

离散数学 II

Discrete Mathematics II

封筠

fengjun@stdu.edu.cn

20-11

课程回顾

阿贝尔群和循环群：阿贝尔群的定义、循环群、生成元、元素的阶

5-7 陪集和拉格朗日定理

- 学习本节要熟悉如下术语（4个）：

积、逆、左陪集、代表元素

- 要求：

掌握拉格朗日定理和2个推论

一、陪集


1、定义5-7.1 设 $\langle G, * \rangle$ 为群, $A, B \in \wp(G)$, 且 $A \neq \emptyset, B \neq \emptyset$, 记

$$AB = \{ a * b \mid a \in A, b \in B \}$$

和 $A^{-1} = \{ a^{-1} \mid a \in A \}$

分别称为 A , B 的积和逆。

再看5-4节P191例题1（验证 $\langle R, \star \rangle$ 是群）

	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

$$A = \{0^\circ, 60^\circ\}$$


$$B = \{120^\circ, 240^\circ\}$$

求 AB 以及 B^{-1}

2、定义5-7.2 设 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的子群，那么对任一 $a \in G$ ，则集合 $\{a\}H$ （或 $H\{a\}$ ）称为由 a 所确定的 H 在 G 中的左陪集(*left coset*)（或右陪集 *Right coset*），简称为 H 关于 a 的左陪集（右陪集），记为 aH （或 Ha ）。元素 a 称为陪集 aH （或 Ha ）的代表元素。

为确定起见，下面只对左陪集进行讨论。

再看5-4节P191例题1（验证 $\langle R, \star \rangle$ 是群）

	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

$\langle \{0^\circ, 180^\circ\}, \star \rangle$ 是 $\langle R, \star \rangle$ 的子群，
求 $\{0^\circ, 180^\circ\}$ 关于 60° 的左陪集

例1 设 $G=\mathbb{R}\times\mathbb{R}$, \mathbb{R} 为实数集, G 上的一个二元运算 $+$ 定义为

$$\langle x_1, y_1 \rangle + \langle x_2, y_2 \rangle = \langle x_1 + x_2, y_1 + y_2 \rangle$$

显然, $\langle G, + \rangle$ 是一个具有幺元 $\langle 0, 0 \rangle$ 的阿贝尔群。

设 $H = \{ \langle x, y \rangle \mid y = 2x \}$

容易验证 $\langle H, + \rangle$ 是 $\langle G, + \rangle$ 的子群。

对于 $\langle x_0, y_0 \rangle \in G$, H 关于 $\langle x_0, y_0 \rangle$ 的左陪集为
 $\langle x_0, y_0 \rangle H$ 。

这个例子的几何意义为：

G 是笛卡尔平面， H 是通过原点的直线 $y=2x$ ，陪集 $\langle x_0, y_0 \rangle H$ 是通过点 $\langle x_0, y_0 \rangle$ 且平行于 H 的直线。如下图所示。

