

第四讲子群、生成子群

陈建文

October 30, 2022

定义1. 设 S 为群 G 的非空子集, 如果 G 的运算在 S 中封闭且 S 对此运算也构成一个群, 则称 S 为 G 的一个子群。如果 $S \neq G$, 则称 S 为 G 的真子群。

定理1. 设 G 为一个群, 则 $\{e\}$ 为 G 的子群, G 为 G 的子群。

例. $(\mathbb{Z}, +)$ 为 $(\mathbb{Q}, +)$ 的子群, $(\mathbb{Q}, +)$ 为 $(\mathbb{R}, +)$ 的子群, $(\mathbb{R}, +)$ 为 $(\mathbb{C}, +)$ 的子群; (\mathbb{Q}^*, \times) 为 (\mathbb{R}^*, \times) 的子群, (\mathbb{R}^*, \times) 为 (\mathbb{C}^*, \times) 的子群。这里 \mathbb{Q}^* , \mathbb{R}^* 和 \mathbb{C}^* 本别代表非零有理数集合、非零实数集合和非零复数集合。集合 $\{1, -1\}$ 对通常的乘法构成一个群, 但它不是 $(\mathbb{Q}, +)$ 的子群, 因为它们的运算不一样。

定理2. 设 G_1 为 G 的子群, 则 G_1 的单位元必为 G 的单位元; G_1 的元素 a 在 G_1 中的逆元素也是 a 在 G 中的逆元素。

证明. 设 G_1 的单位元为 e_1 , G 的单位元为 e , 则 $e_1 e_1 = e_1 e$, 由消去律得 $e_1 = e$ 。

设 b 为 a 在 G_1 的逆元, 则 $ba = e$, 该式在 G 中也成立, 于是 b 也是 a 在 G 中的逆元。□

定理3. 群 G 的任意多个子群的交还是 G 的子群。

证明. 设 H 为 G 的一些子群的交, 则 $e \in H$, 从而 $H \neq \emptyset$ 。其次, $\forall a, b \in H$, ab 在每个参加交运算的子群中, 从而 $ab \in H$ 。所以, G 的运算在 H 中封闭。最后, $\forall a \in H$, 由 a 在每个参加交运算的子群中知 a^{-1} 在每个参加交运算的子群中, 故 $a^{-1} \in H$ 。因此, H 为 G 的子群。□

定理4. 任一群不能是其两个真子群的并。

证明. 用反证法。设 G_1 和 G_2 为 G 的两个真子群, 且 $G_1 \cup G_2 = G$ 。由于 G_1 和 G_2 为 G 的真子群, 所以 $\exists a, b \in G$, $a \notin G_1$, $b \notin G_2$ 。于是 $a \in G_2$, $b \in G_1$, 从而 $ab \in G$, 但 $ab \notin G_1$ 且 $ab \notin G_2$, 这与 $G = G_1 \cup G_2$ 矛盾。□

定理5. 群 G 的非空子集 S 为 G 的子群的充分必要条件是

- (1) $\forall a, b \in S, ab \in S$ 且
- (2) $\forall a \in S, a^{-1} \in S$ 。

证明. \Rightarrow 显然。

\Leftarrow 运算的封闭性显然成立; 运算的结合律显然成立; 由 S 非空知 $\exists a \in S$, 从而 $a^{-1} \in S$, 于是 $e = a^{-1}a \in S$ 。□

定理6. 群 G 的非空子集 S 为 G 的子群的充分必要条件是 $\forall a, b \in S, ab^{-1} \in S$ 。

证明. \Rightarrow 显然。

\Leftarrow 由 S 非空知 $\exists a \in S$, 从而 $e = aa^{-1} \in S$;

$\forall g \in S, g^{-1} = eg^{-1} \in S$;

$\forall a, b \in S, b^{-1} \in S$, 从而 $ab = a(b^{-1})^{-1} \in S$ 。 \square

定理7. 群 G 的有限非空子集 F 为 G 的子群的充分必要条件是 $\forall a, b \in F, ab \in F$ 。

$\forall A, B \in 2^G$, 定义 $AB = \{ab | a \in A, b \in B\}$, 则以上定理可以写成

定理8. 群 G 的有限非空子集 F 为 G 的子群的充分必要条件是 $FF \subseteq F$ 。

定义2. 群 G 的元素 a 称为 G 的中心元素, 如果 a 与 G 的每个元素可交换, 即 $\forall x \in G, ax = xa$ 。 G 的所有中心元素构成的集合 C 称为 G 的中心。

定理9. 群 G 的中心 C 是 G 的可交换子群。

证明. $\forall x \in G, ex = ex = x$, 所以 $e \in C$, 故 $C \neq \phi$ 。

$\forall a, b \in C, \forall x \in G, (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, 从而 $ab \in C$ 。

$\forall a \in C, \forall x \in G$, 由 $ax = xa$ 可得 $xa^{-1} = a^{-1}x$, 从而 $a^{-1} \in C$ 。

