加法构成一个阿贝尔群 $(\mathbb{Z},+)$，称为整数加群; $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ 表示自然数的 n 的整数被构成的集合，$(n\mathbb{Z},+)$ 是一个阿贝尔群; 去零实数集 $\mathbb{R}\setminus\{0\}$ 关于乘法也构成一个阿贝尔群 $(\mathbb{R}\setminus\{0\},*)$，称为去零实数乘群。

定义 4.1.3 (群的阶). 设 $(G,*)$ 是一个群，如果 G 是有限集，那么称 G 的元素个数为群的阶，记为 $|G|$。如果 G 是无限集，那么称 G 的阶为无穷，记为 $|G| = \infty$。

命题 4.1.1 (群运算的性质). 设 $(G,*)$ 是一个群，$a,b,c\in G$，那么：

1. 单位元是唯一的；
2. 逆元是唯一的；
3. $(a^{-1})^{-1}=a$；
4. $(a*b)^{-1}=b^{-1}*a^{-1}$。
5. 左消去律：如果 $a*b=a*c$，那么 $b=c$；
6. 右消去律：如果 $b*a=c*a$，那么 $b=c$。

定义 4.1.4 (子群 Subgroup). 设 $(G,*)$ 是一个群，$H\subseteq G$，如果 H 本身也是一个群，那么称 H 是 G 的子群，记为 $H\leq G$。$\{e\}$ 和 G 都是 G 的子群，称为平凡子群（*Trivial Subgroup*），其他的子群称为非平凡子群（*Non-trivial Subgroup*）。

定理 4.1.1 (子群判定定理). 设 $(G,*)$ 是一个群，$H\subseteq G$，如果 H 是 G 的子群，当且仅当，

1. $e\in H$
2. 对任意的 $a,b\in H$，都有 $a*b^{-1}\in H$

注解

子群是群的一个重要概念，子群也是一个群，且子群的运算与原群的运算相同。子群判定定理给出了判定一个子集是否为子群的充分必要条件。交换群的子群也是交换群。

定义 4.1.5 (群同态与群同构 Group Homomorphism and Isomorphism). 设 $(G,*)$ 和 $(H,\cdot)$ 是两个群，映射 $f:G\to H$ 称为从 G 到 H 的一个群同态，当且仅当，对任意的 $a,b\in G$，都有

$$f(a*b)=f(a)\cdot f(b)$$

如果 f 是单射，则称 f 为**单同态 *Monomorphism***；如果 f 是满射，则称 f 为**满同态 *Epimorphism***；如果 f 是双射，则称 f 为**群同构 *Isomorphism***，两个同构的群记为 $G\cong H$。

定义 4.1.6 (群同态的核 Kernel). 设 $(G,*)$ 和 $(H,\cdot)$ 是两个群，映射 $f:G\to H$ 是从 G 到 H 的一个群同态，那么称

$$\ker f=\{g\in G:f(g)=e_H\}$$

为群同态 f 的核，其中 e_H 是群 H 的单位元。

命题 4.1.2 (群同态的性质). 设 $(G,*)$ 和 $(H,\cdot)$ 是两个群，映射 $f:G\to H$ 是从 G 到 H 的一个群同态，那么：

1. $f(e_G)=e_H$，其中 e_G 和 e_H 分别是 G 和 H 的单位元
2. 对任意的 $a\in G$，都有 $f(a^{-1})=(f(a))^{-1}$
3. $\ker f\leq G$

注解

群同态是保持群结构的映射，还将单位元与单位元对应、逆元与逆元对应；而群同构还将两个群的所有元素一一对应起来，说明它们在群结构上是完全相同的。如果仅仅研究群的结构，那么同构的群可以看成是同一个群。群同态的核表示与另一个群单位元对应的群元素的集合，它是原群的一个子群。

定义 4.1.7 (群的直和 Direct Sum)**.** 设 $(A,\circ)$ 和 $(B,*)$ 是两个群，定义集合：

$$A\oplus B:=\{(a,b)\in A\times B:a\in A,b\in B\}$$

在 $A\oplus B$ 上定义二元运算：

$$(a_1,b_1)+(a_2,b_2)=(a_1\circ a_2,b_1*b_2)$$

那么 $(A\oplus B,+)$ 满足群的四条公理：

1. 封闭性：$\forall(a_1,b_1),(a_2,b_2)\in A\oplus B$，都有 $(a_1,b_1)+(a_2,b_2)=(a_1\circ a_2,b_1*b_2)\in A\oplus B$；
2. 结合律：$\forall(a_1,b_1),(a_2,b_2),(a_3,b_3)\in A\oplus B$，都有

$$((a_1,b_1)+(a_2,b_2))+(a_3,b_3)=(a_1\circ(a_2\circ a_3),b_1*(b_2*b_3))=(a_1,b_1)+((a_2,b_2)+(a_3,b_3))$$

3. 单位元：(e_A,e_B)，其中 e_A 和 e_B 分别是 A 和 B 的单位元；
4. 存在逆元：$\forall(a,b)\in A\oplus B$，都有 $(a,b)^{-1}=(a^{-1},b^{-1})$。

那么 $(A\oplus B,+)$ 是一个群，称为群 A 和群 B 的直和。类似地，可以定义有限多个群的直和：

$$\bigoplus_{i=1}^{n}G_i:=G_1\oplus G_2\oplus\cdots\oplus G_n$$

$(\bigoplus_{i=1}^{n}G_i,+)$ 也是一个群，称为群 $G_1,G_2,\ldots,G_n$ 的直和。

注解

群的直和是通过将多个群的元素组合成有序对来构造的新群。

定义 4.1.8 (群作用 Group Action)**.** 设 $(G,*)$ 是一个群，X 是一个非空集合，函数 $f:G\times X\to X$ 称为群作用，当且仅当，

1. 单位元不动：$\forall x\in X,\ f(e,x)=x$，其中 e 是 G 的单位元；
2. 结合律：$\forall g_1,g_2\in G,\ \forall x\in X,\ f(g_1*g_2,x)=f(g_1,f(g_2,x))$

定义 4.1.9 (轨道 Orbit)**.** 设 $(G,*)$ 是一个群，X 是一个非空集合，定义集合：

$$\mathrm{Orb}(x):=\{f(g,x):g\in G\},\quad\forall x\in X$$

称为轨道。表示在群作用下，能够遍历到的 X 中的元素。

注解

群作用是一个非常宽泛的框架，群作用到一个非空集合上，表示把集合中的元素进行某种变换，并且这种变换满足群公理。比如，在微分流形中 $(\mathbb{R},+)$ 群作用到一个微分流形上 M 可以定义一个单参变换群，可以刻画流形上点的平移；轨道 $\mathrm{Orb}(x)$ 表示一条 M 上一条光滑的曲线。

4.1.2 幂运算与循环群

定义 4.1.10 (群元素的自然数次幂运算). 设 $(G,*)$ 是一个群，$a\in G$，则 a 的自然数次幂运算定义为：

1. $a^0=e$;
2. $a^n=a^{n-1}*a,\ n>0$

定义 4.1.11 (群元素的负整数次幂运算). 设 $(G,*)$ 是一个群，$n\in\mathbb{N}^+$ 是正整数，$a\in G$ 的 $-n$ 次幂记为 a^{-n}，定义

$$a^{-n}=(a^n)^{-1}=(a^{-1})^n$$

命题 4.1.3 (群元素的整数次幂运算的性质). 设 $(G,*)$ 是一个群，$m,n\in\mathbb{Z}$，$a\in G$，那么：

1. $a^{m+n}=a^m*a^n$;
2. $(a^m)^n=a^{mn}$;
3. 如果 $(G,*)$ 是阿贝尔群，那么 $(a*b)^n=a^n*b^n$

