

子群及其陪集

回顾

2

- 问题1：什么是代数系统？
 - ▣ 非空集合+封闭的(二元)运算
- 问题2：代数系统相关性质？
 - ▣ 封闭性、结合性、交换性、分配性；单位元、零元、逆元；同态同构
- 问题3：什么是群？
 - ▣ 封闭 + 结合律 + 单位元 + 逆元
- 问题4：群具有哪些性质？
 - ▣ 元素的阶、群的阶

本节提要

3

- 问题1：什么是子群，如何判别之？
- 问题2：子群一定存在么，若存在则满足什么性质？

子群的定义

4

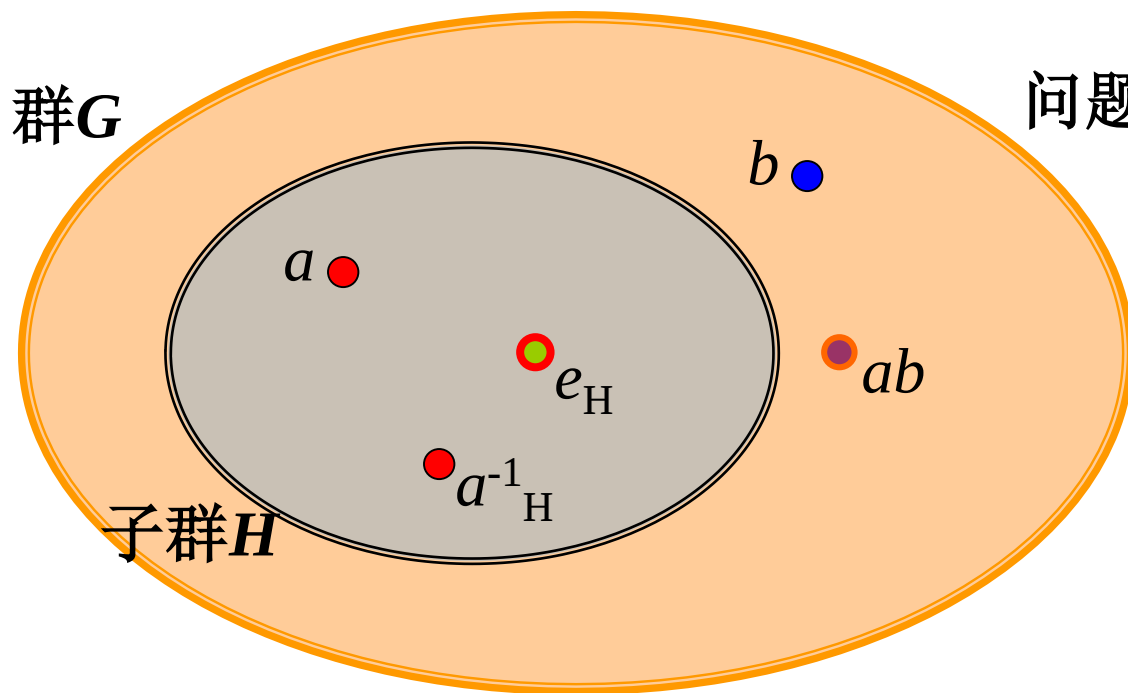
- 设 $(G, \circ)$ 是群， H 是 G 的非空子集，如果 H 关于 G 中的运算构成群，即 $(H, \circ)$ 也是群，则 H 是 G 的子群。
 - ▣ 记作 $(H, \circ) \leq (G, \circ)$ ，简记为 $H \leq G$ 。
- 例子：偶数加系统是整数加群的子群
- 平凡子群 $(G, \circ), (\{e\}, \circ)$

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

5

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

6

□ 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

□ 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。

子群的判定：判定定理二

7

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

子群的判定：判定定理三

8

- 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，只须证明逆元存在性

- 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 $i, j (j > i + 1)$ ，满足： $a^i = a^j$ ，由消去率有 $e = a^{j-i}$ ，因此：

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

本节提要

9

- 问题1：什么是子群，如何判别之？
 - ▣ 非空子集 + 封闭、结合律、单位元、逆元
 - ▣ 判定：根据定义或三个判定定理
- 问题2：子群一定存在么，若存在则满足什么性质？

生成子群

10

- 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:

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

非平凡子群一定存在么?

