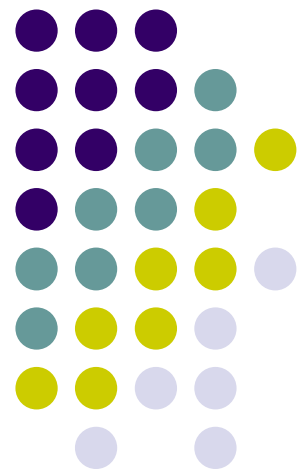


子群与拉格朗日定理

离散数学—代数结构

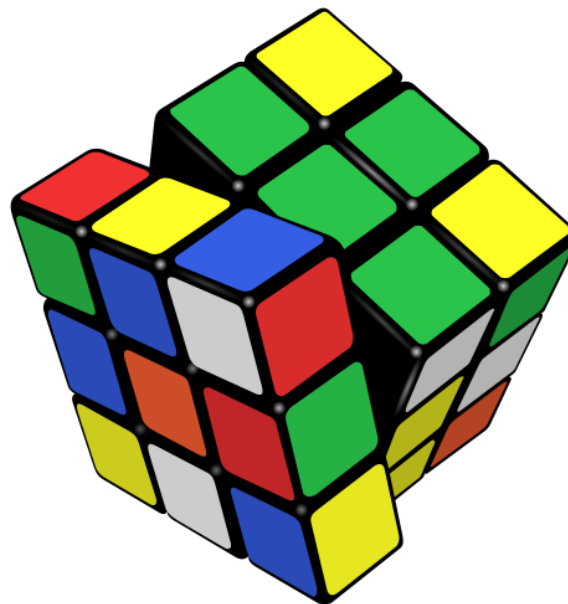
南京大学计算机科学与技术系



回顾



- 半群
- 么半群
- 群
- 群的性质
- 群的术语
- 群方程*





子群与拉格朗日定理

- 子群的定义及其判定
- 生成子群与元素的阶
- 子群的陪集与划分
- 拉格朗日定理
- 拉格朗日定理的推论





子群的定义

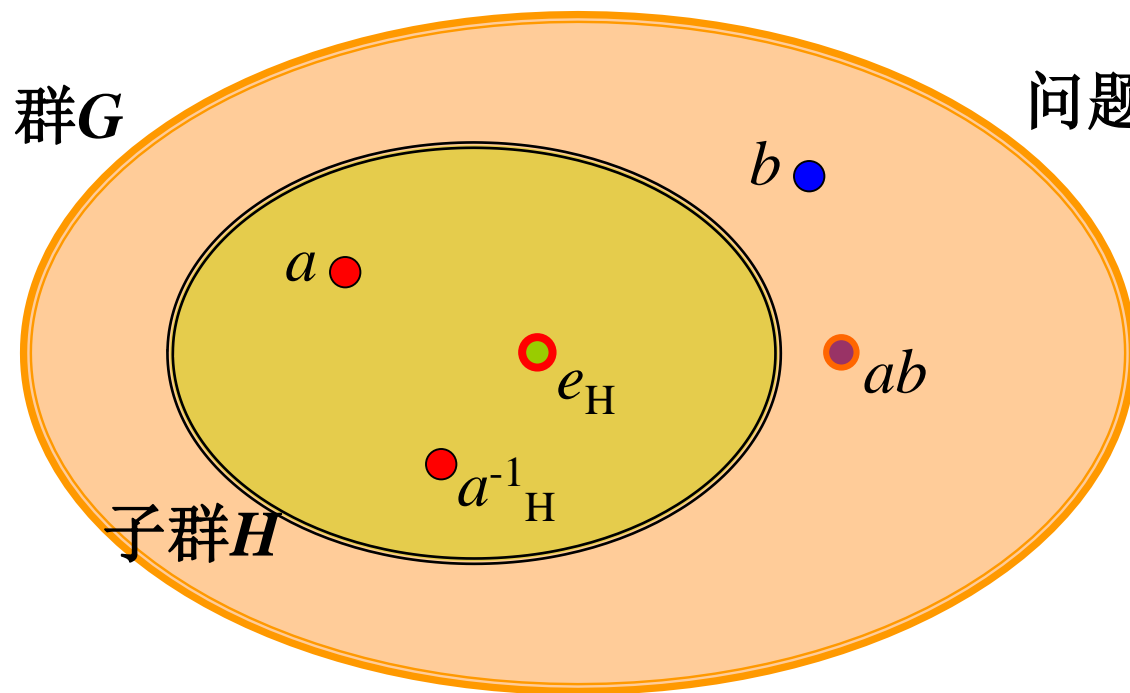
- 设 (G, \circ) 是群， H 是 G 的非空子集，如果 H 关于 G 中的运算构成群，即 (H, \circ) 也是群，则 H 是 G 的子群。
 - 记作 $(H, \circ) \leq (G, \circ)$ ，简记为 $H \leq G$ 。
- 例子：偶数加系统是整数加群的子群
- 平凡子群 (G, \circ) , $(\{e\}, \circ)$