注解

整数加群 $(\mathbb{Z},+)$ 元素的整数次幂运算就是整数的乘法运算。去零实数乘群 $(\mathbb{R}\setminus\{0\},*)$ 元素的整数次幂运算就是实数的乘方运算。

定义 4.1.12 (循环群 Cyclic Group). 设 $(G,*)$ 是一个群，$a\in G$，如果 $G=\{a^n:n\in\mathbb{Z}\}$，那么称 G 是由 a 生成的循环群，记为 $\langle a\rangle$。a 称为循环群的生成元。

定义 4.1.13 (模 n 剩余类加群). 设 $\mathbb{Z}$ 是整数集，设等价关系：

$$\forall a,b\in\mathbb{Z},\ a\equiv b\iff a\mod n=b\mod n$$

称为同余关系。等价类：

$$[a]=\{b\in\mathbb{Z}:b\equiv a\}$$

也就与 a 同余的整数划到同一个等价类中。令 $\mathbb{Z}_n=\{[0],[1],\dots,[n-1]\}$，称为模 n 剩余类集合。定义加法运算：

$$[a]+[b]=[a+b]$$

那么 $(\mathbb{Z}_n,+)$ 是一个群，称为模 n 剩余类加群。

命题 4.1.4 (循环群的性质). 设 $(G,*)$ 是一个循环群，$a\in G$，是生成元，那么：

1. $(G, *)$ 是阿贝尔群；
2. 循环群的生成元不止一个，如果 a 是生成元，那么 a^{-1} 也是生成元；
3. 循环群的子群也是循环群；
4. 如果 $|G| = n$ 是有限的，那么对任意的 $k \in \mathbb{Z}$，都有 $a^{k+n} = a^k$；n 是循环群的阶，也是生成元的循环周期；
5. 任意一个无限循环群都与 $(\mathbb{Z}, +)$ 同构；任意一个 n 阶有限循环群都与 $(\mathbb{Z}_n, +)$ 同构。

注解

循环群是一种特殊的群，其中的任意一个元素都可由生成元的整数次幂运算得到。比如，整数加群 $(\mathbb{Z}, +)$ 是由 1 或 -1 生成的无限循环群；模 n 剩余加群 $(\mathbb{Z}_n, +)$ 是有限循环群，[1] 和 $[n-1]$ 是它的生成元，且 $|\mathbb{Z}_n| = n$。去零整数乘群 $(\mathbb{Z} \setminus \{0\}, *)$ 不是循环群，因为它没有生成元。

4.1.3 变换与变换群

定义 4.1.14 (变换 Transformation)**.** 设 X 是一个非空集合，映射 $f : X \to X$ 称为 X 上的一个变换，当且仅当，f 是双射。

注解

变换是一种特殊的函数，是集合到自身的双射。比如，旋转和平移都可以看成是几何空间的变换。

定义 4.1.15 (变换群 Transformation Group)**.** 设 X 是一个非空集合，S_X 是 X 上所有变换的集合，定义二元运算为映射的复合，满足：

1. 封闭性：对任意的 $f, g \in S_X$，都有 $f \circ g \in S_X$；
2. 结合律：对任意的 $f, g, h \in S_X$，都有 $(f \circ g) \circ h = f \circ (g \circ h)$；
3. 存在单位元：存在恒等映射 $\mathrm{id}_X \in S_X$，使得对任意的 $f \in S_X$，都有 $\mathrm{id}_X \circ f = f \circ \mathrm{id}_X = f$；
4. 存在逆元：对任意的 $f \in S_X$，都存在 $f^{-1} \in S_X$，使得 $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$。

那么 $(S_X, \circ)$ 是一个群，称为 X 上的变换群。

注解

变换群是一种重要的群，变换群中的元素是集合到自身的双射，群运算是映射的复合。变换群在数学和物理学中有广泛的应用。有限集合上的变换群是对称群，置换群是对称群的子群，其中的变换称为置换。线性群是线性空间上线性变换构成的群，它是线性空间上变换群的子群。

4.1.4 置换与置换群

定义 4.1.16 (置换 Permutation). 设 X 是一个非空有限集合，双射函数 $f : X \to X$ 称为 X 上的一个置换。若 $f(x) = x$ 称为恒等置换，记为 id_X。

> 注解
>
> 在组合数学中，置换指对一组元素重新排列。

定义 4.1.17 (对称群 Symmetric Group). 设 X 是一个非空有限集合，$|X| = n$，设 $\mathrm{Sym}(X)$ 是 X 上所有置换的集合，定义二元运算为映射的复合，满足：

1. 封闭性：对任意的 $f, g \in \mathrm{Sym}(X)$，都有 $f \circ g \in \mathrm{Sym}(X)$；
2. 结合律：对任意的 $f, g, h \in \mathrm{Sym}(X)$，都有 $(f \circ g) \circ h = f \circ (g \circ h)$；
3. 存在单位元：存在恒等映射 $\mathrm{id}_X \in \mathrm{Sym}(X)$，使得对任意的 $f \in \mathrm{Sym}(X)$，都有 $\mathrm{id}_X \circ f = f \circ \mathrm{id}_X = f$；
4. 存在逆元：对任意的 $f \in \mathrm{Sym}(X)$，都存在 $f^{-1} \in \mathrm{Sym}(X)$，使得 $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$。

那么，$(\mathrm{Sym}(X), \circ)$ 是一个群，称为 X 上的一般对称群。

命题 4.1.5. 设 X 是一个非空有限集合，$|X| = n$，那么 X 上的对称群 $(\mathrm{Sym}(X), \circ)$ 的阶为 $|\mathrm{Sym}(X)| = n!$。

定义 4.1.18 (置换群 Permutation Group). 设 X 是一个非空有限集合，$G \leq \mathrm{Sym}(X)$，那么称 G 是 X 上的置换群。

例 4.1.1. 有限集合 $X = \{1, 2, 3\}$ 上的置换有 $3! = 6$ 个，分别是：

$$\mathrm{id}_X = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

那么 $\mathrm{Sym}(X) = \{\mathrm{id}_X, f_1, f_2, f_3, f_4, f_5\}$ 是一个对称群，其中

1. 存在单位元：id_X
2. 存在逆元：
   (a) $\mathrm{id}_X^{-1} = \mathrm{id}_X$
   (b) $f_1^{-1} = f_1$
   (c) $f_2^{-1} = f_2$
   (d) $f_3^{-1} = f_4$
   (e) $f_4^{-1} = f_3$
   (f) $f_5^{-1} = f_5$
3. 结合律：$(f_i \circ f_j) \circ f_k = f_i \circ (f_j \circ f_k),\ i, j, k = 1, 2, 3, 4, 5$

那么 $|\mathrm{Sym}(X)| = |X|! = 6$。其中，$\{\mathrm{id}_X, f_1\}$，$\{\mathrm{id}_X, f_5\}$，$\{\mathrm{id}_X, f_3, f_4\}$ 都是 $\mathrm{Sym}(X)$ 的非平凡子群，是置换群。

4.1.5 线性变换与线性群

定义 4.1.19 (线性变换 Linear Transformation). 设 V 是域 F 上的 n 维线性空间，双射 $L : V \to V$ 称为 V 上的一个线性变换，当且仅当，对任意的 $\mathbf{u}, \mathbf{v} \in V$ 和 $a, b \in F$，都有

$$L(a\mathbf{u} + b\mathbf{v}) = aL(\mathbf{u}) + bL(\mathbf{v})$$

定义 4.1.20 (一般线性群 General Linear Group). 设 V 是域 F 上的 n 维线性空间，$\mathrm{GL}_n(F)$ 是 V 上所有线性变换的集合，定义二元运算为映射的复合，满足：

