数学基本概念

2024/2/15, *Nicolas Keng*

CONTENTS

Part I

Set Theory

Chapter 1

Sets, Maps and Relations

1.1 Sets and Elements

集合的概念是数学中的一个基本概念, 很难用更简单的概念进行下定义, 只能基于一种描述. 在朴素集合论中我们先采取 Cantor 在 1895 年所下的定义:

A set is a gathering together into a whole of definite, distinct objects of our perception or of our thought, which are called elements of the set.

定义 1.1.1 凡是具有某种性质的, 确定的, 有区别的对象的全体就是一个集合 (set), 这些对象称作该集合的元素 (element). 若对象 x 是集合 A 内的元素, 则称 x 属于 (belongs to) A, 记为 $x \in A$; 否则记为 $x \notin A$.

以上定义给出了集合所需满足的三个性质: 确定性, 互异性, 无序性.

例 1.1.1 约定 $\mathbb{N}$ 表示自然数集, $\mathbb{Z}$ 表示整数集, $\mathbb{Q}$ 表示有理数集, $\mathbb{R}$ 表示实数集.

当集合 A 的元素只有有限多个时, 我们可以将其全部列出, 也即 $A = \{a_1, \cdots, a_n\}$, 并称其为有限集 (finite set). 但当其有无限多个元素时, 即 A 为无限集 (infinite set) 时我们不一定可以将其全部列出, 于是我们采用如下的描述法来刻画:

$$A = \{x \mid x \text{ 具有性质} P\} = \{x \mid p(x)\},\ p(x) \text{ 代表 } x \text{ 具有性质} P.$$

我们考虑将性质 P 作为刻画集合 A 的一种方式, 即 $x \in A \Leftrightarrow p(x)$.

定义 1.1.2 定义空集 (empty set) 为没有任何元素的集合, 记作 $\varnothing$.

定义 1.1.3 若 $\forall x \in B, x \in A$, 则称 B 是 A 的子集 (subset), 也称作 A 包含 (contain) B, 记作 $B \subset A$. 此时若 $A \neq B$, 则称 B 是 A 的真 (proper) 子集, 记作 $B \subsetneq A$.

显然空集 $\varnothing$ 是任何集合的子集.

命题 1.1.1 若 $A \subset B$ 且 $B \subset A$, 则 $A = B$.

命题 1.1.2 包含关系的传递性: 若 $A \subset B, B \subset C$, 则 $A \subset C$.

定义 1.1.4 集合 A 的所有子集组成的集合称作 A 的幂集 (power set), 记作 2^A 或 $P(A)$. 描述法表示作

$\{X \mid X \subset A\}$.

定义 1.1.5 我们引入逻辑中的五个联结词和两个量词:

(1) $\neg$ 否定, $\wedge$ 且, $\vee$ 或, $\rightarrow$ 蕴含, $\leftrightarrow$ 互相蕴含;

(2) $\forall$ 全称量词, $\exists$ 存在量词.

注意这里的蕴含是集合论中的表述方式, 我们也在表述命题关系时常用 $\Rightarrow$.

定义 1.1.6 由集合构成的集合称为集族 (family of sets), 一般记作 $\{A_i\}_{i\in I}$, 其中集合 A_i 为集族的元素, I 为指标集 (index set). 特殊地, 以 $\mathbb{N}_+$ 为指标集的集族 $\{A_n\}_{n=1}^{\infty}$ 也称作集列 (sequence).

练习 1.1 用描述法表示空集, 并证明空集唯一. 这里, 唯一指两空集 A, B 相等.

1.2 Operations of Sets

数学理论一般是在确定的范围内展开讨论的, 如在有理数集中 $x^2-2=0$ 的根不存在, 但在实数集中其为 $\pm\sqrt{2}$. 所以我们必须规定在什么范围内讨论. 这个范围 U 就称作该情况下的全集 (universal set). 之后在没有特殊说明的前提下, 我们都默认在全集 U 下考虑.

定义 1.2.1 集合的运算: 考虑集合 A, B, 定义:

(1) 交 (intersection): $A\cap B=\{x \mid x\in A \wedge x\in B\}$;

(2) 并 (union): $A\cup B=\{x \mid x\in A \vee x\in B\}$;

(3) 差 (difference): $A-B=\{x \mid x\in A, x\notin B\}$;

(4) 补 (complement): $A^c=U-A$, 其中 U 为全集.

定理 1.2.1 在全集 U 下, 取集合 A, B, C, 则其交并补具有如下性质:

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

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

(3) 幂等律: $A\cap A=A$, $A\cup A=A$;

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

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

(6) $\varnothing\cap A=\varnothing$, $\varnothing\cup A=A$, $U\cap A=A$, $U\cup A=U$, $A\cap A^c=\varnothing$, $A\cup A^c=U$;

(7) De Morgan 律: $(A\cap B)^c=A^c\cup B^c$, $(A\cup B)^c=A^c\cap B^c$.

证明概要 留作练习. □

定义 1.2.2 对集族 $\{A_i\}_{i\in I}$, 则定义集族的交与并

$$\bigcap_{i\in I}A_i=\{x \mid \forall i\in I,\, x\in A_i\};\quad \bigcup_{i\in I}A_i=\{x \mid \exists i\in I,\, x\in A_i\}.$$

差的定义事实上是相对的. 它不具有对称性; 而不考虑 A, B 的特异性, 只考虑在某一个集合而不在另一集合中的元素, 我们便有了如下定义:

定义 1.2.3 定义集合 A, B 的对称差 (symmetric difference)

$$A\Delta B = (A - B) \cup (B - A).$$

命题 1.2.1 对称差成立如下运算律:

(1) 交换律: $A\Delta B = B\Delta A$;

(2) 结合律: $A\Delta(B\Delta C) = (A\Delta B)\Delta C$;

(3) 分配律: $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$;

(4) $A\Delta B = (A \cup B) - (A \cap B)$.

证明概要 留作练习. □

定义 1.2.4 笛卡尔积 (Cartesian product): 对非空集合 A, B, 定义其笛卡尔积为

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

这里 (a, b) 称为有序对 (ordered pair). 递归地, 我们有

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = (A_1 \times \cdots \times A_{n-1}) \times A_n,\ (a_1, \cdots, a_n) = ((a_1, \cdots, a_{n-1}), a_n).$$

定义 1.2.5 无交并 (Disjoint union): 对非空集合 A_1, A_2, 定义其无交并为

$$A_1 \sqcup A_2 = \{(a_i, i) \mid a_i \in A_i,\, i = 1, 2\},$$

也即将 A_1, A_2 内相同元素视作不同元素 (标记来源) 得到的并. 类似地,

$$\bigsqcup_{i=1}^{n} A_i = A_1 \sqcup \cdots \sqcup A_n = \{(a_i, i) \mid a_i \in A_i,\, i = 1, \cdots, n\}.$$

练习 1.2 证明若 $A \cap C \subset B \cap C$, $A \cup C \subset B \cup C$, 则 $A \subset B$.

练习 1.3 将集合的分配律与 De Morgan 律推广到集族情形.

练习 1.4 证明对称差的四条运算律.

练习 1.5 若 $A - B = C - D$, 则是否一定有 $A \cup D = B \cup C$? 证明或举出反例.

练习 1.6 若 $X \subset A$, $Y \subset B$, 证明 $X \times Y \subset A \times B$.

练习 1.7 证明 $(X \times Y) \cap (A \times B) = (X \cap A) \times (Y \cap B)$.

1.3 Maps

定义 1.3.1 对集合 A 和 B, 若 $\forall a\in A$ 对应 B 中唯一元素 b, 则称其为 A 到 B 的函数 (function) 或映射 (map), 记作 $f:A\to B, a\mapsto b$. 这里, b 称作 a 的像 (image), 记作 $f(a)$; A 称作函数的定义域 (domain), B 称作函数的像集 (range) 或值域 (codomain).

定义 1.3.2 对函数 $f:A\to B$, 若 $S\subset A$, 则 $\forall a\in S$, 由映射关系 $a\mapsto f(a)$ 给出的 $f\big|_S:S\to B$ 称为 f 在 S 上的限制 (restriction).

例 1.3.1 对任一集合 A, 称 $1_A:A\to A$, $a\mapsto a$ 为 A 上的恒等映射 (identity map); 若 $S\subset A$, 则称 $1_A\big|_S:S\to A$ 为 S 在 A 上的包含映射 (inclusion map).

定义 1.3.3 对函数 $f:X\to Y, g:Y\to Z$, 则定义复合 (composition)

$$g\circ f=gf:X\to Z,\, x\mapsto g(f(x)).$$

命题 1.3.1 对函数 $f:X\to Y, g:Y\to Z, h:Z\to W$, 则 $h(gf)=(hg)f$.

定义 1.3.4 对函数 $f:A\to B$, 若 $S\subset A$, 则称 $\{b\in B\mid \exists a\in S,\, b=f(a)\}$ 为 S 的像, 记作 $f(S)$; $f(A)$ 称作 f 的像, 记作 $\operatorname{Im} f$.

若 $T\subset B$, 则称 $\{a\in A\mid f(a)\in T\}$ 是 T 的原像 (inverse image), 记作 $f^{-1}(T)$.

命题 1.3.2 对 $f:X\to Y, A\subset B\subset X, C\subset D\subset Y$, 则

(1) $f(A)\subset f(B), f^{-1}(C)\subset f^{-1}(D)$;

(2) $A\subset f^{-1}(f(A)), C\supset f(f^{-1}(C)), (f(A))^c\subset f(A^c), (f^{-1}(C))^c=f^{-1}(C^c)$.

证明概要 略 □

命题 1.3.3 对 B 的任一子集族 $\{T_i\}_{i\in I}$,

$$f^{-1}\left(\bigcup_{i\in I}T_i\right)=\bigcup_{i\in I}f^{-1}(T_i),\ f^{-1}\left(\bigcap_{i\in I}T_i\right)=\bigcap_{i\in I}f^{-1}(T_i).$$

定义 1.3.5 若函数 $f:A\to B$ 满足 $\forall a,a'\in A, f(a)=f(a')\Rightarrow a=a'$, 则称 f 为单射 (injection).

若函数 $f:A\to B$ 满足 $f(A)=B$, 即 $\forall b\in B,\exists a\in A,\, b=f(a)$, 则称 f 为满射 (surjection).

若函数 $f:A\to B$ 既是单射又是满射, 则称 f 为双射 (bijection) 或一一对应.

定理 1.3.1 对函数 $f:A\to B$, 若 $A\neq\varnothing$, 则:

(1) f 是单射 $\Leftrightarrow\exists g:B\to A$, 使得 $gf=1_A$. g 称为 f 的左逆 (left inverse).

(2) 若 A 是集合, 则 f 是满射 $\Leftrightarrow\exists h:B\to A$, 使得 $fh=1_B$. h 称为 f 的右逆 (right inverse).

证明概要 (1) ($\Leftarrow$) 显然; 对单射 f, $\forall b\in f(A)$, 存在唯一 $a\in A$, 使得 $f(a)=b$. 取 $a_0\in A$, 定义

$$g:B\to A,\, b\mapsto\begin{cases}a, & b\in f(A)\vee f(a)=b;\\ a_0, & b\notin f(A).\end{cases}$$

显然 $gf = 1_A$.

(2) ($\Leftarrow$) 显然; 对满射 $f, \forall b \in B, f^{-1}(b) \subset A$ 非空. 于是 $\forall b \in B$, 取 $a_b \in f^{-1}(b)$ 并定义 $h : B \to A, b \mapsto a_b$. 显然 $fh = 1_B$. □

推论 对函数 $f : A \to B$, 若 A 是集合, 则 f 是双射的充要条件是 f 有双侧逆, 记作 f^{-1}.

定义 1.3.6 若 $f = gh, GF = KH$, 则称如下图表 (disgram) 是交换的 (commutative):

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "h"'] & & C \\ & B \arrow[ur, "g"'] & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "F"] \arrow[d, "H"'] & B \arrow[d, "G"] \\ C \arrow[r, "K"'] & D \end{tikzcd}$$

练习 1.8 对函数 f, g, 若 $f \circ g$ 单, 则 g 单; 若 $f \circ g$ 满, 则 g 满.

练习 1.9 对有限集合 X 上的函数 $f : X \to X$, 则 f 单的充要条件是 f 满.

1.4 Relations

定义 1.4.1 称 $R \subset A \times B$ 为 $A \times B$ 上的关系 (relation); $R = \{(a, f(a)) \mid a \in A\}$ 为 f 的图像 (graph). 特殊地, $B = A$ 时称 R 为 A 上的二元关系.

定义 1.4.2 若 $A \times A$ 上的关系 R 满足如下三个条件:

$$a \in A \Rightarrow (a, a) \in R; \quad (a, b) \in R \Rightarrow (b, a) \in R; \quad (a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R,$$

则称 R 为 A 上的等价关系 (equivalence relation); 对 $\forall (a, b) \in R$, 称 a, b 在 R 上等价 (equivalent), 记作 $a \sim b$. 此时 $R(\sim)$ 满足:

$$a \sim a; \quad a \sim b \Rightarrow b \sim a; \quad a \sim b, b \sim c \Rightarrow a \sim c.$$

定义 1.4.3 设 $R(\sim)$ 是 A 上的等价关系, 若 $a \in A$, 则称 A 中等价于 A 的所有元素构成的类为等价类 (equivalence class), 记作 $\bar{a} = \{b \in A \mid b \sim a\}$.

A 中所有等价类构成的类称作 A 对于 R 的商集 (quotient class), 记作 A/R.

命题 1.4.1 对集合 A, 则 $\forall a \in A, \bar{a} \neq \varnothing$ 且 $\bigcup\limits_{a \in A} \bar{a} = \bigcup\limits_{\bar{a} \in A/R} \bar{a}$.

命题 1.4.2 对集合 $A, \forall a, b \in A$, 若 $\bar{a} \neq \bar{b}$, 则 $\bar{a} \cap \bar{b} = \varnothing$.

定义 1.4.4 对非空类 A 及其子集族 $\{A_i\}_{i \in I}$, 若它满足:

$$\forall i \in I, A_i \neq \varnothing; \quad \bigcup_{i \in I} A_i = A; \quad \forall i \neq j \in I, A_i \cap A_j = \varnothing,$$

则称 $\{A_i\}_{i \in I}$ 是 A 的一个分析 (partition).

定理 1.4.1 对非空集合 A, $R \to A/R$ 定义了 A 上全部等价关系和 A 的全部分拆之间的双射.

证明概要 对等价关系 R, 等价类集合 A/R 是 A 的一个分拆, 从而 $R \mapsto A/R$ 定义函数 $f: E(A) \to Q(A)$, 这里 $E(A)$ 为全部等价关系, $Q(A)$ 为全部分拆. 考虑 $g: Q(A) \to E(A)$, 其中分拆 $S = \{A_i\}_{i\in I}$ 对应关系 $g(S): a \sim b \Leftrightarrow$ 有唯一 $i \in I$, 使得 $a, b \in A_i$. 显然这里 $g(S)$ 为等价关系且 f, g 互为逆, 于是 f 给出如题的双射. □

定义 1.4.5 对 X 和 Y 上的关系 R, Y 和 Z 上的关系 S, 定义其复合

$$R \circ S = \{(x, z) \in X \times Z \mid \exists y \in Y,\, xRy,\, yRz\}.$$

定义 1.4.6 对集族 $\{A_i\}_{i\in I}$, 定义它们的笛卡尔积 $\displaystyle\prod_{i\in I} A_i = \{f : I \to \bigcup_{i\in I} A_i \mid \forall i \in I,\, f(i) \in A_i\}$.

推论 对集族 $\{A_i\}_{i\in I}, \{B_i\}_{i\in I}$, 若 $\forall i \in I, B_i \subset A_i$, 则 $\displaystyle\prod_{i\in I} B_i \subset \prod_{i\in I} A_i$.

定义 1.4.7 对笛卡尔积 $\displaystyle\prod_{i\in I} A_i, \forall k \in I$, 定义映射 $\pi_k : \displaystyle\prod_{i\in I} A_i \to A_k,\ f \mapsto f(k)$ 或 $\{a_i\} \mapsto a_k$ 为其在第 k 分量上的典范射影 (canonical projection). 若每个 A_i 均非空, 则每个 π_k 均是满射.

定理 1.4.2 对集族 $\{A_i\}_{i\in I}$, 则存在集合 D 及映射族 $\{\pi_i : D \to A_i\}_{i\in I}$, 满足: 对任意集合 C 与映射族 $\{\varphi_i : C \to A_i\}_{i\in I}$, 存在唯一的映射 $\varphi : C \to D$ 使得 $\forall i \in I, \pi_i\varphi = \varphi_i$.

注. 集族 $\{A_i\}_{i\in I}$ 确定时 D 在双射意义下唯一; 即若集合 D' 与映射族 $\{\pi'_i : D' \to A_i\}_{i\in I}$ 具有与 D, $\{\pi_i\}$ 同样的性质, 则 D 与 D' 之间存在双射.

Chapter 2

Ordinal and Cardinal

2.1 Axioms of Zermelo-Fraenkel Set Theory

我们先在这里简要介绍 Zermelo–Fraenkel 公理集合论, 并承认选择公理; 这套系统简称 ZFC 公理体系.

定义 2.1.1 Zermelo–Fraenkel 公理体系包含如下公理:

1. 外延公理: 若两集合有相同元素, 则两者相等.
2. 配对公理: 对任意 x, y, 存在集合 $\{x, y\}$, 其元素恰好是 x 与 y.
3. 分离公理模式: 设 P 为关于集合的一个性质, $P(x)$ 表示集合 x 满足性质 P, 则对任意集合 X 存在集合 $Y = \{x \in X \mid P(x)\}$.
4. 并集公理: 对任意集合 X, 存在相应的并集 $\bigcup X = \{u \mid \exists v \in X \text{ s.t. } u \in v\}$.
5. 幂集公理: 对任意集合 X, 其子集构成一集合 $2^X := \{u \mid u \subset X\}$.
6. 无穷公理: 存在无穷集.
7. 替换公理模式: 设 F 为以一个集合 X 为定义域的函数, 则存在集合 $F(X) = \{F(x) \mid x \in X\}$.
8. 正则公理: 任意非空集都含有一个对从属关系 $\in$ 的最小元素.

要注意分离公理模式并不意味着存在集合 $Y' = \{x \mid P(x)\}$, 因为我们有如下的 Russell 悖论:

例 2.1.1 Russell's Paradox: 记 $S = \{X \mid X \notin X\}$, 即其元素是所有不属于其自身的集合; 于是有 $S \notin S \Rightarrow S \in S, S \in S \Rightarrow S \notin S$, 矛盾.

因此我们将 $Y' = \{x \mid P(x)\}$ 修正为分离公理模式中的 $Y = \{x \in X \mid P(x)\}$. Russell 悖论也表明了所有集合组成的集合是不存在的. 所以我们将扩展集合的概念; 在这之前我们需要重述逻辑语言, 即

定义 2.1.2 一个谓词逻辑系统通常由一阶逻辑词 (五个联结词, 两个量词) 与主词, 谓词组成; 集合论中主词一般是集合或元素, 谓词一般是命题或性质, 通常采用主词 (谓词) 的形式表述.

