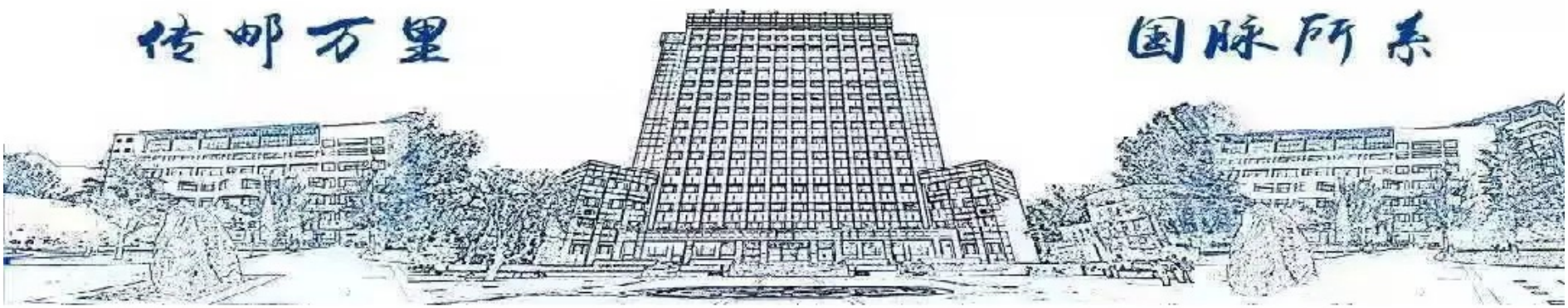
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

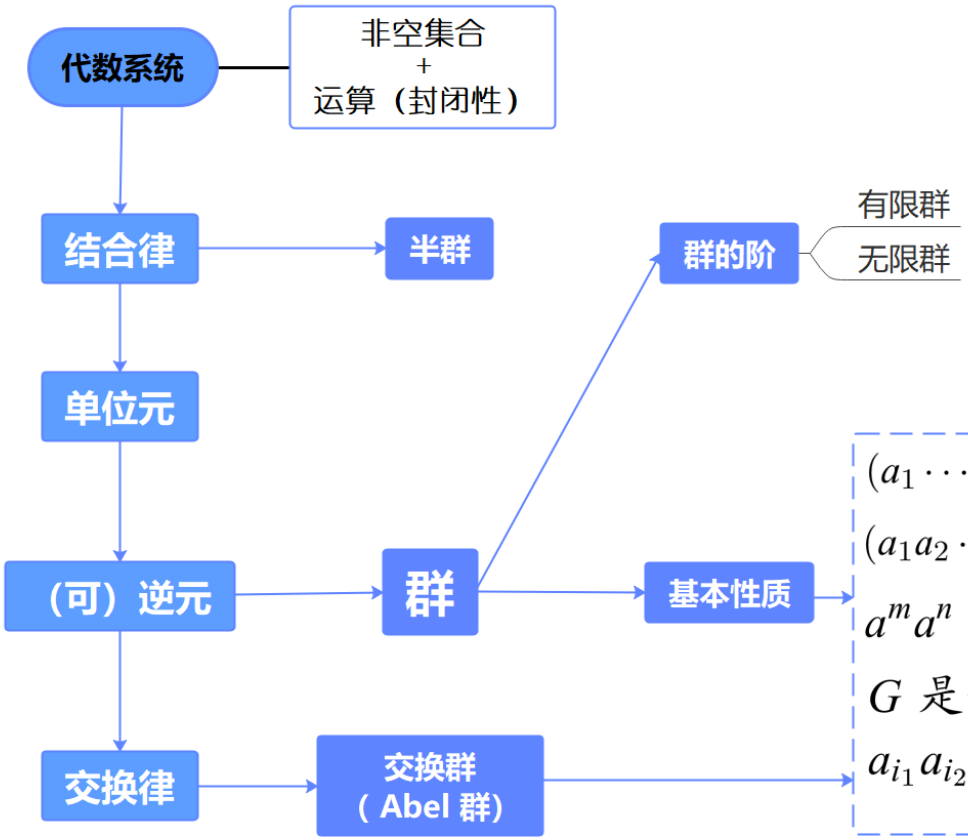
—— 群 (2)

信数课题组

北京邮电大学



上次课回顾



$$(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n.$$

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

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

G 是一个群 $\Leftrightarrow$ $ax = b, \ ya = b$ 在 G 中有解.

$$a_{i_1} a_{i_2} \cdots a_{i_n} = a_1 a_2 \cdots a_n.$$

目录

目录

定义 6.2.1

设 H 是群 G 的一个子集合. 如果对于群 G 的运算, H 成为一个群, 那么 H 就叫做群 G 的**子群**, 记作 $H \leqslant G$.

定义 6.2.1

设 H 是群 G 的一个子集合. 如果对于群 G 的运算, H 成为一个群, 那么 H 就叫做群 G 的**子群**, 记作 $H \leqslant G$.

注：$H = \{e\}$ 和 $H = G$ 都是群 G 的子群, 叫做群 G 的**平凡子群**. 如果群 G 的子群 H 不是群 G 的平凡子群, 则 H 叫做群 G 的**真子群**.

定义 6.2.1

设 H 是群 G 的一个子集合. 如果对于群 G 的运算, H 成为一个群, 那么 H 就叫做群 G 的**子群**, 记作 $H \leqslant G$.

注: $H = \{e\}$ 和 $H = G$ 都是群 G 的子群, 叫做群 G 的**平凡子群**. 如果群 G 的子群 H 不是群 G 的平凡子群, 则 H 叫做群 G 的**真子群**.

例 6.2.1 设 n 是一个正整数, 运算为普通加法 $+$, 则 $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ 是 $\mathbb{Z}$ 的子群.

定义 6.2.1

设 H 是群 G 的一个子集合. 如果对于群 G 的运算, H 成为一个群, 那么 H 就叫做群 G 的**子群**, 记作 $H \leqslant G$.

注: $H = \{e\}$ 和 $H = G$ 都是群 G 的子群, 叫做群 G 的**平凡子群**. 如果群 G 的子群 H 不是群 G 的平凡子群, 则 H 叫做群 G 的**真子群**.

例 6.2.1 设 n 是一个正整数, 运算为普通加法 $+$, 则 $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ 是 $\mathbb{Z}$ 的子群.

证: (0) $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个子集合.

定义 6.2.1

设 H 是群 G 的一个子集合. 如果对于群 G 的运算, H 成为一个群, 那么 H 就叫做群 G 的**子群**, 记作 $H \leqslant G$.

注: $H = \{e\}$ 和 $H = G$ 都是群 G 的子群, 叫做群 G 的**平凡子群**. 如果群 G 的子群 H 不是群 G 的平凡子群, 则 H 叫做群 G 的**真子群**.

例 6.2.1 设 n 是一个正整数, 运算为普通加法 $+$, 则 $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ 是 $\mathbb{Z}$ 的子群.

证: (0) $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个子集合.

(下证, 对 $\mathbb{Z}$ 的运算 "$+$" 满足 "4 条" .)

(1) 封闭性. $\forall\, nk_1, nk_2 \in n\mathbb{Z}, nk_1 + nk_2 = n(k_1 + k_2) \in n\mathbb{Z}, k_1 + k_2 \in \mathbb{Z}$.