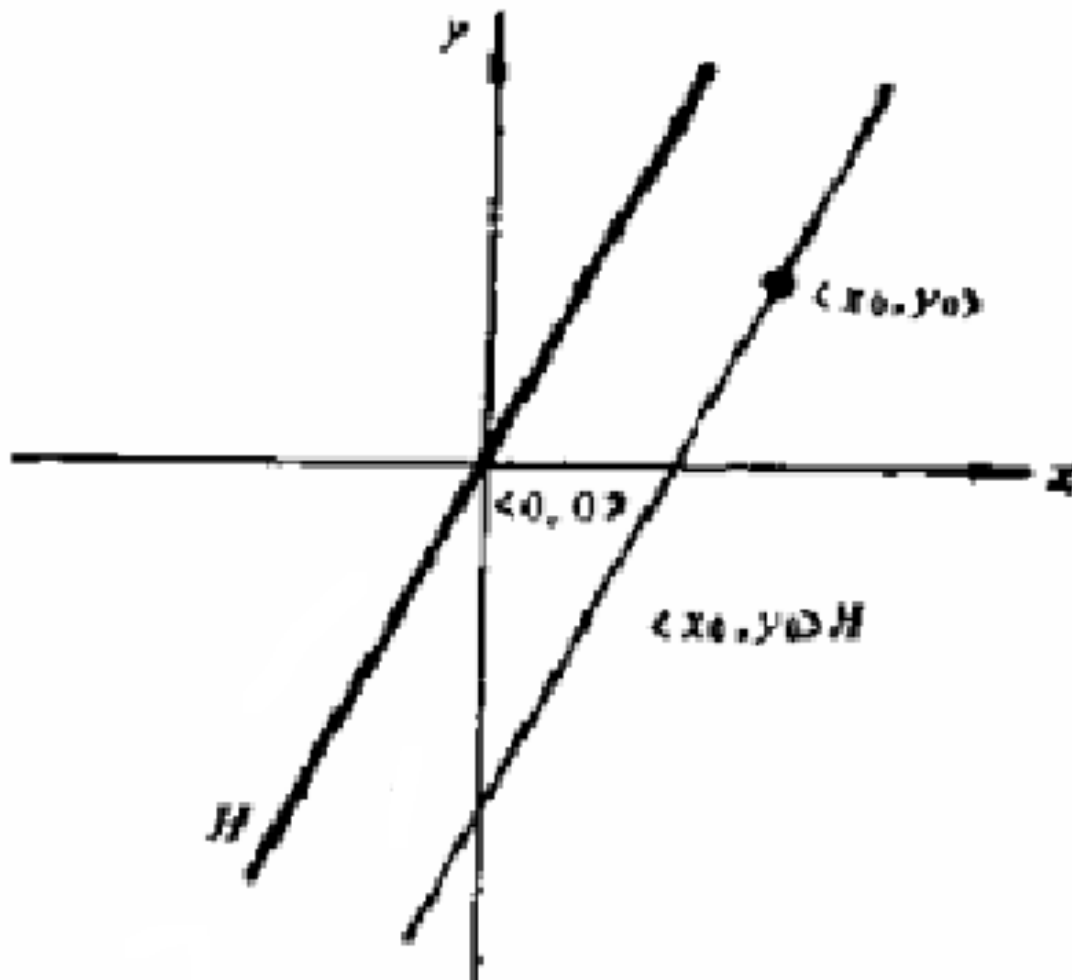


图 5-7.1

练习：211页 (1)



练习211页 (1)

设 $G = \{\varphi \mid \varphi: x \rightarrow ax + b, \text{其中 } a, b \in R \text{ 且 } a \neq 0, x \in R\}$

二元运算 \circ 是映射的复合。

a) 证明 $\langle G, \circ \rangle$ 是一个群。

b) 若 S 和 T 分别是由 G 中 $a=1$ 和 $b=0$ 的所有映射构成的集合，证明 $\langle S, \circ \rangle$ 和 $\langle T, \circ \rangle$ 都是子群。

c) 写出 S 和 T 在 G 中所有的左陪集。

证明: a)

1. 对于任意的 $\varphi_1, \varphi_2 \in G$, 设 $\varphi_1(x) = a_1x + b_1, a_1 \neq 0$,
 $\varphi_2(x) = a_2x + b_2, a_2 \neq 0$

$$\begin{aligned}\varphi_1 \circ \varphi_2(x) &= \varphi_1(\varphi_2(x)) = \varphi_1(a_2x + b_2) = a_1(a_2x + b_2) + b_1 \\ &= (a_1a_2)x + a_1b_2 + b_1\end{aligned}$$

因为 $a_1a_2 \in R, a_1b_2 + b_1 \in R$ 且 $a_1a_2 \neq 0$, 所以 $\varphi_1 \circ \varphi_2 \in G$
满足封闭性。

2. 对于任意的 $\varphi_1, \varphi_2, \varphi_3 \in G$, 有 $(\varphi_1 \circ \varphi_2) \circ \varphi_3(x) =$
 $(\varphi_1 \circ \varphi_2)(\varphi_3(x)) = \varphi_1(\varphi_2(\varphi_3(x)))$

而 $\varphi_1 \circ (\varphi_2 \circ \varphi_3)(x) = \varphi_1(\varphi_2(\varphi_3(x))) = \varphi_1(\varphi_2(\varphi_3(x)))$

所以 $(\varphi_1 \circ \varphi_2) \circ \varphi_3 = \varphi_1 \circ (\varphi_2 \circ \varphi_3)$ 满足结合性。

3. 设 $\varphi_e(x) = x$, 对于任意的 $\varphi \in G$, 设 $\varphi(x) = ax + b$, 则:
 $\varphi_e \circ \varphi(x) = \varphi_e(ax + b) = ax + b$, $\varphi \circ \varphi_e(x) = \varphi(x) = ax + b$,
所以 $\varphi_e \circ \varphi = \varphi \circ \varphi_e$; 所以 $\varphi_e = x$ 是幺元。

