本章主要讲述如下问题

- 群的基本概念
- 子群的基本概念
- 常见的群
- 已学知识的抽象化
- 群同态、同构
- 群同态分解定理
- 应用

8.1 群

- **定义1** 设S 是一个非空集合. 那么$S \times S$ 到S 的映射叫做S 的**结合法**或**运算**; 对于这个映射, 元素对(a, b) 的像叫做a 与b 的**乘积**, 记成$a \otimes b$ 或$a \cdot b$ 或$a * b$ 等, 简记ab, 叫做**乘法**.
  也常叫做**加法**, (a, b) 的像叫做a 与b 的**和**, 记成$a \oplus b$ 或$a + b$.
- 始终设S 是一个具有结合法的非空集合.
- 如果任意a, b, c, 都有$(ab)c = a(bc)$, 则称该结合法满足**结合律**.

- **定义2** 如果S 满足结合律, 那么S 叫做S 的**半群**.
- 若对任意$a,\ b$, 有$ba = ab$, 则称该结合法满足交换律.
- 如果S 中有一个元素e 使得$ea = ae = a$ 对S 中所有元素a 都成立, 则称该元素e 为S 中的**单位元**.
- 当S 的结合法写作加法时, 这个e 叫做S 中的**零元**, 通常记作0.
- **性质1** : S 中的单位元e 是惟一的.
- **证** 设e 和e' 都是单位元.则$e' = ee' = e$. 因此, 单位元是惟一的.

- 设a 是S 中元素. 如果S 存在一个元素a' 使得$aa' = a'a = e$, 则称该元素a 为S 中的**可逆元**, a' 称为a 的**逆元**, 通常记作a^{-1}.
- 当结合法叫做加法时, 这个a' 叫做元素a 的负元, 通常记作$-a$.
- **性质2**：设S 是一个有单位元的半群. 则对S 中任意可逆元a, 其逆元a' 是惟一的.
- **证** 设a' 和a'' 都是a 的逆元, 即

$$aa' = a'a = e, \quad aa'' = a''a = e.$$

分别根据a' 和a'' 为a 的逆元及结合律, 得到

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

因此, a 的逆元a' 是惟一的.

- **定义3** 设G 是一个具有结合法的非空集合. 如果满足:
  (i) **结合律**, 即对任意的$a,\ b,\ c \in G$, 都有
  $$(ab)c = a(bc);$$
  (ii) **单位元**, 即存在一个元素$e \in G$, 使得对任意的$a \in G$, 都有$ae = ea = a$;
  (iii) **可逆性**, 即对任意的$a \in G$, 都存在$a' \in G$, 使得$aa' = a'a = e$,
  那么, G 叫做**一个群**.
- 特别地, 当G 的结合法写作乘法时, G 叫做**乘群**;
- 当G 的结合法写作加法时, G 叫做**加群**.

- 群G 的元素个数叫做群G 的**阶**, 记为$|G|$.
- 当$|G|$ 为有限数时, G 叫做**有限群**, 否则, G 叫做**无限群**.
- 如果群G 中的结合法还满足交换律, 即对任意的$a,\ b\in G$, 都有$ab=ba$, 那么, G 叫做**一个交换群或阿倍尔(Abel)群**.
- **例1** 自然数集$\mathbf{N}=\{1,2,\ldots,n,\ldots\}$
  对于通常意义下的加法有结合律, 但没有零元和逆元;
  而对于通常意义下的乘法, 有结合律和单位元$e=1$, 但没有可逆元.

$$2^{-1}=?$$

- **例2** 整数集

$$\mathbf{Z} = \{\ldots, -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, \ldots\}$$

对于通常意义下的加法, 有结合律, 交换律和零元0, 并且每个元素a 有负元$-a$. 因此, $\mathbf{Z}$ 是一个交换加群.

- 非零整数集$\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$ 对于通常意义下的乘法, 有结合律, 交换律和单位1, 但不是每个元素a 都有逆元, 因此$\mathbf{Z}^*$ 不是一个群.

- **例3** 有理数集$\mathbf{Q}$ 对于加法有结合律, 交换律和零元0, 并且每个元素a 有负元$-a$, 因此, $\mathbf{Q}$ 是交换加群.
- 非零有理数集$\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$ 对于乘法有结合律, 交换律和单位1, 并且每个元素a 都有逆元$a^{-1} = \dfrac{1}{a}$, 因此,$\mathbf{Q}^*$ 是交换乘群.
- 类似地, 实数集$\mathbf{R}$ 和复数集 $\mathbf{C}$ 都是交换加群. 而非零实数集$\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ 和非零复数集$\mathbf{C}^* = \mathbf{C} \setminus \{0\}$ 都是交换乘群.

- **例4** 设D是非平方整数. 则集合

$$\mathbf{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbf{Z}\}$$

对于加法运算:

$$(a + b\sqrt{D}) \oplus (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$$

构成一个交换加群.

- 但对于乘法运算

$$(a + b\sqrt{D}) \otimes (c + d\sqrt{D}) = (ac + bdD) + (bc + ad)\sqrt{D}$$

不构成一个乘群.

- **例5** 设n 是正整数. $\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, \ldots, n-1\}$. 证明: 集合$\mathbf{Z}/n\mathbf{Z}$ 对于加法:

$$a \oplus b = (a + b \pmod n)$$

构成一个交换加群, 其中$a \pmod n$ 是整数a 模n 的最小非负剩余.

零元是0, a 的负元是$n - a$. $n = 6$

$a \setminus x$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- **例6** 设p 是一个素数, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. 设$\mathbf{F}_p^* = \mathbf{F}_p \setminus \{0\}$.
  证明: 集合$\mathbf{F}_p^*$ 对于乘法:

$$a \otimes b = (a \cdot b \pmod p)$$

  构成一个交换乘群.
  单位元是1, a 的逆元是$(a^{-1} \pmod p)$. $\qquad p = 7$

$a \setminus x$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- **例7** 设n 是一个合数. 证明: 集合$\mathbf{Z}/n\mathbf{Z}\setminus\{0\}$ 对于乘法:

$$a\otimes b=(a\cdot b\,(\mathrm{mod}\,n))$$

不构成一个乘群.

单位元是1. 但n 的真因数d 没有逆元, 即对任意的$d'\in\mathbf{Z}/n\mathbf{Z}\setminus\{0\}$, 都有$d\otimes d'=(d\cdot d'\,(\mathrm{mod}\,n))\neq 1.$

- $n=6$

$a\setminus x$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

- **例8** n 是合数. $(\mathbf{Z}/n\mathbf{Z})^* = \{a | a \in \mathbf{Z}/n\mathbf{Z},\ (a, n) = 1\}$.
  证明: 集合$(\mathbf{Z}/n\mathbf{Z})^*$ 对于乘法:

$$a \otimes b = (a \cdot b \pmod{n})$$

  构成一个交换乘群.
  单位元是1, a 的逆元是$(a^{-1} \pmod{n})$. $n = 15$

$a \setminus x$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

- **例9** 设元素在数域$\mathbf{K}$ 中的n 级矩阵组成的集合

$$M_n(\mathbf{K}) = \{(a_{ij})_{1\le i\le n, 1\le j\le n} \mid a_{ij} \in \mathbf{K}\}.$$

- 设$A = (a_{ij}),\ B = (b_{ij}) \in M_n(\mathbf{K})$. 定义加法:

$A+B = C,\quad$ 其 $c_{ij} = a_{ij}+b_{ij},\ 1 \le i \le n, 1 \le j \le n.$

则$M_n(\mathbf{K})$ 对于加法构成一个交换群.

