



第八章 群 I

计算机系网络所：张小平



主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- 8.4 变换群和置换群 Cayley定理
- 8.5 陪集和群的陪集分解 Lagrange定理
- 8.6 正规子群与商群
- 8.7 群的同态、同态基本定理
- 8.8 群的直积



半群

- 定义8.1.1 设 S 是非空集合, \cdot 是 S 上的一个二元运算, 如果 \cdot 满足结合律, 则代数系统 (S, \cdot) 称为半群

换句话说, 如果对于任意的 $a, b, c \in S$, 若

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 成立, 则称 (S, \cdot) 为半群。



半群

- 例： $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

半群！

- 例： $(R, -)$

$$\forall a, b, c \in R \quad (a - b) - c \neq a - (b - c)$$



半群

- 例： $(M_n(R), \times)$

其中 $M_n(R)$ 是全体 $n \times n$ 实矩阵的集合

$$\forall A, B, C \in M_n(R) \quad (A \times B) \times C = A \times (B \times C)$$

半群！

- 例： 设 $Z_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ 是模 m 同余的等价类集合， \cdot 是 Z_m 上的模 m 加法运算。

$$(Z_m, \cdot)$$

半群！



半群

- 定义8.1.2 若半群 (M, \bullet) 中有单位元 e 存在, 则称 (M, \bullet) 是一个**含幺半群**或简称**幺群**。
幺群有时会用三元组 (M, \bullet, e) 表示, 方便起见, 简称 M 为幺群



半群

- 例: $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

$$\forall a \in R \quad a + 0 = 0 + a = a$$

半群! 么群!



半群

- 例： $(M_n(R), \times)$

其中 $M_n(R)$ 是全体 $n \times n$ 实矩阵的集合

$$\forall A, B, C \in M_n(R) \quad (A \times B) \times C = A \times (B \times C)$$

半群！ 么群！

- 例： 设 $Z_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ ， \bullet 是 Z_m 上的模 m 加法运算。 (Z_m, \bullet) 半群！

$\bar{0}$

么群！



半群

- 定义8.1.3 设 (M, \cdot, e) 是一个么群, 若 \cdot 适合交换律, 则称 M 是交换么群。



半群

- 例： $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

$$\forall a \in R \quad a + 0 = 0 + a = a$$

半群！ 么群！ 交换么群！

- 例： $(M_n(R), \times)$

其中 $M_n(R)$ 是全体 $n \times n$ 实矩阵的集合

$$\forall A, B, C \in M_n(R) \quad (A \times B) \times C = A \times (B \times C)$$

半群！ 么群！ 交换么群？



半群

- 例：设 $Z_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$, \bullet 是 Z_m 上的模 m 加法运算。 (Z_m, \bullet)

半群！

么群！

交换么群！



半群

- 定理8.1.1 如果二元运算 \cdot 适合结合律，那么也适合广义结合律。

— 根据定理显见

$$a^n a^m = a^{n+m} \qquad (a^m)^n = a^{mn}$$

其中定义 $a^0 = e$ ，即M中的单位元。



半群

- 定义8.1.4 设 (M, \cdot, e) 是一个幺群，若存在一个元素 $g \in M$ ，使得对任意 $a \in M$ ， a 都可以写成 g 的方幂形式，即 $a = g^m$ (m 是非负整数)，则称 (M, \cdot, e) 是一个循环幺群，并且称 g 是 M 的一个生成元。



半群

- 例： $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

$$\forall a \in R \quad a + 0 = 0 + a = a$$

半群！ 么群！ 交换群！ 循环么群？

- 例： $(N, +)$

循环么群？



半群

- 例：设 $Z_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$, \bullet 是 Z_m 上的模 m 加法运算。 (Z_m, \bullet)

半群！

么群！

交换么群！

循环么群！



半群

- 定理8.1.2 循环幺群是可交换幺群。

证明：设 g 是循环幺群中的一个生成元，则对任意 $a, b \in M$ ，有 $a = g^m$ ， $b = g^n$ ，($m, n \geq 0$)

由于二元运算适合结合律，因此

$$ab = g^m g^n = g^{m+n} = g^n g^m = ba$$

所以循环幺群是可交换的。

证毕！



半群

- 定义8.1.5 设 (S, \bullet) 是一个半群, $T \subseteq S$, 在运算 \bullet 的作用下如果 T 是封闭的, 则称 (T, \bullet) 是 (S, \bullet) 的子半群。



半群

- 定义8.1.6 设 (M, \cdot, e) 是一个幺群, $T \subseteq M$, 在运算 \cdot 的作用下如果 T 是封闭的, 且 $e \in T$, 则称 (T, \cdot, e) 是 (M, \cdot, e) 的 **子幺群**。