(2) 结合律. 因为 $\mathbb{Z}$ 是群, 所以运算 "$+$" 在 $\mathbb{Z}$ 中满足结合律. $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个子集合, 所以在 $n\mathbb{Z}$ 集合中, 运算 "$+$" 仍然满足结合律.

(3) 单位元 (零元) 0. 因为 $0 \in n\mathbb{Z}$, 有 $nk + 0 = 0 + nk = nk$.

事实上, 群与子群的单位元是同一个. $\forall\ nk \in n\mathbb{Z}, nk + 0 = 0 + nk$.

则有 $n(k + 0) = n(0 + k)$.

考虑到 n 的任意性, 取 $n \neq 0$, 所以, 0 是 $\mathbb{Z}$ 中的单位元,

$$0 + k = k + 0 = k.$$

(4) 存在逆元. $\forall\ nk \in n\mathbb{Z}$,

$\because k \in \mathbb{Z}, \mathbb{Z}$ 为群,

$\therefore \exists -k \in \mathbb{Z}$, 使得 $k + (-k) = (-k) + k = 0$.

对于 $nk \in n\mathbb{Z}$,

$\exists\ n(-k) \in n\mathbb{Z}$, 使得

$$nk + n(-k) = n(-k) + nk = n[k + (-k)] = n \cdot 0 = 0.$$

综上, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ 是 $\mathbb{Z}$ 的子群.

定理 6.2.1

设 H 是群 G 的一个非空子集合, 则 H 是群 G 的子群的充要条件是对任意的 $a, b \in H$, 有 $ab^{-1} \in H$.

定理 6.2.1

设 H 是群 G 的一个非空子集合, 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. (对任意的 $a, b \in H$, 因为 H 是群, b^{-1} 存在且 $b^{-1} \in H$, 再由群的封闭性, $ab^{-1} \in H$ 成立)

下证充分性. (证明 H 是群 G 的子群, 下证满足“4 条”)

(1) 结合律. 结合律在 G 中成立, 在 H 中自然成立.

(2) 单位元. 因为 H 非空, 故 H 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.

(3) 逆元. 对于任意 $a \in H$, 由 $e \in H$, 再应用假设, 我们有 $a^{-1} = ea^{-1} \in H$, 即 H 中的每个元素 a 在 H 中有逆元.

(4) 封闭性. 对任意的 $a, b \in H$, 由 (3) 可知 $b^{-1} \in H$, 再应用假设, 有 $a(b^{-1})^{-1} \in H$, 即 $ab \in H$.

因此, H 是群 G 的子群.

例 6.2.2 证明群 G 的两个子群的交集也是 G 的子群.

证: 设 G 的两个子群 H_1 与 H_2.

要证 $H_1 \cap H_2$ 是 G 的子群, 只需证 $ab^{-1} \in H_1 \cap H_2, \forall\, a, b \in H_1 \cap H_2$.

令 $\forall\, a, b \in H_1 \cap H_2$,

$\therefore a \in H_1, b \in H_1, a \in H_2, b \in H_2$.

又因为 H_1 是子群, H_2 是子群, 有 $ab^{-1} \in H_1, ab^{-1} \in H_2$.

所以 $ab^{-1} \in H_1 \cap H_2$,

所以 $H_1 \cap H_2$ 是 G 的子群.

例 6.2.2 证明群 G 的两个子群的交集也是 G 的子群.

证: 设 G 的两个子群 H_1 与 H_2.

要证 $H_1 \cap H_2$ 是 G 的子群, 只需证 $ab^{-1} \in H_1 \cap H_2, \forall\, a, b \in H_1 \cap H_2$.

令 $\forall\, a, b \in H_1 \cap H_2$,

$\therefore a \in H_1, b \in H_1, a \in H_2, b \in H_2$.

又因为 H_1 是子群, H_2 是子群, 有 $ab^{-1} \in H_1, ab^{-1} \in H_2$.

所以 $ab^{-1} \in H_1 \cap H_2$,

所以 $H_1 \cap H_2$ 是 G 的子群.

例 6.2.3 设 G 是一个群, $\{H_i\}_{i \in I}$ 是 G 的一族子群, 则 $\bigcap\limits_{i \in I} H_i$ 是 G 的子群.

证：对任意的 $a, b \in \bigcap\limits_{i \in I} H_i$, 有 $a, b \in H_i, i \in I$.

因为 H_i 是 G 的子群, 根据定理 6.2.1, 我们有 $ab^{-1} \in H_i, i \in I$.

进而, $ab^{-1} \in \bigcap\limits_{i \in I} H_i$. 根据定理 6.2.1, $\bigcap\limits_{i \in I} H_i$ 是 G 的一个子群.

定义 6.2.2

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 $\bigcap\limits_{i\in I} H_i$ 叫做 G 的由 X **生成的子群**, 记作 $< X >$.

X 的元素称为子群 $< X >$ 的**生成元**. 如果 $X = \{a_1, \cdots, a_n\}$, 则记 $< X >$ 为 $< a_1, \cdots, a_n >$.

如果 $G =< a_1, \cdots, a_n >$, 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**.

定义 6.2.2

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 $\bigcap\limits_{i\in I} H_i$ 叫做 G 的由 X **生成的子群**, 记作 $< X >$.

X 的元素称为子群 $< X >$ 的**生成元**. 如果 $X = \{a_1, \cdots, a_n\}$, 则记 $< X >$ 为 $< a_1, \cdots, a_n >$.

如果 $G =< a_1, \cdots, a_n >$, 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**.

定义 6.2.3

若群 G 的每一个元都能表示成一个元素 g 的方幂, 则 G 称为由 g 生成的**循环群**, 记作 $G =< g >$, g 称为循环群 G 的**生成元**.

定义 6.2.2

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 $\bigcap\limits_{i\in I} H_i$ 叫做 G 的由 X **生成的子群**, 记作 $< X >$.

X 的元素称为子群 $< X >$ 的**生成元**. 如果 $X = \{a_1, \cdots, a_n\}$, 则记 $< X >$ 为 $< a_1, \cdots, a_n >$.

如果 $G =< a_1, \cdots, a_n >$, 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**.

定义 6.2.3

若群 G 的每一个元都能表示成一个元素 g 的方幂, 则 G 称为由 g 生成的**循环群**, 记作 $G =< g >$, g 称为循环群 G 的**生成元**.

注：循环群 $G=<g>$ 共有两种类型:

(1) 无限阶循环群.

(2) 由 g 所生成的 n 阶循环群.

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

$$= \{1, g, g^2, g^3, \cdots, g^{n-1}\}.$$

则 G 是 n 阶循环群. 其中, 单位元为 1, g^r 的逆元为 g^{n-r},

$g^{n-r} = g^n g^{-r} = 1g^{-r} = g^{-r}$.

注：循环群 $G=<g>$ 共有两种类型:

(1) 无限阶循环群.

(2) 由 g 所生成的 n 阶循环群.

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

$$= \{1, g, g^2, g^3, \cdots, g^{n-1}\}.$$

则 G 是 n 阶循环群. 其中, 单位元为 1, g^r 的逆元为 g^{n-r},

$g^{n-r} = g^n g^{-r} = 1g^{-r} = g^{-r}$.

