

群论笔记 Chapter 1: 基础概念与结构

整理自手写笔记 P1-P18

2025 年 11 月 23 日

目录

1 群的定义与基本性质 (Groups: Definition & Basics)	3
2 子群 (Subgroups) 与生成元	4
2.1 子群定义	4
2.2 生成子群 (Generated Subgroup)	4
2.3 整数群 \mathbb{Z} 的子群结构	5
3 阶与循环群 (Order & Cyclic Groups)	5
3.1 元素的阶 (Order of an Element)	5
3.2 循环群 (Cyclic Groups)	6
4 拉格朗日定理 (Lagrange's Theorem)	6
4.1 定理与证明	6
4.2 数论应用详解: 欧拉定理 (Euler's Theorem)	7
5 典型群案例: D_n 与 S_n	8
5.1 二面体群 D_n (Dihedral Groups)	9
5.2 全对称群 S_n (Symmetric Groups)	9

6 群作用 (Group Action)	9
7 正规子群与共轭 (Normal Subgroups)	10
7.1 左陪集与商集	10
7.2 正规子群 (Normal Subgroups)	10
7.3 共轭作用与自同构	10

1 群的定义与基本性质 (Groups: Definition & Basics)

群的公理化定义

定义 (群 Group). 设 G 是一个非空集合, $*$ 是定义在 G 上的一个二元运算 (即 $G \times G \rightarrow G$ 的映射)。如果 $(G, *)$ 满足以下四个公理, 则称 $(G, *)$ 为一个群:

1. 封闭性 (*Closure*): 对于任意 $a, b \in G$, 都有 $a * b \in G$ 。
2. 结合律 (*Associativity*): 对于任意 $a, b, c \in G$, 都有 $(a * b) * c = a * (b * c)$ 。
3. 存在单位元 (*Identity Element*): 存在一个元素 $e \in G$, 使得对于任意 $a \in G$, 都有:

$$a * e = e * a = a$$

(注: 群的单位元是唯一的)

4. 存在逆元 (*Inverse Element*): 对于任意 $a \in G$, 都存在一个元素 $b \in G$ (记作 a^{-1}), 使得:

$$a * b = b * a = e$$

(注: 每个元素的逆元是唯一的)

术语百科 (Terminology)

阿贝尔群 (Abelian Group) / 交换群: 若群 G 还满足 交换律 (Commutativity), 即对于任意 $a, b \in G$, 都有:

$$a * b = b * a$$

则称 G 为阿贝尔群。

NOTE: 群的阶

群的阶 (Order of a Group): 群 G 中元素的个数称为群的阶, 记作 $|G|$ 。

- 若 $|G| < \infty$, 称为有限群。
- 若 $|G| = \infty$, 称为无限群。

2 子群 (Subgroups) 与生成元

子群的判定与构造

2.1 子群定义

设 $(G, e, *)$ 是一个群。若 H 是 G 的非空子集 ($H \subseteq G$)，且满足以下三个条件，则称 H 为 G 的子群，记作 $H \leq G$:

1. $e \in H$ (单位元在 H 中)
2. $\forall a, b \in H \Rightarrow a * b \in H$ (运算封闭)
3. $\forall a \in H \Rightarrow a^{-1} \in H$ (逆元封闭)

例 (常见子群链). 数系的加法群链:

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$$

例 (线性群 Linear Groups). • $GL_n(\mathbb{R})$: 一般线性群 (可逆矩阵)。

- $SL_n(\mathbb{R})$: 特殊线性群 ($\det = 1$)。
- $O(n)$: 正交群 (保范数变换)。
- $SO(n)$: 特殊正交群 (旋转群)。
- 关系: $SO(n) \leq O(n) \leq GL_n(\mathbb{R})$ 。

2.2 生成子群 (Generated Subgroup)

设 $S \subseteq G$ 为群的子集，由 S 生成的子群记为 $\langle S \rangle$ 。

$$\langle S \rangle = \{\beta_1 \beta_2 \cdots \beta_r \mid \beta_i \in S \text{ or } \beta_i^{-1} \in S, r \in \mathbb{N}\}$$

这等价于包含 S 的最小子群，也是所有包含 S 的子群的交集。

2.3 整数群 \mathbb{Z} 的子群结构

这是一个经典的群论结论，刻画了循环群 \mathbb{Z} 的所有理想/子群形式。

定理. 整数加法群 \mathbb{Z} 的任意子群 I 都形如 $n\mathbb{Z}$ (其中 $n \in \mathbb{N}$)。即 \mathbb{Z} 是主理想环。