注意：结合律在 G 的子集上均成立。



关于子群定义的进一步思考

问题1: e_H 是否一定是 e_G ? $e_H e_H = e_H \rightarrow e_H = e_G$



问题2: ab 应该在哪儿?



子群的判定 – 判定定理一

- G 是群， H 是 G 的非空子集。 H 是 G 的子群当且仅当：

- $\forall a, b \in H, ab \in H$, 并且

- $\forall a \in H, a^{-1} \in H$

(注意：这里 a^{-1} 是 a 在 G 中的逆元，当 H 确定为群后，它也是 a 在 H 中的逆元)

- 证明

- 必要性显然（注意群中逆元素的唯一性）

- 充分性：只须证明 G 中的单位元也一定在 H 中，它即是 H 的单位元素。



子群的判定 – 判定定理二

- G 是群， H 是 G 的非空子集。 H 是 G 的子群当且仅当：

$$\forall a, b \in H, ab^{-1} \in H$$

- 证明

- 必要性易见

- 充分性：

- 单位元素：因为 H 非空，任取 $a \in H$, $e = aa^{-1} \in H$

- 逆元素： $\forall a \in H$, 因为 $e \in H$, 所以 $a^{-1} = ea^{-1} \in H$

- 封闭性： $\forall a, b \in H$, 已证 $b^{-1} \in H$, 所以 $ab = a(b^{-1})^{-1} \in H$



群的术语：元素的乘幂（次方）

- 定义

$$a^0 = e \quad (e \text{ 是单位元素})$$

$$a^{n+1} = a^n \circ a \quad (n \text{ 是非负整数})$$

$$a^{-k} = (a^{-1})^k \quad (k \text{ 为正整数})$$

- 性质

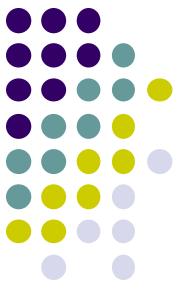
$$a^n \circ a^m = a^{n+m}$$

$$(a^n)^m = a^{nm}$$



群的术语：元素的阶

- 设 G 是群， $a \in G$ ， a 的阶（周期）定义如下：
 - $|a| = \min\{k \in \mathbb{Z}^+ \mid a^k = e\}$
 - 如果这样的 k 不存在， a 为无限阶元
- 性质
 - 有限群不存在无限阶元
 - 群中元素及其逆元具有相同的阶
 - 有限群中阶大于2的元素有偶数个
 - **偶数**群中阶为2的元素有奇数个 ($a = a^{-1}$)



子群的判定 – 有限子群

- G 是群， H 是 G 的非空**有限**子集。 H 是 G 的子群当且仅当：

$$\forall a, b \in H, ab \in H$$

- 证明. 必要性显然. 下证充分性，只须证明逆元素性
 - 若 H 中只含 G 的单位元， H 显然是子群。
 - 否则，任取 H 中异于单位元的元素 a ，考虑序列

$$a, a^2, a^3, \dots$$

注意：该序列中各项均为有限集合 H 中的元素，因此，必有正整数 $i, j (j > i)$ ，满足： $a^i = a^j$ ，因此：

$$a^{-1} = a^{j-i-1} \in H$$



生成子群

- 设 G 是群， $a \in G$ ，构造 G 的子集 H 如下：

$$H = \{a^k \mid k \text{ 是整数} \}$$

则 H 构成 G 的子群，称为 a 生成的子群 $\langle a \rangle$

- 证明：
 - H 非空： a 在 H 中
 - 利用判定定理二：

$$\forall a^m, a^n \in H, a^m(a^n)^{-1} = a^{m-n} \in H,$$

群中元素的阶



● 定义（元素的阶）

设 $(G, *)$ 为群, $n \in \mathbb{Z}$, $a \in G$, 以下定义 a^n :

