离散数学

（第 3 版）

智能科学与技术学院 2024 级

目录

目录

13.1 群的定义及性质

半群与群都是具有一个二元运算的代数系统.

具体地,设 $V = \langle S, \circ \rangle$ 是一个具有二元运算的代数系统,如果运算 $\circ$ 满足结合律,那么称 V 为 半群.

如果半群 $V = \langle S, \circ \rangle$ 中关于 $\circ$ 运算存在单位元 $e \in S$,那么称 V 是 幺半群,也称作 独异点. 有时也将独异点 V 记作 $V = \langle S, \circ, e \rangle$.

进而,如果一个幺半群中每个元素均可逆,那么它构成一个群.

13.1 群的定义及性质

半群与群都是具有一个二元运算的代数系统.

具体地,设 $V = \langle S, \circ \rangle$ 是一个具有二元运算的代数系统,如果运算 $\circ$ 满足结合律,那么称 V 为 半群.

如果半群 $V = \langle S, \circ \rangle$ 中关于 $\circ$ 运算存在单位元 $e \in S$,那么称 V 是 幺半群,也称作 独异点. 有时也将独异点 V 记作 $V = \langle S, \circ, e \rangle$.

进而,如果一个幺半群中每个元素均可逆,那么它构成一个群.

定义 1.1.1

设 G 是非空集合,$\circ$ 是 G 上的二元运算,若下述条件被满足:

1. 结合律,即对 $\forall a, b, c \in G$,有 $(a \circ b) \circ c = a \circ (b \circ c)$;
2. 单位元,即 $\exists e \in G$ 使得对 $\forall a \in G$,有 $e \circ a = a = a \circ e$;
3. 逆元,即对 $\forall a \in G, \exists a^{-1} \in G$ 使得 $a \circ a^{-1} = e = a^{-1} \circ a$;

则称 G 是一个 群.

例 1.1.1

1. $\langle \mathbb{Z}^+, + \rangle, \langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ **都是半群，这里** $+$ **是普通加法. 这些半群中除** $\langle \mathbb{Z}^+, + \rangle$ **外都是独异点，其中** $\langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ **都是群，分别称作** 整数加群 、有理数加群 、实数加群 **和** 复数加群 .

例 1.1.1

1. $\langle \mathbb{Z}^+, + \rangle, \langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ 都是半群，这里 $+$ 是普通加法. 这些半群中除 $\langle \mathbb{Z}^+, + \rangle$ 外都是独异点，其中 $\langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ 都是群，分别称作 整数加群 、有理数加群 、实数加群 和 复数加群 .
2. 设 n 是大于 1 的正整数，$\langle M_n(\mathbb{R}), + \rangle$ 和 $\langle M_n(\mathbb{R}), \cdot \rangle$ 都是半群，也都是独异点，$\langle M_n(\mathbb{R}), + \rangle$ 也是群. 这里的 $+$ 和 $\cdot$ 分别表示矩阵加法和矩阵乘法. $\langle M_n(\mathbb{R}), \cdot \rangle$ 不是群，因为不是每个 n 阶矩阵都有乘法逆元.

例 1.1.1

1. $\langle \mathbb{Z}^+, + \rangle, \langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ 都是半群，这里 $+$ 是普通加法. 这些半群中除 $\langle \mathbb{Z}^+, + \rangle$ 外都是独异点，其中 $\langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ 都是群，分别称作 整数加群 、有理数加群 、实数加群 和 复数加群 .
2. 设 n 是大于 1 的正整数，$\langle M_n(\mathbb{R}), + \rangle$ 和 $\langle M_n(\mathbb{R}), \cdot \rangle$ 都是半群，也都是独异点，$\langle M_n(\mathbb{R}), + \rangle$ 也是群. 这里的 $+$ 和 $\cdot$ 分别表示矩阵加法和矩阵乘法. $\langle M_n(\mathbb{R}), \cdot \rangle$ 不是群，因为不是每个 n 阶矩阵都有乘法逆元.
3. $\langle P(B), \oplus \rangle$ 是半群，也是独异点和群，其中 $\oplus$ 为集合的对称差运算.
4. $\langle \mathbb{Z}_n, \oplus \rangle$ 是半群，也是独异点和群.
5. $\langle A^A, \circ \rangle$ 为半群，也是独异点，其中 $\circ$ 为函数的复合运算. 因为只有双射函数才有反函数，请读者思考：当 A 是什么集合时，它能构成群？

例 1.1.1

1. $\langle \mathbb{Z}^+, + \rangle, \langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ 都是半群，这里 $+$ 是普通加法. 这些半群中除 $\langle \mathbb{Z}^+, + \rangle$ 外都是独异点，其中 $\langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$ 都是群，分别称作 整数加群 、有理数加群 、实数加群 和 复数加群 .
2. 设 n 是大于 1 的正整数，$\langle M_n(\mathbb{R}), + \rangle$ 和 $\langle M_n(\mathbb{R}), \cdot \rangle$ 都是半群，也都是独异点，$\langle M_n(\mathbb{R}), + \rangle$ 也是群. 这里的 $+$ 和 $\cdot$ 分别表示矩阵加法和矩阵乘法. $\langle M_n(\mathbb{R}), \cdot \rangle$ 不是群，因为不是每个 n 阶矩阵都有乘法逆元.
3. $\langle P(B), \oplus \rangle$ 是半群，也是独异点和群，其中 $\oplus$ 为集合的对称差运算.
4. $\langle \mathbb{Z}_n, \oplus \rangle$ 是半群，也是独异点和群.
5. $\langle A^A, \circ \rangle$ 为半群，也是独异点，其中 $\circ$ 为函数的复合运算. 因为只有双射函数才有反函数，请读者思考：当 A 是什么集合时，它能构成群？
6. $\langle \mathbb{R}^*, \circ \rangle$ 为半群，其中 $\mathbb{R}^*$ 为非零实数集，$\circ$ 运算定义如下.

$$\forall x, y \in \mathbb{R}^*, \ x \circ y = y.$$

这个系统不构成独异点和群，因为它没有单位元.

在半群、独异点和群中，由于只有一个二元运算，在不发生混淆的情况下，经常将算符省去. 例如，将 $x \circ y$ 写作 xy. 在下面的讨论中将采用这种简略表示.

在半群、独异点和群中，由于只有一个二元运算，在不发生混淆的情况下，经常将算符省去. 例如，将 $x \circ y$ 写作 xy. 在下面的讨论中将采用这种简略表示.

例 1.1.2

设 $G = \{e, a, b, c\}$, G 上的运算由表 *1.1.1* 给出，不难验证 G 是一个群. 由表 *1.1.1* 可以看出 G 的运算具有以下的特点：e 为 G 中的单位元；G 中的运算是可交换的；每个元素的逆元就是它自己；在 a, b, c 三个元素中，任何两个元素运算的结果都等于另一个元素. 称这个群为 *Klein* 四元群，简称为 *四元群* .

表 1.1.1

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

例 1.1.3

设 Σ 是有穷字母表，$\forall k \in \mathbb{N}$，定义集合：

$$\Sigma_k = \{a_1 a_2 \cdots a_k | a_i \in \Sigma\}.$$

它是 Σ 上所有长度为 k 的串的集合. 当 $k = 0$ 时，$\Sigma_0 = \{\lambda\}$，λ 表示空串. 令 $\Sigma^* = \bigcup_{k=0}^{\infty} \Sigma_k$ 表示 Σ 上所有有限长度的串的集合，$\Sigma^+ = \Sigma^* - \{\lambda\}$ 则表示 Σ 上所有长度至少为 *1* 的有限串的集合. 在 Σ^* 上可以定义串的连接运算：$\forall \omega_1 = a_1 a_2 \cdots a_m, \omega_2 = b_1 b_2 \cdots b_n \in \Sigma^*$，有

$$\omega_1 \omega_2 = a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n.$$

显然 Σ^* 关于连接运算构成一个独异点，称作 Σ 上的 字代数.
Σ^* 的任意子集 L 均称作 Σ 上的 语言（这里的语言指形式语言，不是一般的自然语言）.

例 1.1.4

某二进制码的码字 $x = x_1 x_2 \cdots x_7$ 由 7 位构成，其中 x_1, x_2, x_3 和 x_4 为数据位，x_5, x_6 和 x_7 为校验位，并且满足：

$$\begin{cases} x_5 = x_1 \oplus x_2 \oplus x_3, \\ x_6 = x_1 \oplus x_2 \oplus x_4, \\ x_7 = x_1 \oplus x_3 \oplus x_4, \end{cases}$$

这里的 $\oplus$ 是模 2 加法. 设 G 为所有码字构成的集合，在 G 上定义二元运算: $\forall x, y \in G$, $x \circ y = z_1 z_2 \cdots z_7$, $z_i = x_i \oplus y_i$, $i = 1, 2, \cdots, 7$.

证明 $\langle G, \circ \rangle$ 构成群.

例 1.1.4

某二进制码的码字 $x = x_1x_2\cdots x_7$ 由 7 位构成，其中 x_1, x_2, x_3 和 x_4 为数据位，x_5, x_6 和 x_7 为校验位，并且满足：

$$\begin{cases} x_5 = x_1 \oplus x_2 \oplus x_3, \\ x_6 = x_1 \oplus x_2 \oplus x_4, \\ x_7 = x_1 \oplus x_3 \oplus x_4, \end{cases}$$

这里的 $\oplus$ 是模 2 加法. 设 G 为所有码字构成的集合，在 G 上定义二元运算: $\forall x, y \in G$, $x \circ y = z_1z_2\cdots z_7$, $z_i = x_i \oplus y_i$, $i = 1, 2, \cdots, 7$.

证明 $\langle G, \circ\rangle$ 构成群.

证明.

显然 $G \neq \emptyset$. 任取 $x = x_1x_2\cdots x_7, y = y_1y_2\cdots y_7, x \circ y = z_1z_2\cdots z_7$. 首先验证 $z_5 = z_1 \oplus z_2 \oplus z_3$.

$$\begin{aligned} & z_1 \oplus z_2 \oplus z_3 \\ &= (x_1 \oplus y_1) \oplus (x_2 \oplus y_2) \oplus (x_3 \oplus y_3) \\ &= (x_1 \oplus x_2 \oplus x_3) \oplus (y_1 \oplus y_2 \oplus y_3) \\ &= x_5 \oplus y_5 = z_5. \end{aligned}$$

同理可证 $z_6 = z_1 \oplus z_2 \oplus z_4$, $z_7 = z_1 \oplus z_3 \oplus z_4$.

于是 $x \circ y = z \in G$，证明了封闭性.

$\forall x, y, z \in G$，令 $(x \circ y) \circ z = a_1a_2\cdots a_7$, $x \circ (y \circ z) = b_1b_2\cdots b_7$. 下证 $a_i = b_i$, $i = 1, 2, \cdots, 7$. 由于 $\oplus$ 运算满足结合律，因此有

$$a_i = (x_i \oplus y_i) \oplus z_i = x_i \oplus (y_i \oplus z_i) = b_i.$$

从而证明了 G 满足结合律.

易见单位元为 0000000，$\forall x \in G$, $x^{-1} = x$. 综上所述，G 构成群.

定义 1.1.2

1. 若群 G 是有穷集，则称 G 是*有限群*，否则称作*无限群*. G 的基数称为群 G 的*阶*.
2. 只含单位元的群称作*平凡群*.
3. 若群 G 中的二元运算是可交换的，则称 G 为*交换群*或*阿贝尔(Abel)群*.

定义 1.1.2

1. 若群 G 是有穷集，则称 G 是*有限群*，否则称作*无限群*. G 的基数称为群 G 的*阶*.
2. 只含单位元的群称作*平凡群*.
3. 若群 G 中的二元运算是可交换的，则称 G 为*交换群*或*阿贝尔(Abel)群*.

例如，$\langle \mathbb{Z}, + \rangle$ 和 $\langle \mathbb{R}, + \rangle$ 是无限群，$\langle \mathbb{Z}_n, \oplus \rangle$ 是有限群，也是 n 阶群.
Klein 四元群是 4 阶群. $\langle \{0\}, + \rangle$ 是平凡群.
上述所有的群都是交换群，但 $n(\geqslant 2)$ 阶实可逆矩阵的集合(是 $M_n(\mathbb{R})$ 的真子集)关于矩阵乘法构成的群是非交换群，因为矩阵乘法不满足交换律.

n 次幂

定义 1.1.3

设 G 是群，$a \in G, n \in \mathbb{Z}$，则 a 的 n 次幂 定义为

$$a^n = \begin{cases} e, & n = 0, \\ a^{n-1}a, & n > 0, \\ (a^{-1})^{-n}, & n < 0. \end{cases}$$

n 次幂

定义 1.1.3

设 G 是群，$a \in G, n \in \mathbb{Z}$，则 a 的 n 次幂 定义为

$$a^n = \begin{cases} e, & n = 0, \\ a^{n-1}a, & n > 0, \\ (a^{-1})^{-n}, & n < 0. \end{cases}$$

元素的幂可以推广到半群和独异点. 但是幂指数 n 在半群中只能取正整数，在独异点中只能取自然数，只有在群中可以取负整数.

例如，在 $\langle \mathbb{Z}_3, \oplus \rangle$ 中有 $2^{-3} = (2^{-1})^3 = 1^3 = 1 \oplus 1 \oplus 1 = 0$;

而在 $\langle \mathbb{Z}, + \rangle$ 中有

$3^{-5} = (3^{-1})^5 = (-3)^5 = (-3) + (-3) + (-3) + (-3) + (-3) = -15.$

元素的阶

定义 1.1.4

设 G 是群，$a \in G$，使得等式 $a^k = e$ 成立的最小正整数 k 称为 a 的阶，记作 $|a| = k$，这时也称 a 为 k 阶元.

若不存在这样的正整数 k，则称 a 为无限阶元.

元素的阶

定义 1.1.4

设 G 是群，$a \in G$，使得等式 $a^k = e$ 成立的最小正整数 k 称为 a 的阶，记作 $|a| = k$，这时也称 a 为 k 阶元.

若不存在这样的正整数 k，则称 a 为无限阶元.

例如，$\langle \mathbb{Z}_6, \oplus \rangle$ 中，2 和 4 是 3 阶元，3 是 2 阶元，而 1 和 5 是 6 阶元，0 是 1 阶元；而在 $\langle \mathbb{Z}, + \rangle$ 中，0 是 1 阶元，其他的整数都是无限阶元.

在 Klein 四元群中 e 为 1 阶元，其他元素都是 2 阶元.

定理 1.1.1

设 G 为群，则 G 中的幂运算满足：

1. $\forall a \in G, (a^{-1})^{-1} = a.$
2. $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}.$
3. $\forall a \in G, a^n a^m = a^{n+m},$
   $n, m \in \mathbb{Z}.$
4. $\forall a \in G, (a^n)^m = a^{nm},$
   $n, m \in \mathbb{Z}.$
5. 若 G 为交换群，则
   $(ab)^n = a^n b^n,\ n \in \mathbb{Z}.$

定理 1.1.1

设 G 为群，则 G 中的幂运算满足：

1. $\forall a \in G, (a^{-1})^{-1} = a.$
2. $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}.$
3. $\forall a \in G, a^n a^m = a^{n+m},$ $n, m \in \mathbb{Z}.$
4. $\forall a \in G, (a^n)^m = a^{nm},$ $n, m \in \mathbb{Z}.$
5. 若 G 为交换群，则 $(ab)^n = a^n b^n,\ n \in \mathbb{Z}.$

证明.

只证 (1) 和 (3).

(1) $(a^{-1})^{-1}$ 是 a^{-1} 的逆元，而 a 也是 a^{-1} 的逆元. 由逆元唯一性有 $(a^{-1})^{-1} = a.$

定理 1.1.1

设 G 为群，则 G 中的幂运算满足：

1. $\forall a \in G, (a^{-1})^{-1} = a.$
2. $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}.$
3. $\forall a \in G, a^n a^m = a^{n+m},$ $n, m \in \mathbb{Z}.$
4. $\forall a \in G, (a^n)^m = a^{nm},$ $n, m \in \mathbb{Z}.$
5. 若 G 为交换群，则 $(ab)^n = a^n b^n,\ n \in \mathbb{Z}.$

证明.

只证 (1) 和 (3).

