

## 第二章 群论

### § 1. 群的定义

1. 全体整数的集合对于普通减法来说是不是一个群?

解 不是, 因为普通减法不适合结合律.

例如

$$3 - (2 - 1) = 3 - 1 = 2 \quad (3 - 2) - 1 = 1 - 1 = 0$$

$$3 - (2 - 1) \neq (3 - 2) - 1$$

2. 举一个有两个元的群的例.

解 令  $G = \{ e, a \}$ ,  $G$  的乘法由下表给出

	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

首先, 容易验证, 这个代数运算满足结合律

$$(1) \quad (xy)z = x(yz) \quad x, y, z \in G$$

因为, 由于  $ea = ae = a$ , 若是元素  $e$  在 (1) 中出现, 那么 (1) 成立. (参考第一章, § 4, 习题 3.) 若是  $e$  不在 (1) 中出现, 那么有

$$(aa)a = ea = a \quad a(aa) = ae = a$$

而 (1) 仍成立.

其次， $G$ 有左单位元，就是 $e$ ； $e$ 有左逆元，就是 $e$ ， $a$ 有左逆元，就是 $a$ 。所以 $G$ 是一个群。

读者可以考虑一下，以上运算表是如何作出的。

3. 证明，我们也可以用条件 I，II 以及下面的条件 IV'，V' 来做群的定义：

IV'  $G$ 里至少存在一个右逆元  $a^{-1}$ ，能让

$$ae = a$$

对于 $G$ 的任何元  $a$  都成立；

V' 对于 $G$ 的每一个元  $a$ ，在 $G$ 里至少存在一个右逆元  $a^{-1}$ ，能让

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

**解** 这个题的证法完全平行于本节中关于可以用条件 I，II，IV，V 来做群定义的证明，但读者一定要自己写一下。

## § 2. 单位元、逆元、消去律

1. 若群 $G$ 的每一个元都适合方程  $x^2 = e$ ，那么 $G$ 是交换群。

**解** 令  $a$  和  $b$  是 $G$ 的任意两个元。由题设

$$(ab)(ab) = (ab)^2 = e$$

另一方面

$$(ab)(ba) = ab^2a = aea = a^2 = e$$

于是有  $(ab)(ab) = (ab)(ba)$ 。利用消去律，得

$$ab = ba$$

所以 $G$ 是交换群。

2. 在一个有限群里, 阶大于 2 的元的个数一定是偶数.

解 令  $G$  是一个有限群. 设  $G$  有元  $a$  而  $a$  的阶  $n > 2$ . 考察  $a^{-1}$ . 我们有

$$a^n (a^{-1})^n = e \quad e (a^{-1})^n = (a^{-1})^n = e$$

设正整数  $m < n$  而  $(a^{-1})^m = e$ , 那么同上可得  $a^m = e$ , 与  $n$  是  $a$  的阶的假设矛盾. 这样,  $n$  也是  $a^{-1}$  的阶, 易见  $a^{-1} \neq a$ . 否则

$$a^2 = aa^{-1} = e$$

与  $n > 2$  的假设矛盾. 这样, 我们就有一对不同的阶大于 2 的元  $a$  和  $a^{-1}$ .

设  $G$  还有元  $b$ ,  $b \neq a$ ,  $b \neq a^{-1}$ , 并且  $b$  的阶大于 2. 那么  $b^{-1}$  的阶也大于 2, 并且  $b^{-1} \neq b$ . 我们也有  $b^{-1} \neq a$ . 否则

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

消去  $b^{-1}$  得  $b = a^{-1}$ , 与假设矛盾. 同样可证  $b^{-1} \neq a^{-1}$ . 这样, 除  $a$  和  $a^{-1}$  外, 又有一对不同的阶大于 2 的元  $b$  和  $b^{-1}$ .

由于  $G$  是有限群, 而  $G$  的阶大于 2 的元总是成对出现, 所以  $G$  里这种元的个数一定是偶数.

3. 假定  $G$  是一个阶是偶数的有限群. 在  $G$  里阶等于 2 的元的个数一定是奇数.

解 由习题 2 知,  $G$  里阶大于 2 的元的个数是偶数. 但  $G$  只有一个阶是 1 的元, 就是单位元  $e$ . 于是由于  $G$  的阶是偶数, 得  $G$  里阶等于 2 的元的个数是奇数.

4. 一个有限群的每一个元的阶都有限.

解 令  $G$  是一个有限群而  $a$  是  $G$  的任一元素, 那么

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

不能都不相等。因此存在正整数  $i, j, i > j$ , 使  $a^i = a^j$ . 用  $a^{-j}$  乘两边, 得

$$(1) \quad a^{i-j} = e$$

这样, 存在正整数  $i-j$ , 使 (1) 成立. 因此也存在最小的正整数  $m$ , 使  $a^m = e$ , 这就是说, 元  $a$  的阶是  $m$ .

#### § 4. 群的同态

假定在两个群  $G$  和  $\bar{G}$  的一个同态映射之下,  $a \rightarrow \bar{a}$ .  $a$  与  $\bar{a}$  的阶是不是一定相同?

