



离散数学

大连理工大学软件学院

陈志奎 博士、教授、博士生导师

办公室：综合楼405，Tel: 62274392
实验室：综合楼一楼，教学楼A502/C109，

Mobile: 13478461921
Email: zkchen@dlut.edu.cn
zkchen00@hotmail.com
QQ: 1062258606



离散数学

第七章 群环域



回 顾



- 群的定义
- 群的性质
- 子群的定义
- 子群的判定定理

子群的性质
生成子群
中心 C
子群的交
子群格



主要内容

- 子群的陪集，拉格朗日定理
- 循环群定义及性质
 - 生成元、 n 阶循环群、无限循环群
- 置换群定义及性质
- 群的同态与同构
 - 群同态映射：单一同态、满同态、群同构映射
- 环的概念与性质
- 域的概念
- 应用：群与网络安全

7.3.4 子群的陪集分解：陪集

- **定义7.17** 令 $\langle H, \odot \rangle$ 是群 $\langle G, \odot \rangle$ 的子群且 $a \in G$ ，则把下面集合：

$$a \odot H = \{a \odot h \mid h \in H\}$$

称为由元素 a 所确定的群 $\langle G, \odot \rangle$ 中的 H 的左陪集，或简称为**左陪集**，并简记 **aH** 。此外，称 a 是左陪集 **aH** 的**代表元素**。

类似地可定义由 a 所确定群 $\langle G, \odot \rangle$ 中的 H 的右陪集 **Ha** 。

显然，若 $\langle G, \odot \rangle$ 是Abel群，并且 $\langle H, \odot \rangle$ 是其子群，则 **$aH = Ha$** ，即任意元素的左陪集等于其右陪集。

7.3.4 子群的陪集分解：陪集

- **定义7.18** 给定群 $\langle G, \odot \rangle$ ，子群 $\langle H, \odot \rangle$ 的左陪集关系，记作 C_H ，其定义为：

$$C_H: = \{ \langle a, b \rangle \mid a, b \in G \wedge b^{-1} \odot a \in H \}$$

由此定义不难得到：

$$a C_H b \Leftrightarrow a, b \in G \wedge b^{-1} \odot a \in H$$

可以指出，子群 $\langle H, \odot \rangle$ 的左陪集关系是群 $\langle G, \odot \rangle$ 中的一种等价关系。

(证明在下一页)



• **证明：** 由于 $a^{-1} \odot a = e \in H$ ，则 $a C_H a$ ，即有自反性。

若 $a C_H b$ ，则 $b^{-1} \odot a \in H$ ，

于是 $a^{-1} \odot b = ((a^{-1} \odot b)^{-1})^{-1} = (b^{-1} \odot a)^{-1} \in H$ ，故 $b C_H a$ ，
因而满足对称性。

若 $a C_H b$ 且 $b C_H c$ ，则 $b^{-1} \odot a \in H$ 和 $c^{-1} \odot b \in H$ ，所以

$$c^{-1} \odot a = (c^{-1} \odot b) \odot (b^{-1} \odot a) \in H$$

故有 $a C_H c$ ，因而满足传递性。

显然，左陪集关系能把集合 \mathbf{G} 划分成等价类。



若 $a \in G$, 则

$$\begin{aligned} [a] &= \{b \mid b C_H a\} = \{b \mid \langle b, a \rangle \in C_H\} \\ &= \{b \mid a^{-1} \odot b \in H\} = \{b \mid a^{-1} \odot b = h, h \in H\} \\ &= \{b \mid b = a \odot h, h \in H\} \\ &= \{a \odot h \mid h \in H\} = aH \end{aligned}$$

其中 $h = a^{-1} \odot b$ 。

可见, 由元素 a 所确定群 $\langle G, \odot \rangle$ 中的 H 的左陪集 aH 与子群 $\langle H, \odot \rangle$ 的左陪集关系 C_H 所确定的等价类 $[a]_{C_H}$ 是完全相同的, 即 $aH = [a]_{C_H}$ 。

对于右陪集关系可类似地讨论。

7.3.4 子群的陪集分解：陪集

- 例7.24

(1) 设 $G = \{e, a, b, c\}$ 是Klein四元群, $H = \langle a \rangle$ 是 G 的子群.