谓词逻辑系统中的对象称作公式 (formula). 特殊地, 由等式谓词 $=$ 和隶属谓词 $\in$ 组成的公式称作元公式 (atomic formula); 我们约定带有自由变量的公式为 $\varphi(u_1, \cdots, u_n)$. 没有自由变量的公式称作语句 (sentence).

定义 2.1.3 对公式 $\varphi(x, u_1, \cdots, u_n)$, 我们称 $\{x \mid \varphi(x, u_1, \cdots, u_n)\}$ 是一个类 (class). 若类 A 能被一个集合 U 包含, 则其也是集合; 否则称其为真类 (proper class).

真类可以被视作某种意义上很大的集合. 显然全体集合组成的类是一个真类.

我们将前面朴素集合论中的若干概念平行地移植到公理集合论上, 不再赘述定义. 为了给出无穷公理的精确表述, 我们必须首先定义有限性的概念, 但我们尚未定义自然数. 于是我们以如下方式表述:

定义 2.1.4 称具有下述性质的集合 S 为归纳集 (inductive set):

$$\exists S\,(\varnothing \in S \wedge (\forall x \in S) x \cup \{x\} \in S).$$

定理 2.1.1 无穷公理等价于存在归纳集.

ZFC 公理体系还需要我们承认选择公理, 我们这里介绍两种常用形式:

定理 2.1.2 选择公理 (Axiom of Choice): 对由非空集合组成的集族 $\{A_i\}_{i\in I}$, 若其下标集合 I 非空, 则它们的积集合非空; 即存在 $S = \{a_i\}$, 满足 $\forall i \in I$, $a_i \in A_i$.

定理 2.1.3 选择函数形式: 对非空集合组成的集族 $\{A_i\}_{i\in I}$, 则存在选择函数 $f : \{A_i\} \to \bigcup A_i$, 其视作从每个集合 A_i 中挑一个元素.

2.2 Ordinal Numbers

为了定义序数, 我们首先要阐述几种序关系:

定义 2.2.1 对非空集合 A 及其上的关系 R, 若它们满足如下三条性质:

$$a \in A \Rightarrow (a, a) \in R; \quad (a, b) \in R,\, (b, c) \in R \Rightarrow\, (a, c) \in R; \quad (a, b) \in R,\, (b, a) \in R \Rightarrow a = b,$$

则称 R 是 A 上的偏序 (partial ordering), A 在 R 下成为偏序集 (partially ordered set).

此时, 若 $(a, b) \in R$, 则一般将其记作 $a \le b$, 此时上述性质记为:

$$\forall\, a, b, c \in A,\, a \le a; \quad a \le b,\, b \le c \Rightarrow\, a \le c; \quad a \le b,\, b \le a \Rightarrow\, a = b.$$

定义 2.2.2 对 $a, b \in A$, 若 $a \le b$ 或 $b \le a$, 则称 a, b 是可比较的 (comparable). 若集合 A 在偏序 $R(\le)$ 系所有元素均可比较, 则称 $R(\le)$ 是线性序 (linear order) 或全序 (total order).

定义 2.2.3 定义两个线性序 $(A, <)$, $(B, <)$ 的积是集合 $A \times B$, 且序关系 $(a_1, b_1) < (a_2, b_2)$ 当且仅当 $b_1 < b_2$ 或 $(b_1 = b_2,\, a_1 < a_2)$.

定义 2.2.4 对偏序集 $(A, \le)$, 若 $\exists a \in A$, 使得对 A 中任一与 a 可比较的元素 c, 都有 $c \le a$ (即若 $c \in A$ 且 $a \le c$, 则 $a = c$), 则称 a 为 A 的极大元 (maximum). 极小元 (minimum) 可类似定义.

定义 2.2.5 对偏序集 $(P, \le)$, $(Q, \le)$ 与 $f : P \to Q$, 若 $x < y \Rightarrow f(x) < f(y)$, 则称 f 保序 (order-preserving). 若双射 $f : P \to Q$ 使得 f, f^{-1} 都保序, 则称 f 是一个同构, 记作 $(P, \le) \cong (Q, \le)$.

在固定了偏序 $\le$ 的情况下, 若无争议我们也简写作 $P \cong Q$.

定义 2.2.6 若偏序集 $(A, \leq)$ 的每个非空子集均有最小元, 则称 A 为良序集 (well-ordered set). 这里定义 $a \in A$ 处的截断为 $A_{<a} = \{x \in A \mid x < a\}$.

定义 2.2.7 如果集合 T 的每个元素都是 T 的子集, 即 $T \subset 2^T$, 则称其传递 (transitive). 如果集合 T 可传递且 $(T, \in)$ 良序, 则称其为序数 (ordinal number), 一般用希腊字母表示.

特殊地, 我们定义 $\alpha < \beta \Leftrightarrow \alpha \in \beta$.

显然 $0 = \varnothing$ 是序数, 且若 β 包含在序数 α 中, 则 β 也是序数.

命题 2.2.1 若 $\alpha \neq \beta$ 都是序数且 $\alpha \subset \beta$, 则 $\alpha \in \beta$. 特殊地, 序数 α, β 满足 $\alpha \subset \beta$ 或 $\beta \subset \alpha$.

证明概要 若 $\alpha \subset \beta$, 取 γ 是 $\beta - \alpha$ 中的最小元, 则 $\alpha = \beta_{<\gamma} = \gamma, \alpha \in \beta$. 特殊地, 设 $\alpha \cap \beta = \gamma$, 则由上可得若 $\gamma \neq \alpha$ 且 $\gamma \neq \beta$, 则 $\gamma \in \alpha$ 且 $\gamma \in \beta, \gamma \in \gamma$, 矛盾! □

我们记所有序数组成的类为 Ord, 显然 $<$ 是 Ord 内的线性序.

引理 良序集不能与其某处的截断同构.

定理 2.2.1 每个良序集 $(W, <)$ 都唯一同构于某一序数 α.

证明概要 唯一性已经由引理保证. 构造

$$S = \{\alpha \mid \exists! x \in A,\, (W_{<x} \cong \alpha)\},$$

于是由替换公理, S 是集合, 这里同构均代表良序意义下同构. 对 $x \in S$, 这样的 α 一定存在, 否则 $x \in W_{<x}$ 矛盾. 这时考虑最小满足 $\gamma \notin S$ 的序数 γ, 则 $S = \gamma$ 且我们有 S 到 γ 的同构. □

定义 2.2.8 对序数 α, 定义后继 (successor) 序数 $\alpha + 1 = \{\alpha\} \cup \alpha$; 若 α 不是某个序数的后继, 则称其为极限 (limit) 序数 $\alpha = \sup\{\beta \mid \beta < \alpha\} = \bigcup \alpha$.

若 S 是一个序数集合, 则显然 $\inf S = \bigcap S$, $\sup S = \bigcup S$ 都是序数. 下面我们构造最小的非零极限序数 ω.

例 2.2.1 我们如下归纳定义:

$$0 = \varnothing,\, 1 = \{\varnothing\},\, 2 = \{\varnothing, \{\varnothing\}\} \cdots,$$

记 $\omega = \{0, 1, \cdots\}$, 于是任一非零极限序数一定包含 ω, 也即其为所有非零极限序数的下确界. ω 在其他时候也记作 $\mathbb{N}$ 或 $\mathbb{Z}_{\geq 0}$, 小于 ω 的序数称作有限序数或自然数.

由 $\inf S$ 的定义, 序数类有最小元, 于是 Ord 对 $\leq$ 良序. 自然地我们可以将归纳法由 ω 拓展到 Ord 上, 也即

定理 2.2.2 超限归纳 (Transfinite Induction): 对序数类 S, $0 \in S$ 且 $\alpha \in S \Rightarrow \alpha + 1 \in S$, 且满足若 α 是非零极限序数且 $\forall \beta < \alpha, \beta \in S \Rightarrow \alpha \in S$, 则 $S = \mathsf{Ord}$.

超限归纳法用于递归构造一列对象, 使得规则在后继和极限的情况下均不改变. 我们 (不证明地) 给出超限递归原理:

定理 2.2.3 超限递归 (Transfinite Recursion): 对任意类的映射 $G : \mathsf{Set} \to \mathsf{Set}$, 存在唯一的类映射 $f : \mathsf{Ord} \to \mathsf{Set}$, 使得

$$\forall \alpha,\, f(\alpha) = G(f\big|_{\alpha}) = G(f\big|_{\beta \mid \beta < \alpha}).$$

这里 Set 代表全体集合组成的真类; 一般书上用 V 表示居多, 我们在此承继范畴论中的用法, 若在可能产生矛盾时会予以说明.

命题 2.2.2 序数的算术律: 考虑序数 α, β, 极限序数 γ, 则其满足算术律:

(1) 加法: $\alpha + 0 = \alpha, \alpha + (\beta + 1) = (\alpha + \beta) + 1, \alpha + \gamma = \sup\{\alpha + \xi \mid \xi < \gamma\}$;

(2) 乘法: $\alpha \cdot 0 = 0, \alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha, \alpha \cdot \gamma = \sup\{\alpha \cdot \xi \mid \xi < \gamma\}$;

(3) 指数: $\alpha^0 = 1, \alpha^{\beta+1} = \alpha^\beta \cdot \alpha, \alpha^\gamma = \sup\{\alpha^\xi : \xi < \gamma\}$.

命题 2.2.3 序数的结合律: 考虑序数 α, β, γ, 则其满足 $\alpha + (\beta + \gamma) = \alpha + \beta + \gamma, \alpha(\beta\gamma) = (\alpha\beta)\gamma$.

命题 2.2.4 序数的 Euclid 性质: 对序数 $\alpha > 0$, 则 $\forall \gamma \in \mathsf{Ord}, \exists! \beta, \rho < \alpha$, 使得 $\gamma = \alpha\beta + \rho$.

定理 2.2.4 Cantor 标准型: 任意序数 $\alpha > 0$ 都能表示成如下 Cantor 标准型:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n,\ \alpha \geq \beta_1 > \beta_2 > \cdots > \beta_n,\ k_i \in \mathbb{N}_+.$$

证明概要 归纳 α, $\alpha = 1 = \omega^0 \cdot 1$ 显然. 任取 $\alpha > 0$, 定义 β 为满足 $\omega^\beta \leq \alpha$ 的最大序数, 则由 Euclid 性质, 存在唯一的 δ 和 $\rho < \omega^\beta$ 使得 $\alpha = \omega^\beta\delta + \rho$, 这里 δ 显然有限. 于是我们超限归纳地证明了唯一性. □

最后, 我们介绍选择公理的两种等价表述: Zorn 引理和良序原理.

定义 2.2.9 若 A 上的偏序关系 R 在非空子集 B 下成为线性序, 则称 B 是 A 上的一个链 (chain).

定理 2.2.5 Zorn 引理: 对非空偏序集 $(A, \leq)$, 若 A 中每个链都有上界, 则 A 必包含极大元.

定理 2.2.6 Zermelo 良序原理: 对任意非空集合 A, 均存在其线性序 $R(\leq)$, 使得 $(A, \leq)$ 为良序集.

练习 2.1 证明**引理**: 良序集不能与其某处的截断同构.

练习 2.2 证明序数的如下性质: 对序数 $\alpha < \beta, \gamma > 0, \theta > 1$, 则

$$\alpha + \gamma < \beta + \gamma,\ \alpha\gamma < \beta\gamma,\ \theta^\alpha < \theta^\beta.$$

练习 2.3 证明序数的 Euclid 性质.

练习 2.4 利用超限归纳法, 在 ZFC 体系内证明 Zorn 引理和 Zermelo 良序原理.

2.3 Cardinal Number

定义 2.3.1 有限集 X 的基数 (cardinal number) 定义为其元素个数, 表示作 $|X|$.

定理 2.3.1 容斥原理: $|A_1 \cup \cdots \cup A_n| = \sum\limits_i |A_i| - \sum\limits_{i<j} |A_i \cap A_j| + \sum\limits_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots$.

定义 2.3.2 对集合 X, Y, 若存在双射 $f : X \to Y$, 则称 X, Y 是等势的 (equipotent) 或有相同的基数, 记作 $X \sim Y$.

显然由定义等势是 Set 上的等价关系.

定义 2.3.3 称集合 A 在等势关系下的等价类为 A 的势 (cardinal number), 记作 $|A|$.

定义 2.3.4 对非交集合 $A, B, |A| = \alpha, |B| = \beta$, 则定义 $|A \cup B| = \alpha + \beta, |A \times B| = \alpha\beta$.

为了使势的概念是元素个数的严格推广. 我们必须研究其的可比较性.

定义 2.3.5 对集合 $A, B, |A| = \alpha, |B| = \beta$, 若 $C \subset A$ 有 $C \sim B$, 即存在单射 $A \to B$, 则记 $\alpha \leq \beta$.

定理 2.3.2 对集合 A 及其幂集 2^A, 则 $|A| < |2^A|$.

证明概要 单射 $a \to \{a\}$ 给出 $|A| \leq |2^A|$. 若 $|A| = |2^A|$, 则考虑双射 $f : A \to 2^A$, 记 $B = \{a \in A \mid a \notin f(a)\} \subset A$, 于是 $\exists a_0 \in A, f(a_0) = B$, 这与 B 的定义矛盾! 于是 $|A| < |2^A|$. □

我们接下来会说明为什么幂集会用 2^A 表示.

定理 2.3.3 Bernstein 定理: 对集合 X, Y, 若 $|X| \leq |Y|$ 且 $|Y| \leq |X|$, 则 $|X| = |Y|$.

证明概要 取单射 $f : X \to Y, g : Y \to X$, 显然 $gf : X \to X$ 单. 令 $X_1 = g(Y), X_2 = gf(X)$, 则 $g : Y \to X_1, g \circ f : X \to X_2$ 都是双射,$X_2 \subset X_1 \subset X$. 于是只需证明: 若 $X_2 \subset X_1 \subset X$ 且 X 和 X_2 等势, 则 X 和 X_1 等势.

令 $h^{(1)} = h : X \to X_2$, 递归定义 $h^{(i+1)} = h\big|_{X_2} \circ h^{(i)} : X \to X_2$. 构造

$$T = (X - X_1) \cup \bigcup_{i \in \mathbb{N}_+} h^{(i)}(X - X_1),$$

则计算可得

$$h(T) = h(X - X_1) \cup h\left(\bigcup_{i \in \mathbb{N}_+} h^{(i)}(X - X_1)\right) = \bigcup_{i \in \mathbb{N}_+} h^{(i)}(X - X_1).$$

于是 $T = (X - X_1) \cup h(T)$, 定义 $\xi : X \to X_2$ 使得 $\xi\big|_T = h\big|_T, \xi\big|_{X-T} = 1_{X-T}$. 结合 $h(T) \subset T$, 于是 $h(T) \cap (X - T) = \varnothing, \xi$ 单. 另一方面,

$$\xi(X) = h(T) \cup (X - T) = (h(T) \cup X_1) \cap (h(T) \cup (X - h(T))) = X_1 \cap X = X_1.$$

所以 ξ 满, 因此 ξ 是双射. □

推论 若 α, β 是势, 则下述三者有且仅有一条成立: $\alpha < \beta; \alpha = \beta; \alpha > \beta$.

定义 2.3.6 自然数集 $\mathbb{N}$ 的势记为 $\aleph_0$, 若 $|A| = \aleph_0$, 则称 A 是可数集 (denumerable set).

定理 2.3.4 集合 A 是可数集的充要条件是它能被排为列 $\{a_n\}_{n=1}^{\infty}$; 任何无限集必含有可数子集.

推论 $\aleph_0$ 是最小的无限集的势; 可数集的任何无限子集是可数集.

命题 2.3.1 可数集的可数并是可数集, 即 $\aleph_0 \times \aleph_0 = \aleph_0$.

证明概要 对角线原则. □

注. 我们这里需要用到选择公理 (思考哪里用到的?).

命题 2.3.2 对无限集 A 和可数集 B, 则 $|A \cup B| = |A|$.

证明概要 不失一般性假设 A, B 非交, 取 A 的可数子集 $P, Q = A - P$. 于是 $B + P$ 和 P 之间存在双射, 并且显然能通过恒等映射将其扩大到 $B + P + Q$ 到 $P + Q$ 上. □

定义 2.3.7 对有限集 $A, B, |A| = \alpha, |B| = \beta$, 记所有函数 $f : B \to A$ 的集合为 A^B; 记 $\alpha^\beta = |A^B|$.

定理 2.3.5 幂运算对势成立, 也即 $\alpha^{\beta+\gamma} = \alpha^\beta \times \alpha^\gamma, (\alpha\beta)^\gamma = \alpha^\gamma \times \beta^\gamma, (\alpha^\beta)^\gamma = \alpha^{\beta\times\gamma}$.

定义 2.3.8 我们记 $\aleph_1$ 为最小的不可数 (无穷) 势; 称 $\mathbb{R}$ 的势为连续统, 记作 c.

命题 2.3.3 $c = 2^{\aleph_0}, c \times c = c, c^{\aleph_0} = c$.

证明概要 $c \times c = 2^{\aleph_0} \times 2^{\aleph_0} = 2^{\aleph_0+\aleph_0} = 2^{\aleph_0} = c; c^{\aleph_0} = \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0\times\aleph_0} = 2^{\aleph_0} = c.$ □

定理 2.3.6 Koenig 定理: 设 $A_1 \times A_2 \times \cdots \times A_n = B_1 \cup B_2 \cup \cdots \cup B_n$, 则存在 i 使得 $|A_i| \le |B_i|$.

证明概要 考察 $B_i \subset A_1 \times A_2 \times \cdots \times A_n$ 在 $A_i (i = 1, \cdots, n)$ 上的射影, 即 A_i 中所有作为 B_i 中第 i 个元素出现的元素的集合. 如果其与某个 A_i 相等定理即证; 否则令 $x_i \in A_i$ 是未被覆盖的点, 但 n 元组 $(x_1, \cdots, x_n)$ 不属于任何 B_i, 矛盾. □

定理 2.3.7 基数形式的 Koenig 定理: 若 $\forall i = 0, 1, \cdots$ 都有势的大小关系 $\beta_i < \alpha_i$, 则

$$\beta_0 + \beta_1 + \beta_2 + \cdots < \alpha_0 \times \alpha_1 \times \alpha_2 \times \cdots .$$

练习 2.5 证明等势关系是一种等价关系.

练习 2.6 证明势的大小关系是一种序关系.

练习 2.7 证明 $\mathbb{R}$ 不可数.

练习 2.8 证明 (非严格) 单增函数 $f : \mathbb{R} \to \mathbb{R}$ 在最多除掉某些可数集之外处处连续.

练习 2.9 证明对不可数无限集 A 和可数集 B, 则证明 $|A - B| = |A|$.

Part II

Algebra

Chapter 3

Groups

我们对于代数的研究始于数论, 逐渐转移到各种代数结构上. 在研究各种代数结构的基础上, 人们逐渐总结出了一些基本的抽象概念, 而最基础的便是我们这里研究的群.

3.1 Groups and Homomorphisms

为了研究代数结构, 我们首先要给出一般情况下的代数运算的定义:

定义 3.1.1 对非空集合 G, 称映射 $g : G \circ G \to G$ 为 G 上的一个二元运算 (binary operation).

在无特殊说明时, 采用 ab 代替二元运算 $a \circ b$, 并称 ab 为 a 与 b 的积.