- $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$

零元$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, 负元$\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$

- **例9'** 设$A=(a_{ij}),\ B=(b_{ij}),\ C=(c_{ij})$. 定义乘法:

$$A\cdot B=C,\quad \text{其 } c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj},\ 1\le i,j\le n.$$

则$M_n(\mathbf{K})\setminus\{0\}$ 对于乘法不构成一个群.

- $$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\cdot\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}=\begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}$$

单位元$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, 但$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

- 可逆矩阵A 组成的集合对于矩阵的乘法成一个群, 记为$GL_n(P)$, 称为n 级一般线性群.

- **例10** 设S 是非空集合. G 是S 到自身的所有一一对应的映射f 组成的集合. 对于$f, g \in G$, 定义f 和g 的复合映射$g \circ f$ 为: 对于任意$x \in S$,

$$g \circ f(x) = g(f(x)).$$

则G 对于映射的复合运算, 构成群, 叫做**对称群**.
恒等映射是单位元.

- G 中的元素叫做S 的**一个置换**.
- 当S 是n 元有限集时, G 叫做n **元对称群**, 记作S_n. $|S_n| = n!$.
- $26! = 403291461126605635584000000 \approx 4 \cdot 10^{26} \approx 2^{88}$.

- **例10’** 3 元对称群S_3.

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

- **多个元素的运算** 设$a_1, a_2, \ldots, a_{n-1}, a_n$ 是群G 中的n 个元素. 通常归纳地定义这n 个元素的乘积为

$$a_1a_2\cdots a_{n-1}a_n = (a_1a_2\cdots a_{n-1})a_n.$$

- 当G 的结合法叫做加法时, 通常归纳地定义这n 个元素的和为

$$a_1 + a_2 + \cdots + a_{n-1} + a_n = (a_1 + a_2 + \cdots + a_{n-1}) + a_n.$$

- **性质3**：设$a_1, \ldots, a_n$ 是群G 中的任意$n \geq 2$ 个元素. 则对任意的$1 \leq i_1 < \ldots < i_k < n$, 有

$$(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1a_2\cdots a_{n-1}a_n.$$

- 证 对n 作归纳法. $n=3$ 时, $a_1(a_2a_3)=(a_1a_2)a_3=a_1a_2a_3$. 成立.

  假设$n-1$ 时成立. 对于n, 如果$i_{k+1}=n$, 则根据归纳假设,

$$
\begin{aligned}
(a_1\cdots a_{i_1})\cdots(a_{i_k+1}\cdots a_n) &= (a_1a_2\cdots a_{n-1})a_n \\
&= a_1a_2\cdots a_{n-1}a_n.
\end{aligned}
$$

  如果$i_{k+1}<n$, 则根据归纳假设和结合律,

$$
\begin{aligned}
& (a_1\cdots a_{i_1})\cdots(a_{i_{k-1}+1}\cdots a_{i_k})(a_{i_k+1}\cdots a_n) \\
= & (a_1\cdots a_{i_k})\cdot(a_{i_k+1}\cdots a_{n-1})a_n \\
= & (a_1a_2\cdots a_{n-1})a_n \\
= & a_1a_2\cdots a_{n-1}a_n.
\end{aligned}
$$

  因此, 结论对于n 成立. 由归纳法原理, 结论对任意n 成立.

- **性质4**：设$a_1, a_2, \ldots, a_n$ 是交换群G 中的任意n 个元素. 则对$1, 2, \ldots, n$ 的任一排列$i_1, i_2, \ldots, i_n$, 有

$$a_{i_1}a_{i_2}\cdots a_{i_n} = a_1a_2\cdots a_n.$$

- 证 对n 作归纳法. $n = 2$ 时, $a_2a_1 = a_1a_2$. 结论成立. 假设$n-1$ 成立. 对于n, 如果$i_n = n$, 则

$$a_{i_1}\cdots a_{i_{n-1}}a_{i_n} = (a_{i_1}\cdots a_{i_{n-1}})a_n$$

$$= (a_1a_2\cdots a_{n-1})a_n = a_1a_2\cdots a_{n-1}a_n.$$

如果$i_n < n$, $i_k = n$, 则由结合律, 交换律及前面结果,

$$\begin{aligned} a_{i_1}\cdots a_{i_k-1}a_{i_k}a_{i_k+1}\cdots a_{i_n} &= (a_{i_1}\cdots a_{i_k-1})a_n(a_{i_k+1}\cdots a_{i_n}) \\ &= (a_{i_1}\cdots a_{i_k-1})(a_{i_k+1}\cdots a_{i_n})a_n \\ &= a_1a_2\cdots a_{n-1}a_n. \end{aligned}$$

因此, 结论对于n 成立. 根据数学归纳法原理, 结论对任意n 成立. 证毕.

- 设n 是正整数.如果$a_1 = a_2 = \cdots = a_n = a$, 则记$a_1a_2\cdots a_n = a^n$, 称之为$a$ 的n 次幂. 特别地, 定义$a^0 = e$ 为单位元, $a^{-n} = (a^{-1})^n$ 为逆元a^{-1} 的n 次幂.
- **性质5**: 设$a \in G$, 则对任意$m,\ n \in \mathbf{Z}$,

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

- 证 (i) $m > 0,\ n > 0$. 有

$$a^m a^n = a^{m+n}, \quad a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

(ii) $m = 0,\ n > 0$. 有$a^m a^n = ea^n = a^{m+n}, \quad (a^m)^n = (a^0)^n = e = a^{mn}$.

- (iii) $m < 0,\ n > 0$. 有

$$a^m a^n = (a^{-1})^{-m} a^n = \begin{cases} a^{n-(-m)} = a^{m+n} & \text{如}J\ \ -m < n \\ e = a^{m+n} & \text{如}J\ \ -m = n \\ (a^{-1})^{-m-n} = a^{m+n} & \text{如}J\ \ -m > n \end{cases},$$

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

(iv) $n = 0$.

$$a^m a^n = a^m e = a^m = a^{m+n}, \quad (a^m)^n = e = a^{mn}.$$

(v) $m > 0,\ n < 0$. 类似(iii).

(vi) $m < 0,\ n < 0$. 有

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

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

因此, 性质5 成立.

- **定理1** 设$G \neq \emptyset$ 有结合法. 如果G 是一个群, 则方程$ax = b, \quad ya = b$ 在G 中有解. 反过来, 如果上述方程在G 中有解, 并且结合法满足结合律，则G 是一个群.

- **证** 设G 是一个群. 在$ax = b$ 两端左乘a^{-1}, 得到$a^{-1}(ax) = a^{-1}b$,
即$x = a^{-1}b$ 是$ax = b$ 的解. 同理, $y = ba^{-1}$ 是$ya = b$ 的解.

- 反过来, 设方程$ax = b, \quad ya = b$在G 中有解. 由$G \neq \emptyset$ 知存在$c \in G$, 并且$cx = c$ 有解$x = e_r$. 这个e_r 是G 中的(右)单位元. 事实上, 对任意$a \in G$, 因为$yc = a$ 有解, 所以$ae_r = (yc)e_r = y(ce_r) = yc = a$.
同理, $yc = c$ 的解$y = e_l$ 是G 中的(左)单位元.
因此, $e_r = e_l e_r = e_l = e$ 是G 中的单位元.

- 对G 中任意元素a, 设方程$ax = e, \quad ya = e$在G 中的解分别为$x = a', \ y = a''$. 则$a' = ea' = (a''a)a' = a''(aa') = a''e = a''$.
  因此, a' 是a 在G 中的逆元. 故G 是一个群.

- **定义4** 设H 是群G 的一个子集合. 如果对于群G 的结合法, H 成为一个群, 那么H 叫做群G 的**子群**, 记作$H \leq G$.
- $H = \{e\}$ 和$H = G$ 都是群G 的子群, 叫做群G 的**平凡子群**. 群G 的子群H 叫做群G 的**真子群**, 如果H 不是群G 的平凡子群.
- **例11** 设n 是一个正整数. 则$n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$ 是$\mathbf{Z}$ 的子群.