例 6.2.4　设 $G=<g>=\{g^r \mid g^r \neq 1, 1 \leqslant r < n, g^n = 1\}$, G 是 n 阶循环群, 则 $<g^d>=\{g^{dk} \mid k \in \mathbb{Z}\}$ 是 G 的子群.

证: (i) 非空. $k = 0, 1 \in <g^d>$.

(ii) $\forall\ a = g^{dk_1}, b = g^{dk_2} \in <g^d>$, 则

$$ab^{-1} = g^{dk_1} g^{-dk_2} = g^{d(k_1-k_2)} \in <g^d>.$$

所以, $<g^d>=\{g^{dk} \mid k \in \mathbb{Z}\}$ 是 G 的子群.

目录

群的正规子群是一种重要的子群, 它在群论中起着很重要的作用, 从群的正规子群还可以构造出新的群, 即商群：在讨论正规子群、商群之前, 先给出陪集的概念.

定义 6.2.4

设 H 是群 G 的子群, a 是 G 中任意元, 那么集合

$$aH = \{ah \mid h \in H\} \text{ (对应地, } Ha = \{ha \mid h \in H\})$$

分别叫做 G 中 H 的**左** (对应地, **右**) **陪集**.

其中,

(1) aH (对应地, Ha) 中的元素叫做 aH (对应地, Ha) 的代表元.

(2) 若 $aH = Ha$, 则 aH 叫做 G 中 H 的**陪集**.

群的正规子群是一种重要的子群, 它在群论中起着很重要的作用, 从群的正规子群还可以构造出新的群, 即商群：在讨论正规子群、商群之前, 先给出陪集的概念.

定义 6.2.4

设 H 是群 G 的子群, a 是 G 中任意元, 那么集合

$$aH = \{ah \mid h \in H\} \text{ (对应地, } Ha = \{ha \mid h \in H\})$$

分别叫做 G 中 H 的**左** (对应地, **右**) **陪集**.

其中,

(1) aH (对应地, Ha) 中的元素叫做 aH (对应地, Ha) 的代表元.

(2) 若 $aH = Ha$, 则 aH 叫做 G 中 H 的**陪集**.

例 6.2.5 设 $n > 1$ 是整数, 则 $H = n\mathbb{Z}$ 是 $\mathbb{Z}$ 的子群, 子集

$$a + n\mathbb{Z} = \{a + k \cdot n \mid k \in \mathbb{Z}\}$$

就是 $n\mathbb{Z}$ 的陪集. 这个陪集就是模 n 的剩余类.

定理 6.2.2

设 H 是群 G 的子群, 则

(i) 对任意 $a \in G$, 有

$aH = \{c \mid c \in G, a^{-1}c \in H\}$ (对应地, $Ha = \{c \mid c \in G, ca^{-1} \in H\}$).

(ii) 对任意 $a, b \in G$, $aH = bH$ 的充要条件是 $b^{-1}a \in H$

(对应地, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$).

(iii) 对任意 $a, b \in G$, $aH \cap bH = \varnothing$ 的充要条件是 $b^{-1}a \notin H$

(对应地, $Ha \cap Hb = \varnothing$ 的充要条件是 $ab^{-1} \notin H$).

(iv) 对任意 $a \in H$, 有 $aH = H = Ha$.

定理 6.2.2

设 H 是群 G 的子群, 则

(i) 对任意 $a \in G$, 有

$aH = \{c \mid c \in G, a^{-1}c \in H\}$ (对应地, $Ha = \{c \mid c \in G, ca^{-1} \in H\}$).

(ii) 对任意 $a, b \in G$, $aH = bH$ 的充要条件是 $b^{-1}a \in H$

(对应地, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$).

(iii) 对任意 $a, b \in G$, $aH \cap bH = \varnothing$ 的充要条件是 $b^{-1}a \notin H$

(对应地, $Ha \cap Hb = \varnothing$ 的充要条件是 $ab^{-1} \notin H$).

(iv) 对任意 $a \in H$, 有 $aH = H = Ha$.

证: (i) 令 $H_{al} = \{c \mid c \in G, a^{-1}c \in H\}$. 对任意的 $c \in aH$, 存在 $h \in H$ 使得 $c = ah$. 从而, $a^{-1}c = h \in H$, 即 $c \in H_{al}$. 因此, $aH \subset H_{al}$.

定理 6.2.2

设 H 是群 G 的子群, 则

(i) 对任意 $a \in G$, 有

$aH = \{c \mid c \in G, a^{-1}c \in H\}$ (对应地, $Ha = \{c \mid c \in G, ca^{-1} \in H\}$).

(ii) 对任意 $a, b \in G$, $aH = bH$ 的充要条件是 $b^{-1}a \in H$

(对应地, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$).

(iii) 对任意 $a, b \in G$, $aH \cap bH = \varnothing$ 的充要条件是 $b^{-1}a \notin H$

(对应地, $Ha \cap Hb = \varnothing$ 的充要条件是 $ab^{-1} \notin H$).

(iv) 对任意 $a \in H$, 有 $aH = H = Ha$.

证: (i) 令 $H_{al} = \{c \mid c \in G, a^{-1}c \in H\}$. 对任意的 $c \in aH$, 存在 $h \in H$ 使得 $c = ah$. 从而, $a^{-1}c = h \in H$, 即 $c \in H_{al}$. 因此, $aH \subset H_{al}$.

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

定理 6.2.2

设 H 是群 G 的子群, 则

(i) 对任意 $a \in G$, 有

$aH = \{c \mid c \in G, a^{-1}c \in H\}$ (对应地, $Ha = \{c \mid c \in G, ca^{-1} \in H\}$).

(ii) 对任意 $a, b \in G$, $aH = bH$ 的充要条件是 $b^{-1}a \in H$

(对应地, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$).

(iii) 对任意 $a, b \in G$, $aH \cap bH = \varnothing$ 的充要条件是 $b^{-1}a \notin H$

(对应地, $Ha \cap Hb = \varnothing$ 的充要条件是 $ab^{-1} \notin H$).

(iv) 对任意 $a \in H$, 有 $aH = H = Ha$.

证: (i) 令 $H_{al} = \{c \mid c \in G, a^{-1}c \in H\}$. 对任意的 $c \in aH$, 存在 $h \in H$ 使得 $c = ah$. 从而, $a^{-1}c = h \in H$, 即 $c \in H_{al}$. 因此, $aH \subset H_{al}$.

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

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

定理 6.2.2

设 H 是群 G 的子群, 则

(i) 对任意 $a \in G$, 有

$aH = \{c \mid c \in G, a^{-1}c \in H\}$ (对应地, $Ha = \{c \mid c \in G, ca^{-1} \in H\}$).

(ii) 对任意 $a, b \in G$, $aH = bH$ 的充要条件是 $b^{-1}a \in H$

(对应地, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$).

(iii) 对任意 $a, b \in G$, $aH \cap bH = \varnothing$ 的充要条件是 $b^{-1}a \notin H$

(对应地, $Ha \cap Hb = \varnothing$ 的充要条件是 $ab^{-1} \notin H$).

(iv) 对任意 $a \in H$, 有 $aH = H = Ha$.

证: (i) 令 $H_{al} = \{c \mid c \in G, a^{-1}c \in H\}$. 对任意的 $c \in aH$, 存在 $h \in H$ 使得 $c = ah$. 从而, $a^{-1}c = h \in H$, 即 $c \in H_{al}$. 因此, $aH \subset H_{al}$.