我们能看到这是一个相当广泛的概念, 它只给出了同一个集合 G 中任两个 (可相等的) 元素对应到 G 中一个 (不必与前面的元素互异的) 元素. 我们可以举出各样的二元运算的例子, 但是为了更贴合某些代数结构, 我们一般只考虑某些具有特定性质的运算. 此外, 要注意到这里的运算只涉及到一个集合, 诸如向量的内积等涉及到两个集合的运算并不在我们此处的考虑范围之内.

我们首先来介绍群的概念及其各种下层概念:

定义 3.1.2 半群 (semigroup) 是含满足结合律 $\forall a, b, c \in G, a(bc) = (ab)c$ 的二元运算的集合 G.

幺半群 (monoid) 是含有双侧幺元 (identity element) 的半群 G. 其中, 幺元 $e \in G$ 是指使得 $\forall a \in G$, $ae = ea = a$ 的元素.

群 (group) 是含双侧逆元 (inverse element) 的幺半群 G. 其中, $\forall a \in G$ 的逆元是指 $\exists a^{-1} \in G$, 使得 $a^{-1}a = aa^{-1} = e$. 一般将运算 $\circ$ 下的群 G 记作群 $(G, \circ)$.

若 G 上的二元运算满足交换律 $\forall a, b \in G$, $ab = ba$, 则称 G 是交换的 (commutative). 若 G 是群, 则称 G 是 Abel 群 (abelian group).

我们首先来看几个常见的例子:

例 3.1.1 全体正实数 $\mathbb{R}_+$ 对于通常意义下的乘法成为一个群 $(\mathbb{R}_+, \times)$; $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 在通常意义下的加法下都是群.

例 3.1.2 数域 F 上的全体 n 阶矩阵全体对矩阵乘法构成幺半群, 其幺元为单位矩阵, 但它不是群 (零矩阵不可逆). 可逆矩阵全体对矩阵乘法构成一个群, 记作 $\mathrm{GL}_n(F)$, 称作一般线性群 (general linear group); $\mathrm{GL}_n(F)$ 中全体行列式为 1 的矩阵对于矩阵乘法也构成一个群, 记为 $\mathrm{SL}_n(F)$, 称作特殊线性群 (special linear group).

这里需要注意的一点是幺元和逆元的写法并不唯一, 如加法群下幺元一般记作 0 而逆元记作 $-a$, 但乘法群下幺元一般记作 e 或 1 而逆元记作 a^{-1}. 另外地, 乘幂和可列个元素的积也采用类似的方式递归定义. 上述矩阵所构成的群下, 幺元一般记作单位矩阵 I. 我们在一般情况下更多地将 Abel 群表示作加法群, 非 Abel 群表示作乘法群, 其他情况依照题目所给元素考虑.

定义 3.1.3 称群 G 的势 $|G|$ 为 G 的阶 (order). 若 $|G|$ 有限 (无限), 则称 G 是有限群 (无限群).

命题 3.1.1 若 G 是幺半群, 则其幺元 e 唯一; 若 G 是群, 则:

(1) $\forall c \in G, cc = c \Rightarrow c = e$.

(2) 左右消去律 (cancellation): $\forall a, b, c \in G, ab = ac \Rightarrow b = c; ba = ca \Rightarrow b = c$.

(3) $\forall a \in G$, 逆元 a^{-1} 存在且唯一.

(4) $\forall a, b \in G, (a^{-1})^{-1} = a, (ab)^{-1} = b^{-1}a^{-1}$.

(5) $\forall a, b \in G$, 方程组 $ax = ya = b$ 在 G 上有唯一解: $x = a^{-1}b, y = ba^{-1}$.

证明概要 幺元唯一: 考虑若 e, e' 都是双侧幺元, 则 $e = ee' = e'e = e'$.

(1): $cc = c \Rightarrow c^{-1}cc = c^{-1}c \Rightarrow ec = e \Rightarrow c = e$;

(4): $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$.

剩下的部分也可类似地通过同乘幺元或逆元得到, 留作练习. □

很显然这里我们给出群的定义之后, 如果总是依靠定义去判断是否是群显然是很繁琐的. 于是我们首先要给出一些判定方式:

命题 3.1.2 对半群 G, 若 G 上存在单侧幺元且任一元素均有同侧逆元, 则 G 是群.

证明概要 设左幺元 $e \in G$, 左逆元存在, 考虑 $(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = aa^{-1}$, 则 $aa^{-1} = e$, a^{-1} 为双侧逆. 于是 $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$, 则 e 为双侧幺元, G 是群. □

思考: 为什么一定要求幺元和逆元同侧? 参见练习中的范例: floop.

事实上群这一概念在最早的论文:

Mémoire sur les conditions de résolubilité des équations par radicaux, Galois

中群的定义与现在是大不相同的. 最早 Galois 在考虑多项式时, 将 $f(x)$ 根的集合 $\{x_1, x_2, \cdots, x_n\}$ 到其自身的单射称为这些根的一个置换, 而 $G_j = \{\sigma_{jl}\}$, $l = 1, 2, \cdots, m$ 这 m 个不同映射构成的集合为一个置换的群 (un groupe de permutations). 用现代语言来讲, 就是:

例 3.1.3 对非空集合 X, 双射 $X \to X$ 称为 X 的一个置换 (permutation). X 的所有置换组成的集合 $S(X)$ 在函数结合律下成为群, 称为 X 的置换群 (the group of permutations).

设 $X = \{1, 2, 3, \cdots, n\}$, 则称 $S(X)$ 为 n 元对称群 (symmetric group), 记作 S_n. $|S_n| = n!$.

这下我们知道了群现在定义的本质: 结合律是自然的要求, 幺元和逆元是加法与乘法的自然推广, 也即映射的线性运算与结合.

实际上在最开始的定义中我们可以看到群是与对称紧密结合的,群也就是一些封闭的对称的总体. 置换群作为群的引入与群作用的等价,在群论中有着极其重要的地位,我们会在后面详细介绍.

例 3.1.4 S_3 是 6 阶 Abel 群, 是阶最小的非 Abel 群.

下面我们考虑一些利用已有的群定义新群的方式. 我们一般称群 $(G, \circ)$ 中元素所组成的集合 G 为该群的底集 (underlying set). 自然地,我们采用第一部分中集合论的一些运算方式,在群的底集上进行集合的运算.

定义 3.1.4 群 G, H 在二元运算 $\forall a, a' \in G,\ b, b' \in H,\ (a, b)(a', b') = (aa', bb')$ 下成为群, 称为 G, H 的直积 (direct product), 记为 $G \times H$.

这里, $G \times H$ 的幺元为 (e_G, e_H), (a, b) 的逆元为 (a^{-1}, b^{-1}); 且 $|G \times H| = |G|\,|H|$. 另外, 若 G, H 都是 Abel 群, 则 $G \times H$ 也是 Abel 群.

定义 3.1.5 对幺半群 G 上的等价关系 $\sim$, 若 $\forall a, b, c, d \in G,\ a \sim b,\ c \sim d \Rightarrow ac \sim bd$, 则称 $\sim$ 是 G 上的一个同余关系 (congruence relation).

命题 3.1.3 若 $\sim$ 是幺半群 G 上的同余关系, 则 G 对 $\sim$ 的商集 $G/\sim$ 对于运算 $(\overline{a})(\overline{b}) = \overline{ab}$ 是幺半群, 其中 $\overline{x}$ 表示 $x \in G$ 在 $\sim$ 下的等价类. 特殊地, 若 G 是 (Abel) 群, 则 $G/\sim$ 也是 (Abel) 群.

证明概要 依次验证定义即可. □

现在我们从在某种方面限制群,给出一个类似子集的结构.

定义 3.1.6 对群 G 及其非空子集 H, 若 H 在 G 中二元运算 ab 下成为群且 H 对 ab 乘积封闭, 则称 H 是 G 的子群 (subgroup), 表示为 $H < G$. 这里, 对乘积封闭 (closed) 指 $\forall a, b \in H, ab \in H$.

若 $H < G, H \neq G$ 且 H 不为平凡 (trivial) 子群 $\{e\}$, 则称其为 G 的真子群 (proper subgroup).

定理 3.1.1 若 H 是 G 的非空子集, 则 $H < G \Leftrightarrow \forall a, b \in H,\ ab^{-1} \in H$.

证明概要 只需证明 $\Leftarrow$, 这时 $e = aa^{-1} \in H$, 于是 $\forall b \in H, b^{-1} = eb^{-1} \in H, ab = a(b^{-1})^{-1} \in H$. 因此 $H < G$. □

显然我们有对群 G 的非空子群族 $\{H_i\}_{i \in I}$, $\bigcap\limits_{i \in I} H_i$ 是 G 的子群.

定义 3.1.7 若 G 是群且 $X \subset G$, 令 $\{H_i\}_{i \in I}$ 是 G 中包含 X 的全体子群构成的子群族, 则称 $\bigcap\limits_{i \in I} H_i$ 是 X 生成 (generate) 的 G 的子群, 记作 $\langle X \rangle$. 这里, X 的元素称为 $\langle X \rangle$ 的生成元. 特殊地,

(1) 若 $X = \{a_1, \cdots, a_n\}$, 则记 $\langle X \rangle = \langle a_1, \cdots, a_n \rangle$, 称其为是有限生成的, 记作 f.g;

(2) 若 $X = \{a\}$, 则 $\langle X \rangle = \langle a \rangle$ 称作 a 生成的循环群 (cyclic group).

注. $\langle X \rangle$ 的生成元不一定唯一, 即有可能 $\exists X, Y \in G, X \neq Y$ 但 $\langle X \rangle = \langle Y \rangle$.

例 3.1.5 Klein 四元群 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 是阶最小的非循环 Abel 群.

定义 3.1.8 若 G 是群且 $a \in G$, 则循环子群 $\langle a \rangle$ 的阶也简记作 a 的阶 (order), 记作 $|a|$.

定理 3.1.2 若 X 是群 G 的非空子集, 则 $\langle X \rangle$ 是全体有限乘积 $\prod\limits_{i=1}^{t} a_i^{n_i}$, $(a_i \in X,\ n_i \in \mathbb{Z})$ 构成的集合. 特

别地, $\langle a\rangle = \{a^n \mid n\in\mathbb{Z}\}$.

证明概要 考虑证明这样的乘积全体构成的集合 H 是 G 中包含 X 的子群, 且 G 中每个包含 X 的子群也包含 H. □

定义 3.1.9 对群 G 的子集族 $\{H_i\}_{i\in I}$, $\bigcup\limits_{i\in I} H_i$ 一般不是 G 的子群. 称 $\langle\bigcup\limits_{i\in I} H_i\rangle$ 为由集族 $\{H_i\}_{i\in I}$ 生成的子群. 记 $\langle H_1\bigcup H_2\rangle = H_1\vee H_2$. G 是 Abel 群时, $H_1\vee H_2=\{ab \mid a\in H_1,\, b\in H_2\}$.

在代数学的研究中我们聚焦于代数结构, 而我们期望那个在某种运算之下代数结构能保持一定的稳定性. 而同态的意义便是使得代数结构保持不变的函数.

定义 3.1.10 对半群 G,H, 若 $\exists f: G\to H$, 使得 $\forall a,b\in G$, $f(ab)=f(a)f(b)$, 则称 f 为同态 (homomorphism). 若 f 是单射, 则称其为单同态 (monomorphism); 若 f 是满射, 则称其为满同态 (epimorphism); 若 f 是双射, 则称其为同构 (isomorphism).

同态 $f: G\to G$ 称作 G 上的自同态 (endomorphism), 同构 $f: G\to G$ 称为 G 上的自同构 (automorphism).

定义 3.1.11 对群 G,H 上的同态 $f: G\to H$, 若 $e_G\mapsto e_H$, $a^{-1}\mapsto f(a)^{-1}$ $(\forall a\in G)$, 则称 f 是群同态. 类似定义群的 (满, 单, 自) 同态.

这时, 定义 f 的核 (kernel) 为 $\operatorname{Ker} f=\{a\in G \mid f(a)=e\in H\}$; 定义 f 的像 (image) 为 $\operatorname{Im} f = f(G)=\{b\in H \mid \exists a\in G,\, b=f(a)\}$. 此时对 $A\in G$, $\operatorname{Im} A=\{b\in H\mid \exists a\in A,\, b=f(a)\}$ 称为 A 的像; 对 $B\subset H$, $f^{-1}(B)=\{a\in G \mid f(a)\in B\}$ 称作 B 的原像 (inverse image).

例 3.1.6 对群 G,H,

(1) $\operatorname{Hom}(G,H)$ 表示 $G\to H$ 全体同态组成的集合;

(2) $\operatorname{End} G=\operatorname{Hom}(G,G)$ 表示 G 上全体自同态组成的集合, 它是幺半群;

(3) $\operatorname{Aut} G$ 表示由 G 上全体自同构组成的集合, 它是群.

定理 3.1.3 对群同态 $f: G\to H$,

(1) f 是单同态的充要条件是 $\operatorname{Ker} f=\{e\}$;

(2) f 是同构的充要条件是存在逆同态 $f^{-1}: H\to G$, 使得 $ff^{-1}=1_H$, $f^{-1}f=1_G$.

证明概要 (1) 注意到 $f(a)=f(b)\Leftrightarrow e_H=f(a)f(b)^{-1}=f(a)f(b^{-1})=f(ab^{-1})$, $ab^{-1}=\operatorname{Ker} f$ 即可; (2) 依定义依次验证单与满. □

练习 3.1 证明或否定: 若半群 G 中成立消去律, 则其一定是群.

练习 3.2 证明或否定: 具有左幺元, 且每个元素均有右逆的半群 G 一定是群.

练习 3.3 对半群 G, 证明它是群的充要条件是 $\forall a,b\in G$, 方程组 $ax=ya=b$ 在 G 上均有解.

练习 3.4 记 $\mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\cdots,\overline{m-1}\}$ 为 $\mathbb{Z}$ 在模 m 下的等价类集合, 证明:

(1)$\mathbb{Z}_m$ 关于运算 $\overline{a}+\overline{b}=\overline{a+b}$, $(a,b\in\mathbb{Z})$ 成为 m 阶有限 Abel 群;

(2)$\mathbb{Z}_m$ 关于运算 $(\overline{a})(\overline{b})=\overline{ab}$, $(a,b\in\mathbb{Z})$ 成为有限交换幺半群;

(3) 若 p 是素数, 则 $\mathbb{Z}_p$ 中的非零元形成 $p-1$ 阶乘法群.

练习 3.5 证明若对群 G 的任意元素 a, 都有 $a^2=e$, 则 G 是 Abel 群.

练习 3.6 对群同态 $f: G \to H$, 证明 $\operatorname{Ker} f < G, \operatorname{Im} f < H$.

练习 3.7 证明 $\{\sigma \in S_n \mid \sigma(n)=n\} \cong S_{n-1}$.

练习 3.8 证明有限群 G 中的每个元素的阶一定有限; 并判断反之是否成立.

练习 3.9 证明偶数阶有限群一定包含阶为 2 的元素.

练习 3.10 证明 Abel 群 G 的有限阶元素全体构成 G 的子群; 并判断若 G 非 Abel 该命题是否还成立.

3.2 Cyclic Groups

为了更好地研究群的相关性质, 我们从一类结构相当简单的群入手: 循环群, 并考虑刻画出同构意义下的全体循环群.

命题 3.2.1 $\mathbb{Z}$ 的每个子群 G 在加法下成为循环群. 记 G 中最小非负整数为 m, 则 $G=\langle m\rangle$.

证明概要 $m=0$ 时平凡, 只考虑 G 包含一最小的正整数 m, 此时显然有 $\langle m\rangle = k\mathbb{Z} \subset G$. 另一方面, $\forall k \in G$, 取其带余除法 $k=qm+r$ 形式, 这里 $q, r \in \mathbb{Z}$, $0 \le r < m$. 于是 $r \in G$, 由 m 最小性推出 $r=0, k=qm, G \subset \langle m\rangle$. 这就证明了 $G=\langle m\rangle$. □

定理 3.2.1 每个无限循环群均同构于加法群 $\mathbb{Z}$, 每个 m 阶有限循环群均同构于加法群 $\mathbb{Z}_m$.

证明概要 对循环群 $G=\langle a\rangle$, 考虑满射 $\varphi: \mathbb{Z} \to G$, $k \mapsto a^k$. 分类讨论:

(1) $\operatorname{Ker}\varphi = 0$, 则其为同构, $\mathbb{Z} \cong G$.

(2) $\operatorname{Ker}\varphi \neq 0$, 则 $\operatorname{Ker}\varphi < G$. 由上述命题可知 $\operatorname{Ker}\varphi = \langle m\rangle$, 其中 m 为 a 的阶. 计算可知 $\forall r, s \in \mathbb{Z}$, $a^r = a^s \Leftrightarrow \bar{r} = \bar{s} \in \mathbb{Z}_m$, 于是 $\psi: \mathbb{Z}_m \to G$, $\bar{k} \mapsto a^k$ 良定义. 类似 (1) 便有 $\mathbb{Z}_m \cong G$. □

命题 3.2.2 若 G 是群且 $a \in G$, e 是 G 的幺元,

(1) 若 a 无限阶, 则: (i) $a^k = e \Leftrightarrow k=0$; (ii) 元素 a^k, $(k \in \mathbb{Z})$ 两两互异.

(2) 若 a 有限阶, 则设其阶数为 $m>0$, 则:

(i) m 是满足 $a^m=e$ 的最小整数, $a^k = e \Leftrightarrow m|k$, $a^r = a^s \Leftrightarrow r \equiv s \pmod m$;

(ii) $\langle a\rangle$ 由元素 $a, a^2, \cdots, a^m = e$ 所构成;

(iv) 对任意满足 $k|m$ 的 $k \in \mathbb{Z}$, 则 a^k 的阶 $|a^k| = \dfrac{m}{k}$.

证明概要 类似上述**定理** 3.2.1 的证明过程即可. □

事实上, 循环群 $G=\langle m\rangle$ 的每个子群都是循环群. 特别地, $H \subset G$ 且 H 非平凡时, 记 n 为满足 $m^n \in H$ 的最小正整数, 则 $H=\langle m^n\rangle$. 更一般地, 循环群的同态像也是循环群 $\langle f(m)\rangle$.

命题 3.2.3 对循环群 $G = \langle a \rangle$, 则:

(1) G 是无限群时, 只有 a 和 a^{-1} 为 G 的生成元;

(2) G 是有限群时, a^k 为 G 生成元的充要条件是 $(k, m) = 1$.

证明概要 留作练习. 提示: 只需假定 $G = \mathbb{Z}$ 或 $G = \mathbb{Z}_m$ 即可. □

练习 3.11 若群 G 的所有子群都是循环群, 则 G 是否一定是循环群?

练习 3.12 完善**命题** 3.2.3 的证明.

练习 3.13 对群 G 及其循环子群 $H \neq K$, 若 $|H| = |K|$, 则是否 $H \cap K = \{e\}$?

练习 3.14 证明群 G 为无限循环群的充要条件是它同构于其任一真子群.

练习 3.15 证明素数阶的有限群一定是循环群.

3.3 Cosets

这一节里我们首先考虑研究陪集的性质,从而引出有限群的结构与其阶数之间的关系. 若 $ab^{-1} \in H$ ($a^{-1}b \in H$), 则称 a 模 H 右 (左) 同余于 b.

命题 3.3.1 对群 G 及其子群 H, 模 H 左右同余均是 G 上的等价关系.