H 所有的右陪集是:

$$He = \{e, a\} = H, \quad Ha = \{a, e\} = H,$$

$$Hb = \{b, c\}, \quad Hc = \{c, b\}$$

不同的右陪集只有两个, 即 H 和 $\{b, c\}$.

7.3.4 子群的陪集分解：陪集

(2) 设 $A=\{1,2,3\}$, f_1, f_2, \dots, f_6 是 A 上的双射函数. 其中

$$f_1=\{<1,1>, <2,2>, <3,3>\}, \quad f_2=\{<1,2>, <2,1>, <3,3>\}$$

$$f_3=\{<1,3>, <2,2>, <3,1>\}, \quad f_4=\{<1,1>, <2,3>, <3,2>\}$$

$$f_5=\{<1,2>, <2,3>, <3,1>\}, \quad f_6=\{<1,3>, <2,1>, <3,2>\}$$

令 $G = \{f_1, f_2, \dots, f_6\}$, 则 G 关于函数的复合运算构成群. 考虑 G 的子群 $H=\{f_1, f_2\}$. 做出 H 的全体右陪集如下:

$$Hf_1=\{f_1 \circ f_1, f_2 \circ f_1\}=H, \quad Hf_2=\{f_1 \circ f_2, f_2 \circ f_2\}=H$$

$$Hf_3=\{f_1 \circ f_3, f_2 \circ f_3\}=\{f_3, f_5\}, \quad Hf_5=\{f_1 \circ f_5, f_2 \circ f_5\}=\{f_5, f_3\}$$

$$Hf_4=\{f_1 \circ f_4, f_2 \circ f_4\}=\{f_4, f_6\}, \quad Hf_6=\{f_1 \circ f_6, f_2 \circ f_6\}=\{f_6, f_4\}$$

结论: $Hf_1=Hf_2, \quad Hf_3=Hf_5, \quad Hf_4=Hf_6.$

7.3.4 子群的陪集分解：陪集的性质

• **定理7.15** 设 H 是群 G 的子群，则

(1) $He = H$

(2) $\forall a \in G$ 有 $a \in Ha$

• **证明：**

(1) $He = \{ he \mid h \in H \} = \{ h \mid h \in H \} = H$

(2) 任取 $a \in G$ ，由 $a = ea$ 和 $ea \in Ha$ 得 $a \in Ha$

7.3.4 子群的陪集分解：陪集的性质

• **定理7.16** 设 H 是群 G 的子群，则 $\forall a, b \in G$ 有
$$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$$

• **证明：** 先证 $a \in Hb \Leftrightarrow ab^{-1} \in H$

$$\begin{aligned} a \in Hb &\Leftrightarrow \exists h(h \in H \wedge a = hb) \\ &\Leftrightarrow \exists h(h \in H \wedge ab^{-1} = h) \Leftrightarrow ab^{-1} \in H \end{aligned}$$

再证 $a \in Hb \Leftrightarrow Ha = Hb$.

充分性. 若 $Ha = Hb$ ，由 $a \in Ha$ 可知必有 $a \in Hb$.

必要性. 由 $a \in Hb$ 可知存在 $h \in H$ 使得 $a = hb$ ，即 $b = h^{-1}a$
任取 $h_1a \in Ha$ ，则有

$$h_1a = h_1(hb) = (h_1h)b \in Hb$$

从而得到 $Ha \subseteq Hb$. 反之，任取 $h_1b \in Hb$ ，则有

$$h_1b = h_1(h^{-1}a) = (h_1h^{-1})a \in Ha$$

从而得到 $Hb \subseteq Ha$. 综合上述， $Ha = Hb$ 得证.

7.3.4 子群的陪集分解：陪集的性质

- **定理7.17** 设 H 是群 G 的子群，在 G 上定义二元关系 R ：

$$\forall a, b \in G, \langle a, b \rangle \in R \Leftrightarrow ab^{-1} \in H$$

则 R 是 G 上的等价关系，且 $[a]_R = Ha$.

