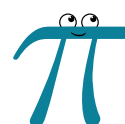


Algebra Chapter 0 - Paolo Aluffi - NoteBook

作者：若水

时间：May 4, 2024



上善若水任方圆



Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

— Evariste Galois

目录

第一章 集合论与范畴论	1
1.1 朴素集合论	1
1.1.1 集合	1
1.1.2 集合的关系	1
1.1.3 集合的运算	1
1.1.4 不交并与积	1
1.1.5 等价关系, 划分与商	1
1.2 集合间的函数	4
1.2.1 定义	4
1.2.2 多重集合与指标集	6
1.2.3 复合函数	6
1.2.4 单射, 满射与双射	7
1.2.5 单态射与满态射	8
1.2.6 自然投影	10
1.2.7 正则分解	10
1.3 范畴论	11
1.3.1 定义	11
1.3.2 范畴例子	12
1.4 态射	14
1.4.1 同构	14
1.4.2 单态射与满态射	14
1.5 万有性质	15
1.5.1 初始对象与终止对象	15
1.5.2 万有性质	16
1.5.3 商	16
1.5.4 积	16
1.5.5 余积	17
第二章 群论 I	18
2.1 群的定义	18
2.1.1 群和群胚	18
2.1.2 定义	19
2.1.3 基本性质	20
2.1.4 消去律	20
2.1.5 交换群	20
2.1.6 阶	20
2.1.7 有限群结构	22
2.2 群的例子	23
2.2.1 对称群	23
2.2.2 二面体群	24
2.2.3 循环群	24

2.2.4	矩阵群	26
2.2.5	初等数论	27
2.3	Grp 范畴	29
2.3.1	群同态映射	29
2.3.2	Grp 的定义	29
2.3.3	小小反思	30
2.3.4	积	30
2.3.5	Abel 群	30
2.4	群同态映射	31
2.4.1	例子	31
2.4.2	同态映射与阶	31
2.4.3	群同构映射	31
2.4.4	Abel 群的同态映射	37
2.5	自由群	37
2.5.1	生成元集	37
2.5.2	万有性质	38
2.5.3	具体结构	40
2.5.4	自由 Abel 群	40
2.6	子群	42
2.6.1	定义	42
2.6.2	核与像	44
2.6.3	由子集生成的子群	44
2.6.4	循环群的子群	45
2.6.5	单态射与满态射	46
2.7	商群	47
2.7.1	正规子群	47
2.7.2	商群	49
2.7.3	陪集	50
2.7.4	正规子群的商	50
2.7.5	核 \iff 正规子群	53
2.8	同构定理与 Lagrange 定理	54
2.8.1	同构定理	54
2.8.2	正则分解	54
2.8.3	表示	56
2.8.4	第三同构定理	56
2.8.5	第二同构定理	56
2.8.6	Lagrange 定理	56
2.8.7	余核与余像	58
2.9	群作用	58
2.9.1	作用	58
2.9.2	集合作用	58
2.9.3	轨道-稳定化子定理与范畴 $G\text{-Set}$	60
2.10	范畴中的群对象	61
2.10.1	范畴论的观点	61

第三章 群论 II	62
3.1 共轭作用	62
3.1.1 集合上的群作用	62
3.1.2 关于群的共轭作用	63
3.1.3 关于幂集的共轭作用	65
3.2 Sylow 定理	66
3.2.1 Sylow p -子群	66
3.2.2 特征子群	68
3.2.3 幂零群	68
3.2.4 Cauchy 定理	68
3.2.5 Sylow 第一定理	69
3.2.6 Sylow 第二定理	69
3.2.7 Sylow 第三定理	70
3.2.8 应用	70
3.3 合成列与可解性	73
3.3.1 Jordan-Hölder 定理	73
3.3.2 Schreier 定理	75
3.3.3 换位子群与可解性	76
3.4 对称群	81
3.4.1 轮换	81
3.4.2 S_n 中的型与共轭类	82
3.4.3 交错群	82
3.4.4 A_n 的结构	85
3.4.5 S_n 的结构	88
3.5 群的积	89
3.5.1 直积	89
3.5.2 半直积	90
3.5.3 群的正合序列	91
3.6 有限 Abel 群	92
3.6.1 有限 abel 群的分类	92
3.6.2 有限 Abel 群的结构定理	93
3.6.3 域的乘法群的有限子群	93
第四章 环论 I	95
4.1 环的定义	96
4.1.1 定义	96
4.1.2 零因子与单位	101
4.1.3 幂零与 Bool 环	105
4.1.4 多项式环	107
4.1.5 单环与群环	110
4.2 Ring 范畴	110
4.2.1 环同态映射	110
4.2.2 子环与中心	111
4.2.3 特征	113
4.2.4 多项式环的万有性质	114

4.2.5 单态射与满态射	115
4.2.6 积	115
4.2.7 $\text{End}_{\text{Ab}}(G)$	115
4.3 理想与商环	116
4.3.1 理想	116
4.3.2 基本运算	118
4.3.3 商环	120
4.3.4 核 \iff 理想	120
4.3.5 正则分解	121
4.4 素理想与极大理想	122
4.4.1 生成理想	122
4.4.2 多项式环的商	123
4.4.3 素理想与极大理想	124
4.5 环上的模	127
4.5.1 R -模的定义	127
4.5.2 $R\text{-Mod}$ 范畴	127
4.5.3 子模与商	128
4.5.4 正则分解与同构定理	128
第五章 环论 II	130
5.1 分解整环与 Noether 环	130
5.1.1 素元与不可约元	130
5.1.2 分解整环	132
5.1.3 Noether 环	134
5.2 UFD, PID, ED	136
5.2.1 最大公因子	136
5.2.2 UFD	136
5.2.3 $\text{PID} \implies \text{UFD}$	138
5.2.4 Euclid 整环	138
5.3 间奏曲: Zorn 引理	139
5.3.1 集合论: 再一次邂逅	139
5.3.2 应用: 极大理想的存在性	141
5.4 多项式环的唯一完全因子分解	141
5.4.1 Gauss 引理	141
5.4.2 整环的分式域	144
5.4.3 R 为 UFD $\implies R[x]$ 为 UFD	145
5.5 多项式的不可约性	145
5.5.1 根与可约性	145
5.5.2 代数闭域	146
5.5.3 $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x]$ 的可约性	147
5.5.4 Eisenstein 判别法	148
5.6 Gauss 整数与 Fermat 平方和定理	149
5.6.1 Gauss 整数	149
5.6.2 Fermat 平方和定理	150

第六章 域论	152
6.1 域扩张 I	152
6.1.1 基本定义	152
6.1.1.1 域扩张	152
6.1.1.2 域的特征	152
6.1.2 单扩张	154
6.1.2.1 单扩张结构	154
6.1.2.2 k -自同构映射群	156
6.1.3 有限扩张与代数扩张	157
6.1.3.1 有限扩张	157
6.1.3.2 代数扩张	158
6.1.3.3 有限生成域	159
6.2 代数闭包与 Nullstellensatz	161
6.2.1 代数闭包	161
6.2.2 Hilbert's Nullstellensatz	162
6.2.3 一点点代数几何	162
6.3 尺规作图	164
6.3.1 尺规作图	164
6.3.2 可构造数与二次扩张	164
6.4 域扩张 II	165
6.4.1 分裂域与正规扩张	165
6.4.1.1 分裂域	165
6.4.1.2 正规扩张	166
6.4.2 可分多项式	166
6.4.3 代数闭包中的可分扩张与嵌入	168
6.5 域扩张 III	168
6.5.1 有限域	168
6.5.2 分圆多项式与分圆域	169
6.6 可分性与单扩张	170
6.7 Galois 理论	171
6.7.1 Galois 对应与 Galois 扩张	171
6.7.2 Galois 基本定理	172
6.8 Galois 理论的应用	173
6.8.1 代数基本定理	173
6.8.2 正 n 边形的尺规作图	173
6.8.3 对称函数基本定理	175
6.8.4 多项式方程的根式可解性	175
6.8.4.1 根式扩张	175
6.8.4.2 多项式的根式可解性	176
附录 A 群论的 MATLAB 函数	178
A.1 特殊群	179
A.2 群结构	184
A.3 群运算	191
A.4 辅助函数	196

第一章 集合论与范畴论

1.1 朴素集合论

1.1.1 集合

定理 1.1.1 (Russell 悖论)

Russell 悖论: 对于集合 $R = \{r : r \notin r\}$, 成立

$$R \in R \iff R \notin R$$



1.1.2 集合的关系

- 集合: $\emptyset, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- 量词: $\exists, \forall, \exists!$
- 包含: $\subset, \subseteq, \subsetneq$
- 势: $|S|$
- 幂集 (power set): $\mathcal{P}(S) = \{T \subset S\}$

1.1.3 集合的运算

- 运算: $\cup, \cap, \setminus, \sqcup, \times$

1.1.4 不交并与积

定义 1.1.1 (不交并 disjoint union)

$$A \sqcup B = (\{0\} \times A) \times (\{1\} \times B)$$



定义 1.1.2 (积 product)

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



1.1.5 等价关系, 划分与商

定义 1.1.3 (关系 relation)

定义集合 S 上的一个关系为 $R \subset S \times S$, 称 a 和 b 存在关系 R , 并记做记作 aRb , 如果 $(a, b) \in R$.



定义 1.1.4 (等价关系 equivalence relation)

称集合 S 上的关系 \sim 为等价关系, 如果其满足如下性质。

- 自反性 (reflexivity): $a \sim a$
- 对称性 (symmetry): $a \sim b \implies b \sim a$
- 传递性 (transitivity): $a \sim b, b \sim c \implies a \sim c$



定义 1.1.5 (等价类 equivalence class)

对于 $a \in S$, 定义 a 关于等价关系 \sim 的等价类为

$$[a]_{\sim} = \{s \in S : a \sim s\}$$

对于 $A \subset S$, 定义 A 关于等价关系 \sim 的等价类为

$$[A]_{\sim} = \{s \in S : \exists a \in A, \text{ s.t. } a \sim s\}$$



例题 1.1 好朋友: 满足自反性和对称性, 但不满足传递性。

命题 1.1.1 (等价类的性质)

$$\left[\bigcup_{\lambda \in \Lambda} S_{\lambda} \right]_{\sim} = \bigcup_{\lambda \in \Lambda} [S_{\lambda}]_{\sim} = \left[\bigcup_{\lambda \in \Lambda} [S_{\lambda}]_{\sim} \right]_{\sim}, \quad \left[\bigcap_{\lambda \in \Lambda} S_{\lambda} \right]_{\sim} \subset \bigcap_{\lambda \in \Lambda} [S_{\lambda}]_{\sim} = \left[\bigcap_{\lambda \in \Lambda} [S_{\lambda}]_{\sim} \right]_{\sim}$$

**定义 1.1.6 (划分 partition)**

称子集族 $\mathcal{P} \subset \mathcal{P}(S)$ 为集合 S 的一个划分, 如果

$$\bigsqcup_{T \in \mathcal{P}} T = S$$

定义集合 S 关于等价关系 \sim 的划分为

$$\mathcal{P}_{\sim} = \{[a]_{\sim} : a \in S\}$$

**定义 1.1.7 (商 quotient)**

定义集合 S 关于等价关系 \sim 的商为

$$S / \sim = \{[a]_{\sim} : a \in S\}$$



例题 1.2 对于实数域 \mathbb{R} , 定义等价关系 \sim :

$$a \sim b \iff a - b \in \mathbb{Z}$$

对于实数平面 \mathbb{R}^2 , 定义等价关系 \approx :

$$(a_1, a_2) \approx (b_1, b_2) \iff a_1 - b_1 \in \mathbb{Z}, a_2 - b_2 \in \mathbb{Z}$$

那么

$$\mathbb{R} / \sim = [0, 1), \quad \mathbb{R}^2 / \approx = [0, 1) \times [0, 1)$$

定理 1.1.2 (等价类的不变性)

如果 \sim 为集合 S 上的等价关系, 那么对于任意 $a, b \in S$, 或 $[a]_{\sim} = [b]_{\sim}$ 成立, 或 $[a]_{\sim} \cap [b]_{\sim} = \emptyset$ 成立, 且仅成立其中之一。



证明 第一, 显然二者不能同时成立。事实上, 如果 $[a]_{\sim} = [b]_{\sim}$ 且 $[a]_{\sim} \cap [b]_{\sim} = \emptyset$, 那么 $[a]_{\sim} = [b]_{\sim} = \emptyset$, 但是 $a \in [a]_{\sim}$, 矛盾!

第二, 如果 $[a]_{\sim} = [b]_{\sim}$, 那么命题得证! 如果 $[a]_{\sim} \neq [b]_{\sim}$, 我们来证明 $[a]_{\sim} \cap [b]_{\sim} = \emptyset$ 。反证, 假设存在 $c \in S$, 使得 $c \in [a]_{\sim} \cap [b]_{\sim}$, 那么 $c \in [a]_{\sim}$ 且 $c \in [b]_{\sim}$ 。任取 $m \in [a]_{\sim}$, 由于 $c \in [a]_{\sim}$, 那么 $c \sim m$, 又 $c \in [b]_{\sim}$, 那么 $m \in [b]_{\sim}$, 于是 $[a]_{\sim} \subset [b]_{\sim}$, 同理 $[b]_{\sim} \subset [a]_{\sim}$, 进而 $[a]_{\sim} = [b]_{\sim}$, 矛盾! 因此 $[a]_{\sim} \cap [b]_{\sim} = \emptyset$ 。

定理 1.1.3 (划分 \iff 等价关系)

1. 如果子集族 $\mathcal{P} \subset \mathcal{P}(S)$ 为集合 S 上的划分, 那么存在 S 上的等价关系 \sim , 使得 $\mathcal{P} = \mathcal{P}_{\sim}$ 。
2. 如果关系 \sim 为集合 S 上的等价关系, 那么子集族 \mathcal{P}_{\sim} 为 S 上的一个划分。



证明 对于 1, 如果子集族 $\mathcal{P} \subset \mathcal{P}(S)$ 为集合 S 上的划分, 那么

$$\bigsqcup_{T \in \mathcal{P}} T_\lambda = S$$

定义 S 上的一个等价关系:

$$a \sim b \iff \exists T \in \mathcal{P}, a, b \in T$$

事实上, 对于任意 $a \in S$, 由于 $\bigsqcup_{T \in \mathcal{P}} T_\lambda = S$, 那么存在 $T \in \mathcal{P}$, 使得成立 $a \in T$, 自反性得证!

对于任意 $a, b \in S$, 如果 $a \sim b$, 那么存在 $T \in \mathcal{P}$, 使得成立 $a, b \in T$, 显然 $b \sim a$, 对称性得证!

对于任意 $a, b, c \in S$, 如果 $a \sim b, b \sim c$, 那么存在 $T_1, T_2 \in \mathcal{P}$, 使得成立 $a, b \in T_1, b, c \in T_2$, 于是 $b \in T_1 \cap T_2$. 而 \mathcal{P} 中元素的不交性保证了 $T_1 = T_2$, 进而 $a, c \in T_1 = T_2$, 即 $a \sim c$, 传递性得证!

于是 \sim 为 S 上的等价关系. 由 \sim 的定义, 不难发现对于任意 $T \in \mathcal{P}$, 任取 $t \in T \subset S$, 那么 $T = [t]_\sim$, 这是因为

$$T = [t]_\sim \iff T = \{s \in S : s \sim t\} \iff T = \{s \in S : \exists R \in \mathcal{P}, s, t \in R\} \iff T = \{s \in T\}$$

下面我们依托这个事实来证明: $\mathcal{P} = \mathcal{P}_\sim$.

一方面, 任取 $T \in \mathcal{P}$, 那么任取 $t \in T \subset S$, 可得 $T = [t]_\sim \in \mathcal{P}_\sim$, 于是 $\mathcal{P} \subset \mathcal{P}_\sim$.

另一方面, 任取 $[t]_\sim \in \mathcal{P}_\sim$, 由于 $\bigsqcup_{T \in \mathcal{P}} T_\lambda = S \ni t$, 那么存在 $T \in \mathcal{P}$, 使得成立 $t \in T$, 于是 $[t]_\sim = T \in \mathcal{P}$, 于是 $\mathcal{P}_\sim \subset \mathcal{P}$.

综合两方面, $\mathcal{P} = \mathcal{P}_\sim$ 成立, 原命题得证!

对于 2, 如果关系 \sim 为集合 S 上的等价关系, 那么 \mathcal{P}_\sim 中元素的不交性由定理 1.1.2 保证. 我们来证明

$$\bigsqcup_{T \in \mathcal{P}_\sim} T = S \iff \bigsqcup_{a \in S} [a]_\sim = S$$

一方面, 由于 $[a]_\sim \subset S$, 于是 $\bigsqcup_{a \in S} [a]_\sim \subset S$.

另一方面, 由于对于任意 $a \in S$, 显然 $a \in [a]_\sim$, 于是 $\bigsqcup_{a \in S} [a]_\sim \supset S$. 综合两方面, $\bigsqcup_{a \in S} [a]_\sim = S$.

综上所述, 原命题得证!

定义 1.1.8 (第二类 Stirling 数)

称将 n 个两两不同的元素划分为 k 个互不区分的非空子集的方案数称为第二类 Stirling 数, 记作 $S(n, k)$. 递推公式如下

$$S(n+1, k) = S(n, k-1) + kS(n, k)$$

通项公式如下:

$$S(n, k) = \frac{1}{k!} \sum_{i=0}^k (-1)^k \binom{k}{i} (k-i)^n$$



定义 1.1.9 (Bell 数)

称将 n 个两两不同的元素划分为互不区分的非空子集的方案数为第 n 个 Bell 数, 记作 $B(n)$. 解析表达式为

$$B(n) = \sum_{k=0}^n S(n, k) = \sum_{k=0}^n \sum_{i=0}^k (-1)^k \frac{1}{k!} \binom{k}{i} (k-i)^n$$



命题 1.1.2

n 个元素的集合上可以定义 $B(n)$ 个不同的等价关系, 其中 $B(n)$ 为第 n 个 Bell 数.



表 1.1: 第二类 Stirling 数与 Bell 数表

n	$S(n, 0)$	$S(n, 1)$	$S(n, 2)$	$S(n, 3)$	$S(n, 4)$	$S(n, 5)$	$S(n, 6)$	$S(n, 7)$	$S(n, 8)$	$S(n, 9)$	$S(n, 10)$	$B(n)$
0	1	0	0	0	0	0	0	0	0	0	0	1
1	0	1	0	0	0	0	0	0	0	0	0	1
2	0	1	1	0	0	0	0	0	0	0	0	2
3	0	1	3	1	0	0	0	0	0	0	0	5
4	0	1	7	6	1	0	0	0	0	0	0	15
5	0	1	15	25	10	1	0	0	0	0	0	52
6	0	1	31	90	65	15	1	0	0	0	0	203
7	0	1	63	301	350	140	21	1	0	0	0	877
8	0	1	127	966	1701	1050	266	28	1	0	0	4140
9	0	1	255	3025	7770	6951	2646	462	36	1	0	21147
10	0	1	511	9330	34105	42525	22827	5880	750	45	1	115975

1.2 集合间的函数

1.2.1 定义

定义 1.2.1 (函数 function)

称 f 为定义域为 A , 陪域为 B 的函数, 如果对于任意 $a \in A$, 存在且存在唯一 $b \in B$, 使得成立 $f(a) = b$. 记作

$$\begin{aligned} f : A &\longrightarrow B \\ a &\longmapsto f(a) \end{aligned}$$

或者以图 (diagram) 表示

$$A \xrightarrow{f} B$$



定义 1.2.2 (图像 graph)

对于函数 $f : A \rightarrow B$, 定义其图像为

$$\Gamma_f = \{(a, b) : a \in A, b = f(a)\} \subset A \times B$$



命题 1.2.1

对于函数 $f : A \rightarrow B$, 成立 $\Gamma_f \cong A$.



证明 定义函数

$$\begin{aligned} \varphi : A &\longrightarrow \Gamma_f \\ a &\longmapsto (a, f(a)) \end{aligned}$$

显然 φ 为双射。

定义 1.2.3 (单位函数 identity function)

$$\begin{aligned} \mathbb{1}_A : A &\longrightarrow A \\ a &\longmapsto a \end{aligned}$$



定义 1.2.4

定义 $A \rightarrow B$ 上的所有函数构成集合 $B^A = \{f : A \rightarrow B\}$.



定义 1.2.5 (函数在子集上的限制)

对于函数 $f: A \rightarrow B$, 以及 $S \subset A$, 定义

$$\begin{aligned} f|_S: S &\longrightarrow B \\ s &\longmapsto f(s) \end{aligned}$$

**定义 1.2.6 (像 image)**

对于函数 $f: A \rightarrow B$, 定义子集 $S \subset A$ 的像为

$$f(S) = \{f(s) : s \in S\}$$

**定义 1.2.7 (原像 preimage)**

对于函数 $f: A \rightarrow B$, 定义子集 $T \subset B$ 的原像为

$$f^{-1}(T) = \{a \in A : f(a) \in T\}$$

**命题 1.2.2 (像与原像的性质)**

对于函数 $f: X \rightarrow Y$, 如下命题成立。

1. 如果 $A \subset B \subset X$, 那么

$$f(A) \subset f(B)$$

2. 如果 $A \subset B \subset Y$, 那么

$$f^{-1}(A) \subset f^{-1}(B)$$

3. 如果 $B \subset Y$, 那么

$$f^{-1}(B^c) = (f^{-1}(B))^c$$

4. 如果 $B, D \subset Y$, 那么

$$f^{-1}(B \setminus D) = f^{-1}(B) \setminus f^{-1}(D)$$

5. 如果 $\{B_\lambda\}_{\lambda \in \Lambda} \subset \mathcal{P}(Y)$, 那么

$$f^{-1}\left(\bigcup_{\lambda \in \Lambda} B_\lambda\right) = \bigcup_{\lambda \in \Lambda} f^{-1}(B_\lambda), \quad f^{-1}\left(\bigcap_{\lambda \in \Lambda} B_\lambda\right) = \bigcap_{\lambda \in \Lambda} f^{-1}(B_\lambda)$$

6. 如果 $\{A_\lambda\}_{\lambda \in \Lambda} \subset \mathcal{P}(X)$, 那么

$$f\left(\bigcup_{\lambda \in \Lambda} A_\lambda\right) = \bigcup_{\lambda \in \Lambda} f(A_\lambda), \quad f\left(\bigcap_{\lambda \in \Lambda} [A_\lambda]_\sim\right) = \bigcap_{\lambda \in \Lambda} f(A_\lambda)$$

其中等价关系 $x \sim y \iff f(x) = f(y)$ 。

7. 如果 $B \subset Y$, 那么

$$f(f^{-1}(B)) = B \cap \text{im } f$$

8. 如果 $A \subset X$, 那么

$$f^{-1}(f(A)) = [A]_\sim$$

其中等价关系 $x \sim y \iff f(x) = f(y)$ 。

**命题 1.2.3**

对于集合 S , 定义 $2^S = \{f: S \rightarrow \{0, 1\}\}$, 那么 $2^S \cong \mathcal{P}(S)$ 。



证明 定义函数

$$\begin{aligned}\varphi : 2^S &\longrightarrow \mathcal{P}(S) \\ f &\longmapsto \{s \in S : f(s) = 1\}\end{aligned}$$

下面我们证明 φ 为双射。

对于单射性，任取 $f_1, f_2 \subset 2^S$ ，满足 $\varphi(f_1) = \varphi(f_2)$ ，即 $\{s \in S : f_1(s) = 1\} = \{s \in S : f_2(s) = 1\}$ ，那么 $f_1 = f_2$ ，因此 φ 为单射。

对于满射性，任取 $A \subset S$ ，令

$$f(s) = \begin{cases} 1, & s \in A \\ 0, & s \in S \setminus A \end{cases}$$

显然 $\varphi(f) = A$ ，因此 φ 为满射。

综上所述， $2^S \cong \mathcal{P}(S)$ ，原命题得证！

1.2.2 多重集合与指标集

定义 1.2.8 (多重集合 multiset)

定义元素可重复的集合为多重集合。事实上，多重集合可以函数的观点考虑，例如对于多重集合 M ，其中 m_k 出现了 n_k 次，那么 M 即与如下函数同构。

$$\begin{aligned}\text{count}_M : \{m_k : k \in \mathbb{N}^*\} &\longrightarrow \mathbb{N}^* \\ m_k &\longmapsto n_k\end{aligned}$$



定义 1.2.9 (指标集 indexed set)

数列 $\{a_n\}_{n=1}^{\infty}$ 的本质为如下函数。

$$\begin{aligned}a : \mathbb{N}^* &\longrightarrow \mathbb{C} \\ n &\longmapsto a_n\end{aligned}$$



定义 1.2.10 (多重集合的包含)

对于有限多重集合 M 与 N ，称 M 包含于 N ，并记作 $M \leq N$ ，如果对于任意 $m \in M$ ，成立 $\text{count}_M(m) \leq \text{count}_N(m)$ 。



1.2.3 复合函数

定义 1.2.11 (复合函数 composition of function)

对于函数 $f : A \rightarrow B$ 和 $g : B \rightarrow C$ ，定义其复合函数为

$$\begin{aligned}f \circ g : A &\longrightarrow C \\ a &\longmapsto g(f(a))\end{aligned}$$

交换图如下

$$\begin{array}{ccc} A & \xrightarrow{f} & B \xrightarrow{g} C \\ & \searrow g \circ f & \nearrow \\ & & \end{array} \quad \text{或} \quad \begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow g \circ f & \downarrow g \\ & & C \end{array}$$



1.2.4 单射，满射与双射

定义 1.2.12 (单射 injection)

称函数 $f: A \rightarrow B$ 是单的，如果 $f(a_1) = f(a_2)$ ，那么 $a_1 = a_2$ 。单射记作 $f: A \hookrightarrow B$ 。

定义 1.2.13 (满射 surjection)

称函数 $f: A \rightarrow B$ 是满的，如果对于任意 $b \in B$ ，存在 $a \in A$ ，使得成立 $f(a) = b$ 。满射记作 $f: A \twoheadrightarrow B$ 。

定义 1.2.14 (双射 bijection)

称函数 $f: A \rightarrow B$ 是双射，并记作 $f: A \xrightarrow{\sim} B$ ，如果其既单又满。

例题 1.3 对于有 n 个元素的集合 S ，存在 $n!$ 个双射。

命题 1.2.4 (双射的复合为双射)

双射的复合为双射。

证明 如果函数 f, g 均为双射，那么其逆函数 f^{-1}, g^{-1} 满足

$$f \circ f^{-1} = f^{-1} \circ f = \mathbb{1}, \quad g \circ g^{-1} = g^{-1} \circ g = \mathbb{1}$$

于是

$$(f \circ g)(g^{-1} \circ f^{-1}) = (g^{-1} \circ f^{-1})(f \circ g) = \mathbb{1}$$

由定理 1.2.1 与定理 1.2.2，复合 $f \circ g$ 为双射。

命题 1.2.5 (双射的逆为双射)

双射的逆为双射。

证明 如果函数 f 为双射，其逆函数 f^{-1} 满足

$$f \circ f^{-1} = f^{-1} \circ f = \mathbb{1}$$

由定理 1.2.1 与定理 1.2.2，逆 f^{-1} 为双射。

定义 1.2.15 (同构的 isomorphic)

称集合 A 与 B 为同构的，并记做 $A \cong B$ ，如果存在双射 $f: A \rightarrow B$ 。

命题 1.2.6 (同构为等价关系)

同构为等价关系。

证明 定义关系

$$A \sim B \iff A \cong B \iff \exists \text{ 双射 } f: A \rightarrow B$$

对于反身性，显然 $\mathbb{1}_A$ 为双射，因此 $A \sim A$ 。

对于对称性，如果 $A \sim B$ ，那么存在双射 $f: A \rightarrow B$ ，由命题 1.2.5， $f^{-1}: B \rightarrow A$ 为双射，因此 $B \sim A$ 。

对于传递性，如果 $A \sim B, B \sim C$ ，那么存在双射 $f: A \rightarrow B, g: B \rightarrow C$ ，由命题 1.2.4， $f \circ g: A \rightarrow C$ 为双射，因此 $A \sim C$ 。

因此，同构为等价关系。

命题 1.2.7

如果 $A_1 \cong A_2, B_1 \cong B_2$ ，且 $A_1 \cap B_1 = A_2 \cap B_2 = \emptyset$ ，那么 $A_1 \cup B_1 \cong A_2 \cup B_2$ 。

证明 由于 $A_1 \cong A_2, B_1 \cong B_2$, 那么存在双射 $f: A_1 \rightarrow A_2$ 和 $g: B_1 \rightarrow B_2$, 定义函数

$$h: A_1 \cup B_1 \rightarrow A_2 \cup B_2$$

$$x \mapsto \begin{cases} f(x), & x \in A_1 \\ g(x), & x \in B_1 \end{cases}$$

由 $A_1 \cap B_1 = A_2 \cap B_2 = \emptyset$, 容易验证 h 为双射, 因此 $A_1 \cup B_1 \cong A_2 \cup B_2$ 。

定义 1.2.16 (逆 inverse)

对于双射 $f: A \rightarrow B$, 定义其逆为

$$f^{-1}: B \rightarrow A$$

$$f(a) \mapsto a$$

交换图如下

$$A \xrightarrow{f} B \xrightarrow{g} A, \quad B \xrightarrow{f} A \xrightarrow{g} B$$

$$\quad \quad \quad \mathbb{1}_A \quad \quad \quad \mathbb{1}_B$$

定义 1.2.17 (左逆 left-inverse)

称函数 $g: \text{im } f \rightarrow A$ 为函数 $f: A \rightarrow B$ 的左逆, 如果成立 $g \circ f = \mathbb{1}_A$ 。

定义 1.2.18 (右逆 right-inverse)

称函数 $g: B \rightarrow A$ 为函数 $f: A \rightarrow B$ 的右逆, 如果成立 $f \circ g = \mathbb{1}_B$ 。

命题 1.2.8 (双射 \iff 存在左右逆)

双射 \iff 存在左逆和右逆。

证明 见定理 1.2.1 与定理 1.2.2。

1.2.5 单态射与满态射

定义 1.2.19 (单态射 monomorphism)

称函数 $f: A \rightarrow B$ 是单态射, 如果对于任意集合 Z , 以及任意函数 $\alpha_1, \alpha_2: Z \rightarrow A$, 成立

$$f \circ \alpha_1 = f \circ \alpha_2 \implies \alpha_1 = \alpha_2$$

定义 1.2.20 (满态射 epimorphism)

称函数 $f: A \rightarrow B$ 是满态射, 如果对于任意集合 Z , 以及任意函数 $\beta_1, \beta_2: B \rightarrow Z$, 成立

$$\beta_1 \circ f = \beta_2 \circ f \implies \beta_1 = \beta_2$$

定理 1.2.1

对于函数 $f: A \rightarrow B$, 如下命题等价。

1. f 为单射。
2. f 存在左逆。
3. f 为单态射。

证明 $1 \implies 2$: 如果 f 为单射, 定义函数

$$g : \text{im } f \longrightarrow A$$

$$f(a) \longmapsto a$$

首先来验证 g 的定义是良好的。取 $a_1, a_2 \in A$, 满足 $f(a_1) = f(a_2)$, 由 f 的单射性, $a_1 = a_2$, 于是 g 定义良好。其次来验证 $g \circ f = \mathbb{1}$ 。任取 $a \in A$, 注意到 $(g \circ f)(a) = g(f(a)) = a$, 那么 $g \circ f = \mathbb{1}$ 。综合这两点, f 存在左逆 g 。

$1 \implies 3$: 如果 f 为单射, 任取 $\alpha_1, \alpha_2 : Z \rightarrow A$, 满足 $f \circ \alpha_1 = f \circ \alpha_2$ 。任取 $z \in Z$, 注意到

$$f(\alpha_1(z)) = (f \circ \alpha_1)(z) = (f \circ \alpha_2)(z) = f(\alpha_2(z))$$

于是 $\alpha_1 = \alpha_2$, 进而 f 是单态射。

$2 \implies 3$: 如果 f 存在左逆 g , 任取 α_1, α_2 , 满足 $f \circ \alpha_1 = f \circ \alpha_2$, 那么

$$\alpha_1 = \mathbb{1} \circ \alpha_1 = g \circ f \circ \alpha_1 = g \circ f \circ \alpha_2 = \mathbb{1} \circ \alpha_2 = \alpha_2$$

于是 f 是单态射。

$2 \implies 1$: 如果 f 存在左逆 g , 任取 $a_1, a_2 \in A$, 满足 $f(a_1) = f(a_2)$, 那么

$$a_1 = \mathbb{1}(a_1) = (g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2) = \mathbb{1}(a_2) = a_2$$

于是 f 是单射。

$3 \implies 1$: 如果 f 是单态射, 任取 $a_1, a_2 \in A$, 满足 $f(a_1) = f(a_2)$ 。定义 $\alpha_1 : Z \rightarrow \{a_1\}$ 和 $\alpha_2 : Z \rightarrow \{a_2\}$, 任取 $z \in Z$, 注意到

$$(f \circ \alpha_1)(z) = f(\alpha_1(z)) = f(a_1) = f(a_2) = f(\alpha_2(z)) = (f \circ \alpha_2)(z)$$

因此 $f \circ \alpha_1 = f \circ \alpha_2$, 于是 $\alpha_1 = \alpha_2$, 即 $a_1 = a_2$, 进而 f 是单射。

定理 1.2.2

对于函数 $f : A \rightarrow B$, 如下命题等价。

1. f 为满射。
2. f 存在右逆。
3. f 为满态射。



证明 $1 \implies 2$: 如果 f 是满射, 定义函数

$$g : B \longrightarrow A$$

$$b \longmapsto a$$

这里要说明的是对于特别的 $b \in B$, $f^{-1}(b)$ 中的元素可能不唯一, 这时候任取其一即可, 此时便说明 g 定义良好。然后我们来验证 $f \circ g = \mathbb{1}$ 。任取 $b \in B$, 注意到 $(f \circ g)(b) = f(g(b)) = f(f^{-1}(b)) = b$, 那么 $f \circ g = \mathbb{1}$, 进而 f 存在右逆 g 。

$1 \implies 3$: 如果 f 为满射, 任取 β_1, β_2 , 满足 $\beta_1 \circ f = \beta_2 \circ f$ 。任取 $b \in B$, 存在 $a \in A$, 使得成立 $f(a) = b$, 因此

$$\beta_1(b) = \beta_1(f(a)) = (\beta_1 \circ f)(a) = (\beta_2 \circ f)(a) = \beta_2(f(a)) = \beta_2(b)$$

于是 $\beta_1 = \beta_2$, 进而 f 是满态射。

$2 \implies 3$: 如果 f 存在右逆 g , 任取 β_1, β_2 , 满足 $\beta_1 \circ f = \beta_2 \circ f$, 那么

$$\beta_1 = \beta_1 \circ \mathbb{1} = \beta_1 \circ f \circ g = \beta_2 \circ f \circ g = \beta_2 \circ \mathbb{1} = \beta_2$$

于是 f 是满态射。

$2 \implies 1$: 如果 f 存在右逆 g , 任取 $b \in B$, 注意到 $g(b) \in A$, 且 $f(g(b)) = (f \circ g)(b) = \mathbb{1}(b) = b$, 因此 f 为满射。

3 \implies 1: 如果 f 是满态射, 任取 $b \in B$. 定义 $\beta_1 : B \rightarrow \{1\}$ 以及

$$\beta_2 : B \longrightarrow \{0, 1\}$$

$$b \longmapsto \begin{cases} 1, & b \in \text{im} f \\ 0, & b \in B \setminus \text{im} f \end{cases}$$

任取 $a \in A$, 注意到

$$(\beta_1 \circ f)(a) = \beta_1(f(a)) = 1 = \beta_2(f(a)) = (\beta_2 \circ f)(a)$$

因此 $\beta_1 \circ f = \beta_2 \circ f$, 于是 $\beta_1 = \beta_2$, 即 $b \in \text{im} f$, 进而 f 是满射。

1.2.6 自然投影

定义 1.2.21 (自然投影 natural projection)

对于集合 A 和 B , 定义其自然投影为

$$\pi_A : A \times B \longrightarrow A$$

$$(a, b) \longmapsto a$$

$$\pi_B : A \times B \longrightarrow B$$

$$(a, b) \longmapsto b$$

交换图如下

$$\begin{array}{ccc} & A \times B & \\ \pi_A \swarrow & & \searrow \pi_B \\ A & & B \end{array}$$



例题 1.4 解释函数 $f : A \rightarrow B$ 如何决定 π_A 的右逆。

由于

$$\pi_A : A \times B \longrightarrow A$$

$$(a, b) \longmapsto a$$

定义

$$\varphi : A \longrightarrow A \times B$$

$$a \longmapsto (a, f(a))$$

显然 $\pi_A \circ \varphi = \mathbb{1}_A$, 且 g 由 f 决定。交换图如下

$$\begin{array}{ccccc} A & \xrightarrow{\varphi} & A \times B & \xrightarrow{\pi_A} & A \\ & \searrow a \mapsto (a, f(a)) & & \nearrow (a, b) \mapsto a & \\ & & \mathbb{1}_A & & \end{array}$$

1.2.7 正则分解

定义 1.2.22 (正则分解 canonical decomposition)

对于函数 $f : A \rightarrow B$, 以及等价关系 $a_1 \sim a_2 \iff f(a_1) = f(a_2)$, f 可作如下正则分解。

$$\begin{array}{ccccccc} & & & f & & & \\ & & & \curvearrowright & & & \\ A & \xrightarrow{a \mapsto [a]_{\sim}} & A / \sim & \xrightarrow{[a]_{\sim} \mapsto f(a)} & \text{im} f & \xrightarrow{f(a) \mapsto f(a)} & B \end{array}$$



定义 1.3.4 (子范畴 subcategory)

称 C' 为范畴 C 的子范畴, 如果 $\text{Obj}(C') \subset \text{Obj}(C)$, 且对于任意对象 $A, B \in C'$, 成立 $\text{Hom}_{C'}(A, B) \subset \text{Hom}_C(A, B)$ 。

**定义 1.3.5 (满的 full)**

称范畴 C 的子范畴 C' 是满的, 如果对于任意对象 $A, B \in C'$, 成立 $\text{Hom}_{C'}(A, B) = \text{Hom}_C(A, B)$ 。

**1.3.2 范畴例子**

例题 1.7 集合范畴:

- $\text{Obj}(\text{Set})$: 所有集合。
- $\text{Hom}_{\text{Set}}(A, B) = B^A$

例题 1.8 矩阵范畴:

- $\text{Obj}(\mathbf{V}) = \mathbb{N}$
- $\text{Hom}_{\mathbf{V}}(m, n) = \{\{a_{ij}\}_{m \times n} : a_{ij} \in \mathbb{R}\}$

例题 1.9 余范畴 (opposite category):

- $\text{Obj}(C^{\text{op}}) = \text{Obj}(C)$
- $\text{Hom}_{C^{\text{op}}}(A, B) = \text{Hom}_C(B, A)$

例题 1.10 点范畴: 令 $*$ $\in \text{Set}$, 定义如下由点 $*$ 诱导的集合范畴 Set^* 。

- 对象: $\text{Obj}(\text{Set}^*) = (S, s)$, 意指态射 $\text{Hom}_C(\{*\}, S)$ 将 $*$ 映为 $s \in S$ 。
- 态射:

$$\text{Hom}_{\text{Set}^*}((S, s), (T, t)) = \{\sigma : S \rightarrow T \mid \sigma(s) = t\}$$

例题 1.11 关系范畴: 令 S 为一个集合, 关系 \sim 满足自反性和传递性, 定义如下由 S 以及 \sim 诱导的关系范畴 $C_{S, \sim}$ 。

- $\text{Obj}(C_{S, \sim}) = S$
-

$$\text{Hom}_{C_{S, \sim}}(a, b) = \begin{cases} \{(a, b)\}, & a \sim b \\ \emptyset, & a \not\sim b \end{cases}$$

例题 1.12 切片范畴 (slice category) 和余切片范畴 (co-slice category): 对于范畴 C , 以及对象 $S \in \text{Obj}(C)$, 定义如下由 S 诱导的切片范畴 C_S 。

- 对象:

$$\text{Obj}(C_S) = \{(f, A) : f \in \text{Hom}_C(A, S), A \in \text{Obj}(C)\}$$

通常以如下图表示

$$\begin{array}{c} A \\ \downarrow f \\ S \end{array}$$

- 态射:

$$\text{Hom}_{C_S}((f, A), (g, B)) = \{\sigma \in \text{Hom}_C(A, B) : f = g \circ \sigma\}$$

通常以如下交换图表示

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & B \\ & \searrow f & \swarrow g \\ & S & \end{array}$$

对于范畴 \mathbf{C} ，以及对象 $S \in \text{Obj}(\mathbf{C})$ ，定义如下由 S 诱导的余切范畴 \mathbf{C}^S 。

- 对象：

$$\text{Obj}(\mathbf{C}_S) = \{(f, A) : f \in \text{Hom}_{\mathbf{C}}(S, A), A \in \text{Obj}(\mathbf{C})\}$$

通常以如下图表示

$$\begin{array}{c} S \\ \downarrow f \\ A \end{array}$$

- 态射：

$$\text{Hom}_{\mathbf{C}_A}((f, A), (g, B)) = \{\sigma \in \text{Hom}_{\mathbf{C}}(A, B) : g = \sigma \circ f\}$$

通常以如下交换图表示

$$\begin{array}{ccc} & S & \\ f \swarrow & & \searrow g \\ A & \xrightarrow{\sigma} & B \end{array}$$

例题 1.13 对于对象 $A, B \in \mathbf{C}$ ，定义范畴 $\mathbf{C}_{A,B}$ 如下。

Obj :

$$\begin{array}{ccc} & A & \\ f \nearrow & & \searrow g \\ Z & & \\ & B & \end{array}$$

Hom :

$$\begin{array}{ccccc} & & & A & \\ & f_1 & & f_2 & \\ Z_1 & \xrightarrow{\sigma} & Z_2 & & \\ & g_1 & & g_2 & \\ & & & B & \end{array}$$

对于对象 $A, B \in \mathbf{C}$ ，定义范畴 $\mathbf{C}^{A,B}$ 如下。

Obj :

$$\begin{array}{ccc} A & & \\ & f \searrow & \\ & & Z \\ & g \nearrow & \\ B & & \end{array}$$

Hom :

$$\begin{array}{ccccc} A & & & & \\ & f_1 \searrow & & f_2 \searrow & \\ & & Z_1 & \xrightarrow{\sigma} & Z_2 \\ & g_1 \nearrow & & g_2 \nearrow & \\ B & & & & \end{array}$$

例题 1.14 对于态射 $\alpha : A \rightarrow C, \beta : B \rightarrow C$ ，定义范畴 $\mathbf{C}_{\alpha,\beta}$ 如下。

Obj :

$$\begin{array}{ccccc} & A & & & \\ f \nearrow & & \searrow \alpha & & \\ Z & & & C & \\ g \searrow & & \nearrow \beta & & \\ & B & & & \end{array}$$

Hom :

$$\begin{array}{ccccc} & A & & & \\ f_1 \nearrow & & \searrow f_2 & & \searrow \alpha \\ Z_1 & \xrightarrow{\sigma} & Z_2 & & \\ g_1 \searrow & & \nearrow g_2 & & \nearrow \beta \\ & B & & & \end{array}$$

对于态射 $\alpha : C \rightarrow A, \beta : C \rightarrow B$ ，定义范畴 $\mathbf{C}^{\alpha,\beta}$ 如下。

Obj :

$$\begin{array}{ccccc} & A & & & \\ \nearrow \alpha & & \searrow f & & \\ C & & & Z & \\ \searrow \beta & & \nearrow g & & \\ & B & & & \end{array}$$

Hom :

$$\begin{array}{ccccc} & A & & & \\ \nearrow \alpha & & \searrow f_1 & & \searrow f_2 \\ C & & & Z_1 & \xrightarrow{\sigma} & Z_2 \\ \searrow \beta & & \nearrow g_1 & & \nearrow g_2 \\ & B & & & \end{array}$$

1.4 态射

1.4.1 同构

定义 1.4.1 (左逆态射 left-inverse morphism)

对于范畴 \mathcal{C} , 以及对象 $A, B \in \text{Obj}(\mathcal{C})$, 称态射 $g \in \text{Hom}_{\mathcal{C}}(B, A)$ 为态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 的左逆态射, 如果成立 $g \circ f = \mathbb{1}_A$ 。



定义 1.4.2 (右逆态射 right-inverse morphism)

对于范畴 \mathcal{C} , 以及对象 $A, B \in \text{Obj}(\mathcal{C})$, 称态射 $g \in \text{Hom}_{\mathcal{C}}(B, A)$ 为态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 的右逆态射, 如果成立 $f \circ g = \mathbb{1}_B$ 。



定义 1.4.3 (同构态射 isomorphism)

对于范畴 \mathcal{C} , 以及对象 $A, B \in \text{Obj}(\mathcal{C})$, 称态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 为同构态射, 如果存在逆态射 $g \in \text{Hom}_{\mathcal{C}}(B, A)$, 使得成立

$$g \circ f = \mathbb{1}_A, \quad f \circ g = \mathbb{1}_B$$



定义 1.4.4 (同构的 isomorphic)

对于范畴 \mathcal{C} , 称对象 $A, B \in \text{Obj}(\mathcal{C})$ 是同构的, 且记作 $A \cong B$, 如果存在同构态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 。



定义 1.4.5 (自同构态射 automorphism)

对于范畴 \mathcal{C} , 称同构态射 $f \in \text{Hom}_{\mathcal{C}}(S, S)$ 为对象 $S \in \text{Obj}(\mathcal{C})$ 的自同构态射。



定义 1.4.6 (自同构态射群 automorphism group)

对于范畴 \mathcal{C} , 对象 $S \in \text{Obj}(\mathcal{C})$ 的自同构态射构成自同构态射群 $\text{Aut}_{\mathcal{C}}(S)$ 。



命题 1.4.1 (同构态射的性质)

- 同构态射存在且存在唯一逆。
- 恒等态射 $\mathbb{1}$ 为同构态射, 且 $\mathbb{1}^{-1} = \mathbb{1}$ 。
- 同构态射 f 的逆 f^{-1} 亦为同构态射, 且 $(f^{-1})^{-1} = f$ 。
- 如果 f, g 均为同构态射, 那么 $g \circ f$ 亦为同构态射, 且 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ 。



1.4.2 单态射与满态射

定义 1.4.7 (单态射 monomorphism)

对于范畴 \mathcal{C} , 以及对象 $A, B \in \text{Obj}(\mathcal{C})$, 称态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 为单态射, 如果对于任意对象 $Z \in \text{Obj}(\mathcal{C})$, 以及任意态射 $\alpha_1, \alpha_2 \in \text{Hom}_{\mathcal{C}}(Z, A)$, 成立

$$f \circ \alpha_1 = f \circ \alpha_2 \implies \alpha_1 = \alpha_2$$



定义 1.4.8 (满态射 epimorphism)

对于范畴 \mathcal{C} , 以及对象 $A, B \in \text{Obj}(\mathcal{C})$, 称态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 为满态射, 如果对于任意对象 $Z \in \text{Obj}(\mathcal{C})$, 以及任意态射 $\beta_1, \beta \in \text{Hom}_{\mathcal{C}}(B, Z)$, 成立

$$\beta_1 \circ f = \beta_2 \circ f \implies \beta_1 = \beta_2$$

**命题 1.4.2 (存在左逆 \implies 单态射)**

对于范畴 \mathcal{C} , 以及对象 $A, B \in \text{Obj}(\mathcal{C})$, 如果态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 存在左逆态射, 那么态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 为单态射。



证明 如果态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 存在左逆态射 $g \in \text{Hom}_{\mathcal{C}}(B, A)$, 那么任取 α_1, α_2 , 满足 $f \circ \alpha_1 = f \circ \alpha_2$, 由于

$$\alpha_1 = 1 \circ \alpha_1 = g \circ f \circ \alpha_1 = g \circ f \circ \alpha_2 = 1 \circ \alpha_2 = \alpha_2$$

于是 f 是单态射。

命题 1.4.3 (存在右逆 \implies 满态射)

对于范畴 \mathcal{C} , 以及对象 $A, B \in \text{Obj}(\mathcal{C})$, 如果态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 存在右逆态射, 那么态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 为满态射。



证明 如果态射 $f \in \text{Hom}_{\mathcal{C}}(A, B)$ 存在右逆态射 $g \in \text{Hom}_{\mathcal{C}}(B, A)$, 那么任取 β_1, β_2 , 满足 $\beta_1 \circ f = \beta_2 \circ f$, 由于

$$\beta_1 = \beta_1 \circ 1 = \beta_1 \circ f \circ g = \beta_2 \circ f \circ g = \beta_2 \circ 1 = \beta_2$$

于是 f 是满态射。

命题 1.4.4

单态射的复合为单态射, 满态射的复合为满态射。



1.5 万有性质

1.5.1 初始对象与终止对象

定义 1.5.1 (初始对象 initial object)

对于范畴 \mathcal{C} , 称对象 $I \in \text{Obj}(\mathcal{C})$ 为 \mathcal{C} 的初始对象, 如果对于任意对象 $S \in \text{Obj}(\mathcal{C})$, 存在且存在唯一 \mathcal{C} 中的态射 $I \rightarrow S$ 。

$$I \xrightarrow{\exists! \varphi} \forall S$$

**定义 1.5.2 (终止对象 final object)**

对于范畴 \mathcal{C} , 称对象 $F \in \text{Obj}(\mathcal{C})$ 为 \mathcal{C} 的终止对象, 如果对于任意对象 $S \in \text{Obj}(\mathcal{C})$, 存在且存在唯一 \mathcal{C} 中的态射 $S \rightarrow F$ 。

$$S \xrightarrow{\exists! \varphi} \forall F$$

**定义 1.5.3 (终端对象 terminal object)**

初始对象和终止对象统称为终端对象。



命题 1.5.1 (终端对象的结构)

对于范畴 \mathcal{C} , 终端对象至多同构。

- 如果 I_1, I_2 均为 \mathcal{C} 的初始对象, 那么 $I_1 \cong I_2$, 且同构态射为 $I_1 \rightarrow I_2$ 。
- 如果 F_1, F_2 均为 \mathcal{C} 的终结对象, 那么 $F_1 \cong F_2$, 且同构态射为 $F_1 \rightarrow F_2$ 。

命题 1.5.2

范畴的终止对象为其余范畴的初始对象。

范畴的初始对象为其余范畴的终止对象。

1.5.2 万有性质**定义 1.5.4 (万有性质 universal property)**

称结构 (construction) 满足万有性质, 如果其可被视为一个范畴的终端对象。

1.5.3 商**定义 1.5.5 (商范畴 quotient category)**

令 \sim 为集合 S 上的等价关系, 定义商范畴 \mathcal{C}_{\sim}^S 如下。

- 对象: $\text{Obj}(\mathcal{C}_{\sim}^S) = \{(\varphi, T) \mid \varphi: S \rightarrow T, a \sim b \implies \varphi(a) = \varphi(b)\}$
- 态射: $(\varphi, A) \rightarrow (\psi, B)$ 为如下交换图。

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & B \\ \varphi \swarrow & & \nearrow \psi \\ & S & \end{array}$$

命题 1.5.3 (商范畴的初始对象)

对于商范畴 \mathcal{C}_{\sim}^S , $(\pi, S/\sim)$ 为其初始对象, 交换图为

$$\begin{array}{ccc} S/\sim & \xrightarrow{\exists! \sigma} & \forall T \\ \pi \swarrow & & \nearrow \forall \varphi \\ & S & \end{array}$$

1.5.4 积**命题 1.5.4 (范畴 $\mathcal{C}_{A,B}$ 的终止对象)**

对于对象 $A, B \in \mathcal{C}$, 定义范畴 $\mathcal{C}_{A,B}$ 如下。

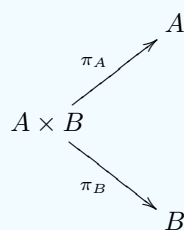
$\text{Obj} :$

$$\begin{array}{ccc} & & A \\ & \nearrow f & \\ Z & & \\ & \searrow g & \\ & & B \end{array}$$

$\text{Hom} :$

$$\begin{array}{ccccc} & & & & A \\ & & f_1 & \nearrow & \\ & & f_2 & & \\ Z_1 & \xrightarrow{\sigma} & Z_2 & & \\ & \searrow g_1 & \searrow g_2 & & \\ & & & & B \end{array}$$

那么其终止对象为



定义 1.5.6 (积 product)

称范畴 \mathcal{C} 存在积, 如果对于任意对象 $A, B \in \text{Obj}(\mathcal{C})$, 范畴 $\mathcal{C}_{A,B}$ 存在终止对象。称该终止对象为 \mathcal{C} 关于 A 和 B 的积, 记为 $A \times B$, 以及 $A \times B \rightarrow A$ 和 $A \times B \rightarrow B$ 。



例题 1.15

- 集合范畴 Set 中, $A \times B$ 表示 A 与 B 的 Descartes 积。
- 关系范畴 $\mathcal{C}_{\mathbb{R}, \leq}$ 中, $a \times b$ 表示 a 与 b 的最小值 $\min(a, b)$ 。
- 群范畴 Grp 中, $(G, *_G) \times (H, *_H)$ 表示直积 $(G \times H, *_{G \times H})$ 。
- Abel 群范畴 Ab 中, $(G, *_G) \times (H, *_H)$ 表示直积 $(G \times H, *_{G \times H})$ 。

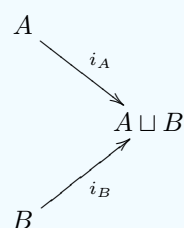
1.5.5 余积

命题 1.5.5 (范畴 $\mathcal{C}^{A,B}$ 的初始对象)

对于对象 $A, B \in \mathcal{C}$, 定义范畴 $\mathcal{C}^{A,B}$ 如下。



那么其初始对象为



定义 1.5.7 (余积 coproduct)

称范畴 \mathcal{C} 存在余积, 如果对于任意对象 $A, B \in \text{Obj}(\mathcal{C})$, 范畴 $\mathcal{C}^{A,B}$ 存在初始对象。称该初始对象为 \mathcal{C} 关于 A 和 B 的余积, 记为 $A \sqcup B$, 以及 $A \sqcup B \rightarrow A$ 和 $A \sqcup B \rightarrow B$ 。



例题 1.16

- 集合范畴 Set 中, $A \sqcup B$ 表示 A 与 B 的不交并。
- 关系范畴 $\mathcal{C}_{\mathbb{R}, \leq}$ 中, $a \sqcup b$ 表示 a 与 b 的最大值 $\max(a, b)$ 。
- 群范畴 Grp 中, $(G, *_G) \sqcup (H, *_H)$ 表示自由积 $G * H$ 。
- Abel 群范畴 Ab 中, $(G, *_G) \sqcup (H, *_H)$ 表示为直和 $G \oplus H$ 。

第二章 群论 I

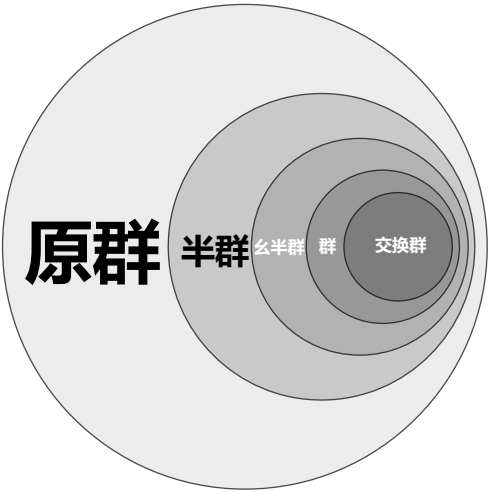


图 2.1: 群的关系

表 2.1: 群定义表

	原群	半群	么半群	群	交换群
封闭性	✓	✓	✓	✓	✓
结合律		✓	✓	✓	✓
单位元			✓	✓	✓
逆元				✓	✓
交换律					✓

2.1 群的定义

2.1.1 群和群胚

定义 2.1.1 (群胚 groupoid)

称范畴 C 为群胚，如果其中任意态射均为同构态射。



定义 2.1.2 (群 group)

群是仅有一个对象的群胚。



2.1.2 定义

定义 2.1.3 (原群 magma)

称代数系统 $(G, *)$ 为原群, 如果 $*$ 为二元运算 $*: G \times G \rightarrow G$ 。



定义 2.1.4 (半群 semigroup)

称代数系统 $(G, *)$ 为半群, 如果二元运算 $*: G \times G \rightarrow G$ 成立如下命题。

1. 结合律 (associative):

$$\forall g, h, k \in G, \quad (g * h) * k = g * (h * k)$$



定义 2.1.5 (幺半群 monoid)

称代数系统 $(G, *)$ 为幺半群, 如果二元运算 $*: G \times G \rightarrow G$ 成立如下命题。

1. 单位元 (identity element):

$$\exists e \in G, \forall g \in G, \quad e * g = g * e = g$$

2. 结合律 (associative):

$$\forall g, h, k \in G, \quad (g * h) * k = g * (h * k)$$



定义 2.1.6 (群 group)

称代数系统 $(G, *)$ 为群, 如果二元运算 $*: G \times G \rightarrow G$ 成立如下命题。

1. 单位元 (identity element):

$$\exists e \in G, \forall g \in G, \quad e * g = g * e = g$$

2. 逆元 (inverse):

$$\forall g \in G, \exists g^{-1}, \quad g * g^{-1} = g^{-1} * g = e$$

3. 结合律 (associative):

$$\forall g, h, k \in G, \quad (g * h) * k = g * (h * k)$$



定义 2.1.7 (交换群 commutative group)

称代数系统 $(G, *)$ 为交换群, 如果二元运算 $*: G \times G \rightarrow G$ 成立如下命题。

1. 单位元 (identity element):

$$\exists e \in G, \forall g \in G, \quad e * g = g * e = g$$

2. 逆元 (inverse):

$$\forall g \in G, \exists g^{-1}, \quad g * g^{-1} = g^{-1} * g = e$$

3. 结合律 (associative):

$$\forall g, h, k \in G, \quad (g * h) * k = g * (h * k)$$

4. 交换律 (commutative):

$$\forall g, h \in G, \quad g * h = h * g$$



2.1.3 基本性质

命题 2.1.1 (单位元与逆元存在且存在唯一)

- 单位元存在且存在唯一。
- 逆元存在且存在唯一。

命题 2.1.2 (运算与逆元素按可换序)

对于群 $(G, *)$, 以及 $g, h \in G$, 成立 $(g * h)^{-1} = h^{-1} * g^{-1}$ 。

证明

$$\begin{aligned}(g * h) * (h^{-1} * g^{-1}) &= g * (h * h^{-1}) * g^{-1} = g * e * g^{-1} = e \\ (h^{-1} * g^{-1}) * (g * h) &= h * (g * g^{-1}) * h^{-1} = h * e * h^{-1} = e\end{aligned}$$

2.1.4 消去律

定理 2.1.1 (消去律 cancellation)

对于群 $(G, *)$, 以及任意 $a, g, h \in G$, 成立

$$a * g = a * h \implies g = h \quad hg * a = h * a \implies g = h$$

命题 2.1.3

对于群 $(G, *)$, 以及 $g \in G$, 成立 $g * G = G$, 其中 $g * G = \{g * h : h \in G\}$ 。

证明 首先, 证明集合 $g * G$ 中没有重复元素。任取 $h_1, h_2 \in G$, 如果 $g * h_1 = g * h_2$, 那么由消去律 2.1.1, $h_1 = h_2$, 于是集合 $g * G$ 中没有重复元素。

其次, 任取 $h \in G$, 注意到

$$h = e * h = (g * g^{-1}) * h = g * (g^{-1} * h) \in g * G \implies G \subset g * G$$

而显然 $g * G \subset G$, 因此 $g * G = G$, 命题得证!

2.1.5 交换群

定义 2.1.8 (交换群 commutative group)

称群 $(G, *)$ 是可交换的, 如果对于任意 $g, h \in G$, 成立 $g * h = h * g$ 。

2.1.6 阶

定义 2.1.9 (元素的阶 order)

对于群 $(G, *)$, 定义元素 $g \in G$ 的阶为

$$|g| = \begin{cases} \min\{n \in \mathbb{N}^* : g^n = e\}, & \exists n \in \mathbb{N}^*, g^n = e \\ \infty, & \forall n \in \mathbb{N}^*, g^n \neq e \end{cases}$$

定义 2.1.10 (群的阶 order)

定义有限群 $(G, *)$ 的阶 $|G|$ 为其元素的个数, 无限群 $(G, *)$ 的阶为 $|G| = \infty$ 。

**命题 2.1.4**

如果群 $(G, *)$ 对于任意 $g \in G$, 成立 $g^2 = e$, 那么 G 为 Abel 群。



证明 由命题 2.1.2

$$g * h = g^{-1} * h^{-1} = (h * g)^{-1} = h * g$$

命题 2.1.5

对于群 $(G, *)$, 以及元素 $g \in G$, 如果 $|g| = n < \infty$, 那么

$$g^N = e \iff n \mid N$$



证明 充分性显然。

对于必要性, 如果 $g^N = e$, 且 $|g| = n$, 那么 $g^n = e$, 且 $N \geq n$ 。令 $N = mn + r$, 其中 $0 \leq r < n$, 那么 $e = g^N = g^{mn+r} = (g^n)^m * g^r = g^r$, 于是 $r = 0$, 因此 $n \mid N = mn$ 。

命题 2.1.6

对于群 $(G, *)$ 中元素 $a, g \in G$, 成立 $|a * g * a^{-1}| = |g|$ 。



证明 记 $|g| = n$, 那么 $g^n = e$, 且对于任意 $1 \leq k < n$, 成立 $g^k \neq e$ 。注意到

$$(a * g * a^{-1})^k = a * g^k * a^{-1} \begin{cases} = e, & k = n \\ \neq e, & 1 \leq k < n \end{cases}$$

因此

$$|a * g * a^{-1}| = n = |g|$$

引理 2.1.1

对于群 $(G, *)$, 以及元素 $g \in G$, 如果 $g^n = e$, 那么 $|g| \mid n$, 其中 $n \in \mathbb{Z}$ 。

**命题 2.1.7**

对于群 $(G, *)$, 如果 $|G| < \infty$, 那么对于任意 $g \in G$, 成立 $|g| < \infty$, 且对于任意 $n \in \mathbb{N}^*$, 成立

$$|g^n| = \frac{\text{lcm}(n, |g|)}{n} = \frac{|g|}{\text{gcd}(n, |g|)}$$

**命题 2.1.8**

对于群 $(G, *)$, 以及 $g, h \in G$, 如果 $g * h = h * g$, 那么 $|g * h| \mid \text{lcm}(|g|, |h|)$ 。



证明 记 $|g| = m, |h| = n$, 且 $\text{gcd}(|g|, |h|) = r$, 那么 $r \mid m, n$, 且 $\text{lcm}(|g|, |h|) = mn/r$, 进而

$$(g * h)^{\text{lcm}(|g|, |h|)} = (g * h)^{mn/r} = g^{mn/r} * h^{nm/r} = e^{n/r} * e^{m/r} = e$$

由引理 2.1.1, 可得 $|g * h| \mid \text{lcm}(|g|, |h|)$ 。

命题 2.1.9

对于群 $(G, *)$, 以及 $g, h \in G$, 如果 $g * h = h * g$, 且 $\text{gcd}(|g|, |h|) = 1$, 那么 $|g * h| = |g||h|$ 。



证明 记 $|g| = m, |h| = n, |g * h| = r$, 由引理 2.1.1

$$(g * h)^{mn} = g^{mn} * h^{mn} = e \implies r \mid mn$$

$$g^{nr} = g^{nr} * h^{nr} = (g * h)^{nr} = e \implies m \mid nr$$

$$h^{mr} = g^{mr} * h^{mr} = (g * h)^{mr} = e \implies n \mid mr$$

又因为 $\gcd(m, n) = \gcd(|g|, |h|) = 1$, 于是 $m \mid r$ 且 $n \mid r$, 因此 $mn \mid r$, 进而 $mn = r$, 即 $|g * h| = |g||h|$ 。

命题 2.1.10

对于 n 阶群 $(G, *)$, 令 m 为 G 中 2 阶元素的个数, 证明: $n - m$ 为奇数。

证明 1 阶元素仅为 e , 3 阶及以上元素成对出现, 因此 $n - m$ 为非 2 阶元素的个数, 显然为奇数。

命题 2.1.11

如果有有限群 $(G, *)$ 存在且存在唯一 2 阶元素 $h \in G$, 那么

$$\prod_{g \in G} g = h$$

证明 任取 $g \in G$, 考虑 g 和 g^{-1} 的关系, 如果 $g = g^{-1}$, 那么 $g^2 = e$, 因此 $g = e$ 或 $g = h$, 因此

$$\prod_{g \in G} g = h * \prod_{g \in G \setminus \{e, h\}} (g * g^{-1}) = h$$

命题 2.1.12

对于交换群 $(G, *)$, $g \in G$ 为极大有限阶元素, 即对于任意有限阶元素 $h \in G$, 成立 $|h| \leq |g|$, 那么对于有限阶元素 $h \in G$, 成立 $|h| \mid |g|$ 。

证明 记 $|g| = N, |h| = n$ 。反证, 如果 $n \nmid N$, 那么存在素数 p , 使得成立 $N = p^i r, n = p^j s$, 其中 $i < j$ 且 $\gcd(p, r) = \gcd(p, s) = 1$ 。考察 $g^{p^i} * h^s$, 注意到 $\gcd(|g^{p^i}|, |h^s|) = \gcd(r, p^j) = 1$, 因此由命题 2.1.9

$$|g^{p^i} * h^s| = |g^{p^i}| |h^s| = p^j r > p^i r = N$$

矛盾! 于是 $n \mid N$ 。

2.1.7 有限群结构

表 2.2: 有限群结构

阶数	Abel 群	非 Abel 群
1	$\{e\}$	
6	\mathbb{Z}_6	D_3
8	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_4, Q_8
12	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6$	$D_6, A_4, \mathbb{Z}_3 \rtimes \mathbb{Z}_4$
$p : p$ 为素数	\mathbb{Z}_p	
$2p : p$ 为奇素数	\mathbb{Z}_{2p}	D_p
$p^2 : p$ 为素数	$\mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p$	
$pq : p, q$ 为素数且 $p > q, q \nmid p - 1$	\mathbb{Z}_{pq}	
$pq : p, q$ 为素数且 $p \neq q$	\mathbb{Z}_{pq}	$\mathbb{Z}_p \rtimes \mathbb{Z}_q$

2.2 群的例子

2.2.1 对称群

定义 2.2.1 (对称群 symmetric group / 置换群 permutation group)

对于集合 A , 定义由 A 诱导的对称群/置换群为

$$S_A = \text{Aut}_{\text{Set}}(A) = \{f : A \rightarrow A\}$$

特别的, 当 $A = \{1, \dots, n\}$ 时, 由 A 诱导的对称群/置换群记为 S_n .



例题 2.1 对于任意 $1 \leq d \leq n$, 存在 d 阶元 $\sigma \in S_n$.

$$\sigma = \begin{pmatrix} 1 & \cdots & d-1 & d & d+1 & \cdots & n \\ 2 & \cdots & d & 1 & d+1 & \cdots & n \end{pmatrix}$$

例题 2.2 对于任意 $n \in \mathbb{N}^*$, 存在 n 阶元 $\sigma \in S_{\mathbb{N}^*}$.

$$\sigma = \begin{pmatrix} 1 & \cdots & n-1 & n & n+1 & \cdots \\ 2 & \cdots & n & 1 & n+1 & \cdots \end{pmatrix}$$

命题 2.2.1

对于对称群 S_n , 以及置换 $\sigma \in S_n$, 定义 M_σ 如下

$$M_\sigma(i, j) = \begin{cases} 1, & (i, j) = (i, \sigma(i)) \\ 0, & \text{其他} \end{cases}$$

那么对于任意 $\sigma, \tau \in S_n$, 成立 $M_{\sigma\tau} = M_\sigma \circ M_\tau$.