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

故 $aH = \{c \mid c \in G, a^{-1}c \in H\}$. 同理得, $Ha = \{c \mid c \in G, ca^{-1} \in H\}$.

(ii) 设 $aH = bH$, 则 $a = ae \in aH = bH$, 故 $b^{-1}a \in H$.

(ii) 设 $aH = bH$, 则 $a = ae \in aH = bH$, 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,

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

因此, $bH \subset aH$.

故 $aH = bH$.

(ii) 设 $aH = bH$, 则 $a = ae \in aH = bH$, 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,

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

因此, $bH \subset aH$.

故 $aH = bH$. 同理可得, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$.

(ii) 设 $aH = bH$, 则 $a = ae \in aH = bH$, 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,

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

因此, $bH \subset aH$.

故 $aH = bH$. 同理可得, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$.

(iii) 由 (ii) 知必要性成立. 再证充分性.

若不然, $aH \cap bH \neq \varnothing$, 则存在 $c \in aH \cap bH$. 根据 (i), 有 $ac^{-1} \in H$ 及 $b^{-1}c \in H$. 进而, $b^{-1}a = (b^{-1}c)(a^{-1}c)^{-1} \in H$. 这与假设条件矛盾.

(ii) 设 $aH = bH$, 则 $a = ae \in aH = bH$, 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,

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

因此, $bH \subset aH$.

故 $aH = bH$. 同理可得, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$.

(iii) 由 (ii) 知必要性成立. 再证充分性.

若不然, $aH \cap bH \neq \varnothing$, 则存在 $c \in aH \cap bH$. 根据 (i), 有 $ac^{-1} \in H$ 及 $b^{-1}c \in H$. 进而, $b^{-1}a = (b^{-1}c)(a^{-1}c)^{-1} \in H$. 这与假设条件矛盾.

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

(ii) 设 $aH = bH$, 则 $a = ae \in aH = bH$, 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,

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

因此, $bH \subset aH$.

故 $aH = bH$. 同理可得, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$.

(iii) 由 (ii) 知必要性成立. 再证充分性.

若不然, $aH \cap bH \neq \varnothing$, 则存在 $c \in aH \cap bH$. 根据 (i), 有 $ac^{-1} \in H$ 及 $b^{-1}c \in H$. 进而, $b^{-1}a = (b^{-1}c)(a^{-1}c)^{-1} \in H$. 这与假设条件矛盾.

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

(iv) 因为 $e, a^{-1} \in H$, 所以由 (ii) 可以得到结论成立.

根据定理 6.2.2 可以进一步得到：

定理 6.2.3

设 H 是群 G 的子群, 则群 G 可以表示为不相交的左 (对应地, 右) 陪集的并集. $G = \bigcup_{i \in I} a_i H$. (对应地, $G = \bigcup_{i \in I} H a_i$.)

例 6.2.6 令 $n=3$, 则 $H=3\mathbb{Z}=\{\cdots,-6,-3,0,3,6,9,\cdots\}$, 已经证明, H 是 $\mathbb{Z}$ 的子群. $\forall\, a\in\mathbb{Z}$,

(1) 若 $a=0$, 则 $0+H=\{\cdots,-3,0,3,6,9,12,\cdots\}=H$.

若 $a=3$, 则 $3+H=\{\cdots,-3,0,3,6,9,12,\cdots\}=H$.

也就是说, 若 $a\in H$, 则 $aH=H$.

(2) 若 $a=1$, 则 $1+H=\{\cdots,-2,1,4,7,10,13,\cdots\}$.

即此集合是模 3 余 1 的集合, 记作 $[1]$（模 3 余 1 剩余类）.

当然, H 记作 $[0]$.

(3) 若 $a=2$, 则得到 $[2]=2+H$.

因此, $\mathbb{Z}$ 被分为 3 个互不相交的集合 $[0]$, $[1]$, $[2]$, 即剩余类集合 $\{[0],[1],[2]\}$. 或者说, $\mathbb{Z}$ 被子群 H 分为了 3 个互不相交的左陪集的集合 H, $1+H$, $2+H$. 同时, $\mathbb{Z}$ 也可以被子群 H 分为了 3 个互不相交的右陪集的集合 $H, H+1, H+2$.

另外, 左陪集 $=$ 右陪集, $H=H, 1+H=H+1, 2+H=H+2$.

定义 6.2.5

设 H 是群 G 的子群, 则 H 在 G 中不同左 (对应地, 右) 陪集组成的新集合 $\{aH \mid a \in G\}$ (对应地, $\{Ha \mid a \in G\}$) 叫做 H 在 G 中的**商集**, 记作 G/H.

G/H 中不同左 (对应地, 右) 陪集的个数叫做 H 在 G 中的 **指数**, 记作 $[G : H]$.

定义 6.2.5

设 H 是群 G 的子群, 则 H 在 G 中不同左 (对应地, 右) 陪集组成的新集合 $\{aH \mid a \in G\}$ (对应地, $\{Ha \mid a \in G\}$) 叫做 H 在 G 中的**商集**, 记作 G/H.

G/H 中不同左 (对应地, 右) 陪集的个数叫做 H 在 G 中的 **指数**, 记作 $[G : H]$.

定理 6.2.4

(i) 设 H 是群 G 的子群, 则

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

(ii) 更进一步地, 如果 K, H 是群 G 的子群, 且 K 是 H 的子群, 则

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

如果其中两个指数是有限的, 则第三个指数也是有限的.

证：(i) 根据定理 6.2.2, 我们有 $G = \bigcup_{i \in I} a_i H$ 和 $|G| = \sum_{i \in I} |a_i H|$.

对 H 到 $a_i H$ 的映射 $f : h \to a_i h$ 是一一对应的双射,

所以有 $|a_i H| = |H|$.

进而, $|G| = \sum_{i \in I} |a_i H| = \sum_{i \in I} |H| = [G : H]|H|$.

证：(i) 根据定理 6.2.2, 我们有 $G = \bigcup_{i\in I} a_iH$ 和 $|G| = \sum_{i\in I} |a_iH|$.

对 H 到 a_iH 的映射 $f: h \to a_ih$ 是一一对应的双射,

所以有 $|a_iH| = |H|$.

进而, $|G| = \sum_{i\in I} |a_iH| = \sum_{i\in I} |H| = [G:H]|H|$.

(ii) 若 K, H 是群 G 的子群, 且 K 是 H 的子群,

根据定理 6.2.2, 我们有 $G = \bigcup_{i\in I} a_iH$ 和 $H = \bigcup_{j\in J} b_jK$,

其中 $|I| = [G:H], |J| = [H:K]$.

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

证：(i) 根据定理 6.2.2, 我们有 $G = \bigcup_{i\in I} a_iH$ 和 $|G| = \sum_{i\in I} |a_iH|$.

对 H 到 a_iH 的映射 $f: h \to a_ih$ 是一一对应的双射,

所以有 $|a_iH| = |H|$.

进而, $|G| = \sum_{i\in I} |a_iH| = \sum_{i\in I} |H| = [G:H]|H|$.

(ii) 若 K, H 是群 G 的子群, 且 K 是 H 的子群,

根据定理 6.2.2, 我们有 $G = \bigcup_{i\in I} a_iH$ 和 $H = \bigcup_{j\in J} b_jK$,

其中 $|I| = [G:H], |J| = [H:K]$.