证明概要 依定义逐次验证. □

定义 3.3.1 对群 G 的子群 H 及 $a \in H$, 则 a 模 H 左 (右) 同余的等价类是集合

$$aH = \{ah \mid h \in H\}\ .(Ha = \{ha \mid h \in H\}).$$

称 $aH(Ha)$ 为 H 在 G 中生成的左 (右) 陪集 (coset); 称 H 在 G 中全体左 (右) 陪集组成的集合为 G 对 H 的左 (右) 商集 (quotient set).

更一般地, 对群 G 及 $H, K \subseteq G$, 则 $HK = \{ab \mid a \in H, b \in K\}$.

显然有 $\forall a \in G, |Ha| = |aH| = |H|$.

命题 3.3.2 对群 G 的子群 H, 则:

(1) G 是 H 在 G 中的全体左 (右) 陪集之并;

(2) H 在 G 中的任意两个左 (右) 陪集非交或相等, 其中

$$\forall a, b \in G,\ Ha = Hb \Leftrightarrow ab^{-1} \in H,\ aH = bH \Leftrightarrow a^{-1}b \in H;$$

(3) 设 G 对 H 的左右商集为 $\mathcal{L}, \mathcal{R}$, 则 $|\mathcal{L}| = |\mathcal{R}|$.

证明概要 (1), (2) 类似集合论中的证明, (3) 注意到 $Ha \mapsto a^{-1}H$ 是双射即可. □

定义 3.3.2 对群 G 的子群 H, 定义 H 在 G 中的指数 (index) 为 $[G:H]=|\mathcal{L}|=|\mathcal{R}|$.

我们主要感兴趣的是指数有限的情形, 从而建立若干子群的数论性质与群 G 本身的数论性质之间的对应. 但要注意的是 G,H 均为无限群时, $[G:H]$ 也可能有限. 如 $[\mathbb{Z}:m\mathbb{Z}]=m$.

命题 3.3.3 若群 K,H,G 满足 $K<H<G$, 则 $[G:K]=[G:H][H:K]$.

证明概要 考虑非交陪集之并 $G=\bigcup\limits_{i\in I}Ha_i, a_i\in G, |I|=[G:H]; H=\bigcup\limits_{j\in J}Kb_j$ 类似. 于是

$$G=\bigcup_{i\in I}Ha_i=\bigcup_{i\in I,j\in J}Kb_ja_i.$$

若 $Kb_ja_i=Kb_ra_t\Rightarrow b_ja_i=kb_ra_t,\ k\in K$. 于是 $b_j,b_r,k\in H, Ha_i=Ha_t, i=t$. 类似地, $j=r$. 于是这里 Kb_ja_i 也两两非交, $[G:K]=|I\times J|=|I|\cdot|J|=[G:H][H:K]$. □

定理 3.3.1 Lagrange 定理: 对群 $H<G$, 则 $|G|=[G:H]\cdot|H|$. 特别地, G 是有限群时, $|H|\mid|G|$.

证明概要 是上述命题的直接推论. □

Lagrange 定理的逆命题不成立. 这事实上是群论中 Sylow 定理部分的内容, 但我们这份讲义不涉及. 有兴趣者可参考抽象代数的任一本教材进行进一步学习. 但是我们在这里依旧用例子来说明.

例 3.3.1 Lagrange 定理逆命题不成立: 考虑对称群 S_4 中所有偶置换构成的交错群

$$A_4=\{(1),(12)(34),(13)(24),(14)(23),(123),(132),(124),(142),(134),(143),(234),(243)\},$$

它有三个二阶元素 $(12)(34),(13)(24),(14)(23)$, 其余八个元素都是三阶元素, 但是没有 6 阶元素.

这里所用到的交错群与置换群的一般性质我们会在本章最后加以阐述.

命题 3.3.4 对群 G 的有限子群 H,K, 有 $|HK|=\dfrac{|H||K|}{|H\cap K|}$.

证明概要 考虑 $H\cap K<K$, 设 $[K:H\cap K]=n$. 注意到 K 是 n 个非交右陪集的并 $K=\bigcup\limits_{i=1}^{n}(H\cap K)k_i$, 同时左乘 H 且注意到 $H(H\cap K)=H$ 便有 $HK=\bigcup\limits_{i=1}^{n}Hk_i$, 结合 Lagrange 定理, $|HK|=|H|n=\dfrac{|H||K|}{|H\cap K|}$. □

其实还有很多重要的关于指数的性质, 但我们在本讲义中不作进一步探讨. 我们将其列出若干:

命题 3.3.5 对群 G 的指数有限子群 H,K, 若 $[G:H],[G:K]$ 互素, 则 $G=HK$.

命题 3.3.6 对群 $H,K<G$, $[H:H\cap K]\le[G:K]$. 特别地, $[G:K]$ 有限时,

$$[H:H\cap K]=[G:K]\Leftrightarrow G=KH.$$

练习 3.16 对群 G 及其子群 $H,K,\forall a\in G$, 证明或否定:

(1) 左右陪集 aH,Ha 是否一定是 G 的子群?

(2) 左右陪集 aH, Ha 是否一定相等?

(3) 若 H, K 都是有限子群, 则 HK 是否一定是 G 的子群?

练习 3.17 完善**命题** 3.3.2 的证明.

练习 3.18 证明四阶群在同构意义下只有 $\mathbb{Z}_4$ 和 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

练习 3.19 对群 G 及其子群 H, K, 证明 HK 是 G 的子群的充要条件是 $HK = KH$.

3.4 Normal Groups

这部分我们考虑说明所谓正规子群的性质, 它与商群, 同态, 同构之间有着及其密切的关系. 最后我们引入了同态基本定理和三大同构基本定理, 它们在之后的学习中应用十分广泛. 我们前面已经说过 G 模 H 左右同余不一定一致, 但是在研究某些以 G 为定义域的同态时我们需要尽可能使其结构对称. 所以我们引入如下定义:

定义 3.4.1 对群 G 及其子群 N, 下面 5 个条件彼此等价:

(1) G 上模 N 的左右同余在 G 上定义出相同的等价关系, 即 $\forall a \in G, aN = Na$;

(2) N 在 G 中的每个左陪集均是 N 在 G 中的右陪集;

(3) $\forall a \in G, aNa^{-1} = N$, 其中 $aNa^{-1} = \{ana^{-1} \mid n \in \mathbb{N}\}$;

(4) $\forall a \in G, aNa^{-1} \subset N$.

满足上述等价条件的子群 N 称作 G 中的正规子群 (normal group), 记作 $N \lhd G$.

证明概要 (2) $\Rightarrow$ (1): 若 $aN = Nb$, 则 $a \in Nb \cap Na \Rightarrow Nb = Na$.

(4) $\Rightarrow$ (3): 注意到 $aNa^{-1} \subset N, a^{-1}Na \subset N$, 于是 $\forall n \in \mathbb{N}, n = a(a^{-1}na)a^{-1} \in aNa^{-1}, aNa^{-1} \supset N$. 于是 $\forall a \in G, aNa^{-1} = N$.

其余地, (1) $\Rightarrow$ (4), (3) $\Rightarrow$ (2) 都是显然的. □

显然地, Abel 群的每个子群都正规; 对群同态 $f: G \to H$, $\operatorname{Ker} f$ 是 G 的正规子群.

例 3.4.1 正规子群不具有传递性, 即若 $N \lhd M, M \lhd G$, 不一定能推出 $N \lhd G$. 如取

$$N = \{(1), (12)(34)\},\ M = \{(1), (12)(34), (13)(24), (14)(23)\},\ G = S_4.$$

定义 3.4.2 若群 G 无真正规子群, 则称 G 为单群 (simple group).

命题 3.4.1 对群 G 的子群 N, K, 若 $N \lhd G$, 则:

(1) $N \cap K \lhd K$;

(2) 若 $N < K$, 则 $N \lhd K$, 特殊地, $N \lhd \langle N \cup K \rangle$;

(3) $NK = \langle N \cup K \rangle = KN$.

证明概要 (1): 考虑 $n \in N \cap K, a \in K$, 则 $N \lhd G \Rightarrow ana^{-1} \in N, K < G \Rightarrow ana^{-1} \in K$. 于是

$a(N\cap K)a^{-1}\subset N\cap K, N\cap K\lhd K$.

(2): 注意到由定义 $\forall a\in G, aNa^{-1}\subset N$, 于是 $\forall a\in K, aNa^{-1}\subset N, N\lhd K$. 结合 $N<\langle N\cup K\rangle$ 即证.

(3): $NK\subset\langle N\cup K\rangle$ 显然. 注意到 $\forall x\in\langle N\cup K\rangle, x$ 具有形式 $\prod n_ik_i, n_i\in N, k_i\in K$. 结合 $N\lhd G$, $n_ik_j=k_jn_i'$, 则 x 具有形式 $n(\prod k_i)\in NK, \langle N\cup K\rangle\subset NK$. 于是 $NK=\langle N\cup K\rangle=KN$. $\square$

定义 3.4.3 对群 G 的正规子群 N, 称 N 在 G 中全体陪集构成的集合为 G 对于 N 的商群 (quotient group), 记作 G/N.

命题 3.4.2 对群 G 的正规子群 N, 对于二元运算 $(aN)(bN)=abN, G/N$ 是 $[G:N]$ 阶群.

证明概要 首先依定义验证模 N 同余是等价关系, 然后结合陪集与指数的定义即可. $\square$

定义 3.4.4 若 $N\lhd G$, 则映射 $\pi: G\to G/N, a\mapsto aN$ 是满同态, $\operatorname{Ker}\pi=N$. 称 π 为 G 对 N 的典范同态 (canonical epimorphism), 也记作 $\pi: G\hookrightarrow G/N$.

定理 3.4.1 同态基本定理 (Homomorphism Theroem): 对群同态 $f: G\to H$, 若 $N\lhd G$ 且 $N\subseteq\operatorname{Ker}f$, 则存在唯一的同态

$$g: G/N\to H,\ aN\mapsto f(a),\ (\forall a\in G).$$

这里, $\operatorname{Im}f=\operatorname{Im}g, \operatorname{Ker}g=\operatorname{Ker}f/N$, g 是同构的充要条件是 f 为满同态且 $N=\operatorname{Ker}f$.

该结论也可以叙述为: 存在唯一的同态 $g: G/N\to H$, 使得下图交换:

$$\begin{tikzcd}
 & G \arrow[dl, hook] \arrow[dr] & \\
G/N \arrow[rr, "g"] & & H
\end{tikzcd}$$

证明概要 考虑 $b=an\in aN, n\in N<\operatorname{Ker}f$, 则 $f(b)=f(an)=f(a)f(n)=f(a)e=f(a)$, 于是映射 $g: G/N\to H, aN\mapsto f(a)$ 良定义. 验证定义则知 g 是同态. 于是 $\operatorname{Im}f=\operatorname{Im}g$,

$$aN\in\operatorname{Ker}g\Leftrightarrow f(a)=e\Leftrightarrow a\in\operatorname{Ker}f, \Rightarrow\operatorname{Ker}g=\{aN\mid a\in\operatorname{Ker}f\}=(\operatorname{Ker}f)/N.$$

显然 g 为满同态 $\Leftrightarrow f$ 是满同态, g 为单同态 $\Leftrightarrow\operatorname{Ker}g=\operatorname{Ker}f/N=\{e\}\Leftrightarrow\operatorname{Ker}f=N$. $\square$

定理 3.4.2 第一同构定理 (1st Isomorphism Theroem): 群同态 $f: G\to H$ 诱导出同构

$$G/\operatorname{Ker}f\cong\operatorname{Im}f.$$

证明概要 将同态基本定理应用于 $N=\operatorname{Ker}f$ 即可. $\square$

定理 3.4.3 第二 (2nd) 同构定理: 对群 G 的子群 K, N, 若 $N\lhd G$, 则

$$K/(N\cap K)\cong NK/N.$$

证明概要 考虑合成映射 $f: K\to NK/N$, 则 $\operatorname{Ker}f=K\cap N$. 注意到 N 正规且 NK/N 中每个元素都有形式 nkN, 则 $nkN=kn'N=kN=f(k)$, f 满. 由第一同构定理则有 $K/(N\cap K)\cong\operatorname{Im}f=NK/N$. $\square$

定理 3.4.4 第三 (3rd) 同构定理: 对群 G 的正规子群 K, N, 若 $K < N$, 则

$$N/K \lhd G/K,\ (G/K)/(N/K) \cong G/N.$$

证明概要 考虑满同态 $f: G/K \to G/H, aK \mapsto aH$. 由于 $H = f(aK) \Leftrightarrow a \in H$, 则 $\operatorname{Ker} f = \{aK \mid a \in H\} = H/K \lhd G/K$, 结合第一同构定理则有 $G/H = \operatorname{Im} f \cong (G/K)/\operatorname{Ker} f = (G/K)/(H/K)$. □

练习 3.20 证明群 G 中的每个指数为 2 的子群都正规.

练习 3.21 对群 G 及 $H, K \lhd G$, 若 $H \cap K = \{e\}$, 证明 $\forall a \in H, b \in K, ab = ba$, 并举例说明反之不一定成立.

练习 3.22 证明或否定非 Abel 群的商群一定是非 Abel 群.

练习 3.23 对群同态 $f: G \to H$ 且 $N \lhd G$, 证明 $f(N) \lhd f(G)$ 并举例说明 $f(N) \lhd H$ 不一定成立.

练习 3.24 对群 G 的正规子群 N 证明则 G/N 的每个子群都有形式 K/N, 其中 $K < G$ 且 $N < K$. 进而, $K/N \lhd G/N \Leftrightarrow K \lhd G$.

练习 3.25 对群 $G, N \lhd G$, 证明或否定:

(1) 若 G/N Abel, 则 G Abel;

(2) 若 G 非 Abel, 则 G/N 非 Abel;

(3) 若 G/N 是循环群, 则 G 是循环群.

3.5 Symmetric Groups

这部分我们将较为详细地研究对称群和它的某些子群.

定义 3.5.1 设 $\{i_1, \cdots, i_r\} \subseteq I_n = \{1, \cdots, n\}$, $(r \leq n)$, 则 $(i_1, \cdots, i_r)$ 表示置换

$$i_1 \mapsto i_2,\ i_2 \mapsto i_3,\ \cdots, i_{r-1} \mapsto i_r,\ i_r \mapsto i_1,$$

同时将 I_n 中其他元素映到自身, 这里称 $(i_1, \cdots, i_r)$ 为长为 r 的轮换 (cycle) 或 r-轮换. 其中, 2-轮换又被称作对换 (transposition).

这里轮换 $(i_1, \cdots, i_r)$ 代表置换 $\begin{pmatrix} i_1 & \cdots & i_r \\ i_2 & \cdots & i_1 \end{pmatrix}$, 它共有 r 种不同表达方式.

定义 3.5.2 设 $\sigma_1, \cdots, \sigma_r \in S_n$, 若

$$\forall 1 \leq i \leq n,\ k \in I_n,\ \sigma_i(k) \neq k \Rightarrow \forall j \neq i, \sigma_j(k) = k,$$

则称 $\sigma_1, \cdots, \sigma_r$ 非交 (disjoint). 若 σ_1, σ_2 非交, 则 $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

注. $\sigma_1,\cdots,\sigma_r\in S_n$ 非交的充要条件是 I_n 中没有元素被 $\sigma_1,\cdots,\sigma_r$ 中多于一个置换所改变.

例 3.5.1 考虑置换 $\tau=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$, 它实际上是 4-轮换 (2143). 另外考虑 $\sigma=(125)$, 则 $\sigma\tau=(1435)\neq\tau\sigma=(2543)$.

定理 3.5.1 Cayley 定理: 对群 G, 必存在单同态 $G\to S(G)$, 即每个群均同构于某个置换群.

证明概要 考虑 $\tau_a:G\to G,\ x\mapsto ax$, 其单性由 $\tau_a(x)=\tau_a(y)\Leftrightarrow ax=ay\Leftrightarrow x=y$ 给出而满性显然. 于是 τ_a 是双射. 记 $G'=\{\tau_a\mid a\in G\}$, 则通过验证定义可知 G' 是群, 下面我们证明 $G\cong G'$. 令 $\varphi:G\to G',\ a\mapsto\tau_a$, 其单性由 $\tau_a=\tau_b\Leftrightarrow\forall x\in G, ax=bx\Leftrightarrow a=b$ 给出而满性显然; 注意到 $\varphi(ab)=\tau_{ab}=\tau_a\tau_b=\varphi(a)\varphi(b)$, 则 φ 是同态, $G\cong G'$. □

特别地, 每个有限群 G 均同构于 S_n 的某个子群, 其中 $n=|G|$. 我们接下来探究 S_n 的生成元. 首先我们需要

定理 3.5.2 S_n 中每个非恒等置换均可唯一表示为非交轮换之积, 且每个轮换长度不小于 2.

证明概要 我们考虑对 n 归纳, 奠基显然. 假设结论对 $n-1$ 阶成立, 考虑 n 阶置换 $\sigma=\begin{pmatrix}1&\cdots&n\\i_1&\cdots&i_n\end{pmatrix}$. 若 $i_n=n$ 则其自然成为一个 $n-1$ 阶置换; 考虑 $i_n\neq n$, 则设 $i_k=n$, 考虑

$$(i_ki_n)\sigma=(i_ki_n)\begin{pmatrix}1&\cdots&k-1&k&k+1&\cdots&n\\i_1&\cdots&i_{k-1}&n&i_{k+1}&\cdots&i_n\end{pmatrix}=\begin{pmatrix}1&\cdots&k-1&k&k+1&\cdots&n\\i_1&\cdots&i_{k-1}&i_n&i_{k+1}&\cdots&n\end{pmatrix},$$

则由归纳假设取 $(i_ki_n)\sigma=\tau_1\tau_2\cdots\tau_r$, 则 $\sigma=(i_ki_n)\tau_1\tau_2\cdots\tau_r$, 只需证明 τ_i 均与 (i_ki_n) 不交.

若 τ_i 中有与 (i_ki_n) 中相交的, 则显然只能与 i_n 相交, 这是因为 $i_k=n$ 不在归纳假设范围之内. 于是设 $\tau_1=(i_na\cdots b)$, 则

$$\sigma=(i_ki_n)\alpha=(i_ki_n)(i_na\cdots b)\tau_2\cdots\tau_r=(i_ki_na\cdots b)\tau_2\cdots\tau_r$$

为不交轮换乘积. 由数学归纳法可知结论成立. □

推论 S_n 中每个置换均可写成 (不一定非交的) 对换之积.

定义 3.5.3 若 $\sigma\in S_n$ 能被写成奇 (偶) 个对换之积, 则称其为奇 (odd) 置换或偶 (even) 置换. 此时, 定义 $\sigma\in S_n$ 的符号 (sign) 为 $\operatorname{sgn}\sigma=\begin{cases}-1, & \sigma\text{是奇置换}\\1, & \sigma\text{是偶置换}\end{cases}$.

我们要先检验 sgnσ 的良定义性, 即 $S_n\,(n\geq 2)$ 中的置换不能同时是奇置换和偶置换. 证明比较繁琐, 我们不在这里介绍, 可以自行参考其他资料学习.

定义 3.5.4 记 $S_n\,(n\geq 2)$ 中所有偶置换构成的集合 A_n 为 n 次交错群 (alternating group).

定理 3.5.3 $A_n\lhd S_n$, $|A_n|=\dfrac{|S_n|}{2}=\dfrac{n!}{2}$; $[S_n:A_n]=2$.