4. 对于任意的 $\varphi \in G$, 设 $\varphi(x) = ax + b, a \neq 0$, 于是存在
 $\varphi^{-1} \in G$, 使得 $\varphi^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$.

$$\varphi \circ \varphi^{-1}(x) = \varphi(\varphi^{-1}(x)) = \varphi\left(\frac{1}{a}x - \frac{b}{a}\right) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x.$$

$$\varphi^{-1} \circ \varphi(x) = \varphi^{-1}(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x$$

所以 $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = \varphi_e$, 逆元存在。

综上所述 $\langle G, \circ \rangle$ 是一个群。

b). 对于任意的 $\varphi_1, \varphi_2 \in S$, $\varphi_1(x) = x + b_1, \varphi_2(x) = x + b_2$,
有 $\varphi_2^{-1}(x) = x - b_2$,

$$\varphi_1 \circ \varphi_2^{-1}(x) = \varphi_1(\varphi_2^{-1}(x)) = x - b_2 + b_1 = x + (b_1 - b_2) \in S$$

$$\text{即 } \varphi_1 \circ \varphi_2^{-1} \in S$$

因此, $\langle S, o \rangle$ 是 $\langle G, o \rangle$ 的子群。

对于任意的 $\varphi_1, \varphi_2 \in T$, 设 $\varphi_1(x) = a_1 x, \varphi_2(x) = a_2 x$,

$$a_1 \neq 0, a_2 \neq 0, \text{ 有 } \varphi_2^{-1}(x) = \frac{1}{a_2} x$$

$$\varphi_1 \circ \varphi_2^{-1}(x) = \varphi_1(\varphi_2^{-1}(x)) = \varphi_1\left(\frac{1}{a_2} x\right) = a_1\left(\frac{1}{a_2} x\right) = \frac{a_1}{a_2} x, \frac{a_1}{a_2} \neq 0$$

所以 $\varphi_1 \circ \varphi_2^{-1} \in T$, 因此 $\langle T, o \rangle$ 也是 $\langle G, o \rangle$ 的子群。

c).

S 的左陪集应为 $\varphi \circ S, \varphi \in G$,

对于任意的 $\varphi \in G$, 设 $\varphi(x) = ax + b, a \neq 0$, 那么

$$\varphi \circ S = \{\varphi \circ \varphi' \mid \varphi' \in S\} = \{\varphi \circ \varphi' \mid \varphi': x \rightarrow x + b', b' \in R, x \in R\}$$

$$= \{\tilde{\varphi} \mid \tilde{\varphi}: x \rightarrow a(x + b') + b = ax + (ab' + b), b' \in R, x \in R\}$$

$$= \{\tilde{\varphi} \mid \tilde{\varphi}: x \rightarrow ax + c, c \in R, x \in R\}$$

故, S 在 G 中的所有左陪集为 $\tilde{\varphi} \mid \tilde{\varphi}: x \rightarrow ax + c, c \in R, x \in R\}$,

$a \in R$.

T 的左陪集应为 $\varphi \circ T, \varphi \in G$.

对于任意的 $\varphi \in G$, 设 $\varphi(x) = ax + b, a \neq 0$, 那么

$$\varphi \circ T = \{\varphi \circ \varphi' \mid \varphi' \in T\} = \{\varphi \circ \varphi' \mid \varphi': x \rightarrow a'x, a' \in R, x \in R\}$$

$$= \{\tilde{\varphi} \mid \tilde{\varphi}: x \rightarrow a(a'x) + b, a' \in R, x \in R\}$$

$$= \{\tilde{\varphi} \mid \tilde{\varphi}: x \rightarrow cx + b, c \in R, x \in R\}$$

故, T 在 G 中的所有左陪集为 $\{\tilde{\varphi} \mid \tilde{\varphi}: x \rightarrow cx + b, c \in R, x \in R\}$
 $b \in R$.

对于有限群，有下面一个很重要的结论。

二、拉格朗日定理

1、定理5-7.1 设 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的子群，那么

(a) $R = \{ \langle a, b \rangle \mid a \in G, b \in G \text{ 且 } a^{-1} * b \in H \}$ 是 G 中的一个等价关系。对于 $a \in G$ ，若记

$$[a]_R = \{ x \mid x \in G \text{ 且 } \langle a, x \rangle \in R \},$$

则 $[a]_R = aH$

(b) 设 $\langle H, * \rangle$ 为有限群 $\langle G, * \rangle$ 的子群， $|G|=n$ ， $|H|=m$ ，那么 H 的阶整除 G 的阶，即 $m \mid n$ 。