证明. 设 $I \subseteq \mathbb{Z}$ 是一个子群。

- 若 $I = \{0\}$, 则取 $n = 0$, 结论成立。
- 若 $I \neq \{0\}$, 则 I 中必含有非零整数。因 I 包含逆元, 故 I 中必有正整数。设 a 为 I 中最小的正整数。
 1. 证明 $a\mathbb{Z} \subseteq I$: 由于 $a \in I$, 根据封闭性, 对于任意 $k \in \mathbb{Z}$, $ka \in I$ 。故 $a\mathbb{Z} \subseteq I$ 。
 2. 证明 $I \subseteq a\mathbb{Z}$: 任取 $x \in I$ 。由带余除法, 存在 $q, r \in \mathbb{Z}$ 使得:

$$x = qa + r, \quad 0 \leq r < a$$

移项得 $r = x - qa$ 。因为 $x \in I$ 且 $a \in I \Rightarrow qa \in I$, 由子群性质知 $r \in I$ 。

由于 $r \in I$ 且 $0 \leq r < a$, 而 a 是 I 中最小的正整数:

– 必须有 $r = 0$ 。

因此 $x = qa$, 即 $x \in a\mathbb{Z}$ 。

综上, $I = a\mathbb{Z}$ 。 □

3 阶与循环群 (Order & Cyclic Groups)

衡 量 元 素 与 群 的 “大 小”

3.1 元素的阶 (Order of an Element)

设 $a \in G$ 。

定义. 元素 a 的阶 $|a|$ 定义为满足 $a^n = e$ 的最小正整数 n 。若不存在这样的 n , 则称 a 为无限阶元素。

重要性质: 若 $a^m = e$, 则 $|a|$ 整除 m ($|a| \mid m$)。

3.2 循环群 (Cyclic Groups)

若群 G 由单个元素生成，即 $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ ，则称 G 为循环群。

类型	符号与同构	备注
无限循环群	$C_\infty \cong (\mathbb{Z}, +)$	生成元为 1 或 -1
有限循环群 (n 阶)	$C_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$	模 n 加法群

表 1: 循环群的分类

直观理解: C_n 的子群唯一性

对于 n 阶有限循环群 $C_n = \langle a \rangle$ ，其子群结构非常完美：对于 n 的每一个正因子 d ($d \mid n$)，存在且仅存在一个阶为 d 的子群。该子群由 $a^{n/d}$ 生成。

4 拉格朗日定理 (Lagrange's Theorem)

有限群论的基石

4.1 定理与证明

定理 (拉格朗日定理). 设 G 是有限群， H 是 G 的子群。则 H 的阶整除 G 的阶，即：

$$|H| \mid |G|$$

且 $|G| = [G : H] \cdot |H|$ ，其中 $[G : H]$ 是 H 在 G 中的指数（左陪集的个数）。

基于陪集的证明. 定义左陪集 $aH = \{ah \mid h \in H\}$ 。

1. 建立双射：映射 $f : H \rightarrow aH$ ($h \mapsto ah$) 是双射，故所有陪集的大小相等，均为 $|H|$ 。
2. 构成划分：定义等价关系 $a \sim b \iff a^{-1}b \in H$ 。等价类即为左陪集。群 G 被划分为 k 个互不相交的陪集之并：

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

3. 计数： $|G| = \sum_{i=1}^k |a_iH| = k \cdot |H|$ 。

□

4.2 数论应用详解：欧拉定理 (Euler's Theorem)

为了利用群论证明欧拉定理，我们首先需要引入描述群“大小”的数论函数。

定义 (欧拉函数 Euler's Totient Function). 设 n 为正整数。欧拉函数 $\phi(n)$ 定义为小于等于 n 的正整数中与 n 互质的数的个数。即：

$$\phi(n) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq n, \gcd(k, n) = 1\}|$$

例子：

- 若 $n = p$ (素数)，则 $1, \dots, p - 1$ 都与 p 互质，故 $\phi(p) = p - 1$ 。
- 若 $n = 10$ ，与 10 互质的数为 $\{1, 3, 7, 9\}$ ，故 $\phi(10) = 4$ 。

关键构造：模 n 乘法群

考虑模 n 的剩余类环 $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$ 。我们需要从中提取出一个关于乘法构成群的子集。