- **定理2** 设H 是群G 的非空子集. 则H 是群G 的子群的充要条件是: 对任意的$a, b \in H$, 有$ab^{-1} \in H$.
- **证** 必要性是显然的. 我们来证充分性.

  因为G 非空, 所以G 中有元素a. 根据假设, 我们有$e = aa^{-1} \in H$. 因此, H 中有单位元. 对于$e \in H$ 及任意a, 再应用假设, 我们有$a^{-1} = ea^{-1} \in H$, 即H 中每个元素a 在H 中有逆元. 因此, H 是群G 的子群. 证毕.

- **定理3** 设G 是一个群, $\{H_i\}_{i\in I}$ 是G 的一族子群. 则

$$\bigcap_{i\in I} H_i = H_1 \bigcap H_2 \bigcap \cdots \bigcap H_n \bigcap \cdots$$

是G 的一个子群.

- **证** 对任意的$a,\ b \in \bigcap_{i\in I} H_i$, 有

$$a,\ b \in H_i, \qquad i \in I.$$

因为H_i 是G 的子群, 根据定理2, 有$ab^{-1} \in H_i,\ i \in I$. 进而,

$$ab^{-1} \in \bigcap_{i\in I} H_i.$$

根据定理2, $\bigcap_{i\in I} H_i$ 是G 的一个子群.

- **定义5** 设G 是一个群, X 是G 的子集. 设$\{H_i\}_{i\in I}$ 是G 的包含X 的所有子群. 则
$$\bigcap_{i\in I} H_i$$
叫做G 的由X **生成的子群**. 记为$< X >$.
- X 的元素称为子群$< X >$ 的**生成元**.
- 如果$X = \{a_1, \ldots, a_n\}$, 则记$< X >$ 为
$$< X > = < a_1, \ldots, a_n > .$$
- 如果$G = < a_1, \ldots, a_n >$, 则称G 为**有限生成的**.
- 特别地, 如果$G = < a >$, 则称G 为a 生成的**循环群**.

- **定理4** 设G 是一个群, X 是G 的非空子集. 则由X 生成的子群为

$$< X >= \{a_1^{n_1}\cdots a_t^{n_t} \mid t \in \mathbf{N},\, a_i \in X,\, n_i \in \mathbf{Z},\, 1 \le i \le t\}$$

特别, 对任意的$a \in G$, 有$< a >= \{a^n \mid n \in \mathbf{Z}\}$.

- **证** 因X 非空, 所以

$$H_0 = \{a_1^{n_1}\cdots a_t^{n_t} | \, t \in N,\; a_i \in X,\; n_i \in Z,\; 1 \le i \le t\}$$

非空. $\forall x = a_1^{n_1}\cdots a_t^{n_t},\; y = a_{t+1}^{n_{t+1}}\cdots a_s^{n_s} \in H_0$, 有

$$x \cdot y^{-1} = a_1^{n_1}\cdots a_t^{n_t}\cdot a_s^{-n_s}\cdots a_{t+1}^{-n_{t+1}} \in H_0.$$

因此, H_0 是G 的子群. 再设H_j 是包含X 的任意子群. 则$\forall a = a_1^{n_1}\cdots a_t^{n_t} \in H_0$, $a_i \in X$, 有$a_i \in H_j$. 因为H_j 是子群, 所以$a \in H_j$. 即$H_0 \subset H_j$, $H_0 \subset \cap_j H_j$. 因此, $H_0 =< X >$ 是由X 生成的子群.

- **例12** 设

$$G=< g >= \{g^r \mid g^r \neq 1,\ 1 \leq r < n,\ g^n = 1\}.$$

G 是n 阶循环群. 则

$$< g^d >= \{g^{dk} \mid k \in \mathbf{Z}\}$$

是G 的子群.

§8.2 同态和同构

- **定义1** 设G, G' 是两个群, f 是G 到G' 的一个映射. 如果对任意的a, $b \in G$, 都有
$$f(ab) = f(a)f(b),$$
那么, f 叫做G 到G' 的一个**同态**.
- 由所有G 到G' 的同态组成的集合记作$\mathrm{Hom}(G, G')$.
- 如果f 是一对一的, 则称f 为**单同态**; 如果f 是满的, 则称f 为**满同态**; 如果f 是一一对应的, 则称f 为**同构**.
- 当$G = G'$ 时, 同态f 叫做**自同态**, 同构f 叫做**自同构**.

- **定义2** 设G, G' 是两个群. 我们称G 与G' **同构**, 如果存在一个G 到G' 的同构. 记作$G \cong G'$.
- 同构是对群的一个有效分类. 如果G, G' 是两个同构的群, 则它们拥有相同的代数结构. 这意味着, 借助于同构, 我们可以将群的运算转换为另一个已知群的运算, 进而可以更清楚地研究群的性质和运算规律.
- $f(e) = e', \quad f(a^{-1}) = f(a)^{-1}$.
- $ab = f^{-1}(f(a))f^{-1}(f(b)) = f^{-1}(f(a)f(b))$.
左端ab 是群G 的运算, 右端$f(a)f(b)$ 是群G' 的运算, 它们借助于f 关联.

- **定理1** 设f 是群G 到群G' 的一个同态. 则
  (i) $f(e) = e'$,
  (ii) 对任意$a \in G$, $f(a^{-1}) = f(a)^{-1}$.
  证 (i) 因为
  $$f(e)^2 = f(e^2) = f(e),$$
  所以$f(e) = e'$. 结论成立.
  (ii)由
  $$f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e',$$
  $$f(a)f(a^{-1}) = e',$$
  得$f(a^{-1}) = f(a)^{-1}$.

- **定理1**(续1) 设f 是群G 到群G' 的一个同态. 则
(iii) $\ker f = \{a \mid a \in G,\ f(a) = e'\}$ 是G 的子群, 且f 是单同态的充要条件是$\ker f = \{e\}$.
- **证** (iii) 对$\forall a,\ b \in \ker f$, 有$f(a) = e',\ f(b) = e'$. 从而,

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e'.$$

因此, $ab^{-1} \in \ker f$. 由§8.1 定理2, $\ker f$ 是G 的子群.
若f 是单同态, 则满足$f(a) = e' = f(e)$ 的元素只有$a = e$. 因此, $\ker f = \{e\}$.
反过来, 设$\ker f = \{e\}$. 则对任意的$a,\ b \in G$ 使得$f(a) = f(b)$, 有

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e'.$$

这说明, $ab^{-1} \in \ker f = \{e\}$ 或$a = b$. 故f 是单同态.

- **定理1**(续2) 设f 是群G 到群G' 的一个同态. 则

(iv) $f(G) = \{f(a) \mid a \in G\}$ 是G' 的子群,

且f 是满同态的充要条件是$f(G) = G'$.

证 (iv) 对任意x, $y \in f(G)$, 存在a, $b \in G$ 使得$f(a)x$, $f(b) = y$. 从而,

$$xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(G).$$

根据§8.1 定理2, $f(G)$ 是G' 的子群, 且f 是满同态的充要条件是$f(G) = G'$.

- **定理1**(续3) 设f 是群G 到群G' 的一个同态. 则
  (v) 设H' 是群G' 的子群, 则集合
  $$f^{-1}(H') = \{a \in G \mid f(a) \in H'\}$$
  是G 的子群.
  证 (v) 对任意$a, b \in f^{-1}(H')$, 根据(ii) 及H' 为子群, 我们有
  $$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in H',$$
  因此, $ab^{-1} \in f^{-1}(H')$. $f^{-1}(H')$ 是G 的子群. 证毕.
- $\ker f$ 叫做同态f 的核子群, $f(G)$ 叫做象子群.