**解** 不一定. 例如, 令  $G$  是本章 § 1 中例 2 所给出的群而  $\bar{G}$  是该节中例 1 所给出的群. 那么读者容易证明

$$\Phi: \quad n \rightarrow g \quad n \text{ 是 } G \text{ 的任意元}$$

是  $G$  到  $\bar{G}$  的一个同态映射. 但  $G$  的每一个元  $n \neq 0$  都是无限阶的, 而  $g$  的阶是 1.

#### § 5. 变换群

1. 假定  $\tau$  是集合  $A$  的一个非一一变换.  $\tau$  会不会有一个左逆元  $\tau^{-1}$  使得  $\tau^{-1}\tau = \varepsilon$ ?

**解** 可能有. 例如令  $A = \{ \text{所有正整数} \}$ , 则

$$\tau: \quad 1 \rightarrow 1, \quad n \rightarrow n-1 \quad n > 1$$

显然是  $A$  的一个非一一变换. 而  $A$  的变换

$$\tau^{-1}: \quad n \rightarrow n+1 \quad n \in A$$

就能使  $\tau^{-1}\tau = \varepsilon$ .

2. 假定  $A$  是所有实数作成的集合。证明，所有  $A$  的可以写成

$$x \rightarrow ax + b \quad a \text{ 和 } b \text{ 是有理数, } a \neq 0$$

形式的变换作成变换群。这个群是不是一个交换群？

解 令  $G$  是由一切上述变换作成的集合。考察  $G$  的任何两个元素

$$\tau: \quad x \rightarrow ax + b \quad a \text{ 和 } b \text{ 是有理数, } a \neq 0$$

$$\lambda: \quad x \rightarrow cx + d \quad c \text{ 和 } d \text{ 是有理数, } c \neq 0$$

那么

$$\begin{aligned} \tau\lambda: \quad x \rightarrow x^{\tau\lambda} &= (ax + b)^\lambda = c(ax + b) + d \\ &= (ca)x + (cb + d) \end{aligned}$$

这里  $ca$  和  $cb + d$  都是有理数，并且  $ca \neq 0$ 。

所以  $\tau\lambda$  仍属于  $G$ 。

结合律对一般变换都成立，所以对上述变换也成立。

单位变换

$$\varepsilon: \quad x \rightarrow x$$

属于  $G$ 。

容易验证， $\tau$  在  $G$  中有逆，即

$$\tau^{-1}: \quad x \rightarrow \frac{1}{a}x + \left(-\frac{b}{a}\right)$$

因此  $G$  作成变换群。

但  $G$  不是一个交换群。令

$$\tau_1: \quad x \rightarrow x + 1$$

$$\tau_2: \quad x \rightarrow 2x$$

那么

$$\tau_1\tau_2: \quad x \rightarrow (x^{\tau_1})^{\tau_2} = (x + 1)^{\tau_2} = 2x + 2$$

$$\tau_2\tau_1: \quad x \rightarrow (x^{\tau_2})^{\tau_1} = (2x)^{\tau_1} = 2x + 1$$

$$\tau_1\tau_2 \neq \tau_2\tau_1$$

3. 假定  $S$  是一个集合  $A$  的所有变换作成的集合。我们暂时仍用符号

$$\tau: \quad a \longrightarrow a' = \tau(a)$$

来说明一个变换  $\tau$ 。证明，我们可以用

$$\tau_1\tau_2: \quad a \longrightarrow \tau_1[\tau_2(a)] = \tau_1\tau_2(a)$$

来规定一个  $S$  的乘法，这个乘法也适合结合律并且对于这个乘法来说， $\varepsilon$  还是  $S$  的单位元。

解 令  $\tau_1$  和  $\tau_2$  是  $S$  的任意两个元而  $a$  是  $A$  的任意一个元。那么  $\tau_2(a)$  和  $\tau_1[\tau_2(a)]$  都是  $A$  的唯一确定的元。因此如上规定的  $\tau_1\tau_2$  仍是  $S$  的一个唯一确定的元而我们得到了一个  $S$  的乘法。

令  $\tau_3$  也是  $S$  的一个任意元，那么

$$[(\tau_1\tau_2)\tau_3](a) = \tau_1\tau_2[\tau_3(a)] = \tau_1\{\tau_2[\tau_3(a)]\}$$

$$[\tau_1(\tau_2\tau_3)](a) = \tau_1[\tau_2\tau_3(a)] = \tau_1\{\tau_2[\tau_3(a)]\}$$

所以  $(\tau_1\tau_2)\tau_3 = \tau_1(\tau_2\tau_3)$  而乘法适合结合律。

令  $\tau$  是  $S$  的任意元。由于对一切  $a \in A$ ，都有  $\varepsilon(a) = a$ ，所以

$$\varepsilon\tau(a) = \varepsilon[\tau(a)] = \tau(a)$$

$$\tau\varepsilon(a) = \tau[\varepsilon(a)] = \tau(a)$$

即  $\varepsilon\tau = \tau\varepsilon = \tau$  而  $\varepsilon$  仍是  $S$  的单位元。

4. 证明，一个变换群的单位元一定是恒等变换。

解 设  $G$  是由某一集合  $A$  的变换组成的一个变换群，而  $\varepsilon$  是  $G$  的单位元。任取  $G$  的一个元  $\tau$  和  $A$  的一个元  $a$ 。由于