定义集合 G 为 $\mathbb{Z}/n\mathbb{Z}$ 中所有可逆元 (单位元) 组成的集合：

$$G = (\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$$

- 群的阶：根据 $\phi(n)$ 的定义，显然有 $|G| = \phi(n)$ 。
- 封闭性：若 $\gcd(a, n) = 1, \gcd(b, n) = 1$ ，则 $\gcd(ab, n) = 1$ ，故封闭。
- 单位元： $\bar{1} \in G$ 。
- 逆元：由贝祖等式，若 $\gcd(a, n) = 1$ ，存在 x, y 使 $ax + ny = 1$ ，即 $ax \equiv 1 \pmod{n}$ ，故 \bar{a} 存在逆元 \bar{x} 。

结论： $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ 是一个阶为 $\phi(n)$ 的有限阿贝尔群。

欧拉定理的证明

定理 (欧拉定理 Euler's Theorem). 设 $n \in \mathbb{Z}^+$ ，对于任意整数 a ，若 $\gcd(a, n) = 1$ ，则：

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

基于拉格朗日定理的证明。步骤 1：转化为群语言因为 $\gcd(a, n) = 1$ ，所以 a 在模 n 下对应的剩余类 \bar{a} 属于群 $G = (\mathbb{Z}/n\mathbb{Z})^\times$ 。回顾群 G 的阶为 $|G| = \phi(n)$ ，单位元为 $e = \bar{1}$ 。

步骤 2：考虑元素的阶设 \bar{a} 在群 G 中的阶为 k 。根据元素的阶的定义， k 是满足 $\bar{a}^k = \bar{1}$ 的最小正整数。

步骤 3：应用拉格朗日定理推论根据拉格朗日定理的推论 (Lagrange's Corollary)：在有限群中，任意元素的阶整除群的阶。

$$k \mid |G| \implies k \mid \phi(n)$$

这意味着存在整数 m ，使得 $\phi(n) = k \cdot m$ 。

步骤 4：计算幂次在群 G 中进行运算：

$$\bar{a}^{\phi(n)} = \bar{a}^{k \cdot m} = (\bar{a}^k)^m$$

因为 $\bar{a}^k = \bar{1}$ (阶的定义)，所以：

$$(\bar{a}^k)^m = (\bar{1})^m = \bar{1}$$

步骤 5：还原为同余式上述群方程 $\bar{a}^{\phi(n)} = \bar{1}$ 在数论语言中即表示：

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

证毕。 □

NOTE: 费马小定理作为特例

当 $n = p$ (素数) 时：

1. $\phi(p) = p - 1$ 。
2. 若 $p \nmid a$ ，则 $\gcd(a, p) = 1$ 。
3. 代入欧拉定理公式直接得到： $a^{p-1} \equiv 1 \pmod{p}$ 。

5 典型群案例： D_n 与 S_n

具体的非交换群实例

5.1 深度解析：二面体群 D_n (Dihedral Groups)

二面体群 D_n 是正 n 边形 ($n \geq 3$) 的全特对称群。它是理解非交换群结构的最佳入门模型。

5.1.1 1. 生成元与定义关系 (Generators & Relations)

D_n 的 $2n$ 个元素可以完全由两个核心变换生成：

- 旋转 (Rotation) r : 绕中心逆时针旋转 $2\pi/n$ 。
- 反射 (Reflection) s : 关于某条固定对称轴的翻转。

群的展示 (Presentation) 为：

$$D_n = \langle r, s \mid r^n = e, \quad s^2 = e, \quad srs = r^{-1} \rangle$$

直观理解：核心运算规则： s 是“开关”

D_n 非交换的本质在于关系式 $srs = r^{-1}$ ，它通常变形为以下两种交换规则，用于化简运算：

1. 右交换律： $sr = r^{-1}s$ (或 $sr = r^{n-1}s$)
2. 左交换律： $rs = sr^{-1}$

直观口诀：只要 s 从 r 的左边跳到右边 (或反之)， r 的指数就要变符号 (取逆)。

5.1.2 2. 元素的标准型 (Standard Form)