1. 封闭性：对任意的 $L_1, L_2 \in \mathrm{GL}_n(F)$，都有 $L_1 \circ L_2 \in \mathrm{GL}_n(F)$；
2. 结合律：对任意的 $L_1, L_2, L_3 \in \mathrm{GL}_n(F)$，都有 $(L_1 \circ L_2) \circ L_3 = L_1 \circ (L_2 \circ L_3)$；
3. 存在单位元：存在恒等映射 $\mathrm{id}_V \in \mathrm{GL}_n(F)$，使得对任意的 $L \in \mathrm{GL}_n(F)$，都有 $\mathrm{id}_V \circ L = L \circ \mathrm{id}_V = L$；
4. 存在逆元：对任意的 $L \in \mathrm{GL}_n(F)$，都存在 $L^{-1} \in \mathrm{GL}_n(F)$，使得 $L \circ L^{-1} = L^{-1} \circ L = \mathrm{id}_V$。

那么 $(\mathrm{GL}_n(F), \circ)$ 是一个群，称为 V 上的一般线性群。

注解

在 n 维线性空间中，线性变换可以表示为 $n \times n$ 的可逆矩阵。那么一般线性群 $\mathrm{GL}_n(F)$ 也可以表示为所有 $n \times n$ 可逆矩阵构成的群，群运算为矩阵乘法。一般线性群是线性空间 V 上变换群的子群 $\mathrm{GL}_n(F) \leq S_V$。

定义 4.1.21 (特殊线性群 Special Linear Group). 设 V 是域 F 上的 n 维线性空间，$\mathrm{SL}_n(F)$ 是 V 上所有行列式为 1 的 $n \times n$ 矩阵构成的集合，二元运算为矩阵乘法，那么 $(\mathrm{SL}_n(F), \cdot)$ 是一个群，称为 V 上的特殊线性群。

注解

行列式为 1，说明该线性变换不拉伸空间（在一维空间中能保证长度不变，在二维空间中能保证面积不变，在三维空间中能保证体积不变）。特殊线性群是一般线性群的子群 $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$。

定义 4.1.22 (正交矩阵 Orthogonal Matrix). 设 V 是实数域 $\mathbb{R}$ 上的 n 维线性空间，A 是 V 上的一个 $n \times n$ 矩阵，如果 A 满足

$$A^T A = AA^T = I$$

其中，A^T 是 A 的转置矩阵，那么称 A 是一个正交矩阵。

定义 4.1.23 (正交群 Orthogonal Group). 设 V 是实数域 $\mathbb{R}$ 上的 n 维线性空间，O_n 是 V 上所有正交矩阵构成的集合，二元运算为矩阵乘法，那么 $(\mathrm{O}_n, \cdot)$ 是一个群，称为 V 上的正交群。

定义 4.1.24 (特殊正交群 Special Orthogonal Group). 设 V 是实数域 $\mathbb{R}$ 上的 n 维线性空间，SO_n 是 V 上所有行列式为 1 的正交矩阵构成的集合，二元运算为矩阵乘法，那么 $(\mathrm{SO}_n, \cdot)$ 是一个群，称为 V 上的特殊正交群。

注解

正交矩阵表示的线性变换能保持向量间的夹角不变。正交变换群是一般线性群的子群。特殊正交矩阵表示的旋转变换。特殊正交矩阵群即是特殊线性群的子群，又是正交变换群的子群 $\mathrm{SO}_n \leq \mathrm{O}_n \leq \mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$。

定义 4.1.25 (酉矩阵 Unitary Matrix)**.** 设 V 是复数域 $\mathbb{C}$ 上的 n 维线性空间，A 是 V 上的一个 $n \times n$ 矩阵，如果 A 满足

$$A^\dagger A = AA^\dagger = I$$

其中，$A^\dagger = \overline{A^T}$ 是 A 的共轭转置矩阵，那么称 A 是一个酉矩阵。

定义 4.1.26 (酉群 Unitary Group)**.** 设 V 是复数域 $\mathbb{C}$ 上的 n 维线性空间，U_n 是 V 上所有酉矩阵构成的集合，二元运算为矩阵乘法，那么 $(\mathrm{U}_n, \cdot)$ 是一个群，称为 V 上的酉群。

定义 4.1.27 (特殊酉群 Special Unitary Group)**.** 设 V 是复数域 $\mathbb{C}$ 上的 n 维线性空间，SU_n 是 V 上所有行列式为 1 的酉矩阵构成的集合，二元运算为矩阵乘法，那么 $(\mathrm{SU}_n, \cdot)$ 是一个群，称为 V 上的特殊酉群。

注解

酉矩阵是正交矩阵在复数域上的推广。酉矩阵表示的线性变换能保持复向量间的夹角不变。酉变换群是一般线性群的子群。特殊酉矩阵表示的旋转变换。特殊酉矩阵群即是特殊线性群的子群，又是酉变换群的子群 $\mathrm{SU}_n \leq \mathrm{U}_n \leq \mathrm{SL}_n(\mathbb{C}) \leq \mathrm{GL}_n(\mathbb{C})$。

4.1.6 陪集与群划分

定义 4.1.28 (左陪集 Left Coset)**.** 设 $(G, *)$ 是一个群，$H \leq G$ 是 G 的子群。定义 G 上的等价关系 $\sim$ 为：

$$a \sim b \iff a^{-1}b \in H, \quad \forall a, b \in G$$

等价类：

$$\begin{aligned}
[a]_\sim &= \{x \in G : x \sim a\} = \{x \in G : a^{-1}x \in H\} \\
&= \{x \in G : a^{-1}x = h, h \in H\} \\
&= \{x \in G : x = ah, h \in H\} \\
&= \{ah : h \in H\}
\end{aligned}$$

记为 $aH := [a]_\sim$，称为 H 关于 a 的左陪集。

定义 4.1.29 (左商集 Left Quotient Set)**.** 设 $(G, *)$ 是一个群，$H \leq G$ 是 G 的子群，$a \in G$，那么 G 关于 H 的所有左陪集的集合称为 G 关于 H 的左商集，记为 $(G/H)_l$，即

$$(G/H)_l := \{aH : a \in G\}$$

定义 4.1.30 (右陪集 Right Coset)**.** 设 $(G,*)$ 是一个群，$H \leq G$ 是 G 的子群。定义 G 上的等价关系 $\sim$ 为：

$$a \sim b \iff ab^{-1} \in H, \quad \forall a,b \in G$$

等价类：

$$\begin{aligned}[a]_\sim &= \{x \in G : x \sim a\} = \{x \in G : ax^{-1} \in H\} \\ &= \{x \in G : ax^{-1} = h, h \in H\} \\ &= \{x \in G : x = ha, h \in H\} \\ &= \{ha : h \in H\}\end{aligned}$$

记为 $Ha := [a]_\sim$，称为 H 关于 a 的右陪集。

定义 4.1.31 (右商集 Right Quotient Set)**.** 设 $(G,*)$ 是一个群，$H \leq G$ 是 G 的子群，$a \in G$，那么 G 关于 H 的所有右陪集的集合称为 G 关于 H 的右商集，记为 $(G/H)_r$，即

$$(G/H)_r := \{Ha : a \in G\}$$

例 4.1.2. 整数加群 $(\mathbb{Z},+)$ 关于 $(3\mathbb{Z},+)$ 的所有左陪集：

$$\begin{aligned}0+3\mathbb{Z} &= \{\cdots,-6,-3,0,3,6,\cdots\} \\ 1+3\mathbb{Z} &= \{\cdots,-5,-2,1,4,7,\cdots\} \\ 2+3\mathbb{Z} &= \{\cdots,-4,-1,2,5,8,\cdots\}\end{aligned}$$