- **例1** 加群$\mathbf{Z}$ 到乘群$G =< g >= \{g^n \mid n \in \mathbf{Z}\}$ 的映射$f : n \longmapsto g^n$ 是$\mathbf{Z}$ 到$< g >$ 的一个同态.

  因为对任意的$a, b \in \mathbf{Z}$, 有

  $$f(a + b) = g^{a+b} = g^a g^b = f(a)f(b).$$

- **例2** 加群$\mathbf{Z}$ 到乘群$\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ 的映射$f : a \longmapsto e^a$ 是$\mathbf{R}$ 到$\mathbf{R}^*$ 的一个同态.
- **例** 3 加群$\mathbf{Z}$ 到加群$\mathbf{Z}/n\mathbf{Z}$ 的映射$f : n \longmapsto g^n$ 是一个同态.
- **例** 4 加群$\mathbf{Z}$ 到乘群$G = \{\theta^k | \theta = e^{\frac{2\pi i}{n}},\ k \in \mathbf{Z}\}$ 的映射$f : k \longmapsto \theta^k$ 是一个同态.

- **例** 5 加群$\mathbf{Z}/n\mathbf{Z}$ 到乘群

$$G = \{\theta^k \mid \theta = e^{\frac{2\pi i}{n}},\ k = 0,\ 1,\ \ldots, n-1\}$$

的映射$f : k + n\mathbf{Z} \longmapsto \theta^k$ 是一个同构.

- **例6** 设a 是群G 的一个元. 那么映射

$$f : b \longmapsto aba^{-1}$$

是G 自同态. 事实上,

$$f(bc) = a(bc)a^{-1} = (aba^{-1})(aca^{-1}) = f(a)f(b).$$

§8.3 商 群

- **定义1** 设H 是群G 的子群, a 是G 中任意元. 那么集合

$$aH = \{ah \mid h \in H\}$$

(对应地

$$Ha = \{ha \mid h \in H\}$$

) 分别叫做G 中H 的左(右)**陪集**. aH (对应地Ha)中的元素叫做aH (对应地Ha) 的代表元. 如果$aH = Ha$, aH 叫做G 中H 的**陪集**

- **例1** 设$n > 1$ 是整数. 则$H = n\mathbf{Z}$ 是$\mathbf{Z}$ 的子群, 子集

$$a + n\mathbf{Z} = \{a + nk \mid k \in \mathbf{Z}\}$$

就是$n\mathbf{Z}$ 的陪集. 这个陪集就是模n 的剩余类.

- **例2** 3 元对称群S_3. 设

$$a_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=(1),\quad a_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(23),$$
$$a_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(13),\quad a_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12),$$
$$a_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(123),\ a_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132)$$

则$S_3=\{a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5\}$ 构成一个6 元群.

- $a_1\cdot a_2=a_4,\ a_1\cdot a_3=a_5,\ a_1\cdot a_4=a_2,\ a_1\cdot a_5=a_3,$
- $a_2\cdot a_1=a_5,\ a_2\cdot a_3=a_4,\ a_2\cdot a_4=a_3,\ a_2\cdot a_5=a_1,$
- $a_3\cdot a_1=a_4,\ a_3\cdot a_2=a_5,\ a_3\cdot a_4=a_1,\ a_3\cdot a_5=a_2,$
- $a_4\cdot a_1=a_3,\ a_4\cdot a_2=a_1,\ a_4\cdot a_3=a_2,\ a_4\cdot a_5=a_0,$
- $a_5\cdot a_1=a_2,\ a_5\cdot a_2=a_3,\ a_5\cdot a_3=a_1,\ a_5\cdot a_4=a_0.$

- 由单位元不变的置换组成一个子群$H_0 = \{a_0, a_1\}$.
- 保持1 不变的置换组成一个子群$H_1 = \{a_0, a_1\}$.
- 保持2 不变的置换组成一个子群$H_2 = \{a_0, a_2\}$.
- 保持3 不变的置换组成一个子群$H_3 = \{a_0, a_3\}$.
- 将3 个数作轮换的置换组成一个群$H_4 = \{a_0, a_4, a_5\}$.

- $H_1 = \{a_0, a_1\}$ 的左陪集:

$$a_0H_1 = \{a_0, a_1\}, \quad a_1H_1 = \{a_1, a_0\},$$
$$a_2H_1 = \{a_2, a_5\}, \quad a_5H_1 = \{a_5, a_2\},$$
$$a_3H_1 = \{a_3, a_4\}, \quad a_4H_1 = \{a_4, a_3\}.$$

- $H_1 = \{a_0, a_1\}$ 的右陪集:

$$H_1a_0 = \{a_0, a_1\}, \quad H_1a_1 = \{a_1, a_0\},$$
$$H_1a_2 = \{a_2, a_4\}, \quad H_1a_4 = \{a_4, a_2\},$$
$$H_1a_3 = \{a_3, a_5\}, \quad H_1a_5 = \{a_5, a_3\}.$$

- 左陪集与右陪集的比较

$$a_0H_1 = H_1a_0, \quad a_3H_1 \neq H_1a_3,$$
$$a_1H_1 = H_1a_1, \quad a_4H_1 \neq H_1a_4,$$
$$a_2H_1 \neq H_1a_2, \quad a_5H_1 \neq H_1a_5.$$

- $H_2 = \{a_0, a_2\}$ 的左陪集:

$$a_0H_2 = \{a_0, a_2\}, \quad a_2H_2 = \{a_2, a_0\},$$
$$a_1H_2 = \{a_1, a_4\}, \quad a_4H_2 = \{a_4, a_1\},$$
$$a_3H_2 = \{a_3, a_5\}, \quad a_5H_2 = \{a_5, a_3\}.$$

- $H_2 = \{a_0, a_2\}$ 的右陪集:

$$H_2a_0 = \{a_0, a_2\}, \quad H_2a_2 = \{a_2, a_0\},$$
$$H_2a_1 = \{a_1, a_5\}, \quad H_2a_5 = \{a_5, a_1\},$$
$$H_2a_3 = \{a_3, a_4\}, \quad H_2a_4 = \{a_4, a_3\}.$$

- 左陪集与右陪集的比较

$$a_0H_2 = H_2a_0, \quad a_3H_2 \neq H_2a_3,$$
$$a_1H_2 \neq H_2a_1, \quad a_4H_2 \neq H_2a_4,$$
$$a_2H_2 = H_2a_2, \quad a_5H_2 \neq H_2a_5.$$

- $H_3 = \{a_0, a_3\}$ 的左陪集:

$$a_0H_3 = \{a_0, a_3\}, \quad a_3H_3 = \{a_3, a_0\},$$
$$a_1H_3 = \{a_1, a_5\}, \quad a_5H_3 = \{a_5, a_1\},$$
$$a_2H_3 = \{a_2, a_4\}, \quad a_4H_3 = \{a_4, a_2\}.$$

- $H_3 = \{a_0, a_3\}$ 的右陪集:

$$H_3a_0 = \{a_0, a_3\}, \quad H_3a_3 = \{a_3, a_0\},$$
$$H_3a_1 = \{a_1, a_4\}, \quad H_3a_4 = \{a_4, a_1\},$$
$$H_3a_2 = \{a_2, a_5\}, \quad H_3a_5 = \{a_5, a_2\}.$$

- 左陪集与右陪集的比较

$$a_0H_3 = H_3a_0, \quad a_3H_3 = H_3a_3,$$
$$a_1H_3 \neq H_3a_1, \quad a_4H_3 \neq H_3a_4,$$
$$a_2H_3 \neq H_3a_2, \quad a_5H_3 \neq H_3a_5.$$