证明 记 $M_{\sigma\tau} = (a_{ij}), M_\sigma = (b_{ik}), M_\tau = (c_{kj})$, 只需证明

$$a_{ij} = \sum_{k=1}^n b_{ik} c_{kj}, \quad \forall 1 \leq i, j \leq n$$

任取 $1 \leq i \leq n$, 注意到

$$a_{ij} = \begin{cases} 1, & j = \tau \circ \sigma(i) \\ 0, & j \neq \tau \circ \sigma(i) \end{cases}, \quad b_{ik} = \begin{cases} 1, & k = \sigma(i) \\ 0, & k \neq \sigma(i) \end{cases}, \quad c_{kj} = \begin{cases} 1, & k = \tau^{-1}(j) \\ 0, & k \neq \tau^{-1}(j) \end{cases}$$

因此

$$b_{ik} c_{kj} = \begin{cases} 1, & k = \sigma(i) = \tau^{-1}(j) \\ 0, & \text{其他} \end{cases}$$

于是 $M_{\sigma\tau} = M_\sigma \circ M_\tau$.

命题 2.2.2 (对称群的中心)

$$\text{Cent}(S_n) = S_n, \quad n = 1, 2$$

$$\text{Cent}(S_n) = \{1\}, \quad n \geq 3$$



2.2.2 二面体群

定义 2.2.2 (二面体群 dihedral group)

对于正 n 边形, 令 σ 表示绕中心旋转 $\frac{2\pi}{n}$, τ 表示关于某条对称轴的反射, 那么正 n 边形的对称群为

$$D_n = \{\sigma^i \circ \tau^j : \sigma^n = \tau^2 = \sigma \circ \tau \circ \sigma \circ \tau = \mathbb{1}, 0 \leq i < n, j \in \{0, 1\}\}$$



命题 2.2.3 (二面体群的性质)

- 非 Abel 群

-

$$\tau^{-1} = \tau, \quad \sigma^i \circ \tau = \tau \circ \sigma^{-i}$$

-

$$|\sigma^i \circ \tau^j| = 2 \iff i = 0 \text{ 或 } i = \frac{n}{2} \text{ 或 } j = 1$$

- 换位子群:

$$[D_{2n-1}, D_{2n-1}] = \{\sigma^i : 0 \leq i \leq 2n-2\} \cong \mathbb{Z}/(2n-1)\mathbb{Z}$$

$$[D_{2n}, D_{2n}] = \{\sigma^{2i} : 0 \leq i \leq n-1\} \cong \mathbb{Z}/n\mathbb{Z}$$

- 中心:

$$\text{Cent}(D_{2n-1}) = \{\mathbb{1}\}, \quad \text{Cent}(D_{2n}) = \{\mathbb{1}, \sigma^n\}$$



2.2.3 循环群

定义 2.2.3 (循环群 cyclic group)

称群 $(G, *)$ 为 n 阶循环群, 如果 $G \cong C_n = \mathbb{Z}/n\mathbb{Z}$.

定义 2.2.4 (模 n 群 group of modulo n)

$$\mathbb{Z}/n\mathbb{Z} = \{[k]_n : 0 \leq k < n\}$$



命题 2.2.4 (循环群的性质)

- Abel 群
- 子群: $\mathbb{Z}/p\mathbb{Z}$, 其中 $p \mid n$.
- 正规子群: $\mathbb{Z}/p\mathbb{Z}$, 其中 $p \mid n$.
- 换位子群: $\mathbb{Z}/1\mathbb{Z}$



例题 2.3 求 $1238237^{18238456}$ 的个位数字。

证明

$$1238237^{18238456} \equiv 7^{18238456} \equiv (7^4)^{4559614} \equiv 2401^{4559614} \equiv 1 \pmod{10}$$

因此 $1238237^{18238456}$ 的个位数字为 1。

例题 2.4 证明: 方程 $x^3 = 9$ 在群 $\mathbb{Z}/31\mathbb{Z}$ 中不存在根。

证明 如果 c 为方程 $x^3 = 9$ 在群 $\mathbb{Z}/31\mathbb{Z}$ 中的根, 那么由命题 2.1.7

$$\frac{|[c]_{31}|}{\gcd(3, |[c]_{31}|)} = |[c^3]_{31}| = |[9]_{31}| = 15$$

如果 $\gcd(3, |[c]_{31}|) = 1$, 那么 $|[c]_{31}| = 15$, 矛盾!

如果 $\gcd(3, |[c]_{31}|) = 3$, 那么 $|[c]_{31}| = 45 > 30$, 矛盾!

因此方程 $x^3 = 9$ 在群 $\mathbb{Z}/31\mathbb{Z}$ 中不存在根。

例题 2.5 证明: 不定方程 $a^2 + b^2 = 3c^2$ 不存在整数解。

证明 在 $\mathbb{Z}/4\mathbb{Z}$ 中考虑不定方程

$$a^2 + b^2 = 3c^2 \implies [a]_4^2 + [b]_4^2 = 3[c]_4^2$$

注意到 $[0]_4^2 = [2]_4^2$ 且 $[1]_4^2 = [3]_4^2$, 因此 $[a]_4^2 = [b]_4^2 = [c]_4^2 = [0]_4^2$, 因此 $2 \mid a, b, c$, 于是存在 a_1, b_1, c_1 , 使得成立 $a = 2a_1, b = 2b_1, c = 2c_1$, 代入方程

$$a_1^2 + b_1^2 = 3c_1^2 \implies [a_1]_4^2 + [b_1]_4^2 = 3[c_1]_4^2$$

归纳可得, $a = b = c = 0$, 因此不定方程 $a^2 + b^2 = 3c^2$ 不存在整数解。

命题 2.2.5

对于循环群 $(\mathbb{Z}/n\mathbb{Z}, +)$, 成立

$$|[m]_n| = \frac{n}{\gcd(m, n)}$$

推论 2.2.1

等价类 $[m]_n$ 生成循环群 $\mathbb{Z}/n\mathbb{Z}$, 当且仅当 $\gcd(m, n) = 1$ 。

定义 2.2.5 (模 n 单位群 group of units modulo n)

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[p]_n : \gcd(p, n) = 1\}$$

命题 2.2.6 (模 n 单位群的性质)

- Abel 群
- 换位子群: $\mathbb{Z}/1\mathbb{Z}$

例题 2.6 在群 $(\mathbb{Z}/31\mathbb{Z})^\times$ 中, 计算 $[9]_{31}$ 的阶。

证明 由于

$$(\mathbb{Z}/31\mathbb{Z})^\times = \{[n]_{31} : 1 \leq n \leq 30\}$$

那么

$$\begin{aligned} [9^1]_{31} &= [9]_{31}, & [9^2]_{31} &= [19]_{31}, & [9^3]_{31} &= [16]_{31}, & [9^4]_{31} &= [20]_{31}, & [9^5]_{31} &= [25]_{31} \\ [9^6]_{31} &= [8]_{31}, & [9^7]_{31} &= [10]_{31}, & [9^8]_{31} &= [28]_{31}, & [9^9]_{31} &= [4]_{31}, & [9^{10}]_{31} &= [5]_{31} \\ [9^{11}]_{31} &= [14]_{31}, & [9^{12}]_{31} &= [2]_{31}, & [9^{13}]_{31} &= [18]_{31}, & [9^{14}]_{31} &= [7]_{31}, & [9^{15}]_{31} &= [9]_{31} \end{aligned}$$

因此 $|[9]_{31}| = 15$ 。

定理 2.2.1 (互素的等价条件)

$$\gcd(m, n) = 1 \iff \exists a, b \in \mathbb{Z}, \quad am + bn = 1$$

证明

$$\gcd(m, n) = 1 \iff a[m]_n = [1]_n \iff [am]_n = [1]_n \iff am + bn = 1$$

命题 2.2.7

如果 $m \equiv n \pmod{p}$, 那么

$$\gcd(m, p) = 1 \iff \gcd(n, p) = 1$$



证明 由于 $m \equiv n \pmod{p}$, 那么存在 $r \in \mathbb{Z}$, 使得成立 $m = pr + n$ 。由

$$\gcd(m, p) = 1 \iff \exists a, b \quad am + bp = 1 \iff \exists a, b \quad an + (ar + b)p = 1 \iff \gcd(n, p) = 1$$

命题 2.2.8

1. 对于正奇数 n , 成立

$$\gcd(m, n) = 1 \implies \gcd(2m + n, 2n) = 1$$

2. 对于正奇数 n , 成立

$$\gcd(m, 2n) = 1 \implies \gcd\left(\frac{m-n}{2}, n\right) = 1$$

3. 对于正奇数 n , 如下函数为双射。

$$\begin{aligned} \varphi : (\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/2n\mathbb{Z})^\times \\ [m]_n &\longmapsto [2m + n]_{2n} \end{aligned}$$



证明 对于 1, 由于 n 为奇数, 那么 $\gcd(2m + n, 2n) = \gcd(2m + n, n)$ 。由定理 2.2.1

$$\gcd(m, n) = 1 \iff am + b(2k - 1) = 1 \iff \frac{a}{2}(2m + n) + (b - \frac{a}{2})n = 1$$

如果 a 为偶数, 那么 $\gcd(2m + n, n) = 1$; 如果 a 为奇数, 那么令 $a' = a + n, b' = b - m$, 于是

$$\frac{a'}{2}(2m + n) + (b' - \frac{a'}{2})n = 1$$

因此 $\gcd(2m + n, n) = 1$, 进而 $\gcd(2m + n, 2n) = 1$ 。

对于 2, 如果 $\gcd(m, 2n) = 1$, 那么 $\gcd(m, n) = 1$ 。由定理 2.2.1

$$\gcd(m, n) = 1 \iff am + bn = 1 \iff 2a\left(\frac{m-n}{2}\right) + (a+b)n = 1 \iff \gcd\left(\frac{m-n}{2}, n\right) = 1$$

对于 3, 首先, 对于单射性, 任取 $a, b \in \mathbb{Z}$, 如果 $[2a + n]_{2n} = [2b + n]_{2n}$, 那么 $[2a]_{2n} = [2b]_{2n}$, 于是 $[a]_n = [b]_n$, 于是 φ 为单射。

其次, 对于满射性, 任取 $m \in \mathbb{Z}$, 满足 $[m]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^\times$, 于是 $\gcd(m, 2n) = 1$, 由 2, $\gcd(\frac{m-n}{2}, n) = 1$, 因此 $[\frac{m-n}{2}]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$, 且 $\varphi([\frac{m-n}{2}]_n) = [m]_{2n}$ 。

2.2.4 矩阵群

定义 2.2.6 (矩阵群 matrix group)

$$\mathrm{GL}_n(\mathbb{R}) = \{\mathbb{R}\text{上的 } n \times n \text{ 可逆矩阵}\}$$

$$\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : \det(M) = 1\}$$

$$\mathrm{Orb}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : MM^t = M^t M = I_n\}$$

$$\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : \det(M) = 1, MM^t = M^t M = I_n\}$$

$$\mathrm{GL}_n(\mathbb{C}) = \{\mathbb{C}\text{上的 } n \times n \text{ 可逆矩阵}\}$$

$$\mathrm{SL}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : \det(M) = 1\}$$

$$\mathrm{U}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : MM^\dagger = M^\dagger M = I_n\}$$

$$\mathrm{SU}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : \det(M) = 1, MM^\dagger = M^\dagger M = I_n\}$$

**2.2.5 初等数论****定义 2.2.7 (Euler 函数)**

$\phi(n)$ = 小于 n 且与 n 互素的正整数的个数

**命题 2.2.9 (Euler 函数的性质)**

- 解析表达式:

$$\phi(N) = \phi(p_1^{r_1} \cdots p_n^{r_n}) = \prod_{k=1}^n p_k^{r_k-1} (p_k - 1) = N \prod_{\text{素数 } p|N} \left(1 - \frac{1}{p}\right)$$

- 如果 p 为素数, 那么 $\phi(p^n) = p^{n-1}(p-1)$; 特别的, $\phi(p) = p-1$ 。
- 如果 $\gcd(m, n) = 1$, 那么 $\phi(mn) = \phi(m)\phi(n)$ 。
- 对于 $n \in \mathbb{N}^*$ 且 $n > 1$, 成立

$$\sum_{\substack{\gcd(m,n)=1 \\ 1 \leq m \leq n}} m = \frac{n}{2} \phi(n), \quad \sum_{p|n} \phi(p) = n$$

**定义 2.2.8 (模 n 单位群 group of units modulo n)**

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[p]_n : \gcd(p, n) = 1\}$$

**命题 2.2.10 $(\mathbb{Z}/n\mathbb{Z})^*$ 的性质**

-

$$|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$$

-

$$p \text{ 为素数} \iff (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

-

$$(\mathbb{Z}/n\mathbb{Z})^* \text{ 为循环群} \iff n = 1, 2, 4, p^r, 2p^r, \text{ 其中 } p \text{ 为奇素数}$$



定理 2.2.2 (Fermat 小定理)

对于素数 p , 如果 $\gcd(a, p) = 1$, 那么

$$a^{p-1} \equiv 1 \pmod{p}$$

**定理 2.2.3 (Euler 定理)**

如果 $\gcd(a, n) = 1$, 那么

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

**定理 2.2.4 (Wilson 定理)**

$$p \text{ 为素数} \iff (p-1)! \equiv -1 \pmod{p}$$



证明 对于充分性, 如果 $(p-1)! \equiv -1 \pmod{p}$, 且 p 为合数。显然 $p \neq 4$, 当 $p \geq 5$ 时, 存在 $1 \leq a < b \leq p-1$, 使得成立 $ab = p$, 于是 $(p-1)! \equiv 0 \pmod{p}$, 矛盾! 因此 p 为素数。

对于必要性, 如果 p 为素数。 $p = 2$ 时显然成立, 因此考虑 p 为奇素数。由原根存在定理, 令 a 为模 p 的原根。由 Fermat 小定理 2.2.2, $a^{p-1} \equiv 1 \pmod{p}$, 因此 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, 进而

$$(p-1)! \equiv \prod_{k=1}^{p-1} a^k \equiv (a^{\frac{p-1}{2}})^p \equiv (-1)^p \equiv -1 \pmod{p}$$

定义 2.2.9 (指数 index)

对于 $a, n \in \mathbb{N}^*$, 如果 $\gcd(a, n) = 1$, 那么定义 a 关于模 n 的指数

$$\delta_n(a) = \min\{r \in \mathbb{N}^* : a^r \equiv 1 \pmod{n}\}$$

**定义 2.2.10 (原根 primitive root)**

对于 $a, n \in \mathbb{N}^*$, 如果 $\gcd(a, n) = 1$, 那么称 a 为模 n 的原根, 如果 $\delta_n(a) = \phi(n)$, 即对于任意 $1 \leq r < \phi(n)$, 成立 $a^r \not\equiv 1 \pmod{n}$ 。

**命题 2.2.11 (原根的性质)**

- 如果 $\gcd(a, n) = 1$, 且 $a^r \equiv 1 \pmod{n}$, 那么 $\delta_n(a) \mid r$ 。
- 如果 p 为素数, 那么模 p 存在原根。
- 如果 p 为奇素数, 那么对于任意 $n \in \mathbb{N}^*$, 模 p^n 存在原根。
- 如果 a 为模 n 的原根, 那么 a^r 为模 n 的原根, 当且仅当 $\gcd(r, \phi(n)) = 1$ 。

**定理 2.2.5 (原根存在的等价条件)**

$$\text{模 } n \text{ 存在原根} \iff n = 1, 2, 4, p^r, 2p^r, \text{ 其中 } p \text{ 为奇素数}$$

**定理 2.2.6 (a 为模 n 的原根的等价条件)**

- 对于任意 $1 \leq r < \phi(n)$, 成立 $a^r \not\equiv 1 \pmod{n}$ 。
- 对于任意与 n 互素的 m , 存在 r , 使得成立 $a^r \equiv m \pmod{n}$ 。
- $[a]_n$ 是模 n 单位群 $(\mathbb{Z}/n\mathbb{Z})^\times$ 的生成元。



定理 2.2.7 (原根存在性定理)

- 如果模 n 存在原根, 那么存在 $\phi(\phi(n))$ 个原根。
- 如果 p 为素数, 那么模 p 存在原根, 且存在 $\phi(p-1)$ 个原根。

**表 2.3:** 原根列表

n	原根	$\phi(n)$	n	原根	$\phi(n)$
1	1	1	11	2, 6, 7, 8	10
2	1	1	12		4
3	2	2	13	2, 6, 7, 11	12
4	3	2	14	3, 5	6
5	2, 3	4	15		8
6	5	2	16		8
7	3, 5	6	17	3, 5, 6, 7, 10, 11, 12, 14	16
8		4	18	5, 11	6
9	2, 5	6	19	2, 3, 10, 13, 14, 15	18
10	3, 7	4	20		8

2.3 Grp 范畴

2.3.1 群同态映射

定义 2.3.1 (群同态映射 group homomorphism)

对于群 $(G, *_G)$ 和 $(H, *_H)$, 定义群同态映射为 $\varphi: (G, *_G) \rightarrow (H, *_H)$, 其中 $\varphi(g *_G h) = \varphi(g) *_H \varphi(h)$, 交换图为

$$\begin{array}{ccc}
 G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\
 \downarrow *_G & & \downarrow *_H \\
 G & \xrightarrow{\varphi} & H
 \end{array}$$



2.3.2 Grp 的定义

定义 2.3.2 (Grp 范畴)

$$\text{Obj}(\text{Grp}) = \{\text{群}(G, *)\}$$

$$\text{Hom}_{\text{Grp}}((G, *_G), (H, *_H)) = \{\varphi: (G, *_G) \rightarrow (H, *_H) \mid \varphi(g *_G h) = \varphi(g) *_H \varphi(h)\}$$



2.3.3 小小反思

命题 2.3.1 (群同态映射保单位元与逆)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$\varphi(e_G) = e_H, \quad \varphi(g^{-1}) = \varphi(g)^{-1}$$



2.3.4 积

命题 2.3.2 (Grp 范畴的终端对象)

对于 Grp 范畴, 平凡群即为初始对象, 亦为终止对象。



定义 2.3.3 (直积 direct product)

对于群 $(G, *_G)$ 和 $(H, *_H)$, 定义其直积为群 $(G \times H, *_G \times *_H)$, 其中

$$(g_1, h_1) *_G \times *_H (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$



定义 2.3.4 (Grp 的积)

群 $(G, *_G)$ 与 $(H, *_H)$ 的积 $(G, *_G) \times (H, *_H)$ 为直积 $(G \times H, *_G \times *_H)$ 。



定义 2.3.5 (Grp 的余积)

群 $(G, *_G)$ 与 $(H, *_H)$ 的余积 $(G, *_G) \sqcup (H, *_H)$ 记作 $G * H$, 称为自由积。



2.3.5 Abel 群

定义 2.3.6 (Ab 范畴)

$$\text{Obj}(\text{Grp}) = \{\text{Abel 群}(G, *_G)\}$$

$$\text{Hom}_{\text{Grp}}((G, *_G), (H, *_H)) = \{\varphi: (G, *_G) \rightarrow (H, *_H) \mid \varphi(g *_G h) = \varphi(g) *_H \varphi(h)\}$$



定义 2.3.7 (直和 direct sum)

对于 Abel 群 $(G, *_G)$ 和 $(H, *_H)$, 定义其直和 $G \oplus H$ 为直积 $(G \times H, *_G \times *_H)$ 。



定义 2.3.8 (Ab 的积)

Abel 群 $(G, *_G)$ 与 $(H, *_H)$ 的积 $(G, *_G) \times (H, *_H)$ 为直积 $(G \times H, *_G \times *_H)$ 。



定义 2.3.9 (Ab 的余积)

Abel 群 $(G, *_G)$ 与 $(H, *_H)$ 的余积 $(G, *_G) \sqcup (H, *_H)$ 为直和 $G \oplus H$ 。



命题 2.3.3 (Ab 范畴中积、余积、直积与直和的关系)

$$\text{积} = \text{余积} = \text{直积} = \text{直和}$$



2.4 群同态映射

2.4.1 例子

例题 2.7 对于 $m \mid n$, 定义

$$\begin{aligned}\pi_m^n : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \\ [k]_n &\mapsto [k]_m\end{aligned}$$

交换图为

$$\begin{array}{ccc}\mathbb{Z} & & \\ \pi_n \downarrow & \searrow \pi_m & \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\pi_m^n} & \mathbb{Z}/m\mathbb{Z}\end{array}$$

2.4.2 同态映射与阶

命题 2.4.1

对于群同态映射 $\varphi : G \rightarrow H$, 以及任意元素 $g \in G$, 如果 $|g| < \infty$, 那么 $|\varphi(g)| \mid |g|$ 。

2.4.3 群同构映射

定义 2.4.1 (群同构映射 group isomorphism)

称群同态映射 $\varphi : G \rightarrow H$ 为群同构映射, 如果存在群同态映射 $\psi : H \rightarrow G$, 使得成立

$$\psi \circ \varphi = \mathbb{1}_G, \quad \varphi \circ \psi = \mathbb{1}_H$$

定义 2.4.2 (群同构的 group isomorphic)

称群 G 和 H 是同构的, 且记作 $G \cong H$, 如果存在群同构映射 $\varphi : G \rightarrow H$ 。

例题 2.8 证明:

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$$

证明 构造映射

$$\begin{aligned}\varphi : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto e^x\end{aligned}$$

首先, 证明 φ 为群同态映射。任取 $x, y \in \mathbb{R}$, 注意到

$$\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$$

因此 φ 为群同态映射。

其次, 证明 φ 为双射。构造映射

$$\begin{aligned}\psi : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto \ln x\end{aligned}$$

注意到

$$\psi \circ \varphi = \varphi \circ \psi = \mathbb{1}$$

于是 φ 为双射。

综上所述, 由定理2.4.1, φ 为群同构态射, 因此

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$$

例题 2.9 证明:

$$C_4 \not\cong C_2 \times C_2$$

证明 考察 C_4 和 $C_2 \times C_2$ 非零元的阶。对于 C_4

$$|[2]_4| = 2, \quad |[1]_4| = |[3]_4| = 4$$

对于 $C_2 \times C_2$

$$|([1]_2, [0]_2)| = |([0]_2, [1]_2)| = |([1]_2, [1]_2)| = 2$$

由群同构映射的保阶性2.4.2, 所以不存在同构态射 $C_4 \rightarrow C_2 \times C_2$, 进而

$$C_4 \not\cong C_2 \times C_2$$

例题 2.10 证明:

$$(\mathbb{R} \setminus \{0\}, \times) \not\cong (\mathbb{C} \setminus \{0\}, \times)$$

证明 如果 $(\mathbb{R} \setminus \{0\}, \times) \cong (\mathbb{C} \setminus \{0\}, \times)$, 那么存在群同构态射 $\varphi: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{C} \setminus \{0\}$, 即 φ 为双射。

注意到存在 $x \in \mathbb{R}$, 使得 $\varphi(x) = i$, 那么

$$\varphi(x^4) = (\varphi(x))^4 = i^4 = 1$$

由命题2.3.1, φ 保持单位元, 那么

$$\varphi(1) = 1 = \varphi(x^4)$$

于是 $x^4 = 1$, 因此 $x^2 = 1$, 进而

$$1 = \varphi(1) = \varphi(x^2) = (\varphi(x))^2 = i^2 = -1$$

矛盾! 因此

$$(\mathbb{R} \setminus \{0\}, \times) \not\cong (\mathbb{C} \setminus \{0\}, \times)$$

定理 2.4.1 (群同构映射的等价条件)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$\varphi \text{ 为群同构映射} \iff \varphi \text{ 为双射}$$



证明 对于必要性, 如果 $\varphi: G \rightarrow H$ 为群同构映射, 那么存在群同态映射 $\psi: H \rightarrow G$, 使得成立

$$\psi \circ \varphi = \mathbb{1}_G, \quad \varphi \circ \psi = \mathbb{1}_H$$

从集合函数的意义上, φ 存在左右逆, 由命题1.2.8, 那么 φ 为双射, 必要性得证!

对于充分性, 如果 $\varphi: G \rightarrow H$ 为双射, 那么定义映射

$$\psi: H \longrightarrow G$$

$$\varphi(g) \longmapsto g$$

此时成立

$$\psi \circ \varphi = \mathbb{1}_G, \quad \varphi \circ \psi = \mathbb{1}_H$$

考察映射 ψ , 注意到

$$\psi(\varphi(g) * \varphi(h)) = \psi(\varphi(g * h)) = g * h = \psi(\varphi(g)) * \psi(\varphi(h))$$

因此 ψ 为群同态映射, 进而 $\varphi: G \rightarrow H$ 为群同构映射, 充分性得证!

命题 2.4.2 (群同构映射的保阶性)

对于群同构映射 $\varphi: G \rightarrow H$, 以及任意 $g \in G$, 成立 $|\varphi(g)| = |g|$ 。



证明 记 $|g| = n$, 注意到

$$\varphi(g)^k = \varphi(g^k) \begin{cases} \neq e, & 1 \leq k < n \\ = e, & k = n \end{cases}$$

因此 $|\varphi(g)| = n$ 。

命题 2.4.3

对于 n 阶群 $(G, *)$, 成立

$$G \cong \mathbb{Z}/n\mathbb{Z} \iff \exists g \in G, |g| = n$$

。



证明 对于必要性, 如果 $G \cong \mathbb{Z}/n\mathbb{Z}$, 那么存在群同构映射 $\varphi: \mathbb{Z}/n\mathbb{Z} \rightarrow G$, 由命题 2.4.2

$$|\varphi([1]_n)| = |[1]_n| = n$$

对于充分性, 如果存在 $g \in G$, 使得成立 $|g| = n$, 又因为 $|G| = n$, 那么 G 为由 g 生成的 n 阶循环群, 于是 $G \cong \mathbb{Z}/n\mathbb{Z}$ 。

命题 2.4.4 (群同构映射的保交换性与保循环性)

对于群 G 和 H , 如果 $G \cong H$, 那么

$$G \text{ 为 Abel 群} \iff H \text{ 为 Abel 群}$$

$$G \text{ 为循环群} \iff H \text{ 为循环群}$$

**命题 2.4.5 (循环群间的同构映射由生成元唯一确定)**

对于循环群 G 和 H , 如果 $G \cong H$, 那么取生成元 $g \in G$, 如下映射为双射。

$$\Psi: \{h \in H : \langle h \rangle = H\} \longrightarrow \{\text{群同构映射 } \varphi: G \rightarrow H\}$$

$$h \longmapsto \varphi_h, \text{ 其中 } \varphi_h(g) = h$$

**命题 2.4.6**

对于群 $(G, *)$, 成立

$$\varphi: g \mapsto g^{-1} \text{ 为群同态映射} \iff \psi: g \mapsto g^2 \text{ 为群同态映射} \iff G \text{ 为 Abel 群}$$



证明 如果 G 为 Abel 群。任取 $g, h \in G$, 由于

$$\varphi(g * h) = (g * h)^{-1} = h^{-1} * g^{-1} = g^{-1} * h^{-1} = \varphi(g) * \varphi(h)$$

$$\psi(g * h) = (g * h)^2 = g^2 * h^2 = \psi(g) * \psi(h)$$

于是 φ 和 ψ 为同态映射。

如果 φ 为同态映射。任取 $g, h \in G$, 由于

$$g * h = (h^{-1} * g^{-1})^{-1} = \varphi(h^{-1} * g^{-1}) = \varphi(h^{-1}) * \varphi(g^{-1}) = h * g$$

因此 G 为 Abel 群。

如果 ψ 为同态映射。任取 $g, h \in G$, 由于

$$(g * h)^2 = \psi(g * h) = \psi(g) * \psi(h) = g^2 * h^2 \implies h * g = g * h$$

因此 G 为 Abel 群。

定理 2.4.2 (素数群的单位群)

对于素数 p , 成立

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$$



证明 $p=2$ 时结论显然, 当 p 为奇素数时

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{[n]_p : \gcd(n, p) = 1\} = \{[n]_p : 1 \leq n < p\}$$

取 a 为模 p 的原根, 构造映射

$$\begin{aligned} \varphi : \mathbb{Z}/(p-1)\mathbb{Z} &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \\ [n]_{p-1} &\longmapsto [a^n]_p \end{aligned}$$

首先, 证明 φ 的定义良好性。一方面, 任取 $[n]_{p-1}$, 由于 $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$, 那么 $\gcd(a, p) = 1$, 于是 $\gcd(a^n, p) = 1$, 于是 $[a^n]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ 。另一方面, 任取 $[m]_{p-1} = [n]_{p-1}$, 那么由 Fermat 小定理 2.2.2, $[a^m]_p = [a^n]_p$ 。于是 φ 定义良好。

其次, 证明 φ 为同构态射。任取 $[m]_{p-1}, [n]_{p-1} \in \mathbb{Z}/(p-1)\mathbb{Z}$, 注意到

$$\varphi([m]_{p-1} + [n]_{p-1}) = \varphi([m+n]_{p-1}) = [a^{m+n}]_p = [a^m]_p [a^n]_p = \varphi([m]_{p-1}) \varphi([n]_{p-1})$$

最后, 证明 φ 为双射。任取 $[m]_{p-1}, [n]_{p-1} \in \mathbb{Z}/(p-1)\mathbb{Z}$, 不妨 $m \geq n$, 注意到

$$\begin{aligned} \varphi([m]_{p-1}) &= \varphi([n]_{p-1}) \\ \implies [a^m]_p &= [a^n]_p \\ \implies a^{m-n} &\equiv 1 \pmod{p} \\ \implies \phi(p) &\mid m-n \\ \implies m &\equiv n \pmod{p-1} \\ \implies [m]_{p-1} &= [n]_{p-1} \end{aligned}$$

任取 $[m]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$, 由于 a 为模 p 的原根, 所以存在 $n \in \mathbb{N}^*$, 使得成立 $a^n \equiv m \pmod{p}$, 于是 $\varphi([n]_{p-1}) = [a^n]_p = [m]_p$ 。因此 φ 为双射。

综上所述, 对于素数 p , 成立

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

定理 2.4.3

对于 $p, q \in \mathbb{N}^*$, 如果 $\gcd(p, q) = 1$, 那么

$$\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$



证明 构造映射

$$\begin{aligned} \varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} &\longrightarrow \mathbb{Z}/pq\mathbb{Z} \\ ([a]_p, [b]_q) &\longmapsto [anq + bmq]_{pq} \end{aligned}$$

其中 $[mp]_q = [1]_q$ 且 $[nq]_p = [1]_p$, $\gcd(p, q) = 1$ 保证了 m, n 的存在性。事实上, 由定理 2.2.1, 存在 m, n , 使得成立 $mp + nq = 1$, 于是 $[mp]_q = [1]_q$ 且 $[nq]_p = [1]_p$ 。

首先, 证明 φ 的定义良好性。任取 a, b, c, d , 满足 $[a]_p = [c]_p$ 且 $[b]_q = [d]_q$, 那么

$$\varphi([a]_p, [b]_q) = [anq + bmq]_{pq} = [bnq + dmq]_{pq} = \varphi([c]_p, [d]_q)$$

其次, 证明 φ 为群同态映射。任取 a, b, c, d , 注意到

$$\begin{aligned} & \varphi([a]_p, [b]_q) + ([c]_p, [d]_q) \\ &= \varphi([a+c]_p, [b+d]_q) \\ &= [(a+c)nq + (b+d)mp]_{pq} \\ &= [anq + bmp]_{pq} + [cnq + dmp]_{pq} \\ &= \varphi([a]_p, [b]_q) + \varphi([c]_p, [d]_q) \end{aligned}$$

最后, 证明 φ 为双射。任取 a, b, c, d , 注意到

$$\begin{aligned} & \varphi([a]_p, [b]_q) = \varphi([c]_p, [d]_q) \\ \implies & [anq + bmp]_{pq} = [cnq + dmp]_{pq} \\ \implies & [(a-c)nq + (b-d)mp]_{pq} = 0 \\ \implies & [(a-c)nq + (b-d)mp]_p = 0, \\ & [(a-c)nq + (b-d)mp]_q = 0 \\ \implies & [(a-c)nq]_p = 0, \\ & [(b-d)mp]_q = 0 \\ \implies & [a]_p = [c]_p, \quad [b]_q = [d]_q \end{aligned}$$

于是 φ 为单射。又 $|\mathbb{Z}/pq\mathbb{Z}| = |C_p \times C_q| = pq$, 那么 φ 为双射。

综上所述, 得到如下结论, 原命题得证!

$$\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

命题 2.4.7

对于奇素数 $p \neq q$, $(\mathbb{Z}/pq\mathbb{Z})^\times$ 不是循环群。

证明 令 $n = \frac{(p-1)(q-1)}{2}$, 任取 $[m]_{pq} \in (\mathbb{Z}/pq\mathbb{Z})^\times$, 那么 $p \nmid m$ 且 $q \nmid m$, 由 Fermat 小定理 2.2.2

$$m^{p-1} \equiv 1 \pmod{p}, \quad m^{q-1} \equiv 1 \pmod{q}$$

由于 p, q 均为奇数, 那么 $p-1 \mid n$ 且 $q-1 \mid n$, 因此 $p \mid m^n - 1$ 且 $q \mid m^n - 1$, 又因为 p, q 互素, 所以 $pq \mid m^n - 1$, 即

$$m^n \equiv 1 \pmod{pq}$$

所以 $(\mathbb{Z}/pq\mathbb{Z})^\times$ 中元素的阶均为 n , 不存在阶为 $|(\mathbb{Z}/pq\mathbb{Z})^\times| = (p-1)(q-1)$ 的元素, 因此 $(\mathbb{Z}/pq\mathbb{Z})^\times$ 不是循环群。

推论 2.4.1

对于奇素数 $p \neq q$, 如果 $\gcd(n, pq) = 1$, 那么

$$n^{\frac{(p-1)(q-1)}{2}} \equiv 1 \pmod{pq}$$

定义 2.4.3 (群自同构映射 group automorphism)

群 $(G, *)$ 的自同构映射为群同构映射 $\varphi: G \rightarrow G$ 。

定义 2.4.4 (群内自同构映射 group inner automorphism)

对于群 $(G, *)$, 以及 $g \in G$, 定义群 $(G, *)$ 的内自同构映射为自同构映射

$$\begin{aligned}\gamma_g : G &\longrightarrow G \\ g &\longmapsto g * g * g^{-1}\end{aligned}$$



证明 首先, 证明 γ_g 为群同态映射。任取 $g, h \in G$, 由于

$$\gamma_g(g * h) = g * g * h * g^{-1} = (g * g * g^{-1}) * (g * h * g^{-1}) = \gamma_g(g) * \gamma_g(h)$$

因此 γ_g 为群同态映射。

其次, 证明 γ_g 为双射。构造映射

$$\begin{aligned}\gamma_g^{-1} : G &\longrightarrow G \\ g &\longmapsto g^{-1} * g * g\end{aligned}$$

显然 $\gamma_g^{-1} \circ \gamma_g = \gamma_g \circ \gamma_g^{-1} = \mathbb{1}_G$, 因此 γ_g 为双射。由定理 2.4.1, γ_g 为 G 的自同构映射。

定义 2.4.5 (群自同构映射群 group automorphism group)

群 $(G, *)$ 的自同构映射构成自同构映射群 $\text{Aut}_{\text{Grp}}(G)$ 。

**命题 2.4.8 (群自同构映射群的性质)**

- 单位元为 $\mathbb{1}_G$ 。
- $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = \mathbb{1}_G$

**命题 2.4.9**

$$|\text{Aut}_{\text{Grp}}(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$$



证明 任取 $p \in \{p \in \mathbb{N}^* : 1 \leq p < n, \gcd(p, n) = 1\}$, 那么 $[p]_n$ 为 $\mathbb{Z}/n\mathbb{Z}$ 的生成元, 容易知道这样的 p 有 $\phi(n)$ 个。同构态射 $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ 由 $\varphi(p)$ 确定且唯一确定, 因此 $|\text{Aut}_{\text{Grp}}(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$ 。

命题 2.4.10

对于素数 p , 成立

$$\text{Aut}_{\text{Grp}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$$



证明 由于 p 为素数, 那么 G 中任意非零元 g 均为 $\mathbb{Z}/p\mathbb{Z}$ 的生成元, 且同构态射 $\varphi : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ 由 $\varphi(g)$ 确定且唯一确定, 而 $\mathbb{Z}/p\mathbb{Z}$ 中任意非零元构成 $(\mathbb{Z}/p\mathbb{Z})^\times$, 于是由定理 2.4.2

$$\text{Aut}_{\text{Grp}}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

定义 2.4.6 (群内自同构映射群 group inner automorphism group)

群 $(G, *)$ 的内自同构映射构成群 $\text{Inn}_{\text{Grp}}(G) = \{\gamma_g : g \in G\}$ 。

**命题 2.4.11 (群内自同构映射群的性质)**

- 单位元为 $\gamma_e = \mathbb{1}_G$ 。
- $\gamma_g \circ \gamma_h = \gamma_{g * h}$
- $\text{Inn}_{\text{Grp}}(G) \triangleleft \text{Aut}_{\text{Grp}}(G)$



命题 2.4.12

如下态射为群同态映射。

$$\begin{aligned}\Gamma : G &\longrightarrow \text{Inn}_{\text{Grp}}(G) \\ g &\longmapsto \gamma_g\end{aligned}$$

证明 任取 $g, h, k \in G$, 由于

$$\gamma_{g*h}(k) = (g*h)*k*(g*h)^{-1} = h*(g*k*g^{-1})*g*h^{-1} = \gamma_g(\gamma_h(k)) = \gamma_g \circ \gamma_h(k)$$

因此

$$\Gamma(g*h) = \gamma_{g*h} = \gamma_g \circ \gamma_h = \Gamma(g) \circ \Gamma(h)$$

于是 Γ 为群同态映射。

命题 2.4.13

$$\text{Inn}(G) \text{ 为循环群} \iff \text{Inn}(G) \text{ 为平凡群} \iff G \text{ 为 Abel 群}$$

证明 如果 G 是 Abel 群, 那么对于任意 $g \in G$, $\gamma_g = \mathbb{1}_G$, 因此 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群。

如果 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群, 那么显然 $\text{Inn}(G) = \{\mathbb{1}_G\} \cong \mathbb{Z}/1\mathbb{Z}$ 为循环群。

如果 $\text{Inn}(G)$ 为循环群, 那么存在 $g_0 \in G$, 使得对于任意 $g \in G$, 存在 $n \in \mathbb{Z}$, 使得成立 $\gamma_g = \underbrace{\gamma_{g_0} \circ \cdots \circ \gamma_{g_0}}_{n \text{ 个}}$,

因此对于任意 $g \in G$, 成立 $g*g*g^{-1} = g_0^n * g * g_0^{-n}$ 。取 $g = g_0$, 可得 $g*g_0 = g_0*g$, 因此 $\gamma_{g_0} = \mathbb{1}_G$, 于是对于任意 $g \in G$, $\gamma_g = \mathbb{1}_G$, 因此 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群。

如果 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群, 那么对于任意 $g \in G$, $\varphi(g) = \gamma_g = \mathbb{1}_G$, 因此对于任意 $g \in G$, 成立 $\gamma_g(g) = g$, 于是

$$g^{-1} * g * g = g \implies g * g = g * g$$

进而 G 为 Abel 群。

2.4.4 Abel 群的同态映射**命题 2.4.14**

对于群 $(G, *)$ 和交换群 H , $\text{Hom}_{\text{Grp}}(G, H)$ 关于 $+$ 运算构成交换群。

命题 2.4.15

对于任意集合 S 和交换群 $(G, *)$, $\text{Hom}_{\text{Set}}(S, G)$ 构成群。

2.5 自由群**2.5.1 生成元集****定义 2.5.1 (生成子群 generated subgroup)**

对于群 $(G, *)$, 由子集 $S \subset G$ 生成的子群 $\langle S \rangle$ 的等价定义如下。

1. $\langle S \rangle$ 为包含 S 的最小的 G 的子群, 即 $\langle S \rangle = \bigcap_{S \subset H < G} H$ 。
2. $\langle S \rangle = \{s_1 * \cdots * s_n : s_k \in S, n \in \mathbb{N}\}$

定义 2.5.2 (生成正规子群 generated normal subgroup)

对于群 $(G, *)$, 由子集 $S \subset G$ 生成的正规子群 $[S]$ 的等价定义如下。

1. $[S]$ 为包含 S 的最小的 G 的正规子群, 即 $[S] = \bigcap_{S \subset N \triangleleft G} N$ 。
2. $[S] = \{(g_1 * s_1^{r_1} * g_1^{-1}) * \cdots * (g_n * s_n^{r_n} * g_n^{-1}) : s_k \in S, g_k \in G, r_k \in \mathbb{Z}, n \in \mathbb{N}\}$

**定义 2.5.3 (生成元集 set of generators)**

对于群 $(G, *)$, 称子集 $S \subset G$ 为 G 的生成元集, 如果 $\langle S \rangle = G$ 。

**定义 2.5.4 (自由生成元集 free set of generators)**

对于群 $(G, *)$, 称 G 的生成元集 $S \subset G$ 为 G 的一个自由生成元集, 如果对于任意 $s_1, \dots, s_n \in S$, 以及 $r_1, \dots, r_n \in \mathbb{Z} \setminus \{0\}$, 成立 $s_1^{r_1} * \cdots * s_n^{r_n} \neq e$ 。

**定义 2.5.5 (自由群 free group)**

称群 $(G, *)$ 为自由群, 如果其存在自由生成元集。

**2.5.2 万有性质****定义 2.5.6 (自由群 free group)**

对于集合 S , 定义由 S 生成的自由群 $F(S)$ 为由 S 诱导的范畴 \mathcal{F}^S 的初始对象 $(j, F(S))$ 的群分量, 其中定义范畴 \mathcal{F}^S 如下。

1. 对象: $\text{Obj}(\mathcal{F}^S) = (j, G)$, 其中 G 为群, 且 $j: S \rightarrow G$ 为集合函数。
2. 态射: $\text{Hom}_{\mathcal{F}^S}((j_1, G_1), (j_2, G_2)) = \{\varphi \in \text{Hom}_{\text{Grp}}(G_1, G_2) : \varphi \circ j_1 = j_2\}$, 其交换图为

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ j_1 \uparrow & \nearrow j_2 & \\ S & & \end{array}$$

换言之, 对于集合 S , 称 $F(S)$ 为由 S 生成的自由群, 如果存在集合函数 $j: S \rightarrow F(S)$, 使得对于任意群 $(G, *)$ 和集合函数 $f: S \rightarrow G$, 存在且存在唯一群同态映射 $\varphi: F(S) \rightarrow G$, 使得成立 $\varphi \circ j = f$, 其交换图为

$$\begin{array}{ccc} F(S) & \xrightarrow{\varphi} & G \\ j \uparrow & \nearrow f & \\ S & & \end{array}$$



笔记 由初始对象的性质, 由 S 生成的自由群至多同构。

例题 2.11 单点集的自由群:

$$F(\{*\}) \cong \mathbb{Z}$$

命题 2.5.1 (范畴 \mathcal{F}^S 的终止对象)

由集合 S 诱导的范畴 \mathcal{F}^S 的终止对象为 $(j_e, \{e\})$, 其中 $j_e: S \rightarrow \{e\}$ 。

**命题 2.5.2**

$(j_e, \{e\})$ 不为 \mathcal{F}^S 的初始对象, 其中 $j_e: S \rightarrow \{e\}$, 除非 $S = \emptyset$ 。



证明 如果 $(j_e, \{e\})$ 为 \mathcal{F}^S 的初始对象, 那么取 $G = \mathbb{Z}/2\mathbb{Z}$, 那么不存在群同态映射 $\varphi: \{e\} \rightarrow \{[0]_2, [1]_2\}$, 于是 $(j_e, \{e\})$ 不为 \mathcal{F}^S 的初始对象, 除非 $S = \emptyset$ 。

命题 2.5.3

$j: A \rightarrow F(A)$ 为单射。

证明 对于对称群 S_A , 定义映射 $g_a: A \rightarrow A$ 为 $x \mapsto a$, 那么 $g_a \in S_A$, 因此定义映射 $f: A \rightarrow S_A$ 为 $a \mapsto g_a$, 于是存在且存在唯一群同态映射 $\varphi: F(A) \rightarrow S_A$, 使得成立 $\varphi \circ j = f$, 于是

$$\begin{aligned} j(x) = j(y) &\implies \varphi(j(x)) = \varphi(j(y)) \iff (\varphi \circ j)(x) = (\varphi \circ j)(y) \\ &\iff f(x) = f(y) \iff g_x = g_y \iff x = y \end{aligned}$$

命题 2.5.4

自由群 $F(\{x, y\})$ 在范畴 \mathbf{Grp} 中是余积 $\mathbb{Z} * \mathbb{Z}$ 。

证明 定义群同态映射

$$i_x: \mathbb{Z} \rightarrow F(\{x, y\}), \quad n \mapsto x^n i_y: \mathbb{Z} \rightarrow F(\{x, y\}), \quad n \mapsto y^n$$

我们需要证明对于任意群 $(G, *)$, 以及群同态映射 $\varphi_x, \varphi_y: (\mathbb{Z}, +) \rightarrow (G, *)$, 存在且存在唯一群同态映射 $\varphi: F(\{x, y\}) \rightarrow (G, *)$, 使得如下图交换。

$$\begin{array}{ccc} (\mathbb{Z}, +) & \xrightarrow{\varphi_x} & (G, *) \\ & \searrow i_x & \uparrow \varphi \\ & F(\{x, y\}) & \\ & \nearrow i_y & \uparrow \varphi_y \\ (\mathbb{Z}, +) & \xrightarrow{\varphi_y} & (G, *) \end{array}$$

定义群同态映射

$$\varphi: F(\{x, y\}) \longrightarrow (G, *)$$

$$z_1^{r_1} \cdots z_n^{r_n} \longmapsto \varphi_x(r_1)^{\mathbb{1}_{\{x\}}(z_1)} * \varphi_y(r_1)^{\mathbb{1}_{\{y\}}(z_1)} * \cdots * \varphi_x(r_n)^{\mathbb{1}_{\{x\}}(z_n)} * \varphi_y(r_n)^{\mathbb{1}_{\{y\}}(z_n)}, z_k \in \{x, y\}$$

此时 $\varphi \circ i_x = \varphi_x$ 且 $\varphi \circ i_y = \varphi_y$ 。

命题 2.5.5

自由群 $F(\{x_1, \dots, x_n\})$ 在范畴 \mathbf{Grp} 中是余积 $\prod_{k=1}^n \mathbb{Z}$ 。

命题 2.5.6

$$F(A \sqcup B) = F(A) * F(B), \quad F^{\text{ab}}(A \sqcup B) = F^{\text{ab}}(A) \oplus F^{\text{ab}}(B)$$

2.5.3 具体结构

定义 2.5.7 (自由群 free group)

对于集合 S , 通过如下过程构造由 S 生成的自由群 $F(S)$, 以及范畴 \mathcal{F}^S 的初始对象 $(j, F(S))$ 。

1. 定义集合 $S' = \{s^{-1} : s^{-1} \text{ 为 } s \in S \text{ 的逆且与 } s \in S \text{ 对应}\}$ 。
2. 通过并置 (juxtaposition) 定义由有限有序列表 (s_1, s_2, \dots, s_n) 生成 S 中的字为 $w = s_1 s_2 \cdots s_n$, 其中对于每一个 s_k , 或 $s_k \in S$, 或 $s_k \in S'$ 。特别的, 空字 $() \in S$ 。
3. 定义 S 中全部字构成集合 $W(S)$ 。
4. 定义初等化简映射 $r: W(S) \rightarrow W(S)$, 对于 $w \in W(S)$, 从左向右找到第一个形如 ss^{-1} 或 $s^{-1}s$ 的符号对, 并移除该符号对, 构成单词 $r(w) \in W(S)$; 如果找不到, 那么 $r(w) = w \in W(S)$ 。
5. 容易知道, 记 $w \in W(S)$ 的长度为 $|w| \in \mathbb{N}$, 那么 $r^{\lfloor |w|/2 \rfloor}(w)$ 为最简字, 即不含形如 ss^{-1} 或 $s^{-1}s$ 的符号对。
6. 定义化简映射 $R: W(S) \rightarrow W(S)$ 为 $R(w) = r^{\lfloor |w|/2 \rfloor}(w)$ 。
7. 定义由 S 生成的自由群 $F(S) = R(W(S))$, 二元运算为 $w_1 * w_2 = R(w_1 w_2)$ 。
8. 定义范畴 \mathcal{F}^S 的初始对象 $(j, F(S))$ 的映射分量 $j: S \rightarrow F(S)$ 为 $j(s) = s$ 。



2.5.4 自由 Abel 群

定义 2.5.8 (自由 Abel 群 free abelian group)

对于集合 S , 定义由 S 生成的自由 Abel 群 $F^{\text{ab}}(S)$ 为由 S 诱导的范畴 $\mathcal{F}^{\text{ab}S}$ 的初始对象 $(j, F^{\text{ab}}(S))$ 的群分量, 其中定义范畴 $\mathcal{F}^{\text{ab}S}$ 如下。


1. 对象: $\text{Obj}(\mathcal{F}^{\text{ab}S}) = (j, G)$, 其中 G 为 Abel 群, 且 $j: S \rightarrow G$ 为集合函数。
2. 态射: $\text{Hom}_{\mathcal{F}^{\text{ab}S}}((j_1, G_1), (j_2, G_2)) = \{\varphi \in \text{Hom}_{\text{Ab}}(G_1, G_2) : \varphi \circ j_1 = j_2\}$, 其交换图为

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ j_1 \uparrow & \nearrow j_2 & \\ S & & \end{array}$$

换言之, 对于集合 S , 称 $F^{\text{ab}}(S)$ 为由 S 生成的自由 Abel 群, 如果存在集合函数 $j: S \rightarrow F^{\text{ab}}(S)$, 使得对于任意 Abel 群 $(G, *)$ 和集合函数 $f: S \rightarrow G$, 存在且存在唯一群同态映射 $\varphi: F^{\text{ab}}(S) \rightarrow G$, 使得成立 $\varphi \circ j = f$, 其交换图为

$$\begin{array}{ccc} F^{\text{ab}}(S) & \xrightarrow{\varphi} & G \\ j \uparrow & \nearrow f & \\ S & & \end{array}$$



 **笔记** 由初始对象的性质, 由 S 生成的 Abel 自由群至多同构。

例题 2.12 单点集的自由 Abel 群:

$$F^{\text{ab}}(\{*\}) = F(\{*\}) \cong \mathbb{Z}$$

定理 2.5.1 (由有限集生成的自由 Abel 群)

对于有限集 $S = \{1, \dots, n\}$, $\mathbb{Z}^{\oplus n} = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \uparrow} = \mathbb{Z}^n$ 为 S 生成的自由 Abel 群 $F^{\text{ab}}(S)$, 且范畴 $\mathcal{F}^{\text{ab}S}$ 的初始对象 $(j, F^{\text{ab}}(S))$ 的映射分量 $j: S \rightarrow \mathbb{Z}^{\oplus n}$ 为 $j(k) = (0, \dots, 0, \underset{k \text{ th}}{1}, 0, \dots, 0)$ 。



定理 2.5.2 (由一般集合生成的自由 Abel 群)

对于一般的集合 S , 以及 Abel 群 $(G, *)$, 定义

$$G^{\oplus S} = \{f : S \rightarrow G : \text{仅存在有限个 } s \in S \text{ 使得成立 } f(s) \neq e\}$$

注意到, $G^{\oplus S}$ 为 G^S 的子群, 且当 S 有限时, $G^{\oplus S} = G^S$, 同时当 $S = \{1, \dots, n\}$ 时, $\mathbb{Z}^{\oplus S} \cong \mathbb{Z}^{\oplus n}$ 。

对于集合 S , 成立 $F^{\text{ab}}(S) \cong \mathbb{Z}^{\oplus S}$, 且范畴 $\mathcal{F}^{\text{ab}S}$ 的初始对象 $(j, F^{\text{ab}}(S))$ 的映射分量 $j : S \rightarrow \mathbb{Z}^{\oplus S}$ 为 $j(s) = j_s$, 其中

$$j_s : S \rightarrow \mathbb{Z}$$

$$t \mapsto \begin{cases} 1, & t = s \\ 0, & t \in S \setminus \{s\} \end{cases}$$

**命题 2.5.7**

$$\mathbb{Z}^{\oplus \mathbb{N}} \times \mathbb{Z}^{\oplus \mathbb{N}} \cong \mathbb{Z}^{\oplus \mathbb{N}}$$



证明 构造映射

$$\varphi : \mathbb{Z}^{\oplus \mathbb{N}} \times \mathbb{Z}^{\oplus \mathbb{N}} \rightarrow \mathbb{Z}^{\oplus \mathbb{N}}$$

$$((a_1, a_2, \dots), (b_1, b_2, \dots)) \mapsto (a_1, b_1, a_2, b_2, \dots)$$

首先证明 φ 为群同态映射。

$$\begin{aligned} & \varphi(((a_1, a_2, \dots), (b_1, b_2, \dots)) + ((c_1, c_2, \dots), (d_1, d_2, \dots))) \\ &= \varphi(((a_1 + c_1, a_2 + c_2, \dots), (b_1 + d_1, b_2 + d_2, \dots))) \\ &= (a_1 + c_1, b_1 + d_1, a_2 + c_2, b_2 + d_2, \dots) \\ &= (a_1, b_1, a_2, b_2, \dots) + (c_1, d_1, c_2, d_2, \dots) \\ &= \varphi(((a_1, a_2, \dots), (b_1, b_2, \dots))) + \varphi(((c_1, c_2, \dots), (d_1, d_2, \dots))) \end{aligned}$$

其次容易证明 φ 为双射, 进而 $\mathbb{Z}^{\oplus \mathbb{N}} \times \mathbb{Z}^{\oplus \mathbb{N}} \cong \mathbb{Z}^{\oplus \mathbb{N}}$, 命题得证!

命题 2.5.8

定义 $F^{\text{ab}}(S)$ 上的等价关系:

$$a \sim b \iff \exists a - b \in 2F^{\text{ab}}(S)$$

那么

$$|F^{\text{ab}}(S)/\sim| < \infty \iff |S| < \infty \implies |F^{\text{ab}}(S)/\sim| = 2^{|S|}$$

**命题 2.5.9**

如果 $F^{\text{ab}}(A) \cong F^{\text{ab}}(B)$, 那么 $A \cong B$, 且 $|A| < \infty \iff |B| < \infty$ 。



2.6 子群

2.6.1 定义

定义 2.6.1 (子群 subgroup)

称原群 $(H, *)$ 为 $(G, *)$ 的子群, 如果存在单的群同态映射 $\varphi: H \rightarrow G$.



定义 2.6.2 (子群 subgroup)

称原群 $(H, *)$ 为 $(G, *)$ 的子群, 并记作 $H < G$, 如果 $H \subset G$, 且对于任意 $g, h \in H$, 成立 $g * h^{-1} \in H$.



例题 2.13 记 \mathbb{C} 上的 n 阶可逆矩阵群为 $GL_n(\mathbb{C})$, \mathbb{C} 上的 n 阶可逆上三角矩阵群为 $U_n^\times(\mathbb{C})$, 那么 $U_n^\times(\mathbb{C})$ 为 $GL_n(\mathbb{C})$ 的子群。

例题 2.14 如果 $(G, *)$ 为交换群, 那么对于 $n \in \mathbb{N}^*$, $\{g^n : g \in G\}$ 为 G 的子群。

证明

$$g^n * (h^n)^{-1} = g^n * (h^{-1})^n = (g * h^{-1})^n \in \{g^n : g \in G\}$$

命题 2.6.1 (子群的交为子群)

子群的交为子群。



命题 2.6.2

对于群 $(G, *)$ 的子群 H 与 K , 成立

$$H \cup K \text{ 为子群} \iff H \subset K \text{ 或 } K \subset H$$

一般的, 如果 $H_0 \subset H_1 \subset \cdots \subset G$ 为 G 的子群, 那么 $\bigcup_{n=0}^{\infty} H_n$ 为 G 的子群。



证明 充分性显然, 对于必要性, 如果 $H \subset K$, 那么命题成立。如果 $H \not\subset K$, 那么存在 $h_0 \in H$, 使得成立 $h_0 \notin K$ 。由于 $H \cup K$ 为子群, 任取 $k \in K$, 因此 $h_0, k \in H \cup K$, 那么 $h_0 * k \in H \cup K$, 于是存在 $g \in H \cup K$, 使得成立 $h_0 * k = g$ 。如果 $g \in K$, 那么 $h_0 = g * k^{-1} \in K$, 矛盾! 因此 $g \in H$, 于是 $k = h_0^{-1} * g \in H$, 进而 $K \subset H$ 。充分性得证!

一般的, 如果 $H_0 \subset H_1 \subset \cdots \subset G$ 为 G 的子群, 那么任取 $h_1, h_2 \in \bigcup_{n=0}^{\infty} H_n$, 存在 $n_1, n_2 \in \mathbb{N}$, 使得成立 $h_1 \in H_{n_1}, h_2 \in H_{n_2}$ 。不妨记 $n_1 \leq n_2$, 那么 $h_1 \in H_{n_1} \subset H_{n_2}$, 因此 $h_1 * h_2^{-1} \in H_{n_2} \subset \bigcup_{n=0}^{\infty} H_n$, 于是 $\bigcup_{n=0}^{\infty} H_n$ 为 G 的子群。

命题 2.6.3 (子群的像为子群)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$I < G \implies \varphi(I) < \text{im } \varphi$$



证明 由于 $\varphi(I) \subset \text{im } \varphi$, 且

$$g, h \in \varphi(I) \iff \exists i, j \in I, \varphi(i) = g, \varphi(j) = h \implies \exists i, j \in I, g * h^{-1} = \varphi(i) * \varphi(j)^{-1} = \varphi(i * j^{-1}) \in \varphi(I)$$

因此 $\varphi(I)$ 为 $\text{im } \varphi$ 的子群。

命题 2.6.4 (子群的原像为子群)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$J < \text{im } \varphi \implies \ker \varphi \subset \varphi^{-1}(J) < G$$



证明 由于 $\varphi^{-1}(J) \subset G$, 且

$$g, h \in \varphi^{-1}(J) \iff \varphi(g), \varphi(h) \in J \implies \varphi(g) * \varphi(h)^{-1} \in J \iff \varphi(g * h^{-1}) \in J \iff g * h^{-1} \in \varphi^{-1}(J)$$

因此 $\varphi^{-1}(J)$ 为 G 的子群。而 $0_H \in J$, 因此 $\ker \varphi = \varphi^{-1}(0_H) \subset \varphi^{-1}(J)$ 。

命题 2.6.5 (由群同态映射诱导的子群双射)

对于群同态映射 $\varphi: G \rightarrow H$, 如下集合函数为双射。

$$\begin{aligned} \Psi: \{I: \ker \varphi \subset I < G\} &\longrightarrow \{J < \text{im } \varphi\} \\ I &\longmapsto \varphi(I) \end{aligned}$$



证明 由命题 2.6.3, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性

$$\Psi(I) = \Psi(J) \iff \varphi(I) = \varphi(J) \implies \varphi^{-1}(\varphi(I)) = \varphi^{-1}(\varphi(J)) \iff I * \ker \varphi = J * \ker \varphi \iff I = J$$

其次对于 Ψ 的满射性。如果 $J < \text{im } \varphi$, 那么由命题 2.6.4, $\ker \varphi \subset \varphi^{-1}(J) < G$ 。注意到, $\Psi(\varphi^{-1}(J)) = \varphi(\varphi^{-1}(J)) = J \cap \text{im } \varphi = J$, 因此 Ψ 为满射。

命题 2.6.6 (由群同态逆映射诱导的子群双射)

对于群同态映射 $\varphi: G \rightarrow H$, 如下集合函数为双射。

$$\begin{aligned} \Psi: \{J < \text{im } \varphi\} &\longrightarrow \{I: \ker \varphi \subset I < G\} \\ J &\longmapsto \varphi^{-1}(J) \end{aligned}$$



证明 由命题 2.6.4, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性

$$\Psi(I) = \Psi(J) \iff \varphi^{-1}(I) = \varphi^{-1}(J) \implies \varphi(\varphi^{-1}(I)) = \varphi(\varphi^{-1}(J)) \iff I \cap \text{im } \varphi = J \cap \text{im } \varphi \iff I = J$$

其次对于 Ψ 的满射性。如果 $\ker \varphi \subset I < G$, 那么由命题 2.6.3, $\varphi(I) < \text{im } \varphi$ 。注意到, $\Psi(\varphi(I)) = \varphi^{-1}(\varphi(I)) = I * \ker \varphi = I$, 因此 Ψ 为满射。

命题 2.6.7

对于群 $(G, *)$, 如果 N 为 G 的正规子群, 那么

$$\{H * N: H < G\} = \{H \supset N < G\}$$



证明 如果 $H < G$ 为正规子群, 那么容易知道 $H * N < G$, 因此

$$\{H * N: H < G\} \subset \{H \supset N < G\}$$

如果 $H \supset N < G$, 那么 $H * N = H$, 因此

$$\{H * N: H < G\} \supset \{H \supset N < G\}$$

综上所述

$$\{H * N: H < G\} = \{H \supset N < G\}$$

2.6.2 核与像

定义 2.6.3 (核 kernel)

定义群同态映射 $\varphi: G \rightarrow H$ 的核为

$$\ker \varphi = \{g \in G : \varphi(g) = e_H\} = \varphi^{-1}(e_H)$$

定义 2.6.4 (像 image)

定义群同态映射 $\varphi: G \rightarrow H$ 的像为

$$\operatorname{im} \varphi = \{\varphi(g) \in H : g \in G\} = \varphi(G)$$

命题 2.6.8 (因子通过 factor through)

对于群同态映射 $\varphi: G \rightarrow H$, 满足 $\varphi \circ \alpha$ 为平凡映射的群同态映射 $\alpha: K \rightarrow G$ 唯一因子通过 $\ker \varphi$, 其交换图如下。

$$\begin{array}{ccccc} & & 0 & & \\ & \searrow & & \searrow & \\ K & \xrightarrow{\alpha} & G & \xrightarrow{\varphi} & H \\ & \searrow & \uparrow & & \\ & & \ker \varphi & & \end{array}$$

$\exists! \bar{\alpha}$

命题 2.6.9

对于任意集合函数 $\varphi: G \rightarrow H$, 满足 $\varphi \circ \alpha = \mathbb{1}_K$ 的集合函数 $\alpha: K \rightarrow G$ 因子通过 $\ker \varphi$ 。

2.6.3 由子集生成的子群

定义 2.6.5 (由子集生成的子群 subgroup generated by subset)

对于群 $(G, *)$, 子集 $S \subset G$ 生成自由群 $F(S)$, 那么存在且存在唯一群同态映射 $\varphi: F(S) \rightarrow G$, 因此记 $\langle S \rangle = \varphi(F(S))$ 为由子集 S 生成的子群。事实上, $\langle S \rangle$ 的显性表达式如下

$$\langle S \rangle = \{s_1^{r_1} * \cdots * s_n^{r_n} : s_k \in S, r_k \in \mathbb{Z}\}$$

事实上, 如果群 $(G, *)$ 由子集 $S \subset G$ 生成, 那么

$$\langle S \rangle = \bigcap_{S \subset H < G} H$$

定义 2.6.6 (有限生成群 finitely generated group)

称群 $(G, *)$ 为有限生成的, 如果存在有限子集 $S \subset G$, 使得成立 $\langle S \rangle = G$ 。

证明 对于 $m, n \in \mathbb{N}^*$, 记 $\gcd(m, n) = r$, 那么 $\langle m, n \rangle = r\mathbb{Z}$ 。

证明 由定理 2.2.1, 存在 $p, q \in \mathbb{Z}$, 使得成立 $pm + qn = r$, 于是 $r\mathbb{Z} \subset \langle m, n \rangle$ 。任取 $s \in \langle m, n \rangle$, 于是存在 $a, b \in \mathbb{Z}$, 使得成立 $s = am + bn$ 。而 $\gcd(m, n) = r$, 那么存在 $m_0, n_0 \in \mathbb{Z}$, 使得成立 $m = m_0r, n = n_0r$, 且 $\gcd(m_0, n_0) = 1$, 因此 $s = (am_0 + bn_0)r \in r\mathbb{Z}$, 于是 $\langle m, n \rangle \subset r\mathbb{Z}$, 进而 $\langle m, n \rangle = r\mathbb{Z}$ 。

命题 2.6.10 (有限生成群的等价条件)

群 $(G, *)$ 为有限生成群 \iff 存在 $n \in \mathbb{N}^*$, 使得存在满的群同态映射 $\mathbb{Z}^n \twoheadrightarrow G$ 。

证明 对于必要性, 如果 Abel 群 $(G, *)$ 是有限生成的, 那么存在 $g_1, \dots, g_n \in G$, 使得对于任意 $g \in G$, 存在 $r_1, \dots, r_n \in \mathbb{Z}$, 使得成立 $g = g_1^{r_1} * \dots * g_n^{r_n}$ 。构造映射

$$\begin{aligned} \varphi: \quad \mathbb{Z}^n &\longrightarrow G \\ (r_1, \dots, r_n) &\longmapsto g_1^{r_1} * \dots * g_n^{r_n} \end{aligned}$$

由 $G = \langle g_1, \dots, g_n \rangle$ 可知 φ 为满射, 且由 G 为 Abel 群容易证明 φ 为群同态映射。

对于充分性, 如果存在 $n \in \mathbb{N}^*$, 使得存在满的群同态映射 $\psi: \mathbb{Z}^n \rightarrow G$ 。记 $\psi(0, \dots, 0, 1, 0, \dots, 0) = g_k$, 其中 $1 \leq k \leq n$ 。由于 ψ 为满的, 那么对于任意 $g \in G$, 存在 $(r_1, \dots, r_n) \in \mathbb{Z}^n$, 使得成立

$$g = \psi(r_1, \dots, r_n) = \psi\left(\sum_{k=1}^n r_k(0, \dots, 0, 1, 0, \dots, 0)\right) = \prod_{k=1}^n (\psi(0, \dots, 0, 1, 0, \dots, 0))^{r_k} = g_1^{r_1} * \dots * g_n^{r_n}$$

于是 $G = \langle g_1, \dots, g_n \rangle$ 。

命题 2.6.11

$(\mathbb{Q}, +)$ 的有限生成子群为循环群。

证明 仅对 $(\mathbb{Q}, +)$ 的三元生成子群 $\langle \frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3} \rangle$ 进行证明, 其中 $p_k, q_k \in \mathbb{N}^*$, 不妨 $\gcd(p_k, q_k) = 1$, 且 $p_i q_j \nmid p_j q_i$, 其中 $i, j, k \in \{1, 2, 3\}$, 且 $i \neq j$ 。

注意到

$$\langle \frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3} \rangle = \frac{1}{q_1 q_2 q_3} \langle p_1 q_2 q_3, q_1 p_2 q_3, q_1 q_2 p_3 \rangle$$

记

$$A = p_1 q_2 q_3, B = q_1 p_2 q_3, C = q_1 q_2 p_3$$

并记 $\gcd(A, B, C) = r$, 那么存在 $a, b, c, A_0, B_0, C_0 \in \mathbb{Z}$, 使得成立

$$aA + bB + cC = r, \quad A = rA_0, B = rB_0, C = rC_0, \quad \gcd(A_0, B_0, C_0) = 1$$

于是 $r\mathbb{Z} \subset \langle A, B, C \rangle$ 。任取 $s \in \langle A, B, C \rangle$, 于是存在 $m, n, l \in \mathbb{Z}$, 使得成立

$$s = mA + nB + lC = (mA_0 + nB_0 + lC_0)r \in r\mathbb{Z}$$

于是 $\langle A, B, C \rangle \subset r\mathbb{Z}$, 因此 $\langle A, B, C \rangle = r\mathbb{Z}$, 进而

$$\langle \frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3} \rangle = \frac{1}{q_1 q_2 q_3} \langle p_1 q_2 q_3, q_1 p_2 q_3, q_1 q_2 p_3 \rangle = \frac{1}{q_1 q_2 q_3} \langle A, B, C \rangle = \frac{r}{q_1 q_2 q_3} \mathbb{Z}$$

为循环群。

命题 2.6.12

$(\mathbb{Q}, +)$ 不为有限生成群。

证明 反证, 如果 $(\mathbb{Q}, +)$ 为有限生成群, 那么由命题 2.6.11, $(\mathbb{Q}, +) \cong \mathbb{Z}$, 于是存在 $p/q \in \mathbb{Q}$, 不妨 $\gcd(p, q) = 1$ 且 $p, q \in \mathbb{N}^*$, 使得对于任意 $r \in \mathbb{Q}$, 存在 $n \in \mathbb{Z}$, 使得成立 $r = (p/q)^n$ 。取 $r \in \mathbb{N}^* \subset \mathbb{Q}$ 满足 $\gcd(p, q, r) = 1$, 于是存在 $n \in \mathbb{Z}$, 使得成立 $r = (p/q)^n$, 不妨假设 $n \in \mathbb{N}$, 那么 $p^n = rq^n$, 矛盾! 因此 $(\mathbb{Q}, +)$ 不为有限生成群。