证明思路:先证 (a)

对于任意 $a \in G$, 必有 $a^{-1} \in G$, 使得 $a^{-1} * a = e \in H$, 所以 $\langle a, a \rangle \in R$ 。关系 R 是自反的。

若 $\langle a, b \rangle \in R$ 。则 $a^{-1} * b \in H$, 因为 H 是 G 的子群, 故

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

所以, $\langle b, a \rangle \in R$ 。关系 R 是对称的。

若 $\langle a, b \rangle \in R, \langle b, c \rangle \in R$ 。则 $a^{-1} * b \in H, b^{-1} * c \in H$, 所以 $a^{-1} * b * b^{-1} * c = a^{-1} * c \in H$, $\langle a, c \rangle \in R$, 关系 R 是传递的。

因此, 证明了关系 R 是等价关系。

对于 $a \in G$, 有 $b \in [a]_R$ 当且仅当 $\langle a, b \rangle \in R$, 即当且仅当 $a^{-1} * b \in H$, 而 $a^{-1} * b \in H$ 就是 $b \in aH$ 。因此 $[a]_R = aH$ 。

再证(b)

由于**R**是**G**中的一个等价关系，所以必定将**G**划分成不同的等价类 $[a_1]_R, [a_2]_R, \dots, [a_k]_R$ ，使得

$$G = \bigcup_{i=1}^k [a_i]_R = \bigcup_{i=1}^k a_i H$$

又因为**H**中任意两个不同的元素 $h_1, h_2, a \in G$ ，必有 $a * h_1 \neq a * h_2$ ，所以 $|a_i H| = |H| = m, i=1, 2, \dots, k$ 。因此

$$n = |G| = \left| \bigcup_{i=1}^k a_i H \right| = \sum_{i=1}^k |a_i H| = mk$$

所以**H**阶的整除**G**的阶 $m|n$ 。

2、**推论1** 任何质数阶的群不可能有非平凡子群。

这是因为，如果有非平凡子群，那么该子群的阶必定是原来群的阶的一个因子，这就与原来群的阶是质数相矛盾。

3、推论2 设 $\langle G, * \rangle$ 为 n 阶有限群, 那么对于任意 $a \in G$, a 的阶必是 n 的因子且必有 $a^n = e$, 这里 e 是群 $\langle G, * \rangle$ 的幺元。如果 n 为质数, 则 $\langle G, * \rangle$ 必是循环群。

这是因为, 由 G 中的任意元素 a 生成的循环群

$$H = \{a^i | i \in \mathbb{I}, a \in G\}$$

一定是 G 的一个子群。如果 H 的阶是 m , 那么由定理5-5.3可知 $a^m = e$, 即 a 的阶等于 m 。由拉格朗日定理必有 $n = mk, k \in \mathbb{N}$, 因此, a 的阶 m 是 n 的因子, 且有

$$a^n = a^{mk} = (a^m)^k = e^k = e$$

因为质数阶群只有平凡子群, 所以, 质数阶群必定是循环群。

例题1 设 $K=\{e,a,b,c\}$ ，在 K 上定义二元运算 $*$ 如下表所示。证明 $\langle K, * \rangle$ 是一个群，但不是循环群。

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证明 由上表可知，运算 $*$ 是封闭的和可结合的。幺元是 e ，每个元素的逆元是自身，所以， $\langle K, * \rangle$ 是群。因为 a, b, c 都是二阶元，故 $\langle K, * \rangle$ 不是循环群。