- **证明：**先证明 R 为 G 上的等价关系.

自反性. 任取 $a \in G$, $aa^{-1} = e \in H \Leftrightarrow \langle a, a \rangle \in R$

对称性. 任取 $a, b \in G$, 则

$$\langle a, b \rangle \in R \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow \langle b, a \rangle \in R$$

传递性. 任取 $a, b, c \in G$, 则

$$\begin{aligned} \langle a, b \rangle \in R \wedge \langle b, c \rangle \in R &\Rightarrow ab^{-1} \in H \wedge bc^{-1} \in H \\ &\Rightarrow ac^{-1} \in H \Rightarrow \langle a, c \rangle \in R \end{aligned}$$

下面证明: $\forall a \in G, [a]_R = Ha$. 任取 $b \in G$,

$$b \in [a]_R \Leftrightarrow \langle a, b \rangle \in R \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb \Leftrightarrow b \in Ha$$

7.3.4 子群的陪集分解：推论

• **推论** 设 H 是群 G 的子群, 则

(1) $\forall a, b \in G, Ha = Hb$ 或 $Ha \cap Hb = \emptyset$

(2) $\cup \{Ha \mid a \in G\} = G$

• **证明：**由等价类性质可得.

• **定理7.18** 设 H 是群 G 的子群, 则

$$\forall a \in G, H \approx aH(\text{等势})$$

• **证明：**令 $f \in (aH)^H$ 如下:

$f(h) = a \odot h$, 其中 $h \in H$ 则 f 是双射。满射是显然的, 下面再证它是单射。

假定它不是单射, 即 $h_1 \neq h_2$, $h_1, h_2 \in H$, $f(h_1) = f(h_2)$, 也就是 $a \odot h_1 = a \odot h_2$, 则根据群的可约律知 $h_1 = h_2$, 这与 $h_1 \neq h_2$ 矛盾



附：左陪集

设 G 是群， H 是 G 的子群， H 的左陪集，即

$$aH = \{ah \mid h \in H\}, a \in G$$

关于左陪集有下述性质：

(1) $eH = H$

(2) $\forall a \in G, a \in aH$

(3) $\forall a, b \in G, a \in bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH$

(4) 若在 G 上定义二元关系 R ,

$$\forall a, b \in G, \langle a, b \rangle \in R \Leftrightarrow b^{-1}a \in H$$

则 R 是 G 上的等价关系，且 $[a]_R = aH$.

(5) $\forall a \in G, H \approx aH$ (等势)

7.3.5 拉格朗日定理

- **定理7.19(Lagrange)** 如果**G**是一个有限群和**H**是**G**的一个的子群，则

$$[G:H] = \frac{|G|}{|H|}$$

其中|**G**|和|**H**|分别是**G**和**H**的阶数。

- **证明：** 设 $[G:H] = r$, a_1, a_2, \dots, a_r 分别是**H** 的r个右陪集的代表元素，

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_r$$

$$|G| = |Ha_1| + |Ha_2| + \dots + |Ha_r|$$

由 $|Ha_i| = |H|$, $i = 1, 2, \dots, r$, 得

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

7.3.5 拉格朗日定理

- 每一个 G 的子群的阶数（和每一个 G 内元素的阶数）都必须为 $|G|$ 的因子。
- 若对于每个在 G 内的 a , $aH = Ha$, 则 H 称之为正规子群。
每一个指数 2 的子群皆为正规的：左陪集和右陪集都简单地为此一子群和其补集。

7.3.5 拉格朗日定理

- **例7.25** 证明6阶群中必含有3阶元。

- **证明：** 设 G 是6阶群，由拉格朗日定理可知 G 中的元素只能是1阶，2阶3阶或6阶元。

若 G 中含有6阶元，设这6阶元为 a ，则 a^2 是3阶元。

若 G 中不含6阶元，下面证明 G 中必含有3阶元。若不然， G 中只含有1阶和2阶元，即 $\forall a \in G$ ，有 $a^2 = e$ ，可知 G 是Abel群，取 G 中的两个不同的2阶元 a 和 b ，令 $H = \{e, a, b, ab\}$ 易知 H 是 G 的子群，但 $|H| = 4$ ， $|G| = 6$ ，与拉格朗日定理矛盾。