证明概要 考虑 $f:S_n\to\{-1,1\}$, $\sigma\mapsto\operatorname{sgn}\sigma$, 验证定义可知 f 是群满同态. 由 $\operatorname{Ker}f=A_n$, 则

$A_n \lhd S_n$; 再由第一同构定理则知道 $S_n/A_n \cong \{-1,1\}$, $[S_n : A_n] = 2$. □

定义 3.5.5 定义二面体群 (dihedral group) 为 $S_n\,(n \geq 3)$ 的由 $a = (1, \cdots, n)$ 和

$$b = \begin{pmatrix} 1 & 2 & 3 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} = \prod_{2 \leq i < n+2-i} (i, n+2-i)$$

生成的子群, 记作 D_n.

二面体群等同于正 n 边形的全体对称所组成的群, 故也被称作正 n 边形群. 其中, 正 n 边形 P_n 的对称指一个保距双射 $P_n \to P_n$, 它将相邻顶点映成相邻顶点.

交错群是最早的一类非交换有限单群. 由于篇幅原因, 我们将交错群与二面体群的相关性质给出结论, 但不在此介绍其具体证明:

定理 3.5.4 交错群 A_n 是单群的充要条件是 $n \neq 4$.

定理 3.5.5 二面体群 D_n, $(n \geq 3)$ 是 $2n$ 阶群, 且上述生成元 a, b 满足:

(i) $a^n = (1)$, $b^2 = (1)$, $a^k \neq 1$, $(\forall k < n,\ k \in \mathbb{N}_+)$, 其中 (1) 代表恒等置换;

(ii) $ba = a^{-1}b$.

反之, 任意由满足上述两条件的元素 a, b 生成的群 $G \cong D_n$, 其中用幺元 $e \in G$ 代替 (1).

练习 3.26 置换 $\sigma \in S_n$ 的阶是其所有非交轮换长度的最小公倍数.

练习 3.27 证明 A_n 是 S_n 唯一的指数为 2 的子群.

我们已经完成了群论的最基本的介绍, 一些进阶内容 (群作用, Sylow 定理, 自由群, 幂零群, 可解群等) 不在此展开讨论.

Chapter 4

Rings

4.1 Rings and Homomorphisms

除了群以外,另一个最基本的代数结构是环,它具有加法与乘法两种代数运算.

定义 4.1.1 对非空集合 R 和两个二元运算 (通常表示为加法 $a+b$ 和乘法 ab), 若它们满足:

(1) $(R,+)$ 是 Abel 群;

(2) $(R,\times)$ 是半群, 即满足结合律 $\forall a,b,c\in R$, $(ab)c=a(bc)$;

(3) 分配律: $\forall a,b,c\in R$, $a(b+c)=ab+ac$, $(a+b)c=ac+bc$,

则称 R 在加法和乘法运算下成为环 (ring). 更进一步地,

(i) 若此时 $\forall a,b\in R$, $ab=ba$, 则称 R 为交换环 (commutative ring);

(ii) 若 $\exists 1_R\in R$, 使得 $\forall a\in R$, $1_R a=a1_R=a$, 则称 R 为幺环 (ring with identity).

这里, R 对于加法的单位元称作环 R 的零元, 记作 0; $\forall a\in R$, n 个 a 相加记作 na.

有时将幺环称作 ring, 无幺环称作 rng. 我们需要注意的是环在不同教材中的定义有所不同: 本章中并不一定要求环含幺, 但由于环的主要结果都是对幺环成立且无幺环能够嵌入幺环内 (我们后面会介绍), 故大多数书上将环设置为一定含幺. 请注意这里的区别.

命题 4.1.1 设 R 是环, 0 是 R 的零元, 则:

(1) $\forall a\in R, 0a=a0=0$;

(2) $\forall a,b\in R, (-a)b=a(-b)=-(ab), (-a)(-b)=ab$;

(3) $\forall n\in\mathbb{Z},\ a,b\in R, (na)b=a(nb)=n(ab)$;

(4) $\forall a_i,b_j\in R, \left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^m b_j\right)=\sum_{i=1}^n\sum_{j=1}^m a_ib_j$.

证明概要 都是环的基础运算性质, 请类似于群的运算给出证明. □

定义 4.1.2 对环 R 及非零元 $a,b\in R$, 若 $ab=0$, 则称 a 是左零因子, b 是右零因子. 同时是左右零因子的元素称作 R 的零因子 (zero divisor).

于是环 R 无零因子的充要条件是它对乘法满足消去律, 即 $ab=ac,\ ba=ca\Rightarrow b=c$.

定义 4.1.3 对幺环 R 及 $a\in R$, 若 $\exists c\in R, ca=1_R(ac=1_R)$, 则称 c 为 a 的左 (右) 逆. 若 a 同时具有左右逆, 则称 a 可逆 (invertable) 或 a 为单位 (unit).

显然地, 若 a 是幺环 R 中的单位, 则 a 的左右逆相等.

定义 4.1.4 若交换环 R 含幺元 $1_R\neq 0$ 且无零因子, 则称 R 是整环 (integral domain).

若幺环 R 中非零元对于乘法构成群, 则称 R 为除环 (division ring) 或体. 若该乘法群是 Abel 群, 则称 R 为域 (field).

于是整环和除环均至少有两个元素：零元和幺元.

定义 4.1.5 幺环 R 中全部单位组成一个乘法群, 称作 R 的单位群, 记作 $U(R)$ 或 $R^\times$.

推论 幺环 R 是除环的充要条件是 $1_R\neq 0$ 且 R 中每个非零元素均是单位.

例 4.1.1 对正整数 $n, \mathbb{Z}_n$ 是环; 对素数 $p, \mathbb{Z}_p$ 是域.

例 4.1.2 对群 A, $\operatorname{End}A$ 在函数的加法下与合成下成为幺环.

定理 4.1.1 具有多于 1 个元素的无零因子有限环必是除环.

证明概要 考虑 $x\neq 0\in R, \{x_i\mid i\in\mathbb{N}\}\subset R$, 由 R 有限, $\exists k>l$, 使得 $x^k=x^l$. 再由 R 无零因子, $x^{k-l}=1$, x 可逆, R 是除环. □

推论 有限整环是域.

例 4.1.3 对复数域 $\mathbb{C}$, 考虑

$$H=\left\{\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\mid \alpha,\beta\in\mathbb{C}\right\},$$

则 H 是除环但不是域. 它被称为 Hamilton 四元数 (quaternion) 除环, 是二阶复矩阵环的子环. 它也可表为 $\{a+bi+cj+dk\mid a,b,c,d\in\mathbb{Z}\}$, 且满足

$$ij=-ji=k,\ jk=-kj=i,\ ki=-ik=j,\ i^2=j^2=k^2=-1.$$

定义 4.1.6 对环 R,S, 若对 $f:R\to S$, 有 $\forall a,b\in R, f(a+b)=f(a)+f(b),\ f(ab)=f(a)f(b)$, 则称 f 为环同态 (homomorphism of rings).

由环的加法底群上的单 (满) 同态, (自) 同构可类似定义环上的单 (满) 同态, (自) 同构. 特别地, 环单同态 $f:R\to S$ 又被称作 R 在 S 中的嵌入 (embedding).

对环同态 $f:R\to S$, 核 $\operatorname{Ker}f=\{r\in R\mid f(r)=0\}$, 像 $\operatorname{Im}f=\{s\in S\mid \exists r\in R,\ s=f(r)\}$.

定义 4.1.7 对环 R, 若 $\exists n\in\mathbb{N}_+$, 使得 $\forall a\in R$, $na=0$, 则称 n 是 R 的特征 (characteristic), 记作 $\operatorname{char}(R)=n$. 若这样的 n 不存在, 则记作 $\operatorname{char}(R)=0$.

定理 4.1.2 对幺环 R, 设 $\operatorname{char}(R)=n>0$, 则：

(1) 映射 $\varphi:\mathbb{Z}\to R,\ m\mapsto m1_R$ 是环同态, $\operatorname{Ker}f=(n)$;

(2) n 是满足 $n1_R = 1_R n = 0$ 的最小正整数;

(3) 若 R 无零因子, 则 n 是素数.

证明概要 (1) 由定义显然; (2) 否则设 k 最小, 则 $\forall a \in R, ka = k(1_R a) = (k1_r)a = 0$, 矛盾; (3) 否则设 $n = qr, q, r > 1$, 则 $0 = n1_R(kr)1_R 1_R = (k1_R)(r1_R) \Rightarrow k1_R = 0$ 或 $r1_R = 0$, 与 (2) 矛盾. □

下面我们说明我们在第一节最开始提到的无幺环能够嵌入幺环内:

定理 4.1.3 每个环 R 都能嵌入幺环 S 中, 且 $\text{char}(S) = 0$ 或 $\text{char}(S) = \text{char}(R)$.

证明概要 记 $S = R \oplus \mathbb{Z}_n$, 其中 $\text{char}(R) = n$, 则定义乘法

$$(r_1, \bar{k_1})(r_2, \bar{k_2}) = (r_1 r_2 + k_2 r_1 + k_1 r_2, \bar{k_1}\bar{k_2})(r_i \in R, \bar{k_i} \in \mathbb{Z}_n),$$

验证定义知 S 含幺且可交换, 其中幺元 $1_S = (0, 1)$, $\text{char}\, S = n$. $n = 0$ 时取 $\mathbb{Z}_n = \mathbb{Z}$ 即可得到类似结果. □

定义 4.1.8 对环 R 及 $a \in R$, 若 $\exists n \in \mathbb{N}_+$, $a^n = 0$, 则称 a 是幂零的 (nilpotent).

命题 4.1.2 对环 R 的单位 a 和幂零元 x, 则 $a + x$ 也是 R 中的单位.

证明概要 若 $x^n = 0$, 取 $y = -a^{-1}x$, $y^n = 0$; 注意到 $(1-y)(1+y+\cdots+y^{n-1}) = 1 - y^n = 1$, $a + x = a(1-y)$ 可逆. □

定义 4.1.9 无非零幂零元的环称作既约环 (reduced ring).

例 4.1.4 对环 $(R, +, \times)$, 若 $(S, +, \circ)$ 满足 R, S 底集相同, 加法相同, 乘法相反, 则 $(S, +, \circ)$ 成为环, 称作 R 的反环 (opposite ring), 记作 R^{op}; 其中, 乘法相反是指 $\forall a, b \in R, S$, $a \circ b = ba$.

练习 4.1 证明**命题** 4.1.1.

练习 4.2 对环 R, 若 $\forall a \in R$, $a^2 = a$, 证明 R 是交换环且 $a + a = 0$. 此时 R 称作 Boole 环.

练习 4.3 举例说明 f 不一定将 1_R 映为 1_S, 并证明:

(1) f 为满同态时 $f(1_R) = 1_S$;

(2) 若 $\exists r \in R$, $r \neq 0$, $f(r) \neq 0$ 且 S 无零因子, 则 $f(1_R) = 1_S$.

练习 4.4 证明或否定: 若环 R 中 b 是 a 的左零因子, 则 a 是 b 的右零因子.

4.2 Subrings and Ideals

类似群论中的正规子群, 我们研究环中类似的结构:

定义 4.2.1 对环 R 的非空子集 S, 若 S 对于 R 的加法和乘法封闭, 则 S 构成环, 称作 R 的子环 (subring), 也记作 $S < R$. 这时,

(1) 若 S 满足 $\forall r \in R$, $a \in S$, $ra \in S$, 则称 S 是 R 的左理想 (left ideal);

(2) 若 S 满足 $\forall r \in R,\ a \in S,\ ar \in S$, 则称 S 是 R 的右理想 (right ideal).

若 S 同时是 R 的左右理想, 则称 S 为 R 的理想 (ideal), 一般记作 $S \lhd R$.

例 4.2.1 对环 R, R 和零环是 R 的理想, 其中 0 称作 R 的平凡理想. 若 R 的理想 S 满足 $S \neq R, S \neq 0$, 则称 S 为真理想.

例 4.2.2 环 R 的中心 $C = \{c \in R \mid \forall r \in R,\ cr = rc\}$ 是 R 的子环, 但不一定是理想.

接下来大量结论平行于正规子群的情形, 我们若略去证明则视为留作习题.

命题 4.2.1 对环 R 及其非空子集 S,

(1) S 是 R 的子环的充要条件是 $\forall a, b \in S,\ a - b \in S,\ ab \in S$;

(2) S 是 R 的左 (右) 理想的充要条件是 $\forall a, b \in S,\ r \in R,\ a - b \in S,\ ra \in S(ar \in S)$.

于是对环 R 的 (左, 右) 理想族 $\{R_i\}_{i \in I}$, 则 $\bigcap\limits_{i \in I} R_i$ 也是 R 的 (左, 右) 理想.

定义 4.2.2 对环 R 的非空子集 X, 则所有包含 X 的 (左, 右) 理想之交也是 R 的 (左, 右) 理想, 称作由 X 生成 (generate) 的 (左, 右) 理想, 记作 (X). 其中, X 中的元素称作 (X) 的生成元.

(1) 若 X 包含有限个元素, 则称 (X) 是有限生成的 (finitely generate).

(2) 若 $X = \{x\}$, 则记 $(X) = (x)$, 称作主理想 (principal ideal).

显然地, (X) 是 R 中包含 X 的最小理想.

定义 4.2.3 若环 R 的每个理想都是主理想, 则称其为主理想环 (principal ideal ring); 是主理想的整环称作主理想整环 (principal ideal domain), 简称作 PID.

定理 4.2.1 对环 R, 设 $a \in R, X \subset R$, 则

$$(a) = \left\{ ra + as + na + \sum_{i=1}^{m} r_i a s_i \mid r, s, r_i, s_i, \in R, m \in \mathbb{N}_+, n \in \mathbb{Z} \right\}.$$

特殊地, (1) 若 R 为幺环, 则 $(a) = \left\{ \sum\limits_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R, m \in \mathbb{N}_+ \right\}$;

(2) 若 a 属于 R 的中心 C, 即 $\forall r \in R,\ ar = ra$, 则 $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$;

(3) 若 R 为幺环且 X 包含于 R 的中心, 则 $(X) = \left\{ \sum\limits_{i=1}^{m} r_i x_i \mid r_i \in R, x_i \in X, m \in \mathbb{N}_+ \right\}$.

命题 4.2.2 陪集 $Ra = \{ra \mid r \in R\}$, $aR = \{ar \mid r \in R\}$ 分别是 R 中的左右理想. 若 R 是幺环, 则 $a \in aR,\ a \in Ra$; 若此时 $a \in C$, 则 $aR = Ra = (a)$.

证明概要 依定义验证. □

命题 4.2.3 对 $I \lhd R$ 及 R 上的关系 $a \sim b \Leftrightarrow a - b \in I$, 则它对于加法和乘法是同余关系.

此时, 记 $a \in R$ 的等价类为 $a + I$, 则加法商集 R/I 在运算

$$(a + I) + (b + I) = (a + b) + I,\ (a + I)(b + I) = (ab) + I$$

下成为环; 这里 () 仅代表运算顺序.

证明概要 只需证明上述乘法良定义, 即可依定义验证 R/I 是环. 这里取 $a' = a + i \in a + I$, $b' = b + j \in b + I$, 则

$$a' + b' = ab + ib + aj + ij,\, a'b' - ab = ib + aj + ij \in I.$$

于是 $a'b' + I = ab + I$, 上述乘法良定义. □

定义 4.2.4 上述环称作 R 对于理想 I 的商环 (quotient ring).

推论 R 是交换环 (幺环) 的充要条件是 R/I 是交换环 (幺环).

定理 4.2.2 对环同态 $R \to S$, 则 $\operatorname{Ker} f \lhd R$. 反之, 对 $I \lhd R, \pi : R \hookrightarrow R/I$, $r \mapsto r + I$ 是环的满同态, 且 $\operatorname{Ker} \pi = I$. 这里, 称 π 为典范满同态 (canonical epimorphism).

下面, 我们不证明地将群上的同态定理与三大同构定理移植到环上, 即:

定理 4.2.3 同态基本定理: 对环同态 $f : R \to S$, 若 I 是 R 的理想且 $I \subset \operatorname{Ker} f$, 则存在唯一环同态 $g : R/I \to S$, $a + I \mapsto f(a)$, $(\forall a \in R)$.

此时, $\operatorname{Im} g = \operatorname{Im} f$, $\operatorname{Ker} g = (\operatorname{Ker} f)/I$, g 是同构的充要条件是 f 满且 $I = \operatorname{Ker} f$.

定理 4.2.4 第一同构定理: 环同态 $f : R \to S$ 诱导同构 $R/(\operatorname{Ker} f) \cong \operatorname{Im} f$.

定理 4.2.5 第二同构定理: 环 R 的理想 I, J 诱导出同构 $I/(I \cap J) \cong (I + J)/J$.

定理 4.2.6 第三同构定理: 对环 R 的理想 $I \subset J$, 则 J/I 是 R/I 的理想, 且 $(R/I)/(J/I) \cong R/J$.

命题 4.2.4 对交换幺环 R, 以下几条件等价:

(1) R 是域;

(2) R 只有平凡理想;

(3) 每个非零的环同态 $f : R \to S$ 都是单同态.

证明概要 (1) ⇒ (2): 对 R 的非零理想 I, 设 $x \neq 0, x \in R$, 显然 x 是单位, 则 $(x) = R$, 即 $I = R$;
(2) ⇒ (3): 对环同态 $\varphi : R \to S$, $\operatorname{Ker} \varphi$ 是 R 的理想, 显然 $\operatorname{Ker} \varphi \neq r \Rightarrow \operatorname{Ker} \varphi = 0$, 即 φ 是单同态;
(3) ⇒ (1): 设 $x \in R$ 不是单位, 则 $(x) \neq R$, 又由典范满同态 $R \to R/(x)$ 是同构, 则 $(x) = 0$. □

定义 4.2.5 对交换幺环 $R, P \lhd R$, 若 $\forall A, B \lhd R$, 有 $AB \subset P \Rightarrow A \subset P$ 或 $B \subset P$, 则称 P 为素理想 (prime ideal). 称 R 的全体素理想组成的集合 $\operatorname{Spec}(R)$ 为 R 的素谱 (prime spectrum).

定理 4.2.7 对交换幺环 R 的理想 P, 它是素理想的充要条件是:

(1) $\forall a, b \in R$, $ab \in P \Rightarrow a \in P$ 或 $b \in P$;

(2) 商环 R/P 是整环.

证明概要 (1): ⇐: 对 $A, B \lhd R$, $AB \subset P$. 若 $A \not\subset P$, 则取 $a \in A - P$, 于是 $\forall b \in B$, $ab \in Ab \subset P$, $b \in P$, $B \subset P$. ⇒: 此时取 $a, b \in P$, 由 R 可交换, $(a)(b) \subset (ab) \subset P$, 即 $(a) \subset P$ 或 $(b) \subset P$, $a \in P$ 或 $b \in P$.

(2) ⇔ (1): ⇐: 此时 R/I 交换, 考虑其零因子 $(a + I)(b + I) = 0 + I \Rightarrow ab \in I \Rightarrow a \in I$ 或

$b \in I \Rightarrow a+I=0+I$ 或 $b+I=0+I$, R/I 是整环. $\Rightarrow$ 只需反向进行上述推导即可. $\square$

于是自然可以推得, 交换幺环 R 是整环当且仅当 $\{0\}$ 是其素理想.