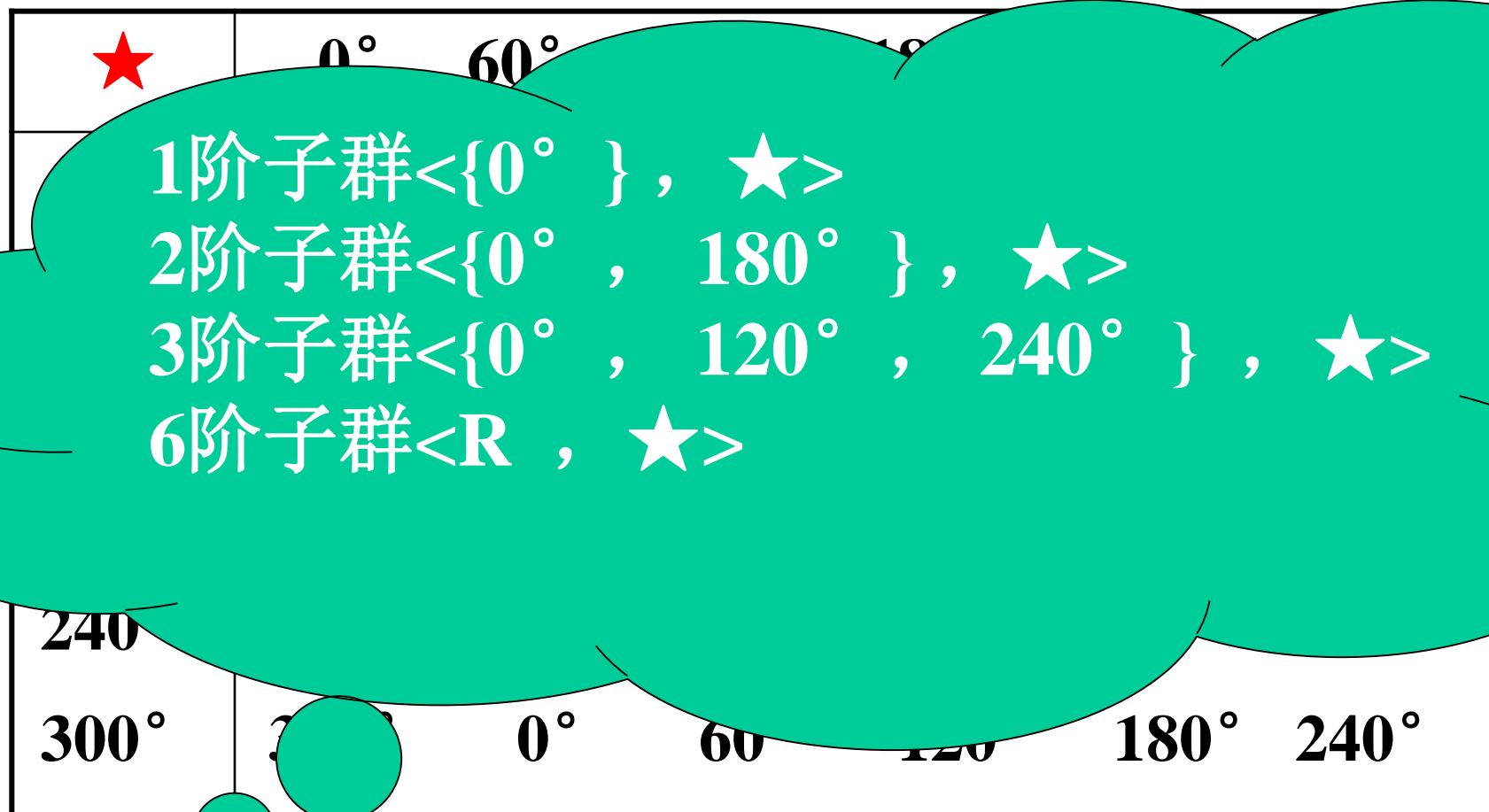
我们称 $\langle K, * \rangle$ 为Klein四元群。

例题2 任何一个四阶群只可能是四阶循环群或者是Klein四元群。

证明 设四阶群为 $\langle \{e, a, b, c\}, * \rangle$ 。其中 e 是幺元。当四阶群至少含有一个四阶元素时，这个群就是循环群。

当四阶群不含有四阶元素时，则由推论2可知，除幺元 e 外， a, b, c 的阶一定都是2。 $a*b$ 不可能等于 a, b 或 e ，否则将导致 $b=e, a=e$ 或 $a=b$ 的矛盾，所以 $a*b=c$ 。同样地有 $b*a=c$ 以及 $a*c=c*a=b, b*c=c*b=a$ 。因此，这个群就是Klein四元群。

求 $\langle R, \star \rangle$ 的子群



求 $\langle F, \star \rangle$ 的子群

0	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2

1阶子群 $\langle \{f^0\}, 0 \rangle$

2阶子群 $\langle \{f^0, f^2\}, 0 \rangle$

4阶子群 $\langle \{f^0, f^1, f^2, f^3\}, 0 \rangle$

求 $\langle G, \star \rangle$ 的子群

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

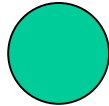
1阶子群 $\langle \{\alpha\}, * \rangle$

2阶子群 $\langle \{\alpha, \beta\}, * \rangle$

4阶子群 $\langle \{\alpha, \beta, \gamma, \delta\}, * \rangle$

作业:

P211 (2)、 (3)、 (5)



讨论：

一阶群、二阶群、三阶群

四阶群、五阶群、六阶群

The End