综上所述，6阶群中必含有3阶元。

7.3.6 集合的置换

- **定义7.19** 集合的置换：令 X 是非空有限集合，从 X 到 X 的双射函数，称为集合 X 中的**置换**，并称 $|X|$ 为置换的**阶**。

集合上的所有**置换（双射）**与**复合运算**，构成的代数系统是一个群，称为**对称群**。

由 n 个元素的集合而构成的所有 $n!$ 个 **n 阶置换**的集合 S_n 与复合置换运算 \diamond 构成群 $\langle S_n, \diamond \rangle$ ，它便是 **n 次 $n!$ 阶对称群**。

若 $Q \subseteq P_x = S_{|x|}$ ，则称由 Q 和 \diamond 构成的群 $\langle Q, \diamond \rangle$ 为**置换群**。

集合的置换

- **例7.26** 设 G 是 n 字母的对称群, $G' = \{0,1\}$, $+$ 是如下表定义在 G' 上的运算, 易知 G' 是一个群。 $f: G \rightarrow G'$ 定义如下:
对于 $p \in G$, 有

$$f(p) = \begin{cases} 0, & p \in A_n \text{ (} G \text{中所有偶置换的子群)} \\ 1, & p \notin A_n \end{cases}$$

表

+	0	1
0	0	1
1	1	0

那么 f 是一个同态。



集合的置换

- **定义7.20** 集合 X 是无限的，令 T_x 表示所有从集合 X 到 X 的变换的集合，具有下列性质：

$$(\forall f)(\forall g)(f, g \in T_x \rightarrow f \circ g, g \circ f \in T_x)$$

$$(\forall f)(\forall g)(\forall h)(f, g, h \in T_x, \rightarrow (f \circ g) \circ h = f \circ (g \circ h))$$

$$(\exists id_A)(id_A \in T_x \wedge (\forall f)(f \in T_x \rightarrow id_A \circ f = f \circ id_A = f))$$

$$(\forall f)(f \in T_x \rightarrow (\exists f^{-1})(f^{-1} \in T_x \wedge f \circ f^{-1} = f^{-1} \circ f = id_A))$$

$\langle T_x, \circ \rangle$ 构成群，在代数中称为**变换群**。**置换群**是变换群的特例。



集合的置换

- **定义7.21** 设 p 是集合 $X = \{x_1, x_2, \dots, x_n\}$ 上的 n 阶置换, 若 $p(x_1) = x_2, p(x_2) = x_3, \dots, p(x_{n-1}) = x_n, p(x_n) = x_1$, 并且 X 中其余元素保持不变, 则称 p 为 X 上的 n 阶轮换, 记为 $(x_1 x_2 \cdots x_n)$, 若 $n=2$, 称 p 为 X 上的对换。

由轮换的定义可知, 轮换中任何元素均可排在首位, 他们表示是一个轮换, 如 $(x_1 x_2 \cdots x_n) = (x_i x_{i+1} \cdots x_j)$ 。

- **例7.27** 令 $S = \{1, 2, 3, 4, 5\}$, S 上的5阶置换 $p = \begin{pmatrix} 12345 \\ 24315 \end{pmatrix}$ 是 S 上的3阶轮换 $(1\ 2\ 4)$ 。



7.4 循环群

- **定义7.22** 设 $\langle G, \otimes \rangle$ 是群，若 $\exists a \in G$ ，对 $\forall x \in G, \exists k \in \mathbb{Z}$, 有 $x = a^k$ ，则称 $\langle G, \otimes \rangle$ 是**循环群**，记作 $G = \langle a \rangle$ ，称 a 是群 $\langle G, \otimes \rangle$ 的**生成元**。
- **定义7.23** 若存在 $a \in G$ ，使得 $G = \langle a \rangle$ ，则称 **G** 是**循环群**，称 a 为 **G** 的**生成元**。