(1) $(a^{-1})^{-1}$ 是 a^{-1} 的逆元，而 a 也是 a^{-1} 的逆元. 由逆元唯一性有 $(a^{-1})^{-1} = a.$

(3) 先考虑 n, m 都是自然数的情况. 任意给定 n，对 m 进行归纳.

当 $m = 0$ 时有

$a^n a^0 = a^n e = a^n = a^{n+0}$ 成立.

假设对 $m \in \mathbb{N}$ 有 $a^n a^m = a^{n+m}$ 成立，则有 $a^n a^{m+1} = a^n(a^m a) = (a^n a^m)a = a^{n+m}a = a^{n+m+1}$，由归纳法等式得证.

下面考虑存在负整数次幂的情况. 设 $n < 0, m \geqslant 0$，令 $n = -t, t \in \mathbb{Z}^+$，则

$$a^n a^m = a^{-t}a^m = (a^{-1})^t a^m$$

$$= \begin{cases} a^{-(t-m)} = a^{m-t} = a^{n+m}, & t \geqslant m, \\ a^{m-t} = a^{n+m}, & t < m. \end{cases}$$

对于 $n \geqslant 0, m < 0$ 以及 $n < 0, m < 0$ 的情况同理可证. □

定理 1.1.1(2) 中的结果可以推广到有限多个元素的情况，即

$$(a_1 a_2 \cdots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$$

注意上述定理中的最后一个等式只对交换群成立.

如果 G 是非交换群，那么只有

$$(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n\text{ 个}}.$$

定理 1.1.1(2) 中的结果可以推广到有限多个元素的情况，即

$$(a_1 a_2 \cdots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$$

注意上述定理中的最后一个等式只对交换群成立.

如果 G 是非交换群，那么只有

$$(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n\text{ 个}}.$$

定理 1.1.2

设 G 为群，则 G 中满足消去律，即对任意 $a, b, c \in G$ 有

1. 若 $ab = ac$，则 $b = c$.
2. 若 $ba = ca$，则 $b = c$.

证明留作练习.

例 1.1.5

设 $G = \{a_1, a_2, \cdots, a_n\}$ **是** n **阶群，令**

$$a_i G = \{a_i a_j | j = 1, 2, \cdots, n\}.$$

证明：$a_i G = G$.

例 1.1.5

设 $G = \{a_1, a_2, \cdots, a_n\}$ 是 n 阶群，令

$$a_i G = \{a_i a_j | j = 1, 2, \cdots, n\}.$$

证明：$a_i G = G$.

证明.

由群中运算的封闭性有 $a_i G \subseteq G$. 假设 $a_i G \subset G$，即 $|a_i G| < n$，则必有 $a_j, a_k \in G, j \neq k$, 使得 $a_i a_j = a_i a_k$. 由消去律得 $a_j = a_k$，与 $|G| = n$ 矛盾. □

例 1.1.5

设 $G = \{a_1, a_2, \cdots, a_n\}$ 是 n 阶群，令

$$a_i G = \{a_i a_j | j = 1, 2, \cdots, n\}.$$

证明：$a_i G = G$.

证明.

由群中运算的封闭性有 $a_i G \subseteq G$. 假设 $a_i G \subset G$，即 $|a_i G| < n$，则必有 $a_j, a_k \in G, j \neq k$, 使得 $a_i a_j = a_i a_k$. 由消去律得 $a_j = a_k$，与 $|G| = n$ 矛盾. □

当 G 是 n 阶群时，$a_i G$ 恰好是 G 的运算表中第 i 行的全体元素.

例 1.1.5 说明 G 的运算表的每一行都是 G 中元素的一个排列. 不难看出，对于每一列也有同样的性质.

如果一个代数系统的运算表不满足这个性质，它肯定不是群. 但是，满足这个性质的也可能不是群. 请读者给出一个反例.

定理 1.1.3

设 G 为群，$a \in G$，且 $|a| = r$. 则

1. 对任意 $k \in \mathbb{Z}, a^k = e$ 当且仅当 $r \mid k$，即 r 整除 k.
2. $|a^{-1}| = |a|$.
3. $|a^t| = \frac{r}{(t,r)}$，这里 $t \in \mathbb{Z}, (t, r)$ 是 t 与 r 的最大公因数 $\gcd(t, r)$.

定理 1.1.3

设 G 为群，$a \in G$，且 $|a| = r$. 则

1. 对任意 $k \in \mathbb{Z}, a^k = e$ 当且仅当 $r \mid k$，即 r 整除 k.
2. $|a^{-1}| = |a|$.
3. $|a^t| = \frac{r}{(t,r)}$，这里 $t \in \mathbb{Z}, (t, r)$ 是 t 与 r 的最大公因数 $\gcd(t, r)$.

证明.

(1) 充分性. 由于 $r \mid k$，必存在整数 m 使得 $k = mr$，所以有

$$a^k = a^{mr} = (a^r)^m = e^m = e.$$

必要性. 根据带余除法，存在整数 m 和 i 使得 $k = mr + i, 0 \leqslant i \leqslant r - 1$，从而有

$$e = a^k = a^{mr+i} = (a^r)^m a^i = ea^i = a^i.$$

因为 $|a| = r$，所以必有 $i = 0$. 这就证明了 $r \mid k$.

定理1.1.3证明(续)

(2) 由 $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$ 可知 a^{-1} 的阶是存在的. 令 $|a^{-1}| = t$, 根据上面的证明有 $t \mid r$.

这说明 a 的逆元的阶是 a 的阶的因子. 而 a 又是 a^{-1} 的逆元, 所以 a 的阶也是 a^{-1} 的阶的因子, 故有 $r \mid t$. 从而证明了 $r = t$, 即 $|a^{-1}| = |a|$.

定理1.1.3证明(续)

(2) 由 $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$ 可知 a^{-1} 的阶是存在的. 令 $|a^{-1}| = t$, 根据上面的证明有 $t \mid r$.

这说明 a 的逆元的阶是 a 的阶的因子. 而 a 又是 a^{-1} 的逆元, 所以 a 的阶也是 a^{-1} 的阶的因子, 故有 $r \mid t$. 从而证明了 $r = t$, 即 $|a^{-1}| = |a|$.

(3) 令 $|a^t| = s, (t, r) = d$, 则存在 $p, q \in \mathbb{Z}$, 使得 $t = dp,\ r = dq,\ (p, q) = 1,$ $\frac{r}{(t,r)} = \frac{r}{d} = q$. 下面只需要证明 $s = q$.

由 $(a^t)^q = (a^t)^{r/d} = (a^r)^{t/d} = e^p = e$ 及定理1.1.31知, $s|q$.

同时, 由 $(a^t)^s = e$ 得, $a^{ts} = e$. 根据定理1.1.31, 有 $r|ts$, 即 $dq|dps$, 故 $q|ps$. 因为 $(p, q) = 1$, 所以有 $q|s$, 这就证明了 $s = q$. □

例 1.1.6

设 G 是群，$a, b \in G$ 是有限阶元. 证明：

1. $|b^{-1}ab| = |a|$.
2. $|ab| = |ba|$.

例 1.1.6

设 G 是群，$a, b \in G$ 是有限阶元. 证明：

1. $|b^{-1}ab| = |a|$.
2. $|ab| = |ba|$.

证明.

(1) 设 $|a| = r, |b^{-1}ab| = t$，则有

$$
\begin{aligned}
(b^{-1}ab)^r &= \underbrace{(b^{-1}ab)(b^{-1}ab)\cdots(b^{-1}ab)}_{r\text{ 个}} \\
&= b^{-1}a^r b \\
&= b^{-1}eb \\
&= e.
\end{aligned}
$$

根据定理 1.1.3得 $t \mid r$.

另一方面，由

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

$(b^{-1})^{-1}(b^{-1}ab)b^{-1}$

可知，$(b^{-1})^{-1}(b^{-1}ab)b^{-1}$ 的阶是 $b^{-1}ab$ 的阶的因子，即 $r \mid t$. 从而有 $|b^{-1}ab| = |a|$.

例 1.1.6

设 G 是群，$a, b \in G$ 是有限阶元. 证明：

1. $|b^{-1}ab| = |a|$.
2. $|ab| = |ba|$.

证明.

(1) 设 $|a| = r, |b^{-1}ab| = t$，则有

$$\begin{aligned}(b^{-1}ab)^r &= \underbrace{(b^{-1}ab)(b^{-1}ab)\cdots(b^{-1}ab)}_{r\text{ 个}} \\ &= b^{-1}a^r b \\ &= b^{-1}eb \\ &= e.\end{aligned}$$

根据定理 1.1.3得 $t \mid r$.

另一方面，由

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

$(b^{-1})^{-1}(b^{-1}ab)b^{-1}$

可知，$(b^{-1})^{-1}(b^{-1}ab)b^{-1}$ 的阶是 $b^{-1}ab$ 的阶的因子，即 $r \mid t$. 从而有 $|b^{-1}ab| = |a|$.

(2) 设 $|ab| = r, |ba| = t$，则有

$$\begin{aligned}(ab)^{t+1} &= \underbrace{(ab)(ab)\cdots(ab)}_{t+1\text{ 个}} \\ &= a\underbrace{(ba)(ba)\cdots(ba)}_{t\text{ 个}}b \\ &= a(ba)^t b \\ &= aeb \\ &= ab.\end{aligned}$$

由消去律得 $(ab)^t = e$，从而可知 $r \mid t$.

同理可证 $t \mid r$. 因此 $|ab| = |ba|$. □

例 1.1.7

设 G 为有限群，则 G 中阶大于 2 的元素有偶数个.

例 1.1.7

设 G 为有限群，则 G 中阶大于 2 的元素有偶数个.

证明.

根据定理 1.1.2，对于任意 $a \in G$ 有 $a^2 = e$ 当且仅当 $a^{-1}a^2 = a^{-1}e$，即 $a = a^{-1}$.

因此对 G 中阶大于 2 的元素 a，必有 $a \neq a^{-1}$.

又由于 $|a| = |a^{-1}|$，所以 G 中阶大于 2 的元素一定成对出现. G 中若含有阶大于 2 的元素，一定是偶数个. 若 G 中不含阶大于 2 的元素，而 0 也是偶数. □

13.2 子群与群的陪集分解

子群就是群的子代数.

定义 1.2.1

设 G 是群, H 是 G 的非空子集, 如果 H 关于 G 中的运算构成群, 那么称 H 是 G 的子群, 记作 $H \leqslant G$. 若 H 是 G 的子群, 且 $H \subset G$, 则 H 是 G 的真子群, 记作 $H < G$.

13.2 子群与群的陪集分解

子群就是群的子代数.

定义 1.2.1

设 G 是群, H 是 G 的非空子集, 如果 H 关于 G 中的运算构成群, 那么称 H 是 G 的 子群 , 记作 $H \leqslant G$. 若 H 是 G 的子群, 且 $H \subset G$, 则 H 是 G 的 真子群 , 记作 $H < G$.

例如, 对任意自然数 n, $n\mathbb{Z}$ 是整数加群 $\langle \mathbb{Z}, + \rangle$ 的子群. 当 $n \neq 1$ 时, $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的真子群.

任何群 G 都存在子群. 事实上, G 和 $\{e\}$ 都是 G 的子群, 称作 G 的 平凡子群 .

子群判定定理一

定理 1.2.1

设 G 为群，H 是 G 的非空子集，则 $H \leqslant G$ 当且仅当下面的条件成立.

1. $\forall a, b \in H$ 有 $ab \in H$；
2. $\forall a \in H$ 有 $a^{-1} \in H$.

子群判定定理一

定理 1.2.1

设 G 为群，H 是 G 的非空子集，则 $H \leqslant G$ 当且仅当下面的条件成立.

1. $\forall a, b \in H$ 有 $ab \in H$；
2. $\forall a \in H$ 有 $a^{-1} \in H$.

证明.

必要性是显然的. 为证明充分性，只需证明 $e \in H$.

因为 H 非空，必存在 $a \in H$. 由条件 (2) 可知 $a^{-1} \in H$，再使用条件 (1) 有 $aa^{-1} \in H$，即 $e \in H$. □

子群判定定理二

定理 1.2.2

设 G 为群，H 是 G 的非空子集，则 $H \leqslant G$ 当且仅当 $\forall a, b \in H$ 有 $ab^{-1} \in H$.

子群判定定理二

定理 1.2.2

设 G 为群，H 是 G 的非空子集，则 $H \leqslant G$ 当且仅当 $\forall a, b \in H$ 有 $ab^{-1} \in H$.

证明.

必要性. 任取 $a, b \in H$，由于 H 是 G 的子群，必有 $b^{-1} \in H$，从而有 $ab^{-1} \in H$.

充分性. 因为 H 非空，必存在 $a \in H$. 根据给定条件得 $aa^{-1} \in H$，即 $e \in H$. 任取 $a \in H$，由 $e, a \in H$ 得 $ea^{-1} \in H$，即 $a^{-1} \in H$. 任取 $a, b \in H$，由刚才的证明知 $b^{-1} \in H$. 再利用给定条件得 $a(b^{-1})^{-1} \in H$，即 $ab \in H$.

综上所述，根据判定定理一，可知 H 是 G 的子群. □

子群判定定理三

定理 1.2.3

设 G 为群，$\emptyset \neq H \subseteq G$，如果 H 是有穷集，则 $H \leqslant G$ 当且仅当 $\forall a, b \in H$ 有 $ab \in H$.

子群判定定理三

定理 1.2.3

设 G 为群,$\emptyset \neq H \subseteq G$,如果 H 是有穷集,则 $H \leqslant G$ 当且仅当 $\forall a, b \in H$ 有 $ab \in H$.

证明.

必要性是显然的. 为证明充分性,只需证明 $\forall a \in H$ 有 $a^{-1} \in H$.

任取 $a \in H$,若 $a = e$,则 $a^{-1} = e^{-1} = e \in H$. 若 $a \neq e$,令 $S = \{a, a^2, \cdots\}$,则 $S \subseteq H$. 由于 H 是有穷集,必有 $a^i = a^j, i < j$. 根据 G 中的消去律得 $a^{j-i} = e$. 由 $a \neq e$ 可知 $j - i > 1$,由此得

$$a^{j-i-1}a = e \text{ 且 } aa^{j-i-1} = e.$$

从而证明了 $a^{-1} = a^{j-i-1} \in H$. 由定理1.2.1知,H 是 G 的子群. □

由元素生成的子群

例 1.2.1

设 G 为群，$a \in G$，令

$$H = \{a^k | k \in \mathbb{Z}\},$$

即 a 的所有幂构成的集合，则 H 是 G 的子群，称作 由 a 生成的子群，记作 $\langle a \rangle$.

由元素生成的子群

例 1.2.1

设 G 为群，$a \in G$，令

$$H = \{a^k | k \in \mathbb{Z}\},$$

即 a 的所有幂构成的集合，则 H 是 G 的子群，称作 由 a 生成的子群，记作 $\langle a \rangle$.

首先由 $a \in \langle a \rangle$ 知道 $\langle a \rangle \neq \emptyset$. 任取 $a^m, a^l \in \langle a \rangle$，则有

$$a^m (a^l)^{-1} = a^m a^{-l} = a^{m-l} \in \langle a \rangle.$$

根据判定定理二可知 $\langle a \rangle \leqslant G$.

对于整数加群，由 2 生成的子群是 $\langle 2 \rangle = \{2k | k \in \mathbb{Z}\} = 2\mathbb{Z}$，而在群 $\langle \mathbb{Z}_6, \oplus \rangle$ 中，由 2 生成的子群是 $\langle 2 \rangle = \{0, 2, 4\}$.

对于 Klein 四元群 $G = \{e, a, b, c\}$ 来说，分别由它的每个元素生成的子群是：

$$\langle e \rangle = \{e\}, \ \langle a \rangle = \{e, a\}, \ \langle b \rangle = \{e, b\}, \ \langle c \rangle = \{e, c\}.$$

群的中心

例 1.2.2

设 G 为群，令 C 是与 G 中所有的元素都可交换的元素构成的集合，即 $C = \{a \in G | \forall x \in G, ax = xa\}$，则 C 是 G 的子群，称作 G 的中心 .

群的中心

例 1.2.2

设 G 为群，令 C 是与 G 中所有的元素都可交换的元素构成的集合，即 $C = \{a \in G | \forall x \in G, ax = xa\}$，则 C 是 G 的子群，称作 G 的 中心 .

证明.