$\varepsilon\tau = \tau$ , 有

$$a^{\varepsilon\tau} = (a^\varepsilon)^\tau = a^\tau$$

由于  $\tau$  是  $A$  的一个一一变换, 所以  $a^\varepsilon = a$  而  $\varepsilon$  是  $A$  的恒等变换。

5. 证明, 实数域上一切有逆的  $n \times n$  矩阵对于矩阵乘法来说, 作成一群。

解 这个题的解法很容易, 这里从略。

## § 6. 置换群

1. 找出所有  $S_3$  的不能和  $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$  交换的元。

解  $S_3$  有 6 个元:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

其中的

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2$$

显然可以和  $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$  交换。通过计算, 易见其它三个元不能和  $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$  交换。

2. 把  $S_3$  的所有元写成不相连的循环置换的乘积。

解  $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1), \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \ 3)$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \ 2), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \ 3), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \ 3 \ 2)$$

### 3. 证明:

(i) 两个不相连的循环置换可以交换;

(ii)  $(i_1 i_2 \cdots i_k)^{-1} = (i_k i_{k-1} \cdots i_1)$ .

**解** (i) 看  $S_n$  的两个不相连的循环置换  $\sigma$  和  $\tau$ . 我们考察乘积  $\sigma\tau$  使数字  $1, 2, \dots, n$  如何变动. 有三种情况.

(a) 数字  $i$  在  $\sigma$  中出现, 并且  $\sigma$  把  $i$  变成  $j$ . 这时由于  $\sigma$  和  $\tau$  不相连,  $j$  不在  $\tau$  中出现, 因而  $\tau$  使  $j$  不变, 所以  $\sigma\tau$  仍把  $i$  变成  $j$ .

(b) 数字  $k$  在  $\tau$  中出现, 并且  $\tau$  把  $k$  变成  $l$ . 这时  $k$  不在  $\sigma$  中出现, 因而  $\sigma$  使  $k$  不变, 所以  $\sigma\tau$  仍把  $k$  变成  $l$ .

(c) 数字  $m$  不在  $\sigma$  和  $\tau$  中出现, 这时  $\sigma\tau$  使  $m$  不动.

如上考察  $\tau\sigma$  使数字  $1, 2, \dots, n$  如何变动, 显然得到同样的结果. 因此  $\sigma\tau = \tau\sigma$ .

(ii) 由于  $(i_1 i_2 \cdots i_k)(i_k i_{k-1} \cdots i_1) = (1)$ , 所以

$$(i_1 i_2 \cdots i_k)^{-1} = (i_k i_{k-1} \cdots i_1)$$

### 4. 证明一个 $k$ -循环置换的阶是 $k$ .

**解** 一个  $k$ -循环置换  $\pi = (i_1 i_2 \cdots i_k)$  的一次方, 二次方,  $\dots$ ,  $k$  次方分别把  $i_1$  变成  $i_2, i_3, \dots, i_1$ . 同理  $\pi^k$  把  $i_2$  变成  $i_3, \dots$ , 把  $i_k$  变成  $i_1$ . 因此  $\pi^k = (1)$ . 由上面的分析, 若是  $l < k$ , 那么  $\pi^l \neq (1)$ . 这就证明了,  $\pi$  的阶是  $k$ .

### 5. 证明 $S_n$ 的每一个元都可以写成

$$(1\ 2), (1\ 3), \dots, (1\ n)$$

这  $n-1$  个 2-循环置换中的若干个的乘积.

**解** 由于每一个置换都可以写成不相连的循环置换的乘积, 所以只须证明, 一个循环置换可以写成若干个  $(1\ i)$  形的置换的乘积. 设  $\pi$  是一个  $k$ -循环置换. 我们分两个情形

加以讨论.

(a) 1 在  $\pi$  中出现, 这时  $\pi$  可以写成  
$$(1 i_1 i_2 \cdots i_{k-1})$$

容易验算

$$(1 i_1 i_2 \cdots i_{k-1}) = (1 i_1)(1 i_2) \cdots (1 i_{k-1})$$

(b) 1 不在  $\pi$  中出现, 这时

$$\begin{aligned}\pi &= (i_1 i_2 \cdots i_k) = (1 i_1 i_2 \cdots i_k)(1 i_1) \\ &= (1 i_1)(1 i_2) \cdots (1 i_k)(1 i_1)\end{aligned}$$

## § 7. 循环群

1. 证明, 一个循环群一定是交换群.

解 设循环群  $G = (a)$ . 那么  $G$  的任何两个元都可以写成  $a^m$  和  $a^n$  ( $m, n$  是整数) 的形式. 但

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

所以  $G$  是一个交换群.

2. 假定群的元  $a$  的阶是  $n$ . 证明  $a^r$  的阶是  $\frac{n}{d}$ , 这里  $d = (r, n)$  是  $r$  和  $n$  的最大公因子.

解 由于  $d \mid r$ ,  $r = ds$ , 所以

$$(a^r)^{\frac{n}{d}} = (a^{ds})^{\frac{n}{d}} = (a^n)^s = e$$

现在证明,  $\frac{n}{d}$  就是  $a^r$  的阶. 设  $a^r$  的阶为  $k$ . 那么  $k \leq \frac{n}{d}$ .

