

游戏开发工程师数学基础

木头骨头石头

2025 年 9 月 20 日

目录

1	集合论简介	5
1.1	朴素集合论	5
1.2	ZFC 公理集合论	6
1.2.1	外延公理	6
1.2.2	配对公理	7
1.2.3	分类公理模式	7
1.2.4	并集公理	9
1.2.5	幂集公理	10
1.2.6	无穷公理	11
1.2.7	替代公理模式	12
1.2.8	正则公理	13
1.2.9	选择公理	14
2	关系与结构	15
2.1	二元关系	16
2.1.1	二元关系的定义	16
2.1.2	关系矩阵与关系图	17
2.1.3	自反性与反自反性	17
2.1.4	对称性与反对称性	18
2.1.5	传递性	19
2.2	函数	20
2.2.1	集合的势	20
2.3	等价关系	22
2.3.1	划分	23
2.4	代数结构	24
2.4.1	代数常数	24
2.4.2	代数算律	25
2.4.3	同态与同构	26
2.4.4	群	26
2.4.5	环与域	27
2.4.6	模与线性空间	29
2.5	序结构	30
2.5.1	上下界	30

2.6	拓扑结构	32
2.6.1	度量空间	33
2.6.2	赋范线性空间	33
2.6.3	内积空间	34
3	数系的扩充	35
3.1	整数	35
3.2	有理数	38
3.3	实数	41
3.3.1	柯西序列与实数	41
3.3.2	实数集的完备性	43
3.4	复数	44
3.5	四元数	45

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 \emptyset 。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

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

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 $\emptyset \in A$ ，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 $x \cap A = \emptyset$ 。
9. **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 $f(A) \in A$ 。

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, \dots, 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, \dots, 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

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

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

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 \emptyset

注解

因为满足性质 $x \neq x$ 的元素并不存在, 所以 \emptyset 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

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

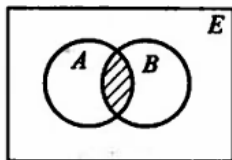


图 1.1: 交集

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

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 $A - B$, 那么

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

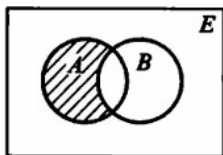


图 1.2: 差集

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

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

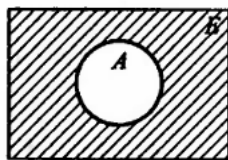


图 1.3: 补集

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

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

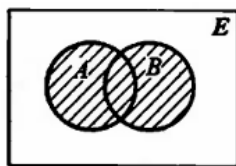


图 1.4: 并集

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:

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

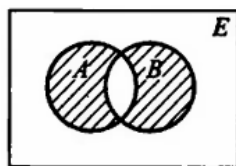


图 1.5: 并集

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: $A \cap \complement_E A = \emptyset$

7. 德摩根律:

$$(a) \quad A - (B \cup C) = (A - B) \cap (A - C)$$

$$(b) \quad A - (B \cap C) = (A - B) \cup (A - C)$$

$$(c) \quad \complement_E(B \cup C) = \complement_E B \cap \complement_E C$$

$$(d) \quad \complement_E(B \cap C) = \complement_E B \cup \complement_E C$$

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, \dots, S_n 的笛卡尔积, 记为 $\prod_{i=1}^n S_i$, 那么

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

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 $\emptyset \in A$, 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 $0 := \emptyset$

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，

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

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:

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

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 $x \cap A = \emptyset$ 。

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

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

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 $\text{dom}R$; 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 $\text{ran}R$.

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:

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

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

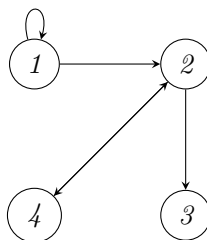
例 2.1.1. 设一个二元关系 $R = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 2, 4 \rangle, \langle 4, 2 \rangle\}$, 其关系矩阵为

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

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, $I_X \cap R = \emptyset$

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: $\forall x \in \text{dom} f$, 如果 $(x, y_1) \in f$ 且 $(x, y_2) \in f$, 则 $y_1 = y_2$

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

1. 满射 (Surjection): 如果 $\text{ran} f = Y$, 则称 f 为满射。
2. 单射 (Injection): 如果 $\forall y \in \text{ran} f$, $(x_1, y) \in f$ 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 $f: \mathbb{N} \rightarrow \mathbb{Z}$ ，将 \mathbb{Z} 中的整数按如下方式排列：

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

这样就可以定义双射 $f(n)$ 为上述排列中第 n 个整数

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

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

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 $X = \{1, 2, \dots, 8\}$ 上的关系 R :