首先，由 e 与 G 中所有元素的交换性可知 $e \in C$，所以 C 是 G 的非空子集.

任取 $a, b \in C$，为证明 $ab^{-1} \in C$，只需证明 ab^{-1} 与 G 中所有的元素都可交换.

事实上，$\forall x \in G$，有

$$\begin{aligned}(ab^{-1})x &= ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} \\ &= (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}),\end{aligned}$$

即 $(ab^{-1})x = x(ab^{-1})$. 由判定定理二可知 $C \leqslant G$. □

群的中心

例 1.2.2

设 G 为群，令 C 是与 G 中所有的元素都可交换的元素构成的集合，即 $C = \{a \in G | \forall x \in G, ax = xa\}$，则 C 是 G 的子群，称作 G 的 中心 .

证明.

首先，由 e 与 G 中所有元素的交换性可知 $e \in C$，所以 C 是 G 的非空子集.
任取 $a, b \in C$，为证明 $ab^{-1} \in C$，只需证明 ab^{-1} 与 G 中所有的元素都可交换.
事实上，$\forall x \in G$，有

$$\begin{aligned}(ab^{-1})x &= ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} \\ &= (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}),\end{aligned}$$

即 $(ab^{-1})x = x(ab^{-1})$. 由判定定理二可知 $C \leqslant G$. □

对于 Abel 群 G，因为 G 中所有的元素互相都可交换，所以 G 的中心就等于 G.
但是对某些非交换群 G，它的中心是 $\{e\}$.

例 1.2.3

设 G 是群, H, K 是 G 的子群. 证明:

1. $H \cap K \leq G$.
2. $H \cup K \leq G$ 当且仅当 $H \subseteq K$ 或 $K \subseteq H$.

例 1.2.3

设 G 是群，H, K 是 G 的子群. 证明：

1. $H \cap K \leq G$.
2. $H \cup K \leq G$ 当且仅当 $H \subseteq K$ 或 $K \subseteq H$.

证明.

(1) 由 $e \in H \cap K$ 知，$H \cap K \neq \emptyset$. 任取 $a, b \in H \cap K$，则有 $a \in H$, $a \in K$, $b \in H$, $b \in K$. 由于 H 和 K 是 G 的子群，必有 $ab^{-1} \in H$ 和 $ab^{-1} \in K$. 从而有 $ab^{-1} \in H \cap K$. 根据判定定理二，结论得证.

(2) 充分性是显然的. 只证必要性，用反证法. 假设 $H \not\subseteq K$ 且 $K \not\subseteq H$，那么存在 h 和 k 使得

$$h \in H, h \notin K; k \in K, k \notin H.$$

这意味着 $hk \notin H$. 若不然，由 $h^{-1} \in H$ 可得 $k = h^{-1}(hk) \in H$, 与假设矛盾. 同理可证 $hk \notin K$，从而有 $hk \notin H \cup K$，这与 $H \cup K$ 是子群矛盾. □

由子集生成的子群

任取群 G 的两个子群 H_1, H_2，一般说来 $H_1 \cup H_2$ 不是 G 的子群，而只是 G 的子集.

设 B 是 G 的非空子集，将 G 的所有包含 B 的子群的交记作 $\langle B \rangle$，即

$$\langle B \rangle = \cap \{H | B \subseteq H, H \leqslant G\}.$$

易见 $\langle B \rangle \leq G$，称作 *由 B 生成的子群*.

由子集生成的子群

任取群 G 的两个子群 H_1, H_2，一般说来 $H_1 \cup H_2$ 不是 G 的子群，而只是 G 的子集.

设 B 是 G 的非空子集，将 G 的所有包含 B 的子群的交记作 $\langle B \rangle$，即

$$\langle B \rangle = \cap \{ H | B \subseteq H, H \leqslant G \}.$$

易见 $\langle B \rangle \leq G$，称作 *由 B 生成的子群*.

不难证明 $\langle B \rangle$ 中的元素恰为如下形式：

$$a_1 a_2 \cdots a_k, \ k \in \mathbb{Z}^+,$$

其中 a_i 是 B 中的元素或者其逆元.

子群格

设 G 为群，令 $S = \{H | H \leq G\}$ 是 G 的所有子群的集合. 在 S 上定义关系 R 如下：

$$\forall H_1, H_2 \in S, \quad H_1 R H_2 \Leftrightarrow H_1 \leq H_2.$$

那么 $\langle S, R \rangle$ 构成偏序集，称作群 G 的 子群格 .

子群格

设 G 为群，令 $S = \{H | H \leq G\}$ 是 G 的所有子群的集合. 在 S 上定义关系 R 如下：

$$\forall H_1, H_2 \in S, \quad H_1 R H_2 \Leftrightarrow H_1 \leq H_2.$$

那么 $\langle S, R \rangle$ 构成偏序集，称作群 G 的 子群格 .

Klein 四元群 G 与模 12 加群 $\mathbb{Z}_{12}$ 的子群格如图 1.2.1 所示.

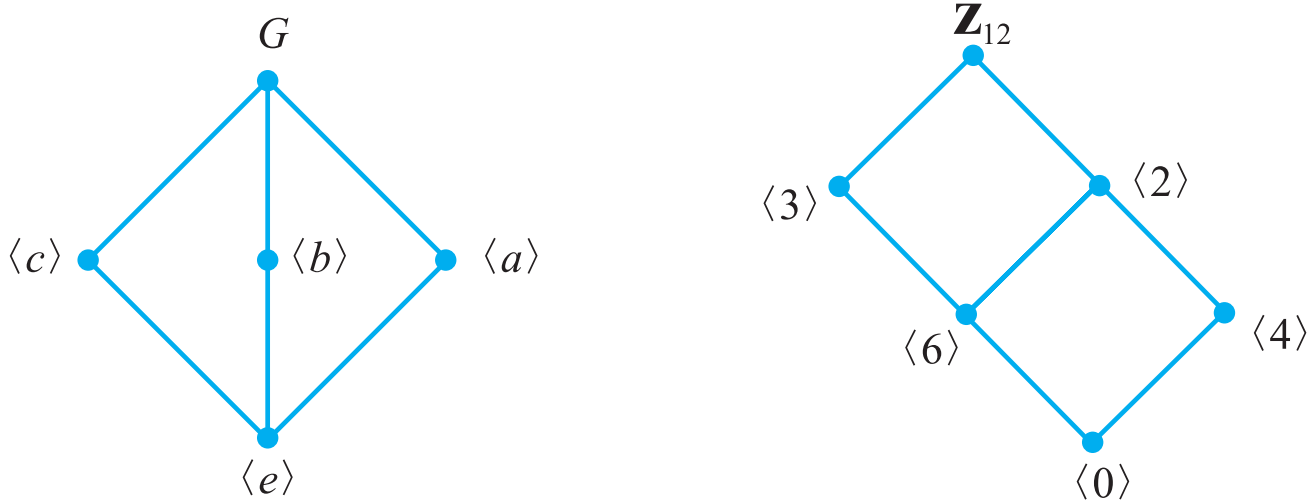


图 1.2.1

陪集

定义 1.2.2

设 H 是群 G 的子群, $a \in G$. 令

$$Ha = \{ha | h \in H\},$$

称 Ha 是子群 H 在 G 中的右陪集 ,称 a 为 Ha 的代表元素 .

陪集

定义 1.2.2

设 H 是群 G 的子群，$a \in G$. 令

$$Ha = \{ha | h \in H\},$$

称 Ha 是子群 H 在 G 中的右陪集，称 a 为 Ha 的代表元素.

例 1.2.4

设 $G = \{e, a, b, c\}$ 是 *Klein* 四元群，$H = \{e, a\}$ 是 G 的子群. 那么 H 的所有的右陪集是：

$$He = \{e, a\} = H = Ha,$$
$$Hb = \{b, c\} = Hc.$$

不同的右陪集只有两个，即 H 和 Hb.

陪集的性质

定理 1.2.4

设 H 是群 G 的子群，则

1. $He = H$.
2. $\forall a \in G$ 有 $a \in Ha$.

陪集的性质

定理 1.2.4

设 H 是群 G 的子群，则

1. $He = H$.
2. $\forall a \in G$ 有 $a \in Ha$.

证明.

(1) $He = \{he | h \in H\} = \{h | h \in H\} = H$.

(2) 任取 $a \in G$，由 $a = ea$ 和 $ea \in Ha$ 得 $a \in Ha$. □

定理 1.2.5

设 H 是群 G 的子群，则 $\forall a, b \in G$，下述条件彼此等价：

1. $a \in Hb$.
2. $ab^{-1} \in H$.
3. $Ha = Hb$.

定理 1.2.5

设 H 是群 G 的子群，则 $\forall a, b \in G$，下述条件彼此等价：

1. $a \in Hb$.
2. $ab^{-1} \in H$.
3. $Ha = Hb$.

证明.

先证 (1) 与 (2) 等价，即 $a \in Hb$ 当且仅当 $ab^{-1} \in H$. 事实上，$a \in Hb$ 等价于 $\exists h \in H$ 使得 $a = hb$，即当且仅当 $\exists h \in H$ 使得 $ab^{-1} = h \in H$.

再证 (1) 与 (3) 等价，即 $a \in Hb$ 当且仅当 $Ha = Hb$.

充分性. 若 $Ha = Hb$，由 $a \in Ha$ 可知必有 $a \in Hb$.

必要性. 由 $a \in Hb$ 可知存在 $h \in H$ 使得 $a = hb$，即 $b = h^{-1}a$. 任取 $h_1 a \in Ha$，则有 $h_1 a = h_1(hb) = (h_1 h)b \in Hb$, 从而得到 $Ha \subseteq Hb$. 反之，任取 $h_1 b \in Hb$，则有 $h_1 b = h_1(h^{-1}a) = (h_1 h^{-1})a \in Ha$, 从而得到 $Hb \subseteq Ha$. 综上所述，$Ha = Hb$ 得证. □

定理 1.2.6

设 H 是群 G 的子群，在 G 上定义二元关系 R:$\forall a, b \in G$，

$$\langle a, b \rangle \in R \Leftrightarrow ab^{-1} \in H,$$

则 R 是 G 上等价关系，且 $[a]_R = Ha$.

定理 1.2.6

设 H 是群 G 的子群，在 G 上定义二元关系 R:$\forall a, b \in G$，

$$\langle a, b\rangle \in R \Leftrightarrow ab^{-1} \in H,$$

则 R 是 G 上等价关系，且 $[a]_R = Ha$.

证明.

为证明 R 是等价的，只需证明 R 满足自反、对称、传递性质. 这个证明留给读者思考. 这里只证明 $\forall a \in G, [a]_R = Ha$.

任取 $b \in G$，则有 $b \in [a]_R$ 当且仅当 $\langle a, b\rangle \in R$. 由定义，后者等价于 $ab^{-1} \in H$. 根据定理 1.2.5 有 $ab^{-1} \in H$ 等价于 $Ha = Hb$，后者成立当且仅当 $b \in Ha$. 由此可见，$b \in [a]_R$ 当且仅当 $b \in Ha$，从而证明了 $[a]_R = Ha$. □

推论 1.2.1

设 H 是群 G 的子群，则

1. $\forall a, b \in G, Ha = Hb$ 或 $Ha \cap Hb = \emptyset$.
2. $\cup\{Ha | a \in G\} = G$.

推论 1.2.1

设 H 是群 G 的子群，则

1. $\forall a, b \in G, Ha = Hb$ 或 $Ha \cap Hb = \emptyset$.
2. $\cup\{Ha | a \in G\} = G$.

证明.

由定理 1.2.6 和定理 ?? 可得. □

根据以上定理和推论可以知道，给定群 G 的一个子群 H，H 的所有右陪集的集合 $\{Ha | a \in G\}$ 恰好构成 G 的一个划分，而且可进一步证明，这个划分的所有划分块都与 H 等势，即 $\forall a \in G, Ha \approx H$.

左陪集

以上已经对子群 H 的右陪集及其性质进行了讨论，类似地，也可以定义 H 的左陪集：

$$aH = \{ah | h \in G\},\ a \in G,$$

左陪集

以上已经对子群 H 的右陪集及其性质进行了讨论，类似地，也可以定义 H 的左陪集：

$$aH = \{ah | h \in G\},\ a \in G,$$

并证明关于左陪集的下述性质：

1. $eH = H$.
2. $\forall a \in G, a \in aH$.
3. $\forall a, b \in G, a \in bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH$.
4. 若在 G 上如下定义二元关系 R，

   $$\forall a, b \in G,\ \langle a, b \rangle \in R \Leftrightarrow b^{-1}a \in H,$$

   则 R 是 G 上的等价关系，且 $[a]_R = aH$.
5. $\forall a \in G, H \approx aH$.

正规子群

一般说来，对于群 G 的子群 H 和元素 a，不能保证 $Ha = aH$. 但对于某些特殊的群或子群，这个性质是成立的.

定义 1.2.3

设 H 是群 G 的子群，如果对于所有的 $a \in G$ 都有 $aH = Ha$，那么称 H 为 G 的 正规子群 或 不变子群，记作 $H \trianglelefteq G$.

正规子群

一般说来，对于群 G 的子群 H 和元素 a，不能保证 $Ha = aH$. 但对于某些特殊的群或子群，这个性质是成立的.

定义 1.2.3

设 H 是群 G 的子群，如果对于所有的 $a \in G$ 都有 $aH = Ha$，那么称 H 为 G 的 正规子群 或 不变子群，记作 $H \trianglelefteq G$.

任何群 G 都有正规子群: $\{e\}$ 和 G. 当 G 是交换群时，G 的任意子群都是正规子群.

尽管 Ha 和 aH 可能不一样，但 H 在 G 中的右陪集的个数和左陪集的个数却是相等的. 事实上，令 $S = \{Ha | a \in G\}$ 和 $T = \{aH | a \in G\}$ 分别表示 H 的右陪集和左陪集的集合，定义函数

$$f : S \to T,\ f(Ha) = a^{-1}H,\ \forall a \in G.$$

不难证明 f 是 S 到 T 的双射函数.

拉格朗日定理

由于 H 在 G 中的右陪集的个数和左陪集的个数相等，今后不再区分右陪集数和左陪集数，而统称 H 在 G 中的陪集数，也称作 H 在 G 中的指数，记作 $[G:H]$.

下面著名的拉格朗日定理将给出 $[G:H]$ 和 $|G|$ 及 $|H|$ 间的关系.

拉格朗日定理

由于 H 在 G 中的右陪集的个数和左陪集的个数相等，今后不再区分右陪集数和左陪集数，而统称 H 在 G 中的陪集数，也称作 H 在 G 中的指数，记作 $[G:H]$. 下面著名的拉格朗日定理将给出 $[G:H]$ 和 $|G|$ 及 $|H|$ 间的关系.

定理 1.2.7

设 G 是有限群，$H \leq G$，则 $|G| = |H| \cdot [G:H]$.

证明.

设 $[G:H] = r, a_1, a_2, \cdots, a_r$ 分别是 H 的 r 个右陪集的代表元素. 根据定理 1.2.6 的推论1.2.1有 $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_r$.

由于这 r 个右陪集是两两不交的，所以有

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_r|.$$

因为 $|Ha_i| = |H|, i = 1, 2, \cdots, r$，所以将这些等式代入上式得

$$|G| = |H| \cdot r = |H| \cdot [G:H].$$

推论 1.2.2

设 G 是 n 阶群，则 $\forall a \in G, |a|$ 是 n 的因子，且有 $a^n = e$.

推论 1.2.2

设 G 是 n 阶群，则 $\forall a \in G, |a|$ 是 n 的因子，且有 $a^n = e$.

证明.

任取 $a \in G$，则 $\langle a \rangle$ 是 G 的子群. 由拉格朗日定理知 $\langle a \rangle$ 的阶是 n 的因子. 另一方面，$\langle a \rangle$ 是由 a 生成的子群，若 $|a| = r$，则 $\langle a \rangle = \{a^0 = e, a^1, a^2, \cdots, a^{r-1}\}$. 这说明 $\langle a \rangle$ 的阶与 $|a|$ 相等，所以 $|a|$ 是 n 的因子. 根据定理 1.1.31有 $a^n = e$.

推论 1.2.2

设 G 是 n 阶群，则 $\forall a \in G, |a|$ 是 n 的因子，且有 $a^n = e$.

证明.