令

$$\frac{n}{d} = kq + r_1 \quad 0 \leq r_1 \leq k-1$$

得

$$e = (a^r)^{\frac{n}{d}} = (a^r)^{kq+r_1} = (a^r)^{kq} (a^r)^{r_1} = (a^r)^{r_1}$$

但  $r_1 < k$  而  $k$  是  $a^r$  的阶, 所以  $r_1 = 0$  而

$$\frac{n}{d} = kq$$

于是得  $k \mid \frac{n}{d}$ . (参看本节定理的第二种情形.)

为了证明  $k = \frac{n}{d}$ , 只须反过来证明  $\frac{n}{d} \mid k$ . 由  $a^{rk} = e$  而

$n$  是  $a$  的阶, 同上有  $n \mid rk$ , 因而  $\frac{n}{d} \mid \frac{r}{d} k$ . 但  $d$  是  $n$  和  $r$  的

最大公因子, 所以  $\frac{n}{d}$  和  $\frac{r}{d}$  互素而有  $\frac{n}{d} \mid k$ .

3. 假定  $a$  生成一个阶是  $n$  的循环群  $G$ . 证明:  $a^r$  也生成  $G$ , 假如  $(r, n) = 1$  (这就是说  $r$  和  $n$  互素).

解 由习题 2,  $a^r$  的阶是  $n$ . 所以

$$a^r, (a^r)^2, \dots, (a^r)^{n-1}, (a^r)^n = e$$

互不相同. 但  $G$  只有  $n$  个元, 所以

$$G = \{a^r, (a^r)^2, \dots, (a^r)^n\}$$

而  $a^r$  生成  $G$ .

4. 假定  $G$  是循环群, 并且  $G$  与  $\bar{G}$  同态. 证明  $\bar{G}$  也是循环群.

解 由于  $G$  与  $\bar{G}$  同态,  $\bar{G}$  也是一个群. 设  $G = (a)$ , 而在  $G$  到  $\bar{G}$  的同态满射  $\Phi$  下,  $a \longrightarrow \bar{a}$ . 看  $\bar{G}$  的任意元  $\bar{g}$ . 那么在  $\Phi$  下, 有  $a^m \in G$ , 使  $a^m \longrightarrow \bar{g}$ . 但  $a^m \longrightarrow \bar{a}^m$ . 所以  $\bar{g} = \bar{a}^m$ .

这样， $\bar{G}$ 的每一元都是 $\bar{a}$ 的一个乘方而 $\bar{G} = \langle \bar{a} \rangle$ 。

5. 假定 $G$ 是无限阶的循环群， $\bar{G}$ 是任何循环群。证明 $G$ 与 $\bar{G}$ 同态。

解 令 $G = \langle a \rangle$ ， $\bar{G} = \langle \bar{a} \rangle$ 。定义

$$\Phi: \quad a^m \longrightarrow \bar{a}^m$$

我们证明， $\Phi$ 是 $G$ 到 $\bar{G}$ 的一个同态满射。

(i) 由于 $G$ 是无限阶的循环群， $G$ 的任何元都只能以一种方法写成 $a^m$ 的形式，所以在 $\Phi$ 之下， $G$ 的每一个元有一个唯一确定的象，而 $\Phi$ 是 $G$ 到 $\bar{G}$ 的一个映射。

(ii)  $\bar{G}$ 的每一个元都可以写成 $\bar{a}^m$ 的形式，因此它在 $\Phi$ 之下是 $G$ 的元 $a^m$ 的象，而 $\Phi$ 是 $G$ 到 $\bar{G}$ 的一个满射。

$$(iii) \quad a^m a^n = a^{m+n} \longrightarrow \bar{a}^{m+n} = \bar{a}^m \bar{a}^n$$

所以 $\Phi$ 是 $G$ 到 $\bar{G}$ 的一个同态满射。

## § 8. 子 群

1. 找出 $S_3$ 的所有子群。

解  $S_3$ 显然有以下子群：

$$S_3 \text{ 本身； } \langle (1) \rangle = \{ (1) \} ;$$

$$\langle (12) \rangle = \{ (12), (1) \} ;$$

$$\langle (13) \rangle = \{ (13), (1) \} ;$$

$$\langle (23) \rangle = \{ (23), (1) \} ;$$

$$\langle (123) \rangle = \{ (123), (132), (1) \} .$$

若 $S_3$ 的一个子群 $H$ 含有 $(12)$ ， $(13)$ 这两个2-循环置换，那么 $H$ 含有

$(1\ 2)(1\ 3) = (1\ 2\ 3)$ ,  $(1\ 2\ 3)(1\ 2) = (2\ 3)$   
 因而  $H = S_3$ . 同理, 若是  $S_3$  的一个子群含有两个 2-循环置换  $(2\ 1)$ ,  $(2\ 3)$  或  $(3\ 1)$ ,  $(3\ 2)$ , 这个子群也必然是  $S_3$ .

用完全类似的方法, 读者可以算出, 若是  $S_3$  的一个子群含有一个 2-循环置换和一个 3-循环置换, 那么这个子群也必然是  $S_3$ .

因此上面给出的 6 个子群是  $S_3$  的所有子群.