定义 4.2.6 对交换幺环 R 的理想 $M \neq R$, 若不存在 R 的真理想 N 使得 $M \subset N$, 则称 M 为极大理想 (maximal ideal). 称 R 的全体极大理想组成的集合为 $\mathrm{Max}(R)$ 为 R 的极大谱 (maximal spectrum).

定理 4.2.8 对交换幺环 R 的理想 M, 它是极大理想的充要条件是商环 R/M 是域.

证明概要 注意到环 R 中包含理想 I 的理想 J 与环 R/I 的理想 $\overline{J}$ 之间存在一一对应即可. $\square$

定理 4.2.9 每个交换幺环 $R \neq 0$ 都至少有一个极大理想.

证明概要 考虑 R 中所有真理想组成的集合 $S \neq \varnothing$, 令包含关系代表序关系; 于是对理想链 $(a_i)_{i\in I}$, 则 $\forall i,j \in I$, $(a_i) \subseteq (a_j)$ 或 $(a_j) \subseteq (a_i)$. 这里记 $U=\bigcup\limits_{i\in I}(a_i)$, 显然它也是 R 的理想且是该理想链的上界. 据 Zorn 引理, 它有一个极大元 M, 它便是极大理想. $\square$

于是交换幺环 R 中的任一非单位的元素和任一真理想都能被一极大理想包含. 在代数中素理想是很基本的结构, 上述定理说明了有足够多的素理想.

定义 4.2.7 具唯一极大理想 M 的环 R 称作局部环 (local ring), 记作 (R,M), 此时域 R/M 称作 R 的剩余域 (residue field). 更一般地, 只有有限个极大理想的环 R 称作半局部环 (semi-local ring).

命题 4.2.5 对交换幺环 R 及 $M \lhd R$, 若 $R-M$ 中任一元素都是 R 的单位, 则 (R,M) 是局部环.

证明概要 考虑 R 的单位 x, 注意到 $(x)=rx$ 且 $\exists r \in R$, $rx=1 \Rightarrow (x)=R$ 即可. $\square$

练习 4.5 对环 R 的理想 I, 设 R 中全部包含 I 的理想组成集合 A, R/I 中全部理想组成集合 B, 证明 $f: A \to B$, $J \mapsto J/I$ 是同构. 这实际上说明 R/I 中每个理想都可以唯一表示成形式 J/I, 其中 J 是 R 的理想且 $I \subset J$.

练习 4.6 对素数 p, 说明 $\mathbb{Z}$ 中的主理想 (p) 既是素理想, 又是极大理想.

4.3 Factorization in Commutative Rings

我们这里将整数 $\mathbb{Z}$ 中的某些数论性质推广到任一交换环上.

定义 4.3.1 对交换环 R 中对非零元 a,b, 若 $\exists x \in R$, 使得 $ax=b$, 则称 a 可整除 (divide) b, 记作 $a|b$. 若 $a|b$ 且 $b|a$, 则称 a,b 是相伴的 (associate), 一般记作 $a \sim b$.

命题 4.3.1 对交换幺环 R 中的元素 a,b,u, 有如下主理想表述:

(1) $a|b \Leftrightarrow (b) \subset (a)$;

(2) $a \sim b \Leftrightarrow (a)=(b)$;

(3) u 是单位的充要条件是 $\forall r \in R$, $u|r \Leftrightarrow (u)=R$;

(4) a,b 相伴定义的关系 $\sim$ 是 R 上的等价关系;

(5) 若 r 是单位, $a = br$, 则 $a \sim b$, R 为整环时反之也成立.

定义 4.3.2 对交换幺环 R, 若 $\exists c \in R, c \neq 0$ 且不是单位, 且 $c = ab \Rightarrow a$ 或 b 是单位, 则称 c 是不可约的 (irredncible).

若 $\exists p \in R, p \neq 0$ 且不是单位, 且 $p|ab \Rightarrow p|a$ 或 $p|b$, 则称 p 为素元 (prime).

例 4.3.1 在环 $\mathbb{Z}_6$ 中, $\bar{2}$ 是素元, 但不是不可约元; 在 $\mathbb{R}$ 的子环 $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ 中, 2 是不可约元, 但不是素元.

命题 4.3.2 对整环 R 及非零元 $p, c \in R$, 则:

(1) p 是素元 $\Leftrightarrow (p)$ 是非零素理想;

(2) c 是不可约元 $\Leftrightarrow (c)$ 在 R 的全体真主理想组成的集合 S 中极大;

(3) R 的每个素元均是不可约元;

(4) 若 R 是 PID, 则 p 是素元 $\Leftrightarrow p$ 是不可约元;

(5) R 中与不可约元 (素元) 相伴的元素仍然是不可约元 (素元);

(6) R 中不可约元的因子只有与它相伴的元素及 R 中的单位.

证明概要 略 □

定义 4.3.3 对整环 R, 若:

(1) R 中每个非零非单位的元素 a 均可写成 $a = c_1 \cdots c_n$ 的形式, 其中 c_i 是不可约元;

(2) 若 $a = c_1 \cdots c_n = d_1 \cdots d_m$, 则 $n = m$, 且存在置换 σ, 使得 $\forall i = 1, \cdots, n$, c_i 与 $d_{\sigma(i)}$ 相伴,

则称 R 为唯一因子分解整环 (unique factorization domain), 简记作 UFD.

例 4.3.2 对环 $\mathbb{Z}[\sqrt{-5}]$, 它的每个元素均可分解为不可约元之积, 但分解不唯一 (不满足上述 (2)).

例 4.3.3 域 F 上的多元多项式环 (如 $F[x, y]$) 是 UFD, 但不是 PID.

定义 4.3.4 对交换环 R, 若存在函数 $\varphi : R - \{0\} \to \mathbb{N}$, 使得:

(1) $\forall a, b \in R$, 若 $ab \neq 0$, 则 $\varphi(a) \leq \varphi(ab)$;

(2) $\forall a, b \in R$, 若 $b \neq 0$, 则 $\exists q, r \in R$, 使得 $a = qb + r$, 其中 $r = 0$ 或 $\varphi(r) < \varphi(b)$,

则称其为欧几里得环 (Euclid ring).

若 R 是整环, 则称 R 为欧几里得整环 (Euclidean domain), 简记作 ED.

例 4.3.4 对域 F, 则单变量多项式环 $F[x]$ 在 $\varphi(x) = \deg f$ 下成为 ED.

例 4.3.5 $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ 是整环, 称作 Gauss 整环; 它在 $\varphi(a + bi) = a^2 + b^2$ 下成为 ED.

定理 4.3.1 每个 ED 都是 PID, 每个 PID 都是 UFD.

证明概要 略 □

例 4.3.6 $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right] = \left\{a + \dfrac{1+\sqrt{19}i}{2}b \,\middle|\, a, b \in \mathbb{Z}\right\}$ 是 PID, 但不是 ED.

Part III

Topology

Chapter 5

Topological Spaces

5.1 Topological Spaces

定义 5.1.1 集合 X 上的一个拓扑 (topology) 是 X 的一个子集族 $\mathcal{T}$, 且满足以下条件:

(1) $\varnothing \in \mathcal{T}, X \in \mathcal{T}$;

(2) $\mathcal{T}$ 任意子族的元素的并在 $\mathcal{T}$ 中.

(3) $\mathcal{T}$ 的任意有限子族的元素的交在 $\mathcal{T}$ 中.

一个赋予了拓扑 $\mathcal{T}$ 的集合 X 叫做一个拓扑空间 (topological space), 记作拓扑空间 $(X, \mathcal{T})$.

定义 5.1.2 对拓扑空间 $(X, \mathcal{T})$ 与集合 $U \subset X$, 若 $U \in \mathcal{T}$, 则称 U 是 X 内的一个开集 (open set).

例 5.1.1 对集合 X, $\{\varnothing, X\}$ 称作平凡拓扑 (trivial topology), 2^X 称作离散拓扑 (discrete topology).

例 5.1.2 对集合 X, $\mathcal{T}$ 是所有满足 $X - U$ 是有限集的 U 和 $\varnothing$ 组成的集合, 则 $\mathcal{T}$ 是 X 上的拓扑, 称作有限补拓扑 (finite complement topology).

定义 5.1.3 对集合 X 上的两个拓扑 $\mathcal{T}, \mathcal{T}'$, 若

(1) $\mathcal{T}, \mathcal{T}'$ 有包含关系, 则称二者可比较 (comparable);

(2) $\mathcal{T} \subset \mathcal{T}'$, 则称 $\mathcal{T}$ 比 $\mathcal{T}'$ 细 (finer), $\mathcal{T}'$ 比 $\mathcal{T}$ 粗 (coarser);

(3) $\mathcal{T} \subsetneq \mathcal{T}'$, 则称 $\mathcal{T}$ 比 $\mathcal{T}'$ 严格细, $\mathcal{T}'$ 比 $\mathcal{T}$ 严格粗.

定义 5.1.4 对集合 X, 若 X 的一个子集族 $\mathcal{B}$ 满足:

(1) $\forall x \in X, \exists B \in \mathcal{B}$, s.t. $x \in B$;

(2) 对 $x \in B_1 \cap B_2$, 则 $\exists B_3$ 满足 $B_3 \in \mathcal{B}, B_3 \subset B_1 \cap B_2$,

则称这个族是一个定义在 X 上的拓扑的基 (basis), $B \in \mathcal{B}$ 称为基元.

定理 5.1.1 对集合 X 上的基 $\mathcal{B}$, 则可生成某拓扑 $\mathcal{T}$, 使得 $\forall U \in \mathcal{T}$, 满足:

$$\forall x \in U, \exists B \in \mathcal{B}, \text{ s.t. } x \in B \subset U.$$

证明概要 依定义依次验证, 留作习题. $\square$

命题 5.1.1 对拓扑空间 $(X,\mathcal{T})$ 上的基 $\mathcal{B}$, 则 $\mathcal{T}$ 为 $\mathcal{B}$ 的所有的可能基元的元素的并的族, 即

$$\mathcal{T}=\left\{\bigcup_{B\in\mathcal{B}'}B\mid\mathcal{B}'\subset\mathcal{B}\right\}$$

证明概要 显然 $\mathcal{B}$ 的所有的可能的元素的并在 $\mathcal{T}$ 内, 下面只需说明任意的 $U\in\mathcal{T}$ 都能写成是基元的并. 由定义, $\forall x\in U,\exists B_x\in\mathcal{B}$ 使得 $x\in B_x\subset U$, 于是 $U=\bigcup\limits_{x\in U}B_x$, 结论成立. □

命题 5.1.2 对拓扑空间 $(X,\mathcal{T})$, $\mathcal{T}$ 上的子基 (subbasis) $\mathcal{S}$ 是 X 的子集族, 且其元素之并是 X. 也定义由子基生成的族 $\mathcal{T}$ 为所有可能的有限交的并的族, 即:

$$\mathcal{T}=\left\{\bigcup_{B\in\mathcal{B}'}B\mid\mathcal{B}'\subset\mathcal{B},\quad\mathcal{B}=\{S_1\cap\cdots\cap S_n\mid S_i\in\mathcal{S}\}\right\}$$

证明概要 首先依定义验证族 $\mathcal{T}$ 是一个拓扑, 然后类似**命题** 5.1.1 验证即可. □

命题 5.1.3 对拓扑空间 $(X,\mathcal{T})$ 与 X 的开子集族 $\mathcal{C}$, 若对 X 的每一个开集 U, $\forall x\in U$, $\exists C\in\mathcal{C}$, 满足 $x\in C\subset U$, 则 $\mathcal{C}$ 是 $\mathcal{T}$ 的一个基.

证明概要 首先依定义 $\mathcal{C}$ 是基; 然后验证 $\mathcal{C}$ 生成 $\mathcal{T}$. □

定理 5.1.2 设 $\mathcal{B}$ 和 $\mathcal{B}'$ 分别是 X 的拓扑 $\mathcal{T}$ 和 $\mathcal{T}'$ 的基, 则 $\mathcal{T}$ 细于 $\mathcal{T}$ 的充要条件是 $\forall x\in X$ 及 $x\in B\in\mathcal{B}$, 存在基元 $B'\in\mathcal{B}'$, 使得 $x\in B'\subset B$.

证明概要 $\Leftarrow$: 取 $x\in U$, $\exists B\in\mathcal{B}$ 使得 $x\in B\subset U$. 于是由题设条件, $\exists B'\in\mathcal{B}'$ 使得 $x\in B'\subset B$, $x\in B'\subset U, U\in\mathcal{T}'$. $\Rightarrow$: 取 $x\in X, x\in B\in\mathcal{B}, B\in\mathcal{T}\Rightarrow B\in\mathcal{T}'$. 但是 $\mathcal{B}'$ 是 $\mathcal{T}$ 的基, 于是 $\exists B'\in\mathcal{B}'$ 使得 $x\in B'\subset B$. □

例 5.1.3 给出实轴 $\mathbb{R}$ 上的三种拓扑:

(1) 由开区间 $(a,b)=\{x\mid a<x<b\}$ 生成的拓扑称为 $\mathbb{R}$ 上的标准拓扑 (standard topology);

(2) 由半开区间 $[a,b)=\{x\mid a\le x<b\}$ 生成的拓扑称为 $\mathbb{R}$ 的下限拓扑 (lower limit topology). 装备下限拓扑的 $\mathbb{R}$ 记作 $\mathbb{R}_\ell$, 其严格细于标准拓扑 (不存在 (a,b) 使得 $x\in(a,b)\subset[x,c)$);

(3) 取 $K=\dfrac{1}{\mathbb{N}_+}=\left\{\dfrac{1}{n}\mid n\in\mathbb{N}_+\right\}$, 由所有开区间 (a,b) 及形如 $(a,b)-K$ 形式的集合生成的拓扑称为 $\mathbb{R}$ 上的 K-拓扑 (K-topology). 装备 K-拓扑的 $\mathbb{R}$ 记作 $\mathbb{R}_K$, 其严格细于标准拓扑 (不存在 (a,b) 使得 $0\in(a,b)\subset(-1,1)-K$).

练习 5.1 验证**例** 5.1.1 中的平凡拓扑和离散拓扑是拓扑.

练习 5.2 验证**例** 5.1.2 中的有限补拓扑是拓扑.

练习 5.3 验证**定理** 5.1.1.

练习 5.4 说明 $\mathbb{R}_\ell,\mathbb{R}_K$ 不可比较.

5.2 Common Topology Examples

the Order Topology

定义 5.2.1 设 X 是一个有不止一个元素的全序集. 设 $\mathcal{B}$ 是下述所有集合的族:

(1) 所有 X 中的开区间 (a,b);

(2) 所有 X 中的左闭右开区间 $[a,b)$, 其中 a 是 X 的最小元 (若存在);

(3) 所有 X 中的左开右闭区间 $(a,b]$, 其中 b 是 X 的最大元 (若存在),

则 $\mathcal{B}$ 是 X 的某个拓扑的一组基, 它生成的拓扑定义为序拓扑 (order topology).

序拓扑的意义下, 原来开区间的 “开” 自然对应到了拓扑学中 “开集” 的概念上.

例 5.2.1 $\mathbb{R}$ 上的标准拓扑即为正常序关系下 $\mathbb{R}$ 上的序拓扑. $\mathbb{N}_+$ 上定义的序拓扑是离散拓扑.

例 5.2.2 在字典序下集合 $\mathbb{R}\times\mathbb{R}$ 既无最大元也无最小元, 于是 $\mathbb{R}\times\mathbb{R}$ 上的序拓扑有基

$$\{((a,b),(c,d)) \mid a<c\text{ 或 }a=c, b<d\}.$$

事实上, 仅由第二种类型的区间组成的子族也是 $R\times R$ 上序拓扑的一个基.

定义 5.2.2 定义集合 $(a,+\infty)$, $[a,+\infty)$, $(-\infty,a)$, $(-\infty,a]$ 为射线 (ray), 其中存在闭方向的为闭射线 (closed ray), 不存在的为开射线 (open ray).

开代表了其为序拓扑下的开集, 事实上它们构成了 X 上序拓扑的子基.

the Product Topology $X\times Y$

定义 5.2.3 定义 $X\times Y$ 的积拓扑为由所有的诸如 $U\times V$ 形式的集合的族 $\mathcal{B}$ 生成的拓扑, 这里 U 为 X 的开子集, V 为 Y 的开子集.

定理 5.2.1 设 $\mathcal{B},\mathcal{C}$ 分别对应生成拓扑空间 X,Y 的基, 则拓扑空间 $X\times Y$ 有如下基:

$$\mathcal{D}=\{B\times C \mid B\in\mathcal{B},\, C\in\mathcal{C}\}.$$

证明概要 利用**命题** 5.1.3 将其转化为分别考虑 $\mathcal{B},\mathcal{C}$ 即可. □

定义 5.2.4 设 $\pi_1 : X\times Y\to X$, $(x,y)\mapsto x$, $\pi_2 : X\times Y\to Y$, $(x,y)\mapsto y$, 则 π_1,π_2 称作 $X\times Y$ 到第一, 二分量上的投影 (projection).

显然 π_1,π_2 都是满射. 应用投影的定义, 我们能用子基来表示积拓扑:

命题 5.2.1 $\mathcal{S}=\left\{\pi_1^{-1}(U)\right\}\cup\left\{\pi_2^{-1}(V)\right\}$ 是 $X\times Y$ 的积拓扑的子基; 这里 U,V 分别取遍 X,Y 中的开集.

证明概要 首先注意到 $\pi_1^{-1}(U)$, $\pi_2^{-1}(V)\in\mathcal{T}$, 这里 $\mathcal{T}$ 是积拓扑; 于是有限交也显然在 $\mathcal{T}$ 内, 则 S 生成 $\mathcal{T}'\subset\mathcal{T}$; 反之 $\forall x=U\times V\in\mathcal{T}$, 注意到 $U\times V=\pi_1^{-1}(U)\cap\pi_2^{-1}(V)$, 于是它也是 $\mathcal{S}$ 中元素的有限交, $x\in\mathcal{T}$. □

the Subspace Topology

定义 5.2.5 对拓扑空间 $(X,\mathcal{T})$, $Y \subset X$, 则定义子空间拓扑 $\mathcal{T}_Y = \{Y \cap U \mid U \in \mathcal{T}\}$, 且称 $(Y,\mathcal{T})$ 为 $(X,\mathcal{T})$ 的子空间 (subspace), 且其开集由 X 的开集与 Y 的交组成.

显然若 U 是 Y 上的开集, Y 是 X 上的开集, 则 U 是 X 上的开集.

引理 设 $\mathcal{B}$ 是一个 X 上的拓扑的基, 则 $\mathcal{B}_Y = \{B \cap Y \mid B \in \mathcal{B}\}$ 是 Y 上子空间拓扑的基.

证明概要 留作习题. □

命题 5.2.2 对 X 的子空间 A, Y 的子空间 B, 则 $A \times B$ 上的积拓扑即为 $A \times B$ 在 $X \times Y$ 上一个子空间拓扑.