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

下证 $\{(a_ib_j)K\}, i \in I, j \in J$ 是不同的陪集.

假设

$$(a_ib_j)K = (a_{i'}b_{j'})K.$$

由于 K 是群 G 的子群, 根据定理 6.2.2 (ii), 得到

$(a_{i'}b_{j'})^{-1}(a_ib_j) \in K \subset H$, 即 $b_{j'}^{-1}a_{i'}^{-1}a_ib_j \in K \subset H$.

而 $b_j, b_{j'} \in H$, 故 $a_{i'}^{-1}a_i \in H$, 即 $a_iH = a_{i'}H$.

进而, $b_jK = a_i^{-1}a_ib_jK = a_i^{-1}a_{i'}(b_{j'}K) \subset b_{j'}K$.

同理, $b_{j'}K \subset b_jK$. 从而 $b_jK = b_{j'}K$.

$(a_{i'}b_{j'})^{-1}(a_ib_j) \in K \subset H$, 即 $b_{j'}^{-1}a_{i'}^{-1}a_ib_j \in K \subset H$.

而 $b_j, b_{j'} \in H$, 故 $a_{i'}^{-1}a_i \in H$, 即 $a_iH = a_{i'}H$.

进而, $b_jK = a_i^{-1}a_ib_jK = a_i^{-1}a_{i'}(b_{j'}K) \subset b_{j'}K$.

同理, $b_{j'}K \subset b_jK$. 从而 $b_jK = b_{j'}K$.

因此, 有

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

而 $|G| = [G:K]|K|$,

故 $[G:K] = [G:H][H:K]$.

$(a_{i'}b_{j'})^{-1}(a_ib_j) \in K \subset H$, 即 $b_{j'}^{-1}a_{i'}^{-1}a_ib_j \in K \subset H$.

而 $b_j, b_{j'} \in H$, 故 $a_{i'}^{-1}a_i \in H$, 即 $a_iH = a_{i'}H$.

进而, $b_jK = a_i^{-1}a_ib_jK = a_i^{-1}a_{i'}(b_{j'}K) \subset b_{j'}K$.

同理, $b_{j'}K \subset b_jK$. 从而 $b_jK = b_{j'}K$.

因此, 有

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

而 $|G| = [G:K]|K|$,

故 $[G:K] = [G:H][H:K]$.

推论 6.2.1 (Lagrange)

设 H 是有限群 G 的子群, 则子群 H 的阶是 $|G|$ 的因数.

下面考虑群 G 的两个子群组成的集合.

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, 用 $H + K$ 表示集合

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

下面考虑群 G 的两个子群组成的集合.

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, 用 $H + K$ 表示集合

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

例 6.2.7 设 H, K 是交换群 G 的两个子群, 则 HK 是 G 的子群.

下面考虑群 G 的两个子群组成的集合.

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, 用 $H + K$ 表示集合

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

例 6.2.7　设 H, K 是交换群 G 的两个子群, 则 HK 是 G 的子群.

证：(i) HK 是群 G 的非空子集, $e \in HK$.

(ii) $\forall\ a = h_1k_1, b = h_2k_2 \in HK$, 其中 $h_1, h_2 \in H, k_1, k_2 \in K$.

$ab^{-1} = h_1k_1 \cdot k_2^{-1}h_2^{-1}$.

因为 G 是交换群, 所以 $ab^{-1} = h_1h_2^{-1} \cdot k_1k_2^{-1}$.

又因为 H 是 G 的子群, 所以 $h_1h_2^{-1} = h \in H$.

而 K 也是 G 的子群, 所以 $k_1k_2^{-1} = k \in K$.

则 $ab^{-1} = hk \in HK$. 因此, HK 是 G 的子群.

定理 6.2.5

设 H, K 是有限群 G 的子群, 则 $|HK| = \frac{|H||K|}{|H \cap K|}$.

定理 6.2.5

设 H, K 是有限群 G 的子群, 则 $|HK| = \frac{|H||K|}{|H\cap K|}$.

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

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

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 $h_iK\cap h_jK = \varnothing$.

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

所以, $|HK| = n|K| = \frac{|H||K|}{|H\cap K|}$.

定理 6.2.6

设 H, K 是群 G 的子群, 则 $[H : H \cap K] \leqslant [G : K]$. 如果 $[G : K]$ 是有限的, 则 $[H : H \cap K] = [G : K]$ 当且仅当 $G = HK$.

定理 6.2.6

设 H, K 是群 G 的子群, 则 $[H : H \cap K] \leqslant [G : K]$. 如果 $[G : K]$ 是有限的, 则 $[H : H \cap K] = [G : K]$ 当且仅当 $G = HK$.

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

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

作 $H/H \cap K$ 到 G/K 的映射 $\varphi : h(H \cap K) \to hK$, 则 φ 是单射.

定理 6.2.6

设 H, K 是群 G 的子群, 则 $[H : H \cap K] \leqslant [G : K]$. 如果 $[G : K]$ 是有限的, 则 $[H : H \cap K] = [G : K]$ 当且仅当 $G = HK$.

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 $\varphi : h(H \cap K) \to hK$, 则 φ 是单射.

(事实上, 若有 $h_iK = h_jK$, 则有 $h_i^{-1}h_j \in K$. 进而, $h_i^{-1}h_j \in H \cap K$, 矛盾.)

定理 6.2.6

设 H, K 是群 G 的子群, 则 $[H : H \cap K] \leqslant [G : K]$. 如果 $[G : K]$ 是有限的, 则 $[H : H \cap K] = [G : K]$ 当且仅当 $G = HK$.

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 $\varphi : h(H \cap K) \to hK$, 则 φ 是单射.

(事实上, 若有 $h_iK = h_jK$, 则有 $h_i^{-1}h_j \in K$. 进而, $h_i^{-1}h_j \in H \cap K$, 矛盾.)

从而, $[H : H \cap K] \leqslant [G : K]$.

定理 6.2.6

设 H, K 是群 G 的子群, 则 $[H : H \cap K] \leqslant [G : K]$. 如果 $[G : K]$ 是有限的, 则 $[H : H \cap K] = [G : K]$ 当且仅当 $G = HK$.

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 $\varphi : h(H \cap K) \to hK$, 则 φ 是单射.

(事实上, 若有 $h_iK = h_jK$, 则有 $h_i^{-1}h_j \in K$. 进而, $h_i^{-1}h_j \in H \cap K$, 矛盾.)

从而, $[H : H \cap K] \leqslant [G : K]$.

假设 $[G : K]$ 有限. 若 $[H : H \cap K] = [G : K]$, 则单射 φ 也是满射, 即有 $\{h_iK \mid h_i \in H, h_i^{-1}h_j \notin K\} = \{a_iK \mid a_i \in G, a_i^{-1}a_j \notin K\}$. 因此, 对任意的 $x \in G$, 有 $a_i \in G$ 以及 $h_j \in H$ 使得 $x \in xK = a_iK = h_jK \subseteq HK$, 从而 $G \subseteq HK$, 故 $G = HK$.