$(\mathbb{Z},+)$ 关于 $(3\mathbb{Z},+)$ 的所有左商集：

$$(\mathbb{Z}/3\mathbb{Z})_l = \{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$$

同样可以得到 $(\mathbb{Z},+)$ 关于 $(3\mathbb{Z},+)$ 的所有右陪集：

$$\begin{aligned}3\mathbb{Z}+0 &= \{\cdots,-6,-3,0,3,6,\cdots\} \\ 3\mathbb{Z}+1 &= \{\cdots,-5,-2,1,4,7,\cdots\} \\ 3\mathbb{Z}+2 &= \{\cdots,-4,-1,2,5,8,\cdots\}\end{aligned}$$

$(\mathbb{Z},+)$ 关于 $(3\mathbb{Z},+)$ 的所有右商集：

$$(\mathbb{Z}/3\mathbb{Z})_r = \{3\mathbb{Z}+0, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$$

注解

左（右）陪集将群划分为若干个等价类，这些等价类构成的商集是群 G 的一个划分 Partition。左陪集和右陪集的定义类似，但它们的元素排列顺序不同。一般情况下，左陪集和右陪集不相等，但如果子群是正规子群，那么左陪集和右陪集相等。

命题 4.1.6 (陪集的性质)**.** 设 $(G,*)$ 是一个群，$H \leq G$ 是 G 的子群，$a,b \in G$，那么：

1. 左商集中，$eH = H$
2. 右商集合，$He = H$
3. 左商集中，$\forall a, b \in G\ (aH = bH \leftrightarrow a^{-1}b \in H)$
4. 右商集中，$\forall a, b \in G\ (Ha = Hb \leftrightarrow ba^{-1} \in H)$
5. 左商集中，$\forall a, b \in G\ (a \neq b \rightarrow\ aH \cap bH = \varnothing)$
6. 右商集中，$\forall a, b \in G\ (a \neq b \rightarrow\ Ha \cap Hb = \varnothing)$
7. 存在一个双射 $f : H \to aH$，使得 $\forall h \in H\ (f(h) = ah)$；换句话说，左陪集与子群 H 具有相同的势
8. 存在一个双射 $f : H \to Ha$，使得 $\forall h \in H\ (f(h) = ha)$；换句话说，右陪集与子群 H 具有相同的势
9. 存在一个双射 $f : (G/H)_l \to (G/H)_r$，使得 $\forall a \in G\ (f(aH) = Ha)$；换句话说，左商集和右商集具有相同的势。

定义 4.1.32 (指数 Index)**.** 设 $(G, *)$ 是一个群，$H \leq G$ 是 G 的子群。如果左右配集是有限集，那么左右商集的势称为群 G 关于子群 H 的指数，记为 $[G : H]$，即

$$[G : H] = |(G/H)_l| = |(G/H)_r|$$

定理 4.1.2 (拉格朗日定理 Lagrange's Theorem)**.** 设 $(G, *)$ 是一个有限群，$H \leq G$ 是 G 的子群，那么

$$|G| = [G : H] \cdot |H|$$

证明. 设 H 关于 G 的所有左陪集为 $a_1H, a_2H, \ldots, a_kH$，其中 $k = [G : H]$，那么

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH$$

且 $a_iH \cap a_jH = \varnothing,\ i \neq j$。又因为对任意的 $a \in G$，都有 $|aH| = |H|$，所以

$$|G| = |a_1H| + |a_2H| + \cdots + |a_kH| = k|H| = [G : H] \cdot |H|$$

□

注解

拉格朗日定理说明了有限群的阶与其子群的阶之间的关系。它表明，有限群的阶总是其任意子群的阶的整数倍。在例 4.1.1 中，$H = \{\mathrm{id}_X, f_1\} \leq \mathrm{Sym}(X)$，那么左商集：

$$(\mathrm{Sym}(X)/H)_l = \{H, f_2H, f_3H\} = \{\{\mathrm{id}_X, f_1\}, \{f_2, f_4\}, \{f_3, f_5\}\}$$

那么 $|\mathrm{Sym}(X)| = |H| \cdot |(\mathrm{Sym}(X)/H)_l| = 2 \cdot 3 = 6$。

4.1.7 正规子群与商群

定义 4.1.33 (共轭 Conjugate)**.** 设 $(G,*)$ 是一个群，$a,b\in G$，如果存在 $g\in G$，使得：

$$b=g^{-1}*a*g$$

那么称 b 是 a 的一个共轭。

定义 4.1.34 (正规子群 Normal Subgroup)**.** 设 $(G,*)$ 是一个群。$H\leq G$ 是 G 的正规子群，当且仅当，

$$\forall g\in G,\ \{g^{-1}hg:h\in H\}=H$$

记为 $H\triangleleft G$。

命题 4.1.7. 设 $(G,*)$ 是一个群，$H\leq G$ 是 G 的子群，那么以下命题等价：

1. $H\triangleleft G$
2. $\forall g\in G,\ gHg^{-1}=H$
3. $\forall g\in G,\ gH=Hg$
4. 存在群同态 $f:G\to G'$，使得 $\ker(f)=H$

命题 4.1.8. 所有的交换群的子群都是正规子群。

证明. 设 $(G,*)$ 是一个交换群，$H\leq G$ 是 G 的子群，$\forall g\in G$，那么

$$\begin{aligned}\{g^{-1}*h*g:h\in H\}&=\{h*g^{-1}*g:h\in H\}\\&=\{h*e:h\in H\}=\{h:h\in H\}=H\end{aligned}$$

所以 $H\triangleleft G$。 □

注解

例 4.1.2 中，整数加群 $(\mathbb{Z},+)$ 是交换群，$3\mathbb{Z}\leq\mathbb{Z}$ ，所以 $3\mathbb{Z}\triangleleft\mathbb{Z}$。

定义 4.1.35 (商群 Quotient Group)**.** 设 $(G,*)$ 是一个群，$H\triangleleft G$ 是 G 的正规子群，定义商集：

$$G/H:=(G/H)_l=(G/H)_r=\{aH:a\in G\}=\{Ha:a\in G\}$$

在商集 G/H 上定义二元运算：

$$(aH)\circ(bH)=(a*b)H$$

那么 $(G/H,\circ)$ 满足群的四条公理：

1. 封闭性：$\forall aH,bH\in G/H$，都有 $(aH)\circ(bH)=(a*b)H\in G/H$；
2. 结合律：$\forall aH,bH,cH\in G/H$，都有

$$(aH\circ bH)\circ cH=(a*b)H\circ cH=((a*b)*c)H=(a*(b*c))H=aH\circ(bH\circ cH)$$

3. 单位元：$eH=H$；

4. 存在逆元：$\forall aH \in G/H$，都有 $(aH)^{-1} = a^{-1}H$；

那么 $(G/H, \circ)$ 是一个群，称为 G 关于 H 的商群。

命题 4.1.9 (商群的性质). 设 $(G, *)$ 是一个群，$H \triangleleft G$ 是 G 的正规子群，那么：

1. 如果 G 是有限群，根据拉格朗日定理 *4.1.2*，那么 $|G/H| = [G : H] = |G|/|H|$
2. 如果 G 是交换群，那么 G/H 也是交换群
3. 如果 G 是循环群，那么 G/H 也是循环群