- $H_4 = \{a_0, a_4, a_5\}$ 的左陪集:

$$a_0H_4 = \{a_0, a_4, a_5\}, \quad a_1H_4 = \{a_1, a_2, a_3\},$$
$$a_4H_4 = \{a_4, a_5, a_0\}, \quad a_2H_4 = \{a_2, a_3, a_1\},$$
$$a_5H_4 = \{a_5, a_0, a_4\}, \quad a_3H_4 = \{a_3, a_1, a_2\}.$$

- $H_4 = \{a_0, a_4, a_5\}$ 的右陪集:

$$H_4a_0 = \{a_0, a_4, a_5\}, \quad H_4a_1 = \{a_1, a_3, a_2\},$$
$$H_4a_4 = \{a_4, a_5, a_0\}, \quad H_4a_2 = \{a_2, a_1, a_3\},$$
$$H_4a_5 = \{a_5, a_0, a_4\}, \quad H_4a_3 = \{a_3, a_2, a_1\}.$$

- 左陪集与右陪集的比较

$$a_0H_4 = H_4a_0, \quad a_1H_4 = H_4a_1,$$
$$a_4H_4 = H_4a_4, \quad a_2H_4 = H_4a_2,$$
$$a_5H_4 = H_4a_5, \quad a_3H_4 = H_4a_3.$$

- **定理1** 设H 是群G 的子群, 则

(i) 对任意$a \in G$, 有

$$aH = \{c \mid c \in G,\ c^{-1}a \in H\}$$

(对应地$Ha = \{c \mid c \in G,\ ac^{-1} \in H\}$);

证 (i) 令

$$H_{al} = \{c \mid c \in G,\ c^{-1}a \in H\}.$$

要证明: $aH = H_{al}$. 对任意的$c \in aH$, 存在$h \in H$ 使得$c = ah$. 从而, $c^{-1}a = h^{-1} \in H$, 即$c \in H_{al}$. 因此, $aH \subset H_{al}$. 反过来, $\forall c \in H_{al}$, 有$c^{-1}a \in H$, 从而存在$h \in H$ 使得$c^{-1}a = h$. 由此, $c = ah^{-1} \in aH$. 因此, $H_{al} \subset aH$. 故$aH = \{c \mid c \in G,\ c^{-1}a \in H\}$.

同理可得, $Ha = \{c \mid c \in G,\ ac^{-1} \in H\}$.

- **定理1**(续1) 设H 是群G 的子群, 则

(ii) 对任意$a,\ b \in G$, $aH = bH$ 的充要条件$b^{-1}a \in H$ (对应地$Ha = Hb$ 的充要条件$ab^{-1} \in H$);

证 (ii) 设$aH = bH$. 则$b = be \in bH = aH$. 故$b^{-1}a \in H$. 反过来, 设$b^{-1}a = h_1 \in H$. 对任意$c \in aH$, 存在$h_2 \in H$ 使得$c = ah_2$. 进而,

$$c = b(b^{-1}a)h_2 = b(h_1h_2) \in bH.$$

因此, $aH \subset bH$. 同样, 对任意$c \in bH$, 存在$h_3 \in H$ 使得$c = bh_3$. 进而,

$$c = a(b^{-1}a)^{-1}h_3 = a(h_1^{-1}h_2) \in aH.$$

因此, $bH \subset aH$. 故$aH = bH$.

同理可得, $Ha = Hb$ 的充要条件$ab^{-1} \in H$.

- **定理1**(续2) 设H 是群G 的子群, 则

  (iii) 对任意$a, b \in G$, $aH \cap bH = \emptyset$ 的充要条件是$b^{-1}a \notin H$ (对应地$Ha \cap Hb = \emptyset$ 的充要条件是$ab^{-1} \notin H$);

  (iv) 对任意$a \in H$, 有$aH = H = Ha$.

  证 (iii) 由(ii) 知必要性成立. 再证充分性. 反证法. 假设$aH \cap bH \neq \emptyset$, 则存在$c \in aH \cap bH$. 根据(i), 我们有$c^{-1}a \in H$ 及$c^{-1}b \in H$. 进而,

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

  这与假设条件矛盾.

  同理可得, $Ha \cap Hb = \emptyset$ 的充要条件$ab^{-1} \notin H$.

  (iv) 因为$e, a^{-1} \in H$, 所以结论成立.

- **推论** 设H 是群G 的子群. 则群G 可以表示为不相交的左(对应右)陪集的并集.
- **定义2** 设H 是群G 的子群. 则H 在G 中不同左(对应右)陪集组成的新集合$\{aH \mid a \in G\}$, 叫做H 在G 中的**商集**, 记作G/H. G/H 中不同左(对应右)陪集的个数叫做H 在G 中的**指标**, 记为$[G:H]$.

- **定理2** 设$H \le G$, 则$|G| = [G:H]|H|$.
  更进一步, $K,\ H \le G$, $K \le H$, 则

$$[G:K] = [G:H][H:K].$$

  如果其中两个指标是有限的, 则第三个指标也是有限的.

  证 根据定理1,

$$G = \bigcup_{i\in I} a_i H \quad 和 \quad |G| = \sum_{i\in I} |a_i H|.$$

  因为H 到a_iH 的映射: $f: h \longmapsto a_i h$ 是一一对应的, 所以$|a_iH| = |H|$. 进而, $|G| = [G:H]|H|$.

- 进一步, 根据定理1, $G=\bigcup_{i\in I}a_iH, \quad H=\bigcup_{j\in J}b_jK$, 其中$|I|=[G:H]$, $|J|=[H:K]$. 从而,

$$G=\bigcup_{i\in I}\bigcup_{j\in J}(a_ib_j)K.$$

要证明: $\{(a_ib_j)K\}$, $i\in I$, $j\in J$ 是不同的陪集.
假设$(a_ib_j)K = (a_{i'}b_{j'})K$, 右乘$H$, 得到$a_iH = a_{i'}H$. (因为$b_j$, $b_{j'}\in H$,) 根据定理1 (ii), 得到$a_i = a_{i'}$. 从而, $b_jK=b_{j'}K$. 再根据定理1 (ii), 得到$b_i=b_{i'}$.
因此,

$$|G|=\sum_{i\in I}\sum_{j\in J}|(a_ib_j)K|=[G:H][H:K]|K|.$$

但$|G|=[G:K]|K|$. 故$[G:K]=[G:H][H:K]$.

- **推论** (Lagrange). 设H 是有限群G 的子群, 则子群H 阶是$|G|$ 的因数.
- 设G 是一个群, H, K 是G 的子集. 用HK 表示集合

$$HK = \{hk \mid h \in H,\ k \in K.\}$$

- 如果写成加法, 我们用$H + K$ 表示集合

$$H + K = \{h + k \mid h \in H,\ k \in K.\}$$

- **例2** 设H, K 是交换群G 的两个子群. 则HK 是G 子群.

- **定理3** 设$H,\ K$ 是有限群G 的子群. 则

$$|HK| = |H||K|/|H\cap K|.$$

证 因为$H\cap K$ 是H 的子群, 所以$|H\cap K| \mid |H|$. 令$\frac{|H|}{|H\cap K|}=n$, H 关于$H\cap K$ 的左陪集分解式为

$$H = h_1(H\cap K)\cup\cdots\cup h_n(H\cap K), \quad h_i\in H,\ h_i^{-1}h_j\notin K.$$

由于$(H\cap K)K = K$, 得到

$$\begin{aligned} HK &= (h_1(H\cap K)\cup\cdots\cup h_n(H\cap K))\,K \\ &= h_1(H\cap K)K\cup\cdots\cup h_n(H\cap K)K \\ &= h_1K\cup\cdots\cup h_nK. \end{aligned}$$

再证 $h_iK\cap h_jK=\emptyset$. 若不然, 则有$k_i, k_j\in K$ 使得$h_ik_i = h_jk_j$,从而$h_i^{-1}h_j = k_ik_j^{-1}\in K$, 矛盾.故

$$|HK| = n|K| = |H||K|/|H\cap K|.$$

- **定理4** 设H, K 是群G 子群. 则

$$[H : H \cap K] \leq [G : K].$$

如果$[G : K]$ 是有限的, 则$[H : H \cap K] = [G : K]$ 当且仅当$G = KH$.