左(右)陪集

11

- 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
 - ▣ $\forall h \in H. ah \in H \text{ iff } a \in H$ (陪集不一定是子群)
- 类似可定义右陪集

陪集与划分

12

- 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： a, b 属于同一左陪集
 - $\text{iff } a \in bH$
 - $\text{iff } b^{-1}a \in H$

例

- 令 $H = \{2n | n \in \mathbb{Z}\}$, $\langle H, + \rangle < \langle \mathbb{Z}, + \rangle$, $a \in \mathbb{Z}$,
 $aH = \{2n + a | n \in \mathbb{Z}\}$, $(2k)H = H$,
 $(2k + 1)H = \mathbb{Z} - H$, $\{0H, 1H\}$ 是 $\mathbb{Z}$ 的一个划分。
- $\langle \mathbb{Z}_6, \oplus_6 \rangle$ 为群, 令 $H = \{0, 3\}$, $\langle H, \oplus_6 \rangle < \langle \mathbb{Z}_6, \oplus_6 \rangle$,
 $H0 = H$, $H1 = \{1, 4\}$, $H2 = \{2, 5\}$
 $H3 = H$, $H4 = \{4, 1\} = H1$, $H5 = \{5, 2\} = H2$
 $\{H0, H1, H2\}$ 是 $\mathbb{Z}_6$ 的一个划分。

例：左陪集关系

14

- 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 $b^{-1}a \in H$ 。证明 R 是 G 上的等价关系，并给出 R 的等价类。
- 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
$$c^{-1}a = c^{-1}(bb^{-1})a = (c^{-1}b)(b^{-1}a) \in H$$
- $[a]_R = aH$: $x \in [a]_R \Leftrightarrow aRx \Leftrightarrow x^{-1}a = h \in H \Leftrightarrow x = ah^{-1} \in aH$

例：正规子群

15

- H 是群 G 的一个子群， a 是 G 中的任意一个元素， H 称为 G 的正规子群 *iff*: $aH = Ha$
 - ▣ 即：对任意的 $h_i \in H, a \in G$ ，一定存在 $h_j \in H$ 使得 $h_i a = a h_j$
 - ▣ 注： h_i 与 h_j 不一定相等
- 证明：子群 N 是 G 的正规子群当且仅当对于任意的 $g \in G, n \in N$ 有 $gng^{-1} \in N$ 。
 - ▣ $\Rightarrow$ 存在 $n_1 \in N$ 使得 $gn = n_1 g$ ，即 $gng^{-1} = n_1 \in N$ ；
 - ▣ $\Leftarrow$ 先证 $gN \subseteq Ng$: 对于任意的 $gn \in gN$ ，因 $gng^{-1} \in N$ ，定义 $gng^{-1} = n_1$ ，则有 $gn = n_1 g \in Ng$ ；同理有 $Ng \subseteq gN$ 。

例：正规子群的左陪集关系

16

□ N 是 G 的正规子群，左陪集关系为 $(a,b) \in R$ 当且仅当 $b^{-1}a \in N$ 。如果 $p^{-1}a \in N$, $q^{-1}b \in N$, 则有 $(pq)^{-1}(ab) \in N$ 。

□ 证明：令 $p^{-1}a = n_1$, $q^{-1}b = n_2$ ($n_1, n_2 \in N$)

则有 $(pq)^{-1}(ab) = q^{-1}p^{-1}ab = q^{-1}n_1b = n_3q^{-1}b$ (正规子群)
 $= n_3n_2 \in N$

□ 同余关系：

□ 若 $(S,*)$ 为一个半群， S 上的等价关系 R 如满足：

aRa' and bRb' imply $(a * b)R(a' * b')$ ，则称 R 为同余关系。

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

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 $\{a_i H \mid 1 \leq i \leq N\}$ 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. □

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

22

□ 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 $\langle b \rangle$ 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, 易证 $\{e, a, b, ab\}$ 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。

本节小结

23

- 问题1：什么叫做群的子群，如何判别之？
 - 非空子集 + 封闭、结合律、单位元、逆元
 - 判定：根据定义或三个判定定理
- 问题2：子群一定存在么，若存在则满足什么性质？
 - 一定存在平凡子群
 - 子群 H 的所有陪集构成母群 G 的一个划分
 - 拉格朗日定理及其推论：有限群的子群阶是母群阶的因子、有限质数阶群没有非平凡子群、有限质数阶群一定是循环群

作业

24

□ 见课程主页