2. 证明, 群  $G$  的两个子群的交集也是  $G$  的子群.

**解** 设  $H_1$  和  $H_2$  是  $G$  的子群.

令  $e$  是  $G$  的单位元, 那么  $e$  属于  $H_1$  和  $H_2$ , 因而

$$e \in H_1 \cap H_2$$

而  $H_1 \cap H_2$  不空.

令  $a, b \in H_1 \cap H_2$ . 那么  $a, b$  属于  $H_1$  和  $H_2$ . 但  $H_1$  和  $H_2$  是子群, 所以  $ab^{-1}$  属于  $H_1$  和  $H_2$ , 因而属于  $H_1 \cap H_2$ .

这就证明了,  $H_1 \cap H_2$  是  $G$  的子群.

3. 取  $S_3$  的子集  $S = \{(1\ 2), (1\ 2\ 3)\}$ .  $S$  生成的子群包含哪些元? 一个群的两个不同的子集会不会生成相同的子群?

**解** 见习题 1 的解.

4. 证明, 循环群的子群也是循环群.

**解** 设循环群  $G = (a)$  而  $H$  是  $G$  的一个子群.

若  $H$  只含单位元  $e = a^0$ , 则  $H = (e)$  是循环群. 若  $H$  不仅含单位元, 那么因为  $H$  是子群, 它一定含有元  $a^m$ , 其中  $m$  是正整数. 令  $i$  是最小的使得  $a^i$  属于  $H$  的正整数, 我们证明, 这时  $H = (a^i)$ . 看  $H$  的任一元  $a^j$ . 令

$$t = iq + r \quad 0 \leq r < i$$

那么  $a^t = a^{iq}a^r$ 。由于  $a^i$  和  $a^{iq}$  都属于  $H$ ，有

$$a^r = a^{-iq}a^t \in H$$

于是由假设  $r = 0$ ， $a^t = (a^i)^q$  而  $H = (a^i)$ 。

5. 找出模12的剩余类加群的所有子群。

解 模12的剩余类加群  $G$  是一个阶为12的循环群。因此由题4， $G$ 的子群都是循环群。容易看出：

$$([0]) = [0]$$

$$([1]) = ([5]) = ([7]) = ([11]) = G$$

$$([2]) = ([10]) = \{[2], [4], [6], [8], [10], [0]\}$$

$$([3]) = ([9]) = \{[3], [6], [9], [0]\}$$

$$([4]) = ([8]) = \{[4], [8], [0]\}$$

$$([6]) = \{[6], [0]\}$$

是  $G$  的所有子群。

6. 假定  $H$  是群  $G$  的一个非空子集并且  $H$  的每一个元的阶都有限。证明， $H$  作成子群的充要条件是：

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

解 由本节定理1，条件显然是必要的。

要证明条件也是充分的，由同一定理，只须证明：

$$a \in H \implies a^{-1} \in H$$

设  $a \in H$ 。由于  $H$  的每一元的阶都有限，所以  $a$  的阶是某一正整数  $n$  而  $a^{-1} = a^{n-1}$ 。于是由所给条件得  $a^{-1} \in H$ 。

## § 9. 子群的陪集

1. 证明，阶是素数的群一定是循环群。

**解** 设群 $G$ 的阶为素数 $p$ . 在 $G$ 中取一元 $a \neq e$ , 则 $a$ 生成 $G$ 的一个循环子群 $(a)$ . 设 $(a)$ 的阶为 $n$ , 那么 $n \neq 1$ . 但由定理2,  $n \mid p$ , 所以 $n = p$ 而 $G = (a)$ 是一个循环群.

2. 证明, 阶是 $p^m$ 的群 ( $p$ 是素数,  $m \geq 1$ ) 一定包含一个阶是 $p$ 的子群.

**解** 设群 $G$ 的阶是 $p^m$ . 在 $G$ 中取一元 $a \neq e$ , 那么由定理3,  $a$ 的阶 $n \mid p^m$ . 但 $n \neq 1$ , 所以 $n = p^t$ ,  $t \geq 1$ . 若 $t = 1$ , 那么 $a$ 的阶为 $p$ , 而 $(a)$ 是一个阶为 $p$ 的子群. 若 $t > 1$ , 可取 $b = a^{p^{t-1}}$ , 那么 $b$ 的阶为 $p$ 而 $(b)$ 是一个阶为 $p$ 的子群.

3. 假定 $a$ 和 $b$ 是一个群 $G$ 的两个元, 并且 $ab = ba$ , 又假定 $a$ 的阶是 $m$ ,  $b$ 的阶是 $n$ , 并且 $(m, n) = 1$ . 证明:  
 $ab$ 的阶是 $mn$ .

**解** 设 $ab$ 的阶是 $k$ . 由 $ab = ba$ , 得

$$(ab)^{mn} = a^{mn}b^{mn} = e$$

因此 $k \mid mn$ . 我们反过来证明,  $mn \mid k$ . 由

$$e = (ab)^{kn} = a^{kn}b^{kn} = a^{kn}$$

以及 $a$ 的阶为 $m$ , 得 $m \mid kn$ . 但 $(m, n) = 1$ , 所以 $m \mid k$ . 同理 $n \mid k$ . 又由 $(m, n) = 1$ , 得 $mn \mid k$ .