7.4.1 循环群

循环群 $G=\langle a \rangle$ 根据生成元 a 的阶可以分为两类： **n 阶循环群**和**无限循环群**。

设 $G=\langle a \rangle$ 是循环群，若 a 是 n 阶元，则

$$G = \{a^0 = e, a^1, \dots, a^{n-1}\}$$

那么 $|G|=n$ ，称 G 为 n 阶循环群。

若 a 是无限阶元，则

$$G = \{a^0 = e, a^{\pm 1}, a^{\pm 2} \dots\}$$

这时称 G 为无限循环群。

7.4.1 循环群

- **定理7.20** 设 $G = \langle a \rangle$ 是循环群。

若 G 是**无限循环群**，则 G 只有**两个**生成元，即 **a 和 a^{-1}** 。

若 G 是 **n 阶循环群**，则 G 含有 **$\varphi(n)$ 个生成元**，对与任何小于 n 且与 n 互素的自然数 r ， a^r 是 G 的生成元。

- **定理7.21**

(1) 设 $G = \langle a \rangle$ 是循环群，则 G 的子群仍是**循环群**。

(2) 若 $G = \langle a \rangle$ 是无限循环群，则 G 的子群**除 $\{e\}$ 以外**都是无限循环群。

(3) 若 $G = \langle a \rangle$ 是 **n 阶循环群**，则对于 **n 的每个正因子 d** ， G 恰好含有一个 **d 阶子群**。

7.4.1 循环群

- **例7.28** 设 G_1 是整数加群, G_2 是模12加群, 求出 G_1 和 G_2 的所有子群。

解: G_1 的生成元为1和-1, 易知 $1^m = m$, $m \in \mathbb{N}$ 。所以 G_1 的子群是 $m\mathbb{Z}$, $m \in \mathbb{N}$ 。即

$$\langle 0 \rangle = \{0\} = 0\mathbb{Z}$$

$$\langle m \rangle = \{mz | z \in \mathbb{Z}\} = m\mathbb{Z}, m > 0$$

G_2 是12阶循环群。

12的正因子是1,2,3,4,6和12, 因此 G_2 的子群是:

$\langle 12 \rangle = \langle 0 \rangle = \{0\}$	1阶子群	$\langle 6 \rangle = \{0, 6\}$	2阶子群
$\langle 4 \rangle = \{0, 4, 8\}$	3阶子群	$\langle 3 \rangle = \{0, 3, 6, 9\}$	4阶子群
$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$	6阶子群	$\langle 1 \rangle = \mathbb{Z}_{12}$	12阶子群 ₂₆

7.4.2 置换群

- **定义7.25** 设 $S = \{1, 2, \dots, n\}$, S 上的任何双射函数 $\sigma: S \rightarrow S$ 称为 S 上的 n 元置换。
- **定义7.26** 设 σ, τ 是 n 元置换, σ, τ 的复合 $\sigma \circ \tau$ 也是 n 元置换, 称为 σ 和 τ 的乘积, 记作 $\sigma\tau$ 。
- **定义7.27** 一个置换群是一个群 G , 其元素是一个给定集 M 的置换, 而其群作用是 G 中的置换 (可以看作是从 M 到自身的双射) 的复合; 其关系经常写作 (G, M) 。注意所有置换的群是对称群; 置换群通常是指对称群的一个子群。



7.4.2 置换群

- n 个元素的置换群记为 S_n ；若 M 是任意有限或无限集合，则所有 M 的置换组成的对称群通常写作 $Sym(M)$ 。
- 设 $S \neq \emptyset$ ， $|S| < +\infty$ ， S 上的一个一一变换被称为置换。当 S 上的某些置换关于乘法运算构成群是，就成它为置换群。
- 若 $|S| = n$ ，设 $\{n = 1, 2, \dots, n\}$ ，其置换全体组成的集合一般表示为 S_n ；经过 n 次恒等变换的群称为 n 次对称群。