任取 $a \in G$，则 $\langle a \rangle$ 是 G 的子群. 由拉格朗日定理知 $\langle a \rangle$ 的阶是 n 的因子. 另一方面，$\langle a \rangle$ 是由 a 生成的子群，若 $|a| = r$，则 $\langle a \rangle = \{a^0 = e, a^1, a^2, \cdots, a^{r-1}\}$. 这说明 $\langle a \rangle$ 的阶与 $|a|$ 相等，所以 $|a|$ 是 n 的因子. 根据定理 1.1.31有 $a^n = e$.

推论 1.2.3

设 G 是素数阶的群，则存在 $a \in G$ 使得 $G = \langle a \rangle$.

推论 1.2.2

设 G 是 n 阶群，则 $\forall a \in G, |a|$ 是 n 的因子，且有 $a^n = e$.

证明.

任取 $a \in G$，则 $\langle a \rangle$ 是 G 的子群. 由拉格朗日定理知 $\langle a \rangle$ 的阶是 n 的因子. 另一方面，$\langle a \rangle$ 是由 a 生成的子群，若 $|a| = r$，则 $\langle a \rangle = \{a^0 = e, a^1, a^2, \cdots, a^{r-1}\}$. 这说明 $\langle a \rangle$ 的阶与 $|a|$ 相等，所以 $|a|$ 是 n 的因子. 根据定理 1.1.31有 $a^n = e$.

推论 1.2.3

设 G 是素数阶的群，则存在 $a \in G$ 使得 $G = \langle a \rangle$.

证明.

设 $|G| = p, p$ 是素数. 由 $p \geqslant 2$ 知 G 中必存在非单位元. 任取 $a \in G, a \neq e$，则 $\langle a \rangle$ 是 G 的子群. 根据拉格朗日定理，$\langle a \rangle$ 的阶是 p 的因子，即 $\langle a \rangle$ 的阶是 p 或 1. 显然 $\langle a \rangle$ 的阶不等于 1. 这就得到 $|\langle a \rangle| = p = |G|$，故 $G = \langle a \rangle$. □

推论 1.2.2

设 G 是 n 阶群，则 $\forall a \in G, |a|$ 是 n 的因子，且有 $a^n = e$.

证明.

任取 $a \in G$，则 $\langle a \rangle$ 是 G 的子群. 由拉格朗日定理知 $\langle a \rangle$ 的阶是 n 的因子. 另一方面，$\langle a \rangle$ 是由 a 生成的子群，若 $|a| = r$，则 $\langle a \rangle = \{a^0 = e, a^1, a^2, \cdots, a^{r-1}\}$. 这说明 $\langle a \rangle$ 的阶与 $|a|$ 相等，所以 $|a|$ 是 n 的因子. 根据定理 1.1.31有 $a^n = e$.

推论 1.2.3

设 G 是素数阶的群，则存在 $a \in G$ 使得 $G = \langle a \rangle$.

证明.

设 $|G| = p, p$ 是素数. 由 $p \geqslant 2$ 知 G 中必存在非单位元. 任取 $a \in G, a \neq e$，则 $\langle a \rangle$ 是 G 的子群. 根据拉格朗日定理，$\langle a \rangle$ 的阶是 p 的因子，即 $\langle a \rangle$ 的阶是 p 或 1. 显然 $\langle a \rangle$ 的阶不等于 1. 这就得到 $|\langle a \rangle| = p = |G|$，故 $G = \langle a \rangle$. □

拉格朗日定理的逆命题并不为真. 尽管有时 r 是 n 的因子，但 n 阶群 G 中不一定含有 r 阶元. 例如，Klein 四元群中就没有 4 阶元.

例 1.2.5

证明 *6* 阶群中必含有 *3* 阶元.

例 1.2.5

证明 *6* 阶群中必含有 *3* 阶元.

证明.

设 G 是 6 阶群,由拉格朗日定理的推论1.2.2可知,G 中的元素只可能是 1 阶元、2 阶元、3 阶元或 6 阶元.

若 G 中含有 6 阶元,设这个 6 阶元是 a,则由定理1.1.33知 a^2 是 3 阶元.

若 G 中不含 6 阶元,下面证明 G 中必含有 3 阶元. 如若不然,G 中只含 1 阶元和 2 阶元,即 $\forall a \in G$,有 $a^2 = e$. 取 G 中两个不同的 2 阶元 a 和 b,则有 $(ab)(ab) = (ab)^2 = e$,故 $(ab)^{-1} = ab$. 另一方面,我们有 $(ab)^{-1} = b^{-1}a^{-1} = ba$. 从而有 $ab = ba$. 令

$$H = \{e, a, b, ab\},$$

易证 H 是 G 的子群,但 $|H| = 4, |G| = 6$,与拉格朗日定理矛盾. □

例 1.2.6

证明阶小于 *6* 的群都是 *Abel* 群.

例 1.2.6

证明阶小于 *6* 的群都是 *Abel* 群.

证明.

1 阶群是平凡的,显然是 Abel 群.

$2, 3$ 和 5 都是素数,由拉格朗日定理的推论 1.2.3 可知 2 阶群、3 阶群和 5 阶群都是由一个元素生成的群. 它们都是 Abel 群(见本章习题 13.26).

设 G 是 4 阶群. 若 G 中含有 4 阶元,如 a,则 $G = \langle a \rangle$,由刚才的分析可知 G 是 Abel 群. 若 G 中不含 4 阶元,根据拉格朗日定理,G 中只含 1 阶元和 2 阶元. 由本章习题 13.15 题可知 G 也是 Abel 群. □

Slepian 译码表

下面给出一个群分解的实际例子——Slepian 译码表.

考虑计算机通信中的一种编码 C. C 中的码字 $v = a_1 a_2 \cdots a_n, a_i \in \{0, 1\}$, 可以看作 $\{0, 1\}$ 集合上的 n 维向量,所有 2^n 个 n 维向量构成 n 维线性空间 F_2^n.

Slepian 译码表

下面给出一个群分解的实际例子——Slepian 译码表.

考虑计算机通信中的一种编码 C. C 中的码字 $v = a_1 a_2 \cdots a_n, a_i \in \{0, 1\}$, 可以看作 $\{0, 1\}$ 集合上的 n 维向量,所有 2^n 个 n 维向量构成 n 维线性空间 F_2^n. F_2^n 的一个 k 维子空间,称作 $\{0, 1\}$ 集合上的一个 k 维线性码,记作 $[n, k]$ 码. 由于 C 是 k 维的,因此存在 k 个线性无关的向量 $v_1, v_2, \cdots, v_k$ 作为 C 的一组基,任意 $v \in C$ 都可以唯一地表示成

$$v = x_1 v_1 + x_2 v_2 + \cdots + x_k v_k, \ x_i \in \{0, 1\}, i = 1, 2, \cdots, k.$$

于是 $|C| = 2^k$.

Slepian 译码表

下面给出一个群分解的实际例子——Slepian 译码表.

考虑计算机通信中的一种编码 C. C 中的码字 $v = a_1 a_2 \cdots a_n, a_i \in \{0, 1\}$, 可以看作 $\{0, 1\}$ 集合上的 n 维向量,所有 2^n 个 n 维向量构成 n 维线性空间 F_2^n. F_2^n 的一个 k 维子空间,称作 $\{0, 1\}$ 集合上的一个 k 维线性码,记作 $[n, k]$ 码. 由于 C 是 k 维的,因此存在 k 个线性无关的向量 $v_1, v_2, \cdots, v_k$ 作为 C 的一组基,任意 $v \in C$ 都可以唯一地表示成

$$v = x_1 v_1 + x_2 v_2 + \cdots + x_k v_k, \ x_i \in \{0, 1\}, i = 1, 2, \cdots, k.$$

于是 $|C| = 2^k$.

设 C 是 $\{0, 1\}$ 集合上的 $[n, k]$ 码,因为 C 关于向量加法封闭,向量加法满足结合律,单位元是 n 维 0 向量,向量 v 的加法逆元就是自身,于是 C 关于向量加法构成群,且是 F_2^n 的子群.

Slepian 译码表

下面给出一个群分解的实际例子——Slepian 译码表.

考虑计算机通信中的一种编码 C. C 中的码字 $v = a_1 a_2 \cdots a_n, a_i \in \{0, 1\}$, 可以看作 $\{0, 1\}$ 集合上的 n 维向量,所有 2^n 个 n 维向量构成 n 维线性空间 F_2^n. F_2^n 的一个 k 维子空间,称作 $\{0, 1\}$ 集合上的一个 k 维线性码,记作 $[n, k]$ 码. 由于 C 是 k 维的,因此存在 k 个线性无关的向量 $v_1, v_2, \cdots, v_k$ 作为 C 的一组基,任意 $v \in C$ 都可以唯一地表示成

$$v = x_1 v_1 + x_2 v_2 + \cdots + x_k v_k, \ x_i \in \{0, 1\}, i = 1, 2, \cdots, k.$$

于是 $|C| = 2^k$.

设 C 是 $\{0, 1\}$ 集合上的 $[n, k]$ 码,因为 C 关于向量加法封闭,向量加法满足结合律,单位元是 n 维 0 向量,向量 v 的加法逆元就是自身,于是 C 关于向量加法构成群,且是 F_2^n 的子群.

考虑 C 在 F_2^n 中的陪集 $C + a, a \in F_2^n$. 根据拉格朗日定理,不同的陪集有 2^{n-k} 个.

Slepian 译码表(续)

前面的例1.1.4中的编码就是一种 $[7,4]$ 码,把这个码记作 C_1.
C_1 有 $2^4=16$ 个码字,它们的前 4 位恰好从 0000 到 1111,后 3 个校验位根据公式由前 4 位确定. 即:

$$\begin{aligned} C_1 = \{&0000000, 0001011, 0010101, 0011110,\\ &0100110, 0101101, 0110011, 0111000,\\ &1000111, 1001100, 1010010, 1011001,\\ &1100001, 1101010, 1110100, 1111111\}. \end{aligned}$$

不难验证 $1000111, 0100110, 0010101, 0001011$ 是 C_1 的一组基.
C_1 在 F_2^7 中有 8 个不同的陪集.

Slepian 译码表(续)

下面考虑译码. 在信息传输中有干扰,有时发送的码字是 v,但接收到的向量 u 可能根本不是 C 中的码字. 这时需要对 u 进行纠错,一般将它译成 C 中与它最接近的码字(即不同的位数最少的码字,这个原则称作 最近距离译码原则).

Slepian 译码表(续)

下面考虑译码. 在信息传输中有干扰,有时发送的码字是 v,但接收到的向量 u 可能根本不是 C 中的码字. 这时需要对 u 进行纠错,一般将它译成 C 中与它最接近的码字(即不同的位数最少的码字,这个原则称作 *最近距离译码原则*).

C 的译码阵列由 F_2^n 中的全体向量构成,每个陪集占一行,共有 2^{n-k} 行 2^k 列. 构成规则如下:第一行由 C 中的全体码字构成;第二行是陪集 $C+a_1$,其中 a_1 是 F_2^n-C 中 1 的个数最少且数值最小的向量;第三行是陪集 $C+a_2$,其中 a_2 是 $F_2^n-C-(C+a_1)$ 中 1 的个数最少且数值最小的向量;等等. 称这个译码阵列为 *Slepian 译码表* .

Slepian 译码表(续)

下面考虑译码. 在信息传输中有干扰,有时发送的码字是 v,但接收到的向量 u 可能根本不是 C 中的码字. 这时需要对 u 进行纠错,一般将它译成 C 中与它最接近的码字(即不同的位数最少的码字,这个原则称作 最近距离译码原则).

C 的译码阵列由 F_2^n 中的全体向量构成,每个陪集占一行,共有 2^{n-k} 行 2^k 列. 构成规则如下:第一行由 C 中的全体码字构成;第二行是陪集 $C+a_1$,其中 a_1 是 F_2^n-C 中 1 的个数最少且数值最小的向量;第三行是陪集 $C+a_2$,其中 a_2 是 $F_2^n-C-(C+a_1)$ 中 1 的个数最少且数值最小的向量;等等. 称这个译码阵列为 Slepian 译码表 .

假设接收到的 u 属于陪集 $C+a_j$,由阵列的构成知道 a_j 恰好排在这一行的第一列,这时将 u 译作 $u+a_j$. 因为 $a_j+a_j=0$(这里的 0 指 0 向量),所以 $u=v+a_j$ 当且仅当 $v=u+a_j$. 把译码表的第一列称作错误向量. 可以证明这种译码方法符合最近距离译码原则.

Slepian 译码表(续)

下面以一个简单的码 $C = \{0000, 0110, 1001, 1111\}$ 来说明这种译码方法.
码 C 是一个 $[4, 2]$ 码,它的一组基是 $\{0110, 1001\}$. 整个向量空间 F_2^4 有 16 个向量,C 在 F_2^4 中有 4 个陪集,因此 C 的 Slepian 译码表有 4 行,如下表所示,第一行恰好就是码 C.

编码	错误向量			
C	0000	0110	1001	1111
$C + 0001$	0001	0111	1000	1110
$C + 0010$	0010	0100	1011	1101
$C + 0011$	0011	0101	1010	1100

Slepian 译码表(续)

下面以一个简单的码 $C = \{0000, 0110, 1001, 1111\}$ 来说明这种译码方法.
码 C 是一个 $[4, 2]$ 码,它的一组基是 $\{0110, 1001\}$. 整个向量空间 F_2^4 有 16 个向量,C 在 F_2^4 中有 4 个陪集,因此 C 的 Slepian 译码表有 4 行,如下表所示,第一行恰好就是码 C.

编码	错误向量			
C	0000	0110	1001	1111
$C + 0001$	0001	0111	1000	1110
$C + 0010$	0010	0100	1011	1101
$C + 0011$	0011	0101	1010	1100

如果接收到的是 1001,那么它就是 C 中的码字,在译码时就译作 1001;如果接收到的是 1101,这不是 C 中的码字,通过在表中查找,知道 1101 属于 $C + 0010$,找到错误向量 0010,于是将 1101 译作 $1101 + 0010 = 1111$,而 1111 恰好是 1101 所在列的第一个元素,这正是一个距它最近的码字.

13.3 循环群与置换群

定义 1.3.1

设 G 是群，若 $\exists a \in G$ 使得 $G = \langle a \rangle$，则称 G 为循环群，称 a 为 G 的生成元.

13.3 循环群与置换群

定义 1.3.1

设 G 是群，若 $\exists a \in G$ 使得 $G = \langle a \rangle$，则称 G 为*循环群*，称 a 为 G 的*生成元*.

循环群 $G = \langle a \rangle$ 根据生成元 a 的阶可以分成两类：*n 阶循环群* 和 *无限循环群*.

设 $G = \langle a \rangle$ 是循环群，若 a 是 n 阶元，则

$$G = \{a^0 = e, a^1, a^2, \cdots, a^{n-1}\},$$

那么 $|G| = n$，称 G 为 *n 阶循环群*.

13.3 循环群与置换群

定义 1.3.1

设 G 是群，若 $\exists a \in G$ 使得 $G = \langle a \rangle$，则称 G 为循环群，称 a 为 G 的生成元.

循环群 $G = \langle a \rangle$ 根据生成元 a 的阶可以分成两类：n 阶循环群 和 无限循环群.

设 $G = \langle a \rangle$ 是循环群，若 a 是 n 阶元，则

$$G = \{a^0 = e, a^1, a^2, \cdots, a^{n-1}\},$$

那么 $|G| = n$，称 G 为 n 阶循环群.

例如，模 6 整数加群 $\langle \mathbb{Z}_6, \oplus \rangle$ 是 6 阶循环群，它的生成元是 1 和 5.

13.3 循环群与置换群

定义 1.3.1

设 G 是群，若 $\exists a \in G$ 使得 $G = \langle a \rangle$，则称 G 为*循环群*，称 a 为 G 的*生成元*.

循环群 $G = \langle a \rangle$ 根据生成元 a 的阶可以分成两类：*n 阶循环群* 和 *无限循环群*.

设 $G = \langle a \rangle$ 是循环群，若 a 是 n 阶元，则

$$G = \{a^0 = e, a^1, a^2, \cdots, a^{n-1}\},$$

那么 $|G| = n$，称 G 为 *n 阶循环群*.

例如，模 6 整数加群 $\langle \mathbb{Z}_6, \oplus \rangle$ 是 6 阶循环群，它的生成元是 1 和 5.