这样,  $ab$ 的阶 $k = mn$ .

4. 假定 $\sim$ 是一个群 $G$ 的元间的一个等价关系, 并且对于 $G$ 的任意三个元 $a, x, x'$ 来说

$$ax \sim ax' \implies x \sim x'$$

证明, 与 $G$ 的单位元 $e$ 等价的元所作成的集合是 $G$ 的一个子群.

**解** 令 $H$ 是与 $e$ 等价的元所成的集合.

由于  $e \sim e$ , 所以  $H$  不空.

设  $a, b \in H$ . 那么  $a \sim e, b \sim e$ .  $b \sim e$  可写成

$$a^{-1}ab \sim a^{-1}a$$

因此由题设,  $ab \sim a \sim e$  而  $ab \in H$ .

$a \sim e$  可写成  $ae \sim aa^{-1}$ , 因此由题设,  $e \sim a^{-1}$  而  $a^{-1} \in H$ .

这样,  $H$  作成  $G$  的一个子群.

5. 我们直接下右陪集  $Ha$  的定义如下:  $Ha$  刚好包含  $G$  的可以写成

$$h a \quad (h \in H)$$

形式的元. 由这个定义推出以下事实:  $G$  的每一个元属于而且只属于一个右陪集.

**解** 取任意元  $a \in G$ . 由于  $H$  是一个子群, 单位元  $e \in H$ , 因此  $a = e a \in H a$ , 这就是说, 元  $a$  属于右陪集  $H a$ .

设  $a \in H b, a \in H c$ , 那么

$$a = h_1 b = h_2 c \quad (h_1, h_2 \in H)$$

由此得,  $b = h_1^{-1} h_2 c$ , 而  $H b$  的任意元

$$hb = h h_1^{-1} h_2 c \in H c$$

因而  $H b \subset H c$ . 同样可证  $H c \subset H b$ . 这样  $H b = H c$  而  $a$  只能属于一个右陪集.

6. 若我们把同构的群看成一样的, 一共只存在两个阶是 4 的群, 它们都是交换群.

**解** 先给出两个阶是 4 的群.

模 4 的剩余类加群  $G_1 = \{[0], [1], [2], [3]\}$ .

$G_1$  的元  $[1]$  的阶是 4 而  $G_1$  是  $[1]$  所生成的循环群  $\langle [1] \rangle$ .

### $S_4$ 的子群

$$B_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

叫作克莱因四元群.  $B_4$  是  $S_4$  的子群容易验证. 我们有

$$\begin{aligned} [(12)(34)]^2 &= [(13)(24)]^2 = [(14)(23)]^2 = (1) \\ (12)(34)(13)(24) &= (13)(24)(12)(34) = (14)(23) \\ (13)(24)(14)(23) &= (14)(23)(13)(24) = (12)(34) \\ (14)(23)(12)(34) &= (12)(34)(14)(23) = (13)(24) \end{aligned}$$

这两个群显然都是交换群.

现在证明, 任何阶是 4 的群都和以上两个群之一同构. 设  $G$  是一个阶为 4 的群. 那么  $G$  的元的阶只能是 1, 2 或 4.

若  $G$  有一个阶为 4 的元  $d$ , 那么  $G = \langle d \rangle$  是一个循环群而  $G$  与  $G_1$  同构.

若  $G$  没有阶为 4 的元, 那么除单位元  $e$  外,  $G$  的其它 3 个元的阶都是 2. 因此有

$$G = \{e, a, b, c\} \quad a^2 = b^2 = c^2 = e$$

由于  $G$  是群, 有  $ab \in G$ . 我们证明,  $ab = c$ .

由  $ab = e$  将得  $ab = a^2$  和  $b = a$ , 这不可能.

由  $ab = a$  将得  $b = e$ , 也不可能.

由  $ab = b$  将得  $a = e$ , 也不可能.

因此只能  $ab = c$ . 同样可证

$$ab = ba = c, \quad bc = cb = a, \quad ca = ac = b$$

比较  $G$  和  $B_4$  的代数运算, 易见  $G$  和  $B_4$  同构.

补充题 利用 6 题证明, 一个有限非交换群至少有 6 个元.

## § 10. 不变子群、商群

1. 假定群  $G$  的不变子群  $N$  的阶是 2. 证明,  $G$  的中心包含  $N$ .

解 令  $N = \{e, n\}$ , 这里  $e$  是  $G$  的单位元. 取  $G$  的任意元  $a$ . 由于  $N$  是一个不变子群, 有  $aN = Na$ , 即

$$\{a, an\} = \{a, na\}$$

所以  $an = na$ . 这样,  $N$  的两个元  $e$  和  $n$  都可以和  $G$  的任何元  $a$  交换, 所以  $N$  属于  $G$  的中心.

2. 证明, 两个不变子群的交集还是不变子群.