若 $n \geq 0$, 则 a^n 已在上讲定义。

若 $n < 0$, 则 $a^n = (a^{-n})^{-1}$ 。

若 $(\exists n \in \mathbb{N}^+)(a^n = e)$, 则称 a 的阶(order)是有穷的且记 a 的阶 $|a| = \min\{n > 0 \mid a^n = e\}$ 。

若 $\neg (\exists n \in \mathbb{N}^+)(a^n = e)$, 则称 a 的阶是无穷的, 且记 a 的阶 $|a| = \infty$ 。

性质:

$$a^m a^n = a^{m+n}$$

$$(a^n)^m = a^{nm}$$

群中元素的阶（续）



● 例

在Kleine 4群 $(V, *)$ 中, $|e| = 1$, 当 $a \neq e$ 时, $|a| = 2$ 。

在 $(\mathbb{Z}_7, +_7)$ 中, $|0| = 1$, $a \neq 0$, $|a| = 7$ 。

在 $(\mathbb{Z}_6, +_6)$ 中, $|0| = 1$

元素	0	1	2	3	4	5
阶	1	6	3	2	3	6

*	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>e</i>

群中元素的阶（续）



● 定理（元素的阶的性质）

设 $(G, *)$, $a, b \in G$, $|a|, |b|$ 为有穷

$$(1) \text{ 对 } k \in \mathbb{Z}^+, a^k = e \Leftrightarrow |a| \mid k$$

$$(2) |a| = |a^{-1}|$$

$$(3) |ab| = |ba|$$

$$(4) |b^{-1}ab| = |a|$$

群中元素的阶（续）



-
- (1) 对 $k \in \mathbb{Z}^+$, $a^k = e \Leftrightarrow |a| \mid k$

证明: (1) “ \Rightarrow ” , 设 $|a| = m > 0$, $m = \min\{k \mid a^k = e \wedge k > 0\}$

故 $k \geq m$, 从而 $k = q \times m + r$, 这里 $0 \leq r < m$

$$\therefore a^k = a^{qm} * a^r = (a^m)^q * a^r = e^q * a^r = a^r$$

$$\therefore a^r = e$$

$$\therefore r < m$$

$$\therefore r = 0, \text{ 从而 } k = q \times m, \text{ 故 } m \mid k.$$

“ \Leftarrow ” , 设 $|a| = r$

$$|a| \mid k \rightarrow r \mid k \rightarrow k = n \times r \rightarrow a^k = a^{n \times r} = (a^r)^n = e^n = e$$

群中元素的阶（续）



(2) 令 $|a| = r$

$$\because (a^{-1})^r = (a^r)^{-1} = e^{-1} = e$$

$\therefore |a^{-1}| \mid |a|$, 同理 $|a| \mid |a^{-1}|$, 故 $|a^{-1}| = |a|$ 。

(3) $(ab)^{n+1} = abab \cdots ab = a(ba)^n b$

Case 1: ab 的阶有穷, 设为 r

$$\text{从而 } (ab)^{r+1} = a(ba)^r b$$

$$\text{从而 } ab = a(ba)^r b, \text{ 故 } (ba)^r = e$$

故 ba 的阶有穷, 设为 r' , 由(1)知 $r' \mid r$

同理 $|ba| = r'$ 时有 $|ab|$ 有穷, 若为 r , 则 $r \mid r'$

因此 $|ab| = |ba|$.