7.4.2 置换群

- 例7.24 具体写出三次对称群 S_3 。

解： 设 $S = \{1,2,3\}$ ，于是 $|S_3| = 3! = 6$ ，这6个置换分别是

$$e = \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 123 \\ 213 \end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 123 \\ 231 \end{pmatrix},$$

其运算表在下页。

7.4.2 置换群

运算表

\cdot	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	e	σ_4	σ_5	σ_2	σ_3
σ_2	σ_2	σ_5	e	σ_4	σ_3	σ_1
σ_3	σ_3	σ_4	σ_5	e	σ_1	σ_2
σ_4	σ_4	σ_3	σ_1	σ_2	σ_5	e
σ_5	σ_5	σ_2	σ_3	σ_1	e	σ_4



7.4.2 置换群

由此表可知，**e**为恒等元。

$$\sigma_1^{-1} = \sigma_1, \sigma_2^{-1} = \sigma_2, \sigma_3^{-1} = \sigma_3, \sigma_4^{-1} = \sigma_5, \sigma_5^{-1} = \sigma_4,$$

$$\text{同时, } \sigma_1\sigma_2 = \sigma_4, \sigma_2\sigma_1 = \sigma_5。$$

所以它是不能交换的群。这是一个很典型的**6**（含有**6**个元素）阶的群。

7.5 群的同态与同构

- **定义7.23** 给定群 $\langle G, \odot \rangle$ 和 $\langle H, * \rangle$, 则 $\langle G, \odot \rangle \simeq \langle H, * \rangle$:

$$(\forall g) \left(g \in H^G \wedge (\forall a)(\forall b)(a, b \in G \rightarrow g(a \odot b) = g(a) * g(b)) \right)$$

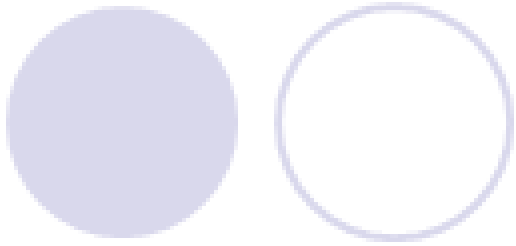
并称 g 为从群 $\langle G, \odot \rangle$ 到群 $\langle H, * \rangle$ 的**群同态映射**。

➤ 群同态保持**幺元**, **逆元**和**子群**。

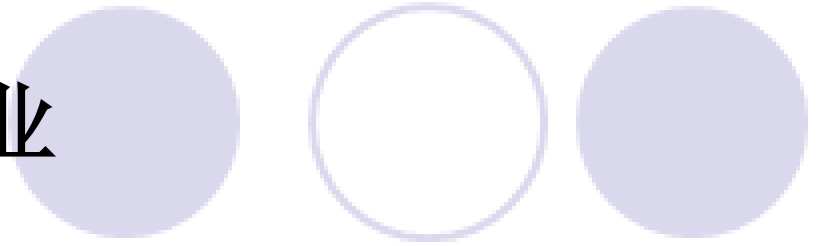
7.5 群的同态与同构

- **定理7.21** 设 g 为从群 $\langle G, \odot \rangle$ 到群 $\langle H, * \rangle$ 的群同态映射, 则
 - (1) 若 e_G 和 e_H 分别为两群的么元, 那么, $g(e_G) = e_H$ 。
 - (2) 若 $a \in G$, 那么, $g(a^{-1}) = (g(a))^{-1}$ 。
 - (3) 若 $\langle S, \odot \rangle$ 是群 $\langle G, \odot \rangle$ 的子群且 $g(S) = \{g(a) \mid a \in S\}$, 那么, $\langle g(S), * \rangle$ 为群 $\langle H, * \rangle$ 的子群。
- **定理7.22** 给定群 $\langle G, \odot \rangle$ 和代数系统 $\langle H, * \rangle$, 若 g 是从群 $\langle G, \odot \rangle$ 到 $\langle H, * \rangle$ 的满同态映射, 则 $\langle H, * \rangle$ 为群。

根据 g 是单射、满射和双射, 群同态分别称为群单一同态映射、群满同态映射和群同构映射。



作 业



- 11-16