解 令  $N_1$  和  $N_2$  是群  $G$  的两个不变子群. 那么  $N_1 \cap N_2$  是  $G$  的一个子群 (§ 8. 习题 2). 我们进一步证明,  $N_1 \cap N_2$  是  $G$  的一个不变子群. 令  $a \in G$ ,  $n \in N_1 \cap N_2$ , 那么  $n \in N_1$ ,  $n \in N_2$ . 但  $N_1$  和  $N_2$  是不变子群, 所以  $ana^{-1} \in N_1$ ,  $ana^{-1} \in N_2$ , 因而

$$ana^{-1} \in N_1 \cap N_2$$

于是由定理 2,  $N_1 \cap N_2$  是一个不变子群.

3. 证明, 指数是 2 的子群一定是不变子群.

解 令  $G$  是一个群而  $N$  是  $G$  的一个指数为 2 的子群.

若  $n \in N$ , 那么显然有  $nN = Nn$ . 设  $b \in G$ ,  $b \notin N$ . 那么由于  $N$  的指数是 2,  $G$  被分成两个左陪集  $N$  和  $bN$ ;  $G$  也被分成两个右陪集  $N$  和  $Nb$ . 因此  $bN = Nb$ . 这样, 对于  $G$  的任何元  $a$  来说,  $aN = Na$  而  $N$  是  $G$  的一个不变子群.

4. 假定  $H$  是  $G$  的子群,  $N$  是  $G$  的不变子群. 证明,  $HN$  是  $G$  的子群.

**解** 由于 $H$ 和 $N$ 都不空, 所以 $HN$ 也不空.

设  $a \in HN$ ,  $b \in HN$ . 那么

$$a = h_1 n_1, \quad b = h_2 n_2 \quad (h_1, h_2 \in H, n_1, n_2 \in N)$$

$$ab^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 n' h_2^{-1} \quad (n' = n_1 n_2^{-1})$$

由于 $N$ 是一个不变子群, 有

$$N h_2^{-1} = h_2^{-1} N, \quad n' h_2^{-1} = h_2^{-1} n \quad (n \in N)$$

由是得  $ab^{-1} = (h_1 h_2^{-1}) n \in HN$  而  $HN$  是一个子群.

5. 举例证明,  $G$  的不变子群  $N$  的不变子群  $N_1$  未必是  $G$  的不变子群 (取  $G = S_4$ ).

**解** 令  $G = S_4$ ,

$$N = \{ (1), (12)(34), (13)(24), (14)(23) \}$$

$$N_1 = \{ (1), (12)(34) \}$$

已知  $N$  是  $G$  的一个子群 (上节习题 6). 我们证明,  $N$  是  $G$  的一个不变子群. 为了证明这一点, 我们考察, 是否对一切  $\pi \in S_4$ , 等式

$$(a) \quad \pi N \pi^{-1} = N$$

成立. 由于任何  $\pi$  都可以写成  $(1i)$  形的 2-循环置换的乘积 (§ 6. 习题 5), 我们只须对  $(1i)$  形的  $\pi$  来看等式

(a) 是否成立. 又由于  $N$  的元的对称性, 我们只须看  $\pi = (12)$  的情形. 但

$$(12) \{ (1), (12)(34), (13)(24), (14)(23) \} (12) \\ = \{ (1), (12)(34), (14)(23), (13)(24) \}$$

所以  $N$  是  $S_4$  的一个不变子群. 由于  $N$  是交换群,  $N_1$  当然是  $N$  的一个不变子群. 但  $N_1$  不是  $S_4$  的一个不变子群. 因为

$$(13) [(12) (34)] (13) = (14) (23) \in N_1$$

6. 一个群  $G$  的可以写成  $a^{-1}b^{-1}ab$  形式的元叫作换位子。证明：

(i) 所有有限个换位子的乘积作成的集合  $C$  是  $G$  的一个不变子群；

(ii)  $G/C$  是交换群；

(iii) 若  $N$  是  $G$  的一个不变子群，并且  $G/N$  是交换群，那么

$$N \supset C$$

**解** (i)  $C$  的两个元的乘积仍是有限个换位子的乘积，因而仍是  $C$  的一个元。一个换位子的逆仍是一个换位子，所以  $C$  的一个元的逆仍是  $C$  的一个元。这样  $C$  是一个子群。

对于  $a \in G$ ,  $c \in C$ ,  $a c a^{-1} = (a c a^{-1} c^{-1}) c \in C$ , 所以  $C$  是  $G$  的一个不变子群。

(ii) 令  $a, b \in G$ . 那么  $a^{-1}b^{-1}ab = c \in C$ . 由此得

$$ab = b a c, \quad a b C = b a c C = b a C$$

即  $a C b C = b C a C$  而  $G/C$  是交换群。

(iii) 因为  $G/N$  是交换群，所以对  $G$  的任何两个元  $a$  和  $b$

$$(aN)(bN) = (bN)(aN), \quad a b N = b a N$$

由此得  $ab = b a n \quad (n \in N) \quad a^{-1}b^{-1}ab = n \in N$ .

这样  $N$  含有一切换位子，因而含有  $C$ 。

补充题. 令  $\pi$  和  $(i_1 i_2 \cdots i_k)$  属于  $S_n$ . 证明

$$\pi^{-1} (i_1 i_2 \cdots i_k) \pi = (i_1^\pi i_2^\pi \cdots i_k^\pi)$$

## § 11. 同态与不变子群

1. 我们看一个集合  $A$  到集合  $\overline{A}$  的满射  $\Phi$ . 证明, 若  $A$  的子集  $S$  是  $\overline{A}$  的子集  $\overline{S}$  的逆象,  $\overline{S}$  一定是  $S$  的象; 但若  $\overline{S}$  是  $S$  的象,  $S$  不一定是  $\overline{S}$  的逆象.