2.6.4 循环群的子群

命题 2.6.13 (无限循环群的子群结构)

$$G < \mathbb{Z} \iff \exists n \in \mathbb{N}, G = n\mathbb{Z} = \langle n \rangle$$

命题 2.6.14 (有限循环群的子群结构)

$$G < \mathbb{Z}/n\mathbb{Z} \iff \exists p, p \mid n \text{ 且 } G = \langle [p]_n \rangle$$

**2.6.5 单态射与满态射****命题 2.6.15**

如果群同态映射存在左逆, 那么其为单态射; 反之不然。



证明 证明见命题 1.4.2。

反例: 构造群同态映射

$$\begin{aligned} \varphi: \mathbb{Z}/3\mathbb{Z} &\longrightarrow S_3 \\ [0]_3 &\longmapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \\ [1]_3 &\longmapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ [2]_3 &\longmapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \end{aligned}$$

一方面, 任取 $\alpha_1, \alpha_2: A \rightarrow \mathbb{Z}/3\mathbb{Z}$, 满足 $\varphi \circ \alpha_1 = \varphi \circ \alpha_2$, 注意到 $\varphi: \mathbb{Z}/3\mathbb{Z} \rightarrow \varphi(\mathbb{Z}/3\mathbb{Z})$ 为双射, 因此 $\alpha_1 = \alpha_2$, 于是 φ 为单态射。

另一方面, $S_3 \rightarrow \mathbb{Z}/3\mathbb{Z}$ 仅存在平凡群同态映射, 因此 φ 不存在左逆。

命题 2.6.16

对于群同态映射 $\varphi: G \rightarrow H$, 如下命题等价。

1. $\varphi: G \rightarrow H$ 为单态射。
2. $\ker \varphi = \{e_G\}$
3. $\varphi: G \rightarrow H$ 为单函数映射。

**命题 2.6.17**

对于 Abel 群同态映射 $\varphi: G \rightarrow H$, 如下命题等价。

1. $\varphi: G \rightarrow H$ 为满态射。
2. $\text{coker } \varphi$ 是平凡的。
3. $\varphi: G \rightarrow H$ 为满函数映射。



2.7 商群

2.7.1 正规子群

定义 2.7.1 (正规子群 normal subgroup)

称群 $(G, *)$ 的子群 $(N, *)$ 为正规子群, 并记做 $N \triangleleft G$, 如果成立如下命题之一。

1. 对于任意 $g \in G$, 以及 $n \in N$, 成立 $g * n * g^{-1} \in N$ 。
2. 对于任意 $g \in G$, 成立 $g * N = N * g$ 。
3. 对于任意 $g \in G$, 成立 $g * N \subset N * g$ 。
4. 对于任意 $g \in G$, 成立 $N * g \subset g * N$ 。
5. 对于任意 $g \in G$, 成立 $g * N * g^{-1} = N$ 。
6. 对于任意 $g \in G$, 成立 $g * N * g^{-1} \subset N$ 。
7. 对于任意 $g \in G$, 成立 $N \subset g * N * g^{-1}$ 。



例题 2.15

$$\mathrm{SL}_n(\mathbb{R}) \triangleleft \mathrm{GL}_n(\mathbb{R})$$

证明 任取 $M \in \mathrm{GL}_n(\mathbb{R}), N \in \mathrm{SL}_n(\mathbb{R})$, 那么

$$\det(MNM^{-1}) = \det(M) \det(N) \det(M^{-1}) = \det(M) \det(M^{-1}) = 1$$

因此 $MNM^{-1} \in \mathrm{SL}_n(\mathbb{R})$, 进而 $\mathrm{SL}_n(\mathbb{R}) \triangleleft \mathrm{GL}_n(\mathbb{R})$ 。

例题 2.16 对于群 $(G, *)$, 以及 $n \in \mathbb{N}^*$, 定义 $N = \langle g \in G : |g| = n \rangle$, 那么 N 为正规子群。

证明 任取 $g \in G, h \in N$, 那么 $|h| = n$, 注意到

$$(g * h * g^{-1})^m = g * h^m * g^{-1} \begin{cases} = e, & m = n \\ \neq e, & 1 \leq m < n \end{cases}$$

因此 $|g * h * g^{-1}| = n$, 于是 $g * h * g^{-1} \in N$, 进而 N 为正规子群。

命题 2.7.1 (Abel 群的子群为正规子群)

Abel 群的子群为正规子群。



命题 2.7.2

对于群 $(G, *)$ 的子群 $N \subset G$, 成立

$$N \triangleleft G \iff \forall g \in G, \gamma_g(N) \subset N$$

其中 γ_g 为群 $(G, *)$ 的内自同构映射

$$\begin{aligned} \gamma_g : G &\longrightarrow G \\ g &\longmapsto g * g * g^{-1} \end{aligned}$$



证明 对于必要性, 如果 N 为正规子群, 那么任取 $g \in G$, 可得 $\gamma_g(N) = g * N * g^{-1} = N$ 。

对于充分性, 任取 $g \in G, n \in N$, 那么 $g * n * g^{-1} = \gamma_g(n) \in \gamma_g(N) \subset N$, 因此 N 为正规子群。

命题 2.7.3

$$N < G, \quad [G : N] = 2 \implies N \triangleleft G$$



证明 记 $G/N = \{N, g_0 * N\}$, 其中 $g_0 \neq e \in G$ 。任取 $g \in G$, 或 $g \in N$, 或 $g \in g_0 * N = G \setminus N$ 。如果 $g \in N$, 那

么 $g * N = N = N * g$; 如果 $g \in g_0 * N = N * g_0$, 那么 $g * N = g_0 * N = G \setminus N = N * g_0 = N * g$, 进而 $N \triangleleft G$ 。

例题 2.17 构造: 群同态映射 $\varphi: G \rightarrow H$, 使得不成立 $\text{im } \varphi \triangleleft H$ 。

证明 构造群同态映射

$$\varphi: \{\sigma, \tau\} \longrightarrow D_3$$

$$\sigma \longmapsto \sigma$$

$$\tau \longmapsto \tau$$

注意到 $\varphi(\{\sigma, \tau\}) = \{\sigma, \tau\}$ 不为 D_3 的正规子群。

命题 2.7.4 (正规子群的像为正规子群)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$N \triangleleft G \implies \varphi(N) \triangleleft \text{im } \varphi$$

证明 由命题 2.6.3, $\varphi(N)$ 为 $\text{im } \varphi$ 的子群。而

$$g \in G, n \in N \implies g * n * g^{-1} \in N \implies \varphi(g * n * g^{-1}) \in \varphi(N) \iff \varphi(g) * \varphi(n) * \varphi(g)^{-1} \in \varphi(N)$$

因此 $\varphi(N)$ 为 $\text{im } \varphi$ 的正规子群。

命题 2.7.5 (正规子群的原像为正规子群)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$M \triangleleft \text{im } \varphi \implies \ker \varphi \subset \varphi^{-1}(M) \triangleleft G$$

证明 由命题 2.6.4, $\varphi(N)$ 为 $\text{im } \varphi$ 的子群, 且 $\ker \varphi \subset \varphi^{-1}(M)$ 。而由于 $\varphi^{-1}(M) \subset G$, 且

$$g \in G, m \in \varphi^{-1}(M) \implies \varphi(g) \in \text{im } \varphi, \varphi(m) \in M \implies \varphi(g * m * g^{-1}) \in M \iff g * m * g^{-1} \in \varphi^{-1}(M)$$

因此 $\varphi^{-1}(M)$ 为 G 的正规子群。

命题 2.7.6 (正规子群的积为正规子群)

$$H, K \triangleleft G \implies H * K \triangleleft G$$

证明

$$\begin{aligned} H, K \triangleleft G &\iff \forall g \in G, h \in H, k \in K, g * h * g^{-1} \in H, g * k * g^{-1} \in K \\ &\implies \forall g \in G, h \in H, k \in K, (g * h * g^{-1}) * (g * k * g^{-1}) \in H * K \\ &\iff \forall g \in G, h \in H, k \in K, g * (h * k) * g^{-1} \in H * K \\ &\iff H * K \triangleleft G \end{aligned}$$

命题 2.7.7

对于群 $(G, *)$, 如果 N 为 G 的正规子群, 那么

$$\{M * N : M \text{ 为正规子群}\} = \{M \supset N \text{ 为正规子群}\}$$

证明 如果 M 为正规子群, 那么由命题 2.7.6, $M * N$ 为正规子群, 因此

$$\{M * N : M \text{ 为正规子群}\} \subset \{M \supset N \text{ 为正规子群}\}$$

如果 $M \supset N$ 为正规子群, 那么 $M * N = M$, 因此

$$\{M * N : M \text{ 为正规子群}\} \supset \{M \supset N \text{ 为正规子群}\}$$

综上所述

$$\{M * N : M \text{ 为正规子群}\} = \{M \supset N \text{ 为正规子群}\}$$

命题 2.7.8

对于群同态映射 $\varphi: G \rightarrow H$, 如下集合函数为双射。

$$\begin{aligned} \Psi : \{N : \ker \varphi \subset N \triangleleft G\} &\longrightarrow \{M \triangleleft \text{im } \varphi\} \\ N &\longmapsto \varphi(N) \end{aligned}$$



证明 由命题2.7.4, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性

$$\Psi(N) = \Psi(M) \iff \varphi(N) = \varphi(M) \implies \varphi^{-1}(\varphi(N)) = \varphi^{-1}(\varphi(M)) \iff N * \ker \varphi = M * \ker \varphi \iff N = M$$

其次对于 Ψ 的满射性。如果 $M \triangleleft \text{im } \varphi$, 那么由命题2.7.5, $\ker \varphi \subset \varphi^{-1}(M) \triangleleft G$ 。注意到, $\Psi(\varphi^{-1}(M)) = \varphi(\varphi^{-1}(M)) = M \cap \text{im } \varphi = M$, 因此 Ψ 为满射。

命题 2.7.9

对于群同态映射 $\varphi: G \rightarrow H$, 如下集合函数为双射。

$$\begin{aligned} \Psi : \{M \triangleleft \text{im } \varphi\} &\longrightarrow \{N : \ker \varphi \subset N \triangleleft G\} \\ M &\longmapsto \varphi^{-1}(M) \end{aligned}$$



证明 由命题2.7.5, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性

$$\Psi(N) = \Psi(M) \iff \varphi^{-1}(N) = \varphi^{-1}(M) \implies \varphi(\varphi^{-1}(N)) = \varphi(\varphi^{-1}(M)) \iff N \cap \text{im } \varphi = M \cap \text{im } \varphi \iff N = M$$

其次对于 Ψ 的满射性。如果 $\ker \varphi \subset N \triangleleft G$, 那么由命题2.7.4, $\varphi(N) \triangleleft \text{im } \varphi$ 。注意到, $\Psi(\varphi(N)) = \varphi^{-1}(\varphi(N)) = N * \ker \varphi = N$, 因此 Ψ 为满射。

2.7.2 商群

命题 2.7.10

对于群 $(G, *)$, \sim 为 G 上的等价关系, 定义群 $(G/\sim, \bullet)$, 运算 $[a] \bullet [b] = [a * b]$ 是定义良好的 \iff 对于任意 $a, b, g \in G$, 如果 $a \sim b$, 那么 $a * g \sim b * g$ 且 $g * a \sim g * b$ 。在此情况下, 商映射 $\pi: G \rightarrow G/\sim$ 为群同态映射, 且 $(\pi, G/\sim)$ 为商范畴 \mathcal{C}_{\sim}^G 的初始对象, 其中商范畴 \mathcal{C}_{\sim}^G 如下。

1. 对象: $\text{Obj}(\mathcal{C}_{\sim}^G) = \{(\varphi, H) \mid \varphi: G \rightarrow H \text{ 为群同态映射且 } a \sim b \implies \varphi(a) = \varphi(b)\}$
2. 态射: $(\varphi, H) \rightarrow (\psi, K)$ 为如下交换图。

$$\begin{array}{ccc} H & \xrightarrow{\sigma} & K \\ \varphi \swarrow & & \nearrow \psi \\ & G & \end{array}$$

换言之, 如果对于任意 $a, b, g \in G$, 成立 $a \sim b \implies a * g \sim b * g$ 且 $g * a \sim g * b$, 那么对于任意满足 $a \sim b \implies \varphi(a) = \varphi(b)$ 的群同态映射 $\varphi: G \rightarrow H$, 存在且存在唯一群同态映射 $\bar{\varphi}: G/\sim \rightarrow H$, 使得成立 $\varphi = \bar{\varphi} \circ \pi$, 交换图为

$$\begin{array}{ccc} G/\sim & \xrightarrow{\exists! \bar{\varphi}} & \forall H \\ \pi \swarrow & & \nearrow \forall \varphi \\ & G & \end{array}$$



定义 2.7.2 (商群 quotient group)

称 $(G/\sim, \bullet)$ 为群 $(G, *)$ 关于等价关系 \sim 的商群, 其中 $[a] \bullet [b] = [a * b]$, 如果对于任意 $a, b, g \in G$, 成立 $a \sim b \implies a * g \sim b * g$ 且 $g * a \sim g * b$ 。

**2.7.3 陪集****定义 2.7.3 (左陪集 (left-coset))**

定义群 $(G, *)$ 关于子群 $(H, *)$ 的左陪集为 $(G/H)_L = \{g * H : g \in G\}$, 简写为 G/H 。

**定义 2.7.4 (右陪集 (right-coset))**

定义群 $(G, *)$ 关于子群 $(H, *)$ 的右陪集为 $(G/H)_R = \{H * g : g \in G\}$ 。

**定义 2.7.5 (左等价关系)**

定义群 $(G, *)$ 关于子群 $(H, *)$ 的左等价关系 \sim_L 为

$$a \sim_L b \iff a^{-1} * b \in H \iff b \in a * H \iff a * H = b * H$$

**定义 2.7.6 (右等价关系)**

定义群 $(G, *)$ 关于子群 $(H, *)$ 的右等价关系 \sim_R 为

$$a \sim_R b \iff a * b^{-1} \in H \iff a \in H * b \iff H * a = H * b$$

**定义 2.7.7 (左商群 left-quotient group)**

定义群 $(G, *)$ 关于子群 $(H, *)$ 的左商群为 $G/\sim_L = \{g * H : g \in G\}$ 。

**定义 2.7.8 (右商群 right-quotient group)**

定义群 $(G, *)$ 关于子群 $(H, *)$ 的右商群为 $G/\sim_R = \{H * g : g \in G\}$ 。

**命题 2.7.11 (左商群 \cong 右商群)**

对于群 $(G, *)$ 关于子群 $(H, *)$ 的陪集, 成立 $(G/H)_L \cong (G/H)_R$, 群同构映射为 $g * H \mapsto H * g^{-1}$ 。

**命题 2.7.12 (左右等价关系的性质)**

对于群 $(G, *)$ 的左等价关系 \sim_L 与右等价关系 \sim_R , 成立

$$a \sim_L b \implies g * a \sim_L g * b, \quad a \sim_R b \implies a * g \sim_R b * g$$

**2.7.4 正规子群的商****命题 2.7.13**

对于群 $(G, *)$ 中关于子群 N 的左等价关系 \sim_L 与右等价关系 \sim_R , 成立 $\sim_L = \sim_R \iff N$ 为正规子群。



定义 2.7.9 (模 N 商群 quotient group modulo N)

对于群 $(G, *)$ 的正规子群 $(N, *)$, 称群 $(G/N, \bullet)$ 为 $(G, *)$ 的模 N 商群, 其中 $G/N = \{g * N : g \in G\}$, $(g * N) \bullet (h * N) = (g * h) * N$; 亦记作 $\frac{G}{N}$.



例题 2.18 描述:

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}}$$

证明 由于

$$\mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z} : x \in \mathbb{R}\} = \{x + \mathbb{Z} : x \in [0, 1)\}$$

那么

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}} = \{(x, y) + \mathbb{Z} \times \mathbb{Z} : (x, y) \in \mathbb{R} \times \mathbb{R}\} = \{(x, y) + \mathbb{Z} \times \mathbb{Z} : (x, y) \in [0, 1) \times [0, 1)\}$$

定理 2.7.1 (商群的万有性质)

如果 $(N, *)$ 为群 $(G, *)$ 的正规子群, 那么对于任意满足 $N \subset \ker \varphi$ 的群同态映射 $\varphi : G \rightarrow H$, 存在且存在唯一群同态映射 $\bar{\varphi} : G/N \rightarrow H$, 使得成立 $\varphi = \bar{\varphi} \circ \pi$, 其中 $\pi : G \rightarrow G/N, g \mapsto g * N$, 交换图为

$$\begin{array}{ccc} G/N & \xrightarrow{\exists! \bar{\varphi}} & \forall H \\ & \nwarrow \pi & \nearrow \forall \varphi \\ & G & \end{array}$$



例题 2.19 取 $\varphi : \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ 为 $[n]_4 \mapsto [n]_2$, 那么 $\ker \varphi = \{[0]_4, [2]_4\}$, 令 $N = \{[0]_4, [2]_4\}$, 于是 $(\mathbb{Z}/4\mathbb{Z})/N = \{\{[0]_4, [2]_4\}, \{[1]_4, [3]_4\}\}$, 因此 $\pi : \mathbb{Z}/4\mathbb{Z} \rightarrow (\mathbb{Z}/4\mathbb{Z})/N$ 为 $[n]_4 \mapsto \{[n]_4, [n+2]_4\}$, 进而存在且存在唯一 $\bar{\varphi} : (\mathbb{Z}/4\mathbb{Z})/N \rightarrow \mathbb{Z}/2\mathbb{Z}$ 为 $\{\{[n]_4, [n+2]_4\}\} \mapsto [n]_2$.

$$\begin{array}{ccc} \{\{[0]_4, [2]_4\}, \{[1]_4, [3]_4\}\} & \xrightarrow{\exists! \bar{\varphi}} & \{[0]_2, [1]_2\} \\ & \nwarrow \pi \quad \nearrow \varphi & \\ & \{[0]_4, [1]_4, [2]_4, [3]_4\} & \end{array}$$

命题 2.7.14 (商群的子群)

如果 N 为群 $(G, *)$ 的正规子群, 那么如下集合函数为双射。

$$\begin{aligned} \varphi : \{H : N \subset H < G\} &\longrightarrow \{K < G/N\} \\ H &\longmapsto H/N \end{aligned}$$



证明 (优雅证明) 注意到如下自然群同态

$$\begin{aligned} \pi : G &\longrightarrow G/N \\ g &\longmapsto g * N \end{aligned}$$

其中 $\ker \pi = N$, 且 $\text{im } \pi = G/N$. 由命题 2.6.5, 如下集合函数为双射。

$$\begin{aligned} \Psi : \{H : N \subset H < G\} &\longrightarrow \{K < G/N\} \\ H &\longmapsto \pi(H) \end{aligned}$$

注意到

$$\Phi(H) = H/N = \{h * N : h \in H\} = \pi(H) = \Psi(H)$$

因此 $\Phi = \Psi$, 进而 Φ 为双射。

(朴素证明) 首先证明 φ 的定义良好性。如果 $N \subset H < G$, 那么任取 $g, h \in H$, 因此 $g * h^{-1} \in H$, 进而

$$(g * N) \bullet (h * N)^{-1} = (g * N) \bullet (h^{-1} * N) = (g * h^{-1}) * N \in H/N$$

因此 H/N 为 G/N 的子群, 所以 φ 定义良好。

其次证明 φ 的单射性。如果 $\varphi(H) = \varphi(K)$, 那么 $H/N = K/N$ 。任取 $h \in H$, 存在 $k \in K$, 使得成立 $h * N = k * N$, 因此 $h \in k * N \subset K$, 进而 $H \subset K$ 。同理可得 $K \subset H$, 因此 $H = K$, 进而 φ 为单射。

最后证明 φ 的满射性。如果 $K < G/N$, 那么存在 $H_0 \subset G$, 使得成立 $K = \{h * N : h \in H_0\}$ 。任取 $g, h \in H_0$, 由于

$$(g * h^{-1}) * N = (g * N) \bullet (h^{-1} * N) = (g * N) \bullet (h * N)^{-1} \in K$$

因此 $g * h^{-1} \in H_0$, 进而 $H_0 < G$ 。记 $H = \langle H_0 \cup N \rangle$, 那么 $N \subset H < G$ 。任取 $h = g_1 * \cdots * g_n \in H$, 其中对于任意 $1 \leq k \leq n$, 成立 $g_k \in H_0$ 或 $g_k \in N$ 。不妨 $n = 2m$, 且当 k 为奇数时, $g_k = h_{\frac{k+1}{2}} \in H_0$; 当 k 为偶数时, $g_k = n_{\frac{k}{2}} \in N$ 。考察 $h * N$

$$\begin{aligned} h * N &= (h_1 * n_1 * \cdots * h_{m-1} * n_{m-1} * h_m * n_m) * N \\ &= h_1 * n_1 * \cdots * h_{m-1} * n_{m-1} * h_m * n_m * N \\ &= h_1 * n_1 * \cdots * h_{m-1} * n_{m-1} * h_m * N \\ &= h_1 * n_1 * \cdots * h_{m-1} * n_{m-1} * N * h_m \\ &= \cdots \\ &= h_1 * n_1 * N * h_2 * \cdots * h_m \\ &= h_1 * N * h_2 * \cdots * h_m \\ &= N * h_1 * h_2 * \cdots * h_m \\ &= (h_1 * h_2 * \cdots * h_m) * N \end{aligned}$$

因此存在 $h_0 = h_1 * h_2 * \cdots * h_m \in H_0$, 使得成立 $h * N = h_0 * N \in K$, 进而 $H/N \subset K$ 。而显然 $K \subset H/N$, 因此 $K = H/N$, 进而 φ 为满射。

综上所述, 命题得证!

命题 2.7.15 (商群的正规子群)

如果 N 为群 $(G, *)$ 的正规子群, 那么如下集合函数为双射。

$$\begin{aligned} \varphi : \{M : N \subset M \triangleleft G\} &\longrightarrow \{L \triangleleft G/N\} \\ M &\longmapsto M/N \end{aligned}$$

证明 (优雅证明) 注意到如下自然群同态

$$\begin{aligned} \pi : G &\longrightarrow G/N \\ g &\longmapsto g * N \end{aligned}$$

其中 $\ker \pi = N$, 且 $\text{im } \pi = G/N$ 。由命题 2.7.8, 如下集合函数为双射。

$$\begin{aligned} \Psi : \{M : N \subset M \triangleleft G\} &\longrightarrow \{L \triangleleft G/N\} \\ M &\longmapsto \pi(M) \end{aligned}$$

注意到

$$\Phi(M) = M/N = \{m * N : m \in M\} = \pi(M) = \Psi(M)$$

因此 $\Phi = \Psi$, 进而 Φ 为双射。

(朴素证明) 首先证明 φ 的定义良好性。如果 $N \subset M \triangleleft G$, 那么任取 $m, n \in M$, 以及 $g \in G$, 因此 $m * n^{-1} \in M$,

且 $g * m * g^{-1} \in M$, 进而

$$(m * N) \bullet (n * N)^{-1} = (m * N) \bullet (n^{-1} * N) = (m * n^{-1}) * N \in M/N$$

$$(g * N) \bullet (m * N) \bullet (g * N)^{-1} = (g * m * g^{-1}) * N \in M/N$$

因此 M/N 为 G/N 的正规子群, 所以 φ 定义良好。

其次证明 φ 的单射性。如果 $\varphi(M) = \varphi(L)$, 那么 $M/N = L/N$ 。任取 $m \in M$, 存在 $l \in L$, 使得成立 $m * N = l * N$, 因此 $m \in l * N \subset L$, 进而 $M \subset L$ 。同理可得 $L \subset M$, 因此 $L = M$, 进而 φ 为单射。

最后证明 φ 的满射性。如果 $L \triangleleft G/N$, 那么存在 $M_0 \subset G$, 使得成立 $L = \{m * N : m \in M_0\}$ 。任取 $m, n \in M_0$, 以及 $g \in G$, 由于

$$(m * n^{-1}) * N = (m * N) \bullet (n^{-1} * N) = (m * N) \bullet (n * N)^{-1} \in L$$

$$(g * m * g^{-1}) * N = (g * N) \bullet (m * N) \bullet (g * N)^{-1} \in L$$

因此 $m * n^{-1} \in M_0$, 且 $g * m * g^{-1} \in M_0$, 进而 $M_0 \triangleleft G$ 。记 $M = [M_0 \cup N]$, 那么 $N \subset M \triangleleft G$ 。任取 $m = (g_1 * h_1 * g_1^{-1}) * \cdots * (g_n * h_n * g_n^{-1}) \in M$, 其中对于任意 $1 \leq i \leq n$, 成立 $g_i \in G$, 且 $h_i \in M_0$ 或 $h_i \in N$ 。不妨 $n = 2r$, 且当 i 为奇数时, $h_i = m_{i+1} \in M_0$; 当 i 为偶数时, $h_k = n_{\frac{k}{2}} \in N$ 。考察 $m * N$

$$\begin{aligned} m * N &= ((g_1 * m_1 * g_1^{-1}) * \cdots * (g_r * m_r * g_r^{-1}) * (g_r * n_r * g_r^{-1})) * N \\ &= g_1 * m_1 * g_1^{-1} * \cdots * g_r * m_r * g_r^{-1} * g_r * n_r * g_r^{-1} * N \\ &= g_1 * m_1 * g_1^{-1} * \cdots * g_r * m_r * g_r^{-1} * g_r * n_r * N * g_r^{-1} \\ &= g_1 * m_1 * g_1^{-1} * \cdots * g_r * m_r * g_r^{-1} * g_r * N * g_r^{-1} \\ &= g_1 * m_1 * g_1^{-1} * \cdots * g_r * m_r * g_r^{-1} * N \\ &= g_1 * m_1 * g_1^{-1} * \cdots * g_r * m_r * N * g_r^{-1} \\ &= g_1 * m_1 * g_1^{-1} * \cdots * g_r * N * m_r * g_r^{-1} \\ &= g_1 * m_1 * g_1^{-1} * \cdots * N * (g_r * m_r * g_r^{-1}) \\ &= \cdots \\ &= N * (g_1 * m_1 * g_1^{-1}) * \cdots * (g_r * m_r * g_r^{-1}) \\ &= (g_1 * m_1 * g_1^{-1}) * \cdots * (g_r * m_r * g_r^{-1}) * N \end{aligned}$$

因此存在 $m_0 = (g_1 * m_1 * g_1^{-1}) * \cdots * (g_r * m_r * g_r^{-1}) \in M_0$, 使得成立 $m * N = m_0 * N \in L$, 进而 $M/N \subset L$ 。而显然 $L \subset M/N$, 因此 $L = M/N$, 进而 φ 为满射。

2.7.5 核 \iff 正规子群

定理 2.7.2

N 是群 $(G, *)$ 的正规子群 \iff 存在群同态映射 $\varphi : G \rightarrow H$, 使得成立 $N = \ker \varphi$ 。



定理 2.7.3 (正规子群是群同态的核; 群同态的核是正规子群)

对于群 $(G, *)$ 的正规子群 N , 成立 $\ker \pi = N$, 其中 $\pi : G \twoheadrightarrow G/N$ 为满的群同态映射; 对于群同态映射 $\varphi : G \rightarrow H$, $\ker \varphi$ 为 G 的正规子群。因此:

核 \iff 正规子群



2.8 同构定理与 Lagrange 定理

2.8.1 同构定理

定理 2.8.1 (第一同构定理 first isomorphism theorem)

$$\varphi: G \rightarrow H \text{ 为群同态映射} \implies G/\ker \varphi \cong \operatorname{im} \varphi$$

定理 2.8.2 (第二同构定理 second isomorphism theorem)

$$H < G \text{ 且 } N \triangleleft G \implies N \triangleleft H * N < G \text{ 且 } (H \cap N) \triangleleft H \text{ 且 } \frac{H}{H \cap N} \cong \frac{H * N}{N}$$

定理 2.8.3 (第三同构定理 third isomorphism theorem)

$$N \subset H \text{ 且 } N, H \triangleleft G \implies \frac{H}{N} \triangleleft \frac{G}{N} \text{ 且 } \frac{G/N}{H/N} \cong \frac{G}{H}$$

2.8.2 正则分解

定理 2.8.4 (群同态映射的正则分解 canonical decomposition)

群同态映射 $\varphi: G \rightarrow H$ 的正则分解如下。

$$G \xrightarrow{g \mapsto g \ker \varphi} G/\ker \varphi \xrightarrow[\varphi: g \ker \varphi \mapsto \varphi(g)]{\sim} \operatorname{im} \varphi \xrightarrow[\varphi(g) \mapsto \varphi(g)]{\hookrightarrow} H$$

φ

定理 2.8.5 (第一同构定理 first isomorphism theorem)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$G/\ker \varphi \cong \operatorname{im} \varphi$$

推论 2.8.1

如果 $N_1 \subset G_1$ 和 $N_2 \subset G_2$ 是正规子群, 那么 $N_1 \times N_2 \subset G_1 \times G_2$ 是正规子群, 且

$$\frac{G_1 \times G_2}{N_1 \times N_2} \cong \frac{G_1}{N_1} \times \frac{G_2}{N_2}$$

命题 2.8.1 (群第一同构定理的推广)

对于群同态映射 $\varphi: G \rightarrow H$, 如果 N 为 G 的正规子群, 那么

$$\frac{G}{\ker \varphi * N} \cong \frac{\operatorname{im} \varphi}{\varphi(N)}$$

证明 (优雅证明) 注意到 $\varphi(\ker \varphi * N) = \varphi(N)$, 由命题 2.8.2

$$\frac{G}{\ker \varphi * N} \cong \frac{\operatorname{im} \varphi}{\varphi(\ker \varphi * N)} = \frac{\operatorname{im} \varphi}{\varphi(N)}$$

(朴素证明) 定义映射

$$\begin{aligned} f : G &\longrightarrow \frac{\text{im } \varphi}{\varphi(N)} \\ g &\longmapsto \varphi(g) * \varphi(N) \end{aligned}$$

首先证明 f 为群同态映射, 注意到

$$f(g * h) = \varphi(g * h) * \varphi(N) = (\varphi(g) * \varphi(N)) \bullet (\varphi(h) * \varphi(N)) = f(g) \bullet f(h)$$

其次证明 $\ker f = \ker \varphi * N$, 注意到

$$\begin{aligned} g \in \ker f &\iff f(g) = \varphi(N) \iff \varphi(g) * \varphi(N) = \varphi(N) \\ &\iff \varphi(g) \in \varphi(N) \iff \exists n \in N, \varphi(g) = \varphi(n) \iff \exists n \in N, g * n^{-1} \in \ker \varphi \\ &\iff \exists n \in N, g \in \ker \varphi * n \iff g \in \ker \varphi * N \end{aligned}$$

最后证明 $\text{im } f = \text{im } \varphi / \varphi(N)$, 这是显然的。

综上所述, 由群同构第一定理 2.8.1

$$\frac{G}{\ker \varphi * N} \cong \frac{\text{im } \varphi}{\varphi(N)}$$

命题 2.8.2 (群第一同构定理的推广)

对于群同态映射 $\varphi : G \rightarrow H$, 如果 $N \supset \ker \varphi$ 为 G 的正规子群, 那么

$$\frac{G}{N} \cong \frac{\text{im } \varphi}{\varphi(N)}$$

证明 (优雅证明) 由于 $N \supset \ker \varphi$ 为 G 的子群, 那么由命题 2.7.7, 存在 G 的正规子群 M , 使得成立 $N = \ker \varphi * M$ 。此时, $\varphi(N) = \varphi(\ker \varphi * M) = \varphi(M)$ 。由命题 2.8.1

$$\frac{G}{N} = \frac{G}{\ker \varphi * M} \cong \frac{\text{im } \varphi}{\varphi(M)} = \frac{\text{im } \varphi}{\varphi(N)}$$

(朴素证明) 定义映射

$$\begin{aligned} f : G &\longrightarrow \frac{\text{im } \varphi}{\varphi(N)} \\ g &\longmapsto \varphi(g) * \varphi(N) \end{aligned}$$

首先证明 f 为群同态映射, 注意到

$$f(g * h) = \varphi(g * h) * \varphi(N) = (\varphi(g) * \varphi(N)) \bullet (\varphi(h) * \varphi(N)) = f(g) \bullet f(h)$$

其次证明 $\ker f = N$, 注意到

$$\begin{aligned} g \in \ker f &\iff f(g) = \varphi(N) \iff \varphi(g) * \varphi(N) = \varphi(N) \\ &\iff \varphi(g) \in \varphi(N) \iff \exists n \in N, \varphi(g) = \varphi(n) \iff \exists n \in N, g * n^{-1} \in \ker \varphi \\ &\iff \exists n \in N, g \in \ker \varphi * n \iff g \in \ker \varphi * N = N \end{aligned}$$

最后证明 $\text{im } f = \text{im } \varphi / \varphi(N)$, 这是显然的。

综上所述, 由群同构第一定理 2.8.1

$$\frac{G}{N} \cong \frac{\text{im } \varphi}{\varphi(N)}$$

2.8.3 表示

定义 2.8.1 (表示 presentation)

群 $(G, *)$ 的表示为同构 $G \cong F(S)/\ker \rho$, 其中 $\rho: F(S) \twoheadrightarrow G$ 。



定义 2.8.2 (表示 presentation)

对于 \mathbb{C} 上的有限维向量空间 V , 记线性映射群 $\text{GL}(V) = \{\text{可逆线性映射 } f: V \rightarrow V\}$, 定义有限群 $(G, *)$ 的表示是群同态映射 $\varphi: G \rightarrow \text{GL}(V)$ 。



2.8.4 第三同构定理

定理 2.8.6 (第三同构定理 third isomorphism theorem)

如果 $N \triangleleft G$, 且 $N < H < G$, 那么 $H \triangleleft G \iff H/N \triangleleft G/N$, 此时成立

$$\frac{G/N}{H/N} \cong \frac{G}{H}$$



2.8.5 第二同构定理

定理 2.8.7 (第二同构定理 second isomorphism theorem)

如果 $H < G$, 且 $N \triangleleft G$, 那么 $N \triangleleft H * N < G$, 且 $(H \cap N) \triangleleft H$, 同时成立

$$\frac{H}{H \cap N} \cong \frac{H * N}{N}$$



2.8.6 Lagrange 定理

定义 2.8.3 (指数 index)

定义群 $(G, *)$ 的子群 H 的指数为 $[G : H] = |G/H|$ 。



引理 2.8.1

对于群 $(G, *)$ 的子群 $(H, *)$, 以及任意 $g \in G$, 如下映射为双射。

$$\begin{aligned} H &\rightarrow g * H, & h &\mapsto g * h \\ H &\rightarrow H * g, & h &\mapsto h * g \end{aligned}$$



定理 2.8.8 (Lagrange 定理)

对于群 $(G, *)$ 的子群 $(H, *)$, 如果 $|G| < \infty$, 那么 $|G| = [G : H]|H|$ 。



推论 2.8.2 (元素阶为群阶的因子)

对于任意 $g \in G$, 成立 $|p| \mid |G|$ 。



推论 2.8.3 (素数阶群为循环群)

素数阶群为循环群。



命题 2.8.3

对于有限交换群 $(G, *)$, 如果 $|G|$ 为奇数, 那么对于任意 $g \in G$, 存在 $h \in G$, 使得成立 $h^2 = g$ 。

命题 2.8.4

对于群 $(G, *)$, 记 $n = |G| < \infty$, 如果 $\gcd(n, k) = 1$, 那么对于任意 $g \in G$, 存在 $h \in G$, 使得成立 $h^k = g$ 。

命题 2.8.5

$2n$ 阶 Abel 群存在且存在唯一 2 阶元, 其中 n 为奇数。

证明 首先证明偶数阶群 G 存在 2 阶元。反证, 如果 G 不存在 2 阶元, 那么对于任意元素 $a \in G \setminus \{e\}$, $a^2 \neq e$, 而存在 $b \in G \setminus \{e\}$, 使得 $a * b = e$, 因此使得互为逆元的元素成对出现, 而由于群 G 的阶为偶数, 那么 $G \setminus \{e\}$ 的阶为奇数, 矛盾! 因此 G 存在 2 阶元。

其次证明 2 阶元唯一。若存在不同的 2 阶元 a, b , 考虑生成子群

$$\langle a, b \rangle = \{e, a, b, ab\}$$

由 Lagrange 定理 2.8.8, 可得 $4 \mid 2n$, 矛盾!

命题 2.8.6

对于有限 Abel 群 G , 如果 p 为 $|G|$ 的因子, 那么 G 存在 p 阶子群。

命题 2.8.7

对于群 $(G, *)$ 的有限子群 H 和 K , 成立

$$|H * K| = \frac{|H||K|}{|H \cap K|}$$

证明 任取 $a, b \in H \cap K$, 那么 $a, b \in H$ 且 $a, b \in K$, 因此 $a * b^{-1} \in H$ 且 $a * b^{-1} \in K$, 于是 $a * b^{-1} \in H \cap K$, 进而 $H \cap K \leq H$ 。

定义等价关系 $a \sim b \iff a^{-1} * b \in H \cap K$, 那么 $[H : H \cap K] = |H / \sim|$ 。记 $H / \sim = \{h_1, \dots, h_r\}$, 下面证明

$$H * K = \bigcup_{k=1}^r h_k K$$

首先证明不交性, 任取 $i \neq j \in \{1, \dots, r\}$, 若 $h_i K \cap h_j K \neq \emptyset$, 令 $a \in h_i K \cap h_j K$, 那么 $a \in h_i K$ 且 $a \in h_j K$, 于是存在 $k_i, k_j \in K$, 使得成立 $a = h_i * k_i = h_j * k_j$, 于是 $h_i^{-1} * h_j = k_i * k_j^{-1} \in K$, 因此 $h_i^{-1} * h_j \in H \cap K$, 进而 $h_i \sim h_j$, 矛盾!

其次证明等式, 任取 $h \in H, k \in K$, 存在 $i \in \{1, \dots, r\}$, 使得成立 $h \sim h_i$, 那么 $h_i^{-1} * h \in H \cap K$, 因此 $h_i^{-1} * h \in K$, 于是存在 $k_h \in K$, 使得成立 $h = h_i * k_h$, 于是 $h * k = h_i * (k_h * k) \in h_i K$, 于是 $H * K \subset \bigcup_{k=1}^r h_k K$ 。

$H * K \supset \bigcup_{k=1}^r h_k K$ 显然, 于是 $H * K = \bigcup_{k=1}^r h_k K$ 。

由 Lagrange 定理 2.8.8

$$|H * K| = |K| |H / \sim| = |K| [H : H \cap K] = \frac{|H||K|}{|H \cap K|}$$

2.8.7 余核与余像

定义 2.8.4 (余核 co-kernel)

定义群同态映射 $\varphi: G \rightarrow H$ 的余核为

$$\text{coker } \varphi = H / \text{im } \varphi$$



定义 2.8.5 (余像 co-image)

定义群同态映射 $\varphi: G \rightarrow H$ 的余像为

$$\text{cokim } \varphi = G / \ker \varphi$$



2.9 群作用

2.9.1 作用

定义 2.9.1 (群作用 group action)

定义群 $(G, *)$ 关于范畴 \mathbf{C} 中的对象 S 的作用为群同态映射 $\Psi: G \rightarrow \text{Aut}_{\mathbf{C}}(S)$ 。



定义 2.9.2 (忠实的 faithful / 有效的 effective)

称群 $(G, *)$ 关于范畴 \mathbf{C} 中的对象 S 的作用 $\Psi: G \rightarrow \text{Aut}_{\mathbf{C}}(S)$ 为忠诚的/有效的, 如果 Ψ 是单态射。



2.9.2 集合作用

定义 2.9.3 (关于集合的作用)

定义群 $(G, *)$ 关于集合 S 的作用为集合函数 $\bullet: G \times S \rightarrow S$, 其中

$$e \bullet s = s, \quad (g * h) \bullet s = g \bullet (h \bullet s)$$



定义 2.9.4 (关于集合的作用的一般性)

群作用 \iff 群同态映射

- 如果 $\bullet: G \times S \rightarrow S$ 为群 $(G, *)$ 关于集合 S 的作用, 那么可定义群同态映射 $\Psi: G \rightarrow \text{Aut}_{\text{Set}}(S)$, $g \mapsto \psi_g$, 其中集合函数 $\psi_g: S \rightarrow S$, $s \mapsto g \bullet s$ 。
- 如果 $\Psi: G \rightarrow \text{Aut}_{\text{Set}}(S)$, $g \mapsto \psi_g$ 为群同态映射, 那么可定义群 $(G, *)$ 关于集合 S 的作用 $\bullet: G \times S \rightarrow S$, $(g, s) \mapsto \psi_g(s)$ 。



定义 2.9.5 (作用的核)

定义群 $(G, *)$ 关于集合 S 的作用 $\bullet: G \times S \rightarrow S$ 的核 $\ker \bullet$ 为群同态映射 $\Psi: G \rightarrow \text{Aut}_{\text{Set}}(S)$, $g \mapsto \psi_g$ 的核 $\ker \Psi$, 其中集合函数 $\psi_g: S \rightarrow S$, $s \mapsto g \bullet s$, 换言之

$$\ker \bullet = \ker \Psi = \{g \in G: \psi_g = \mathbb{1}_S\} = \{g \in G: g \bullet s = s, \forall s \in S\}$$



定义 2.9.6 (忠实的 faithful / 有效的 effective)

称群 $(G, *)$ 关于集合 S 的作用 $\bullet : G \times S \rightarrow S$ 为忠诚的/有效的, 如果成立如下命题之一。

1. \bullet 是单的。
2. 作用 $\bullet : G \times S \rightarrow S$ 对应的群同态映射 $\Psi : G \rightarrow \text{Aut}_{\text{Set}}(S)$, $g \mapsto \psi_g$ 为单态射, 其中集合函数 $\psi_g : S \rightarrow S$, $s \mapsto g \bullet s$ 。
3. $\ker \bullet = \ker \Psi = \{e\}$
4. $\{g \in G : g \bullet s = s, \forall s \in S\} = \{e\}$

**定义 2.9.7 (可传递作用 transitive action)**

称群 $(G, *)$ 关于集合 S 的作用 $\bullet : G \times S \rightarrow S$ 为可传递的, 如果对于任意 $s, t \in S$, 存在 $g \in G$, 使得成立 $t = g \bullet s$ 。

**定义 2.9.8 (关于群的左作用)**

群 $(G, *)$ 关于集合 G 的忠实的左作用为 $(g, g) \mapsto g * g$ 。

**定义 2.9.9 (关于群的右作用)**

群 $(G, *)$ 关于集合 G 的忠实的右作用为 $(g, g) \mapsto g * g$ 。

**定义 2.9.10 (关于左商集的左作用)**

群 $(G, *)$ 关于左商集 $(G/H)_L$ 的左作用为 $(g, g * H) \mapsto (g * g) * H$ 。

**定义 2.9.11 (关于右商集的右作用)**

群 $(G, *)$ 关于右商集 $(G/H)_R$ 的右作用为 $(g, H * g) \mapsto H * (g * g)$ 。

**定义 2.9.12 (关于群的共轭作用 conjugation action)**

群 $(G, *)$ 关于集合 G 的共轭作用为 $(g, g) \mapsto g * g * g^{-1}$ 。

**定义 2.9.13 (关于幂集的共轭作用 conjugation action)**

群 $(G, *)$ 关于幂集 $\mathcal{P}(G)$ 的共轭作用为 $(g, S) \mapsto g * S * g^{-1}$ 。

**定理 2.9.1 (Cayley 定理)**

群同构于对称群的子群。



证明 给定群 $(G, *)$, 可诱导忠实作用, 即群同态映射 $\Psi : G \rightarrow \text{Aut}_{\text{Set}}(G)$, $g \mapsto \psi_g$, 其中集合函数 $\psi_g : G \rightarrow G$, $g \mapsto g * g$ 。由于 Ψ 为单态射, 那么 $G \cong \text{im } \Psi < \text{Aut}_{\text{Set}}(G)$ 。

命题 2.9.1

对于群 $(G, *)$ 在非平凡集合 S 上的可传递作用 $\bullet : G \times S \rightarrow S$, 存在 $g \in G$, 使得对于任意 $s \in S$, 成立 $g \bullet s \neq s$ 。



2.9.3 轨道-稳定化子定理与范畴 $G\text{-Set}$

定义 2.9.14 (轨道 orbit)

对于群 $(G, *)$ 关于集合 S 的作用 $\bullet: G \times S \rightarrow S$, 定义 $s \in S$ 的轨道为

$$\text{Orb}_G(s) = \{g \bullet s : g \in G\}$$



定义 2.9.15 (稳定化子 stabilizer)

对于群 $(G, *)$ 关于集合 S 的作用 $\bullet: G \times S \rightarrow S$, 定义 $s \in S$ 的稳定化子为

$$\text{Stab}_G(s) = \{g \in G : g \bullet s = s\}$$



命题 2.9.2 (轨道的不变性)

如果群 $(G, *)$ 在集合 S 上存在作用 $\bullet: G \times S \rightarrow S$, 那么对于任意 $s, t \in S$, 成立或 $\text{Orb}_G(s) = \text{Orb}_G(t)$, 或 $\text{Orb}_G(s) \cap \text{Orb}_G(t) = \emptyset$.



命题 2.9.3 (稳定化子为子群)

如果群 $(G, *)$ 在集合 S 上存在作用 $\bullet: G \times S \rightarrow S$, 那么对于任意 $s \in S$, $\text{Stab}_G(s)$ 为 G 的子群。



定理 2.9.2 (轨道-稳定化子定理 orbital-stabilizer theorem)

对于群 $(G, *)$ 关于集合 S 的作用 $\bullet: G \times S \rightarrow S$, 以及任意 $s \in S$, 存在双射

$$\varphi: (G/\text{Stab}_G(s))_L \longrightarrow \text{Orb}_G(s)$$

$$g * \text{Stab}_G(s) \longmapsto g \bullet s$$

特别的, 对于有限群 $(G, *)$, 成立

$$|G| = |\text{Stab}_G(s)| |\text{Orb}_G(s)|$$



命题 2.9.4

如果群 $(G, *)$ 在集合 S 上存在作用 $\bullet: G \times S \rightarrow S$, 那么对于 $s, t \in S$, 以及 $g \in G$, 成立

$$t = g \bullet s \implies \text{Stab}_G(t) = g * \text{Stab}_G(s) * g^{-1}$$

定义 2.9.16 (范畴 $G\text{-Set}$)

1. 对象: (\bullet, S) , 其中 $\bullet: G \times S \rightarrow S$ 为群 $(G, *)$ 关于集合 S 的作用。
2. 态射: $(\square, S) \rightarrow (\triangle, T)$ 的态射定义为集合函数 $\varphi: S \rightarrow T$, 满足 $\square \circ \varphi = (\mathbb{1}_G \times \varphi) \circ \triangle$, 交换图如下。

$$\begin{array}{ccc} G \times S & \xrightarrow{\mathbb{1}_G \times \varphi} & G \times T \\ \square \downarrow & & \downarrow \triangle \\ S & \xrightarrow{\varphi} & T \end{array}$$



2.10 范畴中的群对象

2.10.1 范畴论的观点

定义 2.10.1 (群对象 group object)

对于存在有限积和终止对象 1 的范畴 \mathcal{C} , 称 $(G, *, e, i)$ 为范畴 \mathcal{C} 的群对象, 其中 G 为范畴 \mathcal{C} 的对象, $*$: $G \times G \rightarrow G$, $e : 1 \rightarrow G$, 以及 $i : G \rightarrow G$ 为范畴 \mathcal{C} 的态射, 且使得如下交换图成立。

$$\begin{array}{ccc}
 (G \times G) \times G & \xrightarrow{* \times 1_G} & G \times G \\
 \cong \downarrow & & \downarrow * \\
 G \times (G \times G) & \xrightarrow{1_G \times *} & G \\
 \\
 1 \times G & \xrightarrow{e \times 1_G} & G \times G \\
 \searrow \cong & & \downarrow * \\
 & & G \\
 \\
 G & \xrightarrow{1_G \times 1_G} G \times G \xrightarrow{1_G \times i} & G \times G \\
 \downarrow & & \downarrow * \\
 1 & \xrightarrow{e} & G \\
 \\
 G & \xrightarrow{1_G \times 1_G} G \times G \xrightarrow{i \times 1_G} & G \times G \\
 \downarrow & & \downarrow * \\
 1 & \xrightarrow{e} & G
 \end{array}$$



第三章 群论 II

3.1 共轭作用

3.1.1 集合上的群作用

定义 3.1.1 (作用 action)

定义群 $(G, *)$ 关于集合 S 的作用为集合函数 $\bullet : G \times S \rightarrow S$, 其中

$$e \bullet s = s, \quad (g * h) \bullet s = g \bullet (h \bullet s)$$



定理 3.1.1 (作用的本质)

群作用 \iff 群同态映射

- 如果 $\bullet : G \times S \rightarrow S$ 为群 $(G, *)$ 关于集合 S 的作用, 那么可定义群同态映射 $\Psi : G \rightarrow \text{Aut}_{\text{Set}}(S)$, $g \mapsto \psi_g$, 其中集合函数 $\psi_g : S \rightarrow S$, $s \mapsto g \bullet s$.
- 如果 $\Psi : G \rightarrow \text{Aut}_{\text{Set}}(S)$, $g \mapsto \psi_g$ 为群同态映射, 那么可定义群 $(G, *)$ 关于集合 S 的作用 $\bullet : G \times S \rightarrow S$, $(g, s) \mapsto \psi_g(s)$.



定义 3.1.2 (作用的核)

定义群 $(G, *)$ 关于集合 S 的作用 $\bullet : G \times S \rightarrow S$ 的核 $\ker \bullet$ 为群同态映射 $\Psi : G \rightarrow \text{Aut}_{\text{Set}}(S)$, $g \mapsto \psi_g$ 的核 $\ker \Psi$, 其中集合函数 $\psi_g : S \rightarrow S$, $s \mapsto g \bullet s$. 换言之

$$\ker \bullet = \ker \Psi = \{g \in G : \psi_g = \mathbb{1}_S\} = \{g \in G : g \bullet s = s, \forall s \in S\}$$



定义 3.1.3 (轨道 orbit)

对于群 $(G, *)$ 关于集合 S 的作用 $\bullet : G \times S \rightarrow S$, 定义 $s \in S$ 的轨道为

$$\text{Orb}_G(s) = \{g \bullet s : g \in G\}$$

事实上, 定义 S 上的等价关系 $s \sim t \iff \exists g \in G, \text{ s.t. } t = g \bullet s$, 那么 $[s]_{\sim} = \text{Orb}_G(s)$.



定义 3.1.4 (稳定化子 stabilizer)

对于群 $(G, *)$ 关于集合 S 的作用 $\bullet : G \times S \rightarrow S$, 定义 $s \in S$ 的稳定化子为

$$\text{Stab}_G(s) = \{g \in G : g \bullet s = s\}$$



定义 3.1.5 (不动点 fixed point)

对于群 $(G, *)$ 关于集合 S 的作用 $\bullet : G \times S \rightarrow S$, 定义 S 的不动点集为

$$\text{Fix}_G(S) = \{s \in S : g \bullet s = s, \forall g \in G\}$$



定义 3.1.6 (p -群)

对于素数 p , 称有限群 $(G, *)$ 为 p -群, 如果 $|G| = p^n$, 其中 $n \in \mathbb{N}^*$.



命题 3.1.1

$$s \in \text{Fix}_G(S) \iff \text{Stab}_G(s) = G \iff \text{Orb}_G(s) = \{s\}$$

命题 3.1.2

对于群 $(G, *)$ 关于有限集合 S 的作用 $\bullet : G \times S \rightarrow S$, 定义 S 上的等价关系 $s \sim t \iff \exists g \in G, \text{ s.t. } t = g \bullet s$, 成立

$$|S| = |\text{Fix}_G(S)| + \sum_{s \in (S \setminus \text{Fix}_G(S)) / \sim} |\text{Orb}_G(s)|$$

推论 3.1.1

对于 p -群 $(G, *)$ 关于有限集合 S 的作用 $\bullet : G \times S \rightarrow S$, 成立

$$|S| \equiv |\text{Fix}_G(S)| \pmod{p}$$

推论 3.1.2

对于 p -群 $(G, *)$, 如果 $|S| \not\equiv 0 \pmod{p}$, 那么群 $(G, *)$ 关于集合 S 的作用存在不动点。

3.1.2 关于群的共轭作用**定义 3.1.7 (关于群的共轭作用 conjugation action)**

定义群 $(G, *)$ 关于集合 G 的共轭作用为 $(g, g) \mapsto g * g * g^{-1}$ 。

定理 3.1.2 (群作用的本质)

群 $(G, *)$ 关于集合 G 的群共轭作用 $(g, g) \mapsto g * g * g^{-1}$ 对应的群同态映射为 $\Gamma : G \rightarrow \text{Aut}_{\text{Grp}}(G)$, $g \mapsto \gamma_g$, 其中群内自同构映射 $\gamma_g : G \rightarrow G$, $g \mapsto g * g * g^{-1}$ 为群内自同构映射。

定义 3.1.8 (中心 center)

定义 G 关于群 $(G, *)$ 的群共轭作用的不动点集为 G 的中心, 即 $\text{Cent}(G) = \{g \in G : g * g = g * g, \forall g \in G\}$ 。

定义 3.1.9 (共轭类 conjugacy class)

定义 $g \in G$ 关于群 $(G, *)$ 的群共轭作用的轨道为 g 的共轭类, 即 $\text{Conj}_G(g) = \{g * g * g^{-1} : g \in G\}$ 。

定义 3.1.10 (中心化子 centralizer)

定义 $g \in G$ 关于群 $(G, *)$ 的群共轭作用的稳定化子为 g 的中心化子, 即 $\text{Cent}_G(g) = \{g \in G : g * g = g * g\}$ 。

命题 3.1.3

对于奇数阶群 $(G, *)$, 如果 $g \in G$ 与 g^{-1} 共轭, 那么 $g = e$ 。

命题 3.1.4

$$N < \text{Cent}(G) \iff N \triangleleft G$$

命题 3.1.5

对于群 $(G, *)$ 的正规子群 N , 成立

$$N = \bigcup_{n \in N} \text{Conj}_G(n)$$

**命题 3.1.6 (中心的正规性)**

$$G/\text{Cent}(G) \cong \text{Inn}_{\text{Grp}}(G)$$



证明 考虑群同态映射 $\Gamma: G \rightarrow \text{Aut}_{\text{Grp}}(G)$, $g \mapsto \gamma_g$, 其中群内自同构映射 $\gamma_g: G \rightarrow G$, $g \mapsto g * g * g^{-1}$. 注意到 $\ker \Gamma = \text{Cent}(G) \triangleleft G$, $\text{im } \Gamma = \text{Inn}_{\text{Grp}}(G) = \{\gamma_g: G \rightarrow G: g \in G\}$. 由群同构定理 2.8.1, 成立 $G/\text{Cent}(G) \cong \text{Inn}_{\text{Grp}}(G)$.

命题 3.1.7

$$G/\text{Cent}(G) \text{ 为循环群} \iff \text{Inn}_{\text{Grp}}(G) \text{ 为循环群} \iff \text{Inn}_{\text{Grp}}(G) \text{ 为平凡的} \iff G \text{ 为 Abel 群}$$



证明 如果 G 是 Abel 群, 那么对于任意 $g \in G$, $\gamma_g = \mathbb{1}_G$, 因此 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群。

如果 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群, 那么显然 $\text{Inn}(G) = \{\mathbb{1}_G\} \cong \mathbb{Z}/1\mathbb{Z}$ 为循环群。

如果 $\text{Inn}(G)$ 为循环群, 那么存在 $g_0 \in G$, 使得对于任意 $g \in G$, 存在 $n \in \mathbb{Z}$, 使得成立 $\gamma_g = \underbrace{\gamma_{g_0} \circ \cdots \circ \gamma_{g_0}}_{n \text{ 个}}$,

因此对于任意 $g \in G$, 成立 $g * g * g^{-1} = g_0^n * g * g_0^{-n}$. 取 $g = g_0$, 可得 $g * g_0 = g_0 * g$, 因此 $\gamma_{g_0} = \mathbb{1}_G$, 于是对于任意 $g \in G$, $\gamma_g = \mathbb{1}_G$, 因此 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群。

如果 $\text{Inn}(G) = \{\mathbb{1}_G\}$ 为平凡群, 那么对于任意 $g \in G$, $\varphi(g) = \gamma_g = \mathbb{1}_G$, 因此对于任意 $g \in G$, 成立 $\gamma_g(g) = g$, 于是

$$g^{-1} * g * g = g \implies g * g = g * g$$

进而 G 为 Abel 群。

命题 3.1.8

对于素数 p 和 q , 如果 $|G| = pq$, 那么或 G 交换, 或 $\text{Cent}(G) = \{e\}$.



证明 由命题 3.1.6, $\text{Cent}(G) \triangleleft G$, 因此 $|\text{Cent}(G)| \in \{1, p, q, pq\}$.

如果 $|\text{Cent}(G)| = 1$, 那么 $\text{Cent}(G) = \{e\}$.

如果 $|\text{Cent}(G)| = p$, 那么 $|G/\text{Cent}(G)| = q$. 由命题 2.8.3, $G/\text{Cent}(G) \cong \mathbb{Z}/q\mathbb{Z}$. 由命题 3.1.7, $q = 1$, 矛盾! 因此 $|\text{Cent}(G)| \neq p$.

同理, $|\text{Cent}(G)| \neq q$.

如果 $|\text{Cent}(G)| = pq$, 那么 $G = \text{Cent}(G)$, 因此 G 为 Abel 群。

定理 3.1.3 (类公式 class formula)

对于有限群 $(G, *)$, 定义 G 上的等价关系 $g \sim h \iff \exists q \in G$, s.t. $g * q = h * q$, 成立

$$|G| = |\text{Cent}(G)| + \sum_{g \in (G \setminus \text{Cent}(G)) / \sim} [G : \text{Cent}_G(g)]$$

**推论 3.1.3**

非平凡 p -群存在非平凡中心。



3.1.3 关于幂集的共轭作用

定义 3.1.11 (关于幂集的共轭作用 conjugation action)

定义群 $(G, *)$ 关于幂集 $\mathcal{P}(G)$ 的共轭作用为 $(g, S) \mapsto g * S * g^{-1}$ 。



定理 3.1.4 (幂集作用的本质)

群 $(G, *)$ 关于幂集 $\mathcal{P}(G)$ 的共轭作用为 $(g, S) \mapsto g * S * g^{-1}$ 对应的群同态映射为 $\Psi : G \rightarrow \text{AutSet}(\mathcal{P}(G))$, $g \mapsto \psi_g$, 其中集合函数 $\psi_g : \mathcal{P}(G) \rightarrow \mathcal{P}(G)$, $S \mapsto g * S * g^{-1}$ 。



定义 3.1.12 (中心 center)

定义 $S \subset G$ 关于群 $(G, *)$ 的中心为 $\text{Cent}_G(S) = \{g \in G : g * s = s * g, \forall s \in S\}$ 。



定义 3.1.13 (共轭类 conjugacy class)

定义 $S \subset G$ 关于群 $(G, *)$ 的幂集共轭作用的轨道为 S 的共轭类, 即 $\text{Conj}_G(S) = \{g * S * g^{-1} : g \in G\}$ 。



定义 3.1.14 (正规化子 normalizer)

定义 $S \subset G$ 关于群 $(G, *)$ 的幂集共轭作用的稳定化子为 S 的正规化子, 即 $\text{Norm}_G(S) = \{g \in G : g * S = S * g\}$ 。



命题 3.1.9 (正规化子为正规子群)

如果 $H \subset G$ 为群 $(G, *)$ 的子群, 那么 $H \triangleleft \text{Norm}_G(H)$ 。



命题 3.1.10

$N \triangleleft G \iff \text{Norm}_G(N) = G \iff \text{Conj}_G(N) = \{N\}$ 。



命题 3.1.11

如果 $H \subset G$ 为有限群 $(G, *)$ 的子群, 那么 H 的共轭子群的个数为 $[G : \text{Norm}_G(H)]$ 。



推论 3.1.4

对于群 $(G, *)$ 的子群 $H \subset G$, 如果 $[G : H]$ 有限, 那么 $[G : H] = [G : \text{Norm}_G(H)][\text{Norm}_G(H) : H]$ 。



命题 3.1.12

对于 p -群 $(G, *)$, 如果 $N \subset G$ 为非平凡正规子群, 那么 $\{e\} \subsetneq N \cap \text{Cent}(G)$, 且 $p \mid |N \cap \text{Cent}(G)|$ 。



证明 考虑群 G 在集合 N 上的共轭作用 $\bullet : G \times N \rightarrow N$, $(g, n) \mapsto g * n * g^{-1}$, 其不动点为 $\text{Fix}_G(N) = \{n \in N : g * n = n * g, \forall g \in G\}$, 而群 G 的中心为 $\text{Cent}(G) = \{g \in G : g * g = g * g, \forall g \in G\}$, 因此 $\text{Fix}_G(N) = N \cap \text{Cent}(G)$ 。注意到 $|N \cap \text{Cent}(G)| \equiv |\text{Fix}_G(N)| \equiv |N| \equiv 0 \pmod{p}$, 而 $\{e\} \in N \cap \text{Cent}(G)$, 因此 $\{e\} \subsetneq N \cap \text{Cent}(G)$, 且 $p \mid |N \cap \text{Cent}(G)|$ 。

命题 3.1.13

对于 p -群 $(G, *)$, 如果 $N, M \triangleleft G$ 且 $N \leq M$, 那么存在 $L \triangleleft G$, 使得成立 $N < L < M$, 且 $[L : N] = p$ 。



证明 由群第三同构定理 2.8.3, $M/N \triangleleft G/N$ 。由 3.1.12, $p \mid |M/N \cap \text{Cent}(G/N)|$, 其中 $\text{Cent}(G/N) = \{g * N \in G/N : g * g * N = g * g * N, \forall g * N \in G/N\}$ 。由 Cauchy 定理, 群 $M/N \cap \text{Cent}(G/N)$ 存在 p 阶元 $g * N$, 那么群

$\text{Cent}(G/N)$ 存在 p 阶元 $g * N$, 此亦为商群 G/N 的 p 阶元, 同时也为商群 M/N 的 p 阶元。记 $L/N = \langle g * N \rangle$, 其中 $L = \langle g, n : n \in N \rangle$, 因此 $N < L$, 且 $[L : N] = |L/N| = p$ 。而 $L/N < M/N$, 因此 $L < M$ 。由于 $L/N < \text{Cent}(G/N)$, 那么由 3.1.6, $L/N \triangleleft G/N$ 。由群第三同构定理 2.8.3, $L \triangleleft G$ 。

推论 3.1.5

对于素数 p , 如果 $|G| = p^r$, 那么对于任意 $0 \leq k \leq r$, 存在 $N \triangleleft G$, 使得成立 $|N| = p^k$ 。

**命题 3.1.14**

对于有限群 $(G, *)$, 如果存在 $g_1, \dots, g_n \in G$, 使得成立 $G = \bigsqcup_{k=1}^n \text{Conj}_G(g_k)$, 且对于任意 $1 \leq i, j \leq n$, 成立 $g_i * g_j = g_j * g_i$, 那么 G 为 Abel 群。

**命题 3.1.15**

对于群 $(G, *)$, 如果 $[G : \text{Cent}(G)] = n$, 那么对于任意子集 $S \subset G$, S 的共轭子集数不多于 n 。

**命题 3.1.16**

对于有限群 $(G, *)$, 以及子群 $H \subset G$, 满足 $[G : H] = 2$ 。对于 $h \in H$, 记 $[h]_H = \{h * h * h^{-1} : h \in H\}$, $[h]_G = \{g * h * g^{-1} : g \in G\}$, 那么成立

$$\text{Cent}_G(h) \subset H \implies |[h]_G| = 2|[h]_H|$$

$$\text{Cent}_G(h) \not\subset H \implies [h]_G = [h]_H$$

**命题 3.1.17**

如果 H 为有限群 $(G, *)$ 的真子群, 那么 G 不为 H 的共轭子群的并。

**命题 3.1.18**

如果 H 为有限群 $(G, *)$ 的真子群, 那么存在 $g \in G$, 使得成立 $\text{Conj}_G(g) \cap H = \emptyset$ 。

**命题 3.1.19**

对于群 $(G, *)$ 的子群 H, K , 满足 $H \subset \text{Norm}_G(K)$, 定义函数 $\Psi : H \rightarrow \text{Aut}_{\text{Grp}}(K)$, $h \mapsto \psi_h$, 其中 $\psi_h : K \rightarrow K$, $k \mapsto h * k * h^{-1}$, 那么 Ψ 为群同态映射, 且 $\ker \Psi = H \cap \text{Cent}_G(K)$ 。

**命题 3.1.20**

对于有限群 $(G, *)$, 如果 p 为 $|G|$ 的最小素因子, 且 $\mathbb{Z}/p\mathbb{Z} \triangleleft G$, 那么 $\mathbb{Z}/p\mathbb{Z} \subset \text{Cent}(G)$ 。



3.2 Sylow 定理

3.2.1 Sylow p -子群

定义 3.2.1 (p -子群)

对于素数 p , 称群 $(G, *)$ 的子群 $(P, *)$ 为 p -子群, 如果 $|P| = p^n$, 其中 $n \in \mathbb{N}^*$ 。



定义 3.2.2 (Sylow p -子群)

对于素数 p , 称有限群 $(G, *)$ 的子群 $(P, *)$ 为 Sylow p -子群, 如果 $|G| = np^r$, 且 $|P| = p^r$, 其中 $\gcd(n, p) = 1$, 且 $r \in \mathbb{N}^*$.