例 4.1.3. 整数加群 $(\mathbb{Z}, +)$ 关于正规子群 $(3\mathbb{Z}, +)$ 的商集为：

$$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

定义加法运算：

$$(a + 3\mathbb{Z}) + (b + 3\mathbb{Z}) = (a + b) + 3\mathbb{Z}$$

满足群的四条公理：

1. 单位元 $0 + 3\mathbb{Z}$
2. 封闭性

$$\begin{aligned}(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) &= 3 + 3\mathbb{Z} = 0 + 3\mathbb{Z}\\ (0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) &= (1 + 3\mathbb{Z})\\ (0 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) &= (2 + 3\mathbb{Z})\end{aligned}$$

3. 结合律

$$\begin{aligned}((1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z})) + (0 + 3\mathbb{Z}) &= (0 + 3\mathbb{Z}) + (0 + 3\mathbb{Z}) = 0 + 3\mathbb{Z}\\ (1 + 3\mathbb{Z}) + ((2 + 3\mathbb{Z}) + (0 + 3\mathbb{Z})) &= (1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = 0 + 3\mathbb{Z}\end{aligned}$$

4. 逆元

$$\begin{aligned}(1 + 3\mathbb{Z})^{-1} &= 2 + 3\mathbb{Z}\\ (2 + 3\mathbb{Z})^{-1} &= 1 + 3\mathbb{Z}\\ (0 + 3\mathbb{Z})^{-1} &= 0 + 3\mathbb{Z}\end{aligned}$$

那么 $(\mathbb{Z}/3\mathbb{Z}, +)$ 是一个群，且是循环群，生成元为 $1 + 3\mathbb{Z}$ 或 $2 + 3\mathbb{Z}$，$|\mathbb{Z}/3\mathbb{Z}| = 3$。

注解

商群是通过将群 G 的元素划分为若干个等价类（即陪集）来构造的新群。商群在群论中有重要的应用，比如在研究群的结构和分类时，商群提供了一种简化问题的方法。

4.1.8 群同态基本定理

定理 4.1.3 (第一同构定理 First Isomorphism Theorem)**.** 设 $(G,*)$ 和 $(G',\cdot)$ 是两个群，$f:G\to G'$ 是一个群同态，那么 $\ker(f)\triangleleft G$，且 $G/\ker(f)\cong \mathrm{im}(f)$。

证明. □

注解

群同态基本定理说明群的任一同态像，同构于原群关于同态核的商群。

定理 4.1.4 (第二同构定理 Second Isomorphism Theorem)**.** 设 $(G,*)$ 是一个群，$H\leq G$ 是 G 的子群，$N\triangleleft G$ 是 G 的正规子群，那么 $HN\leq G$，且 $N\triangleleft HN$，并且

$$H/(H\cap N)\cong HN/N$$

证明. □

定理 4.1.5 (第三同构定理 Third Isomorphism Theorem)**.** 设 $(G,*)$ 是一个群，$H\triangleleft G$ 和 $N\triangleleft G$ 是 G 的两个正规子群，且 $H\subset N$，那么：

$$(G/H)/(N/H)\cong G/N$$

证明. □

注解

群同态基本定理是群论的核心定理，它们建立了群同态、正规子群与商群之间的深刻联系。

4.2 环

4.2.1 环的定义

定义 4.2.1 (环 Ring). 设 R 是一个非空集合，$+$ 和 $\cdot$ 是定义在 R 上的两种代数运算，如果对任意 $a,b,c \in R$，都有

1. $(R,+)$ 是一个交换群；
   (a) 封闭性：$a+b \in R$；
   (b) 结合律：$(a+b)+c = a+(b+c)$；
   (c) 交换律：$a+b = b+a$；
   (d) 存在加法单位元：存在 $0 \in R$，使得对任意 $a \in R$，都有 $a+0 = 0+a = a$；
   (e) 存在加法逆元：对任意 $a \in R$，存在 $-a \in R$，使得 $a+(-a) = (-a)+a = 0$。
2. $(R,\cdot)$ 是一个半群；
   (a) 封闭性：$a \cdot b \in R$；
   (b) 结合律：$(a \cdot b) \cdot c = a \cdot (b \cdot c)$。
3. 乘法对加法的分配律：
   (a) 左分配律：$a \cdot (b+c) = a \cdot b + a \cdot c$；
   (b) 右分配律：$(a+b) \cdot c = a \cdot c + b \cdot c$。

则称 $(R,+,\cdot)$ 是一个**环**，$+$ 和 $\cdot$ 分别称为环的**加法**和**乘法**。如果 $R = \{0\}$，则称 $(R,+,\cdot)$ 是一个**平凡环** ***Trivial Ring***；否则称为**非平凡环** ***Non-trivial Ring***。

定义 4.2.2 (交换环 Commutative Ring). 设 $(R,+,\cdot)$ 为环。如果乘法 $\cdot$ 满足交换律，则称 $(R,+,\cdot)$ 为交换环。

定义 4.2.3 (无零因子环 Ring without Zero Divisors). 设 $(R,+,\cdot)$ 为环。如果对任意 $a,b \in R$，$a \neq 0$，$b \neq 0$，均有 $a \cdot b \neq 0$，则称环 $(R,+,\cdot)$ 为无零因子环。

定义 4.2.4 (含幺环 Ring with identity). 设 $(R,+,\cdot)$ 为环。如果存在乘法单位元 1 并且 $1 \neq 0$，则称环 $(R,+,\cdot)$ 为含幺环。也即 $(R,\cdot)$ 是幺半群，$(R,+,\cdot)$ 为含幺环。

定义 4.2.5 (整环 Integral Domain). 设 $(R,+,\cdot)$ 为含幺环。如果 $(R,+,\cdot)$ 是无零因子环，则称 $(R,+,\cdot)$ 为整环。

定义 4.2.6 (除环 Division Ring). 设 $(R,+,\cdot)$ 为含幺环。如果对任意 $a \in R$，$a \neq 0$，均存在 $a^{-1} \in R$，使得 $a \cdot a^{-1} = a^{-1} \cdot a = e$，则称 $(R,+,\cdot)$ 为除环。也即 $(R \setminus \{0\},\cdot)$ 是群，$(R,+,\cdot)$ 为含幺环。

注解

环在交换群的基础上，配备了第二代数运算—— “乘法”，并且乘法对加法满足分配律。对环乘法附加更多的结构，可以得到交换环、含幺环、整环、除环等。比如，$(\mathbb{Z},+,\cdot)$ 是一个整环；$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ 都是除环。

定义 4.2.7 (子环 Subring)**.** 设 $(R,+,\cdot)$ 为环，$S\subseteq R$。如果 $(S,+,\cdot)$ 也是环，则称 S 为 R 的子环。0 和 R 都是 R 的子环，称为**平凡子环 *Trivial subring***，其他子环称为**非平凡子环 *Non-trivial subring***。

定理 4.2.1 (子环判定定理)**.** 设 $(R,+,\cdot)$ 为环，$S\subseteq R$。则 S 是 R 的子环的充分必要条件是

1. $0\in S$;
2. $\forall a,b\in S$，$a-b\in S$;
3. $\forall a,b\in S$，$a\cdot b\in S$。

注解

子环判定定理相比子群判定定理，多了一个关于乘法封闭性的条件。

定义 4.2.8 (环同态与环同构 Ring Homomorphism and Isomorphism)**.** 设 R 和 R' 为环。函数 $f:R\to R'$ 是一个环同态，当且仅当，

1. $\forall a,b\in R$，$f(a+b)=f(a)+f(b)$;
2. $\forall a,b\in R$，$f(a\cdot b)=f(a)\cdot f(b)$;