$$(4) \quad |b^{-1}ab| = |abb^{-1}| = |ae| = |a|$$

群中元素的阶（续）

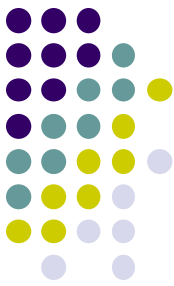


-
- **例题：** 设 $\langle G, * \rangle$ 为群，试证明：若 $|G| = n$ ，则

G 中阶大于2的元素有**偶数个**

证明：

对于 $a \in G$ ，若 $|a| > 2$ ，则 $a \neq a^{-1}$ ，若不然，则 $a = a^{-1}$ ，从而 $a^2 = e$ ，故 $|a| \leq 2$ 与 $|a| > 2$ 矛盾！因此我们有 $|a| > 2 \rightarrow a \neq a^{-1}$ ，故 G 中阶 > 2 的元素 a 与其逆 a^{-1} 成对出现，因此 G 有偶数个阶 > 2 的元素。



群的中心

- 设G是群，构造G的子集C如下：

$$C = \{ a \mid a \in G, \text{ 且 } \forall x \in G, ax = xa \}$$

则C构成G的子群，称为G的中心

证明：

- C非空：单位元在C中
- 利用判定定理二：即证明对任意的 $a, b \in C$, (即 $ax = xa$, $bx = xb$ 对G中一切 x 成立),

$(ab^{-1})x = x(ab^{-1})$ 也对G中一切 x 成立

$$(ab^{-1})x = a(b^{-1}(x^{-1})^{-1}) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1}) = x(ab^{-1})$$



左(右)陪集及其表示

- 若 H 是群 G 的一个子群, a 是 G 中的任意一个元素,
定义: $aH = \{ ah \mid h \in H \}$
- aH 称为 H 的一个左陪集
 - 由群的封闭性可知, aH 也是 G 的子集
 - $\forall h \in H. ah \in H \text{ iff } a \in H$
- 相应地可定义右陪集



陪集与划分

- 设 H 是群 G 的子群，则 H 的所有左陪集构成 G 的划分
 - G 中任意元素 a 一定在某个左陪集中： $a \in aH$
 - $\forall a, b \in G, aH = bH$ 或者 $aH \cap bH = \emptyset$
 - 假设 $aH \cap bH \neq \emptyset$, 即存在 $c \in aH \cap bH$, 令 $c = ah_1 = bh_2$,
 - 则 $a = bh_2h_1^{-1}$, 从而 $aH \subseteq bH$,
 - 同理可得: $bH \subseteq aH$. 所以 $aH = bH$
- 注意: a, b 属于同一左陪集
 - iff* $a \in bH$ 且 $b \in aH$
 - iff* $b^{-1}a \in H$

陪集与划分 (示例)



● 令 $H = \{2n | n \in \mathbb{Z}\}$, $\langle H, + \rangle < \langle \mathbb{Z}, + \rangle$, $a \in \mathbb{Z}$,

$$aH = \{2n + a | n \in \mathbb{Z}\}, \quad (2k)H = H,$$

$$(2k + 1)H = \mathbb{Z} - H, \quad \{0H, 1H\} \text{ 是 } \mathbb{Z} \text{ 的一个划分。}$$

● $\langle \mathbb{Z}_6, \oplus_6 \rangle$ 为群, 令 $H = \{0, 3\}$, $\langle H, \oplus_6 \rangle < \langle \mathbb{Z}_6, \oplus_6 \rangle$

$$, \quad H0 = H, \quad H1 = \{1, 4\}, \quad H2 = \{2, 5\}$$

$$H3 = H, \quad H4 = \{4, 1\} = H1, \quad H5 = \{5, 2\} = H2$$

$\{H0, H1, H2\}$ 是 \mathbb{Z}_6 的一个划分。



陪集与划分 (续)

-
- **定理 (陪集与划分)** : 设 $\langle H, * \rangle < \langle G, * \rangle$,

(1) $eH = H$

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

(3) $\forall a, b \in G, aH = bH$ 或者 $aH \cap bH = \emptyset$

(4) $\{aH \mid a \in G\}$ 为 G 之划分



左陪集关系

- 设 H 是群 G 的子群，定义 G 上的二元关系 R 如下：
 $\forall a, b \in G, (a, b) \in R$ 当且仅当 $b^{-1}a \in H$
- R 是 G 上的等价关系
 - 自反性： $\forall a \in G, a^{-1}a = e$
 - 对称性： 注意 $a^{-1}b = (b^{-1}a)^{-1}$
 - 传递性： 如果 $b^{-1}a \in H, c^{-1}b \in H$, 则
$$c^{-1}a = c^{-1}(bb^{-1})a = (c^{-1}b)(b^{-1}a) \in H$$
- $[a]_R = aH$: $x \in [a]_R \Leftrightarrow aRx \Leftrightarrow x^{-1}a = h \in H \Leftrightarrow x = ah^{-1} \in aH$