证 考虑H 关于$H \cap K$ 的左陪集

$$H/H \cap K = \{h_i(H \cap K) \mid h_i \in H, h_i^{-1}h_j \notin H \cap K\},$$

以及G 关于K 的左陪集,

$$G/K = \{a_iK \mid a_i \in G, a_i^{-1}a_j \notin K\}.$$

作$H/H \cap K$ 到G/K 的映射$\varphi : h(H \cap K) \longmapsto hK$. 则φ 是单射. 事实上, 若有$h_iK = h_jK$, $(h_i, h_j \in H)$. 则$h_i^{-1}h_j \in K, h_i^{-1}h_j \in H \cap K$, 矛盾. 故φ 是单射,

$$[H : H \cap K] \leq [G : K].$$

- 假设$[G:K]$ 有限. 若$[H:H\cap K]=[G:K]$, 则单射φ 也是满射. 即我们有

$$\{h_iK \mid h_i\in H, h_i^{-1}h_j\notin K\}=\{a_iK \mid a_i\in G, a_i^{-1}a_j\notin K\}$$

因此, 对任意$x\in G$, 有$a_i\in G$ 以及$h_j\in H$ 使得

$$x\in xK=a_iK=h_jK\subseteq HK,$$

从而$G\subseteq HK, G=HK.$
反之,若$G=HK$,则对任意左陪集$a_iK\ (a_i\in G)$, 有

$$a_i=h_jk,\quad (h_j\in H,\ k\in K).$$

从而

$$\varphi(h_j(H\cap K))=h_jK=h_jkK=a_iK.$$

φ 是满射, 故

$$[H:H\cap K]=[G:K].$$

- **定理5** 设H, K 是群G 的有限指标子群. 则$[G:H\cap K]$是有限的, 且$[G:H\cap K]\le[G:H][G:K]$. 进一步, $[G:H\cap K]=[G:H][G:K]$ 当且仅当$G=HK$.

证 因为$H\cap K\le H\le G$, 所以

$$[G:H\cap K]=[G:H][H:H\cap K].$$

又因为$[G:H]$与$[G:K]$都有限, 故由定理4知,

$$[H:H\cap K]\le[G:K].$$

于是$[G:H\cap K]\le[G:H][G:K]$. 因为

$[G:H\cap K]=[G:H][G:K]\Leftrightarrow[H:H\cap K]=[G:K]$,

而由定理4知$[H:H\cap K]=[G:K]\Leftrightarrow G=HK$, 故

$$[G:H\cap K]=[G:H][G:K]\Leftrightarrow G=HK.$$

定理成立.证毕.

- **定理6** 设N 是群G 的子群, 则如下条件是等价的:
(i) 对任意$a \in G$, 有$aN = Na$;
(ii) 对任意$a \in G$, 有$aNa^{-1} = N$.
(iii) 对任意$a \in G$, 有$aNa^{-1} \subset N$, 其中

$$aNa^{-1} = \{ana^{-1} | n \in N\}.$$

证 易知, (i) 蕴含(ii) 及(ii) 蕴含(iii) . 现从(iii) 推出(i). 对任意$a \in G$, $n \in N$, 因为$ana^{-1} \in aNa^{-1} \subset N$, 所以$ana^{-1} = n'$, $n' \in N$. 进而, $an = n'a \in Na$ 及$aN \subset Na$. 特别, 也有$a^{-1}N \subset Na^{-1}$ 或$Na \subset aN$. 故$aN = Na$. 定理成立. 证毕.

- **定义3** 设N 是群G 的子群. 我们称N 为群G 的**正规子群**, 如果它满足定理6的条件. 记作$N \lhd G$.

- **定理7** 设$N \lhd G$, $G/N=\{aN \mid a\in G\}$. 则对于结合法$(aN)(bN)=(ab)N$, G/H 构成一个群.

证 首先, 要证明结合法的定义不依赖于陪集的代表元的选择. 即要证明: $aN = a'N$, $bN = b'N$时, $(ab)N=(a'b')N$. 事实上, 根据定理6, 我们有

$$(ab)N=a(bN)=a(b'N)=a(Nb')=(aN)b'=(a'N)b'=(a'b')N.$$

- 其次, $eN=N$ 是单位元. 事实上, 对任意$a\in G$, 有

$$(aN)(eN)=(ae)N=aN, \quad (eN)(aN)=(ea)N=aN.$$

- 最后, aN 的逆元是$a^{-1}N$. 事实上,

$$(aN)(a^{-1}N)=(aa^{-1})N=eN, \quad (a^{-1}N)(aN)=(a^{-1}a)N=eN.$$

因此, G/H 构成一个群. 证毕.

- 定理7 中的群叫做群G 对于正规子群H 的**商群**. 如果群G 的运算写作加法, 则G/N 中的运算写作

$$(a+N)+(b+N)=(a+b)+N.$$

- **定理8** 设f 是群G 到G' 的同态, 则f 的核$\ker(f)$ 是G 的正规子群. 反过来, 设N 是群G 的正规子群, 则G 到G/N 的映射$s: a \longmapsto aN$ 是核为N 的同态.

  证 对任意$a \in G,\ b \in \ker f$, 我们有

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)e'f(a)^{-1} = e'.$$

  故$aba^{-1} \in \ker f$. 由定理6, $\ker(f)$ 是G 的正规子群.

  反过来, 设N 是群G 的正规子群, 则G 到G/N 的映射s 满足:

$$s(ab) = (ab)N = (aN)(bN) = s(a)s(b),$$

  同时, $s(a) = N$ 的充分必要条件是$a \in N$. 因此, s 是核为N 的同态. 证毕.

- 映射$s: G \longrightarrow G/N$ 称为G 到G/N 自然同态.

- **定理9** 设$f \in \mathrm{Hom}(G, G')$，则存在惟一的$G/\ker(f)$到$f(G)$的同构$\overline{f}: a\ker(f) \longmapsto f(a)$使得$f = i\circ\overline{f}\circ s$，其中$s$是$G$到$G/\ker(f)$的自然同态，$i$是$f(G)$到$G'$的恒等同态. 即有如下的交换图:

$$\begin{array}{ccc} G & \stackrel{f}{\longrightarrow} & G' \\ \mathbf{s}\downarrow & & \uparrow\mathbf{i} \\ G/\ker(f) & \stackrel{\overline{f}}{\longrightarrow} & f(G) \end{array}$$

证 因为$\ker(f) \lhd G$，所以存在商群$G/\ker(f)$.
要证明: $\overline{f}: a\ker(f) \longmapsto f(a)$是$G/\ker(f)$到像子群$f(G)$的同构.

- 首先, $\overline{f}$ 是$G/\ker(f)$ 到$f(G)$ 的同态. 事实上, 对任意的$a\ker(f),\ b\ker(f)\in G/\ker(f)$,

$$\begin{aligned}\overline{f}((a\ker(f))(b\ker(f)) &= \overline{f}((ab)\ker(f))\\ &= f(ab)\\ &= f(a)f(b)\\ &= \overline{f}(a\ker(f))\overline{f}(b\ker(f)).\end{aligned}$$

其次, $\overline{f}$ 是一对一. 事实上, 对任意$a\ker(f)\in\ker(\overline{f})$, 有$\overline{f}(a\ker(f)) = f(a) = e'$. 由此, $a\in\ker(f)$ 以及$a\ker(f)=\ker(f)$.