**命题 3.2.1**

对于有限群 $(G, *)$, 记

$$N = \bigcap_{P \text{ 为 Sylow } p\text{-子群}} P$$

那么 N 为极大正规 p -子群。

**命题 3.2.2**

对于有限群 $(G, *)$ 的 Sylow p -子群 P , 如果 $H \subset \text{Norm}_G(P)$ 为 p -子群, 那么 $H \subset P$ 。

**命题 3.2.3**

如果 H 为有限群 $(G, *)$ 的非 Sylow p -子群, 那么存在 p -子群 P , 使得成立 $H \triangleleft P$, 且 $[P : H] = p$ 。

**命题 3.2.4**

对于有限群 $(G, *)$ 的 Sylow p -子群 P , 成立

$$\text{Norm}_G(\text{Norm}_G(P)) = P$$

**引理 3.2.1**

如果 P 为有限群 $(G, *)$ 的 p -子群, 那么

$$[\text{Norm}_G(P) : P] \equiv [G : P] \pmod{p}$$



证明 如果 P 为平凡子群, 那么 $\text{Norm}_G(P) = G$, 因此结论显然成立。

如果 P 为非平凡子群, 考虑群 P 在集合 $(G/P)_L$ 上的作用

$$\begin{aligned} \bullet : P \times (G/P)_L &\longrightarrow (G/P)_L \\ (p, g * P) &\longmapsto (p * g) * P \end{aligned}$$

注意到其不动点集为

$$\text{Fix}_P((G/P)_L) = \{g * P \in (G/P)_L : g * P = P * g\}$$

而 P 的正规化子为

$$\text{Norm}_G(P) = \{g \in G : g * P = P * g\}$$

因此 $\text{Fix}_P((G/P)_L) = \text{Norm}_G(P)/P$ 。进而

$$[G : P] \equiv |(G/P)_L| \equiv |\text{Fix}_P((G/P)_L)| \equiv |\text{Norm}_G(P)/P| = [\text{Norm}_G(P) : P] \pmod{p}$$

证明 因为 H 为非 Sylow p -子群, 那么 $p \nmid [G : H]$, 因此 $p \nmid [\text{Norm}_G(H) : H]$ 。由于 $H \triangleleft \text{Norm}_G(H)$, 因此考虑商群 $\text{Norm}_G(H)/H$ 。由于 $p \nmid |\text{Norm}_G(H)/H|$, 因此商群 $\text{Norm}_G(H)/H$ 存在 p 阶元 $g * H$ 。记 $\langle g * H \rangle = P/H$, 其中 $P = \langle g, h : h \in H \rangle$, 那么 $H < P$ 。而 $P < \text{Norm}_G(H)$, 因此 $H \triangleleft P$, 且 $[P : H] = |P/H| = |\langle g * H \rangle| = p$ 。

命题 3.2.5

对于有限群 $(G, *)$ 的 Sylow p -子群 P , 如果 $\text{Norm}_G(P) \subset H < G$, 那么

$$[G : H] \equiv 1 \pmod{p}$$



3.2.2 特征子群

定义 3.2.3 (特征子群 characteristic subgroup)

称群 $(G, *)$ 的子群 $(H, *)$ 为特征子群, 如果对于任意群同构映射 $\varphi: G \rightarrow G$, 成立 $\varphi(H) \subset H$ 。



定义 3.2.4 (导群为特征子群)

群的导群为特征子群



命题 3.2.6 (特征子群为正规子群)

群的特征子群为正规子群。



证明 取群内自同构映射即可。

$$\begin{aligned}\gamma_g: G &\longrightarrow G \\ g &\longmapsto g * g * g\end{aligned}$$

命题 3.2.7

对于群 $(G, *)$, 如果 $H \subset N \subset G$, 且 H 为 N 的特征子群, N 为 G 的正规子群, 那么 H 为 G 的正规子群。



命题 3.2.8

对于群 $(G, *)$ 与群 $(H, *)$, 如果 G 存在且存在唯一子群 N , 使得成立 $N \cong H$, 那么 N 为 G 的正规子群。



命题 3.2.9

如果 N 为有限群 $(G, *)$ 的正规子群, 且 $\gcd(|N|, |G/N|) = 1$, 那么 N 为 G 的特征子群。



命题 3.2.10

对于有限群 $(G, *)$ 的 Sylow p -子群 P , 如果 $P \triangleleft G$, 那么 P 为 G 的特征子群。



命题 3.2.11

对于有限群 $(G, *)$ 的 Sylow p -子群 P , 如果 $P \triangleleft N \triangleleft G$, 那么 $P \triangleleft G$ 。



3.2.3 幂零群

3.2.4 Cauchy 定理

定理 3.2.1 (Cauchy 定理)

对于有限群 $(G, *)$, 如果 p 为 $|G|$ 的素因子, 那么 G 存在 p 阶元。



证明 记 $S = \{ \{g_1, \dots, g_p\} : g_1 * \dots * g_p = e \}$, 那么 $|S| = |G|^{p-1}$, 因此 p 为 $|S|$ 的素因子。考虑 $\mathbb{Z}/p\mathbb{Z}$ 在集合 S 上的作用

$$\begin{aligned}\bullet: \quad \mathbb{Z}/p\mathbb{Z} \times S &\longrightarrow S \\ ([n]_p, \{g_1, \dots, g_p\}) &\longmapsto \{g_{n+1}, \dots, g_p, g_1, \dots, g_n\}\end{aligned}$$

那么由推论 3.1.1, $|\text{Fix}_{\mathbb{Z}/p\mathbb{Z}}(S)| \equiv |S| \equiv 0 \pmod{p}$ 。注意到 $\text{Fix}_{\mathbb{Z}/p\mathbb{Z}}(S)$ 中元素形式为 $\{g, \dots, g\}$, 而 $\{e, \dots, e\} \in \text{Fix}_{\mathbb{Z}/p\mathbb{Z}}(S)$, 且 $p \geq 2$, 那么存在 $g \neq e$, 使得成立 $\{g, \dots, g\} \in \text{Fix}_{\mathbb{Z}/p\mathbb{Z}}(S) \subset S$, 因此 $g^n = e$ 。

推论 3.2.1

对于有限群 $(G, *)$, 如果 p 为 $|G|$ 的素因子, 那么 G 的 p 阶元个数 n 成立 $n \equiv 1 \pmod{p}$.

**3.2.5 Sylow 第一定理****定理 3.2.2 (Sylow 第一定理——存在性定理)**

对于有限群 $(G, *)$, 如果 p 为 $|G|$ 的素因子, 且 $p^k \mid |G|$, 那么群 $(G, *)$ 存在 p^k 阶群。



证明 如果 $k = 0$, 那么结论显然。下面假设 $1 \leq k \leq r$ 。

对 $|G|$ 进行归纳。当 $|G| = p$ 时, 结论显然成立。

如果存在群 G 的真子群 H , 使得成立 $\gcd([G : H], p) = 1$, 那么 $p^k \mid |H|$, 由归纳假设, 群 H 存在 p^k 阶子群, 此亦为 G 的 p^k 阶子群。

如果对于任意群 G 的真子群 H , 成立 $p \mid [G : H]$ 。由类公式 3.1.3, $p \mid \text{Cent}(G)$, 那么由 Cauchy 定理 3.2.1, $\text{Cent}(G)$ 存在 p 阶元 g , 因此 $N = \langle g \rangle$ 为 $\text{Cent}(G)$ 的子群, 进而 N 为 $\text{Cent}(G)$ 的正规子群。

考虑商群 G/N , 注意到 $p^{k-1} \mid |G/N|$, 由归纳假设, G/N 存在 p^{k-1} 阶子群 P/N , 其中 P 为 G 的子群。此时 $|P| = |P/N||N| = p^k$ 。

引理 3.2.2

对于素数 p , 如果 $(n, p) = 1$, 那么对于任意 $0 \leq k \leq r$, 成立

$$p^{r-k} \mid C_{np^r}^{p^k}, \quad p^{r-k+1} \nmid C_{np^r}^{p^k}$$

**定理 3.2.3 (Sylow 第一定理——存在性定理)**

对于素数 p , 如果 $(n, p) = 1$, 那么对于任意 $0 \leq k \leq r$, np^r 阶群存在 p^k 阶子群。



证明 对于 np^r 阶群 $(G, *)$, 定义集合 $\Omega = \{S \subset G : |S| = p^k\} = \{S_i\}_{i=1}^{C_{np^r}^{p^k}}$, 定义群 G 在集合 Ω 上的作用 $\bullet : G \times \Omega \rightarrow \Omega, (g, S) = g * S$ 。

由轨道-稳定化子定理 2.9.2, $\Omega = \bigsqcup_{i=1}^m \text{Orb}_G(S_i)$, 因此 $|\Omega| = \sum_{i=1}^m |\text{Orb}_G(S_i)|$ 。因为 $|\Omega| = C_{np^r}^{p^k}$, 由引理 3.2.2, $p^{r-k+1} \nmid |\Omega|$, 因此 $p^{r-k+1} \nmid \sum_{i=1}^m |\text{Orb}_G(S_i)|$, 进而存在 $S_{i_0} \in \Omega$, 使得成立 $p^{r-k+1} \nmid |\text{Orb}_G(S_{i_0})|$ 。

由于 $|G| = |\text{Orb}_G(S_{i_0})||\text{Stab}_G(S_{i_0})|$, 从而 $|\text{Stab}_G(S_{i_0})| = p^k q \geq p^k$ 。而对于任意 $g \in \text{Stab}_G(S_{i_0})$, 成立 $g * S_{i_0} = S_{i_0}$, 于是对于任意 $s \in S_{i_0}$, 成立 $g * s \in S_{i_0}$, 从而 $\text{Stab}_G(S_{i_0}) * s \subset S_{i_0}$, 进而 $|\text{Stab}_G(S_{i_0})| = |\text{Stab}_G(S_{i_0}) * a| \leq |S_{i_0}| = p^k$ 。

综上所述, $|\text{Stab}_G(S_{i_0})| = p^k$ 。

3.2.6 Sylow 第二定理**定理 3.2.4 (Sylow 第二定理——包含定理)**

对于有限群 $(G, *)$, 如果 P 为 G 的 Sylow p -子群, H 为 G 的 p -子群, 那么存在 $g \in G$, 使得成立 $H \subset g * P * g^{-1}$ 。



证明 考虑群 $(H, *)$ 在集合 $(G/P)_L$ 上的作用 $\bullet : H \times (G/P)_L \rightarrow (G/P)_L, (h, g * P) = (h * g) * P$ 。由推论 3.1.1

$$|\text{Fix}_H((G/P)_L)| \equiv |(G/P)_L| \equiv n \not\equiv 0 \pmod{p}$$

从而存在 $g * P \in \text{Fix}_H((G/P)_L)$, 使得对于任意 $h \in H$, 成立

$$(h * g) * P = g * P \iff g^{-1} * h * g \in P \iff h \in g * P * g^{-1}$$

进而 $H \subset g * P * g^{-1}$ 。

推论 3.2.2

对于素数 p , 如果 P 为有限群 $(G, *)$ 的 Sylow p -子群, 那么

$$P \triangleleft G \iff G \text{ 存在且存在唯一 Sylow } p\text{-子群 } P$$



3.2.7 Sylow 第三定理

定理 3.2.5 (Sylow 第三定理——计数定理)

对于素数 p , 如果 $(n, p) = 1$, 那么 np^r 阶群 $(G, *)$ 的 Sylow p -子群数 N_p 成立 $N_p \equiv 1 \pmod{p}$, 且 $N_p \mid n$ 。



证明 由 Sylow 第二定理 3.2.4, G 的 Sylow p -子群 P 相互共轭, 因此 $N_p = [G : \text{Norm}_G(P)]$ 。又因为 $[G : P] = [G : \text{Norm}_G(P)][\text{Norm}_G(P) : P]$, 因此 $N_p \mid n$ 。而由引理 3.2.1, $[\text{Norm}_G(P) : P] \equiv [G : P] \pmod{p}$, 进而 $N_p \equiv 1 \pmod{p}$ 。

定理 3.2.6 (Sylow 第三定理——计数定理)

对于素数 p , 如果 $(n, p) = 1$, 那么 np^r 阶群的 p^r 阶子群数 N_p 成立 $N_p \equiv 1 \pmod{p}$, 且 $N_p \mid n$ 。



证明 对于 np^r 阶群 $(G, *)$, 考虑任意 Sylow p -子群 P 在集合 $\Omega = \{P < G : |P| = p^r\} = \{P_k\}_{k=1}^{N_p}$ 上的共轭作用

$$\begin{aligned} \bullet : P \times \Omega &\longrightarrow \Omega \\ (p, Q) &\longmapsto p * Q * p^{-1} \end{aligned}$$

注意到

$$\text{Fix}_P(\Omega) = \{Q \in \Omega : p * Q = Q * p, \forall p \in P\}$$

而

$$\text{Norm}_G(Q) = \{g \in G : g * Q = Q * g\}$$

因此

$$Q \in \text{Fix}_P(\Omega) \iff P < \text{Norm}_G(Q)$$

任取 $Q \in \text{Fix}_P(\Omega)$, 那么 $P < \text{Norm}_G(Q)$ 。因为 $Q \triangleleft \text{Norm}_G(Q)$, 而 Q 为 $\text{Norm}_G(Q)$ 的 Sylow p -子群, 所以 $\text{Norm}_G(Q)$ 存在且存在唯一 Sylow p -子群。又因为 P 为 $\text{Norm}_G(Q)$ 的 Sylow p -子群, 所以 $Q = P$, 从而 $\text{Fix}_P(\Omega) = \{P\}$, 进而由推论 3.1.1

$$N_p \equiv |\Omega| \equiv |\text{Fix}_P(\Omega)| \equiv 1 \pmod{p}$$

由于 P 的共轭子群个数为 $[G : \text{Norm}_G(P)]$, 因此 $N_p = [G : \text{Norm}_G(P)]$, 从而 $N_p \mid |G| = np^r$ 。而 $N_p \equiv 1 \pmod{p}$, 因此 $(N_p, p) = 1$, 进而 $N_p \mid n$ 。

3.2.8 应用

推论 3.2.3

对于有限群 $(G, *)$, 如果 p 为 $|G|$ 的素因子, 那么 G 的 p 阶元个数 n 成立 $n \equiv 1 \pmod{p}$ 。



推论 3.2.4

对于 n 阶群 $(G, *)$, 如果 p 为 n 的素因子, 且

$$\{m : m \mid n, n \equiv 1 \pmod{p}\} = \{1\}$$

那么 G 为单群。

**推论 3.2.5**

pqr 阶群为非单群, 其中 $p < q < r$ 为素数。

**推论 3.2.6**

对于互异素数 p, q , 如果 $m, n \in \mathbb{N}^*$, 且 $(p^m - 1)! < q^n$, 那么 $p^m q^n$ 阶群为非单群。



证明 对于 $p^m q^n$ 阶群 $|G| = p^m q^n$, 由 Sylow 第三定理 3.2.6, G 至多存在 p^k 个 Sylow p -子群, 其中 $0 \leq k \leq m$ 。如果 G 仅存在 1 个 Sylow p -子群, 那么该子群为非平凡正规子群。

如果 G 存在 p^k 个 Sylow p -子群, 其中 $1 \leq k \leq m$, 考虑群 $(G, *)$ 在集合 $\Omega = \{P < G : |P| = p^r\} = \{P_i\}_{i=1}^{p^i}$ 上的共轭作用

$$\begin{aligned} \bullet : G \times \Omega &\longrightarrow \Omega \\ (g, P) &\longmapsto g * P * g^{-1} \end{aligned}$$

其诱导群同态映射

$$\begin{aligned} \Psi : G &\longrightarrow \text{Aut}_{\text{Set}}(\Omega) \\ g &\longmapsto \psi_g \end{aligned}$$

其中集合函数

$$\begin{aligned} \psi_g : \Omega &\longrightarrow \Omega \\ P &\longmapsto g * P * g^{-1} \end{aligned}$$

由群同构定理 2.8.1, $G/\ker \Psi \cong \text{im } \Psi$ 。由于 $\text{im } \Psi < \text{Aut}_{\text{Set}}(\Omega)$, 因此 $|\text{im } \Psi| \leq p^k!$ 。- 如果 $\ker \Psi = \{e\}$, 那么 $|\text{im } \Psi| = |G|/|\ker \Psi| = |G| = p^m q^n > p^m! \geq p^k!$, 矛盾! 如果 $\ker \Psi = G$, 那么对于任意 $g \in G$, 成立 $\psi_g = 1$, 因此对于任意 $P \in \Omega$, 成立 $g * P = P * g$, 进而 $P \triangleleft G$ 。由 Sylow 第二定理, G 存在且存在唯一 Sylow p -子群, 矛盾! 进而 $\ker \Psi$ 为 G 的非平凡正规子群。

综上所述, $p^m q^n$ 阶群 G 为非单群。

推论 3.2.7 (pq 阶群的结构)

对于素数 p, q , 如果 $p < q$ 且 $p \nmid q-1$, 那么 pq 阶群 $(G, *)$ 成立 $G \cong \mathbb{Z}/pq\mathbb{Z}$ 。



证明 (法一) 由 Sylow 第三定理 3.2.6, G 存在且仅存在唯一 p 阶子群 H , 存在且存在唯一 q 阶子群 K 。由 3.2.2, $H, K \triangleleft G$ 。

考虑群 $(G, *)$ 在集合 H 上的共轭作用

$$\begin{aligned} \bullet : G \times H &\longrightarrow H \\ (g, h) &\longmapsto g * h * g^{-1} \end{aligned}$$

其诱导群同态

$$\begin{aligned} \Gamma : G &\longrightarrow \text{Inn}_{\text{Grp}}(H) \\ g &\longmapsto \gamma_g \end{aligned}$$

其中群自同构映射

$$\begin{aligned}\gamma_g : H &\longrightarrow H \\ h &\longmapsto g * h * g^{-1}\end{aligned}$$

由命题2.6.3, 命题3.1.6, 命题2.4.11, 命题2.4.10

$$\begin{aligned}\text{im } \Gamma &< \text{Inn}_{\text{Grp}}(G) \cong G/\text{Cent}(G) \\ \text{im } \Gamma &< \text{Inn}_{\text{Grp}}(G) \triangleleft \text{Aut}_{\text{Grp}}(H) \cong \text{Aut}_{\text{Grp}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}\end{aligned}$$

其中群 G 的中心 $\text{Cent}(G) = \{g \in G : g * g = g * g, \forall g \in G\}$ 。因此

$$|\text{im } \Gamma| \mid pq, \quad |\text{im } \Gamma| \mid (p-1) \implies |\text{im } \Gamma| = 1 \iff \text{im } \Gamma = \{1\} \iff H < \text{Cent}(G)$$

注意到 $p = |H| \mid |\text{Cent}(G)|$, 且 $|\text{Cent}(G)| \mid |G| = pq$, 因此

$$|\text{Cent}(G)| = p \text{ 或 } pq \iff |G/\text{Cent}(G)| = q \text{ 或 } 1 \iff G/\text{Cent}(G) \cong \mathbb{Z}/q\mathbb{Z} \text{ 或 } \mathbb{Z}/\mathbb{Z}$$

进而由命题3.1.7, G 为 Abel 群。

由 Cauchy 定理3.2.1, $H = \langle h \rangle$, $K = \langle k \rangle$ 。注意到 $h * k = k * h$, 且 $\gcd(|h|, |k|) = \gcd(p, q) = 1$, 因此由命题2.1.9, $|h * k| = |h||k| = pq$, 进而 $G = \langle h * k \rangle \cong \mathbb{Z}/pq\mathbb{Z}$ 。

(法二) 由 Sylow 第三定理3.2.6, G 存在且仅存在唯一 p 阶子群 H , 存在且存在唯一 q 阶子群 K , 且 $H \cap K = \{e\}$ 。由3.2.2, $H, K \triangleleft G$ 。

由2.8.3, $H \cong \mathbb{Z}/p\mathbb{Z}$ 且 $K \cong \mathbb{Z}/q\mathbb{Z}$ 。由 Cauchy 定理3.2.1, $H = \{h^i : 0 \leq i < p\}$, $K = \{k^j : 0 \leq j < q\}$ 。由于

$$h^i * k^j = h^k * k^l \implies h^{i-k} = k^{l-j} \in H \cap K = \{e\} \implies i = k, j = l$$

那么

$$G = \{h^i * k^j : 0 \leq i < p, 0 \leq j < q\}$$

由于 $K \triangleleft G$, 那么 $a * K * a^{-1} = K$, 由此定义群内自同构映射

$$\begin{aligned}\varphi : K &\longrightarrow K \\ x &\longmapsto h * x * h^{-1}\end{aligned}$$

由命题2.4.10, $\varphi \in \text{Aut}_{\text{Grp}}(K) \cong \mathbb{Z}/(q-1)\mathbb{Z}$, 因此 $\varphi^{q-1} = 1$ 。由于 $p \nmid q-1$, 那么 $\gcd(p, q-1) = 1$, 因此由命题2.2.1, 存在 a, b , 使得成立 $ap + b(q-1) = 1$ 。由于 $\varphi^p = 1$, 那么

$$\varphi = \varphi^{ap+b(q-1)} = (\varphi^p)^a \circ (\varphi^{q-1})^b = 1$$

因此 $h * k = k * h$ 。由命题2.1.9, $|h * k| = |h||k| = pq$, 进而 $G = \langle h * k \rangle \cong \mathbb{Z}/pq\mathbb{Z}$ 。

推论 3.2.8 ($2p$ 阶非交换群的结构)

如果 p 为奇素数, 那么 $2p$ 阶非交换群 $(G, *)$ 成立 $G \cong D_{2p}$ 。



证明 由 Sylow 第三定理3.2.6, G 存在且存在唯一 p 阶子群 $\langle y \rangle \triangleleft G$ 。又因为 G 为非交换群, 那么 G 不存在 $2p$ 阶元, 因此对于任意 $x \in G \setminus \langle y \rangle$, 成立 $|x| = 2$ 。

注意到 $|x * y * x^{-1}| = p$, 因此 $x * y * x^{-1} \in \langle y \rangle$, 进而存在 $0 \leq r < p$, 使得成立 $x * y * x^{-1} = y^r$. 由于

$$\begin{aligned} (y^r)^r &= (x * y * x^{-1})^r = x * y^r * x^{-1} = x^2 * y * x^{-2} = y \\ \implies y^{r^2-1} &= e \\ \iff p \mid (r^2 - 1) \\ \iff p \mid (r+1)(r-1) \\ \implies p \mid (r+1) \text{ 或 } p \mid (r-1) \\ \implies r = 1 \text{ 或 } r = p-1 \end{aligned}$$

那么若 $r = 1$, 则 $x * y = y * x$, 此时成立 $|x * y| = |x||y| = 2p$, 矛盾! 因此 $r = p-1$, 进而

$$\begin{aligned} x^2 &= y^p = e, \quad x * y = y^{p-1} * x \\ \iff x^2 &= y^p = x * y * x * y = e \\ \implies G &\cong D_p \end{aligned}$$

推论 3.2.9

对于 n 阶群 $(G, *)$, 对于任意 n 的素因子 p , 成立 $N_p! \mid n$, 其中 N_p 为 G 的 Sylow p -子群数。



推论 3.2.10

对于 n 阶群 $(G, *)$, 如果 G 为单群, H 为 G 的子群, 且 $[G : H] = m$, 那么 $m! \mid n$.



3.3 合成列与可解性

3.3.1 Jordan-Hölder 定理

定义 3.3.1 (子群列 subgroup series)

定义群 $(G, *)$ 的子群列为

$$G = G_0 \supsetneq G_1 \supsetneq \cdots$$



定义 3.3.2 (次正规列 subnormal series)

称群 $(G, *)$ 的子群列

$$G = G_0 \supsetneq G_1 \supsetneq \cdots$$

为次正规的, 如果对于任意 $n \in \mathbb{N}$, 成立 $G_{n+1} \triangleleft G_n$, 记作

$$G = G_0 \supsetneq G_1 \supsetneq \cdots$$



定义 3.3.3 (等价 equivalent)

称群 $(G, *)$ 的次正规列

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

$$G = G'_0 \supsetneq G'_1 \supsetneq \cdots \supsetneq G'_m = \{e\}$$

为等价的, 如果 $m = n$, 且存在双射 $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$, 使得对于任意 $1 \leq k \leq n$, 成立

$$\frac{G_{k-1}}{G_k} \cong \frac{G'_{\varphi(k-1)}}{G'_{\varphi(k)}}$$



定义 3.3.4 (合成列 composition series)

称群 $(G, *)$ 的次正规列

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

为合成列, 如果对于任意 $1 \leq k \leq n$, 商群 G_{k-1}/G_k 为单群。



定义 3.3.5 (合成因子 composition factor)

对于群 $(G, *)$ 的合成列

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

称 $\{G_{k-1}/G_k\}_{k=1}^n$ 为 G 的合成因子。



定义 3.3.6 (合成长度 (composition length))

定义群 $(G, *)$ 的合成列长度为合成长度 $\ell(G)$ 。



例题 3.1 \mathbb{Z} 存在任意长度的正规列。

命题 3.3.1 (有限群存在合成列)

有限群存在合成列。



命题 3.3.2

$$G \times H \text{ 存在合成列} \iff G, H \text{ 存在合成列}$$



定理 3.3.1 (Jordan-Hölder 定理)

群的合成列等价; 换言之如果

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

$$G = G'_0 \supsetneq G'_1 \supsetneq \cdots \supsetneq G'_m = \{e\}$$

为群 $(G, *)$ 的合成列, 那么 $m = n$, 且存在双射 $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$, 使得对于任意 $1 \leq k \leq n$, 成立

$$\frac{G_{k-1}}{G_k} \cong \frac{G'_{\varphi(k-1)}}{G'_{\varphi(k)}}$$



证明 (优雅证明) 由 3.3.2, 命题显然!

(朴素证明) 令

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

为群 $(G, *)$ 的合成列, 对 n 进行归纳。

如果 $n = 0$, 那么 $G = \{e\}$, 命题显然成立。

对于 $n \in \mathbb{N}^*$, 令

$$G = G'_0 \supsetneq G'_1 \supsetneq \cdots \supsetneq G'_m = \{e\}$$

为群 $(G, *)$ 的另一合成列, 如果 $G_1 = G'_1$, 那么由归纳假设, G_1 存在 $n-1$ 的合成列, 命题得证。

如果 $G_1 \neq G'_1$, 由命题 2.7.7, $G_1 * G'_1 \triangleleft G$. 由于 $G_1 \subset G_1 * G'_1$, 且商群 G/G_1 为单群, 那么 $G_1 * G'_1 = G_1$ 或 $G_1 * G'_1 = G$. 同理可得 $G_1 * G'_1 = G'_1$ 或 $G_1 * G'_1 = G$. 如果 $G_1 * G'_1 \subsetneq G$, 那么 $G_1 * G'_1 = G_1$ 且 $G_1 * G'_1 = G'_1$, 因此 $G_1 \subset G'_1$ 且 $G'_1 \subset G_1$, 进而 $G_1 = G'_1$, 矛盾! 因此 $G_1 * G'_1 = G$.

令 $K = G_1 \cap G'_1$, 其合成列为

$$K \supsetneq K_1 \supsetneq K_2 \supsetneq \cdots \supsetneq K_r = \{e\}$$

由群第二同构定理 2.8.2, 成立

$$\frac{G_1}{K} = \frac{G_1}{G_1 \cap G'_1} \cong \frac{G_1 * G'_1}{G'_1} = \frac{G}{G'_1}, \quad \frac{G'_1}{K} = \frac{G'_1}{G'_1 \cap G_1} \cong \frac{G'_1 * G_1}{G_1} = \frac{G}{G_1}$$

那么 G_1/K 与 G'_1/K 为单群, 进而群 G 成立两个新的合成列

$$G \supsetneq G_1 \supsetneq K \supsetneq K_1 \supsetneq K_2 \supsetneq \cdots \supsetneq K_r = \{e\}$$

$$G \supsetneq G'_1 \supsetneq K \supsetneq K_1 \supsetneq K_2 \supsetneq \cdots \supsetneq K_r = \{e\}$$

由于

$$G_1 \supsetneq K \supsetneq K_1 \supsetneq K_2 \supsetneq \cdots \supsetneq K_r = \{e\}$$

为 G_1 的合成列, 那么由归纳假设, G_1 的合成列为

$$G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

因此 $r = n - 2$. 同样的, 由于

$$G'_1 \supsetneq K \supsetneq K_1 \supsetneq K_2 \supsetneq \cdots \supsetneq K_{n-2} = \{e\}$$

为 G'_1 的合成列, 且 G'_1 的合成列长度为 $n - 1$, 那么由归纳假设, G'_1 的合成列

$$G'_1 \supsetneq \cdots \supsetneq G'_m = \{e\}$$

的长度为 $n - 1$, 因此 $m = n$.

命题 3.3.3

对于群 $(G, *)$, 如果 $N \triangleleft G$, 那么

$$G \text{ 存在合成列} \iff N \text{ 与 } G/N \text{ 存在合成列}$$

此时

$$\ell(G) = \ell(N) + \ell(G/N)$$

且

$$\{G \text{ 的合成因子}\} = \{N \text{ 的合成因子}\} \cup \{G/N \text{ 的合成因子}\}$$



3.3.2 Schreier 定理

定义 3.3.7 (精细 refinement)

称群 $(G, *)$ 的子群列 $G = G_0 \supsetneq G'_1 \supsetneq \cdots$ 为子群列 $G = G_0 \supsetneq G_1 \supsetneq \cdots$ 的精细, 如果 $\{G_n\} \subset \{G'_n\}$.



引理 3.3.1 (Zassenhaus-蝴蝶引理)

对于群 $(G, *)$ 的子群 A, A', B, B' , 如果 $A \triangleleft A'$ 且 $B \triangleleft B'$, 那么

$$A * (A' \cap B) \triangleleft A * (A' \cap B'), \quad B * (B' \cap A) \triangleleft B * (B' \cap A')$$

$$\frac{A * (A' \cap B')}{A * (A' \cap B)} \cong \frac{A' \cap B'}{(A' \cap B) * (A \cap B')} \cong \frac{(B' \cap A') * B}{(B' \cap A) * B}$$



定理 3.3.2 (Schreier 定理)

群的以 $\{e\}$ 结束的次正规列存在等价精细次正规列。



证明 (优雅证明) 将次正规列精细为合成列, 那么由 3.3.1, 命题得证!

(朴素证明) 对于群 $(G, *)$ 的次正规列

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

$$G = G'_0 \supsetneq G'_1 \supsetneq \cdots \supsetneq G'_m = \{e\}$$

定义

$$G_{i,j} = G_{i+1} * (G_i \cap G'_j), \quad 0 \leq i \leq n-1, 0 \leq j \leq m$$

$$G'_{i,j} = G'_{j+1} * (G_i \cap G'_j), \quad 0 \leq i \leq n, 0 \leq j \leq m-1$$

其中

$$G_{i,m} = G_{i+1,0} = G_{i+1}, \quad G_{n,j} = G_{0,j+1} = G'_{j+1}$$

由 3.3.1, 成立

$$\frac{G_{i,j}}{G_{i,j+1}} \cong \frac{G'_{i,j}}{G'_{i+1,j}}$$

即

$$G = G_{0,0} \supsetneq G_{0,1} \supsetneq \cdots \supsetneq G_{0,m} = G_{1,0} \supsetneq \cdots \supsetneq G_{n-1,0} \supsetneq \cdots \supsetneq G_{n-1,m} = \{e\}$$

$$G = G'_{0,0} \supsetneq G'_{0,1} \supsetneq \cdots \supsetneq G'_{0,m-1} = G'_{0,m} \supsetneq \cdots \supsetneq G'_{n,m-1} = \{e\}$$

为原次正规列的等价加细。

3.3.3 换位子群与可解性

定义 3.3.8 (单群 simple group)

称仅存在平凡正规子群的群为单群。



定义 3.3.9 (换位子 commutator)

对于群 $(G, *)$, 定义元素 $g, h \in G$ 的换位子为 $[g, h] = g * h * g^{-1} * h^{-1}$ 。



定义 3.3.10 (换位子群 commutator subgroup)

定义群 $(G, *)$ 的子群 H, K 的换位子群为

$$[H, K] = \langle h * k * h^{-1} * k^{-1} : h \in H, k \in K \rangle$$



定义 3.3.11 (换位子群 commutator subgroup)

定义群 $(G, *)$ 的换位子群为

$$[G, G] = \langle g * h * g^{-1} * h^{-1} : g, h \in G \rangle$$



例题 3.2 阶数最小的非交换单群为 A_5 , 其阶数为 60。阶数第二小的非交换单群的阶数为 168。

命题 3.3.4

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$\varphi([g, h]) = [\varphi(g), \varphi(h)], \quad \varphi([G, G]) \subset [\text{im } \varphi, \text{im } \varphi]$$



证明

$$\varphi([g, h]) = \varphi(g * h * g^{-1} * h^{-1}) = \varphi(g) * \varphi(h) * \varphi(g)^{-1} * \varphi(h)^{-1} = [\varphi(g), \varphi(h)] \in [\text{im } \varphi, \text{im } \varphi]$$

命题 3.3.5 (单的商群)

对于群 $(G, *)$ 的正规子群 N , 成立

$$G/N \text{ 为单群} \iff \text{若 } N \subset M \triangleleft G \text{ 则 } M = N \text{ 或 } M = G$$

证明 充分性显然! 对于必要性, 如果 G/N 为单群, 那么 G/N 的正规子群仅为 N/N 与 G/N , 而由命题 2.7.15, 必要性得证!

命题 3.3.6 (群的交换化)

对于群 $(G, *)$, $[G, G] \triangleleft G$, 且 $G/[G, G]$ 为交换群。

证明 任取 $g \in G, h \in [G, G]$, 注意到 $g * h * g^{-1} * h^{-1} \in [G, G]$, 因此 $g * h * g^{-1} \in [G, G] * h = [G, G]$, 进而 $[G, G]$ 为 G 的正规子群。

任取 $g, h \in G$, 那么

$$\begin{aligned} (g * [G, G]) \bullet (h * [G, G]) &= (g * h) * [G, G] = (g * h) * ((h^{-1} * g^{-1} * h * g) * [G, G]) \\ &= (g * h * h^{-1} * g^{-1} * h * g) * [G, G] = (h * g) * [G, G] = (h * [G, G]) \bullet (g * [G, G]) \end{aligned}$$

因此 $G/[G, G]$ 为 Abel 群。

命题 3.3.7 (群交换的等价条件)

对于群 $(G, *)$, 成立

$$G \text{ 为交换群} \iff [G, G] = \{e\}$$

证明 如果 G 为 Abel 群, 那么对于任意 $g, h \in G$, 成立 $[g, h] = e$, 因此 $[G, G] = \{e\}$ 。

如果 G 为非 Abel 群, 那么存在 $g, h \in G$, 成立 $[g, h] \neq e$, 因此 $[g, h] \in [G, G] \neq \{e\}$ 。

命题 3.3.8 (像交换的等价条件)

对于群同态映射 $\varphi: G \rightarrow H$, 成立

$$\text{im } \varphi \text{ 为 Abel 群} \iff [G, G] \subset \ker \varphi$$

证明

$\text{im } \varphi$ 为 Abel 群

$$\iff \forall g, h \in G, \varphi(g) * \varphi(h) = \varphi(h) * \varphi(g)$$

$$\iff \forall g, h \in G, \varphi(g * h * g^{-1} * h^{-1}) = e$$

$$\iff \forall g, h \in G, g * h * g^{-1} * h^{-1} \in \ker \varphi$$

$$\iff [G, G] \subset \ker \varphi$$

命题 3.3.9 (商群交换的等价条件)

如果 N 为群 $(G, *)$ 的正规子群, 那么

$$\frac{G}{N} \text{ 为 Abel 群} \iff [G, G] \subset N$$

证明

$$\begin{aligned}
 & G/N \text{ 为 Abel 群} \\
 \iff & \forall g, h \in G, (g * N) \bullet (h * N) = (h * N) \bullet (g * N) \\
 \iff & \forall g, h \in G, (g * h * g^{-1} * h^{-1}) * N = N \\
 \iff & \forall g, h \in G, g * h * g^{-1} * h^{-1} \in N \\
 \iff & [G, G] \subset \ker \varphi
 \end{aligned}$$

命题 3.3.10 (Abel 单群为素数阶群)

对于群 $(G, *)$, 成立

$$G \text{ 为 Abel 单群} \iff G \text{ 为素数阶群}$$



证明 充分性显然! 对于必要性, 如果 G 为 Abel 单群, 而 G 的子群为正规子群, 那么 G 仅存在平凡子群, 由 Lagrange 定理 2.8.8, G 为素数阶群。

命题 3.3.11

对于 p -群 $(G, *)$, 成立

$$G \text{ 为单群} \iff |G| = p$$



命题 3.3.12

如果 $(G, *)$ 为单群, $\varphi: G \rightarrow H$ 为非平凡群同态映射, 那么 φ 为单射。



命题 3.3.13 (换位子群的万有性质)

定义群 G 的换位群范畴为

1. 对象: $\{\alpha: G \rightarrow A \mid A \text{ 为交换群}\}$
2. 态射:

$$\begin{array}{ccc}
 & G & \\
 \alpha \swarrow & & \searrow \beta \\
 A & \xrightarrow{\varphi} & B
 \end{array}$$

那么该范畴的初始对象为自然群同态映射 $\pi: G \rightarrow G/[G, G]$; 换言之, 对于任意交换群 H 与群同态映射 $\varphi: G \rightarrow H$, 存在且存在唯一态射

$$\begin{array}{ccc}
 & G & \\
 \pi \swarrow & & \searrow \varphi \\
 G/[G, G] & \xrightarrow{\bar{\varphi}} & H
 \end{array}$$



证明 为使交换图成立, 可知

$$\begin{aligned}
 \bar{\varphi}: G/[G, G] &\longrightarrow H \\
 g * [G, G] &\longmapsto \varphi(g)
 \end{aligned}$$

只需证明定义良好性, 如果 $g * [G, G] = h * [G, G]$, 那么 $g * h^{-1} \in [G, G]$, 由命题 3.3.8, $g * h^{-1} \in \ker \varphi$, 因此 $\varphi(g) = \varphi(h)$ 。

定义 3.3.12 (导群列 derived groups series)

对于群 $(G, *)$, 定义 $G^{(1)} = [G, G]$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$, 可得次正规列

$$G \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots$$

**定义 3.3.13 (可解群 solvable group)**

称群 $(G, *)$ 为可解群, 如果存在 $n \in \mathbb{N}^*$, 使得成立 $G^{(n)} = \{e\}$ 。

**命题 3.3.14**

单的可解群为 Abel 群。



证明 如果群 $(G, *)$ 为单的可解群, 由 G 的可解性, $G' \neq G$, 而命题 3.3.6, $G' \triangleleft G$, 由 G 的单性, $G = \{e\}$, 由命题 3.3.7, G 为 Abel 群。

定义 3.3.14 (Abel 正规列 Abelian normal series)

称群 $(G, *)$ 的次正规列

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots$$

为 Abel 正规列, 如果对于任意 $n \in \mathbb{N}$, 商群 G_n/G_{n+1} 为 Abel 群。

**定义 3.3.15 (循环正规列 cyclic normal series)**

称群 $(G, *)$ 的次正规列

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots$$

为循环正规列, 如果对于任意 $n \in \mathbb{N}$, 商群 G_n/G_{n+1} 为循环群。

**定义 3.3.16 (中心正规列 central normal series)**

称群 $(G, *)$ 的次正规列

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots$$

为中心正规列, 如果对于任意 $n \in \mathbb{N}$, 成立 $G_n/G_{n+1} \subset \text{Cent}(G/G_{n+1})$ 。

**定义 3.3.17 (幂零群 nilpotent group)**

称群 $(G, *)$ 为幂零群, 如果其存在中心正规列。

**命题 3.3.15**

Abel 正规列的精细为 Abel 正规列。



证明 如果 $N \triangleleft G$ 且 G/N 为 Abel 群, 那么由命题 3.3.9, $[G, G] \subset N$ 。将 $N \triangleleft G$ 精细为 $N \triangleleft H \triangleleft G$, 那么由 $[G, G] \subset N \subset H$, 结合命题 3.3.9, G/H 为 Abel 群。而由命题 2.7.15, $H/N \triangleleft G/N$, 因此 H/N 为 Abel 群。综上所述, Abel 正规列 $N \triangleleft G$ 的精细 $N \triangleleft H \triangleleft G$ 为 Abel 正规列。

命题 3.3.16 (有限群可解的等价条件)

对于有限群 $(G, *)$, 如下命题等价。

1. G 的合成因子为循环群。
2. G 存在以 $\{e\}$ 结束的循环正规列。

3. G 存在以 $\{e\}$ 结束的 Abel 正规列。

4. G 为可解群。

证明 $1 \implies 2 \implies 3$ 显然! 由命题 3.3.6, $4 \implies 3$ 显然!

对于 $3 \implies 1$, 如果 G 存在以 $\{e\}$ 结束的 Abel 正规列, 那么将其精细为合成列, 由引理, 该合成列为 Abel 正规列。而由命题 3.3.10, G 的合成因子为素数阶群, 由命题 2.8.3, G 的合成因子为循环群。

对于 $3 \implies 4$, 如果 G 存在以 $\{e\}$ 结束的 Abel 正规列

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

由 G_k/G_{k+1} 为 Abel 群, 结合命题 3.3.9, 那么 $[G_k, G_k] \subset G_{k+1}$ 。由归纳法, 结合

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \subset [G_k, G_k] \subset G_{k+1}$$

那么 $G^{(k)} \subset G_k$ 。特别的, $G^{(n)} \subset G_n = \{e\}$, 因此 G 为可解群。

推论 3.3.1

如果 $|G| < 120$ 且 $|G| \neq 60$, 那么群 $(G, *)$ 可解。

推论 3.3.2 (p -群可解)

p -群可解。

证明 p -群的合成因子为 p 阶群, 由命题 2.8.3, 因而为循环群。

推论 3.3.3

p^2q 阶群可解, 其中 p, q 为素数。

推论 3.3.4

对于群 $(G, *)$ 的正规子群 N , 成立

$$G \text{ 可解} \iff N \text{ 与 } G/N \text{ 可解}$$

推论 3.3.5

如果 H 为可解群 $(G, *)$ 的非平凡正规子群, 那么 G 存在非平凡正规交换子群 K , 使得成立 $K \subset H$ 。

定理 3.3.3 (Burnside 定理)

$p^m q^n$ 阶群可解, 其中 p, q 为素数。

定理 3.3.4 (Feit-Thompson 定理)

奇数阶群可解。

命题 3.3.17

对于集合 S , 自由群 $F = F(S)$, Abel 群 $(G, *)$, 集合函数 $f: S \rightarrow G$, f 诱导了唯一一个群同态映射 $F/[F, F] \rightarrow G$, 且 $F/[F, F] \cong F^{\text{ab}}(S)$ 。

3.4 对称群

3.4.1 轮换

定义 3.4.1 (轮换 cycle)

义 n 元置换 $\sigma \in S_n$ 关于元素 a_1, \dots, a_r 的 r -轮换为

$$(a_1 \cdots a_r) = a_1 \mapsto a_2 \mapsto \cdots \mapsto a_r \mapsto a_1$$



例题 3.3

$$S_1 = \{1\}, \quad S_2 = \{1, (12)\}, \quad S_3 = \{1, (12), (13), (23), (123), (132)\}$$

$$\begin{aligned} S_4 = \{ & 1, (12), (13), (14), (23), (24), (34), \\ & (123), (124), (132), (134), (142), (143), (234), (243), \\ & (1234), (1243), (1324), (1342), (1423), (1432), \\ & (12)(34), (13)(24), (14)(23) \} \end{aligned}$$

定理 3.4.1 (轮换的本质)

定义 n 元置换 $\sigma \in S_n$, 考虑生成子群 $\langle \sigma \rangle$ 在集合 $\{1, \dots, n\}$ 上的作用

$$\begin{aligned} \bullet : \langle \sigma \rangle \times \{1, \dots, n\} &\longrightarrow \{1, \dots, n\} \\ (\sigma^m, k) &\longmapsto \sigma^m(k) \end{aligned}$$

那么 k 的轨道为

$$\text{Orb}_{\langle \sigma \rangle}(k) = \{\sigma^m(k) : m \in \mathbb{N}\}$$

此即为 k 所在轮换。



引理 3.4.1 (轮换分解)

非平凡置换在置换顺序下存在且存在唯一不交轮换积。



引理 3.4.2 (轮换的逆)

$$(a_1 a_2 \cdots a_r)^{-1} = (a_1 a_r \cdots a_2)$$



引理 3.4.3 (轮换的循环不变性)

$$(a_1 a_2 \cdots a_r) = (a_2 \cdots a_r a_1)$$



引理 3.4.4 (不交轮换可交换)

$$(a_1 a_2 \cdots a_r)(b_1 b_2 \cdots b_s) = (b_1 b_2 \cdots b_s)(a_1 a_2 \cdots a_r)$$



引理 3.4.5 (轮换的共轭)

对于 n 元置换 $\tau \in S_n$, 以及 r -轮换 $(a_1 \cdots a_r)$, 成立

$$\tau(a_1 \cdots a_r)\tau^{-1} = (\tau(a_1) \cdots \tau(a_r))$$



证明 首先, 对于任意 $1 \leq k \leq r$, 由于

$$(\tau(a_1 \cdots a_r) \tau^{-1})(\tau(a_k)) = \tau(a_1 \cdots a_r) \tau^{-1} \tau(a_k) = \tau(a_{k+1})$$

其中 $a_{r+1} = a_1$, 因此 $(\tau(a_1) \cdots \tau(a_r))$ 构成轮换。

其次, 对于任意 $a \in \{1, \cdots, n\} \setminus \{a_1, \cdots, a_r\}$, 成立

$$(\tau(a_1 \cdots a_r) \tau^{-1})(a) = a$$

综上所述

$$\tau(a_1 \cdots a_r) \tau^{-1} = (\tau(a_1) \cdots \tau(a_r))$$

3.4.2 S_n 中的型与共轭类

定义 3.4.2 (划分 partition)

定义 $n \in \mathbb{N}^*$ 的划分为

$$\left\{ [\lambda_1, \cdots, \lambda_r] : \lambda_k \geq \lambda_{k+1}, \sum_{k=1}^r \lambda_k = n, r \in \mathbb{N}^* \right\}$$



定义 3.4.3 (型 type)

定义 n 元置换 $\sigma \in S_n$ 型为由其不交轮换大小构成的 n 的划分。



命题 3.4.1

对于 n 元置换 $\varphi, \psi \in S_n$, 成立

$$\varphi \text{ 与 } \psi \text{ 共轭} \iff \varphi \text{ 与 } \psi \text{ 存在相同型}$$



证明 必要性由引理 3.4.5 推出。对于充分性, 如果 φ 与 ψ 存在相同型, 那么记

$$\varphi = (a_1^{(1)} \cdots a_{r_1}^{(1)}) \cdots (a_1^{(s)} \cdots a_{r_s}^{(s)})$$

$$\psi = (b_1^{(1)} \cdots b_{r_1}^{(1)}) \cdots (b_1^{(s)} \cdots b_{r_s}^{(s)})$$

构造 $\tau \in S_n$ 如下

$$\begin{aligned} \tau : S_n &\longrightarrow S_n \\ a_i^{(j)} &\longmapsto b_i^{(j)} \end{aligned}$$

那么由引理 3.4.5, $\tau \varphi \tau^{-1} = \psi$ 。

推论 3.4.1

n 元对称群 S_n 的共轭类数等于 n 的划分数。



3.4.3 交错群

定义 3.4.4 (符号 sign)

对于轮换积

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \cdots, x_n]$$

考虑作用

$$\begin{aligned} \bullet : S_n \times \{\pm \Delta_n\} &\longrightarrow \{\pm \Delta_n\} \\ \left(\sigma, \prod_{1 \leq i < j \leq n} (x_i - x_j) \right) &\longmapsto \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}) \\ \left(\sigma, - \prod_{1 \leq i < j \leq n} (x_i - x_j) \right) &\longmapsto - \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}) \end{aligned}$$

那么 $\sigma \bullet \Delta_n = \pm \Delta_n$, 定义置换 σ 的符号为 $\sigma \bullet \Delta_n = (-1)^\sigma \Delta_n$ 。



定义 3.4.5 (偶置换 even permutation)

称置换 σ 为偶置换, 如果 $(-1)^\sigma = 1$ 。



定义 3.4.6 (奇置换 odd permutation)

称置换 σ 为奇置换, 如果 $(-1)^\sigma = -1$ 。



引理 3.4.6 (置换复合的符号)

$$(-1)^{\sigma\tau} = (-1)^\sigma (-1)^\tau$$



定理 3.4.2 (置换符号的群同态性)

$$\begin{aligned} \epsilon : S_n &\longrightarrow \{1, -1\} \\ \sigma &\longmapsto (-1)^\sigma \end{aligned}$$



定义 3.4.7 (对换 transposition)

称 2-轮换为对换。



引理 3.4.7

对换生成对称群。



证明 由引理 3.4.1, 结合

$$(a_1 \cdots a_r) = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_r)$$

命题得证!

引理 3.4.8 (对换积的符号)

将置换 σ 表示为对换积 $\sigma = \tau_1 \cdots \tau_r$, 那么

$$\begin{aligned} \sigma \text{ 为偶置换} &\iff 2 \mid r \\ \sigma \text{ 为奇置换} &\iff 2 \nmid r \end{aligned}$$



引理 3.4.9 (轮换的符号)

对于 $\sigma = (a_1 \cdots a_r)$, 成立

$$\sigma \text{ 为偶置换} \iff 2 \nmid r$$

$$\sigma \text{ 为奇置换} \iff 2 \mid r$$

**定义 3.4.8**

定义 n 元交错群为

$$A_n = \{\sigma \in S_n : (-1)^\sigma = 1\}$$

**例题 3.4**

$$A_1 = \{1\}, \quad A_2 = \{1\}, \quad S_3 = \{1, (123), (132)\}$$

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

定理 3.4.3 (交错群的正规性)

交错群为对称群的正规子群。



证明 由命题 3.4.2, 结合 $\ker \epsilon = A_n$, 以及定理 2.7.3, 可得 $A_n \triangleleft S_n$ 。

定理 3.4.4 (交错群的指标)

如果 $n \geq 2$, 那么 $[S_n : A_n] = 2$ 。



证明 由命题 3.4.2, 结合 $\ker \epsilon = A_n$, 以及群第一同构定理 2.8.1, 成立

$$S_n/A_n = S_n/\ker \epsilon \cong \mathbb{Z}/2\mathbb{Z}$$

因此 $[S_n : A_n] = 2$ 。

命题 3.4.2

对于 n 元偶置换 $\sigma \in A_n$, 其中 $n \geq 2$, 成立

$$\text{Cent}_{S_n}(\sigma) \not\subset A_n \implies \text{Conj}_{A_n}(\sigma) = \text{Conj}_{S_n}(\sigma)$$

$$\text{Cent}_{S_n}(\sigma) \subset A_n \implies 2|\text{Conj}_{A_n}(\sigma)| = |\text{Conj}_{S_n}(\sigma)|$$



证明 如果 $\text{Cent}_{S_n}(\sigma) \subset A_n$, 那么 $\text{Cent}_{A_n}(\sigma) = \text{Cent}_{S_n}(\sigma) \subset A_n$ 。由命题 3.4.4

$$[S_n : \text{Cent}_{S_n}(\sigma)] = [S_n : \text{Cent}_{A_n}(\sigma)] = [S_n : A_n][A_n : \text{Cent}_{A_n}(\sigma)] = 2[A_n : \text{Cent}_{A_n}(\sigma)]$$

由轨道-稳定化子定理 2.9.2, $2|\text{Conj}_{A_n}(\sigma)| = |\text{Conj}_{S_n}(\sigma)|$ 。

如果 $\text{Cent}_{S_n}(\sigma) \not\subset A_n$, 那么由命题 3.4.3, 以及命题 2.6.7, $A_n \subsetneq A_n \text{Cent}_{S_n}(\sigma) < S_n$ 。而由命题 3.4.4, 以及 Lagrange 定理 2.8.8, $A_n \text{Cent}_{S_n}(\sigma) = S_n$ 。由群第二同构定理 2.8.2

$$\frac{\text{Cent}_{S_n}(\sigma)}{A_n \cap \text{Cent}_{S_n}(\sigma)} \cong \frac{A_n \text{Cent}_{S_n}(\sigma)}{A_n}$$

因此由轨道-稳定化子定理 2.9.2

$$|\text{Conj}_{A_n}(\sigma)| = [A_n : \text{Cent}_{A_n}(\sigma)] = [A_n : A_n \cap \text{Cent}_{S_n}(\sigma)] = [A_n \text{Cent}_{S_n}(\sigma) : \text{Cent}_{S_n}(\sigma)] = [S_n : \text{Cent}_{S_n}(\sigma)] = |\text{Conj}_{S_n}(\sigma)|$$

而由 $\text{Conj}_{A_n}(\sigma) \subset \text{Conj}_{A_n}(\sigma)$, 于是 $\text{Conj}_{A_n}(\sigma) = \text{Conj}_{S_n}(\sigma)$ 。

命题 3.4.3

对于 n 元偶置换 $\sigma \in A_n$, 其中 $n \geq 2$, 成立

$$\sigma \text{ 的型由互异奇数组成} \iff \text{Cent}_{S_n}(\sigma) \subset A_n$$

证明 如果 σ 的型由互异奇数组成, 那么任取 $\tau \in \text{Cent}_{S_n}(\sigma)$, 即 $\tau\sigma\tau^{-1} = \sigma$ 。记 σ 的轮换分解为

$$\sigma = (a_1^{(1)} \cdots a_{r_1}^{(1)}) \cdots (a_1^{(s)} \cdots a_{r_s}^{(s)})$$

其中对于任意 $1 \leq t \leq s$, r_t 为奇数, 且对于任意 $1 \leq u < v \leq s$, $r_u \neq r_v$ 。由引理 3.4.5

$$\tau\sigma\tau^{-1} = (\tau(a_1^{(1)}) \cdots \tau(a_{r_1}^{(1)})) \cdots (\tau(a_1^{(s)}) \cdots \tau(a_{r_s}^{(s)}))$$

因此

$$(\tau(a_1^{(1)}) \cdots \tau(a_{r_1}^{(1)})) \cdots (\tau(a_1^{(s)}) \cdots \tau(a_{r_s}^{(s)})) = (a_1^{(1)} \cdots a_{r_1}^{(1)}) \cdots (a_1^{(s)} \cdots a_{r_s}^{(s)})$$

那么对于任意 $1 \leq t \leq s$

$$(\tau(a_1^{(t)}) \cdots \tau(a_{r_t}^{(t)})) = (a_1^{(t)} \cdots a_{r_t}^{(t)})$$

进而对于任意 $1 \leq t \leq s$, 存在 $m_t \in \mathbb{N}^*$, 使得成立

$$\tau = (a_1^{(1)} \cdots a_{r_1}^{(1)})^{m_1} \cdots (a_1^{(s)} \cdots a_{r_s}^{(s)})^{m_s}$$

由于对于任意 $1 \leq t \leq s$, r_t 为奇数, 那么由引理 3.4.9, $(a_1^{(t)} \cdots a_{r_t}^{(t)})^{m_t}$ 为偶置换, 进而由引理 3.4.6, τ 为偶置换, 由此可得 $\text{Cent}_{S_n}(\sigma) \subset A_n$ 。

如果 σ 的型存在偶数, 令 τ 为 σ 的轮换分解中的偶轮换, 那么 $\tau\sigma\tau^{-1} = \sigma$ 。而由引理 3.4.9, τ 为奇置换, 因此 $\text{Cent}_{S_n}(\sigma) \not\subset A_n$ 。

如果 σ 的型存在相同奇数, 记 σ 的轮换分解为

$$\sigma = (a_1 \cdots a_m)(b_1 \cdots b_m)(a_1^{(1)} \cdots a_{r_1}^{(1)}) \cdots (a_1^{(s)} \cdots a_{r_s}^{(s)})$$

其中 m 为奇数。由引理 3.4.8, 考虑奇置换

$$\tau = (a_1 b_1) \cdots (a_m b_m)$$

那么 $\tau\sigma\tau^{-1} = \sigma$, 因此 $\text{Cent}_{S_n}(\sigma) \not\subset A_n$ 。

综上所述, 命题得证!

3.4.4 A_n 的结构

表 3.1: A_n 的结构

n	交换性	单性	可解性	非平凡正规子群	换位子群
1	✓	✓	✓		$\{1\}$
2	✓	✓	✓		$\{1\}$
3	✓	✓	✓		$\{1\}$
4			✓	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
≥ 5		✓			A_n

引理 3.4.10

当 $n \geq 5$ 时, A_n 中任意 3-轮换共轭。

证明 考虑任意两个 3-轮换 $(a_1 a_2 a_3)$ 与 $(b_1 b_2 b_3)$, 作置换 $\pi \in S_n$, 使得对于任意 $1 \leq k \leq 3$, 成立 $\pi(a_k) = b_k$ 。由于 $n \geq 5$, 那么存在 $\{c, d\} = \{1, 2, 3, 4, 5\} \setminus \{a_1, a_2, a_3\}$ 。如果 π 为偶置换, 那么令 $\sigma = \pi$; 如果 π 为奇置换, 那么令 $\sigma = \pi(cd)$; 此时, $\sigma \in A_n$ 。由引理 3.4.5, $\sigma(a_1 a_2 a_3)\sigma^{-1} = (b_1 b_2 b_3)$, 从而命题得证!

引理 3.4.11

对于 $n \geq 5$, 如果 $N \triangleleft A_n$, 且 N 包含 3-轮换, 那么 N 包含所有 3-轮换。

证明 这是引理 3.4.10 的直接推论。

引理 3.4.12

对于 $n \geq 5$, 如果 $\{1\} \subsetneq N \triangleleft A_n$, 那么 N 包含 3-轮换。

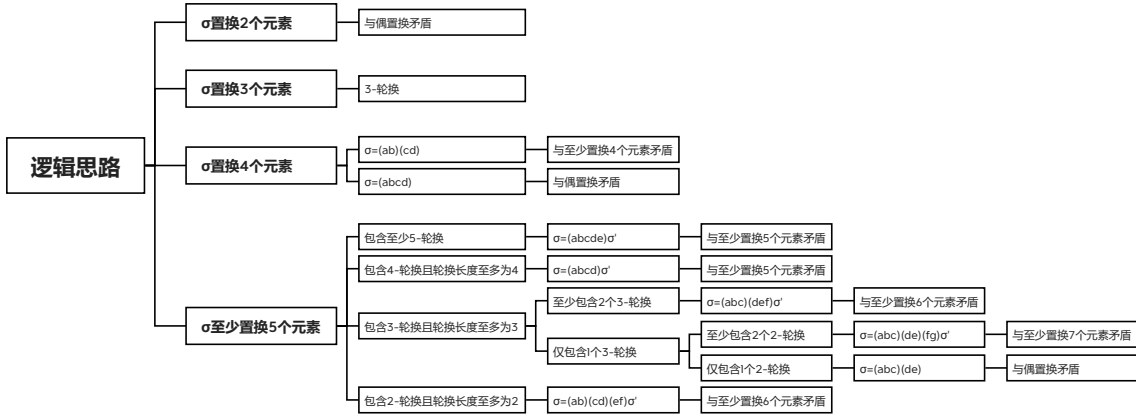


图 3.1: 逻辑思路

证明 在 $N \triangleleft A_n$ 中取置换元素最少的非平凡置换 $\sigma \in N$ 。

如果 σ 置换 2 个元素, 那么由引理 3.4.8, 这与 σ 为偶置换矛盾!

如果 σ 置换 3 个元素, 那么 σ 为 3-轮换。

如果 σ 置换 4 个元素, 且 $\sigma = (ab)(cd)$, 那么由引理 3.4.9, 令 $\tau = (cde) \in A_n$, 由引理 3.4.5

$$(ab)(de) = \tau\sigma\tau^{-1} \in N \implies (cde) = \sigma\tau\sigma\tau^{-1} \in N$$

这与 N 中置换至少置换 4 个元素矛盾!

如果 σ 置换 4 个元素, 且 $\sigma = (abcd)$, 那么由引理 3.4.9, 这与 σ 为偶置换矛盾!

如果 σ 至少置换 5 个元素, 且 σ 的轮换分解中包含长度至少为 5 的轮换, 那么 $\sigma = (abcde_1 \cdots e_r)\sigma'$ 。由引理 3.4.9, 令 $\tau = (bcd) \in A_n$, 由引理 3.4.5

$$(acdbe_1 \cdots e_r)\sigma' = \tau\sigma\tau^{-1} \in N \implies (abd) = \sigma^{-1}\tau\sigma\tau^{-1} \in N$$

这与 N 中置换至少置换 5 个元素矛盾!

如果 σ 至少置换 5 个元素, 且 σ 的轮换分解中包含 4-轮换, 同时包含轮换长度至多为 4, 那么 $\sigma = (abcd)\sigma'$ 。

由引理 3.4.9, 令 $\tau = (bcd) \in A_n$, 由引理 3.4.5

$$(acdb)\sigma' = \tau\sigma\tau^{-1} \in N \implies (abd) = \sigma^{-1}\tau\sigma\tau^{-1} \in N$$

这与 N 中置换至少置换 5 个元素矛盾!

如果 σ 至少置换 5 个元素, 且 σ 的轮换分解中至少包含两个 3-轮换, 同时包含轮换长度至多为 3, 那么 $\sigma = (abc)(def)\sigma'$, 此时 σ 至少置换 6 个元素。由引理 3.4.9, 令 $\tau = (bcd) \in A_n$, 由引理 3.4.5

$$(acd)(bef)\sigma' = \tau\sigma\tau^{-1} \in N \implies (abdcf) = \sigma^{-1}\tau\sigma\tau^{-1} \in N$$

这与 N 中置换至少置换 6 个元素矛盾!

如果 σ 至少置换 5 个元素, 且 σ 的轮换分解中仅包含一个 3-轮换, 与至少两个 2-轮换, 同时包含轮换长度至多为 3, 那么 $\sigma = (abc)(de)(fg)\sigma'$, 此时 σ 至少置换 7 个元素。由引理 3.4.9, 令 $\tau = (bcd) \in A_n$, 由引理 3.4.5

$$(acd)(be)(fg)\sigma' = \tau\sigma\tau^{-1} \in N \implies (abdce) = \sigma^{-1}\tau\sigma\tau^{-1} \in N$$

这与 N 中置换至少置换 7 个元素矛盾！

如果 σ 至少置换 5 个元素，且 σ 的轮换分解中仅包含一个 3-轮换，与一个 2-轮换，那么 $\sigma = (abc)(de)$ ，由引理 3.4.9 与 3.4.8 以及 3.4.6，这与 σ 为偶置换矛盾！

如果 σ 至少置换 5 个元素，且 σ 的轮换分解中仅包含 2-轮换，那么 $\sigma = (ab)(cd)(ef)\sigma'$ ，此时 σ 至少置换 6 个元素。由引理 3.4.9，令 $\tau = (bcd) \in A_n$ ，由引理 3.4.5

$$(ac)(bd)(ef)\sigma' = \tau\sigma\tau^{-1} \in N \implies (ad)(bc) = \sigma^{-1}\tau\sigma\tau^{-1} \in N$$

这与 N 中置换至少置换 6 个元素矛盾！

综上所述， σ 为 3-轮换，进而命题得证！

引理 3.4.13

3-轮换生成交错群。

证明 由引理 3.4.7，结合

$$(ab)(ac) = (acb), \quad (ab)(cd) = (acb)(cda)$$

命题得证！

定理 3.4.5 (A_n 的单性)

当且仅当 $n \neq 4$ 时， A_n 为单群。

证明 当 $n \leq 3$ 时，由命题 3.4.5， A_n 为单群。

当 $n = 4$ 时，由命题 3.4.5， A_4 为非单群。

当 $n \geq 5$ 时，任取 $\{1\} \subsetneq N \triangleleft A_n$ ，那么由引理 3.4.12， N 包含 3-轮换。由引理 3.4.11， N 包含所有 3-轮换。由引理 3.4.13， $N = A_n$ ，进而 A_n 为单群。

命题 3.4.4 (A_n 的交换性)

当且仅当 $n \geq 4$ 时， A_n 为非交换群。

证明 当 $n = 1$ 或 $n = 2$ 时， $A_1 = \{1\}$ 与 $A_2 = \{1\}$ 为交换群。

当 $n = 3$ 时，由命题 2.8.3， $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ 为交换群。

当 $n \geq 4$ 时，由引理 3.4.8， $(12)(13), (12)(14) \in A_4$ 。由于

$$(12)(13)(12)(14) = (14)(23), \quad (12)(14)(12)(13) = (13)(24)$$

因此 A_n 为非交换群。

命题 3.4.5 (A_n 的正规子群)

当 $n \neq 4$ 时， A_n 仅存在平凡正规子群。

当 $n = 4$ 时， A_4 存在且存在唯一非平凡正规子群 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。

证明 当 $n = 1$ 或 $n = 2$ 时， $A_1 = \{1\}$ 与 $A_2 = \{1\}$ 仅存在平凡正规子群。

当 $n = 3$ 时，由命题 2.8.3， $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ 。由命题 3.3.10， A_3 仅存在平凡正规子群。

当 $n = 4$ 时，计算可得 A_4 存在且存在唯一非平凡正规子群

$$[A_4, A_4] = \{1, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

当 $n \geq 5$ 时，由定理 3.4.5， A_n 仅存在平凡正规子群。

命题 3.4.6 (A_n 的换位子群)

$$\begin{aligned} [A_n, A_n] &= \{1\}, & n \leq 3 \\ [A_4, A_4] &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & n = 4 \\ [A_n, A_n] &= A_n, & n \geq 5 \end{aligned}$$



证明 当 $n \leq 3$ 时, 由命题 3.4.4 与 3.3.7, $[A_n, A_n] = \{1\}$ 。

当 $n = 4$ 时, 由命题 3.4.5, $[A_4, A_4] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。

当 $n \geq 5$ 时, 由命题 3.3.6、3.4.5、3.4.4 与 3.3.7, $[A_n, A_n] = A_n$ 。

命题 3.4.7 (A_n 的可解性)

当且仅当 $n \geq 5$ 时, A_n 为不可解群。



证明 当 $n \leq 3$ 时, 由命题 3.4.6, A_n 为可解群。

当 $n = 4$ 时, 由命题 3.4.6

$$A_4^{(1)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad A_4^{(2)} = \{1\}$$

那么 A_n 为可解群。

当 $n \geq 5$ 时, 由命题 3.4.6, A_n 为不可解群。

3.4.5 S_n 的结构

表 3.2: S_n 的结构

n	交换性	单性	可解性	非平凡正规子群	换位子群
1	✓	✓	✓		A_n
2	✓	✓	✓		A_n
3			✓	A_3	A_n
4			✓	$A_4, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	A_n
≥ 5				A_n	A_n

命题 3.4.8 (S_n 的交换性)

当且仅当 $n \geq 3$ 时, S_n 为非交换群。



证明 当 $n = 1$, $S_1 = \{1\}$ 为交换群。

当 $n = 2$ 时, 由命题 2.8.3, $S_2 \cong \mathbb{Z}/2\mathbb{Z}$ 为交换群。

当 $n \geq 3$ 时, 由于

$$(23)(132) = (12), \quad (132)(23) = (13)$$

因此 S_n 为非交换群。

命题 3.4.9 (S_n 的正规子群)

当 $n \neq 2$ 时, S_n 仅存在平凡正规子群。

当 $n = 4$ 时, A_4 仅存在非平凡正规子群 A_n 与 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。

当 $n \geq 3$ 且 $n \neq 4$ 时, S_n 仅存在非平凡正规子群 A_n 。



命题 3.4.10 (S_n 的换位子群)

$$[S_n, S_n] = A_n, \quad n \in \mathbb{N}^*$$

证明 当 $n \leq 2$ 时, 计算可得 $[S_n, S_n] = A_n$ 。

当 $n \geq 3$ 时, 由于

$$(abc) = (bc)(ab)(bc)(ab)$$

那么 3-轮换为换位子, 由引理 3.4.13, $[S_n, S_n] \supset A_n$ 。由命题 3.4.4 与命题 2.8.3, $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, 因此 S_n/A_n 为交换群。由命题 3.3.9, $[S_n, S_n] \subset A_n$ 。因此 $[S_n, S_n] = A_n$ 。

命题 3.4.11 (S_n 的单性)

当且仅当 $n \geq 3$ 时, S_n 为非单群。

证明 由命题 3.4.10 与命题 3.3.6, 命题得证!

定理 3.4.6 (S_n 的可解性)

当且仅当 $n \geq 5$ 时, S_n 为不可解群。

证明 (法一) 由命题 3.4.10 与命题 3.4.7, 命题得证!

(法二) 当 $n \geq 5$ 时, 由定理 3.4.3, 可得次正规列

$$\{1\} \triangleleft A_n \triangleleft S_n$$

由定理 3.4.5, $A_n/\{1\} = A_n$ 为单群。由引理 3.4.4 与命题 2.8.3 以及命题 3.3.10, $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ 为单群。由此可知此次正规列为合成列。由命题 3.4.4, A_n 不为循环群。由 Jordan-Hölder 定理 3.3.1 与命题 3.3.16, S_n 为不可解群。

3.5 群的积

3.5.1 直积

引理 3.5.1

$$M, N \triangleleft G \implies [M, N] \subset M \cap N$$

证明 这几乎是显然的, 任取 $m \in M$ 与 $n \in N$, 由于 $M, N \triangleleft G$, 那么

$$n * m^{-1} * n^{-1} \in M \implies m * n * m^{-1} * n^{-1} \in M \iff [m, n] \in M$$

$$m * n * m^{-1} \in N \implies m * n * m^{-1} * n^{-1} \in N \iff [m, n] \in N$$

因此 $[m, n] \in M \cap N$, 由 m, n 的任意性, $[M, N] \subset M \cap N$ 。

推论 3.5.1

$$M, N \triangleleft G, \quad M \cap N = \{e\} \implies \forall m \in M, \forall n \in N, m * n = n * m$$

证明 由引理 3.5.1, 这是显然的!