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

$x \equiv y \pmod{3}$ 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

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

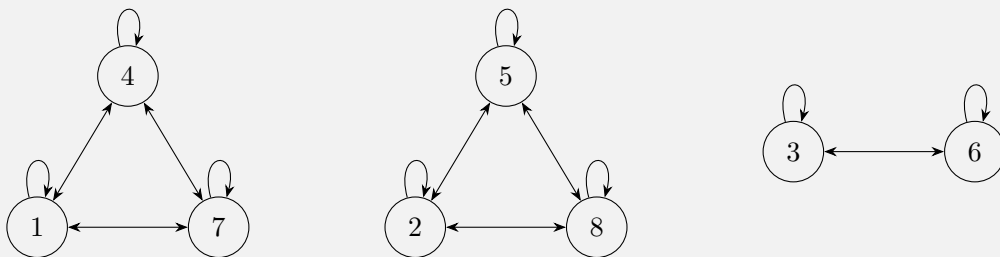
或简记为

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

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 $\emptyset \notin \mathcal{S}$
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 $A \cap B = \emptyset$

注解

划分中, 每一个元素都是一个非空子集, 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 $f: X^n \rightarrow X$ 称为 X 上的 n 元运算, 当且仅当, f 满足:

1. 封闭性: $\text{dom} f = X^n$

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 $\text{dom} f = Y^n$ 。

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 $f: X \rightarrow Y$ 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 $a * b = b * a = e$ 。

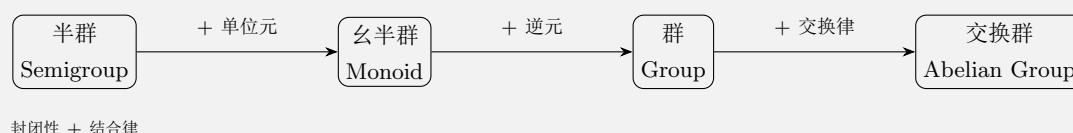
只含有单位元的群称为**平凡群 Trivial Group**, 记为 $\{e\}$; 反之, 含有除单位元外其他元素的群称为**非平凡群 Non-Trivial Group**。

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 $(\mathbb{N}, +)$ 是么半群; 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 (含么环 Ring with identity). 设 $(R, +, \cdot)$ 为环。如果存在乘法单位元, 则称环 $(R, +, \cdot)$ 为含么环。也即 (R, \cdot) 是么半群, $(R, +, \cdot)$ 为含么环。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 $(R, +, \cdot)$ 为含么环。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

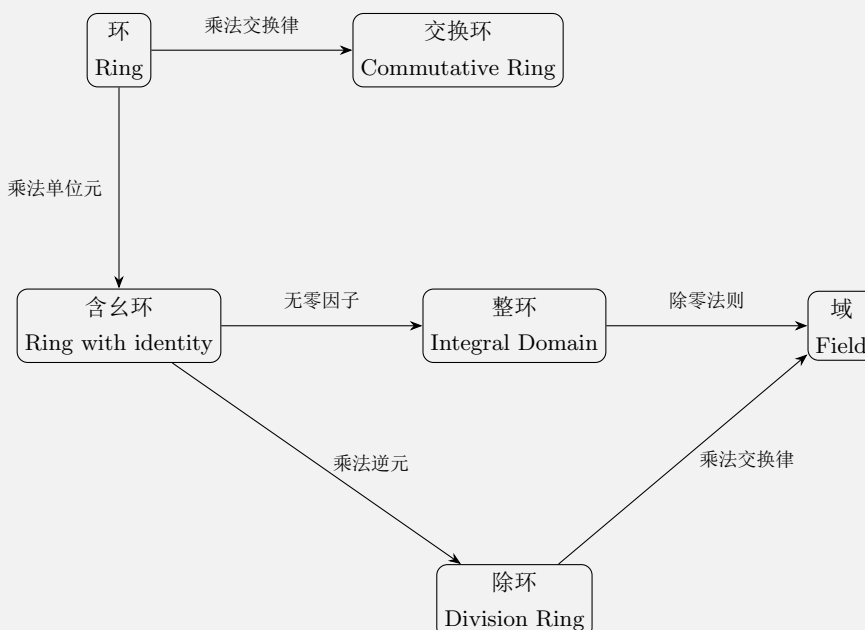
1. $(F, +)$ 是交换群;
2. (F, \cdot) 是交换群;
3. 乘法对加法满足分配律;
4. 除零法则: 对任意 $a \in F, a \neq 0$, 存在 $b \in F$, 使得 $a \cdot b = 1$ 。

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 $(R, +, \cdot)$ 为含么环, $(G, +)$ 为阿贝尔群。如果存在一个标量乘法 $*$: $R \times G \rightarrow G$, 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 $*$: $G \times R \rightarrow G$, 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 $(R, +, \cdot)$ 是含么交换环, 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 : $F \times V \rightarrow V$, 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。 \square

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: $\emptyset \in \mathcal{T}(X)$ 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 $U_1, U_2, \dots, U_n \in \mathcal{T}(X)$, 有 $U_1 \cap U_2 \cap \dots \cap U_n \in \mathcal{T}(X)$ 。

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

根据拓扑空间的定义, 幂集 $\mathcal{P}(X)$ 和 $\{\emptyset, X\}$ 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:

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

下面的子集族不是 X 上的拓扑:

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

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, $\mathbb{C}_X A \in \mathcal{T}(X)$ 。