- 最后, $\overline{f}$ 是满同态. 事实上, 对任意$c \in f(G)$, 存在$a \in G$ 使得$f(a) = c$. 从而, $\overline{f}(a\ker(f)) = f(a) = c$. 即$a\ker(f)$ 是c 的像源.

  因此, $\overline{f}$ 是同构, 并且有$f = i \circ \overline{f} \circ s$. 事实上, 对任意$a \in G$, 有

  $$i \circ \overline{f} \circ s(a) = i(\overline{f}(s(a))) = i(\overline{f}(a\ker(f))) = i(f(a)) = f(a).$$

  假如还有同构$g : G/\ker(f) \longrightarrow f(G)$ 使得$f = i \circ g \circ s$, 则对任意$a\ker(f) \in G/\ker(f)$, 我们有

  $$g(a\ker(f)) = i(g(s(a))) = (i \circ g \circ s)(a) = f(a) = \overline{f}(a\ker(f$$

  因此, $g = \overline{f}$. 证毕.

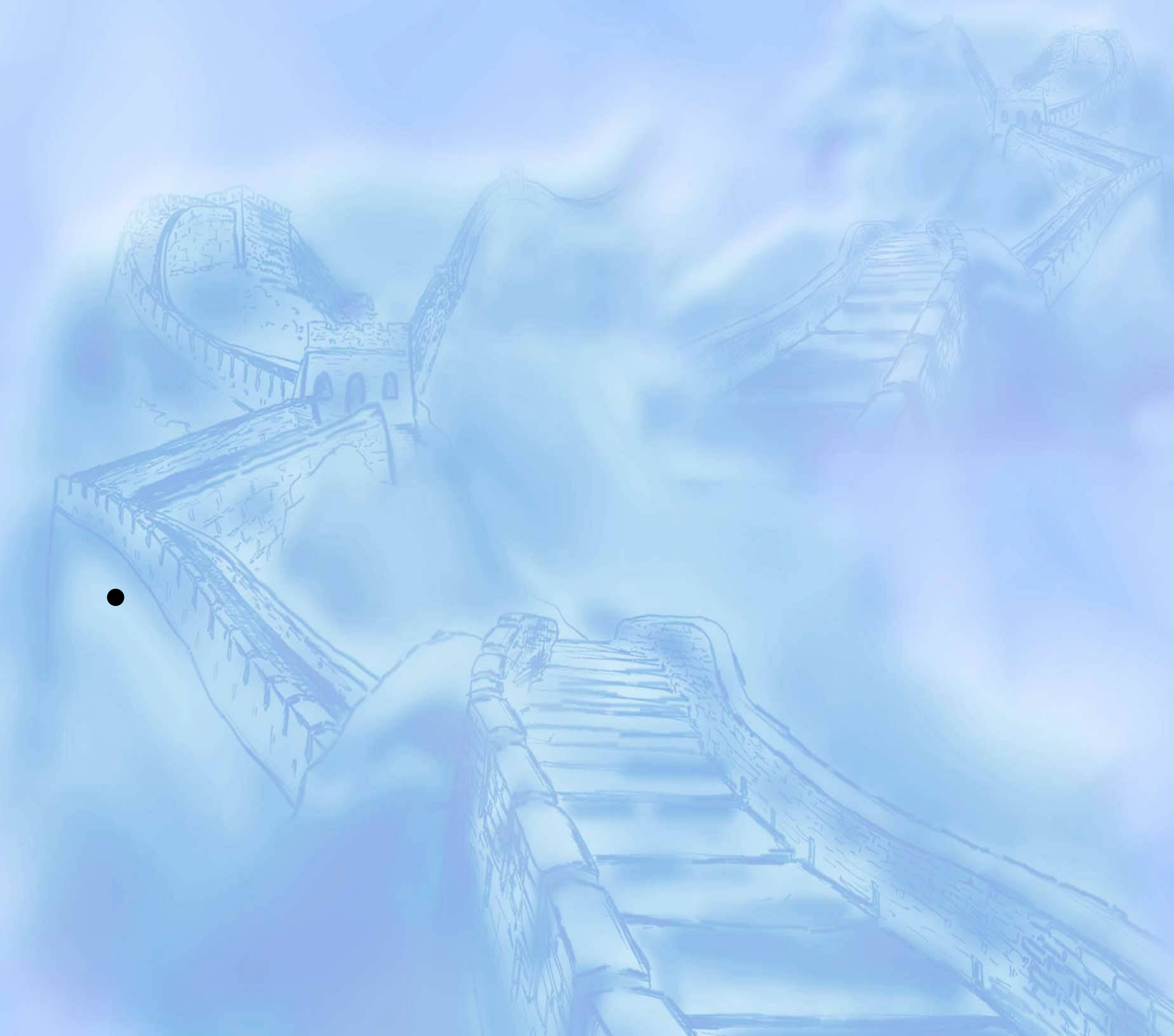
- **定理10** 设K 是群G 的正规子群, H 是G 的包含K 的子群. 则$\overline{H} = H/K$ 是商群$\overline{G} = G/K$ 的子群, 且映射$H \to \overline{H}$ 是G 的包含K 的子群集到$\overline{G}$ 的子群集的一一对应. $H(\supset K)$ 是G 的正规子群当且仅当$\overline{H}$ 是$\overline{G}$ 的正规子群. 这时,

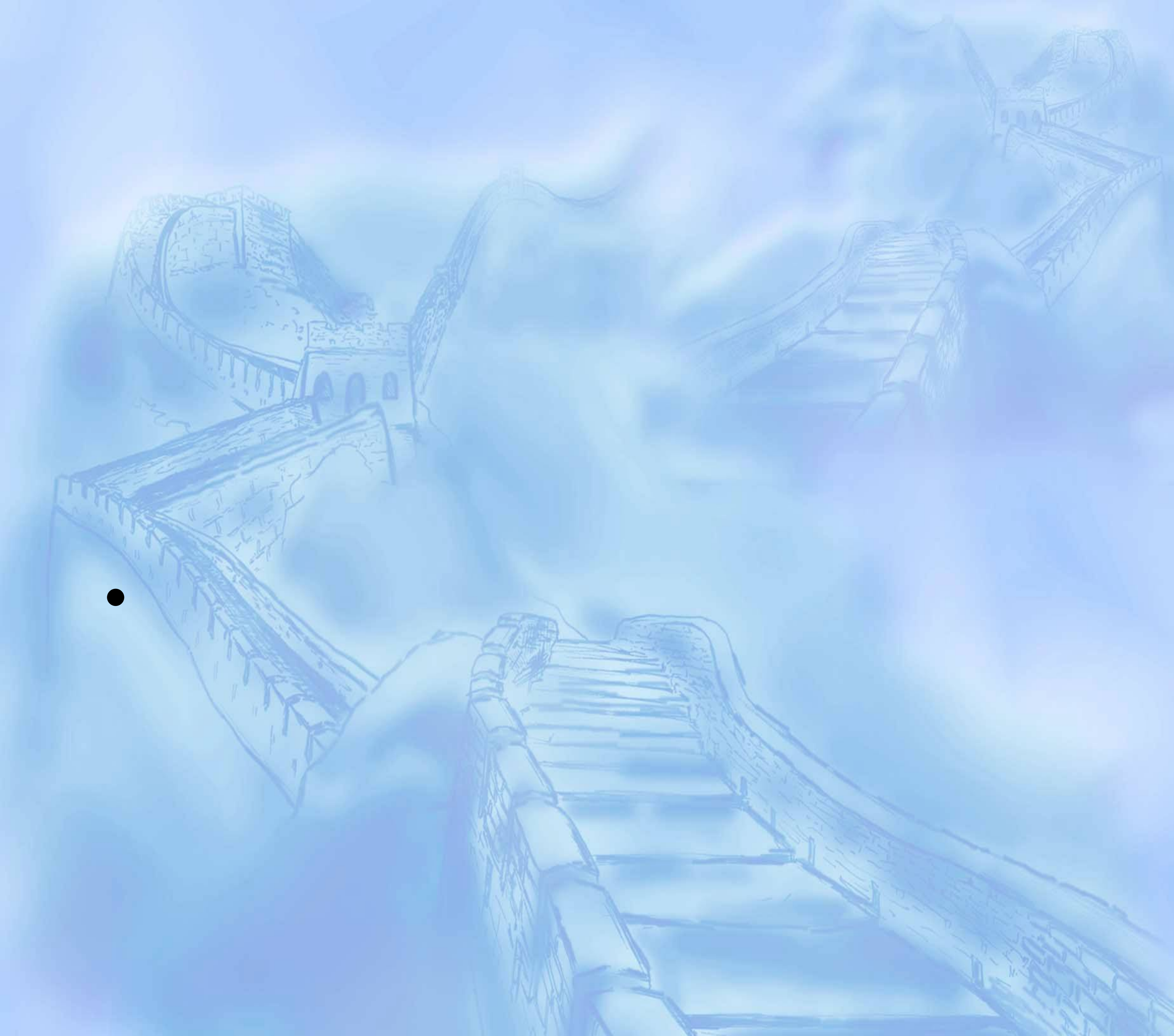
$$\frac{G}{H} \cong \frac{\overline{G}}{\overline{H}} = \frac{G/K}{H/K}.$$