若 a 是无限阶元，则

$$G = \{a^0 = e, a^{\pm 1}, a^{\pm 2}, \cdots\},$$

这时称 G 为*无限循环群*.

例如，整数加群 $\langle \mathbb{Z}, + \rangle$ 是无限循环群，它的生成元是 1 和 -1.

对于循环群 $G = \langle a \rangle$，它的生成元可能不只一个，怎样求出它的所有生成元呢？

定理 1.3.1

设 $G = \langle a \rangle$ 是循环群.

1. 若 G 是无限循环群，则 G 只有两个生成元，即 a 和 a^{-1}.
2. 若 G 是 n 阶循环群，则 G 含有 $\phi(n)$ 个生成元[a]. 对于任何不大于 n 且与 n 互素的正整数 r，a^r 是 G 的生成元.

[a] $\phi(n)$ 是欧拉函数，表示 $1, 2, \cdots, n$ 中与 n 互素的数的个数(见第 4.5 节).

对于循环群 $G=\langle a\rangle$，它的生成元可能不只一个，怎样求出它的所有生成元呢？

定理 1.3.1

设 $G=\langle a\rangle$ 是循环群.

1. 若 G 是无限循环群，则 G 只有两个生成元，即 a 和 a^{-1}.
2. 若 G 是 n 阶循环群，则 G 含有 $\phi(n)$ 个生成元[a]. 对于任何不大于 n 且与 n 互素的正整数 r，a^r 是 G 的生成元.

[a] $\phi(n)$ 是欧拉函数，表示 $1,2,\cdots,n$ 中与 n 互素的数的个数(见第 4.5 节).

证明.

(1) 显然 $\langle a^{-1}\rangle\subseteq G$. 为证明 $G\subseteq\langle a^{-1}\rangle$，只需证明对任意 $a^k\in G$，a^k 都可以表成 a^{-1} 的幂. 由定理 1.1.1 有 $a^k=(a^{-1})^{-k}$，从而得到 $G=\langle a^{-1}\rangle$，故 a^{-1} 是 G 的生成元.

再证明 G 只有 a 和 a^{-1} 这两个生成元. 假设 b 也是 G 的生成元，则 $G=\langle b\rangle$. 由 $a\in G$ 可知存在整数 t 使得 $a=b^t$. 又由 $b\in G=\langle a\rangle$ 可知存在整数 m 使得 $b=a^m$. 从而得到 $a=b^t=(a^m)^t=a^{mt}$，由 G 中的消去律得 $a^{mt-1}=e$.

定理1.3.1证明(续)

因为 G 是无限群,必有 $mt-1=0$. 从而证明了 $m=t=1$ 或 $m=t=-1$,即 $b=a$ 或 $b=a^{-1}$.

定理1.3.1证明(续)

因为 G 是无限群,必有 $mt-1=0$. 从而证明了 $m=t=1$ 或 $m=t=-1$,即 $b=a$ 或 $b=a^{-1}$.

(2) 当 $n=1$ 时显然成立,因此只需证明:当 $n>1$ 时,对任何正整数 $r<n, a^r$ 是 G 的生成元当且仅当 n 与 r 互素.

定理1.3.1证明(续)

因为 G 是无限群,必有 $mt-1=0$. 从而证明了 $m=t=1$ 或 $m=t=-1$,即 $b=a$ 或 $b=a^{-1}$.

(2) 当 $n=1$ 时显然成立,因此只需证明:当 $n>1$ 时,对任何正整数 $r<n, a^r$ 是 G 的生成元当且仅当 n 与 r 互素.

充分性. 设 r 与 n 互素,那么由定理??知,存在整数 u 和 v 使得 $ur+vn=1$. 因此由定理 1.1.1 和 $a^n=e$ 有

$$a=a^{ur+vn}=(a^r)^u(a^n)^v=(a^r)^u.$$

这意味着 $\forall a^k\in G, a^k=(a^r)^{uk}\in\langle a^r\rangle$,即 $G\subseteq\langle a^r\rangle$.

另一方面,显然有 $\langle a^r\rangle\subseteq G$,所以 a^r 是 G 的生成元.

定理1.3.1证明(续)

因为 G 是无限群,必有 $mt-1=0$. 从而证明了 $m=t=1$ 或 $m=t=-1$,即 $b=a$ 或 $b=a^{-1}$.

(2) 当 $n=1$ 时显然成立,因此只需证明:当 $n>1$ 时,对任何正整数 $r<n, a^r$ 是 G 的生成元当且仅当 n 与 r 互素.

充分性. 设 r 与 n 互素,那么由定理??知,存在整数 u 和 v 使得 $ur+vn=1$. 因此由定理 1.1.1 和 $a^n=e$ 有

$$a=a^{ur+vn}=(a^r)^u(a^n)^v=(a^r)^u.$$

这意味着 $\forall a^k\in G, a^k=(a^r)^{uk}\in\langle a^r\rangle$,即 $G\subseteq\langle a^r\rangle$.

另一方面,显然有 $\langle a^r\rangle\subseteq G$,所以 a^r 是 G 的生成元.

必要性. 设 a^r 是 G 的生成元,则 $|a^r|=n$. 令 r 和 n 的最大公因数为 d,则存在正整数 t 使得 $r=dt$,因此有

$$(a^r)^{\frac{n}{d}}=(a^{dt})^{\frac{n}{d}}=(a^n)^t=e.$$

根据定理 1.1.3 可知 $|a^r|$ 是 n/d 的因子,即 n 整除 n/d. 从而证明了 $d=1$,即 n 与 r 互素.

例 1.3.1

1. 设 $G = \langle \mathbb{Z}_9, \oplus \rangle$ 是模 *9* 的整数加群. 因为 $\phi(9) = 6$, 小于等于 *9* 且与 *9* 互素的正整数是 $1, 2, 4, 5, 7, 8$, 根据定理 *1.3.1*, G 的生成元是 $1, 2, 4, 5, 7$ 和 *8*.
2. 设 $G = 3\mathbb{Z} = \{3z | z \in \mathbb{Z}\}$, G 上的运算是普通加法, 那么 G 只有两个生成元: *3* 和 -3.

循环群的子群

定理 1.3.2

1. 设 $G = \langle a \rangle$ 是循环群，则 G 的子群仍是循环群.
2. 若 $G = \langle a \rangle$ 是无限循环群，则 G 的子群除 $\{e\}$ 以外都是无限循环群.
3. 若 $G = \langle a \rangle$ 是 n 阶循环群，则对 n 的每个正因子 d，G 恰好含有一个 d 阶子群.

循环群的子群

定理 1.3.2

1. 设 $G=\langle a\rangle$ 是循环群，则 G 的子群仍是循环群.
2. 若 $G=\langle a\rangle$ 是无限循环群，则 G 的子群除 $\{e\}$ 以外都是无限循环群.
3. 若 $G=\langle a\rangle$ 是 n 阶循环群，则对 n 的每个正因子 d，G 恰好含有一个 d 阶子群.

证明.

(1) 设 H 是 $G=\langle a\rangle$ 的子群，若 $H=\{e\}$，显然 H 是循环群；否则取 H 中的最小正方幂元 a^m，下面证明 a^m 是 H 的生成元.

易见 $\langle a^m\rangle \subseteq H$. 为证明 $H\subseteq\langle a^m\rangle$，只需证明 H 中的任何元素都可以表示成 a^m 的整数次幂. 任取 $a^l\in H$，由带余除法可知存在整数 q 和 r，使得 $l=qm+r$，其中 $0\leqslant r\leqslant m-1$，因此有

$$a^r=a^{l-qm}=a^l(a^m)^{-q}.$$

由 $a^l, a^m\in H$ 且 $H\leq G$ 可知 $a^r\in H$. 因为 a^m 是 H 中最小正方幂元，

定理1.3.2证明(续)

所以必有 $r = 0$. 这就得到 $a^l = (a^m)^q \in \langle a^m \rangle$.

定理1.3.2证明(续)

所以必有 $r = 0$. 这就得到 $a^l = (a^m)^q \in \langle a^m \rangle$.

(2) 设 $G = \langle a \rangle$ 是无限循环群, H 是 G 的子群. 若 $H \neq \{e\}$, 则根据上面证明可知 $H = \langle a^m \rangle$, 其中 a^m 为 H 中最小正方幂元. 假若 $|H| = t$, 则 $|a^m| = t$, 从而得到 $a^{mt} = e$. 这与 a 为无限阶元矛盾.

定理1.3.2证明(续)

所以必有 $r=0$. 这就得到 $a^l=(a^m)^q\in\langle a^m\rangle$.

(2) 设 $G=\langle a\rangle$ 是无限循环群, H 是 G 的子群. 若 $H\neq\{e\}$, 则根据上面证明可知 $H=\langle a^m\rangle$, 其中 a^m 为 H 中最小正方幂元. 假若 $|H|=t$, 则 $|a^m|=t$, 从而得到 $a^{mt}=e$. 这与 a 为无限阶元矛盾.

(3) 设 $G=\langle a\rangle$ 是 n 阶循环群, 则

$$G=\{a^0=e,a^1,\cdots,a^{n-1}\}.$$

根据拉格朗日定理, G 的每个子群的阶都是 n 的因子. 下面证明对于 n 的每个正因子 d 都存在一个 d 阶子群. 易见 $H=\langle a^{n/d}\rangle$ 是 G 的 d 阶子群. 假设 $H_1=\langle a^m\rangle$ 也是 G 的 d 阶子群, 其中 a^m 为 H_1 中的最小正方幂元, 则由 $(a^m)^d=e$ 可知, n 整除 md, 即 n/d 整除 m. 令 $m=(n/d)\cdot l$, 其中 l 是整数, 则有

$$a^m=(a^{n/d})^l\in H.$$

由此可见 $H_1\subseteq H$. 又由于 $|H_1|=|H|=d$, 所以有 $H_1=H$. □

根据上面定理的证明可得求循环群子群的方法：

如果 $G=\langle a\rangle$ 是无限循环群，那么 $\langle a^m\rangle$ 是 G 的子群，其中 m 是自然数，并且易证对于不同的自然数 m 和 t，$\langle a^m\rangle$ 和 $\langle a^t\rangle$ 是不同的子群.

如果 $G=\langle a\rangle$ 是 n 阶循环群，则先求出 n 的所有的正因子，对于每个正因子 d，$\langle a^{n/d}\rangle$ 是 G 的唯一的 d 阶子群.

根据上面定理的证明可得求循环群子群的方法：

如果 $G=\langle a\rangle$ 是无限循环群，那么 $\langle a^m\rangle$ 是 G 的子群，其中 m 是自然数，并且易证对于不同的自然数 m 和 t，$\langle a^m\rangle$ 和 $\langle a^t\rangle$ 是不同的子群.

如果 $G=\langle a\rangle$ 是 n 阶循环群，则先求出 n 的所有的正因子，对于每个正因子 d，$\langle a^{n/d}\rangle$ 是 G 的唯一的 d 阶子群.

例 1.3.2

设 G_1 是整数加群，G_2 是模 12 加群，分别求出 G_1 和 G_2 的所有子群.

根据上面定理的证明可得求循环群子群的方法：

如果 $G=\langle a\rangle$ 是无限循环群，那么 $\langle a^m\rangle$ 是 G 的子群，其中 m 是自然数，并且易证对于不同的自然数 m 和 t，$\langle a^m\rangle$ 和 $\langle a^t\rangle$ 是不同的子群.

如果 $G=\langle a\rangle$ 是 n 阶循环群，则先求出 n 的所有的正因子，对于每个正因子 d，$\langle a^{n/d}\rangle$ 是 G 的唯一的 d 阶子群.

例 1.3.2

设 G_1 是整数加群，G_2 是模 12 加群，分别求出 G_1 和 G_2 的所有子群.

解

G_1 的生成元为 1 和 -1. 易见 $1^m=m, m\in\mathbb{N}$，所以 G_1 的子群是 $m\mathbb{Z}, m\in\mathbb{N}$，即 $\langle 0\rangle=\{0\}=0\mathbb{Z}, \langle m\rangle=\{mz|z\in\mathbb{Z}\}=m\mathbb{Z}, m>0$.

G_2 是 12 阶循环群. 12 的正因子为 $1,2,3,4,6$ 和 12，因此 G_2 的子群是：

$\langle 12\rangle=\langle 0\rangle=\{0\}$	1 阶子群	$\langle 3\rangle=\{0,3,6,9\}$	4 阶子群
$\langle 6\rangle=\{0,6\}$	2 阶子群	$\langle 2\rangle=\{0,2,4,6,8,10\}$	6 阶子群
$\langle 4\rangle=\{0,4,8\}$	3 阶子群	$\langle 1\rangle=\mathbb{Z}_{12}$	12 阶子群

置换群

下面考虑另一类重要的群——置换群. 先定义 n 元置换和置换的乘法.

定义 1.3.2

设 $S=\{1,2,\cdots,n\}$, S 上的任何双射函数 $\sigma: S \to S$ 称为 S 上的 n 元置换.

一般将 n 元置换 σ 记作

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

置换群

下面考虑另一类重要的群——置换群. 先定义 n 元置换和置换的乘法.

定义 1.3.2

设 $S=\{1,2,\cdots,n\}$, S 上的任何双射函数 $\sigma: S \to S$ 称为 S 上的 n 元置换.

一般将 n 元置换 σ 记作

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

例如, $S=\{1,2,3,4,5\}$, 则

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

都是 5 元置换.

定义 1.3.3

设 σ, τ 是 n 元置换，σ 和 τ 的复合 $\sigma \circ \tau$ 也是 n 元置换，称作 σ 与 τ 的乘积，记作 $\sigma\tau$.

定义 1.3.3

设 σ,τ 是 n 元置换,σ 和 τ 的复合 $\sigma\circ\tau$ 也是 n 元置换,称作 σ 与 τ 的乘积,记作 $\sigma\tau$.

例如,上面的 5 元置换 σ 和 τ 有

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix},\quad \tau\sigma=\begin{pmatrix}1&2&3&4&5\\4&3&2&1&5\end{pmatrix}.$$

定义 1.3.3

设 σ,τ 是 n 元置换,σ 和 τ 的复合 $\sigma\circ\tau$ 也是 n 元置换,称作 σ 与 τ 的乘积,记作 $\sigma\tau$.

例如,上面的 5 元置换 σ 和 τ 有

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix},\quad \tau\sigma=\begin{pmatrix}1&2&3&4&5\\4&3&2&1&5\end{pmatrix}.$$

定义 1.3.4

设 σ 是 $S=\{1,2,\cdots,n\}$ 上的 n 元置换. 若

$$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ \cdots,\ \sigma(i_k\_1)=i_k,\ \sigma(i_k)=i_1,$$

且保持 S 中的其他元素不变,则称 σ 为 S 上的 k 阶轮换,记作 $(i_1\,i_2\cdots i_k)$. 若 $k=2$,称 σ 为 S 上的对换.

不交轮换

设 $S=\{1,2,\cdots,n\}$,对于 S 上的任何 n 元置换 σ 一定存在着一个有限序列 $i_1,i_2,\cdots,i_k,k\geqslant 1$,使得

$$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ \cdots,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1.$$

不交轮换

设 $S=\{1,2,\cdots,n\}$,对于 S 上的任何 n 元置换 σ 一定存在着一个有限序列 $i_1,i_2,\cdots,i_k,k\geqslant 1$,使得

$$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ \cdots,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1.$$

令 $\sigma_1=(i_1\,i_2\cdots i_k)$. 它是从 σ 中分解出来的第一个轮换. 根据函数的复合定义可以将 σ 写作 $\sigma_1\sigma'$,其中 σ' 作用于 $S-\{i_1,i_2,\cdots,i_k\}$ 上的元素. 继续对 σ' 进行类似的分解. 由于 S 中只有 n 个元素,所以经过有限步以后,必得到 σ 的轮换分解式

$$\sigma=\sigma_1\sigma_2\cdots\sigma_t.$$

不难看出,在上述分解式中任何两个轮换都作用于不同的元素上,称它们是 不交轮换.