证明概要 注意到 $(U \times V) \cap (A \times B) = (U \cap A) \times (V \cap B)$, 而 $U \cap A, V \cap B$ 是 A, B 上的开集, 于是据定义即有 $(U \cap A) \times (V \cap B)$ 是 $A \times B$ 上积拓扑的基元. □

这个定理告诉我们, 积拓扑和子空间拓扑相容. 但是序拓扑不一定相容, 即对 $Y \subset X$, 将 X 上的序关系限制在 Y 上得到的序拓扑和 Y 上继承的 X 上的子空间拓扑不一定相等:

例 5.2.3 考虑 $Y = [0,1] \subset \mathbb{R}$, 则其基元有形式 $(a,b) \cap Y$, 即 (a,b), $[0,b)$, $(a,1]$, Y 或 $\varnothing$, 而它们的总体又构成了序拓扑的基. 此时二者相等.

例 5.2.4 考虑 $Y = [0,1) \cup \{2\} \subset \mathbb{R}$, 则 $\{2\}$ 是 Y 上子空间拓扑上的一个开集, 但是它不是 Y 上序拓扑的一个开集.

为了说明序拓扑和子空间拓扑的关系, 补充一个定义.

定义 5.2.6 对于全序集 X, $Y \subset X$, 若对于 Y 中的任意一组数 $a < b$, $(a,b) \subset Y$, 则称 Y 是 X 中的凸集 (convex set).

定理 5.2.2 对装备序拓扑的全序集 X 及其凸子集 Y, 则 Y 上的序拓扑和 Y 在 X 上的子空间拓扑相同.

证明概要 取 $(a,+\infty) \subset X$. 若 $a \in Y$, 则 $(a,+\infty) \cap Y$ 是 Y 中开射线; 若 $a \notin Y$, 由于 Y 是一个凸子集, 则 a 是 Y 的一个下界 ($(a,+\infty) \cap Y = Y$) 或上界 ($(a,+\infty) \cap = \varnothing$). 由于所有形如 $(a,+\infty) \cap Y$ 和 $(-\infty,a) \cap Y$ 的集合构成了 Y 的子空间拓扑的一个子基且它们均是序拓扑的开集, 从而序拓扑包含了子空间拓扑. 反之注意 Y 的任一开射线都是 Y 的子空间拓扑的开集且 Y 的开射线构成了 Y 的序拓扑的一个子基即可. □

为了避免混淆, 我们约定当讨论全序集 X 的子集 Y 时, 除非有特别的说明, 默认 Y 装备子空间拓扑.

练习 5.5 验证**例** 5.2.1 和**例** 5.2.2.

练习 5.6 证明本节中的**引理**: 子空间拓扑的基.

5.3 Limit Point and Continuous Function

我们已经了解了若干拓扑空间的例子, 现在开始引入一些基本概念.

定义 5.3.1 对于拓扑空间 X, 若 $A \subset X$ 且 $X - A$ 是开集, 则称 A 为闭集 (closed).

例 5.3.1 对于装备离散拓扑的集合 X, 它的所有子集都是开集, 从而其所有子集也都是闭集.

当涉及子空间时, 闭集一词有时会产生歧义. 于是我们总采取如下定义:

定义 5.3.2 对 X 的子空间 Y, 若 $A \subset Y$ 是 Y 的子空间拓扑中的闭集, 则称 A 是 Y 中的闭集.

通过取补集将闭集运算转化为开集, 我们可以平行地证明如下若干命题:

定理 5.3.1 对拓扑空间 X, 则:

(1) $\varnothing, X$ 是闭集;

(2) 闭集的任意交依然是闭集;

(3) 闭集的有限并依然是闭集.

命题 5.3.1 对 X 的子空间 Y, 则 A 是 Y 中的闭集当且仅当它是 X 中的一个闭集和 Y 的交.

命题 5.3.2 对 X 的子空间 Y, 若 A 是 Y 的闭集, Y 是 X 的闭集, 则 A 是 X 中的闭集.

定义 5.3.3 对 X 的子集 A, 定义所有包含于 A 的开集的并为 A 的内部 (interior), 记为 $\operatorname{Int} A$; 所有包含 A 的闭集的交为集合 A 的闭包 (closure), 记为 $\bar{A}$.

同样, 提到子空间的时候, 还是容易有歧义. 设 Y 为 X 的子空间且 $A \subset Y$, 则默认 $\bar{A}$ 指的是用 X 上的集合做闭包. 而对于 A 在 Y 上的闭包, 有下面的定理:

命题 5.3.3 对 X 的子空间 Y, $A \subset Y$, 则 A 在 Y 上的闭包为 $\bar{A} \cap Y$.

证明概要 留作习题. □

命题 5.3.4 设 A 为拓扑空间 X 的子集, 则

(1) $x \in \bar{A}$ 当且仅当任一 x 的邻域 U 与 A 相交;

(2) 若 X 的拓扑由一组基生成, 则 $x \in \bar{A}$ 当且仅当每一个包含 x 的基元 B 与 A 的相交.

这里, 相交 (intersect) 是指交集非空.

证明概要 (1): 考虑其逆否命题, 即 $x \notin \bar{A}$ 当且仅当有一个包含 x 的开集 $U \cap A = \varnothing$. 取 $x \notin \bar{A}$, 则 $U = X - \bar{A}$ 满足要求; 反之 $X - U \supset A$ 是闭集, 则 $\bar{A} \subset X - U, x \notin \bar{A}$.

(2): 通过 (1) 将 $x \in \bar{A}$ 等价作任一 x 的邻域 U 与 A 相交之后证明即可. □

例 5.3.2 考虑 $Y = (0, 2)$, $A = (0, 1) \subset Y$, 则它在 $\mathbb{R}$ 上的闭包为 $[0, 1]$, 但在 Y 上的闭包为 $(0, 1]$.

定义 5.3.4 对开集 X 及 $x \in X$, 若 $\{x\}$ 在 X 中开, 则称 x 是 X 的孤立点 (isolated point).

定义 5.3.5 若 $A - \{x\}$ 的闭包包含 x, 则称 x 是 A 内的一个极限点 (limit point). A 的所有极限点组成的集合称作 A 的导集 (derived set), 记作 A'.

极限点也可以描述为: 若所有与 A 相交的 x 的邻域与 A 的交集均含有异于 x 的点, 则称 x 是 A 内的一个极限点.

定理 5.3.2 对拓扑空间 X 的子集 A, 则 $\bar{A} = A \cup A'$.

证明概要 $\bar{A} \supset A \cup A'$ 显然; 反之取 $x \in \bar{A}$, 只需考虑 $x \notin A$, 于是任一 x 的邻域 U 与 A 相交且每个交集中一定还有除 x 以外的元素, 于是由极限点的定义 $x \in A'$, $x \in A \cup A'$, 原命题成立. □

推论 拓扑空间 X 的子集 A 为闭集当且仅当 $A' \subset A$.

Continuous Function

定义 5.3.6 对拓扑空间 X, Y, 若对于 Y 的任一开集 V, $f^{-1}(V)$ 都在 X 上开, 则称 $f : X \to Y$ 是连续的 (continuous).

注. 更严谨地, 连续性由两个拓扑空间所对应的拓扑决定; 即连续意味着相对于 $\mathcal{T}_X$ 和 $\mathcal{T}_Y$ 连续.

推论 若 Y 由基 $\mathcal{B}$ 生成, 则只需证明每个基元的逆元都是 X 上的开集即可, 这是由于

$$V = \bigcup_{\alpha \in J} B_\alpha \Rightarrow f^{-1}(V) = \bigcup_{\alpha \in J} f^{-1}(B_\alpha).$$

例 5.3.3 $f : \mathbb{R} \to \mathbb{R}_\ell$, $x \mapsto x$ 不连续, 但是 $g : \mathbb{R}_\ell \to \mathbb{R}$, $x \mapsto x$ 连续.

定理 5.3.3 设 $f : X \to Y$, 则下面命题等价:

(1) f 是连续函数;

(2) f 在 $\forall x \in X$ 处均连续;

(3) 对于 X 任一子集 A, 有 $f(\bar{A}) \subset f(\bar{A})$;

(4) 对于 Y 任一闭集 B, $f^{-1}(B)$ 在 X 中闭,

这里 f 在 x 处连续指对任一 $f(x)$ 的邻域 V, 都存在 x 的邻域 U 满足 $f(U) \subset V$.

证明概要 (1) $\Leftrightarrow$ (2):$\Rightarrow$ 显然, $\Leftarrow$: 取 Y 的开集 V, $x \in f^{-1}(V)$, 则存在邻域 U_x 使得 $f(U_x) \subset V$, $U_x \subset f^{-1}(V)$, 于是 $f^{-1}(V) = \bigcup\limits_{x \in f^{-1}(V)} U_x$ 是开集.

(1) $\Rightarrow$ (3): 取 $x \in \bar{A}$, 取 $f(x)$ 的邻域 V, 则 $x \in f^{-1}(V)$ 且它是开集, 于是其与 A 相交, 也即 V 与 $f(A)$ 相交, $f(x) \in \overline{f(A)}$.

(3) $\Rightarrow$ (4): 取 $A = f^{-1}(B)$, $x \in \bar{A}$, 则 $f(x) \in \overline{f(A)} \subset \bar{B} = B$, 则 $x \in A$, $\bar{A} \subset A$, A 闭.

(4) $\Rightarrow$ (1): 取 Y 的开集 V, $B = Y - V$, 则 $f^{-1}(B) = X - f^{-1}(V)$, B 闭. 据题设 $f^{-1}(B)$ 是 X 中的闭集, $f^{-1}(V)$ 开, f 连续. □

定义 5.3.7 设 $f : X \to Y$ 是双射, 若 f 和 f^{-1} 均连续, 则称 f 是一个同胚 (homeomorphism).

推论 同胚的等价定义: 满足 $f(U)$ 是开集等价于 U 是开集的双射 f 称作同胚.

这说明同胚 $f : X \to Y$, 不仅给出了 X 和 Y 之间的一个双射, 还给出了 X 与 Y 的开集族之间的一个双射. 于是通过 X 的开集所得到的任一条性质通过 f 可以得到 Y 的相应性质. X 的这种性质称作它的拓扑性质 (topological property).

类似于代数中的保持代数结构的同构,同胚也保持拓扑结构.

定义 5.3.8 对连续单射 $f: X \to Y$, 视 $Z = f(X)$ 为 Y 的子空间, 若通过限制 f 的值域得到的 $g: X \to Z$ 是同胚, 则称 f 是一个嵌入 (imbedding), 记作 $f: X \hookrightarrow Y$.

定理 5.3.4 连续函数的构造法则: 对拓扑空间 X, Y, Z 与函数 $f: X \to Y, g: Y \to Z$, 则:

(1) 常值 (constant): 若 $\forall x \in X, f: x \to y_0$, 则 f 连续;

(2) 包含 (inclusion): 若 A 是 X 的子空间, 则典范的单射 $\pi: A \to X$ 连续;

(3) 复合 (composites): 若 f, g 均连续, 则 $g \circ f: X \to Z$ 连续;

(4) 限制定义域 (restrict the domain): 若 f 连续, A 是 X 的子空间, 则限制 $f: A \to Y$ 连续;

(5) 限制或扩张值域 (range): 若 f 连续, Z 是包含 $f(X)$ 的 Y 的子空间, W 以 Y 作为子空间, 则 $i: X \to Z, j: X \to Z$ 均连续;

(6) 局部表示 (local): 若 X 可以被写为开集族 $\{U_\alpha\}$ 的并且 $\forall \alpha, f|_{U_\alpha}$ 连续, 则 f 连续.

证明概要 留作习题. □

定理 5.3.5 粘贴引理 (Pasting Lemma): 设 $X = A \cup B$ 且 A, B 为 X 中闭集, $f: A \to Y, g: B \to Y$ 均连续, 若 $\forall x \in A \cap B, f(x) = g(x)$, 则可以构造连续函数

$$h: X \to Y = \begin{cases} f(x), & x \in A \\ g(x), & x \in B \end{cases}$$

证明概要 取 Y 的闭集 C, 则 $f^{-1}(C)$ 在 A 中闭, $g^{-1}(C)$ 在 B 中闭, $h^{-1}(C) = f^{-1}(C) \cup g^{-1}(C)$ 在 X 中闭, h 连续. □

这个引理相当于说若两个连续函数交集相同,则可以把它们拼成一个更大的连续函数.

定理 5.3.6 设 $f: A \to X \times Y, a \mapsto (f_1(a), f_2(a))$, 则 f 连续的充要条件是 $f_1: A \to X, f_2: A \to Y$ 都连续. 这里 f_1 和 f_2 称为 f 的坐标函数 (coordinate function).

证明概要 显然两个投影函数 $\pi_1: X \times Y \to X, \pi_2: X \times Y \to Y$ 都连续, 则 $\forall a \in A, f_1 = \pi_1 f$, $f_2 = \pi_2 f$ 都连续. 反之, 对任一基元 $U \times V$, 则

$$a \in f^{-1}(U \times V) \Leftrightarrow f(a) \in U \times V \Leftrightarrow f_1(a) \in U,\ f_2 \in V \ \Rightarrow\ f^{-1}(U \times V) = f_1^{-1}(U) \cap f_2^{-1}(V).$$

于是 $f^{-1}(U \times V)$ 是开集, f 连续. □

命题 5.3.5 对拓扑空间 X 及连续函数 $f, g: X \to \mathbb{R}$, 则 $f + g, f - g, f \cdot g$ 都连续; 若 $\forall x \in X, g(x) \neq 0$, 则 f/g 也连续.

证明概要 注意到 $h(x) = f(x) \times g(x): X \to \mathbb{R} \times \mathbb{R}$, $f + g$ 是 h 和加法运算 $+: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ 的复合, 则 $f + g$ 连续. $f - g, f \cdot g, f/g$ 同理可证. □

练习 5.7 证明**命题** 5.3.3.

练习 5.8 $A \subset X$ 的边界 (boundary) 定义为 $\mathrm{Bd}\, A = \bar{A} \cap \overline{X - A}$, 则证明:

(1) $\operatorname{Int} A \cap \operatorname{Bd} A = \varnothing$, $\operatorname{Int} A \cup \operatorname{Bd} A = \bar{A}$; (2) $\operatorname{Bd} A = \varnothing$ 的充要条件是 A 既开又闭; (3) U 是开集的充要条件是 $\operatorname{Bd} U = \bar{U} - U$.

练习 5.9 证明函数 $f : \mathbb{R} \to \mathbb{R}$ 连续性的 ε-δ 定义等价于拓扑定义.

练习 5.10 证明**定理** 5.3.4.

练习 5.11 证明 $\mathbb{R}$ 上的任两个有限开区间或任两个有限闭区间同胚.

5.4 the Product Topology and Box Topology

之前我们介绍了二维的积拓扑, 这里将其推广到多维, 并介绍无限维的情况.

定义 5.4.1 设 J 是指标集, 给定集合 X, 则定义函数 $\boldsymbol{x} : J \to X$, $\alpha \mapsto x_\alpha$. 于是也可以将其表示作 $(x_\alpha)_{\alpha\in J}$, 并称其为 J 元组 (J-tuple); x_α 称作 $\boldsymbol{x}$ 的第 α 元分量.

这相当于把笛卡尔积做了进一步的推广. 之前我们讨论的笛卡尔积的形式都是诸如 $X_1 \times X_2 \times \cdots$ 的形式, 其实这相当于是令 $J = \{1, 2, \cdots\} = \mathbb{N}_+$.

定义 5.4.2 笛卡尔积 (Cartesian product): 设 $X = \bigcup\limits_{\alpha\in J} A_\alpha$, 则定义笛卡尔积 $\prod A_\alpha$ 为所有的满足 $\forall\alpha \in J$, $x_\alpha \in A_\alpha$ 的 J-元组 $(x_\alpha)_{\alpha\in J}$ 的集合, 即

$$\prod_{\alpha\in J} A_\alpha = \{\boldsymbol{x} : J \to X \mid \forall\alpha \in J, \boldsymbol{x}(\alpha) \in A_\alpha\}.$$

之后我们默认取定指标集 $\alpha \in J$, 并将下标略去.

定义 5.4.3 定义投影映射 (projection mapping)

$$\pi_\beta : \prod X_\alpha \to X_\beta, \ ((x_\alpha)) \mapsto x_\beta.$$

定义 5.4.4 对积空间 $\prod X_\alpha$ 上所有形如 $\prod U_\alpha$ 的族, 其中 $\forall\alpha \in J, U_\alpha$ 在 A_α 上是开集; 则这个族生成的拓扑定义为箱拓扑 (box topology).

定义 5.4.5 定义由子基

$$\mathcal{S} = \bigcup_{\beta\in J} \mathcal{S}_\beta, \quad \mathcal{S}_\beta = \left\{\pi_\beta^{-1}(U_\beta) \mid U_\beta \text{ 是 } X_\beta \text{ 上的开集}\right\}$$

生成的拓扑为积拓扑 (product topology), 此时 $\prod X_\alpha$ 称为积空间.

定理 5.4.1 对于每一个空间 X_α, 设它的基为 $\mathcal{B}_\alpha$. 则:

(1) 满足 $\forall\alpha \in J, B_\alpha \in \mathcal{B}_\alpha$ 的 $\prod B_\alpha$ 是 $\prod X_\alpha$ 的箱拓扑的基;

(2) 对有限多的 α 取 $B_\alpha \in \mathcal{B}_\alpha$, 剩下的取 $B_\alpha = X_\alpha$ 的 $\prod B_\alpha$ 是 $\prod X_\alpha$ 的积拓扑的基.

证明概要 略 □

有限情形下积拓扑等价于箱拓扑, 但一般箱拓扑细于积拓扑. 默认积空间装备积拓扑.

命题 5.4.1 若 $\forall\alpha\in J$, A_α 为 X_α 的子空间, 则 $\prod A_\alpha$ 也是 $\prod X_\alpha$ 在同样赋予积拓扑 (箱拓扑) 下的子空间.

证明概要 略 □

下面我们考察箱拓扑在有限推无限时的局限性:

定理 5.4.2 设 $f:A\to\prod X_\alpha$, $a\mapsto(f_\alpha(a))_{\alpha\in J}$, 其中 $f_\alpha:A\to X_\alpha$. 若设 $\prod X_\alpha$ 装备积拓扑, 则 f 连续当且仅当 $\forall\alpha\in J$, f_α 连续.

证明概要 略 □

例 5.4.1 对于箱拓扑上述定理不成立: 若考虑 $\mathbb{R}$ 的可数无限积

$$\mathbb{R}^\omega=\prod_{n\in\mathbb{N}_+}X_n,\quad \forall n\in\mathbb{N}_+,\ X_n=\mathbb{R},$$

则定义函数 $f:\mathbb{R}\to\mathbb{R}^\omega$, $t\mapsto(t,t,t,\cdots)$.

(1) 若对 $\mathbb{R}^\omega$ 赋予积拓扑, 由上述定理 f 连续;

(2) 若赋予箱拓扑, 取基元

$$B=(-1,1)\times\left(-\frac{1}{2},\frac{1}{2}\right)\times\left(-\frac{1}{3},\frac{1}{3}\right)\times\cdots,$$

但是 $f^{-1}(B)$ 在 $\mathbb{R}$ 中不是开集, 否则 $\exists\delta>0,\forall n\in\mathbb{N}_+,(-\delta,\delta)\subset\left(-\frac{1}{n},\frac{1}{n}\right)$ 导出矛盾.

所以积拓扑的好处在于它保持了有限交的限制; 箱拓扑的局限性在于它的基都规定好是某一个开集, 但在无穷的情况下我们不一定能够如此一一找到合适的开集.