反之, 若 $G = HK$, 则对任意左陪集 $a_iK(a_i \in G)$, 有 $a_i = h_jk \ \ (h_j \in H, k \in K)$. 从而 $\varphi(h_j(H \cap K)) = h_jK = h_jkK = a_iK$. φ 是满射, 故 $[H : H \cap K] = [G : K]$.

反之, 若 $G = HK$, 则对任意左陪集 $a_iK(a_i \in G)$, 有 $a_i = h_jk \ \ (h_j \in H, k \in K)$. 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 6.2.7

设 H, K 是群 G 的有限子群, 则 $[G : H \cap K]$ 是有限的, 且

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

进一步, $[G : H \cap K] = [G : H][G : K]$ 当且仅当 $G = HK$.

反之, 若 $G = HK$, 则对任意左陪集 $a_iK(a_i \in G)$, 有 $a_i = h_jk \ \ (h_j \in H, k \in K)$. 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 6.2.7

设 H, K 是群 G 的有限子群, 则 $[G : H \cap K]$ 是有限的, 且

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

进一步, $[G : H \cap K] = [G : H][G : K]$ 当且仅当 $G = HK$.

证：因为 $H \cap K \leqslant H \leqslant G$, 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 6.2.6 知, $[H : H \cap K] \leqslant [G : K]$. 于是 $[G : H \cap K] \leqslant [G : H][G : K]$.

反之, 若 $G = HK$, 则对任意左陪集 $a_iK(a_i \in G)$, 有 $a_i = h_jk \ \ (h_j \in H, k \in K)$. 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 6.2.7

设 H, K 是群 G 的有限子群, 则 $[G : H \cap K]$ 是有限的, 且

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

进一步, $[G : H \cap K] = [G : H][G : K]$ 当且仅当 $G = HK$.

证：因为 $H \cap K \leqslant H \leqslant G$, 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 6.2.6 知, $[H : H \cap K] \leqslant [G : K]$. 于是 $[G : H \cap K] \leqslant [G : H][G : K]$.

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

而由定理 6.2.6 知, $[H : H \cap K] = [G : K] \Leftrightarrow G = HK$,

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

定理 6.2.8

设 N 是群 G 的子群, 则如下条件是等价的:

(i) 对任意的 $a \in G$, 有 $aN = Na$.

(ii) 对任意的 $a \in G$, 有 $aNa^{-1} = N$.

(iii) 对任意的 $a \in G$, 有 $aNa^{-1} \subset N$, 其中 $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

定理 6.2.8

设 N 是群 G 的子群, 则如下条件是等价的:

(i) 对任意的 $a \in G$, 有 $aN = Na$.

(ii) 对任意的 $a \in G$, 有 $aNa^{-1} = N$.

(iii) 对任意的 $a \in G$, 有 $aNa^{-1} \subset N$, 其中 $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

证: 易知, (i) 蕴含 (ii) 及 (ii) 蕴含 (iii) 是显然的.

定理 6.2.8

设 N 是群 G 的子群, 则如下条件是等价的:

(i) 对任意的 $a \in G$, 有 $aN = Na$.

(ii) 对任意的 $a \in G$, 有 $aNa^{-1} = N$.

(iii) 对任意的 $a \in G$, 有 $aNa^{-1} \subset N$, 其中 $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

证: 易知, (i) 蕴含 (ii) 及 (ii) 蕴含 (iii) 是显然的. 现在从 (iii) 推出 (i). 对任意的 $a \in G, n \in N$, 因 $ana^{-1} \in aNa^{-1} \subset N$, 故 $ana^{-1} = n', n' \in N$. 进而, $an = n'a \in Na$ 及 $aN \subset Na$. 特别地, 也有 $a^{-1}N \subset Na^{-1}$. 从而可得, $Na \subset aN$. 故 $aN = Na$.

定理 6.2.8

设 N 是群 G 的子群, 则如下条件是等价的:

(i) 对任意的 $a \in G$, 有 $aN = Na$.

(ii) 对任意的 $a \in G$, 有 $aNa^{-1} = N$.

(iii) 对任意的 $a \in G$, 有 $aNa^{-1} \subset N$, 其中 $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

证: 易知, (i) 蕴含 (ii) 及 (ii) 蕴含 (iii) 是显然的. 现在从 (iii) 推出 (i). 对任意的 $a \in G, n \in N$, 因 $ana^{-1} \in aNa^{-1} \subset N$, 故 $ana^{-1} = n', n' \in N$. 进而, $an = n'a \in Na$ 及 $aN \subset Na$. 特别地, 也有 $a^{-1}N \subset Na^{-1}$. 从而可得, $Na \subset aN$. 故 $aN = Na$.

定义 6.2.6

设 N 是群 G 的子群, 如果 N 满足定理 6.2.8 的任一条件, 则称 N 为群 G 的**正规子群**, 记为 $N \lhd G$.

定理 6.2.8

设 N 是群 G 的子群, 则如下条件是等价的:

(i) 对任意的 $a \in G$, 有 $aN = Na$.

(ii) 对任意的 $a \in G$, 有 $aNa^{-1} = N$.

(iii) 对任意的 $a \in G$, 有 $aNa^{-1} \subset N$, 其中 $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

证: 易知, (i) 蕴含 (ii) 及 (ii) 蕴含 (iii) 是显然的. 现在从 (iii) 推出 (i). 对任意的 $a \in G, n \in N$, 因 $ana^{-1} \in aNa^{-1} \subset N$, 故 $ana^{-1} = n', n' \in N$. 进而, $an = n'a \in Na$ 及 $aN \subset Na$. 特别地, 也有 $a^{-1}N \subset Na^{-1}$. 从而可得, $Na \subset aN$. 故 $aN = Na$.

定义 6.2.6

设 N 是群 G 的子群, 如果 N 满足定理 6.2.8 的任一条件, 则称 N 为群 G 的**正规子群**, 记为 $N \lhd G$.

注: 若群 G 没有非平凡的正规子群, 则称 G 为**单群**.

例 6.2.8 可以证明 $(n\mathbb{Z}, +)$ 是 $(\mathbb{Z}, +)$ 的正规子群 $a(n\mathbb{Z})a^{-1} \subset n\mathbb{Z}$ (因为满足交换律).

例 6.2.8　可以证明 $(n\mathbb{Z},+)$ 是 $(\mathbb{Z},+)$ 的正规子群 $a(n\mathbb{Z})a^{-1}\subset n\mathbb{Z}$ (因为满足交换律).

例 6.2.9　两个正规子群的交集是正规子群.

证：设群 G 的两个正规子群 H_1 与 H_2, 可知, $H_1\cap H_2$ 是 G 的子群.

设 $\forall\, h\in H_1\cap H_2, \forall\, g\in G$, 有 $h\in H_1, h\in H_2$.

$\because H_1$ 是正规子群, $\therefore g^{-1}hg\in H_1$.

$\because H_2$ 是正规子群, $\therefore g^{-1}hg\in H_2$.

$\therefore g^{-1}hg\in H_1\cap H_2$.

$\therefore H_1\cap H_2$ 是正规子群.

定理 6.2.9

设 N 是群 G 的正规子群, G/N 是由 N 中的所有 (左) 陪集组成的集合, 则对于运算 $(aN) \otimes (bN) = (abN)$, G/N 构成一个群.

定理 6.2.9

设 N 是群 G 的正规子群, G/N 是由 N 中的所有 (左) 陪集组成的集合, 则对于运算 $(aN)\otimes(bN)=(abN)$, G/N 构成一个群.