不交轮换

设 $S=\{1,2,\cdots,n\}$,对于 S 上的任何 n 元置换 σ 一定存在着一个有限序列 $i_1,i_2,\cdots,i_k,k\geqslant 1$,使得

$$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ \cdots,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1.$$

令 $\sigma_1=(i_1\,i_2\cdots i_k)$. 它是从 σ 中分解出来的第一个轮换. 根据函数的复合定义可以将 σ 写作 $\sigma_1\sigma'$,其中 σ' 作用于 $S-\{i_1,i_2,\cdots,i_k\}$ 上的元素. 继续对 σ' 进行类似的分解. 由于 S 中只有 n 个元素,所以经过有限步以后,必得到 σ 的轮换分解式

$$\sigma=\sigma_1\sigma_2\cdots\sigma_t.$$

不难看出,在上述分解式中任何两个轮换都作用于不同的元素上,称它们是 不交轮换.

因此,可以说,任何 n 元置换都可以表示成不交轮换之积.

例 1.3.3

设 $S=\{1,2,\cdots,8\}$,

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\5&3&6&4&2&1&8&7\end{pmatrix}$$

是 8 元置换. 考虑 σ 的分解式,观察到

$$\sigma(1)=5,\ \sigma(5)=2,\ \sigma(2)=3,\ \sigma(3)=6,\ \sigma(6)=1,$$

所以从 σ 中分解出来的第一个轮换是 $(1\,5\,2\,3\,6)$,S 中剩下的元素是 $4,7,8$. 由 $\sigma(4)=4$ 得到 1 阶轮换 (4),它是从 σ 中分解出来的第二个轮换. 对于剩下的元素 7 和 8 有 $\sigma(7)=8,\sigma(8)=7$. 这样就得到第三个轮换 $(7\,8)$. 至此,S 中的元素都被分解完毕. 因此可以写出 σ 的轮换表示式 $\sigma=(1\,5\,2\,3\,6)(4)(7\,8)$. □

例 1.3.3

设 $S=\{1,2,\cdots,8\}$,

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\5&3&6&4&2&1&8&7\end{pmatrix}$$

是 8 元置换. 考虑 σ 的分解式,观察到

$$\sigma(1)=5,\ \sigma(5)=2,\ \sigma(2)=3,\ \sigma(3)=6,\ \sigma(6)=1,$$

所以从 σ 中分解出来的第一个轮换是 $(1\,5\,2\,3\,6)$,S 中剩下的元素是 $4,7,8$. 由 $\sigma(4)=4$ 得到 1 阶轮换 (4),它是从 σ 中分解出来的第二个轮换. 对于剩下的元素 7 和 8 有 $\sigma(7)=8,\sigma(8)=7$. 这样就得到第三个轮换 $(7\,8)$. 至此,S 中的元素都被分解完毕. 因此可以写出 σ 的轮换表示式 $\sigma=(1\,5\,2\,3\,6)(4)(7\,8)$. □

为了使得轮换表示式更为简洁,通常省略其中的 1 阶轮换. 例如,例1.3.3中的 σ 可以写作 $(1\,5\,2\,3\,6)(7\,8)$. 如果 n 元置换的轮换表示式中全是 1 阶轮换,如 8 元恒等置换 $(1)(2)\cdots(8)$,则只能省略其中的 7 个 1 阶轮换,而将它简记为 (1).

轮换表示

可以证明，将 n 元置换分解为不交轮换之积时，它的表示式是唯一的.
这里的唯一性是说，若

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t \quad \text{和} \quad \sigma = \tau_1\tau_2\cdots\tau_s$$

是 σ 的两个轮换表示式，则有

$$\{\sigma_1, \sigma_2, \cdots, \sigma_t\} = \{\tau_1, \tau_2, \cdots, \tau_s\}.$$

轮换表示

可以证明，将 n 元置换分解为不交轮换之积时，它的表示式是唯一的.
这里的唯一性是说，若

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t \quad \text{和} \quad \sigma = \tau_1\tau_2\cdots\tau_s$$

是 σ 的两个轮换表示式，则有

$$\{\sigma_1, \sigma_2, \cdots, \sigma_t\} = \{\tau_1, \tau_2, \cdots, \tau_s\}.$$

换句话说，由于分解式中的任意两个轮换都作用于 S 的不同元素上，根据函数复合的性质可以证明，交换轮换的次序以后得到的仍是相等的 n 元置换. 因此，在不考虑表示式中轮换的次序的情况下，该表示式是唯一的.

轮换表示

可以证明，将 n 元置换分解为不交轮换之积时，它的表示式是唯一的.
这里的唯一性是说，若

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t \quad \text{和} \quad \sigma = \tau_1\tau_2\cdots\tau_s$$

是 σ 的两个轮换表示式，则有

$$\{\sigma_1, \sigma_2, \cdots, \sigma_t\} = \{\tau_1, \tau_2, \cdots, \tau_s\}.$$

换句话说，由于分解式中的任意两个轮换都作用于 S 的不同元素上，根据函数复合的性质可以证明，交换轮换的次序以后得到的仍是相等的 n 元置换. 因此，在不考虑表示式中轮换的次序的情况下，该表示式是唯一的.
设 $S = \{1, 2, \cdots, n\}$，σ 是 S 上的 k 阶轮换，那么 σ 可以进一步表成对换之积.
事实上，不难证明

$$(i_1\ i_2\cdots\ i_k) = (i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_k).$$

轮换表示(续)

回顾关于 n 元置换的轮换表示,任何 n 元置换都可以唯一地表示成不交轮换之积,而任何轮换又可以进一步表示成对换之积,所以任何 n 元置换都可以表示成对换之积.

轮换表示(续)

回顾关于 n 元置换的轮换表示,任何 n 元置换都可以唯一地表示成不交轮换之积,而任何轮换又可以进一步表示成对换之积,所以任何 n 元置换都可以表示成对换之积.

例如,8 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

的轮换和对换表示式分别为 $\sigma = (1\,5\,2\,3\,6)(7\,8) = (1\,5)(1\,2)(1\,3)(1\,6)(7\,8)$.

轮换表示(续)

回顾关于 n 元置换的轮换表示,任何 n 元置换都可以唯一地表示成不交轮换之积,而任何轮换又可以进一步表示成对换之积,所以任何 n 元置换都可以表示成对换之积.

例如,8 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

的轮换和对换表示式分别为 $\sigma = (1\,5\,2\,3\,6)(7\,8) = (1\,5)(1\,2)(1\,3)(1\,6)(7\,8)$.

对换表示与轮换表示都是 n 元置换的表示式. 它们的不同点在于:轮换表示式中的轮换是不交的,而对换表示式中的对换是允许有交的. 轮换表示式是唯一的,而对换表示式是不唯一的.

轮换表示(续)

回顾关于 n 元置换的轮换表示,任何 n 元置换都可以唯一地表示成不交轮换之积,而任何轮换又可以进一步表示成对换之积,所以任何 n 元置换都可以表示成对换之积.

例如,8 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

的轮换和对换表示式分别为 $\sigma = (1\,5\,2\,3\,6)(7\,8) = (1\,5)(1\,2)(1\,3)(1\,6)(7\,8)$.

对换表示与轮换表示都是 n 元置换的表示式. 它们的不同点在于:轮换表示式中的轮换是不交的,而对换表示式中的对换是允许有交的. 轮换表示式是唯一的,而对换表示式是不唯一的.

例如,4 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

可以有下面不同的对换表示:$\sigma = (1\,2)(1\,3)$ 和 $\sigma = (1\,4)(2\,4)(3\,4)(1\,4)$.

n 元对称群

尽管 n 元置换的对换表示式是不唯一的，但可以证明表示式中所含对换个数的奇偶性是不变的.

例如，上面的 4 元置换只能表示成偶数个对换之积，而 4 元置换 $\tau = (1\,3\,2\,4)$ 只能表示成奇数个对换之积.

如果 n 元置换 σ 可以表示成奇数个对换之积，则称 σ 为奇置换，否则称 σ 为偶置换.

在偶置换和奇置换之间存在一一对应，因此奇置换和偶置换各有 $n!/2$ 个.

n 元对称群

尽管 n 元置换的对换表示式是不唯一的，但可以证明表示式中所含对换个数的奇偶性是不变的.

例如，上面的 4 元置换只能表示成偶数个对换之积，而 4 元置换 $\tau = (1\,3\,2\,4)$ 只能表示成奇数个对换之积.

如果 n 元置换 σ 可以表示成奇数个对换之积，则称 σ 为奇置换，否则称 σ 为偶置换.

在偶置换和奇置换之间存在一一对应，因此奇置换和偶置换各有 $n!/2$ 个.

考虑所有的 n 元置换构成的集合 S_n. 任何两个 n 元置换之积仍旧是 n 元置换，所以 S_n 关于置换的乘法是封闭的. 置换的乘法满足结合律. 恒等置换 (1) 是 S_n 中的单位元(见定理 ??). 对于任何 n 元置换 $\sigma \in S_n$，逆置换 $\sigma^{-1} \in S_n$ 是 σ 的逆元(见定理 ??). 这就证明了 S_n 关于置换的乘法构成一个群，称作 n 元对称群.

3 元对称群 S_3

例 1.3.4

设 $S = \{1, 2, 3\}$, 则 *3* 元对称群 $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, 其运算表如表 *1.3.1* 所示.

表 1.3.1

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(123)	(132)	(13)	(23)
(13)	(13)	(132)	(1)	(123)	(23)	(12)
(23)	(23)	(123)	(132)	(1)	(12)	(13)
(123)	(123)	(23)	(12)	(13)	(132)	(1)
(132)	(132)	(13)	(23)	(12)	(1)	(123)

n 元置换群

下面考虑 S_n 的子群. 设 A_n 是所有的 n 元偶置换的集合. 使用子群的判定定理不难证明 A_n 是 S_n 的子群,称作 n 元交错群.

例如, $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, 其中的偶置换是 $(1), (123)$ 和 (132), 因此 3 元交错群 $A_3 = \{(1), (123), (132)\}$.

n 元置换群

下面考虑 S_n 的子群. 设 A_n 是所有的 n 元偶置换的集合. 使用子群的判定定理不难证明 A_n 是 S_n 的子群,称作 n 元交错群.

例如, $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, 其中的偶置换是 $(1), (123)$ 和 (132), 因此 3 元交错群 $A_3 = \{(1), (123), (132)\}$.

对于 S_n 来说,它的所有子群都称作 n 元置换群,而 n 元对称群 S_n 和 n 元交错群 A_n 都是 n 元置换群的特例. 以 S_3 为例,除了 S_3 和 A_3 以外,它的其他子群是:

$\{(1), (12)\}$	2 阶子群
$\{(1), (13)\}$	2 阶子群
$\{(1), (23)\}$	2 阶子群
$\{(1)\}$	1 阶子群

这 3 个 2 阶子群都不是正规子群. 两个平凡子群和 A_3 是正规子群.

Polya 定理

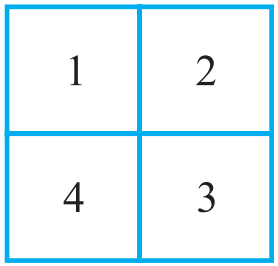


图 1.3.1

置换群经常出现在具有对称结构的实际应用中. 考虑下面一个着色问题的例子.

使用黑白两种颜色对图 1.3.1 中的方格图形进行着色,每个方格着一种颜色. 如果允许方格图形围绕中心点旋转,问不同的着色方案有多少种.

Polya 定理

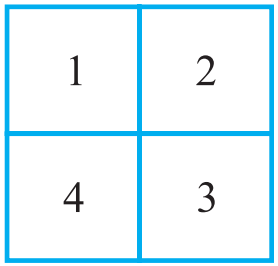


图 1.3.1

置换群经常出现在具有对称结构的实际应用中. 考虑下面一个着色问题的例子.

使用黑白两种颜色对图 1.3.1 中的方格图形进行着色,每个方格着一种颜色. 如果允许方格图形围绕中心点旋转,问不同的着色方案有多少种.

若不考虑图形的运动,每个方格有 2 种颜色选择,总计有 16 个着色方案.

围绕中心逆时针旋转有 4 种可能:$0°, 90°, 180°, 270°$. 这些旋转作用在方格上,由于方格上的文字被置换,从而导致了对着色方案的置换.

令 $N = \{1, 2, 3, 4\}$ 代表 4 个方格的集合,4 种旋转的集合 $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ 恰好构成 N 上的一个置换群. 如果一种方案在 G 中置换作用下变成另一种方案,就说这两个方案属于同一个轨道. 那么问题是:在 G 作用下对 N 上方格的着色方案被分解成多少个不同的轨道?

Polya 定理

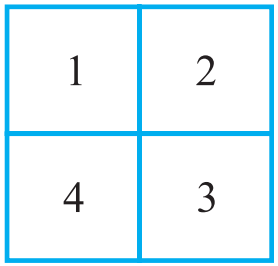


图 1.3.1

置换群经常出现在具有对称结构的实际应用中. 考虑下面一个着色问题的例子.

使用黑白两种颜色对图 1.3.1 中的方格图形进行着色,每个方格着一种颜色. 如果允许方格图形围绕中心点旋转,问不同的着色方案有多少种.

若不考虑图形的运动,每个方格有 2 种颜色选择,总计有 16 个着色方案.

围绕中心逆时针旋转有 4 种可能:$0°, 90°, 180°, 270°$. 这些旋转作用在方格上,由于方格上的文字被置换,从而导致了对着色方案的置换.

令 $N = \{1, 2, 3, 4\}$ 代表 4 个方格的集合,4 种旋转的集合 $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ 恰好构成 N 上的一个置换群. 如果一种方案在 G 中置换作用下变成另一种方案,就说这两个方案属于同一个轨道. 那么问题是:在 G 作用下对 N 上方格的着色方案被分解成多少个不同的轨道?

解决这个计数问题的定理叫做 Polya 定理,是组合学的基本定理之一,它与拉格朗日定理有着密切的关系. 限于篇幅,这里不加证明,而直接给出相关的结果. 后面还会看到它在证明费马小定理中的应用.

Polya 定理(续)

定理 1.3.3

设 $N = \{1, 2, \cdots, n\}$ 是被着色物体的集合, $G = \{\sigma_1, \sigma_2, \cdots, \sigma_g\}$ 是 N 上的置换群. 用 m 种颜色对 N 中的元素进行着色, 则在 G 的作用下不同的着色方案数是

$$M = \frac{1}{|G|} \cdot \sum_{k=1}^{g} m^{c(\sigma_k)},$$

其中, $c(\sigma_k)$ 是置换 σ_k 的轮换表示式中包含 *1* 阶轮换在内的轮换个数.

Polya 定理(续)

定理 1.3.3

设 $N=\{1,2,\cdots,n\}$ 是被着色物体的集合，$G=\{\sigma_1,\sigma_2,\cdots,\sigma_g\}$ 是 N 上的置换群. 用 m 种颜色对 N 中的元素进行着色，则在 G 的作用下不同的着色方案数是

$$M=\frac{1}{|G|}\cdot\sum_{k=1}^{g}m^{c(\sigma_k)},$$

其中，$c(\sigma_k)$ 是置换 σ_k 的轮换表示式中包含 *1* 阶轮换在内的轮换个数.

考虑上面的方格着色问题. 群 G 中的所有置换是：

$\sigma_1=(1)$, $\sigma_2=(1\,2\,3\,4)$,

$\sigma_3=(1\,3)(2\,4)$, $\sigma_4=(1\,4\,3\,2)$.

因此 $c(\sigma_1)=4$, $c(\sigma_2)=1$,

$c(\sigma_3)=2$, $c(\sigma_4)=1$.

代入 Polya 定理得

$$M=\frac{1}{4}(2^4+2^1+2^2+2^1)=6.$$

图 1.3.2 给出了这 6 种不同的着色方案.

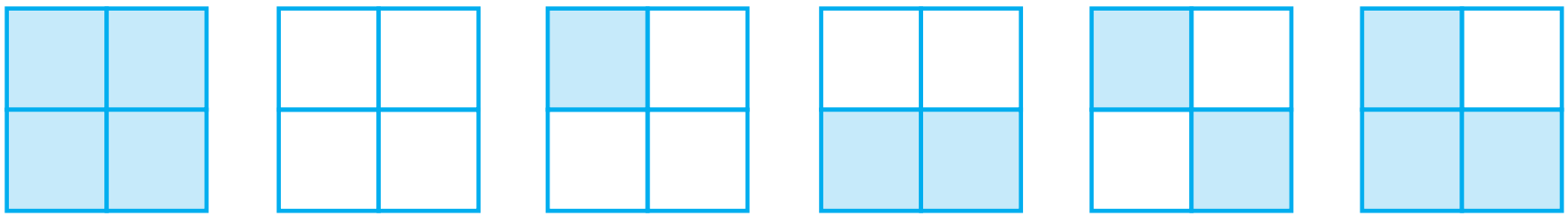


图 1.3.2

13.4 环与域

环是具有两个二元运算的代数系统，它和群及半群有着密切的联系.