5.5 Metric Topology

在集合上定义拓扑最重要最常用的方法之一就是通过这个集合的度量来实现.

定义 5.5.1 集合 X 的一个度量 (metric) 是一个函数 $d:X\times X\to\mathbb{R}$, 它满足:

(1) $\forall x,y\in X$, $d(x,y)\geq 0$, 当且仅当 $x=y$ 时取等;

(2) $\forall x,y\in X$, $d(x,y)=d(y,x)$;

(3) $\forall x,y,z\in X$, $d(x,y)+d(y,z)\geq d(x,z)$.

此时称 $d(x,y)$ 为 x 与 y 在度量 d 下的距离 (distance).

定义 5.5.2 称 $B_d(x,\varepsilon)=\{y\mid d(x,y)<\varepsilon\}$ 为以 x 为中心的 ε-球; 全体 ε-球 $B(x,\varepsilon)$, $(x\in X,\ \varepsilon>0)$ 的族作为基生成的 X 的拓扑称为由度量 d 诱导出来的度量拓扑 (metric topology).

命题 5.5.1 U 是由 d 诱导度量拓扑中的开集的充要条件是 $\forall y\in U,\exists\delta>0$, s.t. $B_d(y,\delta)\subset U$.

证明概要 略 □

例 5.5.1 $d(x,y)=|x-y|$ 定义了 $\mathbb{R}$ 上的标准度量, 由它诱导出来的拓扑等价于序拓扑.

定义 5.5.3 对拓扑空间 X, 若 X 的拓扑由其某度量 d 所诱导, 则称 X 可度量 (metrizable), 这时 X 在 d 下成为度量空间 (metric space), 一般记作度量空间 (X,d).

度量空间在某些具体度量下的性质往往依赖于它的分析特点, 如:

定义 5.5.4 对度量空间 (X,d), 若 $\exists M$, s.t. $\forall a_1,\, a_2\in A\subset X, d(a_1,a_2)\le M$, 则称 A 为有界的 (bounded), 其直径 (diameter) 定义为

$$\operatorname{diam} A=\sup\left\{d(a_1,a_2)\mid a_1,a_2\in A\right\}.$$

定理 5.5.1 对度量空间 (X,d), 则

$$\bar{d}:X\times X\to\mathbb{R},\quad \bar{d}(x,y)=\min\{d(x,y),1\}$$

所定义的 $\bar{d}$ 是一个度量, 它和 d 诱导 X 上的同一个拓扑.

度量 $\bar{d}$ 称为相应于 d 的标准有界度量 (standard bounded metric).

证明概要 略 □

定义 5.5.5 给定 $\mathbb{R}^n$ 中的点 $\boldsymbol{x}=(x_1,\cdots,x_n)$. 定义其模 (norm) 为

$$\|\boldsymbol{x}\|=\sqrt{(x_1^2+\cdots+x_n^2)};$$

定义 $\mathbb{R}^n$ 中的欧氏度量 (Euclidean metric) d 为

$$d(\boldsymbol{x},\boldsymbol{y})=\|\boldsymbol{x}-\boldsymbol{y}\|=\sqrt{(x_1-y_1)^2+\cdots+(x_n-y_n)^2};$$

定义 $\mathbb{R}^n$ 中的平方度量 (square metric) ρ 为

$$\rho(\boldsymbol{x},\boldsymbol{y})=\max\left\{|x_1-y_1|,\cdots,|x_n-y_n|\right\}.$$

引理 对 X 上的两个度量 d,d' 和它们诱导的拓扑 $\mathcal{T},\mathcal{T}'$, 则 $\mathcal{T}'$ 细于 $\mathcal{T}$ 的充要条件是

$$\forall x\in X,\,\varepsilon>0,\,\exists\delta>0,\ \text{s.t. } B_{d'}(x,\delta)\subset B_d(x,\varepsilon).$$

证明概要 略 □

定义 5.5.6 给定指标集 J 以及 $\mathbb{R}^J$ 中的点 $\boldsymbol{x}=(x_\alpha)_{a\in J}$ 和 $\boldsymbol{y}=(y_\alpha)_{a\in J}$, 定义 $\mathbb{R}^J$ 的度量

$$\bar{\rho}(\boldsymbol{x},\boldsymbol{y})=\sup\left\{\bar{d}\left(x_\alpha,y_\alpha\right)\mid\alpha\in J\right\},$$

其中 $\bar{d}$ 是 R 的标准有界度量, $\bar{\rho}$ 称为 $\mathbb{R}^J$ 上的一致度量 (uniform metric), 由 $\bar{\rho}$ 所诱导出来的拓扑称为一致拓扑 (uniform topology).

一致拓扑与积拓扑和箱拓扑之间有以下关系:

定理 5.5.2 $\mathbb{R}^J$ 上的一致拓扑细于积拓扑, 粗于箱拓扑. 当 J 无限时, 这三个拓扑两两不同.

证明概要 略 □

定理 5.5.3 序列引理 (Sequence Lemma): 对拓扑空间 X 及 $A \subset X$, 若 A 中有一个收敛于 x 的序列, 则 $x \in \bar{A}$. 若 X 可度量化, 则逆命题也成立.

证明概要 略 □

命题 5.5.2 对度量空间 X 及 $f : X \to Y$, 则 f 连续等价于对于 X 中任一收敛序列 $x_n \to x$, $f(x_n)$ 收敛于 $f(x)$.

证明概要 略 □

事实上这里只需要 C_1 公理, 具体内容会在之后详细说明.

定义 5.5.7 对度量空间 (Y, d) 和集合 X, $f_n, f : X \to Y$, 若 $\forall \varepsilon > 0, \exists N \in \mathbb{N}_+, \forall n > N, x \in X$, 有 $d\left(f_n(x), f(x)\right) < \varepsilon$, 则称 (f_n) 一致收敛 (converges uniformly) 于函数 $f : X \to Y$.

收敛的一致性不仅依赖于 Y 的拓扑, 也依赖于 Y 上的度量.

定理 5.5.4 一致极限定理 (Uniform Limit Theorem): 对拓扑空间 X, 度量空间 Y 及序列 $(f_n : X \to Y)$, 若 (f_n) 一致收敛于 f, 则 f 连续.

证明概要 略 □

练习 5.12 证明 $\mathbb{R} \times \mathbb{R}$ 在字典序拓扑下可度量化.

练习 5.13 证明由欧氏度量 d 和平方度量 ρ 诱导的 $\mathbb{R}^n$ 上的拓扑都等价于其上的积拓扑.

Chapter 6
Several Important Characters

我们接下来将介绍拓扑空间的两组公理: 分离公理和可数公理, 以及两大基本性质: 连通性与紧致性. 这部分更多地作为介绍性, 因此我们略去了一些较难的定理的证明.

6.1 the Separation Axioms

我们首先给出几个分离公理:

定理 6.1.1 若对于拓扑空间 $X, x \neq y \in X$, 我们有如下分离公理 (the separation axioms):

T_0 公理: 存在开集 U 使得其只包含其中一点;

T_1 公理: 存在邻域 U, V 使得 $y \notin U, x \notin V$;

T_2 公理: 存在不交的开集 $U, V, x \in U, y \in V$;

T_3 公理: X 是 T_1 的且任意 $x \in X$ 与闭集 $x \notin B \subset X$ 可以被两个无交开集分开;

T_4 公理: X 是 T_1 的且其中任何两个不交的闭集可以被两个无交开集分开.

其中 T_0 公理又被称作 Kolmogorov 公理, T_1 公理又被称作 Fréchet 公理, T_2 公理又被称作 Hausdorff 公理, T_3 公理又被称作正则性 (regular) 公理, T_4 公理又被称作正规性 (normal) 公理.

另外我们还有如下两个不常用的公理:

$T_{3.5}$ 公理: X 是 T_1 且任意 $x \in X$ 与闭集 $x \notin B \subset X$ 可以被 X 上的一连续函数分开; 这里 $A, B \subset X$ 被连续函数分开指的是存在连续函数 $f : X \to [0, 1]$, 使得 $f(A) = \{0\}, f(B) = \{1\}$.

T_5 公理: X 是 T_1 且满足 $A \cap \bar{B} = \bar{A} \cap B = \varnothing$ 的集合 A, B 可以被两个无交开集分开.

$T_{3.5}$ 公理又被称作完全正则性公理, T_5 公理又被称作完全正规性公理.

它们都涉及不交的开集, 因此被称作分离公理.

命题 6.1.1 下列条件等价:

(1) X 是 T_1 空间; (2) X 中单点集都是闭集; (3) X 中有限子集都是闭集.

证明概要 略 □

定理 6.1.2 Hausdorff 空间中的有限集都是闭集, 即 $T_2 \Rightarrow T_1$.

证明概要 略 □

定理 6.1.3 Hausdorff 空间 X 中的一个序列最多收敛到一个点; 该点称作该序列的极限 (limit).

证明概要 略 □

命题 6.1.2 对拓扑空间 X, X 的单点集为闭集, 则:

(1) X 是 T_3 的当且仅当对任意 $x \in X$ 与其邻域 U, 存在 x 的邻域 V 使得 $\bar{V} \subset U$;

(2) X 是 T_4 的当且仅当对任意开集 U 和闭集 $A \subset U$, 存在包含 A 的开集 V 使得 $\bar{V} \subset U$.

证明概要 略 □

例 6.1.1 下面给出上面若干分离公理相关的例子:

T_0 非 T_1: $\{a, b, c\}$ 赋予拓扑 $\{\varnothing, \{a\}, \{a, b\}, \{a, b, c\}\}$;

T_1 非 T_2: 有限补拓扑 $(\mathbb{R}, \tau_f)$;

T_2 非 T_3: $\mathbb{R}$ 上的 K-拓扑 $\mathbb{R}_K$;

T_3 非 T_4: $\mathbb{R}$ 上的下限拓扑的积空间 $\mathbb{R}_\ell^2$, 此平面拓扑称为 Sorgenfrey 平面.

定理 6.1.4 分离公理的继承性:

Hausdorff 空间的子空间是 Hausdorff 的, Hausdorff 空间的积空间也是 Hausdorff 的;

正则空间的子空间是正则的, 正则空间的积空间也是正则的;

正规空间的子空间未必是正规的, 正规空间的积空间也未必是正规的.

练习 6.1 证明装备序拓扑的全序集 Hausdorff.

练习 6.2 证明 Hausdorff 空间中的有限集都是闭集, 即 $T_2 \Rightarrow T_1$.

6.2 the Countability Axioms

定义 6.2.1 对拓扑空间 X 及 $x \in X$, 若存在 x 的可数邻域族 $\{U_n\}_{n\in\mathbb{N}_+}$, 使得 x 的任意邻域 U 至少包含一个 U_n, 则称 X 在 x 处有可数基 (countable basis).

定理 6.2.1 若对于拓扑空间 X, 我们有如下可数公理 (the countability axioms):

C_1 公理: 拓扑空间 X 在每一点处都有可数基;

C_2 公理: 拓扑空间 X 具有可数基.

这里我们可以将**定理** 5.5.3 和**命题** 5.5.2 加细到 C_1 的情况下, 不赘述.

定义 6.2.2 若空间 X 的子集 A 满足 $\bar{A} = X$, 则称 A 在 X 中稠密 (dence).

定理 6.2.2 设 X 有一个可数基 (即满足 C_2), 则:

(1) X 的每一个开覆盖有一个可数子覆盖;

(2) 存在一个 X 的可数子集在 X 中稠密.

满足 (1) 的空间称作 Lindelöf 空间, 满足 (2) 的开集称作可分 (separable) 空间.

证明概要 略 □

例 6.2.1 $\mathbb{R}$ 上的下限拓扑 $\mathbb{R}_\ell$ 是 C_1 的, Lindelöf 的, 可分的; 但不是 C_2 的.

定理 6.2.3 可数公理的继承性:

C_1 空间的子空间是 C_1 的, C_1 空间的可数积空间也是 C_1 的;

C_2 空间的子空间是 C_2 的, C_2 空间的可数积空间也是 C_2 的;

Lindelöf 空间的积空间未必是 Lindelöf 的; Lindelöf 空间的子空间也未必是 Lindelöf 的.

例 6.2.2 Lindelöf 空间和可分空间都比 C_2 弱, 且 C_1, Lindelöf, 可分空间三者两两不包含:

C_1 但非 Lindelöf: 不可数集上的离散拓扑;

C_1 但非可分: $X = [-1, 1]$ 上的拓扑 $\{U \subset X \mid 0 \notin U$ 或 $(-1, 1) \subset U\}$;

Lindelöf, 可分但非 C_1: 不可数集上的有限补拓扑;

Lindelöf 但非可分: 不可数集上的可数补拓扑;

可分但非 Lindelöf: 不可数集上的特定点拓扑.

练习 6.3 验证**例** 6.2.1.

6.3 Connectedness

定义 6.3.1 对拓扑空间 X, 它的一个分割 (separation) 指 X 的一对不交的非空开子集 U, V 且 $U \cap V = X$. 若 X 的分割不存在, 则称 X 连通 (connected).

连通性显然是一个拓扑性质, 即与连通空间同胚的每一空间都是连通的.

命题 6.3.1 等价定义: 空间 X 连通当且仅当 X 中既开又闭的子集只有空集和 X 自身.

引理 对 X 及其子空间 Y, Y 的一个分割指 Y 的一对不交的非空开子集 U, V, 满足 $U \cap V = Y$ 且 U, V 不包含对方的极限点. 若这样的分割不存在, 则 Y 连通.

证明概要 略 □

显然 X 的连通子空间 Y 会被包含在 X 的分割 C, D 中的一个空间中.

例 6.3.1 对 $Y = [-1, 0) \cup (0, 1]$, $[-1, 0)$, $(0, 1]$ 构成 Y 的一个分割.

命题 6.3.2 对 X 的连通子空间 A, 若 $A \subset B \subset \bar{A}$, 则 B 也连通.

证明概要 略 □

定理 6.3.1 连通空间在连续映射下的像连通.

证明概要 略 □

命题 6.3.3 连通空间的有限积空间连通.

证明概要 略 □

例 6.3.2 $\mathbb{R}^\omega$ 关于箱拓扑不连通, 但关于积拓扑连通.

定义 6.3.2 对 $x, y \in X$, 则 X 中从 x 到 y 的一条道路 (path) 是指从一个连续映射 $f : [a, b] \to X$, 使得 $f(a) = x$, $f(b) = y$. 如果空间 X 中每一对点都能用 X 中的一条道路连接, 则称 X 是道路连通 (path connected).

显然道路连通必然连通, 但连通不一定道路连通.

例 6.3.3 拓扑学家的正弦曲线 (topologist's sine curve): 取

$$S = \left\{ x \times \sin\left(\frac{1}{x}\right) \mid 0 < x \leq 1 \right\},$$

其在 $\mathbb{R}$ 中连通, $\bar{S} = S \cup 0 \times [-1, 1]$ 也在 $\mathbb{R}$ 中连通但是不道路连通.

定义 6.3.3 对拓扑空间 X 中的等价关系:

(1) 若 X 中存在包含 x, y 的连通子空间, 则规定 $x \sim y$, 则每一等价类称为 X 的一个分支 (component);

(2) 若 X 中存在从 x 到 y 的道路, 则规定 $x \sim y$, 则每一等价类称为 X 的一个道路分支 (path component)

定理 6.3.2 X 的所有分支或道路分支是 X 中一些两两不交的连通子空间, 它们的并等于 X, 且分别满足:

(1) X 中每一非空的连通子空间仅与一个分支相交;

(2) X 中每一非空的道路连通子空间仅与一个道路分支相交.

证明概要 只证明 (1), (2) 类似可得, 留作习题. □

定义 6.3.4 若对于空间 X 及 $x \in X$ 的每一个邻域 U, 若

(1) 存在 x 的一个连通邻域 V 包含于 U, 则称 X 在 x 处局部连通 (locally connected);

(2) 存在 x 的一个道路连通邻域 V 包含于 U, 则称 X 在 x 处局部道路连通 (locally path connected);

(3) 若 X 在它的每一个点处都是局部 (道路) 连通的, 则简称 X 是局部 (道路) 连通的.

例 6.3.4 $\mathbb{R}$ 上的每一个区间都连通且局部连通; $[-1, 0) \cup (0, 1]$ 不连通但局部连通; 拓扑学家的正弦曲线连通但不局部连通; $\mathbb{Q}$ 既不连通也不局部连通.

练习 6.4 证明 $\mathbb{Q}$ 不连通, 且其连通子空间只有单点集.

练习 6.5 验证**例** 6.3.2.

练习 6.6 验证**定理** 6.3.3.

练习 6.7 补全**定理** 6.3.2 的证明.

6.4 Compactness

定义 6.4.1 对空间 X 的子集族 $\mathcal{A}$, 若 $\bigcup\limits_{A\in\mathcal{A}} A = X$, 则称 $\mathcal{A}$ 覆盖 (cover) X. 若 $\mathcal{A}$ 是开子集族, 则称其为开覆盖 (open covering).

对 X 的子空间 Y, $\mathcal{A}$ 是 X 的一个子集族, 若 $\bigcup\limits_{A\in\mathcal{A}} A \supset Y$, 则称 $\mathcal{A}$ 覆盖 Y.

定义 6.4.2 若 X 的任何一个开覆盖 $\mathcal{A}$ 都有有限子覆盖, 则称空间 X 是紧致 (compact) 的.

命题 6.4.1 对 X 的子空间 Y, 则 Y 紧当且仅当其每一个 X 上的开覆盖有有限子覆盖.

证明概要 略 □

定理 6.4.1 紧空间的每个闭子集都是紧的;Hausdorff 空间的每个紧子空间都是闭的.

证明概要 略 □

命题 6.4.2 紧空间的连续像是紧的.

证明概要 略 □

定理 6.4.2 对紧空间 X, Hausdorff 空间 Y 及连续双射 $f : X \to Y$, 则 f 是同胚.

证明概要 略 □

命题 6.4.3 $\mathbb{R}^n$ 中子集 A 紧的充要条件是 A 闭且在欧氏度量 d 或平方度量 ρ 下有界.

证明概要 略 □

例 6.4.1 考虑 $\mathbb{R}^2$ 中如下两个非紧集:

(1) $A = \left\{x \times \dfrac{1}{x} \mid 0 < x \leq 1\right\}$ 闭但不有界;

(2) $S = \left\{x \times \sin\left(\dfrac{1}{x}\right) \mid 0 < x \leq 1\right\}$ 有界但不闭.

定理 6.4.3 极值定理 (extreme value theorem): 对紧集 X, 装备序拓扑的全序集 Y 及连续函数 $f : X \to Y$, 则 $\exists c, d \in X$, 使得 $\forall x \in X$, $f(c) \leq f(x) \leq f(d)$.

证明概要 略 □

定义 6.4.3 若空间 X 中任意一个无穷子集都有极限点, 则称 X 极值点紧 (limit point compact).

定理 6.4.4 紧性蕴含极值点紧性.

证明概要 略 □

例 6.4.2 取 $X = \mathbb{N}_+ \times \{0, 1\}$, 则 X 极值点紧但不紧.

练习 6.8 证明 $\mathbb{R}$ 不紧; 区间 (a, b), $(a, b]$ 均不紧, 但是闭区间 $[a, b]$ 紧.

练习 6.9 验证**例** 6.4.1.

练习 6.10 证明紧空间的有限并是紧的.