命题 3.5.1

$$M, N \triangleleft G, \quad M \cap N = \{e\} \implies M \times N \cong M * N$$

证明 构造映射

$$\begin{aligned}\varphi : M \times N &\longrightarrow M * N \\ (m, n) &\longmapsto m * n\end{aligned}$$

首先证明 φ 为群同态映射, 由推论 3.5.1

$$\begin{aligned}\varphi((m_1, n_1) * (m_2, n_2)) &= \varphi((m_1 * m_2, n_1 * n_2)) \\ &= m_1 * m_2 * n_1 * n_2 \\ &= m_1 * n_1 * m_2 * n_2 \\ &= \varphi((m_1, n_1)) * \varphi((m_2, n_2))\end{aligned}$$

其次证明 φ 为单射

$$\ker \varphi = \{(m, n) \in M \times N : m * n = e\} = \{(m, n) \in M \times N : m, n \in M \cap N\} = \{(e, e)\}$$

而显然 φ 为满射, 因此 φ 为群同构映射, 进而

$$M \times N \cong M * N$$

命题 3.5.2

对于群 $(G, *)$, 如果 $N \triangleleft G$ 且 $H < G$, 那么

$$G = N * H, \quad N \cap H = \{e\} \iff H \cong G/N, \text{ 且群同态映射为 } h \mapsto h * N$$

证明 对于必要性, 如果 $G = N * H$ 且 $N \cap H = \{e\}$, 那么考虑群同态映射

$$\begin{aligned}\varphi : H &\longrightarrow G/N \\ h &\longmapsto h * N\end{aligned}$$

对于单射性

$$\ker \varphi = \{h \in H : h * N = N\} = N \cap H = \{e\}$$

对于满射性, 任取 $g \in G$, 由于 $G = N * H$, 那么存在 $n \in N$ 与 $h \in H$, 使得成立 $g = n * h$, 因此

$$\varphi(h) = h * N = h * (h^{-1} * n * h) * N = (n * h) * N = g * N$$

那么 φ 为群同构映射, 进而 $H \cong G/N$ 。

对于充分性, 如果 $H \cong G/N$, 且群同态映射为

$$\begin{aligned}\varphi : H &\longrightarrow G/N \\ h &\longmapsto h * N\end{aligned}$$

由于 φ 为单射, 那么

$$M \cap N = \{h \in H : h * N = N\} = \{h \in H : h * N = N\} = \{e\}$$

任取 $g \in G$, 由于 φ 为满射, 那么存在 $h \in H$, 使得成立 $h * N = g * N$, 因此存在 $n \in N$, 使得成立 $g = n * h$ 。由 $g \in G$ 的任意性, $G = N * H$ 。

3.5.2 半直积

定义 3.5.1 (半直积 semidirect product)

定义群 $(N, *)$ 与 $(H, *)$ 关于群同态映射

$$\begin{aligned}\Psi : H &\longrightarrow \text{Aut}_{\text{Grp}}(N) \\ h &\longmapsto \psi_h\end{aligned}$$

的半直积为群 $(N \rtimes_{\psi} H, \bullet)$, 其中

$$(n_1, h_1) \bullet (n_2, h_2) = (n_1 * \psi_{h_1}(n_2), h_1 * h_2)$$



命题 3.5.3

对于群 $(G, *)$, 如果

$$N \triangleleft G, \quad H < G, \quad G = N * H, \quad N \cap H = \{e\}$$

那么

$$G \cong N \rtimes_{\gamma} H$$

其中

$$\Gamma : H \longrightarrow \text{Inn}_{\text{Grp}}(N)$$

$$h \longmapsto \psi_h$$



证明 构造映射

$$\varphi : N \rtimes_{\psi} H \longrightarrow G$$

$$(n, h) \longmapsto n * h$$

对于群同态性

$$\begin{aligned} \varphi((n_1, h_1) \bullet (n_2, h_2)) &= \varphi((n_1 * \psi_{h_1}(n_2), h_1 * h_2)) \\ &= n_1 * \psi_{h_1}(n_2) * h_1 * h_2 \\ &= n_1 * h_1 * n_2 * h_1^{-1} * h_1 * h_2 \\ &= n_1 * h_1 * n_2 * h_2 \\ &= \varphi((n_1, h_2)) * \varphi((n_2, h_2)) \end{aligned}$$

对于单射性

$$\ker \varphi = \{(n, h) \in N \rtimes_{\psi} H : n * h = e\} = \{(n, h) \in N \rtimes_{\psi} H : n, h \in N \cap H\} = \{(e, e)\}$$

而 φ 显然为满射, 因此 φ 为群同构映射, 进而

$$G \cong N \rtimes_{\gamma} H$$

3.5.3 群的正合序列

定义 3.5.2 (群的正合 exact of group)

称群 G, H, K 的群同态映射序列

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K$$

在 H 处正合, 如果 $\text{im } \varphi = \ker \psi$ 。



定义 3.5.3 (群的正合序列 exact sequences of group)

称群族 $\{G_n\}_{n=0}^{\infty}$ 的群同态映射序列

$$G_0 \xrightarrow{\varphi_1} G_1 \xrightarrow{\varphi_2} G_2 \xrightarrow{\varphi_3} \cdots$$

为正合序列, 如果对于任意 $n \in \mathbb{N}^*$, 成立 $\text{im } \varphi_n = \ker \varphi_{n+1}$ 。



命题 3.5.4

对于群 G 与 H , 成立

$$\{e\} \longrightarrow G \xrightarrow{\varphi} H \text{ 为群的正合序列} \iff \varphi: G \hookrightarrow H \text{ 为单射}$$

$$G \xrightarrow{\varphi} H \longrightarrow \{e\} \text{ 为群的正合序列} \iff \varphi: G \twoheadrightarrow H \text{ 为满射}$$

证明

$$\{e\} \longrightarrow G \xrightarrow{\varphi} H \text{ 为群的正合序列} \iff \ker \varphi = \{e\} \iff \varphi: G \hookrightarrow H \text{ 为单射}$$

$$G \xrightarrow{\varphi} H \longrightarrow \{e\} \text{ 为群的正合序列} \iff \operatorname{im} \varphi = H \iff \varphi: G \twoheadrightarrow H \text{ 为满射}$$

定义 3.5.4 (延拓 extension)

称群 G 为群 H 关于群 N 的延拓, 如果存在群的正合序列

$$\{e\} \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow \{e\}$$

定义 3.5.5 (分裂 split)

称群的正合序列

$$\{e\} \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow \{e\}$$

为分裂的, 如果存在 $K < G$, 使得成立 $K \cong H$.

3.6 有限 Abel 群

3.6.1 有限 abel 群的分类

引理 3.6.1

对于 Abel 群 $(G, *)$, 如果 H, K 为 G 的有限子群, 且 $\gcd(|H|, |K|) = 1$, 那么 $H * K \cong H \times K$.

证明 由于 G 为 Abel 群, 那么 H, K 为 G 的正规子群。由 Lagrange 定理 2.8.8, $H \cap K = \{e\}$ 。由命题 3.5.1, $H * K \cong H \times K$ 。

推论 3.6.1

有限 Abel 群同构于其 Sylow 子群的积。

证明 对于有限 Abel 群 $(G, *)$, 由推论 3.2.2, G 的 Sylow p -子群唯一。记 G 的 Sylow 子群族为 $\{P_k\}_{k=1}^n$, 那么对于任意 $i \neq j$, 成立 $\gcd(|P_i|, |P_j|) = 1$, 因此由引理 3.6.1

$$G = P_1 * \cdots * P_n \cong P_1 \times \cdots \times P_n$$

引理 3.6.2

对于素数 p 与 $r \in \mathbb{N}^*$, 如果 $(G, *)$ 为 p^{r+1} 阶非循环 Abel 群, 且 $g \in G$ 为 p^r 阶元素, 那么存在 p 阶元素 $h \in G \setminus \langle g \rangle$ 。

证明 由于 G 为 Abel 群, 那么 $\langle g \rangle \triangleleft G$, 因此商群 $G/\langle g \rangle$ 的阶为 p 。任取 $k \in G \setminus \langle g \rangle$, 由 Lagrange 定理 2.8.8, $p \mid |k|$, 且 $k * \langle g \rangle$ 的阶为 p , 因此 $k^p \in \langle g \rangle$ 。由 Lagrange 定理 2.8.8, k^p 的阶为 p 的幂。

令 $|k^p| = p^s$, 其中 $0 \leq s \leq r$. 由命题 2.1.7, $|k| = p|k^p| = p^{s+1}$. 如果 $s = r$, 那么 $|k| = p^{r+1}$, 因此 $G \cong \langle k \rangle$, 与 G 为非循环群矛盾! 进而 $s < r$. 由命题 2.6.14, $\langle k^p \rangle \langle g^{p^{r-s}} \rangle \subset \langle g^p \rangle$, 因此存在 $n \in \mathbb{Z}$, 使得成立 $k^p = g^{np}$. 令 $h = k * g^{-n} \in G \setminus \langle g \rangle$, 那么 $h \neq e$, 且 $h^p = e$, 于是 $|h| = p$.

引理 3.6.3

对于 Abel p -群 $(G, *)$, 如果 $g \in G$ 为其阶最大的元素, 那么存在 $H < G$, 使得成立 $G = H * \langle g \rangle$, 且 $H \cap \langle g \rangle = \{e\}$.

推论 3.6.2 (Abel p -群的结构)

Abel p -群同构于循环 p -群的积。

证明 对于 Abel p -群 $(G, *)$, 对于 $|G|$ 进行数学归纳证明。如果 $|G| = 1$, 那么 $G \cong \{e\}$ 。

如果 $|G| < n$ 时命题成立, 那么当 $|G| = n$ 时, 取 G 中阶最大的元素 g , 由引理 3.6.3, 存在 $H < G$, 使得成立 $G = H * \langle g \rangle$. 由归纳假设, H 同构于循环 p -群的积, 那么 G 同构于循环 p -群的积。

由数学归纳法, 命题得证!

推论 3.6.3

有限 Abel 群可表示为循环 p -群的积。

证明 对于有限 Abel 群 $(G, *)$, 由推论 3.6.1

$$G = P_1 * \cdots * P_n \cong P_1 \times \cdots \times P_n$$

其中 $\{P_k\}_{k=1}^n$ 为 G 的 Sylow 子群族。由推论 3.6.2, 每一个 P_k 同构于循环 p -群的积, 其中 $1 \leq k \leq n$, 那么 G 同构于循环 p -群的积。

3.6.2 有限 Abel 群的结构定理

定理 3.6.1 (有限 Abel 群的结构定理)

1. 对于互异素数 p_1, \dots, p_n , $p_1^{r_1} \cdots p_n^{r_n}$ 阶 Abel 群的结构为

$$\bigotimes_{i=1}^n \bigotimes_{j=1}^{k_i} \frac{\mathbb{Z}}{p_i^{r_i^{(j)}} \mathbb{Z}}$$

其中对于任意 $1 \leq i \leq n$, 成立

$$r_i^{(1)} \leq \cdots \leq r_i^{(k_i)}, \quad r_i^{(1)} + \cdots + r_i^{(k_i)} = r_i$$

2. 有限 Abel 群的结构为

$$\frac{\mathbb{Z}}{d_1 \mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_n \mathbb{Z}}$$

其中 $1 < d_1 \mid \cdots \mid d_n$ 。

3.6.3 域的乘法群的有限子群

引理 3.6.4

对于有限 Abel 群 $(G, *)$, 如果对于任意 $n \in \mathbb{N}^*$, 成立 $|G_n| \leq n$, 其中

$$G_n = \{g \in G : g^n = e\}$$

为 G 的子群, 那么 G 为循环群。

证明 由有限 Abel 群的结构定理 3.6.1, 存在 $1 < d_1 \mid \cdots \mid d_m$, 使得成立

$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_m\mathbb{Z}}$$

如果 $m \geq 2$, 那么

$$|G| = d_1 \cdots d_m > d_m$$

但是对于任意 $g \in G$, 成立 $g^{d_m} = e$, 因此 $G_{d_m} = G$, 于是

$$|G_{d_m}| = |G| > d_m$$

与假设矛盾! 进而 $m = 1$, 那么 $G \cong \mathbb{Z}/d_1\mathbb{Z}$ 为循环群。

定理 3.6.2 (域的乘法群的有限子群为循环群)

对于域 $(F, +, \cdot)$, 如果 G 为乘法群 (F^\times, \cdot) 的有限子群, 那么 G 为循环群。



证明 考察 G 的子群

$$G_n = \{g \in G : g^n = 1\}$$

考虑域 F 上的 n 次多项式 $f(x) = x^n - 1$, 那么 G_n 中的元素均为 $f(x)$ 在 F 中的根。由引理 5.5.1, $f(x)$ 在 F 中至多存在 n 个根, 则 $|G_n| \leq n$, 进而由引理 3.6.4, G 为循环群。

第四章 环论 I

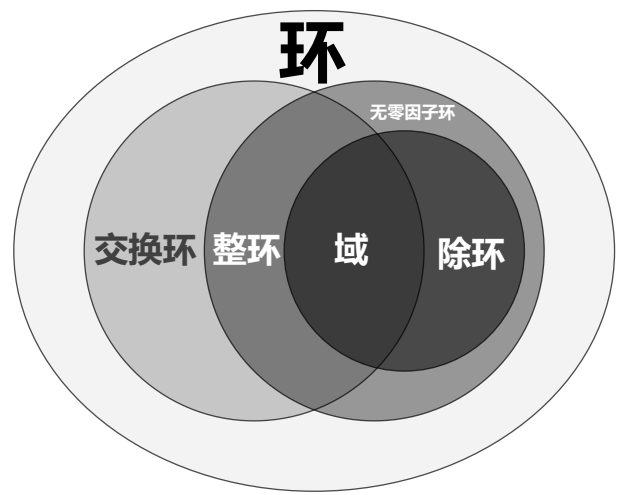


图 4.1: 环的关系

表 4.1: 环定义表

	环	交换环	无零因子环	整环	除环	域
加法封闭性	✓	✓	✓	✓	✓	✓
乘法封闭性	✓	✓	✓	✓	✓	✓
加法单位元	✓	✓	✓	✓	✓	✓
乘法单位元	✓	✓	✓	✓	✓	✓
加法逆元	✓	✓	✓	✓	✓	✓
加法交换律	✓	✓	✓	✓	✓	✓
加法结合律	✓	✓	✓	✓	✓	✓
乘法结合律	✓	✓	✓	✓	✓	✓
分配律	✓	✓	✓	✓	✓	✓
非零性			✓	✓	✓	✓
消去律			✓	✓	✓	✓
乘法交换律		✓		✓		✓
乘法逆元					✓	✓

4.1 环的定义

4.1.1 定义

定义 4.1.1 (零环 zero-ring)

$$\{0\}$$



定义 4.1.2 (非零环 non-zero-ring)

称环 $(R, +, \cdot)$ 为非零环, 如果 $0 \neq 1$ 。



定义 4.1.3 (环 ring)

称代数系统 $(R, +, \cdot)$ 为环, 如果加法运算 $+: R \times R \rightarrow R$ 和乘法运算 $\cdot: R \times R \rightarrow R$ 成立如下命题。

1. 加法单位元 (addition identity element):

$$\exists 0 \in R, \forall r \in R, \quad 0 + r = r + 0 = r$$

2. 乘法单位元 (multiplication identity element):

$$\exists 1 \in R, \forall r \in R, \quad 1 \cdot r = r \cdot 1 = r$$

3. 加法逆元 (addition inverse):

$$\forall r \in R, \exists -r \in R, \quad r + (-r) = (-r) + r = 0$$

4. 加法结合律 (addition associative):

$$\forall r, s, t \in R, \quad (r + s) + t = r + (s + t)$$

5. 乘法结合律 (multiplication associative):

$$\forall r, s, t \in R, \quad (r \cdot s) \cdot t = r \cdot (s \cdot t)$$

6. 加法交换律 (addition commutative):

$$\forall r, s \in R, \quad r + s = s + r$$

7. 分配律 (distributive):

$$\forall r, s, t \in R, \quad (r + s) \cdot t = r \cdot t + s \cdot t$$

$$\forall r, s, t \in R, \quad r \cdot (s + t) = r \cdot s + r \cdot t$$



定义 4.1.4 (交换环 commutative ring)

称代数系统 $(R, +, \cdot)$ 为交换环, 如果加法运算 $+: R \times R \rightarrow R$ 和乘法运算 $\cdot: R \times R \rightarrow R$ 成立如下命题。

1. 加法单位元 (addition identity element):

$$\exists 0 \in R, \forall r \in R, \quad 0 + r = r + 0 = r$$

2. 乘法单位元 (multiplication identity element):

$$\exists 1 \in R, \forall r \in R, \quad 1 \cdot r = r \cdot 1 = r$$

3. 加法逆元 (addition inverse):

$$\forall r \in R, \exists -r \in R, \quad r + (-r) = (-r) + r = 0$$

4. 加法结合律 (addition associative):

$$\forall r, s, t \in R, \quad (r + s) + t = r + (s + t)$$

5. 乘法结合律 (multiplication associative):

$$\forall r, s, t \in R, \quad (r \cdot s) \cdot t = r \cdot (s \cdot t)$$

6. 加法交换律 (addition commutative):

$$\forall r, s \in R, \quad r + s = s + r$$

7. 乘法交换律 (multiplication commutative):

$$\forall r, s \in R, \quad r \cdot s = s \cdot r$$

8. 分配律 (distributive):

$$\forall r, s, t \in R, \quad (r + s) \cdot t = r \cdot t + s \cdot t$$

$$\forall r, s, t \in R, \quad r \cdot (s + t) = r \cdot s + r \cdot t$$

**定义 4.1.5 (无零因子环 without zero-divisor ring)**

称代数系统 $(R, +, \cdot)$ 为无零因子环, 如果加法运算 $+: R \times R \rightarrow R$ 和乘法运算 $\cdot: R \times R \rightarrow R$ 成立如下命题。

1. 加法单位元 (addition identity element):

$$\exists 0 \in R, \forall r \in R, \quad 0 + r = r + 0 = r$$

2. 乘法单位元 (multiplication identity element):

$$\exists 1 \in R, \forall r \in R, \quad 1 \cdot r = r \cdot 1 = r$$

3. 加法逆元 (addition inverse):

$$\forall r \in R, \exists -r \in R, \quad r + (-r) = (-r) + r = 0$$

4. 加法结合律 (addition associative):

$$\forall r, s, t \in R, \quad (r + s) + t = r + (s + t)$$

5. 乘法结合律 (multiplication associative):

$$\forall r, s, t \in R, \quad (r \cdot s) \cdot t = r \cdot (s \cdot t)$$

6. 加法交换律 (addition commutative):

$$\forall r, s \in R, \quad r + s = s + r$$

7. 消去律 (cancellation):

$$\forall r, s \in R, \quad r \cdot s = 0 \implies r = 0 \text{ 或 } s = 0$$

8. 分配律 (distributive):

$$\forall r, s, t \in R, \quad (r + s) \cdot t = r \cdot t + s \cdot t$$

$$\forall r, s, t \in R, \quad r \cdot (s + t) = r \cdot s + r \cdot t$$

**定义 4.1.6 (整环 integral domain)**

称代数系统 $(R, +, \cdot)$ 为整环, 如果加法运算 $+: R \times R \rightarrow R$ 和乘法运算 $\cdot: R \times R \rightarrow R$ 成立如下命题。

1. 加法单位元 (addition identity element):

$$\exists 0 \in R, \forall r \in R, \quad 0 + r = r + 0 = r$$

2. 乘法单位元 (multiplication identity element):

$$\exists 1 \in R, \forall r \in R, \quad 1 \cdot r = r \cdot 1 = r$$

3. 加法逆元 (addition inverse):

$$\forall r \in R, \exists -r \in R, \quad r + (-r) = (-r) + r = 0$$

4. 加法结合律 (addition associative):

$$\forall r, s, t \in R, \quad (r + s) + t = r + (s + t)$$

5. 乘法结合律 (multiplication associative):

$$\forall r, s, t \in R, \quad (r \cdot s) \cdot t = r \cdot (s \cdot t)$$

6. 加法交换律 (addition commutative):

$$\forall r, s \in R, \quad r + s = s + r$$

7. 乘法交换律 (multiplication commutative):

$$\forall r, s \in R, \quad r \cdot s = s \cdot r$$

8. 消去律 (cancellation):

$$\forall r, s \in R, \quad r \cdot s = 0 \implies r = 0 \text{ 或 } s = 0$$

9. 分配律 (distributive):

$$\forall r, s, t \in R, \quad (r + s) \cdot t = r \cdot t + s \cdot t$$

$$\forall r, s, t \in R, \quad r \cdot (s + t) = r \cdot s + r \cdot t$$



定义 4.1.7 (除环 division ring)

称代数系统 $(R, +, \cdot)$ 为除环, 如果加法运算 $+: R \times R \rightarrow R$ 和乘法 $\cdot: R \times R \rightarrow R$ 成立如下命题。

1. 加法单位元 (addition identity element):

$$\exists 0 \in R, \forall r \in R, \quad 0 + r = r + 0 = r$$

2. 乘法单位元 (multiplication identity element):

$$\exists 1 \in R, \forall r \in R, \quad 1 \cdot r = r \cdot 1 = r$$

3. 加法逆元 (addition inverse):

$$\forall r \in R, \exists -r \in R, \quad r + (-r) = (-r) + r = 0$$

4. 乘法逆元 (multiplication inverse):

$$\forall r \in R \setminus \{0\}, \exists r^{-1} \in R, \quad r \cdot r^{-1} = r^{-1} \cdot r = 1$$

5. 加法结合律 (addition associative):

$$\forall r, s, t \in R, \quad (r + s) + t = r + (s + t)$$

6. 乘法结合律 (multiplication associative):

$$\forall r, s, t \in R, \quad (r \cdot s) \cdot t = r \cdot (s \cdot t)$$

7. 加法交换律 (addition commutative):

$$\forall r, s \in R, \quad r + s = s + r$$

8. 分配律 (distributive):

$$\forall r, s, t \in R, \quad (r + s) \cdot t = r \cdot t + s \cdot t$$

$$\forall r, s, t \in R, \quad r \cdot (s + t) = r \cdot s + r \cdot t$$



定义 4.1.8 (域 field)

称代数系统 $(F, +, \cdot)$ 为域, 如果加法运算 $+: F \times F \rightarrow F$ 和乘法运算 $\cdot: F \times F \rightarrow F$ 成立如下命题。

1. 加法单位元 (addition identity element):

$$\exists 0 \in F, \forall f \in F, \quad 0 + f = f + 0 = f$$

2. 乘法单位元 (multiplication identity element):

$$\exists 1 \in F \setminus \{0\}, \forall f \in F, \quad 1 \cdot f = f \cdot 1 = f$$

3. 加法逆元 (addition inverse):

$$\forall f \in F, \exists -f \in F, \quad f + (-f) = (-f) + f = 0$$

4. 乘法逆元 (multiplication inverse):

$$\forall f \in F \setminus \{0\}, \exists f^{-1} \in F, \quad f \cdot f^{-1} = f^{-1} \cdot f = 1$$

5. 加法交换律 (addition commutative):

$$\forall f, g \in F, \quad f + g = g + f$$

6. 乘法交换律 (multiplication commutative):

$$\forall f, g \in F, \quad f \cdot g = g \cdot f$$

7. 加法结合律 (addition associative):

$$\forall f, g, h \in F, \quad (f + g) + h = f + (g + h)$$

8. 乘法结合律 (multiplication associative):

$$\forall f, g, h \in F, \quad (f \cdot g) \cdot h = f \cdot (g \cdot h)$$

9. 分配律 (distributive):

$$\forall f, g, h \in F, \quad (f + g) \cdot h = f \cdot h + g \cdot h$$

$$\forall f, g, h \in F, \quad f \cdot (g + h) = f \cdot g + f \cdot h$$



笔记

- 环 $(R, +, \cdot)$ 包含交换群 $(R, +)$ 和幺半群 (R, \cdot) , 并且满足分配律。
- 除环 $(R, +, \cdot)$ 包含交换群 $(R, +)$ 和群 $(R \setminus \{0\}, \cdot)$, 并且满足分配律。
- 域 $(F, +, \cdot)$ 包含交换群 $(F, +)$ 和交换群 $(F \setminus \{0\}, \cdot)$, 并且满足分配律。

定义 4.1.9 (整数环 integer ring)

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, 其中 $[a]_n + [b]_n = [a + b]_n$, $[a]_n \cdot [b]_n = [ab]_n$ 。



定义 4.1.10 (矩阵环 matrix ring)

$$\mathfrak{gl}_n(\mathbb{R}) = \{\mathbb{R} \text{ 上的 } n \times n \text{ 可逆矩阵}\}$$

$$\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) : \text{tr}(M) = 0\}$$

$$\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) : \text{tr}(M) = 0, M + M^t = 0\}$$

$$\mathfrak{gl}_n(\mathbb{C}) = \{\mathbb{C} \text{ 上的 } n \times n \text{ 可逆矩阵}\}$$

$$\mathfrak{sl}_n(\mathbb{C}) = \{M \in \mathfrak{gl}_n(\mathbb{C}) : \text{tr}(M) = 0\}$$

$$\mathfrak{su}_n(\mathbb{C}) = \{M \in \mathfrak{gl}_n(\mathbb{C}) : \text{tr}(M) = 0, M + M^\dagger = 0\}$$

**定义 4.1.11 (减法 subtraction)**

定义环 $(R, +, \cdot)$ 的减法为 $r - s = r + (-s)$ 。

**定义 4.1.12 (整数数乘 integer multiplication)**

$$\mathbb{Z} \times R \longrightarrow R$$

$$(n, r) \longmapsto nr = \begin{cases} \underbrace{r + \cdots + r}_{n \uparrow}, & n \in \mathbb{N}^* \\ 0, & n = 0 \\ (-n)r, & n \in -\mathbb{N}^* \end{cases}$$

**定义 4.1.13 (非负整数幂 non-negative integer power)**

$$\mathbb{N} \times R \setminus \{(0, 0)\} \longrightarrow R$$

$$(n, r) \longmapsto r^n = \begin{cases} \underbrace{r \cdots r}_{n \uparrow}, & n \in \mathbb{N}^* \\ 1, & n = 0 \end{cases}$$

**命题 4.1.1 (环的简单性质)**

- $-(-r) = r$
- $0r = 0 \cdot r = r \cdot 0 = 0$
- $-r = (-1)r = 0 - r = -1 \cdot r = r \cdot (-1)$
- $(-r) \cdot (-s) = r \cdot s$

**命题 4.1.2 (零环的等价条件)**

对于环 $(R, +, \cdot)$, 如果 $0 = 1$, 那么 R 为零环。



证明 这几乎是显然的, 因为

$$1 \cdot r = r, \quad 0 \cdot r = 0$$

4.1.2 零因子与单位

定义 4.1.14 (左零因子 left-zero-divisor)

称 $e \in R$ 为环 $(R, +, \cdot)$ 的左零因子, 如果存在非零元 $u \in R$, 使得成立 $e \cdot u = 0$; 换言之

$$\exists u \in R \setminus \{0\}, \quad e \cdot u = 0$$



定义 4.1.15 (右零因子 right-zero-divisor)

称 $e \in R$ 为环 $(R, +, \cdot)$ 的右零因子, 如果存在非零元 $v \in R$, 使得成立 $v \cdot e = 0$; 换言之

$$\exists v \in R \setminus \{0\}, \quad v \cdot e = 0$$



定义 4.1.16 (零因子 zero-divisor)

称 $e \in R$ 为环 $(R, +, \cdot)$ 的零因子, 如果存在非零元 $r \in R$, 使得成立 $e \cdot r = 0$ 或 $r \cdot e = 0$; 换言之

$$\exists r \in R \setminus \{0\}, \quad e \cdot r = 0 \text{ 或 } r \cdot e = 0$$



定义 4.1.17 (非零因子 non-zero-divisor)

称 $e \in R$ 为环 $(R, +, \cdot)$ 的非零因子, 如果成立如下命题之一。

1. e 不为零因子。
2. 对于任意非零元 $r \in R$, 成立 $e \cdot r \neq 0$ 且 $r \cdot e \neq 0$; 换言之

$$\forall r \in R \setminus \{0\}, \quad e \cdot r \neq 0 \text{ 且 } r \cdot e \neq 0$$

3. 对于任意 $r \in R$, 如果 $e \cdot r = 0$ 或 $r \cdot e = 0$, 那么 $r = 0$; 换言之

$$\forall r \in R, \quad e \cdot r = 0 \text{ 或 } r \cdot e = 0 \implies r = 0$$



定义 4.1.18 (无零因子环 without zero-divisor ring)

称无非平凡零因子的非零环为无零因子环; 换言之, 称非零环 $(R, +, \cdot)$ 为无零因子环, 如果

$$\forall r, s \in R, \quad r \cdot s = 0 \implies r = 0 \text{ 或 } s = 0$$



定义 4.1.19 (整环 integral domain)

称无零因子非零交换环为整环; 换言之, 称非零环 $(R, +, \cdot)$ 为整环, 如果

$$\forall r, s \in R, \quad r \cdot s = s \cdot r$$

$$\forall r, s \in R, \quad r \cdot s = 0 \implies r = 0 \text{ 或 } s = 0$$



例题 4.1 证明: 方程 $x^2 = 1$ 在整环中仅存在根 $x = \pm 1$ 。

证明

$$x^2 = 1 \implies (x+1) \cdot (x-1) = 0 \implies x+1=0 \text{ 或 } x-1=0 \implies x = \pm 1$$

命题 4.1.3 (无零因子环的非零子环)

无零因子环的非零子环为无零因子环。



命题 4.1.4 (整环的非零子环)

整环的非零子环为整环。



命题 4.1.5

对于环 $(R, +, \cdot)$, $e \in R$ 不为左零因子 \iff 左乘 e 函数 $R \rightarrow R$ 为单射。

**命题 4.1.6**

整环 $(R, +, \cdot)$ 的非零元为非零因子。

**命题 4.1.7 (消去律 cancellation)**

环 $(R, +, \cdot)$ 的非零因子 $e \in R$ 满足对于任意 $r, s \in R$, 成立

$$e \cdot r = e \cdot s \implies r = sr \cdot e = s \cdot e \implies r = s$$

**定义 4.1.20 (左单位 left-unit)**

称 $e \in R$ 为环 $(R, +, \cdot)$ 的左单位, 如果存在 $u \in R$, 使得成立 $e \cdot u = 1$; 换言之

$$\exists u \in R, \quad e \cdot u = 1$$

**定义 4.1.21 (右单位 right-unit)**

称 $e \in R$ 为环 $(R, +, \cdot)$ 的右单位, 如果存在 $v \in R$, 使得成立 $v \cdot e = 1$; 换言之

$$\exists v \in R, \quad v \cdot e = 1$$

**定义 4.1.22 (单位 unit)**

称 $e \in R$ 为环 $(R, +, \cdot)$ 的单位, 如果存在 $e^{-1} \in R$, 使得成立 $e \cdot e^{-1} = e^{-1} \cdot e = 1$; 换言之

$$\exists e^{-1} \in R, \quad e \cdot e^{-1} = e^{-1} \cdot e = 1$$

**定义 4.1.23 (单位群 group of units)**

称环 $(R, +, \cdot)$ 的单位依乘法运算 $\cdot : R \times R \rightarrow R$ 构成的群为单位群 (R^\times, \cdot) 。



证明 对于封闭性, 任取单位 $r, s \in R$, 那么存在非零元 $u, v \in R$, 使得成立 $u \cdot r = s \cdot v = 1$, 因此 $u \cdot (r \cdot s) = (r \cdot s) \cdot v = 1$, 进而 $r \cdot s$ 为单元。

对于单位元, 注意到 $1 \in R$ 为单位。

对于逆元, 任取单位 $e \in R$, 那么存在非零元 $u, v \in R$, 使得成立 $u \cdot e = e \cdot v = 1$, 进而 $u = u \cdot 1 = u \cdot e \cdot v = 1 \cdot v = v$ 。

对于结合律, 这是显然的!

定义 4.1.24 (单位的性质)

- $e \in R$ 为环 $(R, +, \cdot)$ 的左单位 \iff 左乘 e 函数 $R \rightarrow R$ 为满射。
- 如果 $e \in R$ 为环 $(R, +, \cdot)$ 的左单位, 那么右乘 e 函数 $R \rightarrow R$ 为单射, 即 e 不为右零因子。
- 单位的加法逆元为单位。
- 单位的乘法逆元为单位。

**命题 4.1.8**

对于环 $(R, +, \cdot)$, 成立

$$r \in R \text{ 为左单位 } \iff R = r \cdot R$$

$$r \in R \text{ 为右单位 } \iff R = R \cdot r$$



证明 对于必要性, 如果 $r \in R$ 为左单位, 那么注意到对于任意 $x \in R$, 成立

$$x = 1 \cdot x = (r \cdot s) \cdot x = r \cdot (s \cdot x) \in r \cdot R$$

因此 $R \subset r \cdot R$, 而显然 $r \cdot R \subset R$, 因此 $R = r \cdot R$ 。

对于充分性, 如果 $R = r \cdot R$, 那么由 $1 \in R$, 可知存在 $s \in R$, 使得成立 $r \cdot s = 1$, 因此 $r \in R$ 为左单位。

命题 4.1.9

对于环 $(R, +, \cdot)$, 如果 $e \in R$ 为右单位, 且存在至少两个左逆, 那么 e 不为左零因子, 但为右零因子。

证明 如果存在 $u, v, w \in R$, 使得成立 $u \cdot e = 1$ 且 $v \cdot e = w \cdot e = 0$, 因此 v, e 之一为非零元, 进而 e 为有零因子。反证, 如果 e 为左零因子, 那么存在非零元 $r \in R$, 使得成立 $e \cdot r = 0$, 进而 $r = 1 \cdot r = u \cdot e \cdot r = u \cdot 0 = 0$, 矛盾! 因此 e 不为左零因子。

定义 4.1.25 (除环 division ring)

称非零元为单位的非零环为除环; 换言之, 称非零环 $(R, +, \cdot)$ 为除环, 如果

$$\forall r \in R \setminus \{0\}, \exists r^{-1} \in R, \quad r \cdot r^{-1} = r^{-1} \cdot r = 1$$

定义 4.1.26 (域 field)

交换除环为域; 换言之, 称非零环 $(R, +, \cdot)$ 为域, 如果

$$\begin{aligned} \forall r, s \in R, & \quad r \cdot s = s \cdot r \\ \forall r \in R \setminus \{0\}, \exists r^{-1} \in R, & \quad r \cdot r^{-1} = r^{-1} \cdot r = 1 \end{aligned}$$

命题 4.1.10 (除环的等价条件)

对于非零环 $(R, +, \cdot)$, 成立

$$R \text{ 为除环} \iff R \text{ 仅存在平凡左理想} \iff R \text{ 仅存在平凡右理想}$$

证明 如果 R 为除环, 任取 R 的非零左理想 I , 那么存在 $r \in I \setminus \{0\}$, 而 R 为除环, 因此 $1 = r^{-1} \cdot r \in I$, 那么 $I = R$, 进而 R 仅存在平凡左理想。同理对于 R 的右理想。

如果 R 不为除环, 那么存在 $r_0 \in R \setminus \{0\}$, 使得对于任意 $r \in R$, 成立 $r \cdot r_0 \neq 1$ 且 $r_0 \cdot r \neq 1$ 。由命题 4.3.3, 考虑左理想 $R \cdot r_0$, 由条件假设, $1 \notin R \cdot r_0$, 因此 $\{0\} \subsetneq R \cdot r_0 \subsetneq R$, 进而 R 存在非平凡左理想 $R \cdot r_0$ 。同理对于 R 的右理想。

命题 4.1.11 (域的等价条件)

对于非零交换环 $(R, +, \cdot)$, 成立

$$R \text{ 为域} \iff R \text{ 仅存在平凡理想}$$

证明 如果 R 为域, 任取 R 的非零理想 I , 那么存在 $r \in I \setminus \{0\}$, 而 R 为域, 因此 $1 = r^{-1} \cdot r \in I$, 那么 $I = R$, 进而 R 仅存在平凡理想。

如果 R 不为域, 那么存在 $r_0 \in R \setminus \{0\}$, 使得对于任意 $r \in R$, 成立 $r_0 \cdot r \neq 1$ 。考虑主理想 (r_0) , 由条件假设, $1 \notin I$, 因此 $\{0\} \subsetneq (r_0) \subsetneq R$, 进而 R 存在非平凡理想 (r_0) 。

推论 4.1.1

对于环同态映射 $\varphi: F \rightarrow R$, 如果 F 为域, 那么或 $R = \{0\}$, 或 φ 为单的。

证明 由命题 4.3.2, $\ker \varphi$ 为域 F 的理想, 那么由命题 4.1.11, $\ker \varphi = \{0\}$ 或 $\ker \varphi = F$ 。

如果 $\ker \varphi = F$, 那么 $R = \{0\}$ 。

如果 $\ker \varphi = \{0\}$, 那么 φ 为单的。

定理 4.1.1 (Wedderburn 定理)

有限除环为域。



定理 4.1.2 (有限整环为域)

有限整环为域。



证明 对于有限整环 $(R, +, \cdot)$, 任取 $r \in R \setminus \{0\}$, 考虑主理想 (r) 。如果 $|(r)| < |R|$, 那么存在互异元素 $a, b \in R$, 使得成立 $a \cdot r = b \cdot r$ 。由消去律, $a = b$, 矛盾! 因此 $|(r)| = |R|$, 那么 $(r) = R$ 。注意到 $1 \in R = r \cdot R$, 那么存在 $s \in R$, 使得成立 $r \cdot s = s \cdot r = 1$, 进而 R 为域。

命题 4.1.12 (循环群为整环的等价条件)

$$\mathbb{Z}/p\mathbb{Z} \text{ 为整环} \iff \mathbb{Z}/p\mathbb{Z} \text{ 为除环} \iff \mathbb{Z}/p\mathbb{Z} \text{ 为域} \iff p \text{ 为素数}$$



证明 如果 p 为素数, 那么 $\mathbb{Z}/p\mathbb{Z}$ 为非零交换环。任取 $[n]_p \in \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$, 那么 $\gcd(n, p) = 1$ 。由定理 2.2.1, 存在 $a, b \in \mathbb{Z}$, 使得成立

$$an + bp = 1 \iff an \equiv 1 \pmod{p} \iff [an]_p = [1]_p \iff [a]_p[n]_p = [1]_p$$

因此 $\mathbb{Z}/p\mathbb{Z}$ 为域。

如果 p 不为素数, 那么存在 $1 < m, n < p$, 使得成立 $mn = p$, 因此 $[m]_p[n]_p = [0]_p$, 但是 $[m]_p \neq [0]_p$ 且 $[n]_p \neq [0]_p$, 于是 \mathbb{Z}_p 不成立消去律, 进而 \mathbb{Z}_p 不为整环, 亦不为除环。

命题 4.1.13

p^2 阶除环为交换环, 其中 p 为素数。



证明 如果 p^2 阶除环 R 不为交换群, 那么 $\text{Cent}(R) \subsetneq R$ 。而 $0, 1 \in \text{Cent}(R)$, 因此由命题 4.2.7, 以及 Lagrange 定理 2.8.8, 成立 $|\text{Cent}(R)| = p$ 。任取 $r \in R \setminus \text{Cent}(R)$, 那么 $\{r\} \cup \text{Cent}(R) \subset \text{Cent}_R(r)$, 因此 $|\text{Cent}_R(r)| \geq p + 1$, 于是 $|\text{Cent}_R(r)| = p^2$, 矛盾!

定义 4.1.27 (四元数环 quaternion ring)

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

其中 i, j, k 与 \mathbb{R} 可交换且满足

$$i^2 = j^2 = k^2 = -1, i \cdot j = -j \cdot i = k, j \cdot k = -k \cdot j = i, k \cdot i = -i \cdot k = j$$

称 \mathbb{H} 为四元数环, \mathbb{H} 中的元素为四元数, \mathbb{H} 的 8 阶非交换子群

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

为四元数群



命题 4.1.14

四元数环 $(\mathbb{H}, +, \cdot)$ 为除环。



证明

$$(a + bi + cj + dk) \cdot \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} = 1$$

命题 4.1.15 (\mathbb{H} 为 $\mathfrak{gl}_4(\mathbb{R})$ 的子环)

\mathbb{H} 为 $\mathfrak{gl}_4(\mathbb{R})$ 的子环, 单的同态映射为

$$\begin{aligned} \varphi: \quad \mathbb{H} &\longrightarrow \mathfrak{gl}_4(\mathbb{R}) \\ a + bi + cj + dk &\longmapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \end{aligned}$$

命题 4.1.16 (\mathbb{H} 为 $\mathfrak{gl}_2(\mathbb{C})$ 的子环)

\mathbb{H} 为 $\mathfrak{gl}_2(\mathbb{C})$ 的子环, 单的同态映射为

$$\begin{aligned} \psi: \quad \mathbb{H} &\longrightarrow \mathfrak{gl}_2(\mathbb{C}) \\ a + bi + cj + dk &\longmapsto \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \end{aligned}$$

4.1.3 幂零与 Bool 环**定义 4.1.28** (幂零 nilpotent)

称环 $(R, +, \cdot)$ 的元素 $r \in R$ 为幂零的, 如果存在 $n \in \mathbb{N}$, 使得成立 $r^n = 0$.

定义 4.1.29 (幂零根 nilradical)

定义环 $(R, +, \cdot)$ 的幂零根为

$$\text{Nil}(R) = \{r \in R : \exists n \in \mathbb{N}^*, \text{ s.t. } r^n = 0\}$$

定义 4.1.30 (即约部分 reduced part)

称 $R/\text{Nil}(R)$ 为交换环 $(R, +, \cdot)$ 的即约部分。

定义 4.1.31 (即约环 reduced ring)

称环 $(R, +, \cdot)$ 为即约环, 如果 $\text{Nil}(R) = \{0\}$.

命题 4.1.17

$$[m]_n \text{ 为 } \mathbb{Z}/n\mathbb{Z} \text{ 的幂零元} \iff \text{对于 } n \text{ 的任意素因子 } p \text{ 成立 } p \mid m$$

证明 对于必要性, 如果 $[m]_n$ 为 $\mathbb{Z}/n\mathbb{Z}$ 的幂零元素, 那么存在 $k \in \mathbb{N}$, 使得成立 $[m^k]_n = [0]_n$, 即 $n \mid m^k$. 任取 n 的素因子 p , 成立 $p \mid m^k$, 因此 $p \mid m$.

对于充分性, 如果对于 n 的任意素因子 p , 成立 $p \mid m$, 那么对 n 素因子分解 $n = \prod_{i=1}^r p_i$, 因此存在正整数 $\{s_i\}_{i=1}^r$, 使得对于任意 $1 \leq i \leq r$, 成立 $m = s_i p_i$, 注意到 $n = \prod_{i=1}^r p_i \mid \prod_{i=1}^r s_i p_i = m^r$, 因此 $n \mid m^r$, 进而 $[m]_n$ 为 $\mathbb{Z}/n\mathbb{Z}$ 的幂零元素。

例题 4.2 构造 $r, s \in R$ 为幂零的, 但是 $r + s$ 不为幂零的。

证明 定义

$$A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$$

那么

$$A^2 = B^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad (A+B)^n = 2^n \begin{pmatrix} 1 & 0 \\ 0 & (-1)^n \end{pmatrix}$$

命题 4.1.18

如果 $r, s \in R$ 为幂零的, 且 $r \cdot s = s \cdot r$, 那么 $r + s$ 为幂零的。



证明 记 $m, n \in \mathbb{N}$ 满足 $r^m = s^n = 0$, 注意到

$$(r+s)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} r^k \cdot s^{m+n-k} = 0$$

例题 4.3 构造环, 使其幂零根不为理想。

证明

$$A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$$

那么

$$A^2 = B^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad (A+B)^n = 2^n \begin{pmatrix} 1 & 0 \\ 0 & (-1)^n \end{pmatrix}$$

$$(AB)^n = 2^{2n-1} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad (BA)^n = 2^{2n-1} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

因此矩阵环 $\mathbf{M}_2(\mathbb{R})$ 的幂零根不为理想, 甚至不为子群。

命题 4.1.19

交换环的幂零根为理想。



证明 对于交换环 $(R, +, \cdot)$, 由命题 4.1.18, $\text{Nil}(R)$ 为 R 的子群。

任取 $r \in R$, 以及 $n \in \text{Nil}(R)$, 那么存在 $m \in \mathbb{N}^*$, 使得成立 $n^m = 0$ 。由于

$$(r \cdot n)^m = r^m \cdot n^m = r^m \cdot 0 = 0$$

因此 $r \cdot n \in \text{Nil}(R)$, 进而 $\text{Nil}(R)$ 为 R 的理想。

命题 4.1.20 (交换环的即约部分为即约环)

交换环的即约部分为即约环; 换言之, 对于交换环 $(R, +, \cdot)$, 成立 $\text{Nil}(R/\text{Nil}(R)) = \{\text{Nil}(R)\}$



证明 任取 $r + \text{Nil}(R) \in \text{Nil}(R/\text{Nil}(R))$, 因此存在 n , 使得成立

$$(r + \text{Nil}(R))^n = \text{Nil}(R) \iff r^n + \text{Nil}(R) = \text{Nil}(R) \iff r^n \in \text{Nil}(R)$$

$$\iff r \in \text{Nil}(R) \iff r + \text{Nil}(R) = \text{Nil}(R)$$

定义 4.1.32 (Bool 环 Boolean ring)

称非零环 $(R, +, \cdot)$ 为 Bool 环, 如果对于任意 $r \in R$, 成立 $r^2 = r$ 。



例题 4.4 对于集合 S , 定义二元运算

$$\begin{aligned} + : \mathcal{P}(S) \times \mathcal{P}(S) &\rightarrow \mathcal{P}(S) \\ (A, B) &\mapsto (A \cup B) \setminus (A \cap B) \\ \cdot : \mathcal{P}(S) \times \mathcal{P}(S) &\rightarrow \mathcal{P}(S) \\ (A, B) &\mapsto A \cap B \end{aligned}$$

那么 $(\mathcal{P}(S), +, \cdot)$ 为 Bool 环。

命题 4.1.21 (Bool 环的特征)

Bool 环的特征为 2。

证明 由于 Ring 范畴的初始对象为整数环 \mathbb{Z} , 那么对于 Bool 环 $R \in \text{Obj}(\text{Ring})$, 存在且存在唯一环同态映射 $\varphi : \mathbb{Z} \rightarrow R$, $n \mapsto n1_R$ 。注意到对于任意 $r \in R$, 成立

$$2r = (2r)^2 = (r + r)^2 = 4r^2 = 4r \implies 2r = 0_R$$

因此 $\ker \varphi \supset 2\mathbb{Z}$ 。

如果存在奇数 m , 使得成立 $m \in \ker \varphi$, 那么 $\varphi(m) = 0_R$, 此时

$$1_R = \varphi(1) = \varphi(m - (m - 1)) = \varphi(m) - \varphi(m - 1) = 0_R$$

由命题 4.1.2, R 为零环, 矛盾! 进而 $\ker \varphi = 2\mathbb{Z}$, R 的特征为 2。

命题 4.1.22 (Bool 环为交换环)

Bool 环为交换环。

证明 对于任意 $r, s \in R$, 成立

$$r + s = (r + s)^2 = r^2 + r \cdot s + s \cdot r + s^2 = r + r \cdot s + s \cdot r + s \implies r \cdot s + s \cdot r = 0$$

因此由命题 4.1.21

$$r \cdot s = r \cdot s + 0 = r \cdot s + r \cdot s + s \cdot r = 2(r \cdot s) + s \cdot r = 0 + s \cdot r = s \cdot r$$

进而 Bool 环 R 为交换环。

命题 4.1.23

如果整环 R 为 Bool 环, 那么 $R \cong \mathbb{Z}/2\mathbb{Z}$ 。

证明 由于 R 为 Bool 环, 那么对于任意 $r \in R$, 成立 $r(r - 1_R) = 0_R$ 。而 R 为整环, 那么 $r = 0_R$, 或 $r = 1_R$ 。又因为 R 不为零环, 那么 $0_R \neq 1_R$, 因此 $R = \{0_R, 1_R\}$, 进而 $R \cong \mathbb{Z}/2\mathbb{Z}$ 。

4.1.4 多项式环

定义 4.1.33 (环扩张 ring extension)

对于环 R 与 S , 称 S/R 为环扩张, 如果存在单环同态映射 $\varphi : R \hookrightarrow S$ 。

定义 4.1.34 (生成环)

对于环扩张 S/R , 定义 R 关于集合 $A \subset S$ 的生成环为

$$R[A] = \bigcap_{T \supset R \cup A \text{ 为环}} T$$

定义 4.1.35 (多项式环 polynomial ring)

对于环 R , 定义其多项式环

$$R[x] = \left\{ \sum_{k=0}^n a_k x^k : a_k \in R, n \in \mathbb{N} \right\}$$

**定义 4.1.36 (次数 degree)**

对于多项式环 $R[x]$, 定义多项式 $f(x) = \sum_{k=0}^n a_k x^k \in R[x]$ 的次数为

$$\deg(f(x)) = \max\{k : a_k \neq 0, 0 \leq k \leq n\}$$

特别的, 定义 $\deg(0) = -\infty$ 。

**命题 4.1.24**

对于 $f(x), g(x) \in R[x]$, 成立

$$\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x)))$$

**命题 4.1.25 (积的次数为次数的和)**

对于 $f(x), g(x) \in R[x]$, 如果 R 为整环, 那么

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$



证明 记 $f(x) = \sum_{k=0}^m a_k x^k, g(x) = \sum_{k=0}^n b_k x^k$, 其中 $a_m, b_n \neq 0$, 由于 R 为整环, 那么 $a_m b_n \neq 0$, 因此

$$\begin{aligned} f(x)g(x) &= \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j x^k = a_m b_n x^{m+n} + \sum_{k=0}^{m+n-1} \sum_{i+j=k} a_i b_j x^k \\ \implies \deg(f(x)g(x)) &= m+n = \deg(f(x)) + \deg(g(x)) \end{aligned}$$

命题 4.1.26 (多项式整环)

$$R[x] \text{ 为整环} \iff R \text{ 为整环}$$



证明 如果 $R[x]$ 为整环, 那么任取 $a, b \in R$, 使得成立 $ab = 0$, 注意到 $ax, bx \in R[x]$, 因此 $ax \cdot bx = abx^2 = 0$, 进而 $ax = 0$ 或 $bx = 0$, 于是 $a = 0$ 或 $b = 0$, 那么 R 为整环。

如果 R 为整环, 那么任取 $f(x), g(x) \in R[x]$, 使得成立 $f(x)g(x) = 0$, 由命题 4.1.25, 可得 $\deg(f(x)) + \deg(g(x)) = \deg(f(x)g(x)) = d(0) = -\infty$, 因此 $f(x) = 0$ 或 $g(x) = 0$, 进而 $R[x]$ 为整环。

定义 4.1.37 (整除)

对于多项式整环 $R[x]$, 称多项式 $g(x) \in R[x]$ 整除多项式 $f(x) \in R[x]$, 并记作 $g(x) \mid f(x)$, 如果存在多项式 $h(x) \in R[x]$, 使得成立 $f(x) = g(x)h(x)$ 。

**定义 4.1.38 (不可约多项式)**

对于多项式整环 $R[x]$, 称多项式 $f(x) \in R[x]$ 为不可约多项式, 如果 $f(x)$ 不为常多项式, 且不存在 $g(x), h(x) \in R[x]$, 使得成立

$$f(x) = g(x)h(x), \quad \deg(g(x)) < \deg(f(x)), \quad \deg(h(x)) < \deg(f(x))$$



定义 4.1.39 (可约多项式)

对于多项式整环 $R[x]$, 称多项式 $f(x) \in R[x]$ 为可约多项式, 如果 $f(x)$ 为常多项式, 或存在 $g(x), h(x) \in R[x]$, 使得成立

$$f(x) = g(x)h(x), \quad \deg(g(x)) < \deg(f(x)), \quad \deg(h(x)) < \deg(f(x))$$

**定义 4.1.40 (幂级数环 ring of power series)**

对于环 R , 定义幂级数环

$$R[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n : a_n \in R \right\}$$



例题 4.5 $1 - x \in R[[x]]$ 的乘法逆元为 $\sum_{n=0}^{\infty} x^n$.

命题 4.1.27

$$\sum_{n=0}^{\infty} a_n x^n \text{ 为 } R[[x]] \text{ 的单位} \iff a_0 \text{ 为 } R \text{ 的单位}$$



证明 如果 $\sum_{n=0}^{\infty} a_n x^n$ 为 $R[[x]]$ 的单位, 那么存在 $\sum_{n=0}^{\infty} b_n x^n \in R[[x]]$, 使得成立

$$1 = \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \sum_{i+j=n} a_i b_j x^n \implies a_0 b_0 = 1$$

$$1 = \left(\sum_{n=0}^{\infty} b_n x^n \right) \left(\sum_{n=0}^{\infty} a_n x^n \right) = \sum_{n=0}^{\infty} \sum_{i+j=n} a_i b_j x^n \implies b_0 a_0 = 1$$

因此 $a_0 \in R$ 为单位。

如果 a_0 为 R 的单位, 那么存在 $b_0, c_0 \in R$, 使得成立 $a_0 b_0 = c_0 a_0 = 1$, 递归定义

$$b_n = -c_0 \sum_{i=1}^n a_i b_{n-i}, \quad c_n = -\sum_{i=1}^n c_{n-i} a_i \cdot b_0, \quad n \in \mathbb{N}^*$$

那么对于任意 $n \in \mathbb{N}^*$, 成立 $\sum_{i+j=n} a_i b_j x^n = \sum_{i+j=n} c_i a_j x^n = 0$, 进而

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \sum_{i+j=n} a_i b_j x^n = a_0 b_0 + \sum_{n=1}^{\infty} \sum_{i+j=n} a_i b_j x^n = 1$$

$$\left(\sum_{n=0}^{\infty} c_n x^n \right) \left(\sum_{n=0}^{\infty} a_n x^n \right) = \sum_{n=0}^{\infty} \sum_{i+j=n} c_i a_j x^n = c_0 a_0 + \sum_{n=1}^{\infty} \sum_{i+j=n} c_i a_j x^n = 1$$

因此 $\sum_{n=0}^{\infty} a_n x^n$ 为 $R[[x]]$ 的单位。

命题 4.1.28 (幂级数整环)

$$R[[x]] \text{ 为整环} \iff R \text{ 为整环}$$



证明 如果 $R[[x]]$ 为整环, 那么任取 $a, b \in R$, 使得成立 $ab = 0$, 注意到 $ax, bx \in R[[x]]$, 因此 $ax \cdot bx = abx^2 = 0$, 进而 $ax = 0$ 或 $bx = 0$, 于是 $a = 0$ 或 $b = 0$, 那么 R 为整环。

如果 R 为整环, 那么任取 $f(x) = \sum_{n=0}^{\infty} a_n x^n, g(x) = \sum_{n=0}^{\infty} b_n x^n$, 使得成立 $f(x)g(x) = 0$ 。反证, 如果 $f(x) \neq 0$

且 $g(x) \neq 0$, 那么记 $s = \min\{n \in \mathbb{N} : a_n \neq 0\}, r = \min\{n \in \mathbb{N} : b_n \neq 0\}$, 因此 $f(x) = \sum_{n=0}^{\infty} a_n x^n = x^s \sum_{n=0}^{\infty} a_{n+s} x^n, g(x) = x^r \sum_{n=0}^{\infty} b_{n+r} x^n$, 进而

$$\begin{aligned} 0 &= f(x)g(x) = x^{s+r} \left(\sum_{n=0}^{\infty} a_{n+s} x^n \right) \left(\sum_{n=0}^{\infty} b_{n+r} x^n \right) = \sum_{n=0}^{\infty} \sum_{i+j=n} a_{i+s} b_{j+r} x^{n+s+r} \\ &\implies 0 = a_s b_r \implies a_s = 0 \text{ 或 } b_r = 0 \end{aligned}$$

矛盾! 因此 $f(x) = 0$ 或 $g(x) = 0$, 进而 $R[[x]]$ 为整环。

定义 4.1.41 (多元多项式环 multivariate polynomial rings)

对于环 R , 定义多元多项式环

$$\begin{aligned} R[x_1, \dots, x_n] &= R[x_1] \cdots [x_n] = \left\{ \sum_{k=0}^m \sum_{r_1+\dots+r_n=k} a_{r_1, \dots, r_n} x_1^{r_1} \cdots x_n^{r_n} : a_{r_1, \dots, r_n} \in R, r_s \in \mathbb{N}, m \in \mathbb{N} \right\} \\ R[x_1, x_2, \dots] &= R[x_1][x_2] \cdots = \left\{ \sum_{k=0}^n \sum_{r_{s_1}+\dots+r_{s_m}=k} a_{r_{s_1}, \dots, r_{s_m}}^{(s_1, \dots, s_m)} x_{s_1}^{r_{s_1}} \cdots x_{s_m}^{r_{s_m}} : a_{r_{s_1}, \dots, r_{s_m}}^{(s_1, \dots, s_m)} \in R, r_{s_t} \in \mathbb{N}, m, n \in \mathbb{N} \right\} \end{aligned}$$

4.1.5 单环与群环

定义 4.1.42 (单环 monoid ring)

对于幺半群 M 和环 R , 定义单环

$$R[M] = \left\{ \sum_{m \in M} a_m m : a_m \in R \right\}$$

定义 4.1.43 (群环 group ring)

对于群 G 和环 R , 定义群环

$$R[G] = \left\{ \sum_{g \in G} a_g g : a_g \in R \right\}$$

4.2 Ring 范畴

4.2.1 环同态映射

定义 4.2.1 (环同态映射 ring homomorphism)

对于环 $(R, +, \cdot)$ 和 $(S, +, \cdot)$, 称映射 $\varphi: R \rightarrow S$ 为环同态映射, 如果成立

$$\begin{aligned} \varphi(r+s) &= \varphi(r) + \varphi(s) \\ \varphi(r \cdot s) &= \varphi(r) \cdot \varphi(s) \\ \varphi(1_R) &= 1_S \end{aligned}$$

命题 4.2.1

如果 $\varphi: \{0\} \rightarrow R$ 为环同态映射, 那么 $R = \{0\}$ 。

证明 注意到

$$0_R = \varphi(0) = \varphi(1) = 1_R$$

由命题 4.1.2, $R = \{0\}$ 。

命题 4.2.2

对于环 $(R, +, \cdot)$ 和环 $(S, +, \cdot)$, 如果满的集合函数 $\varphi: R \rightarrow S$ 对于 $+$ 与 \cdot 运算封闭, 那么 $\varphi(1_R) = 1_S$ 。

证明 任取 $s \in S$, 由于 φ 为满射, 因此存在 $r \in R$, 使得成立 $\varphi(r) = s$ 。由于

$$s \cdot \varphi(1_R) = \varphi(r) \cdot \varphi(1_R) = \varphi(r \cdot 1_R) = \varphi(r) = s\varphi(1_R) \cdot s = \varphi(1_R) \cdot \varphi(r) = \varphi(1_R \cdot s) = \varphi(r) = s$$

那么 $\varphi(1_R) = 1_S$ 。

命题 4.2.3

对于环 $(R, +, \cdot)$ 和整环 $(S, +, \cdot)$, 如果非零集合函数 $\varphi: R \rightarrow S$ 对于 $+$ 与 \cdot 运算封闭, 那么 $\varphi(1_R) = 1_S$ 。

证明 因为 $\varphi \neq 0$, 因此存在 $r \in R$, 使得成立 $\varphi(r) \neq 0$ 。注意到

$$\varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\varphi(1_R)$$

而 S 为整环, 因此 $\varphi(1_R) = 1_S$ 。

定义 4.2.2 (Ring 范畴)

$$\text{Obj}(\text{Ring}) = \{\text{环}(R, +, \cdot)\}$$

$$\text{Hom}_{\text{Ring}}((R, +, \cdot), (S, +, \cdot)) = \{\text{环同态映射 } \varphi: R \rightarrow S\}$$

命题 4.2.4 (Ring 范畴的初始对象)

Ring 范畴的初始对象为整数环 \mathbb{Z} 。换言之, 对于任意环 $R \in \text{Obj}(\text{Ring})$, 存在且存在唯一环同态映射

$$\varphi: \mathbb{Z} \longrightarrow R$$

$$n \longmapsto n1_R$$

命题 4.2.5 (Ring 范畴的终止对象)

Ring 范畴的终止对象为零环 $\{0\}$ 。换言之, 对于任意环 $R \in \text{Obj}(\text{Ring})$, 存在且存在唯一环同态映射 $\varphi: R \rightarrow \{0\}$, $r \mapsto 0$ 。

4.2.2 子环与中心**定义 4.2.3 (扩环 ring extension)**

称环 $(S, +, \cdot)$ 为环 $(R, +, \cdot)$ 的扩环, 如果存在单环同态映射 $\varphi: R \rightarrow S$ 。

定义 4.2.4 (子环 subring)

称代数系统 $(S, +, \cdot)$ 为环 $(R, +, \cdot)$ 的子环, 如果存在单环同态映射 $\varphi: S \rightarrow R$ 。

定义 4.2.5 (子环 subring)

称代数系统 $(S, +, \cdot)$ 为环 $(R, +, \cdot)$ 的子环, 如果 $(S, +)$ 为 $(R, +)$ 的子群, 且 S 对于 \cdot 运算封闭, 同时 $1 \in S$ 。

**命题 4.2.6 (子环的像为子环)**

对于环同态映射 $\varphi: R \rightarrow S$, 如果 $I \subset R$ 为 R 的子环, 那么 $\varphi(I)$ 为 S 的子环。



证明 作包含映射 $i: \varphi(I) \hookrightarrow S$, 由于对于任意 $r, s \in I$, 成立

$$i(\varphi(r) + \varphi(s)) = i(\varphi(r + s)) = \varphi(r + s) = \varphi(r) + \varphi(s) = i(\varphi(r)) + i(\varphi(s))$$

$$i(\varphi(r) \cdot \varphi(s)) = i(\varphi(r \cdot s)) = \varphi(r \cdot s) = \varphi(r) \cdot \varphi(s) = i(\varphi(r)) \cdot i(\varphi(s))$$

$$i(1_S) = i(\varphi(1_R)) = \varphi(1_R) = 1_S$$

因此 i 为环同态映射, 进而 $\varphi(I)$ 为 S 的子环。

定义 4.2.6 (中心 center)

定义环 $(R, +, \cdot)$ 的中心为 $\text{Cent}(R) = \{x \in R : x \cdot r = r \cdot x, \forall r \in R\}$ 。

**命题 4.2.7**

环的中心为子环。



证明 任取 $x, y \in \text{Cent}(R)$, 那么对于任意 $r \in R$, 成立 $x \cdot r = r \cdot x$, 且 $y \cdot r = r \cdot y$, 因此

$$(x - y) \cdot r = x \cdot r - y \cdot r = r \cdot x - r \cdot y = r \cdot (x - y)$$

$$(x \cdot y) \cdot r = x \cdot (y \cdot r) = x \cdot (r \cdot y) = (x \cdot r) \cdot y = (r \cdot x) \cdot y = r \cdot (x \cdot y)$$

于是 $x - y, x \cdot y \in \text{Cent}(R)$, 进而 $\text{Cent}(R)$ 对于 \cdot 运算封闭, 且 $(\text{Cent}(R), +)$ 为群。而 $1 \in \text{Cent}(R)$, 因此 $\text{Cent}(R)$ 为 R 的子环。

命题 4.2.8

除环的中心为域。

**定义 4.2.7 (中心化子 centralizer)**

定义环 $(R, +, \cdot)$ 的元素 $r \in R$ 的中心化子为 $\text{Cent}_R(r) = \{x \in R : x \cdot r = r \cdot x\}$ 。

**命题 4.2.9**

环的中心化子为子环。



证明 任取 $x, y \in \text{Cent}_R(r)$, 那么成立 $x \cdot r = r \cdot x$, 且 $y \cdot r = r \cdot y$, 因此

$$(x - y) \cdot r = x \cdot r - y \cdot r = r \cdot x - r \cdot y = r \cdot (x - y)$$

$$(x \cdot y) \cdot r = x \cdot (y \cdot r) = x \cdot (r \cdot y) = (x \cdot r) \cdot y = (r \cdot x) \cdot y = r \cdot (x \cdot y)$$

于是 $x - y, x \cdot y \in \text{Cent}_R(r)$, 进而 $\text{Cent}_R(r)$ 对于 \cdot 运算封闭, 且 $(\text{Cent}_R(r), +)$ 为群。而 $1 \in \text{Cent}_R(r)$, 因此 $\text{Cent}_R(r)$ 为 R 的子环。

命题 4.2.10

环的中心为环的中心化子的交, 即

$$\text{Cent}(R) = \bigcap_{r \in R} \text{Cent}_R(r)$$

证明 一方面, 任取 $x \in \text{Cent}(R)$, 那么对于任意 $r \in R$, 成立 $x \cdot r = r \cdot x$, 因此 $x \in \text{Cent}_R(r)$, 那么 $x \in \bigcap_{r \in R} \text{Cent}_R(r)$, 进而 $\text{Cent}(R) \subset \bigcap_{r \in R} \text{Cent}_R(r)$.

另一方面, 任取 $x \in \bigcap_{r \in R} \text{Cent}_R(r)$, 那么对于任意 $r \in R$, 成立 $x \in \text{Cent}_R(r)$, 因此成立 $x \cdot r = r \cdot x$, 那么 $x \in \text{Cent}(R)$, 进而 $\text{Cent}(R) \supset \bigcap_{r \in R} \text{Cent}_R(r)$.