故 C 为 G 的子群。 C 显然是可交换的。 \square

例. 设 G 为一个群, $a \in G, \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$ 为 G 的一个子群。

例. 设 G 为一个有限群, $a \in G, \{e, a, a^2, \dots\}$ 为 G 的一个子群。

例. 设 G 为一个交换群, $a, b \in G$, 则 $\{a^m b^n | m, n \in \mathbb{Z}\}$ 为 G 的一个子群。

定义3. 设 M 为 G 的一个非空子集, G 的包含 M 的所有子群的交称为由 M 生成的子群, 记为 $\langle M \rangle$ 。

$\{a\}$ 简写为 $\langle a \rangle$, $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$ 。

$\{a, b\}$ 简写为 $\langle a, b \rangle$ 。如果 G 为一个交换群, $a, b \in G$, 则 $\langle a, b \rangle = \{a^m b^n | m, n \in \mathbb{Z}\}$ 。

$\langle M \rangle = \{m_1 m_2 \dots m_r | r \in \mathbb{Z}^+, m_i \in M \vee m_i^{-1} \in M, i = 1, 2, \dots, r\}$ 。

课后作业题:

练习1. 举例说明两个子群的并可以不是子群。

解. $S_6 = \{[0], [1], [2], [3], [4], [5]\}$,

$\{[0], [2], [4]\}$ 和 $\{[0], [3]\}$ 为 S_6 的两个子群, 但 $\{[0], [2], [4]\} \cup \{[0], [3]\} = \{[0], [2], [3], [4]\}$ 不是 S_6 的子群, 因为 $[2] + [3] = [5] \notin \{[0], [2], [3], [4]\}$ 。 \square

练习2. 设 G_1 和 G_2 为群 G 的两个真子群, 证明: $G_1 \cup G_2$ 为 G 的子群的充分必要条件是 $G_1 \subseteq G_2$ 或者 $G_2 \subseteq G_1$ 。

证明. 如果 $G_1 \subseteq G_2$ 或者 $G_2 \subseteq G_1$, 则 $G_1 \cup G_2 = G_2$ 或 G_1 , 此时显然 $G_1 \cup G_2$ 为 G 的子群。

如果 $G_1 \cup G_2$ 为 G 的子群, 以下用反证法证明 $G_1 \subseteq G_2$ 或者 $G_2 \subseteq G_1$ 。假设 $G_1 \not\subseteq G_2$ 并且 $G_2 \not\subseteq G_1$, 则存在 $g_2 \in G_2$, 但是 $g_2 \notin G_1$, 同时存在 $g_1 \in G_1$, 但是 $g_1 \notin G_2$ 。于是 G_1 为 $G_1 \cup G_2$ 的真子集, G_2 为 $G_1 \cup G_2$ 的真子集, 易得 G_1 和 G_2 为 $G_1 \cup G_2$ 的真子群, 由于任一群不能是两个真子群的并, 矛盾。 \square

练习3. 设 (G_1, \circ) 和 $(G_2, *)$ 都是群, $\phi: G_1 \rightarrow G_2, \forall a, b \in G_1, \phi(a \circ b) = \phi(a) * \phi(b)$, 证明: $\phi^{-1}(e_2)$ 为 G_1 的子群, 其中 e_2 为 G_2 的单位元素。

证明. 设 e_1 为 G_1 的单位元, 则 $\phi(e_1) = \phi(e_1 \circ e_1) = \phi(e_1) * \phi(e_1)$, 两边同时左乘 $\phi(e_1)^{-1}$, 得 $\phi(e_1) = e_2$, 从而 $e_1 \in \phi^{-1}(e_2)$, 所以 $\phi^{-1}(e_2)$ 非空。

$\forall x, y \in \phi^{-1}(e_2), \phi(x) = \phi(y) = e_2$, 从而 $\phi(x \circ y) = \phi(x) * \phi(y) = e_2 * e_2 = e_2$, 故 $x \circ y \in \phi^{-1}(e_2)$, 于是 G 中的乘法在 $\phi^{-1}(e_2)$ 中封闭。

$\forall x \in \phi^{-1}(e_2), e_2 = \phi(e_1) = \phi(x^{-1} \circ x) = \phi(x^{-1}) * \phi(x) = \phi(x^{-1}) * e_2 = \phi(x^{-1})$, 从而 $x^{-1} \in \phi^{-1}(e_2)$ 。

以上证明了 $\phi^{-1}(e_2)$ 为 G_1 的子群。 □

练习4. 找出3次对称群的所有子群。

解. $\{(1), (1, 2)\}, \{(1), (1, 3)\}, \{(1), (2, 3)\}, \{(1), (123), (132)\}$ □

练习5. 令 $P = \{(12), (123)\} \subseteq S_3$ 。写出由 P 生成的 S_3 的子群 $\langle P \rangle$ 。

解. $\langle P \rangle = S_3$ 。

这可以由以下计算得到:

$(12)(123) = (13), (123)(12) = (23), (123)(123) = (132)$ 。 □