如果函数 f 是单射，则称 f 为单同态；如果函数 f 是满射，则称 f 为满同态；如果映射 f 是双射，则称 f 为环同构，记为 $R\cong R'$。

定义 4.2.9 (环同态的核 Kernel of Ring Homomorphism)**.** 设 R 和 R' 为环，$f:R\to R'$ 是一个环同态。定义集合：

$$\ker f:=\{a\in R:f(a)=0\in R'\}$$

称为环同态 f 的核。

命题 4.2.1 (环同态的性质)**.** 设 R 和 R' 为环，$f:R\to R'$ 是一个环同态。则

1. $f(0)=0$;
2. $\forall a\in R$，$f(-a)=-f(a)$;
3. $\ker f\leq R$

注解

环同态与群同态类似，都是保持代数结构的映射。环同态的核表示与另一个环 0 元对应的环元素的集合，它是原环的一个子环。

4.2.2 多项式环

定义 4.2.10 (多项式 Polynomial). 设 $(R,+,\cdot)$ 为环，定义多项式：

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

其中，x 称为变量，$a_i \in R$ 称为系数，$n \in \mathbb{N}$ 称为次数。如果 $a_n \neq 0$ 称为变量 x 的 n 次多项式。如果 $a_0 = a_1 = \cdots = a_n = 0$，称为 *0* 多项式。全体系数在环 R 上的所有多项式的集合，记为 $R[x]$。

定义 4.2.11 (等于关系). 设 $(R,+,\cdot)$ 为环，$f, g \in R[x]$ 相等，记为 $f = g$，当且仅当 f 和 g 的对应系数相等。

定义 4.2.12 (多项式环 Polynomial Ring). 设 $(R,+,\cdot)$ 为环，$R[x]$ 为全体系数在 R 上的所有多项式的集合。定义 $R[x]$ 上的加法和乘法如下：

1. 多项式加法：设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$，其中 $a_i, b_j \in R$，则

$$f(x) + g(x) = \sum_{k=0}^{\max(n,m)} (a_k + b_k)x^k$$

2. 多项式乘法：设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$，其中 $a_i, b_j \in R$，则

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k$$

其中，

1. $a_i = 0$ 当 $i > n$ 或 $i < 0$;
2. $b_j = 0$ 当 $j > m$ 或 $j < 0$;
3. $c_k = \sum_{i=0}^{k} a_i b_{k-i}$。

则 $(R[x],+,\cdot)$ 满足环公理，称为 R 上的多项式环。

4.2.3 理想与商环

环 $(R,+,\cdot)$ 的 $(R,+)$ 是一个交换群，其所有子群都是正规子群。而 $(R,\cdot)$ 只是一个半群，无法定义乘法的正规子群，我们可以类似地定义一种特殊的子环——理想子环，相关的结论与正规子群中的结论有相似性。

定义 4.2.13 (左理想子环 Left Ideal). 设 $(R,+,\cdot)$ 为环，$I \leq R$。I 是 R 的一个左理想子环，当且仅当，$\forall r \in R$，$\forall i \in I$，$r \cdot i \in I$。

定义 4.2.14 (右理想子环 Right Ideal). 设 $(R,+,\cdot)$ 为环，$I \leq R$。I 是 R 的一个右理想子环，当且仅当，$\forall r \in R$，$\forall i \in I$，$i \cdot r \in I$。

定义 4.2.15 (理想子环 Ideal)**.** 设 $(R,+,\cdot)$ 为环，$I \leq R$。I 是 R 的一个理想子环，当且仅当，I 同时是 R 的一个左理想子环和右理想子环。简称为理想。

定义 4.2.16 (理想的等价定义)**.** 设 $(R,+,\cdot)$ 为环，$I \subset S$。I 是 R 的理想，当且仅当，

1. $0 \in I$；
2. $\forall a,b \in I$，$a-b \in I$；
3. $\forall r \in R$，$\forall i \in I$，$r \cdot i \in I$ 且 $i \cdot r \in I$。

命题 4.2.2. 设 $(R,+,\cdot)$ 为环，存在环同态 f，使得 $I = \ker f$，则 I 是 R 的一个理想。

证明. 设 $a,b \in I$，则 $f(a)=0$，$f(b)=0$，所以

$$f(a-b) = f(a) - f(b) = 0 - 0 = 0$$

因此 $a-b \in I$。又设 $r \in R$，$i \in I$，则 $f(i)=0$，所以

$$f(r \cdot i) = f(r) \cdot f(i) = f(r) \cdot 0 = 0$$

因此 $r \cdot i \in I$。同理可证 $i \cdot r \in I$。综上所述，I 是 R 的一个理想。 □

定义 4.2.17 (主理想 Principal Ideal)**.** 设 $(R,+,\cdot)$ 为环，$a \in R$。定义集合：

$$(a) := \{r \cdot a : r \in R\}$$

称为由 a 生成的主理想。也即一个理想中所有的元素都可以依据子环判定定理生成，那么它是主理想。

例 4.2.1. 设 $(\mathbb{Z},+,\cdot)$ 为整数环，$2\mathbb{Z} = \{\ldots,-4,-2,0,2,4,\ldots\}$ 是 $\mathbb{Z}$ 的一个理想。因为

1. $0 \in 2\mathbb{Z}$；
2. $\forall a,b \in 2\mathbb{Z}$，$a-b \in 2\mathbb{Z}$；
3. $\forall r \in \mathbb{Z}$，$\forall i \in 2\mathbb{Z}$，$r \cdot i \in 2\mathbb{Z}$ 且 $i \cdot r \in 2\mathbb{Z}$。

$(\mathbb{Z},+,\cdot)$ 的所有理想都是主理想，并且 $n\mathbb{Z} = (n)$。

> 注解
>
> 理想是环的一个特殊子环，类似于群的正规子群。理想的定义中，除了满足子环的条件外，还要求对任意环元素与理想元素的乘积仍在理想中。如果 R 是交换环，则 I 是 R 的左理想子环、右理想子环和理想是等价的。

定义 4.2.18 (商环 Quotient Ring)**.** 设 $(R,+,\cdot)$ 为环，I 是 R 的理想。定义集合：

$$R/I := \{a + I : a \in R\}$$

其中，$a+I := \{a+i : i \in I\}$。在 R/I 上定义加法和乘法如下：

1. 加法：$\forall a+I, b+I \in R/I$，$(a+I)+(b+I) = (a+b)+I$；

2. 乘法：$\forall a+I, b+I \in R/I$，$(a+I)\cdot(b+I)=(a\cdot b)+I$。

则 $(R/I,+,\cdot)$ 满足环公理，称为 R 关于理想 I 的商环。

命题 4.2.3 (商环的性质). 设 $(R,+,\cdot)$ 为环，I 是 R 的理想，那么：

1. 如果 R 是交换环，则 R/I 也是交换环；
2. 如果 R 是含幺环，并且 $1\in R$ 是乘法单位元，则 R/I 也是含幺环，且 $(1+I)$ 是 R/I 的乘法单位元；
3. 如果 R 是除环，并且 $I\neq\{0\}$，则 R/I 也是除环，那么 $a^{-1}+I$ 是 R/I 中的乘法逆元。