命题 4.2.11

除环的中心化子为除环。

证明 只需证明, 除环 R 的中心化子 $\text{Cent}_R(r)$ 中的非零元存在乘法逆元。不妨 $r \neq 0$, 任取非零元 $x \in \text{Cent}_R(r)$, 那么成立 $x \cdot r = r \cdot x$ 。 $x \in R$ 存在逆元 x^{-1} , 使得成立 $x \cdot x^{-1} = x^{-1} \cdot x = 1$, 由于

$$r \cdot x^{-1} = r \cdot x^{-1} \cdot r^{-1} \cdot r = r \cdot (r \cdot x)^{-1} \cdot r = r \cdot (x \cdot r)^{-1} \cdot r = r \cdot r^{-1} \cdot x^{-1} \cdot r = x^{-1} \cdot r$$

因此 $x^{-1} \in \text{Cent}_R(r)$, 进而中心化子 $\text{Cent}_R(r)$ 中的非零元存在乘法逆元。

4.2.3 特征**定义 4.2.8 (特征 characteristic)**

环的特征的等价定义如下。

1. 由于 Ring 范畴的初始对象为整数环 \mathbb{Z} , 那么对于环 $R \in \text{Obj}(\text{Ring})$, 存在且存在唯一环同态映射

$$\begin{aligned} \varphi: \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n1_R \end{aligned}$$

定义环 $(R, +, \cdot)$ 的特征为 $\text{char } R \in \mathbb{N}^*$, 其中 $\ker \varphi = (\text{char } R)\mathbb{Z}$ 。

2. 定义环 $(R, +, \cdot)$ 的特征为乘法单位元 1_R 在加法群 $(R, +)$ 的阶, 并记作 $\text{char } R$; 特别的, 如果乘法单位元 1_R 在加法群 $(R, +)$ 阶为 ∞ , 那么 $\text{char } R = 0$ 。
3. 定义环 $(R, +, \cdot)$ 的特征为

$$\text{char } R = \begin{cases} \min\{n \in \mathbb{N}^* : nr = 0, \forall r \in R\}, & \exists n \in \mathbb{N}^*, \forall r \in R, nr = 0 \\ 0, & \forall n \in \mathbb{N}^*, \exists r \in R, nr \neq 0 \end{cases}$$

命题 4.2.12 (常见环的特征)

$$\text{char } \mathbb{Z} = \text{char } \mathbb{Q} = 0, \quad \text{char } \mathbb{Z}/n\mathbb{Z} = n, \quad \text{char } R = 1 \iff R = \{0\}$$

命题 4.2.13 (无零因子环的非零元在加法群中的阶)

无零因子环的非零元在加法群中的阶相同。

证明 对于无零因子环 $(R, +, \cdot)$, 任取 $r, s \in R \setminus \{0_R\}$ 。如果 r 在加法群 $(R, +)$ 中为有限阶 n , 且 s 在加法群 $(R, +)$ 中的阶为 ∞ , 那么 $nr = 0_R$, 且对于任意 $m \in \mathbb{N}^*$, 成立 $ms \neq 0_R$, 因此

$$(nr) \cdot s = 0_R \iff r \cdot (ns) = 0_R \iff ns = 0_R$$

矛盾！因此 R 中非零元在加法群 $(R, +)$ 中的阶均为无限阶或均为有限阶。

如果 r, s 在加法群 $(R, +)$ 中均为有限阶，那么记 r, s 在加法群 $(R, +)$ 的阶为 m, n ，那么

$$mr = 0_R \implies (mr) \cdot s = 0_R \iff r \cdot (ms) = 0_R \iff ms = 0_R$$

由命题 2.1.5, $n \mid m$ 。同理可得, $m \mid n$ ，因此 $m = n$ 。

综上所述，无零因子环的非零元在加法群中的阶相同。

命题 4.2.14 (无零因子环的特征)

无零因子环的特征为 0 或素数。

证明 由于 Ring 范畴的初始对象为整数环 \mathbb{Z} ，那么对于无零因子环 $R \in \text{Obj}(\text{Ring})$ ，存在且存在唯一环同态映射

$$\varphi: \mathbb{Z} \longrightarrow R$$

$$n \longmapsto n1_R$$

由环第一同构定理 4.3.4，以及命题 4.2.6, $\mathbb{Z}/(\text{char } R)\mathbb{Z} \cong \text{im } \varphi$ 为 R 的子环。由命题 4.1.3, $\mathbb{Z}/(\text{char } R)\mathbb{Z}$ 为无零因子环，进而为整环。由命题 4.1.12, $\text{char } R$ 为 0 或素数。

命题 4.2.15

如果环 $(R, +, \cdot)$ 的子环为理想，那么 $R \cong \mathbb{Z}/n\mathbb{Z}$ ，其中 n 为 R 的特征。

证明 由于 Ring 范畴的初始对象为整数环 \mathbb{Z} ，那么对于环 $R \in \text{Obj}(\text{Ring})$ ，存在且存在唯一环同态映射

$$\varphi: \mathbb{Z} \longrightarrow R$$

$$m \longmapsto m1_R$$

由命题 4.2.6, $\text{im } \varphi$ 为 R 的子环。注意到 $1 \in \text{im } \varphi$ ，而 $\text{im } \varphi$ 为理想，因此由命题 4.3.1, $\text{im } \varphi = R$ 。由此可知对于任意 $r \in R$ ，存在 $m_r \in \mathbb{Z}$ ，使得成立 $r = m_r 1_R$ ，因此 $R = \langle 1_R \rangle$ 。

如果 $R = \mathbb{Z}$ ，那么 $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ ， $m \mapsto m$ ，此时 $\ker \varphi = \{0\}$ ，那么 R 的特征为 0，因此 $R = \mathbb{Z} \cong \mathbb{Z}/0\mathbb{Z}$ 。

如果 $R = \mathbb{Z}/n\mathbb{Z}$ ，那么 $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ ， $m \mapsto [m]_n$ ，此时 $\ker \varphi = n\mathbb{Z}$ ，那么 R 的特征为 n ，因此 $R = \mathbb{Z}/n\mathbb{Z}$ 。

4.2.4 多项式环的万有性质

定义 4.2.9 (由集合诱导的环范畴)

对于 n 阶集合 S ，定义由 S 诱导的范畴 \mathcal{R}^S 如下。

1. 对象: $\text{Obj}(\mathcal{R}^S) = (j, G)$ ，其中 R 为交换环，且 $j: S \rightarrow G$ 为集合函数。
2. 态射: $\text{Hom}_{\mathcal{R}^S}((j_1, R_1), (j_2, R_2)) = \{\varphi \in \text{Hom}_{\text{Ring}}(R_1, R_2) : \varphi \circ j_1 = j_2\}$ ，其交换图为

$$\begin{array}{ccc} R_1 & \xrightarrow{\varphi} & R_2 \\ j_1 \uparrow & \nearrow j_2 & \\ S & & \end{array}$$

命题 4.2.16 (由集合诱导的环范畴的初始对象)

对于集合 $S = \{s_1, \dots, s_n\}$ ，由 S 诱导的环范畴 \mathcal{R}^S 的初始对象为 $(i, \mathbb{Z}[x_1, \dots, x_n])$ ，其中 $i: S \rightarrow \mathbb{Z}[x_1, \dots, x_n]$ ， $s_k \mapsto x_k$ 。

4.2.5 单态射与满态射

命题 4.2.17

对于环同态映射 $\varphi: R \rightarrow S$, 如下命题等价。

1. $\varphi: R \rightarrow S$ 为单态射。
2. $\ker \varphi = \{0_R\}$
3. $\varphi: R \rightarrow S$ 为单函数映射。



命题 4.2.18

如果环同态映射 $\varphi: R \rightarrow S$ 为满函数映射, 那么 $\varphi: R \rightarrow S$ 为满态射; 反之不然, 例如包含映射 $i: \mathbb{Z} \hookrightarrow \mathbb{Q}$ 。



4.2.6 积

定义 4.2.10 (积 product)

定义环 $(R, +, \cdot)$ 和 $(S, +, \cdot)$ 的积为环 $(R \times S, +, \cdot)$, 其中

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

4.2.7 $\text{End}_{\text{Ab}}(G)$

定义 4.2.11 (Ab 的自同构映射环)

Abel 群 G 的自同构映射 $\text{End}_{\text{Ab}}(G)$ 依加法和复合运算构成环。

定义 4.2.12 ($\text{End}_{\text{Ab}}(G)$ 的单位群)

$\text{End}_{\text{Ab}}(G)$ 的单位群为 $\text{Aut}_{\text{Ab}}(G)$ 。



命题 4.2.19

在环的意义上, $\text{End}_{\text{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$, 环同构映射为 $\text{End}_{\text{Ab}}(\mathbb{Z}) \rightarrow \mathbb{Z}$, $\varphi \mapsto \varphi(1)$ 。



命题 4.2.20

对于环 $(R, +, \cdot)$, 如果将 R 看作 Abel 群 $(R, +)$, 那么环同态映射 $\lambda: R \rightarrow \text{End}_{\text{Ab}}(R)$, $r \mapsto \lambda_r$ 为单态射, 其中环同态映射 $\lambda_r: R \rightarrow R$, $r \mapsto r \cdot r$ 。



命题 4.2.21

Abel 群 $(\mathbb{Z}, +)$ 上的环至多同构。



命题 4.2.22

对于环 $(R, +, \cdot)$, 记 $\text{End}_{\text{Ab}}(R)$ 为 Abel 群 $(R, +)$ 的自同态环, 那么 $\text{Cent}(\text{End}_{\text{Ab}}(R)) \cong \text{Cent}(R)$ 。



命题 4.2.23

$$\text{End}_{\text{Ab}}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$$



4.3 理想与商环

4.3.1 理想

定义 4.3.1 (左理想 left-ideal)

对于环 $(R, +, \cdot)$, 称群 $(R, +)$ 的子群 $I \subset R$ 为 R 的左理想, 如果对于任意 $r \in R$, 成立 $r \cdot I \subset I$ 。



定义 4.3.2 (右理想 right-ideal)

对于环 $(R, +, \cdot)$, 称群 $(R, +)$ 的子群 $I \subset R$ 为 R 的右理想, 如果对于任意 $r \in R$, 成立 $I \cdot r \subset I$ 。



定义 4.3.3 (理想 ideal)

对于环 $(R, +, \cdot)$, 称群 $(R, +)$ 的子群 $I \subset R$ 为 R 的理想, 如果对于任意 $r \in R$, 成立 $r \cdot I \subset I$ 且 $I \cdot r \subset I$ 。



定义 4.3.4 (理想的同余)

对于环 $(R, +, \cdot)$ 的理想 I , 称 $r, s \in R$ 关于 I 同余, 并记作

$$r \equiv s \pmod{I}$$

如果 $r - s \in I$ 。



命题 4.3.1 (含 1 理想)

对于环 $(R, +, \cdot)$ 的理想 I , 成立

$$1 \in I \iff I = R$$



证明 这几乎是显然的, 因为对于任意 $r \in R$, 成立

$$r = r \cdot 1 \in I$$

命题 4.3.2 (核为理想)

对于环同态映射 $\varphi: R \rightarrow S$, $\ker \varphi$ 为 R 的理想。



命题 4.3.3 ($R \cdot r$ 为理想)

对于环 $(R, +, \cdot)$, 以及 $r \in R$, $R \cdot r$ 为 R 的左理想, $r \cdot R$ 为 R 的右理想。



证明 一方面, 对于任意 $s, t \in R$, 注意到 $s \cdot (t \cdot r) = (s \cdot t) \cdot r \in R \cdot r$, 因此 $R \cdot r$ 为 R 的左理想。

另一方面, 对于任意 $s, t \in R$, 注意到 $(r \cdot t) \cdot s = r \cdot (t \cdot s) \in r \cdot R$, 因此 $r \cdot R$ 为 R 的右理想。

例题 4.6 构造环同态映射 $\varphi: R \rightarrow S$, 使得 $\text{im } \varphi$ 不为 S 的理想。

证明 构造环同态映射

$$\varphi: (\mathbb{Z}, +, \cdot) \longrightarrow (\mathbb{Q}, +, \cdot)$$

$$n \longmapsto n$$

$\text{im } \varphi = \mathbb{Z}$ 不为 \mathbb{Q} 的理想。

命题 4.3.4 (理想的像为理想)

对于环同态映射 $\varphi: R \rightarrow S$, 如果 I 为 R 的理想, 那么 $\varphi(I)$ 为 $\text{im } \varphi$ 的理想。



证明 首先证明 $\varphi(I)$ 为 $\text{im } \varphi$ 的子群, 注意到

$$r, s \in I \implies r - s \in I \implies \varphi(r - s) \in \varphi(I) \iff \varphi(r) - \varphi(s) \in \varphi(I)$$

其次证明 $\varphi(I)$ 满足吸收律, 注意到

$$\begin{aligned} r \in R, i \in I &\implies r \cdot i \in I, i \cdot r \in I \\ \implies \varphi(r \cdot i) \in \varphi(I), \varphi(i \cdot r) \in \varphi(I) &\iff \varphi(r) \cdot \varphi(i) \in \varphi(I), \varphi(i) \cdot \varphi(r) \in \varphi(I) \end{aligned}$$

命题 4.3.5 (理想的原像为理想)

对于环同态映射 $\varphi: R \rightarrow S$, 如果 J 是 $\text{im } \varphi$ 的理想, 那么 $\varphi^{-1}(J)$ 为 R 的理想, 且 $\ker \varphi \subset \varphi^{-1}(J)$.

证明 首先证明 $\varphi^{-1}(J)$ 为 R 的子群, 注意到

$$r, s \in \varphi^{-1}(J) \iff \varphi(r), \varphi(s) \in J \implies \varphi(r) - \varphi(s) \in J \iff \varphi(r - s) \in J \iff r - s \in \varphi^{-1}(J)$$

其次证明 I 满足吸收律, 注意到

$$\begin{aligned} r \in R, i \in \varphi^{-1}(J) &\implies \varphi(r) \in \text{im } \varphi, \varphi(i) \in J \\ \implies \varphi(r) \cdot \varphi(i) \in J, \varphi(i) \cdot \varphi(r) \in J &\iff \varphi(r \cdot i) \in J, \varphi(i \cdot r) \in J \\ \iff r \cdot i \in \varphi^{-1}(J), i \cdot r \in \varphi^{-1}(J) \end{aligned}$$

因此 $\varphi^{-1}(J)$ 为 R 的理想。而 $0_S \in J$, 因此 $\ker \varphi = \varphi^{-1}(0_S) \subset \varphi^{-1}(J)$ 。

命题 4.3.6 (由环同态映射诱导的双射)

对于环同态映射 $\varphi: R \rightarrow S$, 如下集合函数为双射。

$$\begin{aligned} \Psi: \{I \supset \ker \varphi \text{ 为 } R \text{ 的理想}\} &\longrightarrow \{J \text{ 为 } \text{im } \varphi \text{ 的理想}\} \\ I &\longmapsto \varphi(I) \end{aligned}$$

证明 由命题 4.3.4, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性

$$\Psi(I) = \Psi(J) \iff \varphi(I) = \varphi(J) \implies \varphi^{-1}(\varphi(I)) = \varphi^{-1}(\varphi(J)) \iff I + \ker \varphi = J + \ker \varphi \iff I = J$$

其次对于 Ψ 的满射性。如果 J 为 $\text{im } \varphi$ 的理想, 那么由命题 4.3.5, $\varphi^{-1}(J) \supset \ker \varphi$ 为 R 的理想。注意到, $\Psi(\varphi^{-1}(J)) = \varphi(\varphi^{-1}(J)) = J \cap \text{im } \varphi = J$, 因此 Ψ 为满射。

命题 4.3.7 (由环同态逆映射诱导的双射)

对于环同态映射 $\varphi: R \rightarrow S$, 如下集合函数为双射。

$$\begin{aligned} \Psi: \{J \text{ 为 } \text{im } \varphi \text{ 的理想}\} &\longrightarrow \{I \supset \ker \varphi \text{ 为 } R \text{ 的理想}\} \\ J &\longmapsto \varphi^{-1}(J) \end{aligned}$$

证明 由命题 4.3.5, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性

$$\Psi(I) = \Psi(J) \iff \varphi^{-1}(I) = \varphi^{-1}(J) \implies \varphi(\varphi^{-1}(I)) = \varphi(\varphi^{-1}(J)) \iff I \cap \text{im } \varphi = J \cap \text{im } \varphi \iff I = J$$

其次对于 Ψ 的满射性。如果 $I \supset \ker \varphi$ 为 R 的理想, 那么由命题 4.3.4, $\varphi(I)$ 为 $\text{im } \varphi$ 的理想。注意到, $\Psi(\varphi(I)) = \varphi^{-1}(\varphi(I)) = I + \ker \varphi = I$, 因此 Ψ 为满射。

命题 4.3.8

对于环 $(R, +, \cdot)$, 如果 I 为 R 的理想, 那么

$$\{I + J : J \text{ 为理想}\} = \{J \supset I \text{ 为理想}\}$$



证明 如果 J 为 R 的理想, 那么 $I + J$ 为 R 的理想, 且 $I \subset I + J$, 因此

$$\{I + J : J \text{ 为理想}\} \subset \{J \supset I \text{ 为理想}\}$$

如果 $J \supset I$ 为 R 的理想, 那么 $J = I + J$, 因此

$$\{I + J : J \text{ 为理想}\} \supset \{J \supset I \text{ 为理想}\}$$

综上所述

$$\{I + J : J \text{ 为理想}\} = \{J \supset I \text{ 为理想}\}$$

4.3.2 基本运算**定义 4.3.5 (交 intersection)**

环 $(R, +, \cdot)$ 的理想族 $\{I_\lambda\}_{\lambda \in \Lambda}$ 的交 $\bigcap_{\lambda \in \Lambda} I_\lambda$ 为 R 的理想。

**定义 4.3.6 (和 summation)**

环 $(R, +, \cdot)$ 的理想族 $\{I_\lambda\}_{\lambda \in \Lambda}$ 的和 $\sum_{\lambda \in \Lambda} I_\lambda$ 为 R 的理想, 其中

$$\sum_{\lambda \in \Lambda} I_\lambda = \left\{ \sum_{\substack{r_\lambda \in I_\lambda \\ \lambda \in \Lambda}} r_\lambda : \text{仅存在有限 } r_\lambda \neq 0 \right\}$$

特别的

$$I + J = \{r + s : r \in I, s \in J\}$$

**定义 4.3.7 (积 product)**

环 $(R, +, \cdot)$ 的理想族 $\{I_\lambda\}_{\lambda \in \Lambda}$ 的积 $\prod_{\lambda \in \Lambda} I_\lambda$ 为 R 的理想, 其中

$$\prod_{\lambda \in \Lambda} I_\lambda = \left\{ \sum_{r_\lambda \in I_\lambda} \prod_{\lambda \in \Lambda} r_\lambda : \text{仅存在有限 } \prod_{\lambda \in \Lambda} r_\lambda \neq 0 \right\}$$

特别的

$$I \cdot J = \left\{ \sum_{k=1}^n r_k \cdot s_k : r_k \in I, s_k \in J, n \in \mathbb{N}^* \right\}$$

**命题 4.3.9 (主理想的运算)**

对于交换环 $(R, +, \cdot)$, 如果 $r, s \in R$, 那么

$$(r) \cdot (s) = (r \cdot s)$$

$$(r) \cap (s) = (\text{lcm}(r, s))$$

$$(r) + (s) = (\text{gcd}(r, s))$$



命题 4.3.10 (理想运算的包含关系)

对于环 $(R, +, \cdot)$ 的理想 I, J , 成立

$$I \cdot J \subset I \cap J \subset I + J$$

命题 4.3.11 (理想运算的性质)

- 加法交换律:

$$I + J = J + I$$

- 加法结合律:

$$(I + J) + K = I + (J + K)$$

- 乘法结合律:

$$(I \cdot J) \cdot K = I \cdot (J \cdot K)$$

- 分配律:

$$I \cdot (J + K) = I \cdot J + I \cdot K$$

$$(I + J) \cdot K = I \cdot K + J \cdot K$$

定义 4.3.8 (互素 coprime)

称环 $(R, +, \cdot)$ 的理想 I 与 J 互素, 如果 $I + J = R$ 。

命题 4.3.12

对于环 $(R, +, \cdot)$ 的理想 I, J, K , 如果 I 与 K 互素且 J 与 K 互素, 那么 $I \cdot J$ 与 K 互素。

证明 由于 I 与 K 互素且 J 与 K 互素, 那么 $I + K = J + K = R$, 于是存在 $i \in I, j \in J$ 以及 $k_i, k_j \in K$, 使得成立

$$i + k_i = j + k_j = 1$$

因此

$$i \cdot j + i \cdot k_j + k_i \cdot j + k_i \cdot k_j = (i + k_i) \cdot (j + k_j) = 1$$

由于 K 为 R 的理想, 因此 $i \cdot k_j + j \cdot k_i + k_i \cdot k_j \in K$, 而 $i \cdot j \in I \cdot J$, 那么 $1 \in I \cdot J + K$, 进而由 4.3.1, $I \cdot J + K = R$, 即 $I \cdot J$ 与 K 互素。

命题 4.3.13

对于交换环 $(R, +, \cdot)$ 的理想 I 与 J , 如果 I 与 J 互素, 那么 $I \cdot J = I \cap J$ 。

证明 一方面, 由命题 4.3.10, 成立 $I \cdot J \subset I \cap J$ 。

另一方面, 任取 $r \in I \cap J$, 由于 I 与 J 互素, 那么 $I + J = R$, 因此存在 $i \in I, j \in J$, 使得成立 $i + j = 1$, 进而 $r = i \cdot r + j \cdot r \in I \cdot J$, 于是 $I \cap J \subset I \cdot J$ 。

4.3.3 商环

定义 4.3.9 (模 I 商环 quotient ring modulo I)

对于环 $(R, +, \cdot)$ 的理想 I , 称环 $(R/I, +, \cdot)$ 为 $(R, +, \cdot)$ 的模 I 商环, 其中 $R/I = \{r + I : r \in R\}$, $(r + I) + (s + I) = (r + s) + I$, $(r + I) \cdot (s + I) = (r \cdot s) + I$.



命题 4.3.14 (商环理想的结构)

如果 I 为环 $(R, +, \cdot)$ 的理想, 那么如下集合函数为双射。

$$\begin{aligned}\Phi : \{J \supset I \text{ 为 } R \text{ 的理想}\} &\longrightarrow \{K \text{ 为 } R/I \text{ 的理想}\} \\ J &\longmapsto J/I\end{aligned}$$



证明 注意到如下自然环同态

$$\begin{aligned}\pi : R &\longrightarrow R/I \\ r &\longmapsto r + I\end{aligned}$$

其中 $\ker \pi = I$, 且 $\text{im } \pi = R/I$ 。由命题 4.3.6, 如下集合函数为双射。

$$\begin{aligned}\Psi : \{J \supset I \text{ 为 } R \text{ 的理想}\} &\longrightarrow \{K \text{ 为 } R/I \text{ 的理想}\} \\ J &\longmapsto \pi(J)\end{aligned}$$

注意到

$$\Phi(J) = J/I = \{j + I : j \in J\} = \pi(J) = \Psi(J)$$

因此 $\Phi = \Psi$, 进而 Φ 为双射。

4.3.4 核 \iff 理想

定理 4.3.1

I 是环 $(R, +, \cdot)$ 的理想 \iff 存在环同态映射 $\varphi : R \rightarrow S$, 使得成立 $I = \ker \varphi$ 。



定理 4.3.2 (理想是群同态的核; 群同态的核是理想)

对于环 $(R, +, \cdot)$ 的理想 I , 成立 $\ker \pi = I$, 其中 $\pi : R \twoheadrightarrow R/I$ 为满的环同态映射; 对于环同态映射 $\varphi : R \rightarrow S$, $\ker \varphi$ 为 R 的理想。因此:

$$\text{核} \iff \text{理想}$$



定理 4.3.3

如果 I 为环 $(R, +, \cdot)$ 的理想, 那么对于任意满足 $I \subset \ker \varphi$ 的环同态映射 $\varphi : R \rightarrow S$, 存在且存在唯一环同态映射 $\bar{\varphi} : R/I \rightarrow S$, 使得成立 $\varphi = \bar{\varphi} \circ \pi$, 其中 $\pi : R \twoheadrightarrow R/I$, $r \mapsto r + I$, 交换图为

$$\begin{array}{ccc} R/I & \xrightarrow{\exists! \bar{\varphi}} & S \\ \pi \swarrow & & \nearrow \varphi \\ & I & \end{array}$$



4.3.5 正则分解

定义 4.3.10 (环同态映射的正则分解 canonical decomposition)

环同态映射 $\varphi: R \rightarrow S$ 的正则分解如下。

$$R \xrightarrow{r \mapsto r + \ker \varphi} R / \ker \varphi \xrightarrow[\varphi: r + \ker \varphi \mapsto \varphi(g)]{\sim} \text{im } \varphi \xrightarrow[\varphi(g) \mapsto \varphi(g)]{\subset} S$$

φ

定理 4.3.4 (第一同构定理 first isomorphism theorem)

对于环同态映射 $\varphi: R \rightarrow S$, 成立

$$R / \ker \varphi \cong \text{im } \varphi$$

定理 4.3.5 (第二同构定理 second isomorphism theorem)

如果 S 为环 $(R, +, \cdot)$ 的子环, 且 I 为 R 的理想, 那么 $I + S$ 为 R 的理想, 且 $I \cap S$ 为 S 的理想, 同时

$$\frac{S}{I \cap S} \cong \frac{I + S}{I}$$

定理 4.3.6 (第三同构定理 (third isomorphism theorem))

如果 $I \subset S$ 均为环 $(R, +, \cdot)$ 的理想, 那么 S/I 为 R/I 的理想, 并且

$$\frac{R/I}{S/I} \cong \frac{R}{S}$$

命题 4.3.15 (第一同构定理的推论)

对于环同态映射 $\varphi: R \rightarrow S$, 如果 I 为 R 的理想, 那么

$$\frac{R}{\ker \varphi + I} \cong \frac{\text{im } \varphi}{\varphi(I)}$$

证明

证明: (优雅证明) 注意到 $\varphi(\ker \varphi + I) = \varphi(I)$, 由命题 4.3.16

$$\frac{R}{\ker \varphi + I} \cong \frac{\text{im } \varphi}{\varphi(\ker \varphi + I)} = \frac{\text{im } \varphi}{\varphi(I)}$$

(朴素证明) 定义映射

$$f: R \longrightarrow \frac{\text{im } \varphi}{\varphi(I)}$$

$$r \longmapsto \varphi(r) + \varphi(I)$$

首先证明 f 为环同态映射, 注意到

$$f(r + s) = \varphi(r + s) + \varphi(I) = (\varphi(r) + \varphi(I)) + (\varphi(s) + \varphi(I)) = f(r) + f(s)$$

$$f(r \cdot s) = \varphi(r \cdot s) + \varphi(I) = (\varphi(r) + \varphi(I)) \cdot (\varphi(s) + \varphi(I)) = f(r) \cdot f(s)$$

$$f(1) = \varphi(1) + \varphi(I) = 1 + \varphi(I)$$

其次证明 $\ker f = \ker \varphi + I$, 注意到

$$r \in \ker f \iff f(r) = \varphi(I) \iff \varphi(r) + \varphi(I) = \varphi(I)$$

$$\iff \varphi(r) \in \varphi(I) \iff \exists i \in I, \varphi(r) = \varphi(i) \iff \exists i \in I, r - i \in \ker \varphi$$

$$\iff \exists i \in I, r \in \ker \varphi + i \iff r \in \ker \varphi + I$$

最后证明 $\text{im } f = \text{im } \varphi / \varphi(I)$, 这是显然的。

综上所述, 由环第一同构定理4.3.4

$$\frac{R}{\ker \varphi + I} \cong \frac{\text{im } \varphi}{\varphi(I)}$$

命题 4.3.16 (第一同构定理的推论)

对于环同态映射 $\varphi: R \rightarrow S$, 如果 $I \supset \ker \varphi$ 为 R 的理想, 那么

$$\frac{R}{I} \cong \frac{\text{im } \varphi}{\varphi(I)}$$



证明 (优雅证明) 由于 $I \supset \ker \varphi$ 为 R 的理想, 那么由命题4.3.8, 存在 R 的理想 J , 使得成立 $I = \ker \varphi + J$ 。此时, $\varphi(I) = \varphi(\ker \varphi + J) = \varphi(J)$ 。由命题4.3.15

$$\frac{R}{I} = \frac{R}{\ker \varphi + J} \cong \frac{\text{im } \varphi}{\varphi(J)} = \frac{\text{im } \varphi}{\varphi(I)}$$

(朴素证明) 定义映射

$$\begin{aligned} f: R &\longrightarrow \frac{\text{im } \varphi}{\varphi(I)} \\ r &\longmapsto \varphi(r) + \varphi(I) \end{aligned}$$

首先证明 f 为环同态映射, 注意到

$$\begin{aligned} f(r+s) &= \varphi(r+s) + \varphi(I) = (\varphi(r) + \varphi(I)) + (\varphi(s) + \varphi(I)) = f(r) + f(s) \\ f(r \cdot s) &= \varphi(r \cdot s) + \varphi(I) = (\varphi(r) + \varphi(I)) \cdot (\varphi(s) + \varphi(I)) = f(r) \cdot f(s) \\ f(1) &= \varphi(1) + \varphi(I) = 1 + \varphi(I) \end{aligned}$$

其次证明 $\ker f = I$, 注意到

$$\begin{aligned} r \in \ker f &\iff f(r) = \varphi(I) \iff \varphi(r) + \varphi(I) = \varphi(I) \\ &\iff \varphi(r) \in \varphi(I) \iff \exists i \in I, \varphi(r) = \varphi(i) \iff \exists i \in I, r - i \in \ker \varphi \\ &\iff \exists i \in I, r \in \ker \varphi + i \iff r \in \ker \varphi + I = I \end{aligned}$$

最后证明 $\text{im } f = \text{im } \varphi / \varphi(I)$, 这是显然的。

综上所述, 由环第一同构定理4.3.4

$$\frac{R}{I} \cong \frac{\text{im } \varphi}{\varphi(I)}$$

4.4 素理想与极大理想

4.4.1 生成理想

定义 4.4.1 (生成理想 generated ideal)

对于环 $(R, +, \cdot)$, 定义由子集 $S \subset R$ 生成的理想为

$$(S) = \bigcap_{\text{理想 } I \supset S} I$$



定义 4.4.2 (主理想 principal ideal)

对于交换环 $(R, +, \cdot)$, 定义由 $r \in R$ 生成的主理想为 $(r) = r \cdot R$ 。



定义 4.4.3 (生成理想 generated ideal)

对于交换环 $(R, +, \cdot)$, 定义由子集 $S \subset R$ 生成的理想为 $(S) = \sum_{r \in S} (r)$ 。

**定义 4.4.4 (有限生成理想 finitely generated ideal)**

称交换环 $(R, +, \cdot)$ 的理想 I 为有限生成的, 如果存在 $\{r_k\}_{k=1}^n \subset R$, 使得成立 $I = (r_k)_{k=1}^n$ 。

**定义 4.4.5 (主理想环 principal ideal ring)**

称交换环 $(R, +, \cdot)$ 为主理想环, 如果其任意理想为主理想。

**定义 4.4.6 (主理想整环 principal ideal domain, PID)**

称整环 $(R, +, \cdot)$ 为主理想整环, 如果其任意理想为主理想。

**定义 4.4.7 (Noether 环 Noetherian ring)**

称交换环 $(R, +, \cdot)$ 为 Noether 环, 如果其任意理想为有限生成理想。

**命题 4.4.1 (整数环为 PID)**

整数环 \mathbb{Z} 为主理想整环。



证明 容易知道 \mathbb{Z} 为整环。取 \mathbb{Z} 的理想 I , 如果 $I = \{0\}$ 为平凡理想, 那么 $I = (0)$ 。如果 $I \neq \{0\}$, 那么取 I 中绝对值最小正整数 n 。对于任意 $m \in I$, 作带余除法, 成立 $m = kn + r$, 其中 $0 \leq r < n$ 。注意到 $r = m - kn \in I$, 因此 $r = 0$, 进而 $m = kn$ 。由 m 的任意性, $I = (n)$, 进而整数环 \mathbb{Z} 为主理想整环。

命题 4.4.2 (域的多项式环为 PID)

对于域 F , 多项式环 $F[x]$ 为主理想整环。



证明 由命题 4.1.26, $F[x]$ 为整环。取 $F[x]$ 的理想 I , 如果 $I = \{0\}$ 为平凡理想, 那么 $I = (0)$ 。如果 $I \neq \{0\}$, 那么取 I 中次数最小的非零首一多项式 $p(x)$ 。对于任意 $f(x) \in I$, 由 4.4.1, 作带余除法, 成立 $f(x) = p(x)q(x) + r(x)$, 其中 $\deg(r(x)) < \deg(p(x))$ 。注意到 $r(x) = f(x) - p(x)q(x) \in I$, 因此 $r(x) = 0$, 进而 $f(x) = p(x)q(x)$ 。由 $f(x)$ 的任意性, $I = (p(x))$, 进而多项式环 $F[x]$ 为主理想整环。

4.4.2 多项式环的商

定理 4.4.1 (多项式环的带余除法)

对于环 $(R, +, \cdot)$, 如果 $f(x), g(x) \in R[x]$, 且 $f(x)$ 为首一多项式, 那么存在且存在唯一 $q(x), r(x) \in R[x]$, 使得成立 $g(x) = q(x)f(x) + r(x)$, 且 $\deg(r(x)) < \deg(f(x))$ 。

**命题 4.4.3**

对于交换环 $(R, +, \cdot)$, 如果 $f(x)$ 为多项式环 $R[x]$ 中的首一多项式, 那么对于任意 $g(x) \in R[x]$, 存在且存在唯一 $r(x) \in R[x]$, 使得成立 $\deg(r(x)) < \deg(f(x))$, 且 $g(x) + (f(x)) = r(x) + (f(x))$ 。



命题 4.4.4

对于交换环 $(R, +, \cdot)$, 以及 n 次首一多项式 $f(x) \in R[x]$, 成立 $R[x]/(f(x)) \cong R^{\oplus n}$, 环同态映射为

$$\varphi: R[x] \longrightarrow R^{\oplus n}$$

$$g(x) \longmapsto (r_0, \cdots, r_{n-1}), \text{ 其中 } g(x) = q(x)f(x) + (r_0 + \cdots + r_{n-1}x^{n-1})$$

**4.4.3 素理想与极大理想****定义 4.4.8 (素理想 prime ideal)**

称非零交换环 $(R, +, \cdot)$ 的理想 I 为素理想, 如果成立如下命题之一。

1. R/I 为整环。
2. $I \subsetneq R$, 且对于任意 $r, s \in R$, 成立 $r \cdot s \in I \implies r \in I$ 或 $s \in I$ 。



证明

R/I 为整环

$$\iff 1 + I \neq I \text{ 且 } \forall r, s \in R, (r + I) \cdot (s + I) = I \implies r + I = I \text{ 或 } s + I = I$$

$$\iff 1 \notin I \text{ 且 } \forall r, s \in R, (r \cdot s) + I = I \implies r + I = I \text{ 或 } s + I = I$$

$$\iff I \subsetneq R \text{ 且 } \forall r, s \in R, r \cdot s \in I \implies r \in I \text{ 或 } s \in I$$

定义 4.4.9 (极大理想 maximal ideal)

称非零交换环 $(R, +, \cdot)$ 的理想 I 为极大理想, 如果成立如下命题之一。

1. R/I 为域。
2. $I \subsetneq R$, 且对于任意 R 的理想 $J \subset R$, 成立 $I \subset J \implies I = J$ 或 $J = R$ 。



证明 由命题 4.1.11, 以及命题 4.3.14

R/I 为域

$$\iff 1 + I \neq I \text{ 且 } R/I \text{ 仅存在平凡理想}$$

$$\iff 1 \notin I \text{ 且 } R/I \text{ 仅存在理想 } I/IR/I$$

$$\iff I \subsetneq R \text{ 且对于任意 } R \text{ 的理想 } J \subset R \text{ 成立 } I \subset J \implies I = J \text{ 或 } J = R$$

定义 4.4.10 (谱 spectrum)

称非零交换环 $(R, +, \cdot)$ 的素理想族为 R 的谱, 记作 $\text{Spec } R$ 。

**命题 4.4.5**

非零交换环的极大理想为素理想。



证明 由素理想的定义 4.4.8 与极大理想的定义 4.4.9, 命题显然!

命题 4.4.6 (\mathbb{Z} 的素理想与极大理想)

$$p \text{ 为素数} \iff (p) \text{ 为 } \mathbb{Z} \text{ 的素理想} \iff (p) \text{ 为 } \mathbb{Z} \text{ 的极大理想} \iff \mathbb{Z}/(p) \text{ 为整环} \iff \mathbb{Z}/(p) \text{ 为域}$$



证明 如果 p 为素数, 那么任取理想 $I \supset (p)$, 由命题 4.4.1, 存在 $n \in \mathbb{N}^*$, 使得成立 $I = (n)$, 因此

$$(p) \subset (n) \implies p \in (n) \iff n \mid p \iff n = p \text{ 或 } n = 1 \iff (n) = (p) \text{ 或 } (n) = \mathbb{Z}$$

进而 (p) 为 \mathbb{Z} 的极大理想。

如果 p 不为素数, 那么存在 $1 < m, n < p$, 使得成立 $p = mn$, 那么

$$mn \in (p), \quad m \notin (p), \quad n \notin (p)$$

因此 (p) 不为 \mathbb{Z} 的素理想。

命题 4.4.7 ($F[x]$ 的素理想与极大理想)

对于域 F , 成立

$$\begin{aligned} & p(x) \text{ 为 } F[x] \text{ 的不可约多项式} \\ \iff & (p(x)) \text{ 为 } F[x] \text{ 的素理想} \iff (p(x)) \text{ 为 } F[x] \text{ 的极大理想} \\ \iff & F[x]/(p(x)) \text{ 为整环} \iff F[x]/(p(x)) \text{ 为域} \end{aligned}$$



证明 如果 $p(x)$ 为多项式环 $F[x]$ 的不可约多项式, 首先证明 $(p(x)) \subsetneq F[x]$ 。由于 $p(x)$ 不为常多项式, 那么 $\deg(p(x)) \geq 1$ 。对于任意 $f(x) \in F[x] \setminus \{0\}$, 由命题 4.1.25

$$\deg(p(x)f(x)) = \deg(p(x)) + \deg(f(x)) \geq 1 \implies p(x)f(x) \neq 1 \implies (p(x)) \subsetneq F[x]$$

其次任取 $F[x]$ 的理想 $I \supset (p(x))$, 证明成立 $I = (p(x))$ 或 $I = F[x]$ 。不妨 $p(x)$ 为首一多项式。由命题 4.4.2, 存在首一多项式 $f(x) \in F[x]$, 使得成立 $I = (f(x))$, 因此

$$(p(x)) \subset (f(x)) \iff p(x) \in (f(x)) \iff f(x) \mid p(x)$$

由于 $p(x)$ 为不可约多项式, 那么或成立

$$f(x) = p(x) \iff (f(x)) = (p(x))$$

或成立

$$f(x) = 1 \iff (f(x)) = F[x]$$

综合两方面, $p(x)$ 为 $F[x]$ 的极大理想。

如果 $p(x)$ 为可约多项式, 那么 $p(x)$ 可为常多项式, 或存在 $f(x), g(x) \in F[x]$, 使得成立

$$p(x) = f(x)g(x), \quad \deg(f(x)) < \deg(p(x)), \quad \deg(g(x)) < \deg(p(x))$$

若为前者, 则 $(p(x)) = F[x]$, 因此 $(p(x))$ 不为 $F[x]$ 的素理想。

若为后者, 则 $f(x)g(x) \in (p(x))$, 且 $f(x), g(x) \notin (p(x))$, 因此 $(p(x))$ 不为 $F[x]$ 的素理想。

综合两者, $(p(x))$ 不为 $F[x]$ 的素理想。

命题 4.4.8 (素理想的像为素理想)

对于非零交换环间的同态映射 $\varphi: R \rightarrow S$, 如果 $I \supset \ker \varphi$ 为 R 的素理想, 那么 $\varphi(I)$ 为 $\text{im } \varphi$ 的素理想。



证明 如果 I 为 R 的素理想, 那么由命题 4.3.4, $\varphi(I)$ 为 $\text{im } \varphi$ 的理想。由命题 4.3.16

$$\begin{aligned} & I \text{ 为 } R \text{ 的素理想} \\ \iff & R/I \text{ 为整环且 } I \subsetneq R \\ \iff & \text{im } \varphi / \varphi(I) \text{ 为整环且 } \varphi(I) \subsetneq \text{im } \varphi \\ \iff & \varphi(I) \text{ 为 } \text{im } \varphi \text{ 的素理想} \end{aligned}$$

命题 4.4.9 (素理想的原像为素理想)

对于非零交换环间的同态映射 $\varphi: R \rightarrow S$, 如果 J 为 $\text{im } \varphi$ 的素理想, 那么 $\varphi^{-1}(J)$ 为 R 的素理想, 且 $\ker \varphi \subset \varphi^{-1}(J)$ 。



证明 如果 J 为 $\text{im } \varphi$ 的素理想, 那么由命题4.3.5, $\varphi^{-1}(J)$ 为 R 的理想, 且 $\ker \varphi \subset \varphi^{-1}(J)$ 。由命题4.3.16, 以及命题4.3.6

$$\begin{aligned}
 & J \text{ 为 } \text{im } \varphi \text{ 的素理想} \\
 \iff & \text{im } \varphi / J \text{ 为整环且 } J \subsetneq \text{im } \varphi \\
 \iff & \text{im } \varphi / \varphi(\varphi^{-1}(J)) \text{ 为整环且 } \varphi(\varphi^{-1}(J)) \subsetneq \text{im } \varphi \\
 \iff & R / \varphi^{-1}(J) \text{ 为整环且 } \varphi^{-1}(J) \subsetneq R \\
 \iff & \varphi^{-1}(J) \text{ 为 } R \text{ 的素理想}
 \end{aligned}$$

命题 4.4.10

对于非零交换环间的同态映射 $\varphi: R \rightarrow S$, 如下集合函数为双射。

$$\begin{aligned}
 \Psi: \{I \supset \ker \varphi \text{ 为 } R \text{ 的素理想}\} &\longrightarrow \{J \text{ 为 } \text{im } \varphi \text{ 的素理想}\} \\
 I &\longmapsto \varphi(I)
 \end{aligned}$$

证明 由命题4.4.8, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性。由命题4.3.6, Ψ 为单射。

其次对于 Ψ 的满射性。如果 J 为 $\text{im } \varphi$ 的素理想, 那么由命题4.4.9, $\varphi^{-1}(J) \supset \ker \varphi$ 为 R 的素理想。由命题4.3.6, Ψ 为满射。

命题 4.4.11

对于非零交换环间的同态映射 $\varphi: R \rightarrow S$, 如下集合函数为双射。

$$\begin{aligned}
 \Psi: \{J \text{ 为 } \text{im } \varphi \text{ 的素理想}\} &\longrightarrow \{I \supset \ker \varphi \text{ 为 } R \text{ 的素理想}\} \\
 J &\longmapsto \varphi^{-1}(J)
 \end{aligned}$$

证明 由命题4.4.9, 函数 Ψ 定义良好。

首先对于 Ψ 的单射性。由命题4.3.7, Ψ 为单射。

其次对于 Ψ 的满射性。如果 $I \supset \ker \varphi$ 为 R 的素理想, 那么由命题4.4.8, $\varphi(I)$ 为 $\text{im } \varphi$ 的素理想。由命题4.3.7, Ψ 为满射。

命题 4.4.12 (商环素理想的结构)

如果 I 为环 $(R, +, \cdot)$ 的理想, 那么如下集合函数为双射。

$$\begin{aligned}
 \Phi: \{J \supset I \text{ 为 } R \text{ 的素理想}\} &\longrightarrow \{K \text{ 为 } R/I \text{ 的素理想}\} \\
 J &\longmapsto J/I
 \end{aligned}$$

证明 注意到如下自然环同态

$$\begin{aligned}
 \pi: R &\longrightarrow R/I \\
 r &\longmapsto r + I
 \end{aligned}$$

其中 $\ker \pi = I$, 且 $\text{im } \pi = R/I$ 。由命题, 如下集合函数为双射。

$$\begin{aligned}
 \Psi: \{J \supset I \text{ 为 } R \text{ 的素理想}\} &\longrightarrow \{K \text{ 为 } R/I \text{ 的素理想}\} \\
 J &\longmapsto \pi(J)
 \end{aligned}$$

注意到

$$\Phi(J) = J/I = \{j + I : j \in J\} = \pi(J) = \Psi(J)$$

因此 $\Phi = \Psi$, 进而 Φ 为双射。

命题 4.4.13

对于非零交换环 $(R, +, \cdot)$ 的理想 I , 如果 R/I 为有限环, 那么

$$I \text{ 为素理想} \iff I \text{ 为极大理想}$$

**命题 4.4.14**

对于主理想整环 $(R, +, \cdot)$, 如果 I 为 R 的非零理想, 那么

$$I \text{ 为素理想} \iff I \text{ 为极大理想}$$



证明 仅证明必要性。任取由于 R 为 PID, 那么存在素元 $p \in R$, 使得成立 $I = (p)$ 。由引理 5.1.3, p 不可约, 那么 p 非零且非单位, 因此 $(0) \subsetneq (p) \subsetneq (1)$ 。任取理想 $(a) \supset (p)$, 由引理 5.1.1, $a \mid p$, 进而或 $a \sim p$, 或 a 为单位。前者可得 $(a) = (p)$, 后者可得 $(a) = (1)$ 。综上所述, $I = (p)$ 为极大理想。

4.5 环上的模

4.5.1 R -模的定义

定义 4.5.1 (左 R -模 left- R -module)

定义环 $(R, +, \cdot)$ 关于 Abel 群 $(G, *)$ 的左 R -模为 $((G, *), \bullet)$, 其中集合函数 $\bullet: R \times G \rightarrow G$ 满足如下性质。

$$\begin{aligned} 1 \bullet g &= g \\ (r \cdot s) \bullet g &= r \bullet (s \bullet g) \\ r \bullet (g * h) &= r \bullet g + r \bullet h \\ (r + s) \bullet g &= r \bullet g + s \bullet g \end{aligned}$$

**命题 4.5.1 (Abel 群为 \mathbb{Z} -模)**

Abel 群为 \mathbb{Z} -模。



4.5.2 R -Mod 范畴

定义 4.5.2 (R -Mod 范畴)

对于环 $(R, +, \cdot)$, 定义 R -Mod 范畴如下。

1. 对象: $((G, *), \bullet)$, 其中 $(G, *)$ 为 Abel 群, 集合函数 $\bullet: R \times G \rightarrow G$ 为环 $(R, +, \cdot)$ 关于 Abel 群 $(G, *)$ 的 R -模。
2. 态射: $((G, *), \bullet) \rightarrow ((H, \star), \bullet)$ 的态射定义为集合函数 $\varphi: G \rightarrow H$, 满足 $\varphi(g * h) = \varphi(g) \star \varphi(h)$, 且 $\varphi(r \bullet g) = r \bullet \varphi(g)$ 。



4.5.3 子模与商

定义 4.5.3 (R -子模 R -submodule)

称 $((N, *), \bullet)$ 为环 $(R, +, \cdot)$ 的 R -模 $((G, *), \bullet)$ 的 R -子模, 如果 N 为 Abel 群 G 的子群。

定义 4.5.4 (商 quotient)

定义环 $(R, +, \cdot)$ 的 R -模 $((G, *), \bullet)$ 关于子模 $((N, *), \bullet)$ 的商为 R -模 $((G/N), \bullet)$, 其中 $r \bullet (g * N) = (r \bullet g) * N$ 。

定理 4.5.1 (子模的万有性质)

如果 $((N, *), \bullet)$ 为 R -模 $((G, *), \bullet)$ 的 R -子模, 那么对于任意满足 $N \subset \ker \varphi$ 的 R -Mod 态射 $\varphi: G \rightarrow H$, 存在且存在唯一 R -Mod 态射 $\bar{\varphi}: G/N \rightarrow H$, 使得成立 $\varphi = \bar{\varphi} \circ \pi$, 其中 $\pi: G \twoheadrightarrow G/N$, $g \mapsto g * N$, 交换图为

$$\begin{array}{ccc} G/N & \xrightarrow{\exists! \bar{\varphi}} & \forall H \\ \pi \swarrow & & \nearrow \forall \varphi \\ & G & \end{array}$$

定理 4.5.2 (R -子模是 R -Mod 态射的核; R -Mod 态射的核是 R -子模)

对于 R -模 G 的 R -子模 N , 成立 $\ker \pi = N$, 其中 $\pi: G \twoheadrightarrow G/N$ 为满的 R -Mod 态射; 对于 R -Mod 态射 $\varphi: G \rightarrow H$, $\ker \varphi$ 为 G 的子模。因此:

$$\text{核} \iff \text{子模}$$

4.5.4 正则分解与同构定理

定义 4.5.5 (R -Mod 态射的正则分解 canonical decomposition)

R -Mod 态射 $\varphi: G \rightarrow H$ 的正则分解如下。

$$\begin{array}{ccccccc} & & \varphi & & & & \\ & \nearrow & & \searrow & & & \\ G & \xrightarrow{g \mapsto g * \ker \varphi} & G / \ker \varphi & \xrightarrow[\varphi: g * \ker \varphi \mapsto \varphi(g)]{\sim} & \text{im } \varphi & \xrightarrow{\varphi(g) \mapsto \varphi(g)} & H \end{array}$$

定义 4.5.6 (第一同构定理 first isomorphism theorem)

对于 R -Mod 态射 $\varphi: G \rightarrow H$, 成立

$$G / \ker \varphi \cong \text{im } \varphi$$

定义 4.5.7 (第二同构定理 second isomorphism theorem)

如果 H, J 为 R -模 $(G, *)$ 的 R -子模, 那么 $H * J$ 为 G 的 R -子模, $H \cap J$ 为 G 的 R -子模, 且

$$\frac{H}{H \cap J} \cong \frac{H * J}{J}$$

定义 4.5.8 (第三同构定理 third isomorphism theorem)

如果 H, J 为 R -模 $(G, *)$ 的 R -子模, 且 $J \subset H$, 那么 H/J 为 G/J 的 R -子模, 且

$$\frac{G/J}{H/J} \cong \frac{G}{H}$$



第五章 环论 II

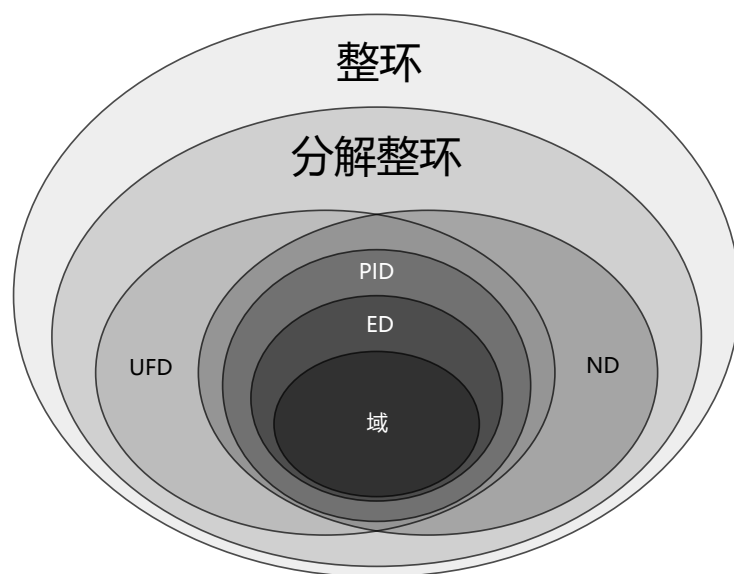


图 5.1: 整环的关系

5.1 分解整环与 Noether 环

5.1.1 素元与不可约元

定义 5.1.1 (整除 divide)

对于交换环 $(R, +, \cdot)$, 称 $a \in R$ 整除 $b \in R$, 并记作 $a \mid b$, 如果存在 $c \in R$, 使得成立 $b = a \cdot c$.

命题 5.1.1 (整除的反身性与传递性)

交换环元素间的整除关系具有反身性与传递性。

证明 对于反身性, 显然 $a = a \cdot 1$, 因此 $a \mid a$.

对于传递性, 如果 $a \mid b$, 且 $b \mid c$, 那么存在 $u, v \in R$, 使得成立 $b = a \cdot u$, 且 $c = b \cdot v$, 那么 $c = (u \cdot v) \cdot a$, 因此 $a \mid c$.

引理 5.1.1 (整除的等价条件)

对于整环 $(R, +, \cdot)$ 的非零元 $a, b \in R$, 成立

$$a \mid b \iff b \in (a) \iff (b) \subset (a)$$

证明 如果 $(b) \subset (a)$, 那么显然 $b \in (a)$.

如果 $b \in (a)$, 那么存在 $c \in R$, 使得成立 $b = a \cdot c$, 因此 $a \mid b$.

如果 $a \mid b$, 那么存在 $c \in R$, 使得成立 $b = a \cdot c$ 。任取 $x \in (b)$, 存在 $d \in R$, 使得成立 $x = b \cdot d$, 因此

$$x = b \cdot d = (c \cdot d) \cdot a \in (a)$$

由 x 的任意性, $(b) \subset (a)$ 。

定义 5.1.2 (因子 divisor)

对于交换环 $(R, +, \cdot)$, 称 $a \in R$ 为 $b \in R$ 的因子, 如果成立 $a \mid b$ 。



定义 5.1.3 (倍元 multiple)

对于交换环 $(R, +, \cdot)$, 称 $b \in R$ 为 $a \in R$ 的倍元, 如果成立 $a \mid b$ 。



定义 5.1.4 (相伴元 associate element)

对于交换环 $(R, +, \cdot)$, 称 $a \in R$ 与 $b \in R$ 相伴, 并记作 $a \sim b$, 如果成立 $a \mid b$, 且 $b \mid a$ 。



命题 5.1.2 (相伴为等价条件)

交换环元素间的相伴关系为等价关系。



证明 对于自反性, 显然 $a \mid a$, 因此 $a \sim a$ 。

对于对称性, 如果 $a \sim b$, 那么 $a \mid b$, 且 $b \mid a$, 因此 $b \sim a$ 。

对于传递性, 如果 $a \sim b$, 且 $b \sim c$, 那么

$$a \mid b, \quad b \mid a, \quad b \mid c, \quad c \mid b$$

由整除关系的传递性 5.1.1, $a \mid c$, 且 $c \mid a$, 那么 $a \sim c$ 。

引理 5.1.2 (相伴的等价条件)

对于整环 $(R, +, \cdot)$ 的非零元 $a, b \in R$, 成立

$$a \mid b \text{ 且 } b \mid a \iff (a) = (b) \iff \exists \text{ 单位 } u \in R, a = u \cdot b$$



证明 由引理 5.1.1, 成立

$$a \mid b \text{ 且 } b \mid a \iff (a) = (b)$$

下面证明

$$a \mid b \text{ 且 } b \mid a \iff \exists \text{ 单位 } u \in R, a = u \cdot b$$

对于必要性, 如果 $a \mid b$, 且 $b \mid a$, 那么存在 $c, d \in R$, 使得成立 $a = b \cdot c$, 且 $b = a \cdot d$, 那么

$$a = b \cdot c = c \cdot d \cdot a \implies (c \cdot d - 1)a = 0$$

由消去律, $c \cdot d = 1$, 因此 c 为单位。

对于充分性, 如果存在单位 $u \in R$, 使得成立 $a = u \cdot b$, 那么 $b \mid a$, 且存在 $v \in R$, 使得成立 $v \cdot u = 1$, 因此

$$b = 1 \cdot b = v \cdot u \cdot b = v \cdot a$$

于是 $b \mid a$ 。

定义 5.1.5 (素元 prime element)

对于整环 $(R, +, \cdot)$, 称 $p \in R$ 为素元, 如果 p 不为零元, 且 p 不为单位, 同时成立如下命题之一。

1.

$$p \mid a \cdot b \implies p \mid a \text{ 或 } p \mid b$$

2.

 (p) 为 R 的非零素理想**定义 5.1.6 (可约元 reducible element)**

对于整环 $(R, +, \cdot)$, 称 $p \in R$ 为可约元, 如果 p 不为零元, 或为单位, 或成立如下命题之一。

1. 存在非单位的元素 $a, b \in R$, 使得成立 $p = a \cdot b$ 。
2. 存在非相伴的元素 $a, b \in R$, 使得成立 $p = a \cdot b$ 。
3. 存在 $a, b \in R$, 使得成立 $p = a \cdot b$, 同时 $(p) \subsetneq (a)$, 且 $(p) \subsetneq (b)$ 。
4. 存在 $q \in R$, 使得成立 $(p) \subsetneq (q) \subsetneq (1)$ 。

**定义 5.1.7 (不可约元 irreducible element)**

对于整环 $(R, +, \cdot)$, 称 $p \in R$ 为不可约元, 如果 p 不为零元, 且 p 不为单位, 同时成立如下命题之一。

1.

$$p = a \cdot b \implies a \text{ 为单位或 } b \text{ 为单位}$$

2.

$$p = a \cdot b \implies p \text{ 与 } a \text{ 相伴或 } p \text{ 与 } b \text{ 相伴}$$

3.

$$p = a \cdot b \implies (p) = (a) \text{ 或 } (p) = (b)$$

4.

$$(p) \subset (q) \implies (p) = (q) \text{ 或 } (q) = (1)$$

**引理 5.1.3 (素元不可约)**

对于整环 $(R, +, \cdot)$, 如果 $p \in R$ 为素元, 那么 p 为不可约元。



证明 任取 $a, b \in R$, 使得成立 $p = a \cdot b$, 因此 $a \cdot b \in (p)$ 。一方面, 由于 p 为素元, 那么 (p) 为非零素理想, 因此 $a \in (p)$, 或 $b \in (p)$ 。不妨 $a \in (p)$, 那么 $(a) \subset (p)$ 。另一方面, 由于 $p = a \cdot b \in (a)$, 那么 $(p) \subset (a)$ 。综合两方面, $(p) = (a)$, 进而 p 为不可约元。

5.1.2 分解整环**定义 5.1.8 (完全因子分解 factorization into irreducibles)**

对于整环 $(R, +, \cdot)$, 称 $r \in R$ 可完全因子分解, 如果存在不可约元 $p_1, \dots, p_n \in R$, 使得成立

$$r = p_1 \cdots p_n$$

**定义 5.1.9 (唯一完全因子分解 unique factorization into irreducibles)**

对于整环 $(R, +, \cdot)$, 称 $r \in R$ 可唯一完全因子分解, 如果存在不可约元 $p_1, \dots, p_n \in R$, 使得成立

$$r = p_1 \cdots p_n$$

且若不可约元 $q_1, \dots, q_m \in R$ 成立

$$r = q_1 \cdots q_m$$

则 $m = n$, 且存在双射 $\tau: \mathbb{N}^* \rightarrow \mathbb{N}^*$, 使得对于任意 $1 \leq k \leq n$, p_k 与 $q_{\tau(k)}$ 相伴。



定义 5.1.10 (分解整环 domains with factorizations)

称整环为分解整环, 如果其任意非零非单位的元素可完全因子分解。

**定义 5.1.11 (唯一因子分解整环 unique factorization domain, UFD)**

称整环为唯一因子分解整环, 如果其任意非零非单位的元素可唯一完全因子分解。

**引理 5.1.4 (整除的等价条件)**

对于 UFD $(R, +, \cdot)$ 的非零元 $a, b \in R$, 并记 a 的不可约因子族构成多重集合 A , b 的不可约因子族构成多重集合 B , 成立

$$a \mid b \iff b \in (a) \iff (b) \subset (a) \iff A \leq B$$



证明 由引理 5.1.1, 成立

$$a \mid b \iff b \in (a) \iff (b) \subset (a)$$

如果 $a \mid b$, 那么存在 $c \in R$, 使得成立 $b = a \cdot c$. 由于 R 为 UFD, 那么记 a 与 c 的唯一完全因子分解为

$$a = p_1 \cdots p_n, \quad c = q_1 \cdots q_m$$

因此

$$b = p_1 \cdots p_n q_1 \cdots q_m$$

那么

$$A = \{p_1, \cdots, p_n\}, \quad B = \{p_1, \cdots, p_n, q_1, \cdots, q_m\}$$

进而 $A \leq B$.

如果 $A \leq B$, 那么由 R 为 UFD, 记 a 与 b 的唯一完全因子分解为

$$a = p_1^{i_1} \cdots p_n^{i_n}, \quad b = p_1^{j_1} \cdots p_n^{j_n} q_1^{k_1} \cdots q_m^{k_m}$$

其中 $p_1, \cdots, p_n, q_1, \cdots, q_m$ 为不可约元, 且

$$i_1, \cdots, i_n, j_1, \cdots, j_n, k_1, \cdots, k_m \in \mathbb{N}^*$$

由于 $A \leq B$, 那么

$$i_1 \leq j_1 \quad \cdots \quad i_n \leq j_n$$

记

$$c = p_1^{j_1 - i_1} \cdots p_n^{j_n - i_n} q_1^{k_1} \cdots q_m^{k_m}$$

因此 $b = a \cdot c$, 进而 $a \mid b$.

引理 5.1.5 (相伴的等价条件)

对于 UFD $(R, +, \cdot)$ 的非零元 $a, b \in R$, 并记 a 的不可约因子族构成多重集合 A , b 的不可约因子族构成多重集合 B , 成立

$$a \mid b \text{ 且 } b \mid a \iff (a) = (b) \iff \exists \text{ 单位 } u \in R, a = u \cdot b \iff A = B$$



证明 由引理 5.1.4 与 5.1.2, 命题显然。

5.1.3 Noether 环

定义 5.1.12 (稳定的 stabilize)

对于偏序集 (S, \preceq) , 称增序列

$$s_1 \preceq s_2 \preceq s_3 \preceq \cdots$$

为稳定的, 如果存在 $N \in \mathbb{N}^*$, 使得对于任意 $n \geq N$, 成立 $s_n = s_N$ 。



定义 5.1.13 (升链条件 ascending chain condition, a.c.c.)

称偏序集 (S, \preceq) 成立升链条件, 如果其任意增序列稳定。



定义 5.1.14 (极大条件 maximal element condition)

称偏序集 (S, \preceq) 成立极大条件, 如果其任意非空子集存在极大元。

定理 5.1.1 (升链条件 \iff 极大条件)

对于偏序集, 成立

$$\text{升链条件} \iff \text{极大条件}$$



证明 如果偏序集 (S, \preceq) 成立极大条件, 即其任意非空子集存在极大元, 那么对于任意增序列

$$s_1 \preceq s_2 \preceq s_3 \preceq \cdots$$

构成的非空子集 $\{s_n\}_{n=1}^{\infty}$ 存在极大元 x_N , 因此对于任意 $n \geq N$, 成立 $s_n = s_N$, 那么该增序列稳定, 进而该偏序集 (S, \preceq) 成立升链条件。

如果偏序集 (S, \preceq) 不成立极大条件, 即存在非空子集 $T \subset S$, 使得对于任意 $x \in T$, 存在 $y \in T$, 使得成立 $x \neq y$, 且 $x \preceq y$, 那么由数学归纳法, 存在增序列 $\{s_n\}_{n=1}^{\infty}$, 使得对于任意 $n \in \mathbb{N}^*$, 成立 $s_n \neq s_{n+1}$, 进而该偏序集 (S, \preceq) 不成立升链条件。

定义 5.1.15 (Noether 环)

称交换环 $(R, +, \cdot)$ 为 Noether 环, 如果成立如下命题之一。

1. R 的任意理想为有限生成理想。
2. R 成立理想升链条件。
3. R 成立理想极大条件。



证明 由定理 5.1.1, 成立

$$R \text{ 成立理想升链条件} \iff R \text{ 成立理想极大条件}$$

下面证明

$$R \text{ 的任意理想为有限生成理想} \iff R \text{ 成立理想升链条件}$$

如果 R 的任意理想为有限生成理想, 但是 R 不成立理想升链条件, 那么存在无限理想序列

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

记 $I = \bigcup_{n=1}^{\infty} I_n$, 那么 I 为 R 的理想。由于 R 的任意理想为有限生成理想, 那么存在 $\{r_k\}_{k=1}^n$, 使得成立 $I = (r_k)_{k=1}^n$, 因此对于任意 $1 \leq k \leq n$, 存在 $n_k \in \mathbb{N}^*$, 使得成立 $r_k \in I_{n_k}$ 。记 $N = \max_{1 \leq k \leq n} n_k$, 那么对于任意 $1 \leq k \leq n$, 成

立 $r_k \in I_N$, 进而 $I \subset I_N = \bigcup_{n=1}^N I_n$ 。而 $\bigcup_{n=1}^N I_n \subset I$, 因此 $I = \bigcup_{n=1}^N I_n$, 产生矛盾!

如果 R 成立理想升链条件, 但是存在无限生成理想 I , 那么由数学归纳法, 存在 $\{r_n\}_{n=1}^{\infty} \subset I$, 使得无限理

想序列

$$(r_1) \subsetneq (r_1, r_2) \subsetneq (r_1, r_2, r_3) \subsetneq \cdots$$

产生矛盾!

命题 5.1.3 (Noether 环的像为 Noether 环)

对于环同态映射 $\varphi: R \rightarrow S$, 如果 $(R, +, \cdot)$ 为 Noether 环, 那么 $\text{im } \varphi$ 为 Noether 环。

证明 任取 $\text{im } \varphi$ 的理想 J , 由命题 4.3.5, $\varphi^{-1}(J)$ 为 R 的理想。由于 R 为 Noether 环, 那么存在 $\{r_k\}_{k=1}^n \subset R$, 使得成立 $\varphi^{-1}(J) = (r_k)_{k=1}^n$, 进而 $J = (\varphi(r_k))_{k=1}^n$, 从而 $\text{im } \varphi$ 为 Noether 环。

定理 5.1.2 (ND \implies 分解整环)

Noether 环为分解整环。

证明 对于 $(R, +, \cdot)$, 任取非零非单位的元素 $r \in R$ 。如果 r 为不可约元, 那么 r 可完全因子分解。

如果 r 为可约元, 那么存在 $r_1, s_1 \in R$, 使得成立 $r = r_1 \cdot s_1$, 同时 $(r) \subsetneq (r_1)$, 且 $(r) \subsetneq (s_1)$ 。若 r_1 与 s_1 为不可约元, 那么 r 可完全因子分解。若 r_1 为可约元, 则重复如上过程。如果对于每一次过程, r_n 均可约, 那么可得无限理想序列

$$(r) \subsetneq (r_1) \subsetneq (r_2) \subsetneq \cdots$$

与 R 为 Noether 环矛盾!

综上所述, r 可完全因子分解, 进而 R 为分解整环。

定理 5.1.3 (PID \implies ND)

PID 为 Noether 环。

证明 任取 PID $(R, +, \cdot)$ 的递增主理想序列

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

由于 R 为 PID, 那么存在 $\{a_n\}_{n=1}^\infty \subset R$, 使得对于任意 $n \in \mathbb{N}^*$, 成立 $I_n = (a_n)$ 。定义

$$I = \bigcup_{n=1}^\infty I_n = \bigcup_{n=1}^\infty (a_n)$$

那么 I 为 R 的理想, 因此存在 $a \in R$, 使得成立 $I = (a)$ 。由于 $a \in \bigcup (a_n)$, 那么存在 $N \in \mathbb{N}^*$, 使得成立 $a \in (a_N)$, 进而 $(a) \subset (a_N)$ 。又因为 $(a_N) \subset (a)$, 那么 $(a) = (a_N)$, 因此对于任意 $n \geq N$, 成立 $(a_n) = (a_N)$, 进而 R 成立理想升链条件, 于是 R 为 Noether 环。

定理 5.1.4

对于 Noether 环 $(R, +, \cdot)$, 如果 I 为多项式环 $R[x_1, \cdots, x_n]$ 的理想, 那么商环 $R[x_1, \cdots, x_n]/I$ 为 Noether 环。

引理 5.1.6 (Hilbert 基定理)

R 为 Noether 环 $\iff R[x]$ 为 Noether 环

定义 5.1.16 (Noether 模)

对于交换环 $(R, +, \cdot)$, 称 R -模 M 为 Noether 模, 如果成立如下命题之一。

1. M 的任意子模为有限生成的。
2. M 的任意升子模链有限。
3. M 的任意子模族存在极大子模。

5.2 UFD, PID, ED

5.2.1 最大公因子

定义 5.2.1 (公因子 common divisor)

对于整环 $(R, +, \cdot)$, 称 $d \in R$ 为 $a, b \in R$ 的公因子, 如果成立如下命题之一。

1. $(a, b) \subset (d)$
2. $d \mid a$, 且 $d \mid b$ 。



定义 5.2.2 (最大公因子 greatest common divisor)

对于整环 $(R, +, \cdot)$, 称 $a, b \in R$ 的公因子 $d \in R$ 为最大公因子, 如果成立如下命题之一。

1. $(a, b) = (d)$
2. 对于任意 a, b 的公因子 d' , 成立 $d' \mid d$ 。



定义 5.2.3 (最大公因子条件 greatest common divisor condition)

称整环 $(R, +, \cdot)$ 成立最大公因子条件, 如果其任意非零元间存在最大公因子。



引理 5.2.1 (UFD \implies 最大公因子条件)

UFD 成立最大公因子条件。



证明 对于 UFD $(R, +, \cdot)$, 任取非零元 $a, b \in R$, 作唯一完全因子分解

$$a = u \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \quad b = v \cdot p_1^{\beta_1} \cdots p_n^{\beta_n}$$

其中 u, v 为单位, 且对于任意 $1 \leq k \leq n$, 成立 $\alpha_k, \beta_k \in \mathbb{N}$ 。记

$$d = p_1^{\min(\alpha_1, \beta_1)} \cdots p_n^{\min(\alpha_n, \beta_n)}$$

由于

$$a = u \cdot p_1^{\alpha_1 - \min(\alpha_1, \beta_1)} \cdots p_n^{\alpha_n - \min(\alpha_n, \beta_n)} \cdot d, \quad b = v \cdot p_1^{\beta_1 - \min(\alpha_1, \beta_1)} \cdots p_n^{\beta_n - \min(\alpha_n, \beta_n)} \cdot d$$

那么 $a \mid d$ 且 $b \mid d$, 因此 d 为 a, b 的公因子。任取 a, b 的公因子 c , 由引理 5.1.4, 作唯一完全因子分解

$$c = w \cdot p_1^{\gamma_1} \cdots p_n^{\gamma_n}$$

其中对于任意 $1 \leq k \leq n$, 成立 $\gamma_k \geq \min(\alpha_k, \beta_k)$ 。由于

$$c = w \cdot p_1^{\gamma_1 - \min(\alpha_1, \beta_1)} \cdots p_n^{\gamma_n - \min(\alpha_n, \beta_n)} \cdot d$$

那么 $c \mid d$, 进而 d 为 a, b 的最大公因子。

5.2.2 UFD

定义 5.2.4 (素元性条件 prime element condition)

称整环 $(R, +, \cdot)$ 成立素元性条件, 如果对于其任意不可约元为素元。



引理 5.2.2

如果整环 $(R, +, \cdot)$ 成立最大公因子条件, 那么对于任意 $a, b, c \in R$, 成立 $\gcd(a \cdot b, a \cdot c) \sim a \cdot \gcd(b, c)$



证明 如果 $a = 0$, 那么 $\gcd(a \cdot b, a \cdot c) \sim a \cdot \gcd(b, c) \sim 0$ 。

如果 $\gcd(b, c) = 0$, 那么 $b = c = 0$, 从而 $\gcd(a \cdot b, a \cdot c) \sim a \cdot \gcd(b, c) \sim 0$ 。

如果 $a \neq 0$ 且 $\gcd(b, c) \neq 0$, 由于 $\gcd(b, c) \mid b$ 且 $\gcd(b, c) \mid c$, 那么 $a \cdot \gcd(b, c) \mid a \cdot b$ 且 $a \cdot \gcd(b, c) \mid a \cdot c$, 进而 $a \cdot \gcd(b, c) \mid \gcd(a \cdot b, a \cdot c)$, 因此存在 $u \in R$, 使得成立 $\gcd(a \cdot b, a \cdot c) = a \cdot u \cdot \gcd(b, c)$ 。由于 $\gcd(a \cdot b, a \cdot c) \mid a \cdot b$, 那么存在 $v \in R$, 使得成立 $a \cdot b = v \cdot \gcd(a \cdot b, a \cdot c)$, 因此 $a \cdot b = v \cdot a \cdot u \cdot \gcd(b, c)$ 。由消去律, $b = v \cdot u \cdot \gcd(b, c)$, 进而 $u \cdot \gcd(b, c) \mid b$ 。同理, $u \cdot \gcd(b, c) \mid c$, 进而 $u \cdot \gcd(b, c) \mid \gcd(b, c)$, 因此存在 $u' \in R$, 使得成立 $\gcd(b, c) = u \cdot u' \cdot \gcd(b, c)$, 由消去律 $u \cdot u' = 1$, 进而 u 为单位, 那么 $\gcd(a \cdot b, a \cdot c) \sim a \cdot \gcd(b, c)$ 。

引理 5.2.3 (最大公因子条件 \implies 素元性条件)

如果整环 $(R, +, \cdot)$ 成立最大公因子条件, 那么 R 成立素元性条件。



证明 任取不可约元 $p \in R$, 取 $a, b \in R$ 使得成立 $p \mid a \cdot b$ 。由于 $\gcd(p, a) \mid p$, 那么或 $\gcd(p, a) \sim p$, 或 $\gcd(p, a)$ 为单位。

如果 $\gcd(p, a) \sim p$, 那么 $p \mid \gcd(p, a)$, 因此 $p \mid a$ 。

如果 $\gcd(p, a)$ 为单位, 那么 $\gcd(p, a) \sim 1$, 因此 $b \cdot \gcd(p, a) \sim b$ 。由引理 5.2.2, $\gcd(p \cdot b, a \cdot b) \sim b$ 。由于 $p \mid p \cdot b$, 且 $p \mid a \cdot b$, 那么 $p \mid \gcd(p \cdot b, a \cdot b)$, 进而 $p \mid b$ 。

综上所述, p 为素元, 进而 R 成立素元性条件。

引理 5.2.4 (UFD \implies 素元性条件)

UFD 成立素元性条件。



证明 (法一) 由引理 5.2.1 与 5.2.3, 命题得证!