证：首先, 要证明运算 $\otimes$ 的定义不依赖于陪集的代表元选择, 即要证明：

$aN=a'N, bN=b'N$ 时, $(ab)N=(a'b')N$.

事实上,

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

定理 6.2.9

设 N 是群 G 的正规子群, G/N 是由 N 中的所有 (左) 陪集组成的集合, 则对于运算 $(aN)\otimes(bN)=(abN)$, G/N 构成一个群.

证: 首先, 要证明运算 $\otimes$ 的定义不依赖于陪集的代表元选择, 即要证明:

$aN=a'N, bN=b'N$ 时, $(ab)N=(a'b')N$.

事实上,

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

其次, 运用群的定义, 证明是一个群.

(0) 满足封闭性. $\forall\, aN, bN\in G/N, (aN)\otimes(bN)=(ab)N\in G/N$.

(1) 满足结合律.

$$\forall\, aN, bN, cN\in G/N, [(aN)\otimes(bN)]\otimes(cN)=(abc)N=(aN)\otimes[(bN)\otimes(cN)].$$

(2) $eN = N$ 是单位元.

事实上, 对任意 $a \in G$, 有

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

(2) $eN = N$ 是单位元.

事实上, 对任意 $a \in G$, 有

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

(3) aN 的逆元是 $a^{-1}N$.

事实上,

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

(2) $eN = N$ 是单位元.

事实上, 对任意 $a \in G$, 有

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

(3) aN 的逆元是 $a^{-1}N$.

事实上,

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

综上, G/N 对于运算 $\otimes$ 构成一个群.

(2) $eN = N$ 是单位元.

事实上, 对任意 $a \in G$, 有

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

(3) aN 的逆元是 $a^{-1}N$.

事实上,

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

综上, G/N 对于运算 $\otimes$ 构成一个群.

注：定理 6.2.9 中的群 G/N 叫做群 G 对于正规子群 N 的**商群**.

(2) $eN = N$ 是单位元.

事实上, 对任意 $a \in G$, 有

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

(3) aN 的逆元是 $a^{-1}N$.

事实上,

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

综上, G/N 对于运算 $\otimes$ 构成一个群.

注：定理 6.2.9 中的群 G/N 叫做群 G 对于正规子群 N 的**商群**.

注：如果群 G 的运算写作加法 $+$, 则 G/N 中的运算可写作 $\oplus$:

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

(2) $eN = N$ 是单位元.

事实上, 对任意 $a \in G$, 有

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

(3) aN 的逆元是 $a^{-1}N$.

事实上,

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

综上, G/N 对于运算 $\otimes$ 构成一个群.

注：定理 6.2.9 中的群 G/N 叫做群 G 对于正规子群 N 的**商群**.

注：如果群 G 的运算写作加法 $+$, 则 G/N 中的运算可写作 $\oplus$:

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

例 6.2.10　可以证明 $G/N = \{H, aH, bH, \cdots\}$ 构成商群, 其中 $G = \mathbb{Z}, H = n\mathbb{Z}$. 例如, $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$ 构成商群, 因为 $3\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个正规子群.

定义 6.3.1

设 $(G,\cdot)$ 和 $(G',*)$ 是两个代数系统. 如果存在 G 到 G' 的映射 f, 并且保持运算, 即

$$f(a\cdot b)=f(a)*f(b),\quad \forall\, a,b\in G,$$

则称 f 是 $(G,\cdot)$ 到 $(G',*)$ 的 **同态** (同态映射).

定义 6.3.1

设 $(G,\cdot)$ 和 $(G',*)$ 是两个代数系统. 如果存在 G 到 G' 的映射 f, 并且保持运算, 即

$$f(a\cdot b)=f(a)*f(b),\quad \forall\, a,b\in G,$$

则称 f 是 $(G,\cdot)$ 到 $(G',*)$ 的 **同态** (同态映射).

例 6.3.1 例如整数集合上加法 $(\mathbb{Z},+)$ 和正实数集合上乘法 $(\mathbb{R}^+,\cdot)$.

令映射 $f:\mathbb{Z}\to\mathbb{R}^+, x\mapsto e^x$ (即 $f(x)=e^x$).

由于

1) f 是映射 (每一个元素都有唯一的像存在).

2) 保持运算: $\forall\, x,y\in\mathbb{Z}, f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)\cdot f(y)$.

所以, f 是 $(\mathbb{Z},+)$ 到 $(\mathbb{R}^+,\cdot)$ 的同态映射.

定义 6.3.2

(1) 如果 G 到 G' 的同态映射 f 是单射, 则称 f 为 G 到 G' 的**单同态**.

(2) 如果 G 到 G' 的同态映射 f 是满射, 则称 f 为 G 到 G' 的**满同态**.

此时, 称 G 与 G' 是同态的.

(3) 如果 G 到 G' 的同态映射 f 是双射 (一一对应的), 则称 f 为 G 到 G' 的**同构**映射.

此时, 称 G 与 G' 是同构的, 记作 $G \cong G'$.

(4) 如果 $G = G'$, f 是 G 到 G' 的同 (态) 构映射, 则称 f 为**自同态 (构)** 映射.

定义 6.3.2

(1) 如果 G 到 G' 的同态映射 f 是单射, 则称 f 为 G 到 G' 的**单同态**.

(2) 如果 G 到 G' 的同态映射 f 是满射, 则称 f 为 G 到 G' 的**满同态**.

此时, 称 G 与 G' 是同态的.

(3) 如果 G 到 G' 的同态映射 f 是双射 (一一对应的), 则称 f 为 G 到 G' 的**同构**映射.

此时, 称 G 与 G' 是同构的, 记作 $G \cong G'$.

(4) 如果 $G = G'$, f 是 G 到 G' 的同 (态) 构映射, 则称 f 为**自同态 (构)** 映射.

例 6.3.2 对于 $(\mathbb{Z}, +)$ 与 $(\mathbb{R}^+, \cdot)$, $f(x) = e^x$, 则 f 是 $\mathbb{Z}$ 到 $\mathbb{R}^+$ 的单同态.

例 6.3.3 设 $(\mathbb{Z}, +)$ 与 $(A, \cdot)$, 这里 $A = \{1, -1\}$, $\cdot$ 为乘法, 映射

$$f : \mathbb{Z} \to A,$$

$$f(x) = \begin{cases} 1, & \text{当 } x \text{ 为偶数 (包括负偶数) 时;} \\ -1, & \text{当 } x \text{ 为奇数 (包括负奇数) 时.} \end{cases}$$

证明: f 是 $\mathbb{Z} \to A$ 的同态 (同态映射).

例 6.3.3 设 $(\mathbb{Z},+)$ 与 $(A,\cdot)$, 这里 $A=\{1,-1\}$, $\cdot$ 为乘法, 映射

$$f:\mathbb{Z}\to A,$$

$$f(x)=\begin{cases}1, & \text{当 } x \text{ 为偶数 (包括负偶数) 时;}\\ -1, & \text{当 } x \text{ 为奇数 (包括负奇数) 时.}\end{cases}$$

证明: f 是 $\mathbb{Z}\to A$ 的同态 (同态映射).