例 4.2.2. 设 $(\mathbb{Z},+,\cdot)$ 为整数环，$2\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个理想。其中，

$$\begin{aligned}
&\vdots\\
-2+2\mathbb{Z}&=\{\ldots,-4,-2,0,2,4,\ldots\}=0+2\mathbb{Z}\\
-1+2\mathbb{Z}&=\{\ldots,-3,-1,1,3,5,\ldots\}=1+2\mathbb{Z}\\
0+2\mathbb{Z}&=\{\ldots,-4,-2,0,2,4,\ldots\}\\
1+2\mathbb{Z}&=\{\ldots,-3,-1,1,3,5,\ldots\}\\
2+2\mathbb{Z}&=\{\ldots,-2,0,2,4,6,\ldots\}=0+2\mathbb{Z}\\
3+2\mathbb{Z}&=\{\ldots,-1,1,3,5,7,\ldots\}=1+2\mathbb{Z}\\
&\vdots
\end{aligned}$$

那么

$$\mathbb{Z}/2\mathbb{Z}=\{0+2\mathbb{Z},1+2\mathbb{Z}\}$$

注解

商环的定义与商群类似，都是将原代数结构划分为若干个等价类，然后在等价类上定义新的代数运算。商环的结构与原环和理想密切相关。

4.2.4 环同态基本定理

定理 4.2.2 (第一同构定理 First Isomorphism Theorem for Rings). 设 $f:R\to R'$ 是一个环同态。那么 $\ker f$ 是 R 的一个理想，并且 $R/\ker f\cong \mathrm{Im} f$。

证明. □

注解

环同态基本定理与群同态基本定理类似，都是通过同态映射将原代数结构与其像联系起来。环同态基本定理说明环的任一同态像，同构于原环关于同态核的商环。

定理 4.2.3 (第二同构定理 Second Isomorphism Theorem for Rings)**.** 设 $(R,+,\cdot)$ 为环，I,J 是 R 的理想。那么

$$I/(I\cap J)\cong (I+J)/J$$

证明. □

定理 4.2.4 (第三同构定理 Third Isomorphism Theorem for Rings)**.** 设 $(R,+,\cdot)$ 为环，I,J 是 R 的理想，并且 $I\subseteq J$。那么

$$(R/I)/(J/I)\cong R/J$$

证明. □

4.3 域

4.3.1 域的定义

定义 4.3.1 (域 Field). 设 F 是一个非空集合，$+$ 和 $\cdot$ 是定义在 F 上的两种代数运算。$(F,+,\cdot)$ 称为域，当且仅当，$(F,+,\cdot)$ 是一个交换环并且是一个除环。

定义 4.3.2 (子域 Subfield). 设 F 是一个域，$K \subseteq F$。K 称为 F 的一个子域，当且仅当，K 在 F 上关于加法和乘法是封闭的，并且 $(K,+,\cdot)$ 也是一个域。

定理 4.3.1 (子域判定定理). 设 $(F,+,\cdot)$ 是一个域，$K \subseteq F$。则 K 是 F 的子域的充分必要条件是：

1. $0,1 \in K$；
2. $\forall a,b \in K$，$a-b \in K$；
3. $\forall a,b \in K \setminus \{0\}$，$a \cdot b^{-1} \in K$；

注解

域是在环的基础上，添加了乘法交换律和乘法逆元存在性两个条件，并且域中没有零因子。常见的，$(\mathbb{Q},+,\cdot)$，$(\mathbb{R},+,\cdot)$ 和 $(\mathbb{C},+,\cdot)$ 都是域。$\mathbb{Q}$ 是 $\mathbb{R}$ 的子域，$\mathbb{R}$ 也是 $\mathbb{C}$ 的子域。

4.3.2 域扩张

定义 4.3.3 (域扩张 Field Extension). 设 F 是一个域，如果存在一个域 K，使得 F 是 K 的一个子域，则称 K 是 F 的一个域扩张，记为 K/F。

注解

域扩张是域论中的一个重要概念，如何从一个小域构造出一个更大的域，或者研究两个域之间的关系，都是通过域扩张来实现的。

定义 4.3.4 (单扩域 Simple Extension). 设 F 是一个域，K/F 是 F 的一个域扩张。如果存在 $a \in K$，使得 $K = F(a)$，则称 K/F 是一个单扩域。这里 $F(a)$ 表示包含 F 和 a 的最小子域。

注解

单扩域在 K/F 所有子域中包含基域 F 和另一个元素 $a \in K$ 的最小子域。例如，$\mathbb{C} = \mathbb{R}(i) = \{a+bi : a,b \in \mathbb{R}\}$ 是 $\mathbb{R}$ 的一个单扩域，因为 $\mathbb{C}$ 是包含 $\mathbb{R}$ 和 i 的最小子域。另一个例子是 $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$ 是 $\mathbb{Q}$ 的一个单扩域，因为它是包含 $\mathbb{Q}$ 和 $\sqrt{2}$ 的最小子域。

定义 4.3.5 (分裂域 Splitting Field). 设 F 是一个域，$f(x) \in F[x]$ 是一个正次数多项式。如果存在一个域扩张 K/F，使得 $f(x)$ 可以写成一系列在 $K[x]$ 中的一次多项式的乘积，也即

$$f(x) = a(x-r_1)(x-r_2)\cdots(x-r_n),\ a,r_1,r_2,\ldots,r_n \in K,$$

并且 K 是包含所有 $f(x)$ 所有根的最小域，则称 K 是 $f(x)$ 在 F 上的一个分裂域。

注解

在某个域上某个多项式方程可能没有解，因此希望通过构造一个更大的域，使得该多项式方程在这个更大的域中有解。分裂域就是这样一个更大的域，它是相对特定多项式而言的，它包含了多项式的所有根，并且是包含这些根的最小域。

定义 4.3.6 (有限扩张与无限扩张 Finite and Infinite Extensions)**.** 设 K/F 是一个域扩张，K 作为 F 上的一个向量空间。如果 K 作为 F 上的向量空间是有限维的，则称 K/F 是一个有限扩张，否则称 K/F 是一个无限扩张。K 的维数称为扩张的次数，记为 $[K:F]$。

注解

$\mathbb{C}$ 是 $\mathbb{R}$ 的一个有限扩展，并且 $\{1,i\}$ 是 $\mathbb{C}$ 作为 $\mathbb{R}$ 上的一个向量空间的一个基，因此 $[\mathbb{C}:\mathbb{R}]=2$。$\mathbb{R}$ 是 $\mathbb{Q}$ 的一个无限扩展，因为 $\mathbb{R}$ 作为 $\mathbb{Q}$ 上的一个向量空间是无限维的。

定义 4.3.7 (代数数与超越数 Algebraic and Transcendental Numbers)**.** 设 F 是一个域，$F[x]$ 是 F 上的多项式环，K 是 F 的一个域扩张。如果存在一个非零多项式 $f(x)\in F[x]$，使得 $f(a)=0$, $a\in K$，则称 a 是 F 上的一个代数数，否则称 a 是 F 上的一个超越数。

定义 4.3.8 (代数扩张和超越扩张 Algebraic and Transcendental Extensions)**.** 设 F 是一个域，K/F 是 F 的一个域扩张。如果 K 中的每个元素都是 F 上的代数数，则称 K/F 是一个代数扩张，否则称 K/F 是一个超越扩张。

注解

代数数是指那些可以作为某个非零多项式的根的数，而超越数则是那些不能作为任何非零多项式的根的数。例如，$\sqrt{2}$ 是 $\mathbb{Q}$ 上的一个代数数，因为它是多项式 x^2-2 的一个根。另一方面，π 是 $\mathbb{Q}$ 上的一个超越数，因为不存在任何非零多项式 $f(x)\in\mathbb{Q}[x]$ 使得 $f(\pi)=0$。代数扩张是指扩张域中的每个元素都是基域上的代数数，而超越扩张则包含至少一个超越数。根据代数基本定理 3.4.1，$\mathbb{C}$ 中的每个元素都是 $\mathbb{R}$ 上的代数数，也即任意一个实数域上的多项式方程在复数域中都有解，因此 $\mathbb{C}$ 是 $\mathbb{R}$ 的一个代数扩张。$\mathbb{R}$ 是 $\mathbb{Q}$ 的一个超越扩张，存在 $\pi\in\mathbb{R}$ 是 $\mathbb{Q}$ 上的一个超越数。