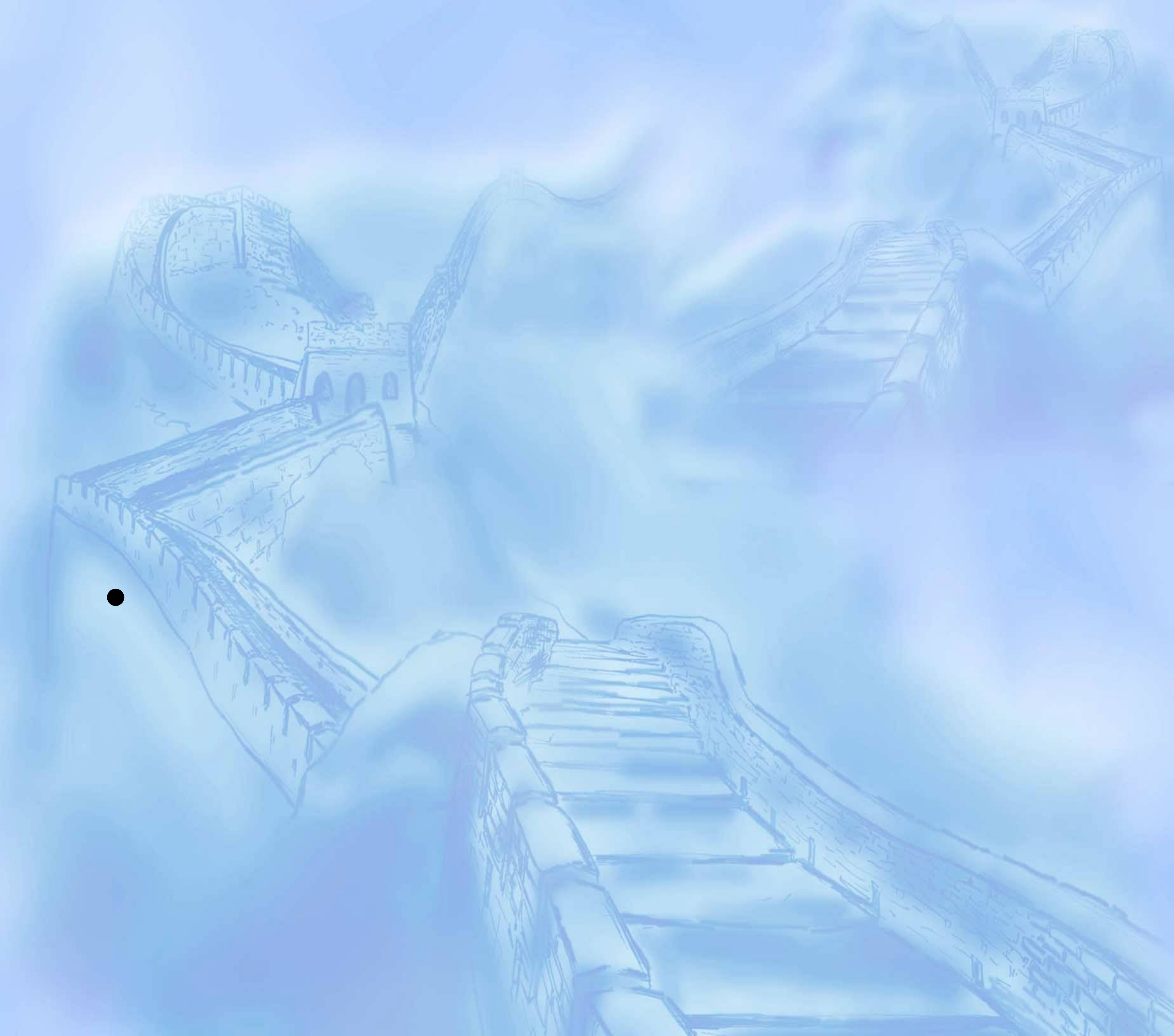
- **定理11** 设H, K 是群G 的子群, K 是G 的正规子群. 则$HK = \{hk \mid h \in H, k \in K\}$ 是G 的包含K 的子群, $H \cap K$ 是H 的正规子群, 且映射

$$hK \longrightarrow h(H \cap K), \quad h \in H$$

是HK/K 到$H/H \cap K$ 的同构.







1. 证明: 如果a, b 是群G 的任意元素, 则

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

2. 证明: 群G 是交换群的充要条件是对任意$a, b \in G$,有$(ab)^2 = a^2b^2$.

3. 证明: 群G 是交换群的充要条件是对任意$a, b \in G$,有

$$(ab)^3 = a^3b^3, \quad (ab)^4 = a^4b^4, \quad (ab)^5 = a^5b^5.$$

4. 设G 是n 阶有限群. 证明: 对任意元$a \in G$, 有$a^n = e$.

5. 证明: 群G 中元素a 与其逆元a^{-1} 有相同的阶.

6. 设G 是一个群. 记

$$\mathrm{cent}(G) = \{a \in G \mid ab = ba \ \ \forall\, b \in G\}.$$

证明: $\mathrm{cent}(G)$ 是G 的正规子群.

7. 设a 是群G 的一个元素. 证明: 映射$\sigma: \ x \longmapsto axa^{-1}$ 是G 到自身的自同构.

8. 设H 是群G 的子群. 在G 中定义关系R: aRb 如果$b^{-1}a \in H$. 证明:

(i) R 是等价关系.

(ii) aRb 的充要条件是$aH = bH$.

9. 每个循环群都是交换群.

10. 给出$\mathbf{F}_7$ 中的加法表和乘法表.

11. 证明$\mathbf{F}_{23}$ 的非零元对于乘法构成一个循环群, 并求出其生成元.

12. 证明: $\mathbf{Z}/n\mathbf{Z}$ 中的可逆元对乘法构成一个群, 记作$\mathbf{Z}/n\mathbf{Z}^*$.

13. 证明: $\mathbf{Z}/26\mathbf{Z}$ 对乘法不构成一个群.

14. 构造26 元的一个乘法群.