半群

• 定义8.1.7 设 (A, \cdot) 、 $(B, *)$ 是两个半群。

$f: A \rightarrow B$ 是 A 到 B 的映射, $\forall a, b \in A$, 若

$f(a \cdot b) = f(a) * f(b)$ 成立, 则称 f 是从半群 A 到半

群 B 的同态映射, 简称同态。若 f 分别是单

射、满射和双射时, 分称 f 是单同态、满同

态和同构。



半群

- 定理8.1.3 设 f 是从代数系统 (A, \bullet) 到 $(B, *)$ 的满同态, S 是 A 的非空子集。 $f(S)$ 表示 S 中的元素在 f 下的象的集合, 即 $f(S) = \{f(a) \mid a \in S\}$
那么

1. 若 (S, \bullet) 是半群, 则 $(f(S), *)$ 也是半群。
2. 若 (S, \bullet) 是幺群, 则 $(f(S), *)$ 也是幺群。



半群

- 推论：设 f 是从半群 (A, \bullet) 到代数系统 $(B, *)$ 的满同态， (S, \bullet) 是 (A, \bullet) 的子半群。

则有：

1. $(B, *)$ 是半群。
2. $(f(S), *)$ 是 $(B, *)$ 的子半群。

半群、么群、子半群的同态象，仍然是半群、么群、子半群！



主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- 8.4 变换群和置换群 Cayley定理
- 8.5 陪集和群的陪集分解 Lagrange定理
- 8.6 正规子群与商群
- 8.7 群的同态、同态基本定理
- 8.8 群的直积



群、群的基本性质

- 定义8.2.1 设 G 是非空集合， \bullet 是 G 上的二元运算

若代数系统 (G, \bullet) 满足

1. 适合结合律，即 $\forall a, b, c \in G$ ，有 $(ab)c = a(bc)$
2. 存在单位元 e ，使得 $\forall a \in G$ ， $ae = ea = a$
3. G 中的元素都是可逆元。即 $\forall a \in G$ ，都 $\exists a^{-1} \in G$ ，使得

$$aa^{-1} = a^{-1}a = e$$

则称代数系统 (G, \bullet) 是一个群，或记为 (G, \bullet, e) 。



群、群的基本性质

- 定义8.2.2 设 (G, \cdot, e) 是含幺半群, e 是其单位元, 如果 $\forall a \in G$, 都 $\exists a^{-1} \in G$ 。使得

$$aa^{-1} = a^{-1}a = e$$

成立, 则称 G 是一个群。



群、群的基本性质

- 定义8.2.3 若群 G 的二元运算 \cdot 满足交换律，
即 $\forall a, b \in G$, 都有 $ab = ba$
则称 G 是交换群，或阿贝尔(Abel)群。

满足交换律的群是交换群！



群、群的基本性质

• 定理8.2.1 设 G 是一个群，则

1. G 中的单位元唯一。

2. G 中每个元素都有唯一的逆元。

3. 指数律成立：即 $\forall a \in G$ ， m 、 n 是任意整数，有

$$a^m a^n = a^{m+n} \quad , \quad (a^m)^n = a^{mn}$$

4. 若 $ab = ba$ ，则 $(ab)^n = a^n b^n$



群、群的基本性质

- **定理8.2.2** 设半群 (G, \cdot) 有一个左单位元 e ，
且对 $\forall a \in G$ ，都有左逆元 $a^{-1} \in G$ ，
使得 $a^{-1}a = e$ 成立，则 G 是群。



群、群的基本性质

- 证明：因为

$$\begin{aligned} ae &= eae = \left((a^{-1})^{-1} a^{-1} \right) a (a^{-1} a) = (a^{-1})^{-1} (a^{-1} a) (a^{-1} a) \\ &= (a^{-1})^{-1} (ea^{-1}) a = \left((a^{-1})^{-1} a^{-1} \right) a = ea = a \end{aligned}$$

所以 e 也是右单位元。



群、群的基本性质

- 证明（续）：

以下证 a^{-1} 也是 a 的右逆元

设 a' 是 a^{-1} 的左逆元，于是有

$$aa^{-1} = eaa^{-1} = (a'a^{-1})aa^{-1} = a'(a^{-1}a)a^{-1} = (a'e)a^{-1} = a'a^{-1} = e$$

因此 G 是群！



群、群的基本性质

- **定理8.2.2** 设半群 (G, \cdot) 有一个左单位元 e ，
且对 $\forall a \in G$ ，都有左逆元 $a^{-1} \in G$ ，
使得 $a^{-1}a = e$ 成立，则 G 是群。