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: \emptyset 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: $A_1 \cup A_2 \cup \dots \cup A_n$ 是闭集, 其中 A_1, A_2, \dots, 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 度量空间

定义 2.6.3 (度量空间 Metric Space). 设 X 是一个非空集合, 映射 $d: X \times X \rightarrow \mathbb{R}$ 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 2.6.4 (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 \emptyset 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。

2.6.2 赋范线性空间

定义 2.6.5 (赋范线性空间 Normed Linear Space). 设 V 是域 \mathbb{F} 上的线性空间, 映射 $\|\cdot\|: V \rightarrow \mathbb{R}$ 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 $d: V \times V \rightarrow \mathbb{R}$, $d(x, y) = \|x - y\|$, 则 (V, d) 为度量空间。

2.6.3 内积空间

定义 2.6.6 (内积空间 Inner Product Space). 设 V 是域 \mathbb{F} 上的线性空间, 映射 $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{F}$ 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 $\| \cdot \| : V \rightarrow \mathbb{R}$, $\|x\| = \sqrt{\langle x, x \rangle}$, 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 $f: X \rightarrow X$ ，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, $0 = [0 - 0]_{=}$, $1 = [1 - 0]_{=}$, $2 = [2 - 0]_{=}$, $3 = [3 - 0]_{=}$, \dots 。 $\mathbb{C}_{\mathbb{Z}}\mathbb{N}$ 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. 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, $0 = [0/1]_{=}$, $1 = [1/1]_{=}$, $2 = [2/1]_{=}$, $3 = [3/1]_{=}$, \dots 。 $\mathbb{C}_{\mathbb{Q}}\mathbb{Z}$ 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

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

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

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

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

定义 3.2.8 (有理数的整数次幂 Integer Power of Rational Numbers). 设 $[a/b]_{=} \in \mathbb{Q}$, $n \in \mathbb{Z}$, 定义 $[a/b]_{=}$ 的整数次幂为

$$([a/b]_{=})^n = \begin{cases} [1/1]_{=}, & n = 0 \\ [(\prod_{i=1}^n a)/(\prod_{i=1}^n b)]_{=}, & n > 0 \\ [(\prod_{i=1}^{-n} b)/(\prod_{i=1}^{-n} a)]_{=}, & n < 0, a \neq [0/1]_{=} \end{cases}$$

定理 3.2.1 (有理数的整数次幂的性质 Properties of Integer Power of Rational Numbers). 设 $x, y \in \mathbb{Q}$, $m, n \in \mathbb{Z}$, 则

1. $x^m \cdot x^n = x^{m+n}$
2. $(x^m)^n = x^{mn}$
3. 若 $x \neq [0/1]_{=}$, 则 $x^m/x^n = x^{m-n}$
4. $(xy)^n = x^n y^n$

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。

定义 3.2.9 (有理数的序关系 Order Relation of Rational Numbers). 设 $[a/b]_{=}, [c/d]_{=} \in \mathbb{Q}$, 定义序关系为

$$[a/b]_{=} \leq [c/d]_{=} \iff \begin{cases} ad \leq bc, & bd > 0 \\ ad \geq bc, & bd < 0 \end{cases}$$

定义 3.2.10 (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 3.2.11 (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

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

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

令 $a_0 = 1$ ，得到一个有理数序列：

$$\begin{aligned} a_1 &= \frac{1}{2}(1 + 2) = \frac{3}{2} = 1.5 \\ a_2 &= \frac{1}{2}\left(\frac{3}{2} + \frac{4}{3}\right) = \frac{17}{12} = 1.416666666666\ldots \\ a_3 &= \frac{1}{2}\left(\frac{17}{12} + \frac{24}{17}\right) = \frac{577}{408} = 1.414215686274\ldots \\ a_4 &= \frac{1}{2}\left(\frac{577}{408} + \frac{816}{577}\right) = \frac{665857}{470832} = 1.414213562374\ldots \\ &\vdots \end{aligned}$$

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：

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

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无理数。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

历史上，实数的定义有多种方式，一种是通过柯西序列的方式，另一种是戴德金分割，下面主要介绍柯西序列定义实数。

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

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: $a_n = a_1 q^{n-1}$, $a_1 \neq 0$, $q \neq 0$, $n = 1, 2, 3, \dots$
2. 等差数列: $a_n = a_1 + (n-1)d$, $n = 1, 2, 3, \dots$
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: $a_1 = 2$, $a_2 = 3$, $a_3 = 5$, $a_4 = 7$, $a_5 = 11$, $a_6 = 13, \dots$

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 $q = [\{q, q, q, \dots\}]_= \in \mathbb{R}$ 。例如， $a_0 = 1, a_2 = 1, a_3 = 1, \dots$ 和 $b_0 = 0, b_2 = 0.9, b_3 = 0.999, \dots$ 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

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

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

证明. 实数加法的封闭性 (任意两个实数相加依然是实数):

□

3.3.2 实数集的完备性

3.4 复数

3.5 四元数