定义 1.4.1

设 $\langle R, +, \cdot \rangle$ 是代数系统，$+$ 和 $\cdot$ 是二元运算，如果满足以下条件：

1. $\langle R, + \rangle$ 构成交换群；
2. $\langle R, \cdot \rangle$ 构成半群；
3. $\cdot$ 运算关于 $+$ 运算满足分配律，

那么称 $\langle R, +, \cdot \rangle$ 是一个 环 .

为了区别环中的两个运算，通常称 $+$ 运算为环中的加法，$\cdot$ 运算为环中的乘法.

例 1.4.1

1. 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环 $\mathbb{Z}$、有理数环 $\mathbb{Q}$、实数环 $\mathbb{R}$ 和复数环 $\mathbb{C}$.
2. $n(\geqslant 2)$ 阶实矩阵的集合 $M_n(\mathbb{R})$ 关于矩阵的加法和乘法构成环，称作 n 阶实矩阵环 .
3. 集合的幂集 $P(B)$ 关于集合的对称差运算和交运算构成环.
4. 设 $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$，$\oplus$ 和 $\otimes$ 分别表示模 n 加法和乘法，则 $\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 构成环，称作模 n 的整数环 .

例 1.4.1

1. 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为 整数环 $\mathbb{Z}$、有理数环 $\mathbb{Q}$、实数环 $\mathbb{R}$ 和 复数环 $\mathbb{C}$.
2. $n(\geqslant 2)$ 阶实矩阵的集合 $M_n(\mathbb{R})$ 关于矩阵的加法和乘法构成环，称作 n 阶实矩阵环 .
3. 集合的幂集 $P(B)$ 关于集合的对称差运算和交运算构成环.
4. 设 $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$，$\oplus$ 和 $\otimes$ 分别表示模 n 加法和乘法，则 $\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 构成环，称作 模 n 的整数环 .

为了今后叙述上的方便，将环中加法的单位元记作 0；乘法的单位元（当存在时）记作 1；对任何环中的元素 x，称 x 的加法逆元为负元，记作 $-x$. 若 x 存在乘法逆元，则将它称作逆元，记作 x^{-1}.

类似地，针对环中的加法，用 $x - y$ 表示 $x + (-y)$，nx 表示 $\underbrace{x + x + \cdots + x}_{n \text{ 个 } x}$，即 x 的 n 次加法幂，并且用 $-xy$ 表示 xy 的负元.

定理 1.4.1

设 $\langle R, +, \cdot \rangle$ 是环，则

1. $\forall a \in R, a0 = 0a = 0.$
2. $\forall a, b \in R, (-a)b = a(-b) = -ab.$
3. $\forall a, b, c \in R, a(b-c) = ab - ac, (b-c)a = ba - ca.$
4. $\forall a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m \in R$，其中 $n, m \geqslant 2$，有

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j.$$

定理 1.4.1

设 $\langle R, +, \cdot \rangle$ 是环，则

1. $\forall a \in R, a0 = 0a = 0.$
2. $\forall a, b \in R, (-a)b = a(-b) = -ab.$
3. $\forall a, b, c \in R, a(b-c) = ab - ac, (b-c)a = ba - ca.$
4. $\forall a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m \in R$，其中 $n, m \geqslant 2$，有

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j.$$

证明.

只证 (1),(2) 和 (4),(3) 留作练习.

(1) $\forall a \in R$，有 $a0 = a(0+0) = a0 + a0$，由环中加法的消去律得 $a0 = 0$. 同理可证 $0a = 0$.

(2) $\forall a, b \in R$，有 $(-a)b + ab = (-a+a)b = 0b = 0$,

$ab + (-a)b = (a + (-a))b = 0b = 0$，因此 $(-a)b$ 是 ab 的负元.

由负元的唯一性可知 $(-a)b = -ab$. 同理可证 $a(-b) = -ab$.

定理1.4.1证明(续)

(4) 先证 $\forall a_1, a_2, \cdots, a_n$ 有

$$\left(\sum_{i=1}^{n} a_i\right) b_j = \sum_{i=1}^{n} a_i b_j. \tag{1.4.1}$$

对 n 进行归纳. 当 $n = 2$ 时,由环中乘法对加法的分配律,等式显然成立.

假设 $\left(\sum_{i=1}^{n} a_i\right) b_j = \sum_{i=1}^{n} a_i b_j$,则有

$$\begin{aligned}\left(\sum_{i=1}^{n+1} a_i\right) b_j &= \left(\sum_{i=1}^{n} a_i + a_{n+1}\right) b_j \\ &= \left(\sum_{i=1}^{n} a_i\right) b_j + a_{n+1} b_j \\ &= \sum_{i=1}^{n} a_i b_j + a_{n+1} b_j = \sum_{i=1}^{n+1} a_i b_j.\end{aligned}$$

由归纳法式(1.4.1)得证.

同理可证,$\forall b_1, b_2, \cdots, b_m$ 有

$$a_i \left(\sum_{j=1}^{m} b_j\right) = \sum_{j=1}^{m} a_i b_j.$$

于是

$$\begin{aligned}&\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) \\ &= \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{m} b_j\right) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j.\end{aligned}$$

例 1.4.2

在环中计算 $(a+b)^3$ 和 $(a-b)^2$.

解

$$
\begin{aligned}
(a+b)^3 &= (a+b)(a+b)(a+b) \\
&= (a^2+ba+ab+b^2)(a+b) \\
&= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3. \\
(a-b)^2 &= (a-b)(a-b) = a^2-ba-ab+b^2.
\end{aligned}
$$

□

整环和域

按照代数系统的子代数和同态定义可以定义子环以及环同态与同构，这里不再赘述. 下面考虑两种特殊的环：整环和域.

定义 1.4.2

设 $\langle R, +, \cdot \rangle$ 是环.

1. 若环中乘法 $\cdot$ 满足交换律，则称 R 为 交换环 .
2. 若环中乘法 $\cdot$ 存在单位元，则称 R 为 含幺环 .
3. 若 $\forall a, b \in R$，当 $ab = 0$ 时，必然有 $a = 0$ 或 $b = 0$，则称 R 为 无零因子环 .
4. 若 R 既是交换环、含幺环，也是无零因子环，则称 R 为 整环 .
5. 设 R 是整环，$|R| \geq 2$，且 $\forall a \in R^* = R - \{0\}$，都有 $a^{-1} \in R$，则称 R 是 域 .

例 1.4.3

1. 整数环 $\mathbb{Z}$、有理数环 $\mathbb{Q}$、实数环 $\mathbb{R}$、复数环 $\mathbb{C}$ 都是交换环、含幺环、无零因子环和整环，其中有理数环 $\mathbb{Q}$、实数环 $\mathbb{R}$、复数环 $\mathbb{C}$ 是域.
2. 令 $2\mathbb{Z} = \{2z | z \in \mathbb{Z}\}$，则 $2\mathbb{Z}$ 关于普通的加法和乘法构成交换环和无零因子环，但不是含幺环和整环，因为 $1 \notin 2\mathbb{Z}$.
3. 设正整数 $n \geq 2$，则 n 阶实矩阵的集合 $M_n(\mathbb{R})$ 关于矩阵加法和乘法构成环，它是含幺环，但不是交换环和无零因子环，也不是整环.
4. $\mathbb{Z}_6$ 关于模 *6* 加法和乘法构成环，它是交换环、含幺环，但不是无零因子环和整环，因为 $2 \otimes 3 = 0$，但 *2* 和 *3* 都不是 *0*，称 *2* 为 $\mathbb{Z}_6$ 中的左零因子，*3* 为右零因子. 类似地，又有 $3 \otimes 2 = 0$，所以 *3* 也是左零因子. *2* 也是右零因子，它们都是零因子. 可以证明 $\mathbb{Z}_n$ 是域当且仅当 n 是素数.

例 1.4.4

设 p 为素数，证明 $\mathbb{Z}_p$ 是域.

例 1.4.4

设 p 为素数，证明 $\mathbb{Z}_p$ 是域.

证明.

因为 p 为素数，$p \geqslant 2$，所以 $|\mathbb{Z}_p| \geqslant 2$.

易见 $\mathbb{Z}_p$ 关于模 p 乘法可交换，单位元是 1. 假设 $i, j \in \mathbb{Z}_p$ 使得 $i \otimes j = 0$，由 $i \otimes j = 0$ 知，$p \mid ij$，故 $p \mid i$ 或 $p \mid j$，即 $i = 0$ 或 $j = 0$. 由此可见，$\mathbb{Z}_p$ 中无零因子，故 $\mathbb{Z}_p$ 为整环.

下面证明 $\mathbb{Z}_p$ 中每个非零元素都有逆元. 任取 $i \in \mathbb{Z}_p, i \neq 0$，令

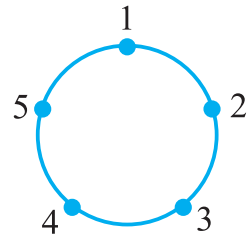
$$i \otimes \mathbb{Z}_p = \{i \otimes j | j \in \mathbb{Z}_p\},$$

则 $i \otimes \mathbb{Z}_p = \mathbb{Z}_p$，否则 $\exists j, k \in \mathbb{Z}_p, j \neq k$，使得 $i \otimes j = i \otimes k$. 于是 $i \otimes (j - k) = 0$，故 $p \mid i(j - k)$. 因为 $i \neq 0$，从而有 $p \mid (j - k)$，即 $j = k$，矛盾. 由于 $1 \in \mathbb{Z}_p$，故存在 $i' \in \mathbb{Z}_p$，使得 $i \otimes i' = 1$. 由于 $\otimes$ 运算的交换性，也有 $i' \otimes i = 1$，由此可见 i' 就是 i 的逆元，从而证明了 $\mathbb{Z}_p$ 是域. □

著名的费马小定理(我们在第 4 章给出了一种证明)给出了素数测试的必要非充分条件,满足这个条件的也可能是合数. 概率算法是目前大量使用的效率比较高的算法,下面先给出费马小定理的组合证明,然后简单介绍素数测试的概率算法.

定理 1.4.2

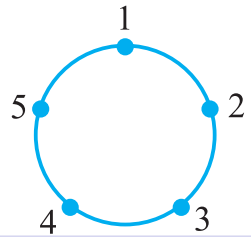
设 p 是素数,n 与 p 互素,则 $n^{p-1} \equiv 1 \pmod{p}$.



著名的费马小定理(我们在第 4 章给出了一种证明)给出了素数测试的必要非充分条件,满足这个条件的也可能是合数. 概率算法是目前大量使用的效率比较高的算法,下面先给出费马小定理的组合证明,然后简单介绍素数测试的概率算法.

定理 1.4.2

设 p 是素数,n 与 p 互素,则 $n^{p-1} \equiv 1 \pmod{p}$.



证明.

对于费马小定理有一个简单的组合证明. 考虑用 n 种颜色对具有 p 颗珠子的手镯进行着色. 这些珠子标记为 $1, 2, \cdots, p$,等距离地顺序排列在圆环上,右上图给出了 5 颗珠子的一个实例. 令 $\theta = 2\pi/p$,当手镯旋转的角度分别等于 θ, 2θ, $\cdots$, $p\theta$ 时就对应于 p 个置换作用于珠子上. 例如,旋转 θ 角的置换可以表示为轮换 $(1\,2\,\cdots\,p)$. 由于 p 是素数,除了 $p\theta = 2\pi$ 对应于恒等置换之外,其他 $p-1$ 个置换都由一个 p 阶轮换构成. 根据 Polya 定理,不同的着色方案数是

$$M = \frac{1}{p}[n^p + (p-1)n^1] = \frac{1}{p}(n^p - n) + n.$$

因为 M 和 n 都是正整数,因此 $n^p - n = n(n^{p-1} - 1)$ 能够被 p 整除,而 n 与 p 互素,故 $n^{p-1} \equiv 1 \pmod{p}$. □

下面再给出另一个素数测试条件，这里要用到有限域的知识.

一个有限域 F 是具有有限个元素的代数系统，其中 F 关于加法构成 Abel 群，$F^* = F - \{0\}$ 关于乘法也构成 Abel 群. 当 n 为素数时，$\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 就是含有 n 个元素的有限域，简记为 $\mathbb{Z}_n$.

下面再给出另一个素数测试条件，这里要用到有限域的知识.

一个有限域 F 是具有有限个元素的代数系统，其中 F 关于加法构成 Abel 群，$F^* = F - \{0\}$ 关于乘法也构成 Abel 群. 当 n 为素数时，$\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 就是含有 n 个元素的有限域，简记为 $\mathbb{Z}_n$.

命题 1.4.1

如果 n 为素数，那么在域 $\mathbb{Z}_n$ 中方程 $x^2 \equiv 1 \pmod{n}$ 的根只有两个，即 $x = 1$ 或 $x = n - 1$.

下面再给出另一个素数测试条件，这里要用到有限域的知识.

一个有限域 F 是具有有限个元素的代数系统，其中 F 关于加法构成 Abel 群，$F^* = F - \{0\}$ 关于乘法也构成 Abel 群. 当 n 为素数时，$\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 就是含有 n 个元素的有限域，简记为 $\mathbb{Z}_n$.

命题 1.4.1

如果 n 为素数，那么在域 $\mathbb{Z}_n$ 中方程 $x^2 \equiv 1 \pmod{n}$ 的根只有两个，即 $x = 1$ 或 $x = n - 1$.

证明.

设 x_0 是方程 $x^2 \equiv 1 \pmod{n}$ 的根，则有 $x_0^2 \equiv 1 \pmod{n}$，即 $(x_0 - 1)(x_0 + 1) = x_0^2 - 1 \equiv 0 \pmod{n}$. 因为域中没有零因子，所以 $x_0 - 1 \equiv 0 \pmod{n}$ 或 $x_0 + 1 \equiv 0 \pmod{n}$，故 $x_0 = 1$ 或 $x_0 = n - 1$. □

下面再给出另一个素数测试条件，这里要用到有限域的知识.

一个有限域 F 是具有有限个元素的代数系统，其中 F 关于加法构成 Abel 群，$F^* = F - \{0\}$ 关于乘法也构成 Abel 群. 当 n 为素数时，$\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 就是含有 n 个元素的有限域，简记为 $\mathbb{Z}_n$.

命题 1.4.1

如果 n 为素数，那么在域 $\mathbb{Z}_n$ 中方程 $x^2 \equiv 1 \pmod{n}$ 的根只有两个，即 $x = 1$ 或 $x = n - 1$.

证明.

设 x_0 是方程 $x^2 \equiv 1 \pmod{n}$ 的根，则有 $x_0^2 \equiv 1 \pmod{n}$，即 $(x_0 - 1)(x_0 + 1) = x_0^2 - 1 \equiv 0 \pmod{n}$. 因为域中没有零因子，所以 $x_0 - 1 \equiv 0 \pmod{n}$ 或 $x_0 + 1 \equiv 0 \pmod{n}$，故 $x_0 = 1$ 或 $x_0 = n - 1$. □

称不同于 1 和 $n - 1$ 的根为非平凡的根.

例如 $n = 12$ 时，$x^2 \equiv 1 \pmod{12}$ 当且仅当 $x = 1, 11, 5, 7$.

上式中 5 和 7 是非平凡的根. 根据命题1.4.1，如果方程有非平凡根，那么 n 必然为合数. 素数判断的问题可归结为 $x^2 \equiv 1 \pmod{n}$ 是否存在非平凡根的问题.

设 n 为奇素数，根据除法，存在正整数 q 和 m，其中 $q \geqslant 1, m$ 为奇数，使得 $n-1=2^q m$. 给定与 n 互素的正整数 a，令 $k=0,1,\cdots,q$，从而得到通项公式为 $a^{2^k m} \mod n$ 的序列：$a^m \mod n,\ a^{2m} \mod n,\ a^{4m} \mod n,\ \cdots,\ a^{2^q m} \mod n$.