定义 4.3.9 (可约多项式与不可约多项式 Reducible and Irreducible Polynomials)**.** 设 F 是一个域，$F[x]$ 是 F 上的多项式环。如果存在两个次数均小于 $f(x)$ 的非零多项式 $g(x),h(x)\in F[x]$，使得 $f(x)=g(x)h(x)$，则称 $f(x)$ 在 F 上是可约的，否则称 $f(x)$ 在 F 上是不可约的。

注解

则多项式 $f(x)=x^2-2$ 在 $\mathbb{Q}$ 上是不可约的，因为它不能分解为两个次数均小于 2 的有理系数多项式的乘积。另一方面，多项式 $g(x)=x^2-1$ 在 $\mathbb{Q}$ 上是可约的，因为它可以分解为 $(x-1)(x+1)$。

定义 4.3.10 (可分多项式与不可分多项式 Separable and Inseparable Polynomials)**.** 设 F 是一个域，$F[x]$ 是 F 上的多项式环。如果正次数多项式 $f(x) \in F[x]$ 的每个根在其分裂域中都是单根，则称 $f(x)$ 在 F 上是可分的；反之，存在至少一个重根，则称 $f(x)$ 在 F 上是不可分的。

注解

多项式 $f(x) = x^2 - 2$ 在 $\mathbb{Q}$ 上是可分的，因为它在其分裂域 $\mathbb{Q}(\sqrt{2})$ 中有两个不同的根 $\sqrt{2}$ 和 $-\sqrt{2}$。另一方面，多项式 $g(x) = x^2 - 2x + 1 = (x-1)^2$ 在 $\mathbb{Q}$ 上是不可分的，因为它在其分裂域 $\mathbb{Q}$ 中只有一个根 1，且该根是重根。

定义 4.3.11 (可分扩张 Separable Extension)**.** 设 F 是一个域，K/F 是 F 的一个代数扩张。K/F 称为可分扩张，当且仅当，K 中的每个元素都是 $F[x]$ 中某个不可约但可分多项式的根。

注解

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是一个可分扩张，其中 $\pm\sqrt{2}$ 是 $\mathbb{Q}$ 上不可约但可分多项式 $x^2 - 2$ 的两个单根。

定义 4.3.12 (正规扩张 Normal Extension)**.** 设 F 是一个域，K/F 是 F 的一个代数扩张。K/F 称为正规扩张，当且仅当，所有 $F[x]$ 中不可约多项式在 K 中能完全可以分解为一次多项式的乘积。也即，K 是包含所有 $F[x]$ 中不可约多项式所有根。

注解

$\mathbb{C}/\mathbb{R}$ 是一个正规扩张，因为 $\mathbb{C}$ 是包含所有 $\mathbb{R}[x]$ 中不可约多项式所有根的代数扩张域。例如，$\mathbb{R}[x]$ 中不可约多项式 x^2+1 在 $\mathbb{C}$ 中可以分解为 $(x-i)(x+i)$。另一方面，$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是一个正规扩张，因为 $\mathbb{Q}(\sqrt[3]{2})$ 不包含不可约多项式 $x^3 - 2$ 的所有根。 $x^3 - 2$ 在 $\mathbb{C}$ 中有三个根，分别是 $\sqrt[3]{2}$、$\sqrt[3]{2}\omega$ 和 $\sqrt[3]{2}\omega^2$，其中 $\omega = e^{2\pi i/3}$ 是一个非实的复数。

4.3.3 伽罗瓦理论

定义 4.3.13 (伽罗瓦扩张 Galois Extension)**.** 设 F 是一个域，K/F 是 F 的一个代数扩张。如果 K/F 既是正规扩张又是可分扩张，则称 K/F 是一个伽罗瓦扩张。

定义 4.3.14 (伽罗瓦群 Galois Group)**.** 设 F 是一个域，K/F 是 F 的一个域扩张。定义 K 上的一个 F-自同构：$\sigma : K \to K$，使得 $\sigma(a) = a,\ \forall a \in F$。所有 K 上的 F-自同构，记为 $\mathrm{Gal}(K/F)$。$\mathrm{Gal}(K/F)$ 上的二元运算时函数的复合，那么 $(\mathrm{Gal}(K/F), \circ)$ 满足群公理，称为 K/F 的伽罗瓦群。

注解

伽罗瓦群是研究域扩张对称性的重要工具。它捕捉了域扩张中元素之间的对称关系，并且与多项式方程的可解性密切相关。伽罗瓦群的结构可以揭示多项式方程根的排列方式，从而帮助理解多项式方程是否可以通过根式来解。

定义 4.3.15 (伽罗瓦对应 Galois Correspondence)**.** 设 F 是一个域，K/F 是 F 的一个伽罗瓦扩张。设 $H \leq \mathrm{Gal}(K/F)$ 是 $\mathrm{Gal}(K/F)$ 的一个子群，定义

$$K^H = \{a \in K : \sigma(a) = a,\ \forall \sigma \in H\}.$$

则 K^H 是 K/F 的一个子扩张域。反之，设 E 是 K/F 的一个子扩张域，定义

$$\mathrm{Gal}(K/E) = \{\sigma \in \mathrm{Gal}(K/F) : \sigma(a) = a,\ \forall a \in E\}.$$

则 $\mathrm{Gal}(K/E)$ 是 $\mathrm{Gal}(K/F)$ 的一个子群。这两个映射 $H \mapsto K^H$ 和 $E \mapsto \mathrm{Gal}(K/E)$ 互为逆映射，并且它们之间存在包含关系的反转。也即，如果 $H_1 \leq H_2 \leq \mathrm{Gal}(K/F)$，则 $K^{H_2} \leq K^{H_1}$；如果 $E_1 \leq E_2$ 是 K/F 的两个子扩张域，则 $\mathrm{Gal}(K/E_2) \leq \mathrm{Gal}(K/E_1)$。这就是伽罗瓦对应。

注解

定理 4.3.2 (伽罗瓦基本定理 Fundamental Theorem of Galois Theory)**.** 设 F 是一个域，K/F 是 F 的一个伽罗瓦扩张。则 K/F 的子扩张域与 $\mathrm{Gal}(K/F)$ 的子群之间存在一一对应关系，这个对应关系是包含关系的反转。

注解

定义 4.3.16 (可解群 Solvable Group)**.** 设 G 是一个群，如果存在一列子群

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G,$$

使得每个商群 G_{i+1}/G_i 都是阿贝尔群，则称 G 是一个可解群。

定理 4.3.3 (多项式方程根式可解定理 Polynomial Equation Solvability by Radicals Theorem)**.** 设 F 是一个域，$f(x) \in F[x]$ 是一个正次数多项式，K 是 $f(x)$ 在 F 上的一个分裂域。则 $f(x)$ 的根可以表示为 F 中元素和根式的有限次运算的结果，当且仅当，伽罗瓦群 $\mathrm{Gal}(K/F)$ 是一个可解群。

定理 4.3.4 (阿贝尔-伽罗瓦定理 Abel Galois Theorem)**.** 一般五次及以上的多项式方程没有根式解。

Chapter 5

线性代数

5.1 线性空间