Lagrange 定理



● 引理（陪集的势）

设 $\langle H, * \rangle < \langle G, * \rangle$, $a \in G$, 则 $H \approx aH \approx Ha$

● 证明：

令 $\sigma: H \rightarrow aH$ 为 $\sigma(h) = ah$, 由消去律可知

τ, σ 为 1-1, 易见 σ 亦为满射, 故 $H \approx aH$ 。

同理可证 $H \approx Ha$ 。

Lagrange 定理 (续)



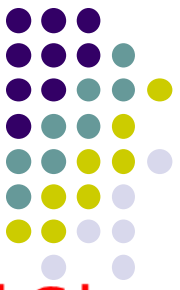
- $\{aH \mid a \in G\}$ 是 G 的一个划分。
- 对有限群 G ，每个陪集元素个数有限且相同，并等于 $|H|$ ，于是 $|G| = k|H|$ ， k 是左（右）陪集的个数，称为 H 在 G 中的指数，记为 $[G:H]$

Lagrange 定理 (续)



- **Lagrange定理**: 设 $\langle G, * \rangle$ 为有限群, $\langle H, * \rangle < \langle G, * \rangle$, 则 $|G| = |H| \cdot [G:H]$
- **证明**: 由于 $|G|$ 有穷, 故 $[G:H]$ 有穷且设为 N , 从而有 $a_1, \dots, a_N \in G$ 使 $\{a_i H \mid 1 < i \leq N\}$ 为 G 之划分, 故 $G = \bigcup_{i=1}^N H a_i$; 由引理, 对任意 i, j , $|H a_i| = |H a_j| = |H| \therefore |G| = |H| \cdot N$ 即 $|G| = |H| \cdot [G:H]. \square$

Lagrange 定理 (续)



- **推论1:** 设 $\langle G, * \rangle$ 为有限群, $a \in G$, 则 $|a|$ 为 $|G|$ 的因子。
- **证明*:** $\because \langle \langle a \rangle, * \rangle \leq \langle G, * \rangle \therefore |\langle a \rangle|$ 为 $|G|$ 的因子,
又由于 $|a|$ 有穷, 故 $|\langle a \rangle| = |a|$, 故 $|a|$ 为 $|G|$ 的因子. \square

Lagrange 定理 (续)



- **推论2***: 设 $\langle G, * \rangle$ 为 p 阶群, 若 p 为质数, 则

$$(\exists a \in G)(\langle a \rangle = G)$$

证: 设 $|G| = p$ 为素数, 可以取 $a \neq e, a \in G$, 由上推论知

$$|\langle a \rangle| \text{ 为 } |G| \text{ 的因子, } \because |\langle a \rangle| \geq 2 \therefore |\langle a \rangle| = p$$

$$\text{故 } G = \langle a \rangle$$



拉格朗日定理的应用

- 6阶群G必含3阶子群
- 证明
 - 如果G中有6阶元素 a , 则 $b=aa$ 是3阶元素, 因此 $\langle a \rangle$ 是3阶子群
 - 如果G中没有6阶元素, 则根据拉格朗日定理的推论, G中元素的阶只可能是1,2或3。
 - 如果没有3阶元素, 即 $\forall x \in G, x^2=e$, 那么 $\forall x, y \in G, xy=(yx)^2(xy)=yx$, 即G是交换群。
 - 因此 $\{e, a, b, ab\}$ 构成4阶子群, 但4不能整除6, 矛盾。
 - 所以G中必含3阶元素 a , 即由 a 生成的子群是3阶子群。

作业

- 教材内容：[屈婉玲] 10.2 节
- 课后习题：见课程网站