(法二) 对于 UFD $(R, +, \cdot)$, 任取不可约元 $p \in R$, 取 $a, b \in R$ 使得成立 $p \mid a \cdot b$ 。分别记 p, a, b 的不可约因子族构成的多重集合为 P, A, B , 那么由引理 5.1.4

$$P = \{p\} \leq A \sqcup B$$

那么不妨 $P \leq A$, 因此由引理 5.1.4, $p \mid a$, 进而 p 为素元。

定义 5.2.5 (主理想升链条件 ascending chain condition for principal ideal)

称整环 $(R, +, \cdot)$ 成立主理想升链条件, 如果其任意递增主理想序列稳定。



引理 5.2.5 (UFD \implies 主理想升链条件)

UFD 成立主理想升链条件。



证明 对于 UFD $(R, +, \cdot)$, 任取严格递增主理想序列

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

那么由引理 5.1.1 与 5.1.2, 对于任意 $n \in \mathbb{N}^*$, a_{n+1} 为 a_n 的非相伴因子。

如果 $a_1 = 0$, 那么对于任意 $n \in \mathbb{N}^*$, $a_n = 0$ 。

如果 a_1 为单位, 那么对于任意 $n \in \mathbb{N}^*$, $(a_n) = (1)$ 。

如果 a_1 非零且非单位, 那么对于 a_1 作唯一完全因子分解

$$a_1 = p_1 \cdots p_n$$

其中 p_1, \dots, p_n 为不可约元, 显然 a_1 的非相伴因子有限。

综上所述, R 成立主理想升链条件。

引理 5.2.6 (素元性条件 + 主理想升链条件 \implies UFD)

如果整环 $(R, +, \cdot)$ 成立素元性条件与主理想升链条件, 那么 R 为 UFD。



证明 对于存在性, 任取非零非单位的元素 $a \in R$, 如果 a 为不可约元, 那么 a 可完全因子分解。如果 a 为可约元, 那么由主理想升链条件, a 存在不可约因子 p_1 , 于是 $a = p_1 a_1$ 。如果 a_1 不可约, 那么 a 可完全因子分解。

如果 a_1 可约, 那么重复上述过程, 结合主理想升链条件, 可得 a 的完全因子分解 $a = p_1 \cdots p_n$ 。

对于唯一性, 如果非零非单位的元素 $a \in R$ 存在完全因子分解

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

对于 n 进行归纳。当 $n = 1$ 时

$$a = p_1 = q_1 \cdots q_m$$

如果 $m \geq 2$, 那么

$$p_1 = q_1(q_2 \cdots q_m)$$

由于 p_1 不可约, 那么 p_1 与 q_1 相伴, 进而存在单位 $u \in R$, 使得成立 $q_1 = p_1 u$, 因此 $p_1 = p_1 u(q_2 \cdots q_m)$ 。由消去律, $1 = u(q_2 \cdots q_m)$, 进而 q_2 为单位, 矛盾! 从而 $m = 1$, 命题得证!

假设当 $n = k$ 时, 命题成立, 那么当 $n = k + 1$ 时, 由于 p_1 不可约, 那么由素元性条件, p_1 为素元。由于 $p_1 \mid q_1 \cdots q_m$, 那么不妨 $p_1 \mid q_1$ 。由于 q_1 不可约, 那么 $p_1 \sim q_1$, 进而存在单位 $v \in R$, 使得成立 $p_1 = q_1 v$, 进而

$$q_1 v p_2 \cdots p_{k+1} = q_1 \cdots q_m$$

由消去律

$$v p_2 \cdots p_{k+1} = q_2 \cdots q_m$$

由归纳假设, $n = k + 1$ 时命题得证!

综上所述, R 为 UFD。

定理 5.2.1 (UFD 的等价条件)

对于整环 $(R, +, \cdot)$, 成立

R 为 UFD $\iff R$ 成立最大公因子条件、素元性条件与主理想升链条件



证明 由引理 5.2.1、5.2.3、5.2.4、5.2.5、5.2.6, 命题得证!

5.2.3 PID \implies UFD

定理 5.2.2 (PID \implies UFD)

PID 为 UFD。



证明 对于 PID $(R, +, \cdot)$, 任取不可约元 p , 由命题 4.4.14, (p) 为非零极大理想, 进而为非零素理想, 因此 p 为素元, 从而 R 成立素元性条件。

由定理 5.1.3, R 成立理想升链条件。特别的, R 成立主理想升链条件。

由引理 5.2.6, R 为 UFD。

5.2.4 Euclid 整环

定义 5.2.6 (Euclid 整环)

称整环 $(R, +, \cdot)$ 为 Euclid 整环, 如果存在映射 $v: R \setminus \{0\} \rightarrow \mathbb{N}$, 使得对于任意 $a \in R$ 与 $b \in R \setminus \{0\}$, 存在 $q, r \in R$, 使得成立

$$a = q \cdot b + r, \quad r = 0 \text{ 或 } r \neq 0, v(r) < v(b)$$



定理 5.2.3 (ED \implies PID)

ED 为 PID。



证明 对于 Euclid 整环 $(R, +, \cdot)$ ，任取非零理想 I ，令 $b \in I \setminus \{0\}$ 满足对于任意 $r \in I \setminus \{0\}$ ，成立 $v(b) \leq v(r)$ ，那么 $(b) \subset I$ 。任取 $a \in I$ ，由于 R 为 Euclid 整环，那么存在 $q, r \in R$ ，使得成立

$$a = q \cdot b + r, \quad r = 0 \text{ 或 } r \neq 0, v(r) < v(b)$$

如果 $r \neq 0$ ，那么与 b 的定义矛盾！因此 $r = 0$ ，于是 $a = q \cdot b \in (b)$ 。由 a 的任意性， $I \subset (b)$ ，进而 $I = (b)$ 。由 I 的任意性， R 为 PID。

引理 5.2.7

对于交换环 $(R, +, \cdot)$ ，如果 $a = q \cdot b + r$ ，那么 $(a, b) = (b, r)$ 。



证明 由于 $a = q \cdot b + r \in (b, r)$ ，那么 $(a, b) \subset (b, r)$ 。由于 $r = a - q \cdot b \in (a, b)$ ，那么 $(a, b) \supset (b, r)$ 。进而 $(a, b) = (b, r)$ 。

定义 5.2.7 (Euclid 算法)

对于 Euclid 整环 $(R, +, \cdot)$ ，计算 $a, b \in R$ 的最大公因子。使用带余除法

$$a = b \cdot q_1 + r_1$$

$$b = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

...

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$

$$r_{n-1} = r_n \cdot q_{n+1}$$

由引理 5.2.7

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n)$$

进而 $\gcd(a, b) = r_n$ 。



5.3 间奏曲：Zorn 引理

5.3.1 集合论：再一次邂逅

定义 5.3.1 (序关系 ordered relation)

称集合 S 上的关系 \preceq 为序关系，如果其成立如下性质。

1. 自反性 (reflexivity): $a \preceq a$
2. 反对称性 (antisymmetry): $a \preceq b$ 且 $b \preceq a \implies a = b$
3. 传递性 (transitivity): $a \preceq b$ 且 $b \preceq c \implies a \preceq c$



定义 5.3.2 (严格序关系 strict ordered relation)

称集合 S 上的关系 \prec 为严格序关系，如果其成立如下性质。

1. 非自反性 (irreflexivity): $\neg a \prec a$
2. 非对称性 (asymmetry): $a \prec b \implies \neg b \prec a$
3. 传递性 (transitivity): $a \prec b$ 且 $b \prec c \implies a \prec c$



定义 5.3.3 (全序集 totally ordered set, toset / 链 chain)

称集合结构 (S, \preceq) 为全序集，如果 \preceq 为 S 上的序关系，且对于任意 $s, t \in S$ ，或成立 $s \preceq t$ ，或成立 $t \preceq s$ 。

定义 5.3.4 (偏序集 partially ordered set, poset)

称集合结构 (S, \preceq) 为偏序集，如果 \preceq 为 S 上的序关系，且存在子集 $T \subset S$ ，使得 (T, \preceq) 为全序集。

定义 5.3.5 (良序集 well ordered set, woset)

称全序集 (S, \preceq) 为良序集，如果任意非空子集存在极小元。

定义 5.3.6 (极大元 maximal element)

对于偏序集 (S, \preceq) ，称 $m \in S$ 为 S 的极大元，如果对于任意 $s \in S$ ，成立

$$m \preceq s \implies m = s$$

定义 5.3.7 (极小元 least element)

对于偏序集 (S, \preceq) ，称 $\flat \in S$ 为 S 的极小元，如果对于任意 $s \in S$ ，成立

$$s \preceq \flat \implies s = \flat$$

定义 5.3.8 (上界 upper bound)

对于偏序集 (S, \preceq) ，称 $u \in S$ 为子集 $T \subset S$ 的上界，如果对于任意 $t \in T$ ，成立 $t \preceq u$ 。

定理 5.3.1 (Zorn 引理)

对于偏序集 (S, \preceq) ，如果 S 的任意全序子集在 S 中存在上界，那么 S 存在极大元。

定理 5.3.2 (选择公理 axiom of choice)

如果 \mathcal{A} 为集合 S 的非空不交子集族，那么可以对于任意 $X \in \mathcal{A}$ ，选择 $x \in X$ ，使得被选择的所有元素构成集合。

定理 5.3.3 (良序定理 well-ordering theorem)

对于任意集合 S ，存在序关系 \preceq ，使得 (S, \preceq) 为良序集。

定理 5.3.4

$$\text{Zorn 引理} \iff \text{选择公理} \iff \text{良序定理}$$

定理 5.3.5 (归纳原理 principle of induction)

1. 对于良序集 (S, \preceq) ，如果子集 $T \subset S$ 成立

$$\forall s \in S, ((\forall t \in S, (t \prec s \implies t \in T)) \implies s \in T)$$

那么 $T = S$ 。

2. 对于良序集 (S, \preceq) ，其极小元为 \flat ，如果命题 $P : S \rightarrow \text{Bool}$ 成立

$$P(\flat) = \text{True}$$

$$\forall s \in S, ((\forall t \in S, (t \prec s \implies P(t) = \text{True})) \implies P(s) = \text{True})$$

那么

$$\forall s \in S, \quad P(s) = \text{True}$$



证明 事实上, $1 \iff 2$. 取

$$P : S \longrightarrow \text{Bool}$$

$$T = \{s \in S : P(s) = \text{True}\} \iff s \mapsto \begin{cases} \text{True}, & s \in T \\ \text{False}, & s \notin T \end{cases}$$

那么

$$\forall s \in S, \quad ((\forall t \in S, \quad (t \prec s \implies t \in T)) \implies s \in T)$$



$$\forall s \in S, \quad ((\forall t \in S, \quad (t \prec s \implies P(t) = \text{True})) \implies P(s) = \text{True})$$

对于极小元 s , 由于命题 $\forall t \in S, (t \prec s \implies t \in T)$ 为 **False**, 那么 $P(s) = \text{True}$. 进而 $1 \iff 2$.

下面证明原命题. 如果 $T \subsetneq S$, 那么 $S \setminus T \neq \emptyset$. 由于 S 为良序集, 那么 $S \setminus T$ 存在极小元 $s^* \in S \setminus T$. 由于对于任意 $t \in S$, 成立若 $t \prec s^*$, 则 $t \in T$, 那么 $s^* \in T$, 因此产生矛盾! 进而原命题得证!

5.3.2 应用: 极大理想的存在性

定理 5.3.6 (极大理想的存在性)

对于交换环 $(R, +, \cdot)$, 如果 $I \subsetneq R$ 为 R 的真理想, 那么 R 存在极大理想 M , 使得成立 $I \subset M$.



证明 记 \mathcal{J} 为 R 中所有包含 I 的真理想, \mathcal{C} 为偏序集 (\mathcal{J}, \subset) 的任意链, 并令

$$U = \bigcup_{J \in \mathcal{C}} J$$

断言 U 为包含 I 的真理想, 因此 U 为 \mathcal{C} 在 \mathcal{J} 中的上界. 由 Zorn 引理 5.3.1, (\mathcal{J}, \subset) 存在极大元 M , 此为 R 的极大理想, 且 $I \subset M$.

5.4 多项式环的唯一完全因子分解

5.4.1 Gauss 引理

引理 5.4.1

对于环 $(R, +, \cdot)$, 如果 I 为 R 的理想, 那么

$$\frac{R[x]}{I[x]} \cong \frac{R}{I}[x]$$

其中

$$I[x] = \left\{ \sum_{k=0}^n a_k x^k : a_k \in I, n \in \mathbb{N} \right\}$$



证明 构造映射

$$\varphi : \frac{R[x]}{I[x]} \longrightarrow \frac{R}{I}[x]$$

$$\sum_{k=0}^n (a_k + I) x^k \mapsto \sum_{k=0}^n a_k x^k$$

首先我们来证明 φ 为环同态映射, 这是因为

$$\begin{aligned}
 & \varphi \left(\sum_{k=0}^n (a_k + I)x^k + \sum_{k=0}^m (b_k + I)x^k \right) \\
 &= \varphi \left(\sum_{k=0}^n (a_k + b_k + I)x^k \right) \\
 &= \sum_{k=0}^n (a_k + b_k)x^k \\
 &= \sum_{k=0}^n (a_k + I)x^k + \sum_{k=0}^m (b_k + I)x^k \\
 &= \varphi \left(\sum_{k=0}^n (a_k + I)x^k \right) + \varphi \left(\sum_{k=0}^m (b_k + I)x^k \right) \\
 &= \varphi \left(\left(\sum_{k=0}^n (a_k + I)x^k \right) \left(\sum_{k=0}^m (b_k + I)x^k \right) \right) \\
 &= \varphi \left(\sum_{k=0}^{m+n} \sum_{i+j=k} (a_i b_j + I)x^k \right) \\
 &= \sum_{k=0}^{m+n} \sum_{i+j=k} (a_i b_j)x^k \\
 &= \left(\sum_{k=0}^n a_k x^k \right) \left(\sum_{k=0}^m b_k x^k \right) \\
 &= \varphi \left(\sum_{k=0}^n (a_k + I)x^k \right) \varphi \left(\sum_{k=0}^m (b_k + I)x^k \right) \\
 &= \varphi(1 + I) = 1
 \end{aligned}$$

其次显然

$$\ker \varphi = I[x], \quad \text{im } \varphi = R[x]$$

从而由环第一同构定理4.3.4, 成立

$$\frac{R[x]}{I[x]} \cong \frac{R}{I}[x]$$

推论 5.4.1

对于环 $(R, +, \cdot)$, 如果 P 为 R 的素理想, 那么 $P[x]$ 为 $R[x]$ 的素理想。



证明 如果 P 为 R 的素理想, 那么 R/P 为整环, 因此由命题4.1.26, $(R/P)[x]$ 为整环。由引理5.4.1, $R[x]/P[x]$ 为整环, 进而 $P[x]$ 为 $R[x]$ 的素理想。

定义 5.4.1 (本原多项式 primitive polynomial)

对于交换环 $(R, +, \cdot)$, 称多项式 $f(x) \in R[x]$ 为本原多项式, 如果对于 R 的任意主素理想 P , 成立 $f(x) \notin P[x]$ 。



定义 5.4.2 (超本原多项式 very primitive polynomial)

对于交换环 $(R, +, \cdot)$, 称多项式 $f(x) = \sum_{k=0}^n a_k x^k \in R[x]$ 为超本原多项式, 如果成立如下命题之一。

1. 对于 R 的任意素理想 P , 成立 $f(x) \notin P[x]$ 。

2. $(a_0, \dots, a_n) = (1)$



证明 $2 \implies 1$: 如果 $(a_0, \dots, a_n) = (1)$, 那么不存在素理想包含所有的 a_k , 因此对于 R 的任意素理想 P , 成立 $f(x) \notin P[x]$ 。

$1 \implies 2$: 由于对于 R 的任意素理想 P , 成立 $f(x) \notin P[x]$, 那么 $f(x)$ 的系数 a_k 并不都包含在任意素理想中, 特备的, $f(x)$ 的系数 a_k 并不都包含在任意极大理想中。由定理 5.3.6, $(a_0, \dots, a_n) = (1)$ 。

引理 5.4.2

对于交换环 $(R, +, \cdot)$, 如果 $f(x), g(x) \in R[x]$, 那么

$$f(x)g(x) \text{ 为本原多项式} \iff f(x) \text{ 与 } g(x) \text{ 均为本原多项式}$$



证明 此为推论 5.4.1 的简单结果:

$$\begin{aligned} f(x)g(x) \text{ 为本原多项式} &\iff \text{对于 } R \text{ 的任意主素理想 } P, \text{ 成立 } f(x)g(x) \notin P[x] \\ &\iff \text{对于 } R \text{ 的任意主素理想 } P, \text{ 成立 } f(x) \notin P[x] \text{ 且 } g(x) \notin P[x] \\ &\iff f(x) \text{ 与 } g(x) \text{ 均为本原多项式} \end{aligned}$$

引理 5.4.3

对于交换环 $(R, +, \cdot)$, 如果 $f(x), g(x) \in R[x]$, 那么

$$f(x)g(x) \text{ 为超本原多项式} \iff f(x) \text{ 与 } g(x) \text{ 均为超本原多项式}$$



证明 此为推论 5.4.1 的简单结果:

$$\begin{aligned} f(x)g(x) \text{ 为超本原多项式} &\iff \text{对于 } R \text{ 的任意素理想 } P, \text{ 成立 } f(x)g(x) \notin P[x] \\ &\iff \text{对于 } R \text{ 的任意素理想 } P, \text{ 成立 } f(x) \notin P[x] \text{ 且 } g(x) \notin P[x] \\ &\iff f(x) \text{ 与 } g(x) \text{ 均为超本原多项式} \end{aligned}$$

引理 5.4.4

对于 UFD $(R, +, \cdot)$, 如果 $f(x) = \sum_{k=0}^n a_k x^k \in R[x]$, 那么

$$f(x) \text{ 为本原多项式} \iff (a_0, \dots, a_n) = (1)$$



证明 由于 R 为 UFD, 结合引理 5.2.4, 那么

$$\begin{aligned} (a_0, \dots, a_n) \neq (1) &\iff \text{存在不可约元 } p \in R, \text{ 使得成立 } (a_0, \dots, a_n) \subset (p) \\ &\iff f(x) \text{ 不为本原多项式} \end{aligned}$$

定义 5.4.3 (容度 content)

对于 UFD $(R, +, \cdot)$, 定义多项式 $f(x) = \sum_{k=0}^n a_k x^k \in R[x]$ 的容度为

$$\text{cont}_f = \gcd(a_0, \dots, a_n)$$


引理 5.4.5

对于 UFD $(R, +, \cdot)$, 以及多项式 $f(x) \in R[x]$, 成立如下命题。

1. 如果 $f(x)$ 为本原多项式, 那么 $(f(x)) = (\text{cont}_f) \cdot (f(x))$ 。

2. 对于 $r \in R$ 与本原多项式 $g(x) \in R[x]$, 如果 $(f(x)) = (r) \cdot (g(x))$, 那么 $(r) = (\text{cont}_f)$ 。

定理 5.4.1 (Gauss 引理)

对于 UFD $(R, +, \cdot)$, 如果 $f(x), g(x) \in R[x]$ 为本原多项式, 那么

$$(\text{cont}_{fg}) = (\text{cont}_f) \cdot (\text{cont}_g)$$

证明 由于 $f(x), g(x)$ 为本原多项式, 那么由引理 5.4.2, $f(x)g(x)$ 为本原多项式。由命题 4.3.9 与 ?? 及引理 5.4.5

$$(f(x)g(x)) = (f(x)) \cdot (g(x)) = (\text{cont}_f) \cdot (f(x)) \cdot (\text{cont}_g) \cdot (g(x)) = (\text{cont}_f) \cdot (\text{cont}_g) \cdot (f(x)g(x))$$

由引理 5.4.5

$$(\text{cont}_{fg}) = (\text{cont}_f) \cdot (\text{cont}_g)$$

推论 5.4.2

对于 UFD $(R, +, \cdot)$, 如果 $f(x), g(x) \in R[x]$ 为本原多项式, 且 $(f(x)) \subset (g(x))$, 那么 $(\text{cont}_f) \subset (\text{cont}_g)$ 。

5.4.2 整环的分式域

定义 5.4.4 (整环范畴)

对于整环 $(R, +, \cdot)$, 定义整环范畴 \mathcal{R} 如下。

1. 对象:

$$R \hookrightarrow K$$

其中 K 为域。

2. 态射:

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & F \\ & \searrow i & \nearrow j \\ & R & \end{array}$$

定义 5.4.5 (分式域 field of fractions)

对于整环 $(R, +, \cdot)$, 其分式域 $K(R)$ 为其生成的整环范畴 \mathcal{R} 的初始对象; 换言之, 对于任意域 F 及单的环同态映射 $j: R \hookrightarrow F$, 存在且存在唯一环同态映射 $\varphi: K(R) \rightarrow F$, 使得成立

$$\begin{array}{ccc} K(R) & \xrightarrow{\exists! \varphi} & \forall F \\ & \searrow i & \nearrow \forall j \\ & R & \end{array}$$

推论 5.4.3

整环生成的分式域为包含该整环的最小域。

定理 5.4.2 (分式域的构造)

对于整环 $(R, +, \cdot)$, 记 $R \times R^\times$ 的元素为 a/r 形式, 并构造等价关系

$$\frac{a}{r} \sim \frac{b}{s} \iff a \cdot s = b \cdot r$$

令

$$K(R) = R \times R^\times / \sim = \left\{ \frac{a}{r} : a \in R, r \in R^\times \right\}$$

定义 $K(R)$ 上的运算

$$\frac{a}{r} + \frac{b}{s} = \frac{a \cdot s + b \cdot r}{r \cdot s}, \quad \frac{a}{r} \cdot \frac{b}{s} = \frac{a \cdot b}{r \cdot s}$$



例题 5.1 $K(\mathbb{Z}) = \mathbb{Q}$

例题 5.2 对于环 $(R, +, \cdot)$, 记多项式环 $R[x]$ 生成的分式域为 $R(x)$ 。

5.4.3 R 为 UFD $\implies R[x]$ 为 UFD

引理 5.4.6

对于 UFD $(R, +, \cdot)$, 其生成的分式域为 K 。对于 $f(x), g(x) \in R[x]$, 记 $(f(x))_R$ 与 $(g(x))_R$ 分别为 $f(x)$ 与 $g(x)$ 在 $R[x]$ 中生成的主理想, $(f(x))_K$ 与 $(g(x))_K$ 分别为 $f(x)$ 与 $g(x)$ 在 $K[x]$ 中生成的主理想。如果 $(\text{cont}_g) \subset (\text{cont}_f)$, 且 $(g(x))_K \subset (f(x))_K$, 那么 $(g(x))_R \subset (f(x))_R$ 。



定理 5.4.3

对于 UFD $(R, +, \cdot)$, 其生成的分式域为 K , 对于非常多项式 $f(x) \in R[x]$, 成立

$$f(x) \text{ 在 } R[x] \text{ 中不可约} \iff f(x) \text{ 在 } K[x] \text{ 中不可约且为本原多项式}$$



定理 5.4.4 (R 为 UFD $\implies R[x]$ 为 UFD)

如果 $(R, +, \cdot)$ 为 UFD, 那么 $R[x]$ 为 UFD。



5.5 多项式的不可约性

5.5.1 根与可约性

定义 5.5.1 (根 root)

对于交换环 $(R, +, \cdot)$ 上的多项式 $f(x) \in R[x]$, 称 $a \in R$ 为 $f(x)$ 的根, 如果 $f(a) = 0$ 。



命题 5.5.1

对于交换环 $(R, +, \cdot)$ 上的多项式 $f(x) \in R[x]$, 成立

$$f(a) = 0 \iff (x - a) \mid f(x)$$



证明 充分性显然! 对于必要性, 如果 $f(a) = 0$, 那么带余除法 4.4.1, 存在且存在唯一 $g(x), r(x) \in R[x]$, 使得成立

$$f(x) = (x - a)g(x) + r(x), \quad \deg(r(x)) < \deg(x - a) = 1$$

而 $f(a) = r(a) = 0$, 因此 $r(x) = 0$, 进而 $f(x) = (x - a)g(x)$, 从而 $(x - a) \mid f(x)$, 必要性得证!

定义 5.5.2 (n 重根 root with multiplicity n)

对于交换环 $(R, +, \cdot)$ 上的多项式 $f(x) \in R[x]$, 称 $a \in R$ 为 $f(x)$ 的 n 重根, 如果

$$(x - a)^n \mid f(x), \quad (x - a)^{n+1} \nmid f(x)$$



引理 5.5.1 (n 次多项式至多存在 n 个根)

对于整环 $(R, +, \cdot)$, 如果 $f(x) \in R[x]$ 为 n 次多项式, 那么 $f(x)$ 至多存在 n 个根, 其中个数依重数计算。❤

证明 记 R 生成的分式域为 K , 那么 $f(x)$ 在 R 中的根亦为 $f(x)$ 在 K 中的根。由定理 5.4.4, $K[x]$ 为 UFD。而 $f(x)$ 的根对应于一次不可约因子, 因此 $f(x)$ 在 K 中至多存在 n 个根, 进而 $f(x)$ 在 R 中至多存在 n 个根。

笔记 若 R 不为整环, 则 n 次多项式 $f(x)$ 在 R 中可能存在不止 n 个根, 例如: $x^2 + x$ 在 $\mathbb{Z}/6\mathbb{Z}$ 中存在 4 个根 0, 1, 3, 5。

推论 5.5.1

对于含无穷多个元素的整环 $(R, +, \cdot)$ 上的多项式 $f(x), g(x) \in R[x]$, 如果对于任意 $a \in R$, 成立 $f(a) = g(a)$, 那么 $f(x) = g(x)$ 。❤

证明 这当然是显然的! 作 $h(x) = f(x) - g(x)$, 那么 R 中元素均为 $h(x)$ 的零点, 进而由引理 5.5.1, $h(x) = 0$ 。

命题 5.5.2

对于域 K 上的 2 次或 3 次多项式 $f(x) \in K[x]$, 成立

$$f(x) \text{ 在 } K \text{ 中不可约} \iff f(x) \text{ 在 } K \text{ 中无根}$$

证明 如果 $f(x)$ 在 K 中存在根 a , 那么由命题 5.5.1, 存在非常数多项式 $g(x) \in K[x]$, 使得成立 $f(x) = (x-a)g(x)$, 进而 $f(x)$ 在 K 中可约。

如果 $f(x)$ 在 K 中可约, 那么存在非常数多项式 $g(x), h(x) \in K[x]$, 使得成立 $f(x) = g(x)h(x)$ 。由于 $\deg(f(x)) = 2$ 或 3 , 那么 $g(x)$ 与 $h(x)$ 之一为一次多项式, 不妨 $h(x) = x - a$, 因此 $f(x) = (x - a)g(x)$, 进而 a 为 $f(x)$ 在 K 中的根。

命题 5.5.3

对于 UFD $(R, +, \cdot)$, 其生成的分式域为 K , 对于多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$$

如果 $p/q \in K$ 为 $f(x)$ 在 K 中的根, 其中 $p, q \in R$ 且 $\gcd(p, q) = 1$, 那么在 R 中成立 $p \mid a_0$ 且 $q \mid a_n$ 。♠

证明 由命题条件

$$a_0 + a_1 \frac{p}{q} + \cdots + a_n \frac{p^n}{q^n} = 0$$

即

$$a_0q^n + a_1pq^{n-1} + \cdots + a_np^n = 0$$

因此

$$a_0q^n = -p(a_1q^{n-1} + \cdots + a_np^{n-1})$$

从而 $p \mid a_0q^n$, 由于 p 与 q 互素, 因此 $p \mid a_0$ 。同理可得 $q \mid a_n$ 。

5.5.2 代数闭域**定义 5.5.3** (域扩张)

对于域 k 与 K , 称 K/k 为域扩张, 如果存在同态映射 $\varphi: k \hookrightarrow K$ 。♣

命题 5.5.4

对于域 k 上的不可约多项式 $f(t) \in k[t]$, 令

$$F = \frac{k[t]}{(f(t))}$$

则成立如下命题。

1. F/k 为域扩张。
2. $f(x) \in k[x] \subset F[x]$ 在 F 中存在根。
3. 对于域扩张 K/k , 如果 $f(x) \in k[x] \subset K[x]$ 在 K 中存在根, 那么 K/F 为域扩张。

定义 5.5.4 (代数闭域 algebraically closed field)

称域 F 为代数闭域, 如果成立如下命题之一。

1. F 上的不可约多项式均为一次多项式。
2. F 上的非常多项式在 K 中存在根。
3. F 上的多项式可分解为一次因式的积。

定义 5.5.5 (代数闭包 algebraic closure)

定义域 F 的代数闭包为

$$\bar{F} = \bigcap_{\text{代数闭域 } K \supset F} K$$

命题 5.5.5

代数闭域存在无穷多元素。

证明 假设存在代数闭域 K , 使得成立 $K = \{a_1, \dots, a_n\}$, 考虑多项式

$$f(x) = (x - a_1) \cdots (x - a_n) + 1$$

显然 $f(x)$ 在 K 中不存在根, 因此矛盾!

5.5.3 $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x]$ 的可约性**定理 5.5.1 (代数基本定理 fundamental theorem of algebra)**

\mathbb{C} 为代数闭域。

证明 考虑 \mathbb{C} 上的 n 次多项式

$$f(z) = a_n z^n + \cdots + a_1 z + a_0, \quad z \in \mathbb{C}$$

假设 $f(z)$ 无根。由于

$$\frac{f(z)}{z^n} = a_n + \left(\frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n} \right) \rightarrow a_n \quad (|z| \rightarrow \infty)$$

那么存在 $r > 0$, 使得成立

$$|f(z)| \geq \frac{|a_n|}{2} |z|^n, \quad |z| > r$$

从而 $f(z)$ 在 $|z| > R$ 时存在下界。由于 P 为连续函数且无零点, 那么 $f(z)$ 在紧集 $|z| \leq r$ 上有界, 因此 $f(z)$ 在 \mathbb{C} 上存在下界, 进而 $1/f(z)$ 为有界整函数。由 Liouville 定理, $1/f(z)$ 为常函数, 即 $f(z)$ 为常函数, 矛盾! 因此 $P(z)$ 存在根, 进而 \mathbb{C} 为代数闭域。

命题 5.5.6 (虚根成对定理)

对于 \mathbb{R} 上的多项式 $f(x)$, 如果 $z \in \mathbb{C}$ 为 $f(x)$ 的根, 那么 \bar{z} 为 $f(x)$ 的根。



证明 这几乎是显然的:

$$f(\bar{z}) = \overline{f(z)} = 0$$

命题 5.5.7

\mathbb{R} 上的 ≥ 3 次多项式均在 \mathbb{R} 上可约。



证明 对于 \mathbb{R} 上的 ≥ 3 次多项式 $f(x)$, 由代数基本定理 5.5.1, $f(x)$ 在 \mathbb{C} 上至少存在 3 个根, 记其中一个根为 z 。

若 $z \in \mathbb{R}$, 则由命题 5.5.1, 存在非常多项式 $g(x) \in \mathbb{R}[x]$, 使得成立 $f(x) = (x - z)g(x)$ 。

若 $z \in \mathbb{C} \setminus \mathbb{R}$, 则由虚根成对定理 5.5.6, \bar{z} 为 $f(x)$ 的根, 进而由命题 5.5.1

$$(x - z)(x - \bar{z}) = (x^2 - (z + \bar{z})x + z\bar{z}) \mid f(x)$$

从而存在非常多项式 $h(x) \in \mathbb{R}[x]$, 使得成立 $f(x) = (x^2 - (z + \bar{z})x + z\bar{z})h(x)$ 。

命题 5.5.8

\mathbb{R} 上的奇次多项式均在 \mathbb{R} 上存在根。



证明 由代数基本定理 5.5.1 与虚根成对定理 5.5.6, 这是显然的!

命题 5.5.9

对于本原多项式 $f(x) \in \mathbb{Z}[x]$, 令 p 为素数, 如果 $f(x)$ 的最高次项系数 a_n 成立 $p \nmid a_n$, 且 $f(x)$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中不可约, 那么 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约。



证明 反证, 如果 $f(x)$ 在 \mathbb{Z} 中可约, 且 $\deg(f(x)) = n$, 那么存在 $g(x), h(x) \in \mathbb{Z}[x]$, 使得成立

$$f(x) = g(x)h(x), \quad \deg(g(x)) < \deg(f(x)), \quad \deg(h(x)) < \deg(f(x))$$

进而 $f(x)$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中可约, 矛盾!

命题 5.5.10

$\mathbb{Z}[x]$ 与 $\mathbb{Q}[x]$ 上存在任意次不可约多项式。



证明 考虑 n 次多项式 $p_n(x) = x^n + 2 \in \mathbb{Z}[x]$, 由 Eisenstein 判别法 5.5.2, $p_n(x)$ 在 $\mathbb{Z}[x]$ 中不可约。由引理 ??, $p_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约。

5.5.4 Eisenstein 判别法**定理 5.5.2 (Eisenstein 判别法)**

对于交换环 $(R, +, \cdot)$, 令 P 为 R 的素理想, 如果多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$$

成立

1. $a_n \notin P$
2. 对于任意 $0 \leq k \leq n-1$, 成立 $a_k \in P$;
3. $a_0 \notin P \cdot P$

那么 $f(x)$ 在 $R[x]$ 中不可约。



证明 反证, 如果 $f(x)$ 在 $R[x]$ 中可约, 那么存在 $g(x)h(x) \in R[x]$, 使得成立

$$f(x) = g(x)h(x), \quad \deg(g(x)) < \deg(f(x)), \quad \deg(h(x)) < \deg(f(x))$$

令

$$g(x) = b_0 + b_1x + \cdots + b_lx^l$$

$$h(x) = c_0 + c_1x + \cdots + c_mx^m$$

其中 $l + m = n$ 且 $l, m \in \mathbb{N}^*$, 因此

$$g(x)h(x) = \sum_{k=0}^n \sum_{i+j=k} (b_i \cdot c_j)x^k$$

对比同次项

$$\sum_{i+j=k} b_i \cdot c_j = a_k \in P, \quad 0 \leq k \leq n-1$$

由于

$$a_0 = b_0 \cdot c_0 \in P \implies b_0 \in P \text{ 或 } c_0 \in P$$

$$a_n = b_l \cdot c_m \notin P \implies b_l \notin P \text{ 且 } c_m \notin P$$

不妨 $b_0 \in P$, 记

$$b_0 \in P, \quad b_1 \in P, \quad \cdots \quad b_{r-1} \in P, \quad b_r \notin P$$

考虑

$$a_r = \sum_{i+j=r} b_i \cdot c_j \in P$$

因此 $b_r c_0 \in P$, 从而 $c_0 \in P$, 进而 $b_0 \cdot c_0 \in P \cdot P$, 矛盾!

5.6 Gauss 整数与 Fermat 平方和定理

5.6.1 Gauss 整数

定义 5.6.1 (Gauss 整数环 Gaussian integer ring)

定义 Gauss 整数环为

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$



定义 5.6.2 (范数 norm)

定义 Gauss 整数的范数为

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$$

$$a + bi \longmapsto a^2 + b^2$$



定理 5.6.1

Gauss 整环 $\mathbb{Z}[i]$ 为 Euclid 整环, 且其 Euclid 映射为 N 。



引理 5.6.1

$\mathbb{Z}[i]$ 的单位为 $\pm 1, \pm i$ 。



证明 如果 u 为 $\mathbb{Z}[i]$ 的单位, 那么存在 $v \in \mathbb{Z}[i]$, 使得成立 $uv = 1$, 因此

$$N(u)N(v) = N(uv) = 1$$

进而 $N(u) = 1$, 从而 $u = \pm 1, \pm i$ 。

引理 5.6.2

如果 $q \in \mathbb{Z}[i]$ 为素元, 那么存在素数 $p \in \mathbb{Z}$, 使得成立 $N(q) = p$ 或 $N(q) = p^2$ 。



证明 由引理 5.6.1, $N(q) \neq 1$, 因此 $N(q)$ 可分解为素数之积。而 q 为素元, 因此 $N(q)$ 存在素因子 $p \in \mathbb{Z}$, 使得成立 $q \mid p$, 从而 $N(q) \mid N(p) = p^2$ 。由于 $N(q) \neq 1$, 从而 $N(q) = p$ 或 $N(q) = p^2$ 。

5.6.2 Fermat 平方和定理

定义 5.6.3 (分裂 split)

称素数 $p \in \mathbb{N}^*$ 在 $\mathbb{Z}[i]$ 中分裂, 如果 p 在 $\mathbb{Z}[i]$ 中不为素元。



引理 5.6.3

对于素数 $p \in \mathbb{N}^*$, 成立

$$p \text{ 在 } \mathbb{Z}[i] \text{ 中分裂} \iff \exists a, b \in \mathbb{Z}, p = a^2 + b^2$$



证明 对于充分性, 如果存在 $a, b \in \mathbb{Z}$, 使得成立 $p = a^2 + b^2$, 因此存在 $z = a + bi, w = a - bi \in \mathbb{Z}[i]$, 使得成立 $p = zw$ 。若 z 或 w 为单位, 则由引理 5.6.1, $p = a^2 + b^2 = N(z) = N(w) = 1$, 矛盾! 因此 z, w 均不为单位, 从而 p 在 $\mathbb{Z}[i]$ 中可约。由引理 5.1.3, p 在 $\mathbb{Z}[i]$ 中不为素元。

对于必要性, 如果 p 在 $\mathbb{Z}[i]$ 中不为素元, 则由素元性条件 5.2.4, p 在 $\mathbb{Z}[i]$ 中可约, 从而存在不可约元 $q \in \mathbb{Z}[i]$, 使得成立 $q \mid p$, 从而 $N(q) \mid N(p) = p^2$, 从而 $N(q) = 1, p, p^2$ 。由于 q 不为单位, 则由引理 5.6.1, $N(q) \neq 1$ 。而显然 $N(q) \neq p^2$, 因此 $N(q) = p$ 。记 $q = a + bi$, 从而 $p = a^2 + b^2$ 。

引理 5.6.4

对于奇素数 $p \in \mathbb{N}^*$, 成立

$$p \text{ 在 } \mathbb{Z}[i] \text{ 中分裂} \iff \text{存在 } n \in \mathbb{Z} \text{ 使得成立 } n^2 \equiv -1 \pmod{p}$$



证明 断言成立同构

$$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[x]/(x^2 + 1)}{(p)} \cong \frac{\mathbb{Z}[x]}{(p, x^2 + 1)} \cong \frac{\mathbb{Z}[x]/(p)}{(x^2 + 1)} \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2 + 1)}$$

因此由引理 5.1.3、素元性条件 5.2.4、命题??与 5.5.2

$$\begin{aligned} p \text{ 在 } \mathbb{Z}[i] \text{ 中分裂} &\iff p \text{ 在 } \mathbb{Z}[i] \text{ 中不为素数} \\ &\iff \mathbb{Z}[i]/(p) \text{ 不为整环} \\ &\iff \mathbb{Z}/p\mathbb{Z}[x]/(x^2 + 1) \text{ 不为整环} \\ &\iff x^2 + 1 \text{ 在 } \mathbb{Z}/p\mathbb{Z}[x] \text{ 中不为素数} \\ &\iff x^2 + 1 \text{ 在 } \mathbb{Z}/p\mathbb{Z}[x] \text{ 中为可约元} \\ &\iff x^2 + 1 \text{ 在 } \mathbb{Z}/p\mathbb{Z} \text{ 中存在根} \\ &\iff \text{存在 } n \in \mathbb{Z} \text{ 使得成立 } n^2 \equiv -1 \pmod{p} \end{aligned}$$

引理 5.6.5

对于奇素数 $p \in \mathbb{N}^*$, 成立

$$\text{存在 } n \in \mathbb{Z} \text{ 使得成立 } n^2 \equiv -1 \pmod{p} \iff p \equiv 1 \pmod{4}$$



证明 由命题??, $\mathbb{Z}/p\mathbb{Z}$ 为域。取 $G = \mathbb{Z}/p\mathbb{Z}^\times$ 为乘法群, 由于域的乘法群的有限子群为循环群3.6.2, 那么 G 为循环群, 令 $G = \langle g \rangle$ 。由于 p 为奇数, 令 $p = 2l + 1$, 从而 $|G| = 2l$ 。对于任意 $n \in \mathbb{Z}$, 存在 $m \in \mathbb{N}$, 使得成立

$$n \equiv g^m \pmod{p}$$

由于 -1 张成了 G 的 2 阶子群 $\langle -1 \rangle$ 。而 g^l 亦张成了 G 的 2 阶子群 $\langle g^l \rangle$, 从而

$$g^l \equiv -1 \pmod{p}$$

从而对于 $n \equiv g^m \pmod{p}$, 成立

$$n^2 \equiv -1 \pmod{p} \iff g^{2m} = g^l \iff 2m \equiv l \pmod{2l}$$

综上所述

$$\begin{aligned} \text{存在 } n \in \mathbb{Z} \text{ 使得成立 } n^2 \equiv -1 \pmod{p} &\iff \text{存在 } m \in \mathbb{Z} \text{ 使得成立 } 2m \equiv l \pmod{2l} \\ &\iff 2 \mid l \\ &\iff p \equiv 1 \pmod{4} \end{aligned}$$

定理 5.6.2 (Fermat 平方和定理)

对于奇素数 $p \in \mathbb{N}^*$, 成立

$$\exists a, b \in \mathbb{Z}, p = a^2 + b^2 \iff p \equiv 1 \pmod{4}$$



证明 由引理5.6.3、5.6.4与5.6.5, 命题得证!

第六章 域论

6.1 域扩张 I

6.1.1 基本定义

6.1.1.1 域扩张

定义 6.1.1 (Fld 范畴)

1. 对象: $\text{Obj}(\text{Fld}) = \{\text{域 } F\}$
2. 态射: $\text{Hom}_{\text{Fld}}(F, K) = \{\text{环同态映射 } \varphi: F \rightarrow K\}$



定义 6.1.2 (域扩张 field extension)

对于域 k 与 K , 称 K/k 为域扩张, 如果存在同态映射 $\varphi: k \rightarrow K$.



定义 6.1.3 (扩域 extend field)

对于域扩张 K/k , 称 K 为 k 的扩域。



定义 6.1.4 (子域 subfield)

对于域扩张 K/k , 称 k 为 K 的子域。



定义 6.1.5 (中间域 intermediate field)

对于域扩张 $k \subset F \subset K$, 称 F 为 K/k 的中间域。



命题 6.1.1

对于域扩张 K/k , 其同态映射 $\varphi: k \hookrightarrow K$ 为单射。



证明 由命题4.1.1, 命题得证!

6.1.1.2 域的特征

定义 6.1.6 (特征 characteristic)

1. 对于域 F , 存在且存在唯一同态映射

$$\begin{aligned}\varphi: \mathbb{Z} &\longrightarrow F \\ n &\longmapsto n1_F\end{aligned}$$

令 $\ker \varphi = p\mathbb{Z}$, 定义域 F 的特征为 $\text{char}(F) = p$ 。

2. 定义域 F 的特征为乘法单位元 1 在加法群 $(F, +)$ 中的阶, 并记作 $\text{char}(F)$; 特别的, 如果乘法单位元 1 在加法群 $(F, +)$ 中的阶为 ∞ , 那么 $\text{char}(F) = 0$ 。
3. 定义域 F 的特征为

$$\text{char}(F) = \begin{cases} \min\{n \in \mathbb{N}^* : nx = 0, \forall x \in F\}, & \exists n \in \mathbb{N}^*, \forall x \in F, nx = 0 \\ 0, & \forall n \in \mathbb{N}^*, \exists x \in F, nx \neq 0 \end{cases}$$



命题 6.1.2 (域的特征为零或素数)

对域 K , 或 $\text{char}(F) = 0$, 或 $\text{char}(F)$ 为素数。

证明 如果域 F 的特征 $p = \text{char}(F)$ 成立 $p \neq 0$ 且 p 不为素数, 那么存在 $m, n \geq 2$, 使得成立 $p = mn$ 。而

$$0 = p1_F = (mn)1_F = (m1_F) \cdot (n1_F)$$

由消去律, $m1_F = 0$ 或 $n1_F = 0$, 矛盾!

命题 6.1.3

对于域扩张 K/k , 成立 $\text{char}(k) = \text{char}(K)$ 。

证明 对于同态映射

$$i: k \hookrightarrow K, \quad \varphi: \mathbb{Z} \rightarrow k, \quad \psi: \mathbb{Z} \rightarrow K$$

其中 $\psi = i \circ \varphi$, 考察其核, 由命题 4.2.17

$$\begin{aligned} n \in \ker \psi &\iff \psi(n) = 0_K \\ &\iff (i \circ \varphi)(n) = 0_K \\ &\iff i(\varphi(n)) = 0_K \\ &\iff \varphi(n) = n_k \\ &\iff n \in \ker \varphi \end{aligned}$$

因此 $\ker \varphi = \ker \psi$, 进而 $\text{char}(k) = \text{char}(K)$ 。

定义 6.1.7 (\mathbf{Fld}_0 范畴)

1. 对象: $\text{Obj}(\mathbf{Fld}) = \{\text{域 } F : \text{char}(F) = 0\}$
2. 态射: $\text{Hom}_{\mathbf{Fld}}(F, K) = \{\text{环同态映射 } \varphi: F \rightarrow K\}$

定义 6.1.8 (\mathbf{Fld}_p 范畴)

1. 对象: $\text{Obj}(\mathbf{Fld}) = \{\text{域 } F : \text{char}(F) = p\}$
2. 态射: $\text{Hom}_{\mathbf{Fld}}(F, K) = \{\text{环同态映射 } \varphi: F \rightarrow K\}$

命题 6.1.4 (\mathbf{Fld}_0 的初始对象)

\mathbf{Fld}_0 的初始对象为 \mathbb{Q} ; 换言之, 对于任意特征为 0 的域 F , 存在且存在唯一同态映射 $\varphi: \mathbb{Q} \hookrightarrow F$ 。

命题 6.1.5 (\mathbf{Fld}_p 的初始对象)

\mathbf{Fld}_p 的初始对象为 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; 换言之, 对于任意特征为 p 的域 F , 存在且存在唯一同态映射 $\varphi: \mathbb{F}_p \hookrightarrow F$ 。

6.1.2 单扩张

6.1.2.1 单扩张结构

定义 6.1.9 (生成域)

对于域扩张 K/k , 定义域 k 关于集合 $S \subset K$ 的生成域为

$$k(S) = \bigcap_{F \supset k \cup S \text{ 为域}} F$$



定义 6.1.10 (有理多项式域)

对于域 F , 定义其有理多项式域为由多项式整环 $F[x]$ 生成的分式域, 即

$$F(x) = \left\{ \frac{\sum_{k=0}^n a_k x^k}{\sum_{k=0}^m b_k x^k} : a_k, b_k \in F, m, n \in \mathbb{N} \right\}$$



定义 6.1.11 (单扩张 simple extension)

称域扩张 K/k 为单扩张, 如果存在 $\alpha \in K$, 使得成立 $K = k(\alpha)$ 。



定义 6.1.12 (极小多项式 minimal polynomial)

对于域扩张 K/k , 称 k 的代数元 α 的极小多项式为 $p(x) \in k[x]$, 如果 $p(\alpha) = 0$, 且 $p(x)$ 为在 $k[x]$ 中不可约的首一多项式。



引理 6.1.1

对于域扩张 $k \subset K \subset F$, 令 $p(x) \in k[x]$ 为 $\alpha \in F$ 在 k 上的极小多项式, 令 $P(x) \in K[x]$ 为 α 在 K 上的极小多项式, 那么 $P(x) \mid p(x)$ 。



定理 6.1.1 (单扩张结构)

对于域扩张 K/k , 考虑 $\alpha \in K$ 生成的单扩张 $k(\alpha)/k$, 令映射

$$\begin{aligned} \varphi: k[t] &\longrightarrow k(\alpha) \\ f(t) &\longmapsto f(\alpha) \end{aligned}$$

那么成立如下命题。

1. φ 为单射 $\iff \ker \varphi = \{0\} \iff [k(\alpha) : k] = \infty$
2. 当 φ 为单射时, $k(t) \cong k(\alpha)$ 。
3. 当 φ 不为单射时, 令 $p(t)$ 为 α 的极小多项式, 则 $\deg(p(x)) = [k(\alpha) : k]$, 且 $k[t]/(p(t)) \cong k(\alpha)$ 。



证明 由命题 4.2.17

$$\varphi \text{ 为单射} \iff \ker \varphi = \{0\}$$

如果 $\ker \varphi = \{0\}$, 那么 φ 为单射。由命题 4.1.26, $k[t]$ 为整环。由分式域的万有性质 5.4.5, 存在且存在唯一

同态映射 $\psi: k(t) \rightarrow k(\alpha)$, 使得成立

$$\begin{array}{ccc} k(t) & \xrightarrow{\psi} & k(\alpha) \\ & \swarrow i \quad \searrow \varphi & \\ & k[t] & \end{array}$$

因此 $\varphi: k[t] \rightarrow k(\alpha)$ 诱导同态映射

$$\begin{aligned} \psi: k(t) &\longrightarrow k(\alpha) \\ f(t) &\longmapsto f(\alpha) \end{aligned}$$

由命题 4.1.1, ψ 为单射。由第一同构定理 4.3.4, $k(t) \cong \text{im } \psi$, 因此 $\text{im } \psi$ 为包含 k 与 α 的最小域, 那么 $\text{im } \psi = k(\alpha)$, 进而 $k(t) \cong k(\alpha)$ 。

由于 $\{t^i\}_{i=1}^{\infty}$ 在 $k(t)$ 中线性无关, 那么 $\{\alpha^i\}_{i=1}^{\infty}$ 在 $k(\alpha)$ 中线性无关, 进而 $[k(\alpha):k] = \infty$ 。

如果 $\ker \varphi \neq \{0\}$, 那么由命题 4.2.17, φ 不为单射。由命题 4.4.2, 存在且存在唯一不可约的首一多项式 $p(t) \in k[t]$, 使得成立 $\ker \varphi = (p(t))$ 。由第一同构定理 4.3.4, $k[t]/(p(t)) \cong \text{im } \varphi$ 。由命题 4.2.6, $\text{im } \varphi$ 为 $k(\alpha)$ 的子环。由命题 4.1.4, $\text{im } \varphi$ 为整环, 因此 $k[t]/(p(t))$ 为整环, 进而 $(p(t))$ 为 $k[t]$ 的素理想。由命题 4.4.7, $(p(t))$ 为 $k[t]$ 的极大理想, 因此 $k[t]/(p(t))$ 为域, 进而 $\text{im } \varphi$ 为 $k(\alpha)$ 的子域。而 $k \cup \{\alpha\} \subset \text{im } \varphi$, 因此 $\text{im } \varphi = k(\alpha)$, 进而 $k[t]/(p(t)) \cong k(\alpha)$ 。

而 $\varphi(t) = \alpha$, 且

$$p(t + (p(t))) = p(t) + (p(t)) = (p(t))$$

因此 $p(\alpha) = 0$, 进而 $p(t)$ 为 α 的极小多项式。

例题 6.1

$$\begin{aligned} \mathbb{Q}(\sqrt{2}) &= \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \\ \frac{\mathbb{Q}[x]}{(x^2 - 2)} &= \{a + bx + (x^2 - 2) : a, b \in \mathbb{Q}\} \end{aligned}$$

例题 6.2

$$\begin{aligned} \mathbb{Q}(\sqrt{3}) &= \{a + b\sqrt{3} : a, b \in \mathbb{Q}\} \\ \frac{\mathbb{Q}[x]}{(x^2 - 3)} &= \{a + bx + (x^2 - 3) : a, b \in \mathbb{Q}\} \end{aligned}$$

推论 6.1.1 (单扩张的基)

1. 对于单扩张 $k(\alpha)/k$, 若 $[k(\alpha):k] = \infty$, 则 $\{\alpha^i\}_{i=0}^{\infty}$ 为域 k 上的向量空间 $k(\alpha)$ 的基, 此时

$$k(\alpha) = \left\{ \sum_{i=0}^{\infty} a_i \alpha^i : a_i \in k, i \in \mathbb{N} \right\}$$

2. 对于单扩张 $k(\alpha)/k$, 若 $[k(\alpha):k] = n$, 则 $\{\alpha^i\}_{i=0}^{n-1}$ 为域 k 上的向量空间 $k(\alpha)$ 的基, 此时

$$k(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i : a_i \in k, 0 \leq i \leq n-1 \right\}$$

命题 6.1.6 (单扩张间的同构映射的延拓)

对于单扩张 $k_1(\alpha_1)/k_1$ 与 $k_2(\alpha_2)/k_2$, 令 $p_1(t) \in k_1[t]$ 与 $p_2(t) \in k_2[t]$ 分别为 α_1 与 α_2 的极小多项式, 如果同构映射 $i: k_1 \rightarrow k_2$ 成立

$$i(p_1(t)) = p_2(t)$$

那么存在且存在唯一同构映射 $j: k_1(\alpha_1) \rightarrow k_2(\alpha_2)$, 使得成立 $j|_{k_1} = i$, 且 $j(\alpha_1) = \alpha_2$ 。

证明 对于存在性, 由于同构映射 $i: k_1 \rightarrow k_2$ 成 $i(p_1(t)) = p_2(t)$, 那么其诱导同构映射

$$\frac{k_1[t]}{(p_1(t))} \xrightarrow{\sim} \frac{k_2[t]}{(p_2(t))}$$

由单扩张结构 6.1.1, 给出

$$j: k_1(\alpha_1) \xrightarrow{\sim} \frac{k_1[t]}{(p_1(t))} \xrightarrow{\sim} \frac{k_2[t]}{(p_2(t))} \xrightarrow{\sim} k_2(\alpha_2)$$

对于唯一性, 如果存在同构映射 $j': k_1(\alpha_1) \rightarrow k_2(\alpha_2)$, 使得成立 $j'_{k_1} = i$, 且 $j'(\alpha_1) = \alpha_2$, 那么由单扩张的基 6.1.1, 令 $n = \deg(p_1(t))$, 则

$$k(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i : a_i \in k, 0 \leq i \leq n-1 \right\}$$

由于

$$j' \left(\sum_{i=0}^{n-1} a_i \alpha_1^i \right) = \sum_{i=0}^{n-1} j'(a_i) j'(\alpha_1)^i = \sum_{i=0}^{n-1} j(a_i) \alpha_2^i = \sum_{i=0}^{n-1} j(a_i) j(\alpha_1)^i = j \left(\sum_{i=0}^{n-1} a_i \alpha_1^i \right)$$

因此 $j' = j$ 。

推论 6.1.2

对于单扩张 $k_1(\alpha_1)/k_1$ 与 $k_2(\alpha_2)/k_2$, 如果同构映射 $i: k_1 \rightarrow k_2$ 保持极小多项式, 那么 i 可唯一延拓为同构映射 $j: k_1(\alpha_1) \rightarrow k_2(\alpha_2)$, 且保持代数元。换言之

$$\begin{array}{ccc} k_1(\alpha_1) & \xrightarrow[\sim]{j} & k_2(\alpha_2) \\ \uparrow & & \uparrow \\ k_1 & \xrightarrow[\sim]{i} & k_2 \end{array}$$



6.1.2.2 k -自同构映射群

定义 6.1.13 (k -同态映射)

对于域扩张 K/k 与 F/k , 称同态映射 $\varphi: K \rightarrow F$ 为 k -同态映射, 如果 $\varphi|_k = \mathbb{1}_k$ 。



定义 6.1.14 (k -同构映射)

对于域扩张 K/k 与 F/k , 称同构映射 $\varphi: K \rightarrow F$ 为 k -同构映射, 如果 $\varphi|_k = \mathbb{1}_k$ 。



定义 6.1.15 (k -自同构映射)

对于域扩张 K/k , 称同构映射 $\varphi: K \rightarrow K$ 为 k -自同构映射, 如果 $\varphi|_k = \mathbb{1}_k$ 。



定义 6.1.16 (k -自同构映射群)

对于域扩张 K/k , k -自同构映射 $\varphi: K \rightarrow K$ 全体依映射复合运算构成 k -自同构映射群, 记作 $\text{Aut}_k(K)$ 。



命题 6.1.7

对于单扩张 $k(\alpha)/k$, 如果 $p(x) \in k[x]$ 为 α 的极小多项式, 令 $\text{Root}_p = \{x \in k(\alpha) : p(x) = 0\}$, 那么成立等式

$$|\text{Aut}_k(k(\alpha))| = |\text{Root}_p|$$

特别的, 成立不等式

$$|\mathrm{Aut}_k(k(\alpha))| \leq [k(\alpha) : k]$$

当且仅当 $p(x)$ 可在 $k(\alpha)$ 中分解为一次因式之积时等号成立。

证明 作映射

$$\begin{aligned} \mathcal{F} : \mathrm{Aut}_k(k(\alpha)) &\longrightarrow \mathrm{Root}_p \\ \varphi &\longmapsto \varphi(\alpha) \end{aligned}$$

首先我们证明映射的定义良好性

$$p(\varphi(\alpha)) = \varphi(p(\alpha)) = \varphi(0) = 0$$

其次我们证明 \mathcal{F} 为单射, 任取 $\varphi, \psi \in \mathcal{F}$, 使得成立 $\varphi(\alpha) = \psi(\alpha)$ 。由单扩张的基 6.1.1, 令 $n = \deg(p(t))$, 则

$$k(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i : a_i \in k, 0 \leq i \leq n-1 \right\}$$

由于

$$\varphi \left(\sum_{i=0}^{n-1} a_i \alpha^i \right) = \sum_{i=0}^{n-1} \varphi(a_i) \varphi(\alpha)^i = \sum_{i=0}^{n-1} a_i \varphi(\alpha)^i = \sum_{i=0}^{n-1} a_i \psi(\alpha)^i = \sum_{i=0}^{n-1} \psi(a_i) \psi(\alpha)^i = \psi \left(\sum_{i=0}^{n-1} a_i \alpha^i \right)$$

因此 $\varphi = \psi$ 。由 φ, ψ 的任意性, \mathcal{F} 为单射。

最后我们证明 \mathcal{F} 为满射, 任取 $\beta \in \mathrm{Root}_p$, 那么 $p(x)$ 为 β 的极小多项式。由命题 6.1.6, 存在同构映射 $\varphi : k(\alpha) \rightarrow k(\beta)$, 使得成立 $\varphi|_k = \mathbb{1}_k$, 且 $\varphi(\alpha) = \beta$ 。由单扩张结构 6.1.1

$$k(\alpha) \cong \frac{k[x]}{(p(x))} \cong k(\beta)$$

因此 $\varphi \in \mathrm{Aut}_k(k(\alpha))$, 进而 $\mathcal{F}(\varphi) = \beta$ 。由 β 的任意性, \mathcal{F} 为满射。

综合以上三点, 成立等式

$$|\mathrm{Aut}_k(k(\alpha))| = |\mathrm{Root}_p|$$

由定理 6.1.1 与引理 5.5.1

$$|\mathrm{Aut}_k(k(\alpha))| = |\mathrm{Root}_p| \leq \dim(p(x)) = [k(\alpha) : k]$$

显然当且仅当 $p(x)$ 可在 $k(\alpha)$ 中分解为一次因式之积时等号成立。

6.1.3 有限扩张与代数扩张

6.1.3.1 有限扩张

定义 6.1.17 (向量空间 vector space)

称 $(V, +, \cdot)$ 为域 F 上的向量空间, 如果加法运算 $+: V \times V \rightarrow V$ 与数乘运算 $\cdot: F \times V \rightarrow V$ 成立如下性质。

1. 加法单位元: 存在 $0 \in V$, 使得对于任意 $x \in V$, 成立 $0 + x = x + 0 = x$ 。
2. 数乘单位元: 存在 $1 \in F$, 使得对于任意 $x \in V$, 成立 $1 \cdot x = x$ 。
3. 加法逆元: 对于任意 $x \in V$, 存在 $y \in V$, 使得成立 $x + y = y + x = 0$ 。
4. 加法交换律: $x + y = y + x$
5. 加法结合律: $x + (y + z) = (x + y) + z$
6. 数乘结合律: $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$

7. 数乘左分配律: $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$

8. 数乘右分配律: $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$



定义 6.1.18 (域扩张的向量空间性)

对于域扩张 K/k , 可将 K 看作 k 上的向量空间。



定义 6.1.19 (扩张次数 degree of extension)

对于域扩张 K/k , 将 K 看作 k 上的向量空间, 定义域扩张的次数为 $[K : k] = \dim(K)$ 。



定义 6.1.20 (有限扩张 finite extension)

称域扩张 K/k 为 n 次扩张, 如果 $[K : k] = n$ 。



引理 6.1.2

对于域扩张 $k \subset K \subset F$, 成立 $[F : k] \geq [K : k]$ 。



证明 若 $[F : k] = \infty$, 则命题显然成立。若 $[F : k] < \infty$, 则由望远镜定理 6.1.8

$$[F : k] = [F : K][K : k] \geq [K : k]$$

引理 6.1.3

对于域扩张 $k \subset K \subset F$, 成立 $[F : k] \geq [F : K]$ 。



证明 若 $[F : k] = \infty$, 则命题显然成立。若 $[F : k] < \infty$, 则由望远镜定理 6.1.8

$$[F : k] = [F : K][K : k] \geq [F : K]$$

引理 6.1.4

对于域扩张 $k \subset K \subset F$, 令 $\alpha \in F$, 则 $[k(\alpha) : k] \geq [K(\alpha) : K]$ 。



证明 若 $[k(\alpha) : k] = \infty$, 则命题显然成立。若 $[k(\alpha) : k] < \infty$, 则 α 为 k 上的代数元。令 $p(x) \in k[x]$ 为 α 在 k 上的极小多项式。那么将 $p(x)$ 看作 $K[x]$ 中的多项式, 从而 α 为 K 上的代数元。令 $P(x) \in K[x]$ 为 α 在 K 上的极小多项式, 由引理 6.1.1, $P(x) \mid p(x)$, 从而 $\deg(P(x)) \leq \deg(p(x))$ 。由定理 6.1.1

$$[k(\alpha) : k] = \deg(p(x)) \geq \deg(P(x)) = [K(\alpha) : K]$$

6.1.3.2 代数扩张

定义 6.1.21 (代数元 algebraic element)

对于域扩张 K/k , 称 $\alpha \in K$ 为 k 的代数元, 如果成立如下命题之一。

1. $[k(\alpha) : k] < \infty$
2. 存在非常多项式 $f(x) \in k[x]$, 使得成立 $f(\alpha) = 0$ 。



定义 6.1.22 (超越元 transcendental element)

对于域扩张 K/k , 称 $\alpha \in K$ 为 k 的超越元, 如果成立如下命题之一。

1. $[k(\alpha) : k] = \infty$
2. 对于任意非常多项式 $f(x) \in k[x]$, 成立 $f(\alpha) \neq 0$ 。



定义 6.1.23 (代数扩张 algebraic extension)

称域扩张 K/k 为代数扩张, 如果对于任意 $\alpha \in K$, α 为 k 的代数元。

**引理 6.1.5 (有限扩张 \implies 代数扩张)**

如果域扩张 K/k 为有限扩张, 那么 K/k 为代数扩张, 且对于任意 $\alpha \in K$, 成立 $[k(\alpha):k] \leq [K:k]$ 。



证明 由于对于任意 $\alpha \in K$, 成立 $k \subset k(\alpha) \subset K$, 那么 $[k(\alpha):k] \leq [K:k]$, 因此 K/k 为代数扩张。

引理 6.1.6 (单扩张时, 有限扩张 \iff 代数扩张)

对于单扩张 $k(\alpha)/k$, 成立

$$k(\alpha)/k \text{ 为有限扩张} \iff k(\alpha)/k \text{ 为代数扩张}$$



证明 一方面, 由引理 6.1.5, 若 $k(\alpha)/k$ 为有限扩张, 则 $k(\alpha)/k$ 为代数扩张。

另一方面, 若 $k(\alpha)/k$ 为代数扩张, 则 α 为代数元, 因此 $[k(\alpha):k] < \infty$, 进而 $k(\alpha)/k$ 为有限扩张。

命题 6.1.8 (望远镜定理)

对于域 $F \subset L \subset K$, 成立

$$[K:F] < \infty \iff [K:L] < \infty \text{ 且 } [L:F] < \infty$$

此时成立

$$[K:F] = [K:L][L:F]$$



证明 对于必要性, 如果 $[K:F] = n$, 那么由于 L 为 K 的子空间, 因此 $[L:F] \leq n$ 。设 $\{\alpha_k\}_{k=1}^n$ 为向量空间 K/F 的基, 那么对于任意 $\beta \in K$, 存在且存在唯一 $\{b_k\}_{k=1}^n \subset F$, 使得成立

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n$$

由于 $F \subset L$, 那么 $\{b_k\}_{k=1}^n \subset L$, 从而 $\{\alpha_k\}_{k=1}^n$ 为向量空间 K/L 的生成元, 因此 $[K:L] \leq n$ 。

对于充分性, 如果 $[K:L] = m$, $[L:F] = n$, 且 $\{\beta_k\}_{k=1}^m$ 为向量空间 K/L 的基, $\{\gamma_k\}_{k=1}^n$ 为向量空间 L/F 的基。对于任意 $\alpha \in K$, 存在且存在唯一 $\{a_k\}_{k=1}^m \subset L$, 且存在且存在唯一 $\{b_{ij}\}_{m \times n} \subset F$, 使得成立

$$\alpha = a_1\beta_1 + \cdots + a_m\beta_m, \quad a_i = b_{i1}\gamma_1 + \cdots + b_{in}\gamma_n$$

从而

$$\alpha = \sum_{i,j} b_{ij}(\gamma_j\beta_i)$$

由于

$$\{\gamma_j\beta_i : 1 \leq i \leq m, 1 \leq j \leq n\} \subset K$$

在 F 上线性无关, 那么其为 K/F 的基, 因此

$$[K:F] = mn = [K:L][L:F]$$

6.1.3.3 有限生成域**定义 6.1.24 (有限生成域)**

对于域扩张 K/k , 称 K 关于 k 为有限生成域, 如果存在 $\alpha_1, \dots, \alpha_n \in K$, 使得成立

$$K = k(\alpha_1, \dots, \alpha_n)$$



引理 6.1.7

对于域扩张 K/k , 则令 $\alpha, \beta \in K$, 成立

$$k(\alpha)(\beta) = k(\alpha, \beta)$$

**命题 6.1.9**

对于域扩张 K/k , 其中 $K = k(\alpha_1, \dots, \alpha_n)$ 为有限生成域, 那么如下命题等价。

1. K/k 为有限扩张。
2. K/k 为代数扩张。
3. 对于任意 $1 \leq i \leq n$, α_i 为 k 的代数元。

此时

$$[K : k] \leq \prod_{i=1}^n [k(\alpha_i) : k]$$



证明 由引理 6.1.5, 可知 $1 \implies 2$ 。由代数扩张 6.1.23, 可知 $2 \implies 3$ 。

下面证明 $3 \implies 1$ 。由于对于任意 $1 \leq i \leq n$, α_i 为 k 的代数元, 那么由引理 6.1.6 与 6.1.7

$$k(\alpha_1, \dots, \alpha_{i+1})/k(\alpha_1, \dots, \alpha_i) = k(\alpha_1, \dots, \alpha_i)(\alpha_{i+1})/k(\alpha_1, \dots, \alpha_i)$$

为有限扩张, 且由引理 6.1.4

$$[k(\alpha_1, \dots, \alpha_{i+1}) : k(\alpha_1, \dots, \alpha_i)] \leq [k(\alpha_{i+1}) : k]$$

由望远镜定理 6.1.8

$$[K : k] \leq \prod_{i=1}^n [k(\alpha_i) : k]$$

因此 K/k 为有限扩张。

推论 6.1.3

对于域扩张 K/k , 令

$$A = \{\alpha \in K : \alpha \text{ 为代数元}\}$$

则 A 为域。

**推论 6.1.4**

对于域扩张 $k \subset K \subset F$, 成立

$$F/k \text{ 为代数扩张} \iff K/k \text{ 与 } F/K \text{ 均为代数扩张}$$



证明 对于必要性, 如果 F/k 为代数扩张, 那么对于任意 $\alpha \in F$, 成立 $[k(\alpha) : k] < \infty$ 。而 $K \subset F$, 因此 K/k 为代数扩张。由引理 6.1.4, $[K(\alpha) : K] \leq [k(\alpha) : k] < \infty$, 从而 F/K 为代数扩张。

对于充分性, 如果 K/k 与 F/K 均为代数扩张, 那么任取 $\alpha \in F$, 令多项式 $p(x) \in K[x]$ 为 α 在 K 上的极小多项式, $S \subset K$ 为 $p(x)$ 的系数全体, 因此 α 为 $k(S) \subset K$ 上的代数元, 因此由定理 6.1.1 与引理 6.1.7 及 6.1.4

$$[k(S, \alpha) : k(S)] = [k(S)(\alpha) : k(S)] \leq [K(\alpha) : K] \leq n$$

从而 $k(S, \alpha)/k(S)$ 为有限扩张。由于 K/k 为代数扩张, 因此 $k(S)/k$ 为代数扩张, 那么由命题 6.1.9, $k(S)/k$ 为有限扩张。由望远镜定理 6.1.8

$$[k(S, \alpha) : k] = [k(S)(\alpha) : k(S)][k(S) : k] < \infty$$

因此 $k(S, \alpha)/k$ 为有限扩张。由引理 6.1.5

$$[k(\alpha) : k] \leq [k(S, \alpha) : k] < \infty$$

因此 α 为 k 上的代数元。由 α 的任意性, F/k 为代数扩张。

定义 6.1.25 (代数数)

对于域扩张 \mathbb{C}/\mathbb{Q} , 定义代数数为

$$\overline{\mathbb{Q}} = \{x \in \mathbb{C} : x \text{ 为代数数}\} = \bigcap_{\text{代数闭域 } F \supset \mathbb{Q}} F$$

命题 6.1.10

域扩张 $\overline{\mathbb{Q}}/\mathbb{Q}$ 为代数扩张, 但非有限扩张。

证明 由代数数 6.1.25, $\overline{\mathbb{Q}}/\mathbb{Q}$ 为代数扩张。由命题 5.5.10, $\mathbb{Q}[x]$ 上存在任意次不可约多项式, 进而 $\overline{\mathbb{Q}}/\mathbb{Q}$ 不为有限扩张。

例题 6.3

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$$

证明 由于 $[\mathbb{Q}(\sqrt{2} : \mathbb{Q})] = [\mathbb{Q}(\sqrt{3} : \mathbb{Q})] = 2$, 因此由命题 6.1.9, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq 4$ 。

由于 $\sqrt{2} + \sqrt{3}$ 在 \mathbb{Q} 中的极小多项式为 $p(x) = x^4 - 10x^2 + 1$, 因此 $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$ 。

而 $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$, 从而 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, 因此 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ 。由命题 6.1.1

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \{a + b(\sqrt{2} + \sqrt{3}) + c(\sqrt{2} + \sqrt{3})^2 + d(\sqrt{2} + \sqrt{3})^3 : a, b, c, d \in \mathbb{Q}\} = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$$

6.2 代数闭包与 Nullstellensatz

6.2.1 代数闭包

定义 6.2.1 (代数闭域 algebraically closed field)

称域 K 为代数闭域, 如果成立如下命题之一。

1. K 上的不可约多项式均为一次多项式。
2. K 上的非常多项式在 K 中存在根。
3. K 上的多项式可分解为一次因式的积。
4. K 不存在非平凡代数扩张。
5. 对于域扩张 F/K , 如果 $\alpha \in F$ 为 K 的代数元, 那么 $\alpha \in K$ 。

定义 6.2.2 (代数闭包 algebraic closure)

1. 称域 k 的代数闭包为代数闭域 \bar{k} , 如果域扩张 \bar{k}/k 为代数扩张。
2. 定义域 k 的代数闭包为

$$\bar{k} = \bigcap_{\text{代数闭域 } K \supset k} K$$

引理 6.2.1

对于域 k , 存在域扩张 K/k , 使得对于任意非常多项式 $f(x) \in k[x]$, 存在 $\alpha \in K$, 使得成立 $f(\alpha) = 0$ 。

引理 6.2.2

对于域扩张 K/k , 如果对于任意非常多项式 $f(x) \in k[x]$, 存在 $\alpha \in K$, 使得成立 $f(\alpha) = 0$, 那么构造

$$F = \bigcup_{f(x) \in k[x]} \{\alpha \in K : f(\alpha) = 0\}$$

则 F 为代数闭域。

**引理 6.2.3**

对于域扩张 K/k , 如果 K 为代数闭域, 那么构造

$$\bar{k} = \{\alpha \in K : \alpha \text{ 为 } k \text{ 的代数元}\}$$

则 \bar{k} 为 k 的代数闭包。

**引理 6.2.4**

对于域扩张 K/k , 如果 K 为代数闭域, 那么对于任意代数扩张 F/k , 存在同态映射 $i: F \rightarrow K$ 。

**定理 6.2.1 (代数闭包的存在唯一性)**

域 k 存在且存在唯一代数闭包 \bar{k} 。

**6.2.2 Hilbert's Nullstellensatz****定理 6.2.2 (Hilbert's Nullstellensatz)**

Let K/k be a field extension, and assume that K is a finite-type K -algebra. Then K/k is a finite extension.