**解** (i) 设  $S$  是  $\overline{S}$  的逆象. 这时对任一元  $a \in S$ , 存在元  $\overline{a} \in \overline{S}$ , 使  $\Phi(a) = \overline{a}$ , 因此  $\Phi(S) \subset \overline{S}$ . 反过来, 对任一元  $\overline{a} \in \overline{S}$ , 存在  $a \in S$ , 使  $\Phi(a) = \overline{a}$ , 因此  $\overline{S} \subset \Phi(S)$ . 这样  $\overline{S} = \Phi(S)$ , 即  $\overline{S}$  是  $S$  的象.

(ii) 令  $A = \{1, 2, 3, 4\}$ ,  $\overline{A} = \{2, 4\}$ ,  $A$  到  $\overline{A}$  的满射是

$$\Phi: \quad 1 \rightarrow 2, \quad 2 \rightarrow 2, \quad 3 \rightarrow 4, \quad 4 \rightarrow 4$$

取  $S = \{1, 3\}$ . 那么  $S$  的象  $\overline{S} = \{2, 4\}$ . 但  $\overline{S}$  的逆象是  $A \neq S$ .

2. 假定群  $G$  与群  $\overline{G}$  同态,  $\overline{N}$  是  $\overline{G}$  的一个不变子群,  $N$  是  $\overline{N}$  的逆象. 证明,  $G/N \cong \overline{G}/\overline{N}$ .

**解** 设所给  $G$  到  $\overline{G}$  的同态满射是

$$\Phi: \quad a \rightarrow \overline{a} = \Phi(a)$$

我们要建立一个  $G/N$  到  $\overline{G}/\overline{N}$  的同构映射. 定义

$$\Psi: \quad aN \rightarrow \overline{a}\overline{N}$$

若  $aN = bN$ , 那么  $b^{-1}a \in N$ . 由于  $\overline{N}$  是  $N$  在  $\Phi$  之下的象, 有

$$\overline{b^{-1}a} = \overline{b^{-1}}\overline{a} \in \overline{N}, \quad \overline{a}\overline{N} = \overline{b}\overline{N}$$

所以  $\Psi$  是  $G/N$  到  $\overline{G}/\overline{N}$  的一个映射.

设  $\overline{aN} \in \overline{G}/\overline{N}$  而  $\Phi(a) = \overline{a}$ , 那么

$$\Psi: \quad aN \rightarrow \overline{aN}$$

所以  $\Psi$  是  $G/N$  到  $\overline{G}/\overline{N}$  的一个满射.

若  $aN \neq bN$ , 那么  $b^{-1}a \notin N$ . 由于  $N$  是  $\overline{N}$  的逆象, 由此得

$$\overline{b^{-1}a} = \overline{b^{-1}a} \in \overline{N}, \quad \overline{aN} \neq \overline{bN}$$

所以  $\Psi$  是  $G/N$  与  $\overline{G}/\overline{N}$  间的一个一一映射.

最后, 由于

$$\Psi: \quad aNbN = abN \longrightarrow \overline{abN} = \overline{aN} \overline{bN}$$

$\Psi$  是  $G/N$  与  $\overline{G}/\overline{N}$  间的一个同构映射.

3. 假定  $G$  和  $\overline{G}$  是两个有限循环群, 它们的阶各是  $m$  和  $n$ . 证明,  $G$  与  $\overline{G}$  同态, 当而且只当  $n \mid m$  的时候.

解 设  $G$  与  $\overline{G}$  同态, 那么由定理 2,  $G/N \cong \overline{G}$ , 这里  $N$  是  $G$  到  $\overline{G}$  的同态满射的核. 所以  $G/N$  的阶是  $n$ . 但  $G/N$  的阶等于不变子群  $N$  在  $G$  里的指数, 所以由 § 9 的定理 2 它能整除  $G$  的阶  $m$ . 由此得  $n \mid m$ .

反过来设  $n \mid m$ . 令  $G = \langle a \rangle$ ,  $\overline{G} = \langle \overline{a} \rangle$ . 定义

$$\Phi: \quad a^k \longrightarrow \overline{a^k}$$

若  $a^h = a^k$ , 那么  $m \mid h - k$ . 于是由  $n \mid m$ , 得  $n \mid h - k$  而  $\overline{a^h} = \overline{a^k}$ . 这样  $\Phi$  是  $G$  到  $\overline{G}$  的一个映射. 容易证明,  $\Phi$  是  $G$  到  $\overline{G}$  的一个同态满射. 因此  $G$  与  $\overline{G}$  同态.

4. 假定  $G$  是一个循环群,  $N$  是  $G$  的一个子群. 证明,  $G/N$  也是循环群.

解 循环群  $G$  是交换群, 所以  $G$  的子群  $N$  是不变子群, 而  $G/N$  有意义.

设  $G = (a)$ 。容易证明  $G/N = (aN)$ 。所以  $G/N$  也是循环群。