设 n 为奇素数，根据除法，存在正整数 q 和 m，其中 $q \geqslant 1, m$ 为奇数，使得 $n-1=2^q m$. 给定与 n 互素的正整数 a，令 $k=0,1,\cdots,q$，从而得到通项公式为 $a^{2^k m} \mod n$ 的序列：$a^m \mod n,\ a^{2m} \mod n,\ a^{4m} \mod n,\ \cdots,\ a^{2^q m} \mod n$. 该序列的最后一项为 $a^{n-1} \mod n$，而且每一项是前面一项的平方. 根据费马小定理，对于素数 n，一定有 $a^{n-1} \equiv 1 \pmod n$. 因此上述序列的最后一项，即 $k=q$ 的项应该等于 1. 根据命题1.4.1，它的前一项，也就是 $k=q-1$ 的项应该等于 1 或 $n-1$. 如果该项等于 1，那么 $k=q-2$ 的项也应该等于 1 或 $n-1$. 照此进行，依次检查序列的各项，判断 $a^{2^k m} \mod n$ 是否为 1 和 $n-1$，且它的后一项是否为 1. 如果存在某一项，如第 k 项，不等于 1 和 $n-1$，但是第 $k+1$ 项等于 1，从而知道 n 不是素数.

设 n 为奇素数，根据除法，存在正整数 q 和 m，其中 $q \geqslant 1, m$ 为奇数，使得 $n-1=2^q m$. 给定与 n 互素的正整数 a，令 $k=0,1,\cdots,q$，从而得到通项公式为 $a^{2^k m} \mod n$ 的序列：$a^m \mod n,\ a^{2m} \mod n,\ a^{4m} \mod n,\ \cdots,\ a^{2^q m} \mod n$. 该序列的最后一项为 $a^{n-1} \mod n$，而且每一项是前面一项的平方. 根据费马小定理，对于素数 n，一定有 $a^{n-1} \equiv 1 \pmod n$. 因此上述序列的最后一项，即 $k=q$ 的项应该等于 1. 根据命题1.4.1，它的前一项，也就是 $k=q-1$ 的项应该等于 1 或 $n-1$. 如果该项等于 1，那么 $k=q-2$ 的项也应该等于 1 或 $n-1$. 照此进行，依次检查序列的各项，判断 $a^{2^k m} \mod n$ 是否为 1 和 $n-1$，且它的后一项是否为 1. 如果存在某一项，如第 k 项，不等于 1 和 $n-1$，但是第 $k+1$ 项等于 1，从而知道 n 不是素数.

例如 $n=561$，那么 $n-1=560=2^4 \cdot 35$. 假设 $a=7$，构造的序列为

$$7^{35} \mod 561 = 241,\ 7^{70} \mod 561 = 298,\ 7^{2^2 \times 35} \mod 561 = 166,$$
$$7^{2^3 \times 35} \mod 561 = 67,\ 7^{2^4 \times 35} \mod 561 = 1.$$

第 5 项为 1，但是第 4 项等于 67，它既不等于 1 也不等于 560，是个非平凡的根，因此可以判定 561 为合数.

Miller–Rabin 算法

根据这个思想设计的计算机算法称为 Miller–Rabin 算法，它随机选择正整数 $a \in \{2, 3, \cdots, n-1\}$，然后进行上述测试.

Miller–Rabin 算法

根据这个思想设计的计算机算法称为 Miller–Rabin 算法，它随机选择正整数 $a \in \{2, 3, \cdots, n-1\}$，然后进行上述测试. **算法 Miller–Rabin(n)**

---

1 令 $n - 1 = 2^q m, q \geqslant 1, m$ 为奇数
2 $a \leftarrow \text{Random}(2, n-1)$ （随机选择 $a \in \{2, \cdots, n-1\}$）
3 $x_0 \leftarrow a^m \mod n$
4 **for** $i \leftarrow 1$ **to** q **do**
5 $\quad x_i \leftarrow x_{i-1}^2 \mod n$
6 $\quad$ **if** $x_i = 1$ *and* $x_{i-1} \neq 1$ *and* $x_{i-1} \neq n-1$ **then**
7 $\quad\quad$ **return** *composite*
8 **if** $x_q \neq 1$ **then return** *composite* ;
9 **return** *prime*

由于 a 是随机选择的，这种测试不能保证检查到所有可能出现非平凡根的情况，这种出错是由于对 a 的选择不当而引起的.

可以证明：在 n 为奇合数的情况下，出错的概率小于 $1/2$. 证明涉及较多的群论和数论的知识，这里只是介绍一下证明的主要思想.

可以证明：在 n 为奇合数的情况下，出错的概率小于 $1/2$. 证明涉及较多的群论和数论的知识，这里只是介绍一下证明的主要思想.

根据费马小定理，有 $a^{n-1} \equiv 1 \pmod{n}$，从而有 $aa^{n-2} \equiv 1 \pmod{n}$，因此存在整数 u, v 使得 $au + nv = 1$. 这是 a 与 n 互素的充要条件(见定理 ??)，于是 $(a, n) = 1$. 这说明所有出现错误的 a 都属于集合 $T = \{x \in \mathbb{Z}_n | (x, n) = 1\}$.

可以证明：在 n 为奇合数的情况下，出错的概率小于 $1/2$. 证明涉及较多的群论和数论的知识，这里只是介绍一下证明的主要思想.

根据费马小定理，有 $a^{n-1} \equiv 1 \pmod{n}$，从而有 $aa^{n-2} \equiv 1 \pmod{n}$，因此存在整数 u, v 使得 $au + nv = 1$. 这是 a 与 n 互素的充要条件(见定理 ??)，于是 $(a, n) = 1$. 这说明所有出现错误的 a 都属于集合 $T = \{x \in \mathbb{Z}_n | (x, n) = 1\}$.

根据习题 13.12，这个集合关于模 n 乘法构成 Abel 群，且 $|T| = \phi(n)$，这里的 $\phi(n)$ 是欧拉函数的值.

定义集合 $B = \{x | x \in T, x^{2^k m} \equiv 1 \pmod{n}$ 或 $x^{2^k m} \equiv n - 1 \pmod{n}\}$.

可以证明：在 n 为奇合数的情况下，出错的概率小于 $1/2$. 证明涉及较多的群论和数论的知识，这里只是介绍一下证明的主要思想.

根据费马小定理，有 $a^{n-1} \equiv 1 \pmod{n}$，从而有 $aa^{n-2} \equiv 1 \pmod{n}$，因此存在整数 u, v 使得 $au + nv = 1$. 这是 a 与 n 互素的充要条件(见定理 ??)，于是 $(a, n) = 1$. 这说明所有出现错误的 a 都属于集合 $T = \{x \in \mathbb{Z}_n | (x, n) = 1\}$.

根据习题 13.12，这个集合关于模 n 乘法构成 Abel 群，且 $|T| = \phi(n)$，这里的 $\phi(n)$ 是欧拉函数的值.

定义集合 $B = \{x | x \in T, x^{2^k m} \equiv 1 \pmod{n}$ 或 $x^{2^k m} \equiv n - 1 \pmod{n}\}$.

利用群和数论的知识，可以证明 B 构成 T 的真子群. 再根据拉格朗日定理，$|B|$ 小于 $\phi(n)$ 且整除 $\phi(n)$，因此至多是 $(n-1)/2$. 由于 B 中含有 1，而 $a \neq 1$，因此使得算法出错的 a 的个数少于 $(n-1)/2$. 这就证明了算法对于素数测试得到正确结果的概率大于 $1/2$.

可以证明：在 n 为奇合数的情况下，出错的概率小于 $1/2$. 证明涉及较多的群论和数论的知识，这里只是介绍一下证明的主要思想.

根据费马小定理，有 $a^{n-1} \equiv 1 \pmod{n}$，从而有 $aa^{n-2} \equiv 1 \pmod{n}$，因此存在整数 u, v 使得 $au + nv = 1$. 这是 a 与 n 互素的充要条件(见定理 ??)，于是 $(a, n) = 1$. 这说明所有出现错误的 a 都属于集合 $T = \{x \in \mathbb{Z}_n | (x, n) = 1\}$.

根据习题 13.12，这个集合关于模 n 乘法构成 Abel 群，且 $|T| = \phi(n)$，这里的 $\phi(n)$ 是欧拉函数的值.

定义集合 $B = \{x | x \in T, x^{2^k m} \equiv 1 \pmod{n}$ 或 $x^{2^k m} \equiv n - 1 \pmod{n}\}$.

利用群和数论的知识，可以证明 B 构成 T 的真子群. 再根据拉格朗日定理，$|B|$ 小于 $\phi(n)$ 且整除 $\phi(n)$，因此至多是 $(n-1)/2$. 由于 B 中含有 1，而 $a \neq 1$，因此使得算法出错的 a 的个数少于 $(n-1)/2$. 这就证明了算法对于素数测试得到正确结果的概率大于 $1/2$.

对这个算法重复运行 k 次，可以将出错概率降到至多 2^{-k}. 令 $k = \lceil \log n \rceil$，出错的概率 $\leqslant 2^{-k} \leqslant 1/n$，即算法给出正确答案的概率为 $1 - 1/n$. 换句话说，如果 n 为素数，那么算法输出素数；如果 n 为合数，那么算法以 $1 - 1/n$ 的概率输出“合数”. 考虑到算法较高的效率，在实际中 Miller–Rabin 算法是一个较好的算法.

最后介绍一个信息安全领域的重要研究课题——全同态加密技术. 2009 年 Craig Gentry 在他的博士学位论文里首次提出了一种基于理想格的全同态加密算法，其使用的全同态加密函数与代数系统中环的同态映射有着类似的性质.

最后介绍一个信息安全领域的重要研究课题——全同态加密技术. 2009 年 Craig Gentry 在他的博士学位论文里首次提出了一种基于理想格的全同态加密算法,其使用的全同态加密函数与代数系统中环的同态映射有着类似的性质. 举例说明如下. 设 M, S 分别代表明文空间和密文空间,x 和 y 是 M 中的数据 (x, y 的二进制表示可看作整数),$+, \cdot$ 分别表示加法运算和乘法运算. 令 $E : M \to S$ 是 M 上的加密函数. 定义同态加密函数如下.

最后介绍一个信息安全领域的重要研究课题——全同态加密技术. 2009 年 Craig Gentry 在他的博士学位论文里首次提出了一种基于理想格的全同态加密算法,其使用的全同态加密函数与代数系统中环的同态映射有着类似的性质. 举例说明如下. 设 M, S 分别代表明文空间和密文空间,x 和 y 是 M 中的数据 (x, y 的二进制表示可看作整数),$+, \cdot$ 分别表示加法运算和乘法运算. 令 $E : M \to S$ 是 M 上的加密函数. 定义同态加密函数如下.

1. 如果存在一个有效的算法 Add,使得 $Add(E(x), E(y)) = E(x + y)$ 成立,那么称加密函数 E 对加法运算是同态的.
2. 如果存在一个有效的算法 $Multi$,使得 $Multi(E(x), E(y)) = E(x \cdot y)$ 成立,那么称加密函数 E 对乘法运算是同态的.

最后介绍一个信息安全领域的重要研究课题——全同态加密技术. 2009 年 Craig Gentry 在他的博士学位论文里首次提出了一种基于理想格的全同态加密算法,其使用的全同态加密函数与代数系统中环的同态映射有着类似的性质. 举例说明如下. 设 M, S 分别代表明文空间和密文空间,x 和 y 是 M 中的数据(x, y 的二进制表示可看作整数),$+, \cdot$ 分别表示加法运算和乘法运算. 令 $E : M \to S$ 是 M 上的加密函数. 定义同态加密函数如下.

1. 如果存在一个有效的算法 Add,使得 $Add(E(x), E(y)) = E(x + y)$ 成立,那么称加密函数 E 对加法运算是同态的.
2. 如果存在一个有效的算法 $Multi$,使得 $Multi(E(x), E(y)) = E(x \cdot y)$ 成立,那么称加密函数 E 对乘法运算是同态的.

定义中的 Add、$Multi$ 是对加密后数据的处理算法. 定义中的等式左边先对 x 和 y 加密,然后利用 Add 或 $Multi$ 算法(分别对应于加法、乘法)对加密后的数据进行运算;而等式右边是对原始数据 x 和 y 先进行运算(加法、乘法),然后对运算后的数据进行加密. 如果函数是同态加密函数,那么两种处理的结果是一样的. 同时满足上述关于加法运算和乘法运算的同态加密函数称作全同态加密函数.

下面对 RSA 公钥密码的同态性进行简单的分析.

在 RSA 公钥密码体制中,假设明文是 m,密文是 c.

下面对 RSA 公钥密码的同态性进行简单的分析.

在 RSA 公钥密码体制中,假设明文是 m,密文是 c.

选取两个不相等的大素数 p, q,令 $n = pq$,且 $m < n$. 根据欧拉函数的公式(见例 ??),有

$$\phi(n) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1).$$

选择大整数 w 使得 w 与 $\phi(n)$ 互素.

下面对 RSA 公钥密码的同态性进行简单的分析.

在 RSA 公钥密码体制中,假设明文是 m,密文是 c.

选取两个不相等的大素数 p, q,令 $n = pq$,且 $m < n$. 根据欧拉函数的公式(见例 ??),有

$$\phi(n) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1).$$

选择大整数 w 使得 w 与 $\phi(n)$ 互素.

令 d 是 w 的模 $\phi(n)$ 乘法逆元,即 $dw \equiv 1 \pmod{\phi(n)}$,则取公钥为 (w, n),私钥为 d.

用公钥对数据 m 加密,得到密文 c,然后用私钥 d 对密文 c 解密.

下面对 RSA 公钥密码的同态性进行简单的分析.

在 RSA 公钥密码体制中,假设明文是 m,密文是 c.

选取两个不相等的大素数 p, q,令 $n = pq$,且 $m < n$. 根据欧拉函数的公式(见例 ??),有

$$\phi(n) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1).$$

选择大整数 w 使得 w 与 $\phi(n)$ 互素.

令 d 是 w 的模 $\phi(n)$ 乘法逆元,即 $dw \equiv 1 \pmod{\phi(n)}$,则取公钥为 (w, n),私钥为 d.

用公钥对数据 m 加密,得到密文 c,然后用私钥 d 对密文 c 解密.

形式化描述如下.

$$\text{加密算法}: c = E(m) = m^w \mod n;$$

$$\text{解密算法}: D(c) = c^d \mod n.$$

RSA 解密算法的正确性在第 4.7 节给出了证明.

对于任意明文 m_1 和 m_2，有

$$E(m_1 \cdot m_2) = (m_1 \cdot m_2)^w \mod n = m_1^w \mod n \otimes m_2^w \mod n = E(m_1) \otimes E(m_2).$$

这就证明了 RSA 加密函数对乘法满足同态性质，其中 $\otimes$ 代表模 n 乘法. 但是对于加法，有以下结果：

$$E(m_1 + m_2) = (m_1 + m_2)^w \mod n,$$
$$E(m_1) \oplus E(m_2) = (m_1^w \mod n) \oplus (m_2^w \mod n).$$

两个等式的右边可能是不相等的，因此加密函数对加法不满足同态性质.

对于任意明文 m_1 和 m_2，有

$$E(m_1 \cdot m_2) = (m_1 \cdot m_2)^w \mod n = m_1^w \mod n \otimes m_2^w \mod n = E(m_1) \otimes E(m_2).$$

这就证明了 RSA 加密函数对乘法满足同态性质，其中 $\otimes$ 代表模 n 乘法. 但是对于加法，有以下结果：

$$E(m_1 + m_2) = (m_1 + m_2)^w \mod n,$$
$$E(m_1) \oplus E(m_2) = (m_1^w \mod n) \oplus (m_2^w \mod n).$$

两个等式的右边可能是不相等的，因此加密函数对加法不满足同态性质.
由于全同态加密技术不需要解密就可以对已加密的数据进行处理，并且与对原始数据直接处理的结果一样，这对于数据处理中的隐私保护有着重要的意义. 例如，在云计算中，用户可以将需要处理的数据加密后送到云端，云端服务器不需要解密就可以直接处理密文，然后将处理结果返回给用户. 用户收到处理过的数据，只要自己进行同态解密即可. 同态加密技术为解决物联网中海量数据的安全存储、高效检索和访问控制等提供了一个新的思路. 因此，研究一种高效的全同态加密解决方案不但具有理论价值，而且具有广泛的应用前景.