**推论 6.2.1**

如果 K 为代数闭域, 那么对于 $K[x]$ 的任意极大理想 $M \subset K$, 存在 $c \in K$, 使得成立 $M = (x - c)$ 。

**推论 6.2.2**

如果 K 为代数闭域, 那么对于 $K[x_1, \dots, x_n]$ 的理想 I , 成立: I 为极大理想 \iff 存在 $c_1, \dots, c_n \in K$, 使得成立 $I = (x_1 - c_1, \dots, x_n - c_n)$ 。

**6.2.3 一点点代数几何****定义 6.2.3 (仿射空间 affine space)**

定义域 K 上的 n 次仿射空间为

$$\mathbb{A}_K^n = \{(c_1, \dots, c_n) : c_k \in K, 1 \leq k \leq n\}$$

**定义 6.2.4**

对于子集 $S \subset \mathbb{A}_K^n$, 定义 $K[x_1, \dots, x_n]$ 的理想

$$\mathcal{I}(S) = \{f \in K[x_1, \dots, x_n] : \forall p \in S, f(p) = 0\}$$

对于 $K[x_1, \dots, x_n]$ 的理想 I , 定义 \mathbb{A}_K^n 的子集

$$\mathcal{V}(I) = \{p \in \mathbb{A}_K^n : \forall f \in I, f(p) = 0\}$$



定义 6.2.5 (仿射代数集 affine algebraic set)

称子集 $S \subset \mathbb{A}_K^n$ 为仿射代数集, 如果存在 $K[x_1, \dots, x_n]$ 的理想 I , 使得成立 $S = \mathcal{V}(I)$ 。

**定义 6.2.6 (根 radical)**

对于交换环 $(R, +, \cdot)$ 的理想 I , 定义 I 的根为理想

$$\begin{aligned}\sqrt{I} &= \{r \in R : \exists n \in \mathbb{N}, r^n \in I\} \\ &= \bigcap_{P \supset I \text{ 为素理想}} P\end{aligned}$$

**定义 6.2.7 (根理想 radical ideal)**

对于交换环 $(R, +, \cdot)$ 的理想 I , 称 I 为根理想, 如果 $I = \sqrt{I}$ 。

**引理 6.2.5**

对于子集 $S \subset \mathbb{A}_K^n$, $\mathcal{I}(S)$ 为 $K[x_1, \dots, x_n]$ 的根理想。

**定理 6.2.3 (Weak Nullstellensatz)**

对于代数闭域 K , 如果 I 为 $K[x_1, \dots, x_n]$ 的理想, 那么

$$\mathcal{V}(I) = \emptyset \iff I = (1)$$

**定理 6.2.4 (Strong Nullstellensatz)**

对于代数闭域 K , 如果 I 为 $K[x_1, \dots, x_n]$ 的理想, 那么

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$$

**推论 6.2.3**

对于代数闭域 K , 双向映射

$$\{\mathbb{A}_K^n \text{ 的仿射代数子集}\} \xrightleftharpoons[\mathcal{V}]{\mathcal{I}} \{K[x_1, \dots, x_n] \text{ 的根理想}\}$$

互为逆映射。

**定义 6.2.8 (坐标环 coordinate ring)**

定义仿射代数子集 $S \subset \mathbb{A}_K^n$ 的坐标环为

$$K[S] = \frac{K[x_1, \dots, x_n]}{\mathcal{I}(S)}$$



6.3 尺规作图

6.3.1 尺规作图

定义 6.3.1 (尺规作图 constructions by straightedge and compass)

给定平面上的两点 O 与 P , 依如下规则构造尺规作图:

1. 若已构造点 A 与 B , 可作直线 AB 。
2. 若已构造点 A 与 B , 可作以 A 为圆心以 $|AB|$ 为半径的圆。
3. 若已构造若干直线与圆, 可作其交点。



定义 6.3.2 (古希腊三大几何问题)

1. 三等分角 (trisecting angles): 给定角 θ , 构造角 $\theta/3$ 。
2. 立方倍积 (doubling cubes): 给定正方体, 构造正方体, 使其体积加倍; 本质为构造 $\sqrt[3]{2}$ 。
3. 画圆为方 (squaring circles): 给定圆, 构造正方形, 使其面积相等; 本质为构造 π 。



定义 6.3.3 (可构造数 constructible number)

称 $r \in \mathbb{R}$ 为可构造数, 如果在平面 \mathbb{C} 上, 可由点 $O = (0, 0)$ 与 $P = (1, 0)$ 经尺规作图构造出点 $(r, 0)$ 。记可构造数全体为 $\mathcal{C}_{\mathbb{R}} \subset \mathbb{R}$ 。



定义 6.3.4 (可构造点 constructible point)

称点 $(x, y) \in \mathbb{C}$ 为可构造点, 如果成立如下命题。

1. $x \in \mathcal{C}_{\mathbb{R}}$ 且 $y \in \mathcal{C}_{\mathbb{R}}$ 。
2. 在平面 \mathbb{C} 上, 可由点 $O = (0, 0)$ 与 $P = (1, 0)$ 经尺规作图构造出点 (x, y) 。

记可构造点全体为 $\mathcal{C}_{\mathbb{C}} \subset \mathbb{C}$ 。



引理 6.3.1

$\mathcal{C}_{\mathbb{R}}$ 为 \mathbb{R} 的子域, $\mathcal{C}_{\mathbb{C}}$ 为 \mathbb{C} 的子域, 且

$$\mathcal{C}_{\mathbb{C}} = \mathcal{C}_{\mathbb{R}}(i), \quad \mathbb{Q} \subset \mathcal{C}_{\mathbb{R}} \subset \mathcal{C}_{\mathbb{C}}$$



6.3.2 可构造数与二次扩张

定理 6.3.1 (可构造数的充分必要条件)

对于 $\gamma \in \mathbb{R}$, 成立: $\gamma \in \mathcal{C}_{\mathbb{R}} \iff$ 存在 $\delta_1, \dots, \delta_n$, 使得对于任意 $1 \leq k \leq n$, 成立

$$[\mathbb{Q}(\delta_1, \dots, \delta_k) : \mathbb{Q}(\delta_1, \dots, \delta_{k-1})] = 2, \quad \gamma \in \mathbb{Q}(\delta_1, \dots, \delta_n)$$



定理 6.3.2 (可构造数的必要条件)

对于可构造点 $\gamma \in \mathcal{C}_{\mathbb{C}}$, $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ 为 2 的幂。



推论 6.3.1

三等分角的反例: 不可构造角 $\pi/9$; 换言之, 9 次单位原根 $\zeta_9 \notin \mathcal{C}_{\mathbb{C}}$ 。



证明 由于

$$x^9 + 1 = (x^3 + 1)(x^6 - x^3 + 1)$$

因此 ζ_9 的极小多项式为 $x^6 - x^3 + 1$, 从而 $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$, 不为 2 的幂, 因此 $\zeta_9 \notin \mathcal{C}_{\mathbb{C}}$ 。

推论 6.3.2

立方倍积的反例: 不可构造 $\sqrt[3]{2}$; 换言之, $\sqrt[3]{2} \notin \mathcal{C}_{\mathbb{C}}$ 。



证明 $\sqrt[3]{2}$ 的极小多项式为 $x^3 - 2$, 从而 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, 不为 2 的幂, 因此 $\sqrt[3]{2} \notin \mathcal{C}_{\mathbb{C}}$ 。

推论 6.3.3

画圆为方的反例: 不可构造 π ; 换言之, $\pi \notin \mathcal{C}_{\mathbb{C}}$ 。



证明 π 不为代数数, 因此 $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$, 不为 2 的幂, 因此 $\pi \notin \mathcal{C}_{\mathbb{C}}$ 。

6.4 域扩张 II

6.4.1 分裂域与正规扩张

6.4.1.1 分裂域

定义 6.4.1 (分裂域 splitting field)

对于域扩张 K/k , 称 K 为 n 次多项式 $f(x) \in k[x]$ 在 k 上的分裂域, 如果

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in K, 1 \leq i \leq n$$

并且 $K = k(\alpha_1, \dots, \alpha_n)$ 。



引理 6.4.1 (分裂域的存在性)

域 k 上的 n 次多项式 $f(x) \in k[x]$ 存在分裂域 K , 且

$$[K : k] \leq n!$$



证明 (法一): 由代数闭包的存在唯一性 6.2.1, k 存在代数闭包 \bar{k} , 因此

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in \bar{k}, 1 \leq i \leq n$$

进而 $k(\alpha_1, \dots, \alpha_n)$ 为 $f(x)$ 在 k 上的分裂域。

(法二): 当 $n = 1$ 时, $f(x) = a(x - \alpha_1)$, 那么 $\alpha_1 \in k$, 因此 k 为 $f(x)$ 在 k 上的分裂域, 且 $[k : k] = 1$ 。

如果当 $n \leq N$ 时, 命题得证, 那么当 $n = N + 1$ 时, 任取 $f(x)$ 的不可约因式 $p(x)$, 令 α_1 为 $p(x)$ 的根, 因此 $p(x)$ 为 α_1 在 k 上的最小多项式, 从而 $f(\alpha_1) = 0$ 。由单扩张结构 6.1.1, $k[x]/(p(x)) = k(\alpha_1)$, 因此

$$f(x) = (x - \alpha_1)g(x), \quad g(x) \in k(\alpha_1)[x]$$

由归纳假设, $g(x)$ 在 $k(\alpha_1)$ 上存在分裂域 K , 且

$$[K : k(\alpha_1)] \leq N!$$

于是

$$g(x) = a(x - \alpha_2) \cdots (x - \alpha_n), \quad \alpha_i \in K, 2 \leq i \leq n$$

其中 $K = k(\alpha_1)(\alpha_2, \dots, \alpha_n)$ 。由定理 6.1.7, $K = k(\alpha_1, \dots, \alpha_n)$ 。从而

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in K, 1 \leq i \leq n$$

且于是 K 为 $f(x)$ 在 F 上的分裂域, 且由望远镜定理 6.1.8 与单扩张结构 6.1.1

$$[K : F] = [K : k(\alpha_1)][k(\alpha_1) : k] \leq N!(N + 1) = (N + 1)!$$

由数学归纳原理, 原命题得证!

引理 6.4.2

对于域扩张 K/k 与 K'/k' , 如果存在同构映射 $\varphi: k \rightarrow k'$, 令 $\alpha \in K$ 为 k 上的代数元, α 在 k 上的极小多项式为 $p(x)$, 那么

$$\varphi \text{ 可延拓为同态映射 } \Phi: k(\alpha) \rightarrow K' \iff \varphi(p(x)) \text{ 在 } K' \text{ 中存在根}$$

此时延拓数为 $\varphi(p(x))$ 在 K' 中的互异根数。



引理 6.4.3

如果 $\varphi: k \rightarrow k'$ 为同构映射, 令多项式 $f(x) \in k[x]$ 在 k 上的分裂域为 K , 多项式 $f'(x) = \varphi(f(x)) \in k'[x]$ 在 k' 上的分裂域为 K' , 那么 φ 可延拓为同构映射 $\Phi: K \rightarrow K'$, 且延拓数 $\leq [K:k]$, 当且仅当 $f'(x)$ 在 K' 中的根互异时等号成立。



引理 6.4.4 (分裂域的唯一性)

对于域 k 上的多项式 $f(x) \in k[x]$ 在 k 上的分裂域为 K 与 F , 那么存在域同构映射 $\varphi: K \rightarrow F$, 使得成立 $\varphi|_k = \mathbb{1}_k$ 。



证明 由引理 6.4.3, 取 $k' = k$ 与 $\varphi = \mathbb{1}$, 那么 φ 可延拓为同构映射 $\varphi: K \rightarrow F$ 。

定理 6.4.1 (分裂域的存在唯一性)

对于域 k 上的多项式 $f(x) \in k[x]$, $f(x)$ 在 k 上的分裂域存在且存在唯一。



证明 由分裂域的存在性 6.4.1 与唯一性 6.4.4, 命题得证!

6.4.1.2 正规扩张

定义 6.4.2 (正规扩张 normal extension)

称域扩张 K/k 为正规扩张, 如果对于任意 $k[x]$ 上的不可约多项式 $f(x) \in k[x]$, 成立

$$f(x) \text{ 在 } K \text{ 中存在根} \iff f(x) \text{ 在 } K \text{ 中可分解为一次因式之积}$$



定理 6.4.2

对于域扩张 K/k , 成立

$$K/k \text{ 为有限扩张且为正规扩张} \iff \text{存在 } f(x) \in k[x], \text{ 使得 } K \text{ 为 } f(x) \text{ 在 } k \text{ 上的分裂域}$$



6.4.2 可分多项式

定义 6.4.3 (可分多项式 separable polynomial)

称域 k 上的多项式 $f(x) \in k[x]$ 为可分多项式, 如果 $f(x)$ 在其分裂域上没有重根。



引理 6.4.5

对于域 k 上的多项式 $f(x) \in k[x]$, 成立

$$f(x) \text{ 为可分多项式} \iff \gcd(f(x), f'(x)) = 1$$



证明 如果 $f(x)$ 为不可分多项式, 那么

$$f(x) = (x - \alpha)^2 g(x)$$

因此

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$$

因此

$$(x - \alpha) \mid \gcd(f(x), f'(x))$$

如果 $\gcd(f(x), f'(x)) \neq 1$, 因此

$$(x - \alpha) \mid \gcd(f(x), f'(x))$$

令 $f(x) = (x - \alpha)h(x)$, 因此

$$f(x) = h(x) + (x - \alpha)h'(x)$$

进而 $(x - \alpha) \mid h(x)$, 进而 $f(x)$ 不为可分多项式。

引理 6.4.6

对于域 k 上的多项式 $f(x) \in k[x]$, 如果 $f(x)$ 不可分且不可约, 那么 $f'(x) = 0$ 。



证明 由于 $f(x)$ 不可分, 那么由引理 6.4.5, 存在 $p(x) \in k[x]$, 使得成立

$$p(x) \mid \gcd(f(x), f'(x))$$

而 $f(x)$ 不可约, 因此 $p(x)$ 与 $f(x)$ 相伴; 特别的, 其次数相等, 进而 $f'(x) = 0$ 。

推论 6.4.1

对于特征为 0 的域 k , 如果 $f(x) \in k[x]$ 为不可约多项式, 那么 $f(x)$ 为可分多项式。



定义 6.4.4 (Frobenius 同态映射)

对于特征为 $p \neq 0$ 的域 k , 定义 Frobenius 同态映射为

$$k \longrightarrow k$$

$$x \longmapsto x^p$$



定义 6.4.5 (完美域 perfect field)

称特征为 p 的域 k 为完美域, 如果成立如下命题之一。

1. 或 $p = 0$, 或其 Frobenius 同态映射为满射。
2. $k[x]$ 中的不可约多项式均为可分多项式。
3. k 的任意代数扩张为可分扩张。



推论 6.4.2

有限域为完美域。



证明 如果域 k 为有限域, 那么由抽屉原理, 其 Frobenius 同态映射为满射, 进而 k 为完美域。

6.4.3 代数闭包中的可分扩张与嵌入

定义 6.4.6 (可分代数元 separable algebraical element)

对于域扩张 K/k , 称 k 上的代数元 α 为可分代数元, 如果其极小多项式为不可分多项式。



定义 6.4.7 (可分扩张 separable extension)

称代数扩张 K/k 为可分扩张, 如果对于任意 $\alpha \in k$, α 为可分代数元。



定义 6.4.8 (可分度 separable degree)

对于代数扩张 K/k , 称同态映射 $K \rightarrow \bar{k}$ 的数目为 k 的可分度, 记作 $[K:k]_s$ 。



引理 6.4.7

对于单代数扩张 $k(\alpha)/k$, $[k(\alpha):k]$ 为 α 的极小多项式在 \bar{k} 中的互异根数。特别的, $[k(\alpha):k]_s \leq [k(\alpha):k]$, 当且仅当 α 在 k 上可分时等号成立。



命题 6.4.1 (望远镜定理)

对于代数扩张 $F \subset L \subset K$, 成立

$$[K:F]_s < \infty \iff [K:L]_s < \infty \text{ 且 } [L:F]_s < \infty$$

此时成立

$$[K:F]_s = [K:L]_s [L:F]_s$$



命题 6.4.2

对于有限扩张 K/k , 如果 $[K:k]_s \leq [K:k]$, 那么如下命题等价:

1. 存在 k 上的可分代数元 $\alpha_1, \dots, \alpha_n$, 使得成立 $F = k(\alpha_1, \dots, \alpha_n)$ 。
2. K/k 为可分扩张。
3. $[K:k]_s = [K:k]$



6.5 域扩张 III

6.5.1 有限域

定义 6.5.1 (Galois 域)

对于素数 p , 称 p^n 阶域为 Galois 域, 记作 \mathbb{F}_{p^n} 。



引理 6.5.1

对于有限域 F , 令 p 为其特征, $[F:\mathbb{F}_p] = n$, 那么 $|F| = p^n$ 。



定理 6.5.1 (有限域的构造)

1. 多项式 $x^{p^n} - x$ 在域 \mathbb{F}_p 上可分。
2. 对于素数 p , 多项式 $x^{p^n} - x$ 在域 \mathbb{F}_p 上的分裂域的阶为 p^n 。
3. 对于素数 p , p^n 阶域为多项式 $x^{p^n} - x$ 在域 \mathbb{F}_p 上的分裂域。



推论 6.5.1

对于素数 p , 成立

$$\text{存在且存在唯一域扩张 } \mathbb{F}_{p^m}/\mathbb{F}_{p^n} \iff n \mid m$$

**推论 6.5.2**

对于素数 p , 如果 $n \mid m$, 那么域扩张 $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ 为单扩张。

**推论 6.5.3**

如果 F 为有限域, 那么 $F[x]$ 中存在任意次不可约多项式。

**命题 6.5.1**

对于素数 p , 令

$$\begin{aligned} \varphi: \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n} \\ x &\longmapsto x^p \end{aligned}$$

则

$$\text{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = \langle \varphi \rangle$$

**6.5.2 分圆多项式与分圆域****定义 6.5.2 (n 次单位根 n -th root of 1)**

定义 n 次单位根为

$$\zeta_n = e^{\frac{2\pi i}{n}}$$

n 次单位根乘法群为

$$\mu_n = \langle \zeta_n \rangle$$

**定义 6.5.3 (n 次单位原根 primitive n -th root of 1)**

称 μ_n 的生成元为 n 次单位原根; 换言之

$$\mu_n = \langle \zeta_n^m \rangle \iff \gcd(m, n) = 1$$

**定义 6.5.4 (n 次分圆多项式 n -th cyclotomic polynomial)**

定义 n 次分圆多项式为

$$\Phi_n(x) = \prod_{\substack{1 \leq m \leq n \\ (m, n) = 1}} (x - \zeta_n^m)$$

**定义 6.5.5 (n 次分圆域 n -th cyclotomic field)**

称多项式 $x^n - 1$ 在 \mathbb{Q} 上分裂域 $\mathbb{Q}(\zeta_n)$ 为 n 次分圆域。

**引理 6.5.2**

如果 p 为素数, 那么

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$



表 6.1: 分圆多项式

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$

引理 6.5.3

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$



推论 6.5.4

$$\Phi_n(x) \in \mathbb{Z}[x]$$



命题 6.5.2

$\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约。



推论 6.5.5

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$$



推论 6.5.6

多项式 $x^n - 1$ 为 ζ_n 在 \mathbb{Q} 上的极小多项式。



命题 6.5.3

$$\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$



6.6 可分性与单扩张

命题 6.6.1

对于代数扩张 K/k , 成立

$$K/k \text{ 为单扩张} \iff \text{中间域 } k \subset F \subset K \text{ 数有限}$$



命题 6.6.2 (有限 + 可分 \implies 单扩张)

有限可分扩张为单扩张。

**推论 6.6.1**

对于有限可分扩张 K/k , 成立

$$|\text{Aut}_k(K)| \leq [K : k]$$

当且仅当 K/k 为正规扩张时等号成立。



6.7 Galois 理论

6.7.1 Galois 对应与 Galois 扩张

定义 6.7.1 (不动域 fixed field)

对于域扩张 K/k , 定义子群 $G < \text{Aut}_k(K)$ 的不动域为中间域

$$\text{Inv}_K(G) = \{x \in K : \forall g \in G, g(x) = x\}$$

**定义 6.7.2 (Galois 对应 Galois correspondence)**

称域扩张 K/k 的 Galois 对应为

$$\{\text{域扩张 } K/k \text{ 的中间域}\} \begin{matrix} \xleftarrow{\varphi} \\ \xrightarrow{\psi} \end{matrix} \{\text{自同构群 } \text{Aut}_k(K) \text{ 子群}\}$$

其中

$$\varphi : \{\text{域扩张 } K/k \text{ 的中间域}\} \longrightarrow \{\text{自同构群 } \text{Aut}_k(K) \text{ 子群}\}$$

$$F \longmapsto \text{Aut}_F(K)$$

$$\psi : \{\text{自同构群 } \text{Aut}_k(K) \text{ 子群}\} \longrightarrow \{\text{域扩张 } K/k \text{ 的中间域}\}$$

$$G \longmapsto \text{Inv}_K(G)$$

**引理 6.7.1**

域扩张 K/k 的 Galois 对应为反包含的; 换言之, 对于子群 $G < \text{Aut}_k(K)$ 与中间域 $k \subset F \subset K$, 成立

$$F \subset \text{Inv}_K(\text{Aut}_F(K)), \quad G \subset \text{Aut}_{\text{Inv}_K(G)}(K)$$

进一步, 对于子群 $G_1, G_2 < \text{Aut}_k(K)$ 与中间域 $k \subset F_1, F_2 \subset K$, 令

$$\langle G_1, G_2 \rangle = \bigcap_{G_1 \cup G_2 \subset G < \text{Aut}_k(K)} G, \quad F_1 F_2 = \bigcap_{F_1 \cup F_2 \subset F \subset K} F$$

那么

$$\text{Aut}_{F_1 F_2}(K) = \text{Aut}_{F_1}(K) \cap \text{Aut}_{F_2}(K), \quad \text{Inv}_K(\langle G_1, G_2 \rangle) = \text{Inv}_K(G_1) \cap \text{Inv}_K(G_2)$$

**引理 6.7.2**

对于有限扩张 K/k 与子群 $G < \text{Aut}_k(K)$, 则 $K/\text{Inv}_K(G)$ 为有限、正规、可分的单扩张。



命题 6.7.1

对于有限扩张 K/k 与子群 $G < \text{Aut}_k(K)$, 成立

$$|G| = [K : \text{Inv}_K(G)], \quad G = \text{Aut}_{\text{Inv}_K(G)}(K)$$

特别的, 对于有限扩张 K/k , Galois 对应

$$\begin{aligned} \varphi : \{\text{域扩张 } K/k \text{ 的中间域}\} &\longrightarrow \{\text{自同构群 } \text{Aut}_k(K) \text{ 子群}\} \\ F &\longmapsto \text{Aut}_F(K) \end{aligned}$$

为满射。



笔记 此处 K/k 为有限扩张是必要的, 因为对于无限扩张 K/k , Galois 对应不一定为满射, 因此如下仅定义有限 Galois 扩张。

定义 6.7.3 (Galois 扩张)

称有限扩张 K/k 为 Galois 扩张, 如果成立如下命题之一。

1. K 为 k 上的可分多项式 $f(x) \in k[x]$ 的分裂域。
2. K/k 为正规且可分的域扩张。
3. $|\text{Aut}_k(K)| = [K : k]$
4. $k = \text{Inv}_K(\text{Aut}_k(K))$
5. K/k 的 Galois 对应为双射。
6. K/k 为可分扩张, 且若 F/K 为代数扩张, $\varphi \in \text{Aut}_k(F)$, 则 $\varphi(K) = K$ 。

**6.7.2 Galois 基本定理****定理 6.7.1 (Galois 基本定理 the fundamental theorem of Galois theory)**

对于 Galois 扩张 K/k , 成立如下命题。

1. 存在非 Galois 扩张; 例如 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 。
2. K/k 的 Galois 对应为双射, 且对于子群 $G < \text{Aut}_k(K)$ 与中间域 $k \subset F \subset K$, 成立

$$\text{Inv}_K(\text{Aut}_F(K)) = F, \quad \text{Aut}_{\text{Inv}_K(G)}(K) = G$$

3. 对于中间域 F , 成立

$$[K : F] = |\text{Aut}_F(K)|$$

且 K/F 为 Galois 扩张, 同时

$$[F : k] = |\text{Aut}_k(K) : \text{Aut}_F(K)|$$

4. 对于中间域 F , 成立

$$F/k \text{ 为 Galois 扩张} \iff \text{Aut}_F(K) \triangleleft \text{Aut}_k(K)$$

此时成立

$$\text{Aut}_k(F) \cong \frac{\text{Aut}_k(K)}{\text{Aut}_F(K)}$$



6.8 Galois 理论的应用

6.8.1 代数基本定理

定理 6.8.1 (代数基本定理 fundamental theorem of algebra)

\mathbb{C} 为代数闭域。



6.8.2 正 n 边形的尺规作图

命题 6.8.1

对于 Galois 扩张 K/k , 如果 $[K:k] = p^n$, 其中 p 为素数, 那么存在升链

$$k = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = K$$

使得成立

$$[F_i : F_{i-1}] = p, \quad 1 \leq i \leq n$$



定义 6.8.1 (Fermat 素数)

称素数 p 为 Fermat 素数, 如果存在 $n \in \mathbb{N}^*$, 使得成立

$$p = 2^{2^n} + 1$$



表 6.2: Fermat 素数

n	$2^{2^n} + 1$	是否为素数
0	3	✓
1	5	✓
2	17	✓
3	257	✓
4	65537	✓
5	4294967297	641×6700417
6	18446744073709551617	$274177 \times 67280421310721$
7	340282366920938463463374607431768211457	$59649589127497217 \times 5704689200685129054721$

定理 6.8.2 (正 n 边形的尺规作图题)

1. 对于素数 p , 成立

可尺规作出正 p 边形 $\iff p$ 为 Fermat 素数

2. 如下命题等价。

- (a). 可尺规作出正 n 边形。
- (b). $\phi(n)$ 为 2 的幂。
- (c). n 为互异 Fermat 素数与 2 的幂之积。



例题 6.4 正多边形作图问题: 可尺规作出如下正 n 边形

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, \dots$$

例题 6.5 正 17 边形的尺规作图：17 次单位原根为

$$\cos \frac{2\pi}{17} = \frac{\sqrt{17} - 1 + \sqrt{2} \sqrt{34 + 6\sqrt{17} + \sqrt{2}(\sqrt{17} - 1)\sqrt{17 - \sqrt{17}} - 8\sqrt{2}\sqrt{17 + \sqrt{17}} + \sqrt{2}\sqrt{17 - \sqrt{17}}}}{16}$$

其极小多项式为

$$256x^8 + 128x^7 - 448x^6 - 192x^5 + 240x^4 + 80x^3 - 40x^2 - 8x + 1$$

因此 $[\mathbb{Q}(2\pi/17) : \mathbb{Q}] = 8$ 为 2 的幂，进而可依尺规作图构造正 17 边形。

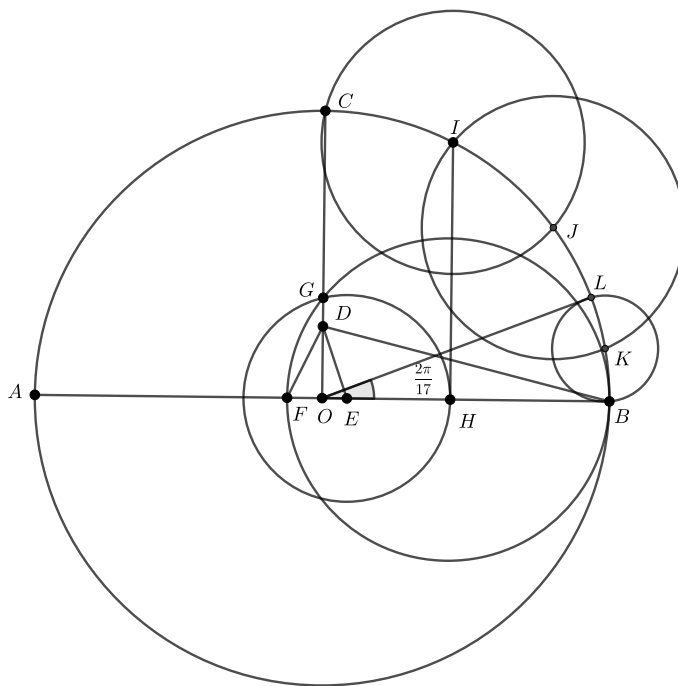


图 6.1: 正 17 边形

1. 给定圆 O ，作直径 AB ；
2. 作半径 OC ，使得 $OC \perp AB$ ；
3. 在线段 OC 上作点 D ，使得 $OD = OC/4$ ；
4. 在线段 OB 上作点 E ，使得 $\angle ODE = \angle ODB/4$ ；
5. 在线段 OA 上作点 F ，使得 $\angle EDF = \pi/4$ ；
6. 以线段 BF 为直径作圆，交线段 OC 于点 G ；
7. 以点 E 为圆心，线段 EG 为半径作圆，交线段 OB 于点 H ；
8. 过点 H ，作线段 AB 的垂线，交圆 O 于点 I ；
9. 以点 I 为圆心，过点 C 作圆，交圆 O 于点 J ；
10. 以点 J 为圆心，过点 I 作圆，交圆 O 于点 K ；
11. 以点 K 为圆心，过点 B 作圆，交圆 O 于点 L ；
12. 得到角 $\angle BOL = 2\pi/17$ 。

6.8.3 对称函数基本定理

定义 6.8.2 (对称多项式 symmetric function)

对于环 $(R, +, \cdot)$, 称多项式 $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ 为对称多项式, 如果对于任意置换 $\sigma \in S_n$, 成立

$$f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$



定义 6.8.3 (初等对称函数 elementary symmetric function)

$$s_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \cdots x_{i_k}, \quad 1 \leq k \leq n$$



引理 6.8.1

对于域 K , 域扩张

$$K(x_1, \dots, x_n)/K(s_1, \dots, s_n)$$

为 Galois 扩张, 其 Galois 群为 S_n 。



定理 6.8.3 (对称函数基本定理 fundamental theorem on symmetric functions)

对于域 K 上的多项式 $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$, 成立

$f(x_1, \dots, x_n)$ 为对称多项式

\iff 存在多项式 $g(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$, 使得成立 $f(x_1, \dots, x_n) = g(s_1, \dots, s_n)$



推论 6.8.1

对于有限群 G , 存在 Galois 扩张 K/k , 使得成立 $\text{Aut}_k(K) \cong G$ 。



推论 6.8.2

对于域 K , 令

$$\Delta = \prod_{1 \leq i < j \leq n} |x_i - x_j|$$

那么域扩张

$$K(x_1, \dots, x_n)/K(s_1, \dots, s_n)(\Delta)$$

为 Galois 扩张, 其 Galois 群为 A_n 。



6.8.4 多项式方程的根式可解性

6.8.4.1 根式扩张

定义 6.8.4 (单根式扩张)

称 n 次单扩张 $k(\alpha)/k$ 为单根式扩张, 如果 $\alpha^n \in k$ 。



定义 6.8.5 (根式扩张 radical extension)

1. 称有限扩张 K/k 为根式扩张, 如果存在升链

$$k = F_0 \subset F_1 \subset \cdots \subset F_{r-1} \subset F_r = K$$

使得对于任意 $1 \leq i \leq r$, F_i/F_{i-1} 为单根式扩张。

2. 称域扩张 $k(\alpha_1, \cdots, \alpha_r)/k$ 为根式扩张, 如果对于任意 $1 \leq i \leq r$, 存在 $n_i \in \mathbb{N}^*$, 使得成立 $\alpha_i^{n_i} \in k(\alpha_1, \cdots, \alpha_{i-1})$ 。

**定义 6.8.6 (可解扩张 solvable extension)**

称域扩张 K/k 为可解扩张, 如果存在根式扩张 F/k , 使得成立 $K \subset F$ 。特别的, 称 Galois 扩张 K/k 为可解的, 如果 $\text{Aut}_k(K)$ 为可解群。

**引理 6.8.2**

对于可分根式扩张 K/k , 存在 Galois 根式扩张 F/k , 使得成立 $K \subset F$ 。

**引理 6.8.3**

对于 Galois 扩张 K/k , 如果 $\text{char}(k) = 0$ 且 k 包含充分多的单位根, 那么

$$K/k \text{ 为根式扩张} \iff K/k \text{ 为可解扩张}$$

**命题 6.8.2**

对于 Galois 扩张 K/k , 如果 $\text{char}(k) = 0$, 那么

$$K/k \text{ 为可解扩张} \iff \text{存在 Galois 根式扩张 } F/k, \text{ 使得成立 } K \subset F$$

**6.8.4.2 多项式的根式可解性****定义 6.8.7 (一般多项式 general polynomial)**

对于特征为 0 的域 k , a_1, \cdots, a_n 为 k 上的未定元, 称 k 上的 n 次一般多项式为 $k(a_1, \cdots, a_n)$ 上的不可约多项式

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

**定义 6.8.8 (多项式的 Galois 群)**

对于域 k 上的多项式 $f(x)$, 其分裂域为 K , 定义 $f(x)$ 的 Galois 群为

$$\text{Gal}_k(f(x)) = \text{Aut}_k(K)$$

**定义 6.8.9 (根式可解 radical solvable)**

对于域 k 上的多项式 $f(x)$, 其分裂域为 K , 称 $f(x)$ 在 k 中根式可解, 如果存在根式扩张 F/k , 使得成立 $K \subset F$ 。

**定理 6.8.4 (一般多项式的 Galois 群)**

对于特征为 0 的域 k 上的 n 次一般多项式 $f(x)$, 成立

$$\text{Gal}_k(f(x)) \cong S_n$$



定理 6.8.5 (Galois 准则 Galois' criterion)

对于特征为 0 的域 k 上的多项式 $f(x)$, 如果 $f(x)$ 为不可约多项式, 那么

$$f(x) \text{ 在 } k \text{ 上根式可解} \iff \text{Gal}_k(f(x)) \text{ 为可解群}$$

**定理 6.8.6 (Abel-Ruffini 定理)**

对于特征为 0 的域 k 上的 n 次一般多项式 $f(x)$, 当且仅当 $n \geq 5$ 时, $f(x)$ 在 k 上根式不可解。



证明 由定理 3.4.6、6.8.4 与 6.8.5, 命题得证!

我希望终将会 有智者能从这混沌之中受益匪浅。

— Evariste Galois

附录 A 群论的 MATLAB 函数

定义名为 `Group` 的数据结构，包含 `element`、`group`、`order` 三个属性。

- 1. `element`: 群元素。每一行代表一个元素，第 k 行元素的指标定义为 k 。
- 2. `group`: 群运算表。 (i, j) 处的数字表示 i 指标对应元素与 j 指标对应元素作运算后的元素对应的指标。
- 3. `order`: 群的阶。

表 A.1: 群论的 MATLAB 函数

类别	函数	名称
特殊群	<code>cyclicGroup</code>	循环群
	<code>moduloNGroup</code>	循环群的单位群
	<code>dihedralGroup</code>	二面体群
	<code>symmetricGroup</code>	对称群
	<code>alternatingGroup</code>	交错群
	<code>quaternionGroup</code>	四元数群
群结构	<code>subgroup</code>	子群
	<code>normalSubgroup</code>	正规子群
	<code>generatedSubgroup</code>	生成子群
	<code>generatedNormalSubgroup</code>	生成正规子群
	<code>centerGroup</code>	中心子群
	<code>characteristicSubgroup</code>	特征子群
	<code>commutatorGroup</code>	换位子群
	<code>centralizer</code>	中心化子
	<code>conjugacyClass</code>	共轭类
	<code>derivedGroup</code>	导群
群运算	<code>groupOperate</code>	群运算
	<code>inverseMatrix</code>	逆元素矩阵
	<code>orderMatrix</code>	元素阶矩阵
	<code>groupHomomorphism</code>	群同态态射
	<code>groupIsomorphism</code>	群同构态射
	<code>isCommutativeGroup</code>	是否为交换群
	<code>isSimpleGroup</code>	是否为单群
	<code>isSolvableGroup</code>	是否为可解群
	<code>directProductOfGroups</code>	直积
辅助函数	<code>EulerFunction</code>	Euler 函数
	<code>fullPermutation</code>	全排列
	<code>generateCombinations</code>	组合矩阵

A.1 特殊群

Listing A.1: 循环群

```
function [element, group, realGroup, order] = cyclicGroup(n)

% 名称: 模n循环群Z/nZ
% 输入: 循环群阶数n
% 输出: 1.群元素element; 2.群运算表group和realGroup; 3.群阶order
% 说明: 以element表中元素的位置建立与元素间的双射
%       如下出现的数字均代表元素的位置, 不代表真实元素
%       realGroup为真实元素
%       group(i,j)=element(i)+element(j)

%% 1.群元素
element = 0: n-1;

%% 2.群阶
order = n;

%% 3.群运算表
[i, j] = meshgrid(1: n, 1: n);
realGroup = mod(i + j - 2, n);
group = realGroup + 1;

end
```

Listing A.2: 循环群的单位群

```
function [element, group, realGroup, order] = moduloNGroup(n)

% 名称: 模n单位群(Z/nZ)*
% 输入: 模n单位群阶数n
% 输出: 1.群元素element; 2.群运算表group和realGroup; 3.群阶order
% 说明: 以element表中元素的位置建立与元素间的双射
%       如下出现的数字均代表元素的位置, 不代表真实元素
%       realGroup为真实元素
%       group(i,j)=element(i)*element(j)

%% 1.群元素和群阶
[order, element] = EulerFunction(n);

%% 3.群运算表
realGroup = mod(element' * element, n);
group = zeros(order, order);
for i = 1: order
    for j = 1: order
        for k = 1: order
            if element(k) == realGroup(i, j)
```

```

        indice = k;
        break
    end
end
% 赋值
group(i, j) = indice;
end
end
end

```

Listing A.3: 二面体群

```

function [element, group, order] = dihedralGroup(n)

% 名称: n阶二面体群D_2n
% 输入: 二面体群阶数n
% 输出: 1.群元素element; 2.群运算表group; 3.群阶order
% 说明: 以element表中元素的位置建立与元素间的双射
%       如下出现的数字均代表元素的位置, 不代表真实元素
%       element为2n行2列矩阵
%       其中element(k)代表第k个元素
%       element的行向量(i,j)代表映射sigma^i tau^j
%       sigma^n = tau^2 = sigma tau sigma tau = 1
%       group(i,j)=element(i) \circ element(j)

%% 1.群元素
element = [(0: n-1)', zeros(n, 1); (0: n-1)', ones(n, 1)];

%% 2.群阶
order = 2 * n;

%% 3.群运算表

% 初始化
group = zeros(order, order);
for i = 1: order
    for j = 1: order

        % 利用sigma^n = tau^2 = sigma tau sigma tau = 1降次
        temp = [element(i, :), element(j, :)];

        % tau^2 = sigma^n = 1降次
        if temp(2) == 0
            map = [mod(temp(1)+temp(3), n), temp(4)];
        elseif temp(3) == 0
            map = [temp(1), mod(temp(2)+temp(4), 2)];
        else
            map = [mod(n+temp(1)-temp(3), n), mod(1+temp(4), 2)];
        end
    end
end

```

```

        % 找到复合映射的编号
        for k = 1: order
            if element(k, :) == map
                indice = k;
                break
            end
        end
        % 赋值
        group(i, j) = indice;

    end
end

end

```

Listing A.4: 对称群

```

function [element, group, order] = symmetricGroup(n)

% 名称: n阶对称群S_n
% 输入: 对称群阶数n
% 输出: 1.群元素element; 2.群运算表group; 3.群阶order
% 说明: 以element表中元素的位置建立与元素间的双射
%       如下出现的数字均代表元素的位置, 不代表真实元素
%       element为n!行n列矩阵
%       其中element(k)代表第k个元素, 即第k个双射
%       第j列代表j在该行代表映射下的像
%       group(i,j)=element(j) \circ element(i)

%% 1.群元素
element = fullPermutation(n);
element = element(end: -1: 1, :);

%% 2.群阶
order = factorial(n);

%% 3.群运算表

% 初始化
group = zeros(order, order);
for i = 1: order
    for j = 1: order
        % 初始化
        permutation = zeros(1, n);
        permutation_i = element(i, :);
        permutation_j = element(j, :);
        % 计算复合映射
        for k = 1: n

```

```

        permutation(k) = permutation_j(permutation_i(k));
    end
    % 找到复合映射的编号
    for k = 1: order
        if element(k, :) == permutation
            indice = k;
            break
        end
    end
    % 赋值
    group(i, j) = indice;
end
end
end

```

Listing A.5: 交错群

```

function [element, group, order] = alternatingGroup(n)

% 名称: n阶交错群A_n
% 输入: 交错群阶数n
% 输出: 1.群元素element; 2.群运算表group; 3.群阶order
% 说明: 以element表中元素的位置建立与元素间的双射
%       如下出现的数字均代表元素的位置, 不代表真实元素
%       element为n!行n列矩阵
%       其中element(k)代表第k个元素, 即第k个双射
%       第j列代表j在该行代表映射下的像
%       group(i,j)=element(j) \circ element(i)

%% 1.群元素
permutations = perms(1: n); % 生成所有n元置换的排列

element = [];
for i = 1:size(permutations, 1)
    perm = permutations(i, :);
    sign = 1; % 初始化符号为正号

    for j = 1:n
        for k = (j+1):n
            if perm(j) > perm(k)
                sign = -sign; % 交换时改变符号
            end
        end
    end

    if sign == 1 % 符号为正号表示是偶置换
        element = [element; perm];
    end
end

```

```

end
element = element(end: -1: 1, :);

%% 2. 群阶
order = factorial(n) / 2;

%% 3. 群运算表

% 初始化
group = zeros(order, order);
for i = 1: order
    for j = 1: order
        % 初始化
        permutation = zeros(1, n);
        permutation_i = element(i, :);
        permutation_j = element(j, :);
        % 计算复合映射
        for k = 1: n
            permutation(k) = permutation_j(permutation_i(k));
        end
        % 找到复合映射的编号
        for k = 1: order
            if element(k, :) == permutation
                indice = k;
                break
            end
        end
        % 赋值
        group(i, j) = indice;
    end
end
end
end

```

Listing A.6: 四元数群

```

function [element, group, realGroup, order] = quaternionGroup

% 名称: 四元数群
% 输出: 1. 群元素element; 2. 群运算表group和realGroup; 3. 群阶order
% 说明: 以element表中元素的位置建立与元素间的双射
%       如下出现的数字均代表元素的位置, 不代表真实元素
%       realGroup为真实元素
%       group(i,j)=element(i)*element(j)

%% 函数

order = 8;

```

```

element = {
    '1', '-1', ...
    'i', '-i', ...
    'j', '-j', ...
    'k', '-k'};

realGroup = {
    '1', '-1', 'i', '-i', 'j', '-j', 'k', '-k'; ...
    '-1', '1', '-i', 'i', '-j', 'j', '-k', 'k'; ...
    'i', '-i', '-1', '1', 'k', '-k', '-j', 'j'; ...
    '-i', 'i', '1', '-1', '-k', 'k', 'j', '-j'; ...
    'j', '-j', '-k', 'k', '-1', '1', 'i', '-i'; ...
    '-j', 'j', 'k', '-k', '1', '-1', '-i', 'i'; ...
    'k', '-k', 'j', '-j', '-i', 'i', '-1', '1'; ...
    '-k', 'k', '-j', 'j', 'i', '-i', '1', '-1'};

group = zeros(order, order);
for i = 1: order
    for j = 1: order
        for n = 1: order
            if isequal(realGroup(i, j), element(n))
                group(i, j) = n;
            end
        end
    end
end
end
end

```

A.2 群结构

Listing A.7: 子群

```

function subgroupMatrix = subgroup(group)

% 名称: 子群
% 输入: 群运算表group
% 输出: 所有子群
% 说明: subgroupMatrix每一行代表一个子群的元素的编号

%% 求解子群的阶
order = size(group, 1);
factors = [];
loc = 1;
for fac = 1: order
    if mod(order, fac) == 0
        factors(loc) = fac;
        loc = loc + 1;
    end
end

```

```

    end
end

%% 求解子群
invMatrix = inverseMatrix(group);
subgroupMatrix = [];
for n = factors
    combinations = generateCombinations(n, order);
    for com = combinations'
        judge = 1;
        for i = com'
            for j = com'
                invj = invMatrix(j);
                if ~ismember(group(i, invj), com)
                    judge = 0;
                    break
                end
            end
        end
        if judge == 0
            break
        end
        if judge == 1 && i == com(end) && j == com(end)
            subgroupMatrix = [subgroupMatrix; com', zeros(1, order - size(com', 2))];
        end
    end
end
end
end
end

```

Listing A.8: 正规子群

```

function normalSubgroupMatrix = normalSubgroup(group)

% 名称: 正规子群
% 输入: 群运算表group
% 输出: 所有正规子群
% 说明: normalSubgroupMatrix每一行代表一个正规子群的元素的编号

%% 函数1
order = size(group, 1);
subgroupMatrix = subgroup(group);
subgroupNumber = size(subgroupMatrix, 1);
invmatrix = inverseMatrix(group);

normalSubgroupMatrix = [];
for N = 1: subgroupNumber

    judge = 1;

```



```

normalSubgroup = subgroupMatrix(N, :);

for n = 1: order

    if normalSubgroup(n) == 0
        break
    end

    for g = 1: order
        temp = group(group(g, normalSubgroup(n)), invmatrix(g));
        if ~ismember(temp, normalSubgroup)
            judge = 0;
            break
        end
    end

    if judge == 0
        break
    end

    if judge == 1
        normalSubgroupMatrix = [normalSubgroupMatrix; normalSubgroup];
    end
end

%% 函数2
% order = size(group, 1);
% subgroupMatrix = subgroup(group);
% subgroupNumber = size(subgroupMatrix, 1);
%
% normalSubgroupMatrix = [];
% for N = 1: subgroupNumber
%
%     judge = 1;
%     normalSubgroup = subgroupMatrix(N, :);
%     normalSubgroup(normalSubgroup == 0) = [];
%     normalSubgroupNumber = size(normalSubgroup, 2);
%
%     for g = 1: order
%         gN = zeros(normalSubgroupNumber, 1);
%         Ng = zeros(normalSubgroupNumber, 1);
%         for n = 1: normalSubgroupNumber
%             gN(n) = group(g, normalSubgroup(n));
%             Ng(n) = group(normalSubgroup(n), g);
%         end
%         gN = unique(sort(gN));
%         Ng = unique(sort(Ng));
%         if ~isequal(gN, Ng)

```

```

%         judge = 0;
%         break
%     end
% end
% if judge == 1
%     normalSubgroupMatrix = [normalSubgroupMatrix; normalSubgroup, zeros(1, order-size(
%         normalSubgroup, 2))];
% end
%
% end
end

```

Listing A.9: 生成子群

```

function generatedSubgroupMatrix = generatedSubgroup(group, subset)

% 名称: 生成子群
% 输入: 群运算表group, 子集subset
% 输出: 生成子群元素的编号

%% 函数
subgroupMatrix = subgroup(group);
% 初始化一个空矩阵来存储符合条件的子集
supsetgroupMatrix = [];
% 逐行比较subset和subgroupMatrix的每一行
for n = 1: size(subgroupMatrix, 1)
    % 如果subset的所有元素都在subgroupMatrix的这一行中
    if all(ismember(subset, subgroupMatrix(n, :)))
        % 将这一行添加到supsetgroupMatrix中
        supsetgroupMatrix = [supsetgroupMatrix; subgroupMatrix(n, :)];
    end
end

% 找出supsetgroupMatrix每一行的公共元素
generatedSubgroupMatrix = supsetgroupMatrix(1, :);
for n = 1: size(supsetgroupMatrix, 1)
    generatedSubgroupMatrix = intersect(generatedSubgroupMatrix, supsetgroupMatrix(n, :));
end
generatedSubgroupMatrix = transpose(nonzeros(generatedSubgroupMatrix));

end

```

Listing A.10: 生成正规子群

```

function generatedNormalSubgroupMatrix = generatedNormalSubgroup(group, subset)

% 名称: 生成正规子群
% 输入: 群运算表group, 子集subset
% 输出: 生成子群元素的编号

```

```

%% 函数
normalSubgroupMatrix = normalSubgroup(group);
% 初始化一个空矩阵来存储符合条件的子集
supsetnormalGroupMatrix = [];
% 逐行比较subset和subgroupMatrix的每一行
for n = 1: size(normalSubgroupMatrix, 1)
    % 如果subset的所有元素都在subgroupMatrix的这一行中
    if all(ismember(subset, normalSubgroupMatrix(n, :)))
        % 将这一行添加到supsetgroupMatrix中
        supsetnormalGroupMatrix = [supsetnormalGroupMatrix; normalSubgroupMatrix(n, :)];
    end
end

% 找出supsetgroupMatrix每一行的公共元素
generatedNormalSubgroupMatrix = supsetnormalGroupMatrix(1, :);
for n = 1: size(supsetnormalGroupMatrix, 1)
    generatedNormalSubgroupMatrix = intersect(generatedNormalSubgroupMatrix,
        supsetnormalGroupMatrix(n, :));
end
generatedNormalSubgroupMatrix = transpose(nonzeros(generatedNormalSubgroupMatrix));

end

```

Listing A.11: 中心子群

```

function centreGroupMatrix = centerGroup(group)

% 名称: 中心子群
% 输入: 群运算表group
% 输出: 中心子群元素的编号

%% 函数
centreGroupMatrix = [];
order = size(group, 1);
for n = 1: order
    judge = 1;
    for k = 1: order
        if group(n, k) ~= group(k, n)
            judge = 0;
        end
    end
    if judge == 1
        centreGroupMatrix = [centreGroupMatrix, n];
    end
end

end

```

Listing A.12: 特征子群

```

function characteristicSubgroupMatrix = characteristicSubgroup(group)

% 名称: 特征子群
% 输入: 群运算表group
% 输出: 所有特征子群
% 说明: characteristicSubgroupMatrix每一行代表特征正规子群的元素的编号

%% 函数
subgroupMatrix = normalSubgroup(group);
mapMatrix = groupIsomorphism(group, group);
order = size(group, 1);
subgroupNumber = size(subgroupMatrix, 1);
mapNumber = size(mapMatrix, 1);
characteristicSubgroupMatrix = [];
for i = 1: subgroupNumber
    judge = 1;
    subgroups = subgroupMatrix(i, :);
    for j = 1: mapNumber
        im = [];
        map = mapMatrix(j, :);
        for n = 1: order
            if subgroups(n) ~= 0
                im = [im map(subgroups(n))];
            end
        end
        if ~all(ismember(im, subgroups))
            judge = 0;
            break
        end
    end
    if judge == 1
        characteristicSubgroupMatrix = [characteristicSubgroupMatrix; subgroups];
    end
end
end

```

Listing A.13: 换位子群

```

function commutatorGroupMatrix = commutatorGroup(group, elementMatrix)

% 名称: 换位子群
% 输入: 群运算表group, 群元素编号(可选)
% 输出: 换位子群元素的编号

%% 函数
matrix = inverseMatrix(group);
narginchk(1, 2); % 检查输入参数数量, 允许1到2个参数

```

```

if nargin == 1
    order = size(group, 1);
    commutatorGroupMatrix = zeros(1, order^2);
    for i = 1: order
        for j = 1: order
            commutatorGroupMatrix((i-1) * order + j) = group(group(group(i, j), matrix(i)), matrix(j));
        end
    end
else
    commutatorGroupMatrix = [];
    for i = elementMatrix
        for j = elementMatrix
            commutatorGroupMatrix = [commutatorGroupMatrix, group(group(group(i, j), matrix(i)), matrix(j))];
        end
    end
end
commutatorGroupMatrix = sort(unique(commutatorGroupMatrix));
% commutatorGroupMatrix = generatedNormalSubgroup(group, commutatorGroupMatrix);

end

```

Listing A.14: 中心化子

```

function matrix = centralizer(g, group)

% 名称: 中心化子
% 输入: 元素编号g, 群运算表group
% 输出: 编号为g的元素的共轭类的编号

%% 函数
order = size(group, 1);
matrix = [];
for n = 1: order
    if group(g, n) == group(n, g)
        matrix = [matrix, n];
    end
end

end

```

Listing A.15: 共轭类

```

function class = conjugacyClass(g, group)

% 名称: 共轭类
% 输入: 元素编号g, 群运算表group
% 输出: 编号为g的元素的共轭类的编号

```

```

%% 函数
order = size(group, 1);
matrix = inverseMatrix(group);
class = [];
for n = 1: order
    element = group(group(n, g), matrix(n));
    class = [class, element];
end
class = sort(unique(class));

end

```

Listing A.16: 导群

```

function derivedGroupMatrix = derivedGroup(group, degree)

% 名称: 导群
% 输入: 群运算表group和导群阶
% 输出: 导群元素的编号

%% 函数
order = size(group, 1);
derivedGroupMatrix = 1: order; % 初始化
for n = 1: degree % 迭代次数
    derivedGroupMatrix = commutatorGroup(group, derivedGroupMatrix);
end

end

```

A.3 群运算

Listing A.17: 群运算

```

function result = groupOperate(Group, g, h)

% 名称: 群运算
% 输入: 群Group, 以及群元素编号g和h
% 输出: 群元素Group(g)*Group(h)的编号
% 关于群Group:
% 给定群Group中元素的编号: 1, ..., |Group|
% Group(n)表示群G中编号为n的元素
% Group为|G|行|G|列矩阵, 其中Group(i,j)=Group(i)*Group(j)

%% 计算群运算
result = Group(g, h);

end

```

Listing A.18: 逆元素矩阵

```

function matrix = inverseMatrix(group)

% 名称: 逆元素矩阵
% 输入: 群运算表group
% 输出: 逆元素编号矩阵matrix
% 说明: matrix(k)表示编号为k的元素的逆元素的编号

%% 函数
order = size(group, 1);
matrix = zeros(1, order);
for i = 1: order
    for j = 1: order
        if group(i, j) == 1
            matrix(i) = j;
            break
        end
    end
end
end

end

```

Listing A.19: 元素阶矩阵

```

function matrix = orderMatrix(group)

% 名称: 元素阶矩阵
% 输入: 群运算表group
% 输出: 元素阶矩阵matrix
% 说明: matrix(k)表示编号为k的元素的阶

%% 函数
order = size(group, 1);
matrix = zeros(1, order);
for loc = 1: order
    if loc == 1
        matrix(loc) = 1;
    else
        element = loc;
        for n = 2: order
            element = group(element, loc);
            if element == 1
                matrix(loc) = n;
                break
            end
        end
    end
end
end

end

```

```
end
```

Listing A.20: 群同态态射

```
function mapMatrix = groupHomomorphism(G, H)

% 名称: 群同态态射
% 输入: 群G和H
% 输出:  $G \rightarrow H$ 的同态态射
% 其中每一行代表一个态射, 第j列代表j在该态射下的像

%% 函数

% 定义群的阶
m = size(G, 1);
n = size(H, 1);

% 初始化映射矩阵
mapMatrix = zeros(n^m, m);

% 生成所有可能的映射
for i = 1: n^m
    temp = i - 1;
    for j = m:-1:1
        quotient = floor(temp / n);
        remainder = mod(temp, n);
        mapMatrix(i, j) = remainder + 1;
        temp = quotient;
    end
end

% 初始化元素矩阵
elementMatrix = [];

% 生成元素矩阵
for k = 1: m
    elementMatrix = [elementMatrix, [k*ones(1, m); 1: m]];
end

% 筛选同态态射
for k = 1: n^m
    for element = elementMatrix
        if mapMatrix(k, groupOperate(G, element(1), element(2))) ~= groupOperate(H, mapMatrix(k,
            element(1)), mapMatrix(k, element(2)))
            mapMatrix(k, :) = zeros(1, m);
            break
        end
    end
end
end
```



```

% 删除非同态态射
mapMatrix = mapMatrix(any(mapMatrix, 2), :);

end

```

Listing A.21: 群同构态射

```

function mapMatrix = groupIsomorphism(G, H)

% 名称: 群同构态射
% 输入: 群G和H
% 输出:  $G \rightarrow H$ 的同构态射
% 其中每一行代表一个态射, 第j列代表j在该态射下的像

%% 函数

% 定义群的阶
m = size(G, 1);
n = size(H, 1);

if m == n

    % 计算 $G \rightarrow H$ 的同态态射
    mapMatrix = groupHomomorphism(G, H);

    % 定义目标排列
    permutation = 1: m;

    % 初始化一个逻辑向量, 用于标记符合条件的行
    is_permutation = false(size(mapMatrix, 1), 1);

    % 遍历每一行
    for k = 1: size(mapMatrix, 1)
        % 判断是否是目标排列
        if isequal(sort(mapMatrix(k, :)), permutation)
            is_permutation(k) = true;
        end
    end

    % 从矩阵中选择符合条件的行
    mapMatrix = mapMatrix(is_permutation, :);

else
    mapMatrix = [];
end

end

```

Listing A.22: 是否为交换群

```
function judge = isCommutativeGroup(group)

% 名称: 判断是否为交换群
% 输入: 群运算表
% 输出: 若可交换, 则输出1; 否则, 输出0

judge = all(all(group == group'));

end
```

Listing A.23: 是否为单群

```
function judge = isSimpleGroup(group)

% 名称: 判断是否为单群
% 输入: 群运算表
% 输出: 若为单群, 则输出1; 否则, 输出0

%% 函数
if size(group, 1) == 1
    judge = 1;
else
    normalSubgroupMatrix = normalSubgroup(group);
    judge = size(normalSubgroupMatrix, 1) == 2;
end

end
```

Listing A.24: 是否为可解群

```
function judge = isSolvableGroup(group)

% 名称: 判断是否为可解群
% 输入: 群运算表
% 输出: 若为可解群, 则输出1; 否则, 输出0

%% 函数
order = size(group, 1);
elementMatrix = 1: order;
m = 1;
n = 0;
while m ~= n
    m = size(elementMatrix, 2);
    elementMatrix = commutatorGroup(group, elementMatrix);
    n = size(elementMatrix, 2);
end
if m == 1
    judge = 1;
else
```

```

        judge = 0;
    end

end

```

Listing A.25: 群的直积

```

function [element, group, order] = directProductOfGroups(G, H)

% 名称: 群的直积
% 输入: 群G和H
% 输出: 1.群元素element; 2.群运算表group; 3.群阶order
% 说明: 以element表中元素的位置建立与元素间的双射
%       如下出现的数字均代表元素的位置, 不代表真实元素
%       element为order行2列矩阵
%       其中element(k)代表第k个元素
%       element的行向量(i,j)代表G的第i个元素与H的第j个元素
%       group(i,j)=element(i) * element(j)

%% 1.群阶
m = size(G, 1);
n = size(H, 1);
order = m * n;

%% 2.群元素
element = zeros(order, 2);
for k = 1: order
    element(k, 1) = ceil(k / n);
    element(k, 2) = k - n * (ceil(k / n)-1);
end

%% 3.群运算表
group = zeros(order, order);

for i = 1: order
    for j = 1: order
        group(i, j) = ...
            n * (G(element(i, 1), element(j, 1)) - 1) ...
            + H(element(i, 2), element(j, 2));
    end
end

end

```

A.4 辅助函数

Listing A.26: Euler 函数

```

function [N, Matrix] = EulerFunction(n)

% 生成 1 到 n-1 的矩阵
numbers = 1: n-1;

% 计算每个数与 n 的最大公约数
gcdMatrix = gcd(numbers, n);

% 使用逻辑索引找到与 n 互素的数
coprime = numbers(gcdMatrix == 1);

% 将结果转换为矩阵
Matrix = reshape(coprime, 1, []);

% 计算元素个数
N = size(Matrix, 2);

end

```

Listing A.27: 全排列

```

function permutation = fullPermutation(n)

% 名称: 全排列
% 输入: n
% 输出: n! 行 n 列矩阵, 每一行为一个全排列

%%

if n == 1
    permutation = 1;
else
    sub_permutations = fullPermutation(n - 1);
    m = size(sub_permutations, 1);
    permutation = zeros(m * n, n);
    for i = 1: m
        for j = 1: n
            permutation((i - 1) * n + j, :) = [sub_permutations(i, 1:j-1), n, sub_permutations(i, j:end)];
        end
    end
end

end

end

```

Listing A.28: 组合矩阵

```

function combinations = generateCombinations(k, n)

% 生成组合矩阵的函数

```

```

% 输入: 组合大小k, 元素总数n
% 输出: 一个C_n~k行, k列矩阵, 包含所有可能的组合

%% 函数1
% 生成所有可能的组合
combinations = cell2mat(arrayfun(@(x) nchoosek(1:n, x), k, 'UniformOutput', false));

%% 函数2

% 初始化组合矩阵为空
combinations = [];
% 初始化当前组合为空
currentCombination = [];
% 调用递归函数来生成组合
generate(1, k, n, currentCombination);

% 递归函数, 生成所有可能的组合
% 输入参数:
%   - start: 当前迭代的起始元素
%   - k: 剩余要选择的元素数量
%   - n: 候选元素的总数
%   - currentCombination: 当前的组合
function generate(start, k, n, currentCombination)
    % 当剩余要选择的元素数量为0时, 表示已经生成一个组合
    if k == 0
        % 将当前组合添加到组合矩阵中
        combinations = [combinations; currentCombination];
        return;
    end

    % 遍历候选元素, 生成组合
    for i = start:n
        % 递归调用generate函数, 继续生成组合
        generate(i+1, k-1, n, [currentCombination, i]);
    end
end

end

```