群、群的基本性质

- **定理8.2.3** 设 (G, \bullet) 是半群, 如果对 G 中任意两个元素 a, b , 方程 $ax=b$ 和 $ya=b$ 在 G 中都有解, 则 G 是一个群。

证明:

$$\because \quad \forall a, b \in G, \quad ya = b \text{ 有解}$$

$$\therefore \quad \forall a \in G, \quad ya = a \text{ 有解, 不妨设某个解为 } e$$



群、群的基本性质

- 证明（续）：

- 对方程 $ax=b$ ，设 x' 是其中的一个解，那么

$$\forall b \in G \quad eb = e(ax') = (ea)x' = ax' = b$$

所以 e 就是左单位元；

- 此外， $\forall a \in G$ ， $ya=e$ 有解 y' ，所以 y' 是 a 的左逆元。

- 由定理8.2.2， G 是群。



群、群的基本性质

- **定理8.2.3** 设 (G, \cdot) 是半群, 如果对 G 中任意两个元素 a, b , 方程 $ax=b$ 和 $ya=b$ 在 G 中都有解, 则 G 是一个群。



群、群的基本性质

- 定理 8.2.4 设 G 是一个群, $\forall a, b \in G$ 恒有:

$$(a^{-1})^{-1} = a, (ab)^{-1} = b^{-1}a^{-1}$$

证明:

$$(a^{-1})^{-1} = (a^{-1})^{-1}e = (a^{-1})^{-1}a^{-1}a = ea = a$$

$$\therefore (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$$

$$\therefore (ab)^{-1} = b^{-1}a^{-1}$$

证毕!





群、群的基本性质

- 定义8.2.4 设 a 是 G 中的一个元素，若有正整数 k 存在，使 $a^k = e$ ，则满足 $a^k = e$ 的最小正整数 k 称为元素 a 的阶(或周期)，记为 $O\langle a \rangle$ ，并称 a 是有限阶元素。



群、群的基本性质

- 例：设 $Z_6 = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$ ， \cdot 是 Z_6 上的模 6 加法运算。 (Z_6, \cdot)

$$O\langle \bar{1} \rangle = 6$$

$$O\langle \bar{3} \rangle = 2$$



群、群的基本性质

- **定理8.2.5** 设 a 是群 G 中的一个 r 阶元素, k 是正整数, 则
 1. $a^k = e$, 当且仅当 $r \mid k$
 2. $O\langle a \rangle = O\langle a^{-1} \rangle$
 3. $r \leq |G|$



群、群的基本性质

- 定义8.2.5 设 H 是群 G 的一个非空子集，若 H 对于 G 的运算仍然构成群，则称 H 是 G 的一个子群，记为 $H \leq G$ 。
 - G ， $\{e\}$ 都是群，称为 G 的平凡子群。
 - 如果 G 的子群 $H \neq G$ ，则称 H 为 G 的真子群，记为 $H < G$



群、群的基本性质

- 定理 8.2.6 H 是 G 的子群的充要条件是：
 1. H 对 G 的乘法运算是封闭的，即 $\forall a, b \in H$ ，都有 $ab \in H$ 。
 2. H 中有单位元 e' ，且 $e' = e$
 3. $\forall a \in H$ ，都有 $a^{-1} \in H$ ，且 a^{-1} 是 a 在 G 中的逆元。



群、群的基本性质

- **定理 8.2.7** G 的非空子集 H 是 G 的子群的充要条件是： $\forall a, b \in H$, 都有 $ab^{-1} \in H$

证明：必要性

- 因为 H 是子群，所以 $\forall b \in H$, $b^{-1} \in H$ 。
- 由于 H 对乘法封闭，故 $ab^{-1} \in H$ 。



群、群的基本性质

- 证明（续）：充分性

- 需要证明H满足子群的条件：

- 封闭性、单位元、逆元素

- $\forall a, b \in H$, $ab^{-1} \in H$, 故 $\forall a \in H$, $e = aa^{-1} \in H$

- $\forall h \in H$, $h^{-1} = eh^{-1} \in H$

- $\forall a, b \in H$, $b^{-1} \in H$, 故 $ab = a(b^{-1})^{-1} \in H$

证毕！



主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- 8.4 变换群和置换群 Cayley定理
- 8.5 陪集和群的陪集分解 Lagrange定理
- 8.6 正规子群与商群
- 8.7 群的同态、同态基本定理
- 8.8 群的直积



作业

- 课后：3, 6, 7, 10, 11, 12