利用上述交换规则，任何复杂的乘积都可以化简为以下形式之一：

- 旋转型： r^k (其中 $0 \leq k < n$) ——共 n 个。
- 反射型： sr^k (其中 $0 \leq k < n$) ——共 n 个。

集合表示： $D_n = \{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$ 。

特性	D_3 (正三角形)	D_4 (正方形)
阶 (Order)	$2 \times 3 = 6$	$2 \times 4 = 8$
同构	$\cong S_3$ (全对称群)	不同构于 S_4 (它是 S_4 的子群)
中心 $Z(G)$	$\{e\}$ (无非平凡中心)	$\{e, r^2\}$ (旋转 180° 与所有元素交换)
几何意义	3 个旋转 + 3 个中线反射	4 个旋转 + 2 个对角线反射 + 2 个对边中线反射

表 2: D_3 与 D_4 的结构对比

5.1.3 3. 实例对比: D_3 vs D_4

5.1.4 4. 运算实战演练

例题: 在 D_4 中, 计算 $x = (sr)(sr^3)$ 。

解:

$$\begin{aligned}
 x &= s \cdot (r \cdot s) \cdot r^3 && (\text{结合律}) \\
 &= s \cdot (sr^{-1}) \cdot r^3 && (\text{利用 } rs = sr^{-1} \text{ 交换}) \\
 &= s^2 \cdot r^{-1} \cdot r^3 && (\text{结合 } s^2) \\
 &= e \cdot r^2 && (\text{利用 } s^2 = e) \\
 &= r^2
 \end{aligned}$$

几何解释: 先沿轴翻转再转 270°, 然后再沿轴翻转再转 90°, 最终效果等于旋转 180°。

NOTE: 注意

在矩阵表示中, r 对应旋转矩阵, s 对应反射矩阵 (如 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$)。此时行列式 $\det(s) = -1$, $\det(r) = 1$ 。这也是为什么 s 的出现会改变旋转方向 (r 变 r^{-1}) 的代数原因。

5.2 全对称群 S_n (Symmetric Groups)

- 定义: 集合 $\{1, \dots, n\}$ 上所有双射 (置换) 构成的群。
- 阶: $|S_n| = n!$ 。

- 重要子群：交错群 A_n ，由所有偶置换组成。

$$|A_n| = \frac{n!}{2}, \quad A_n \trianglelefteq S_n$$

术语百科 (Terminology)

凯莱定理 (Cayley's Theorem): 任何群 G 都同构于某个对称群 $S(X)$ 的子群。(群本质上是变换群)

6 群作用 (Group Action)

群与外部集合的交互

定义。群 G 在集合 X 上的作用是一个映射 $G \times X \rightarrow X$ (记为 $g \cdot x$)，满足：

1. 单位元： $e \cdot x = x, \forall x \in X$ 。
2. 结合律、相容性： $(a * b) \cdot x = a \cdot (b \cdot x)$ 。

NOTE: 同态观点

群 G 在 X 上的作用等价于一个群同态 $\rho : G \rightarrow S(X)$ ，其中 $\rho(g)$ 是 X 上的一个置换。

7 陪集分解与自同构结构 (Coset Decomposition & Automorphism Structure)

从集合划分到群的结构

7.1 左乘作用与陪集划分 (Left Cosets & Partition)

我们将子群的概念与“群作用”结合，研究群 G 自身的内部结构。

7.1.1 1. 左乘作用 (Left Multiplication Action)

设 H 是 G 的一个子群。我们可以让群 H 作用在群 G 上。定义作用 $\lambda : H \times G \rightarrow G$ 为：

$$h \cdot g = hg \quad (\text{左乘})$$

或者更常见地，考虑 H 作用在 G 上的左陪集构造。

7.1.2 2. 左陪集的定义

对于任意 $a \in G$, 由 a 确定的 H 的左陪集 (Left Coset) 定义为：

$$aH = \{ah \mid h \in H\}$$

这里, a 称为该陪集的代表元 (Representative)。

7.1.3 3. 右陪集 (Right Cosets)

同理, 定义 H 的右陪集为：

$$Ha = \{ha \mid h \in H\}$$

NOTE: 左右陪集的区别

一般情况下, 左陪集不等于右陪集 ($aH \neq Ha$)。

- 若 G 是阿贝尔群, 则显然 $aH = Ha$ 。
- 若 $aH = Ha$ 对所有 a 成立, 这将引出正规子群的概念。

7.1.4 4. 陪集构成的划分 (Partition by Cosets)

这是群论中最基础的结构定理之一。左陪集并不是随意重叠的集合, 它们完美地将 G 切分。

定义 G 上的关系 \sim_L :

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

这是一个等价关系 (满足自反、对称、传递)。因此, 等价类 $[a]$ 正是左陪集 aH 。

命题 (划分性质). 群 G 是其所有左陪集的不相交并集 (Disjoint Union):

$$G = \bigsqcup_{a \in I} aH$$

其中 I 是代表元的集合。这意味着:

1. 任意两个陪集要么完全相等，要么互不相交 ($aH = bH$ 或 $aH \cap bH = \emptyset$)。
2. 每个元素 $g \in G$ 恰好属于一个左陪集。

直观理解：回顾：拉格朗日定理的基础

Recall Lagrange's Theorem: 正是基于上述“不相交划分”的性质，我们才能断言：

$$|G| = (\text{陪集的个数}) \times (\text{每个陪集的大小})$$

即 $|G| = [G : H] \cdot |H|$ 。若没有陪集划分的互不相交和等势（大小相等）性质，拉格朗日定理将不复存在。

7.2 正规子群 (Normal Subgroups)

当左陪集与右陪集重合时，产生了一类特殊的子群。

定义 (正规子群). 设 $N \leq G$ 。若对于任意 $g \in G$ ，都有 $gN = Ng$ ，则称 N 为 G 的正规子群，记作 $N \trianglelefteq G$ 。

等价判定条件：

1. $gN = Ng$
2. $gNg^{-1} = N$ (对共轭作用封闭)
3. $\forall n \in N, \forall g \in G \Rightarrow gng^{-1} \in N$

7.3 自同构与结构链 (Automorphisms & The Structure Chain)

我们深入研究从群 G 到自身的映射，这揭示了群的对称性。

7.3.1 1. 自同构群 $\text{Aut}(G)$

令 $\text{Aut}(G)$ 表示 G 到 G 的所有群同构 (Isomorphisms) 组成的集合。

$$\text{Aut}(G) = \{\sigma : G \rightarrow G \mid \sigma \text{ is bijective and homomorphic}\}$$

$\text{Aut}(G)$ 在映射复合运算下构成一个群。显然，它是全变换群 $S(G)$ 的子群。

7.3.2 2. 内自同构 $\text{Inn}(G)$

由共轭作用诱导的同构。对于固定的 $a \in G$, 定义映射 $\phi_a : G \rightarrow G$ 为:

$$\phi_a(x) = axa^{-1}$$

- ϕ_a 是一个自同构 (保持运算, 且是双射)。
- 所有此类映射的集合称为内自同构群, 记为 $\text{Inn}(G)$ 。

7.3.3 3. 正规结构链 (The Normal Chain)

我们有以下重要的群包含链:

$$\text{Inn}(G) \trianglelefteq \text{Aut}(G) \leq S(G)$$

关键证明: 为什么 $\text{Inn}(G)$ 是 $\text{Aut}(G)$ 的正规子群? . 设 $\sigma \in \text{Aut}(G)$ 是任意自同构, $\phi_a \in \text{Inn}(G)$ 是由 a 诱导的内自同构。我们需要证明 $\sigma \circ \phi_a \circ \sigma^{-1}$ 仍然是一个内自同构。

对于任意 $x \in G$:

$$\begin{aligned} (\sigma \circ \phi_a \circ \sigma^{-1})(x) &= \sigma(\phi_a(\sigma^{-1}(x))) \\ &= \sigma(a \cdot \sigma^{-1}(x) \cdot a^{-1}) \quad (\text{展开内自同构}) \\ &= \sigma(a) \cdot \sigma(\sigma^{-1}(x)) \cdot \sigma(a^{-1}) \quad (\sigma \text{ 是同态}) \\ &= \sigma(a) \cdot x \cdot (\sigma(a))^{-1} \end{aligned}$$

观察结果, 这正是由元素 $\sigma(a)$ 诱导的内自同构! 即:

$$\sigma \circ \phi_a \circ \sigma^{-1} = \phi_{\sigma(a)} \in \text{Inn}(G)$$

因此, $\text{Inn}(G)$ 对 $\text{Aut}(G)$ 的共轭作用封闭, 故 $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. \square

NOTE: 群论中心 $Z(G)$ 的联系

存在群同态 $G \rightarrow \text{Aut}(G)$ ($a \mapsto \phi_a$)。其核 (Kernel) 是群的中心 $Z(G)$, 像 (Image) 是 $\text{Inn}(G)$ 。由同态基本定理可得:

$$G/Z(G) \cong \text{Inn}(G)$$

直观理解：群论哲学

Action comes first, Group comes after. 群的本质在于作用。正规子群本质上是共轭作用下的不变子群。