证: 对 $\forall\, x,y\in\mathbb{Z}$,

(1) 当 x,y 都是偶数时, $f(x+y)=1=1\cdot 1=f(x)\cdot f(y)$.

(2) 当 x,y 都是奇数时, $f(x+y)=1=(-1)\cdot(-1)=f(x)\cdot f(y)$.

(3) 当 x 是奇数, y 是偶数时, $f(x+y)=-1=(-1)\cdot 1=f(x)\cdot f(y)$.

(4) 当 x 是偶数, y 是奇数时, $f(x+y)=-1=1\cdot(-1)=f(x)\cdot f(y)$.

即对 $\forall\, x,y\in\mathbb{Z}$, 都有 $f(x+y)=f(x)\cdot f(y)$ 成立.

所以, f 是 $\mathbb{Z}\to A$ 的同态, 且 f 是满射 (A 中元素都有原像), 是满同态.

例 6.3.4　设 $M(m\times n,\mathbb{R})=\{$ 实数上的全体 $m\times n$ 阶矩阵 $\}$, 规定映射

$f: M(m\times n,\mathbb{R})\to M(m\times n,\mathbb{R})$,

$f(A)=A^T$ (A^T 为 A 的转置矩阵), $\forall\ A\in M(m\times n,\mathbb{R})$.

问：(1) 关于矩阵的加法, 即 $(M(m\times n,\mathbb{R}),+)$, f 是否是 $M(m\times n,\mathbb{R})$ 的自同构?

(2) 关于矩阵的乘法, f 是否是 $M(m\times n,\mathbb{R})$ 的自同构?

例 6.3.4 设 $M(m\times n,\mathbb{R})=\{$ 实数上的全体 $m\times n$ 阶矩阵 $\}$, 规定映射

$f: M(m\times n,\mathbb{R})\to M(m\times n,\mathbb{R})$,

$f(A)=A^T$ (A^T 为 A 的转置矩阵), $\forall\ A\in M(m\times n,\mathbb{R})$.

问：(1) 关于矩阵的加法, 即 $(M(m\times n,\mathbb{R}),+)$, f 是否是 $M(m\times n,\mathbb{R})$ 的自同构?

(2) 关于矩阵的乘法, f 是否是 $M(m\times n,\mathbb{R})$ 的自同构?

解：（1）不难证明：f 是 $M(m\times n,\mathbb{R})\to M(m\times n,\mathbb{R})$ 的双射.

对 $\forall\ A,B\in M(m\times n,\mathbb{R})$,

$(A+B)^T=A^T+B^T$, 即 $f(A+B)=f(A)+f(B)$.

所以, f 是 $M(m\times n,\mathbb{R})$ 的自同构.

(2) 当 $n>1$ 时, $(AB)^T=B^TA^T\neq A^TB^T$, 即 $f(AB)\neq f(A)f(B)$.

所以, f 不是 $M(m\times n,\mathbb{R})$ 的自同构.

在有了群的定义之后, 可知群的几个最基本的性质. 将同态应用到群上, 可以随时把一个集合来同一个群比较, 或把两个群来比较. 同态(构) 用处在于比较两个集合之间的性质.

定理 6.3.1

若 $(G,\cdot)$ 与 $(G,*)$ 是同态的, 那么

1）若 $\cdot$ 适合结合律, $*$ 也适合结合律.

2）若 $\cdot$ 适合交换律, $*$ 也适合交换律.

在有了群的定义之后, 可知群的几个最基本的性质. 将同态应用到群上, 可以随时把一个集合来同一个群比较, 或把两个群来比较. 同态(构) 用处在于比较两个集合之间的性质.

定理 6.3.1

若 $(G,\cdot)$ 与 $(G,*)$ 是同态的, 那么

1) 若 $\cdot$ 适合结合律, $*$ 也适合结合律.

2) 若 $\cdot$ 适合交换律, $*$ 也适合交换律.

定理 6.3.2

若 G 是一个群, $\overline{G}$ 是一个不空集合, 则若 G 与 $\overline{G}$ 对于它们各自的运算来说同态, 那么 $\overline{G}$ 也是一个群.

事实上, 若 G 与 $\overline{G}$ 同态, 说明存在一个同态满射 f. 进而根据同态和群的条件, 易得.

例 6.3.5 $(\mathbb{R},+)$ 是群, $T=\{z \mid z\in\mathbb{C},|z|=1\}$, f 是 $\mathbb{R}\to T$ 的一个映射, 其中 $f: x\mapsto e^{ix}$, 可以证明 f 是 $\mathbb{R}\to T$ 的同态满射, 所以 $(T,\cdot)$ 是群.

事实上,

1) f 是 $\mathbb{R}\to T$ 的映射, $\forall\, x\in\mathbb{R}$, $\exists$ 唯一的像 $f(x)=e^{ix}\in T$.

2) f 是 $\mathbb{R}\to T$ 的满射, $\forall\, z\in T$, $\exists\,\theta\in\mathbb{R}$, 使得 $f(\theta)=z$.

3) f 是同态映射, 对 $\forall\, x,y\in\mathbb{R}$,

$$f(x+y)=e^{i(x+y)}=e^{ix}\cdot e^{iy}=f(x)\cdot f(y).$$

所以 f 是 $\mathbb{R}\to T$ 的同态满射,

又因为 $(\mathbb{R},+)$ 是群,

所以 $(T,\cdot)$ 是群.

定理 6.3.3

设 f 是群 G 到群 G' 的一个同态, 则

(i) $f(e)=e'$, 即同态将单位元映射到单位元.

(ii) 对任意 $a\in G, f(a^{-1})=f(a)^{-1}$, 即将 a 的逆元映射到 $f(a)$ 的逆元.

(iii) $\ker f=\{a\in G\mid f(a)=e'\}$ 是 G 的子群, 且 f 是单同态的充要条件是

$$\ker f=\{e\}.$$

(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

$$f(G)=G'.$$

(v) 设 H' 是 G' 的子群, 则 $f^{-1}(H')=\{a\in G\mid f(a)\in H'\}$ 是 G 的子群.

定理 6.3.3

设 f 是群 G 到群 G' 的一个同态, 则

(i) $f(e)=e'$, 即同态将单位元映射到单位元.

(ii) 对任意 $a\in G, f(a^{-1})=f(a)^{-1}$, 即将 a 的逆元映射到 $f(a)$ 的逆元.

(iii) $\ker f=\{a\in G\mid f(a)=e'\}$ 是 G 的子群, 且 f 是单同态的充要条件是

$$\ker f=\{e\}.$$

(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

$$f(G)=G'.$$

(v) 设 H' 是 G' 的子群, 则 $f^{-1}(H')=\{a\in G\mid f(a)\in H'\}$ 是 G 的子群.

证: (i) 因为 $f(e)f(e)=f(e^2)=f(e)$, 两端同乘以 $f(e)^{-1}$ 得, $f(e)=e'$.

定理 6.3.3

设 f 是群 G 到群 G' 的一个同态, 则

(i) $f(e)=e'$, 即同态将单位元映射到单位元.

(ii) 对任意 $a\in G, f(a^{-1})=f(a)^{-1}$, 即将 a 的逆元映射到 $f(a)$ 的逆元.

(iii) $\ker f=\{a\in G\mid f(a)=e'\}$ 是 G 的子群, 且 f 是单同态的充要条件是

$$\ker f=\{e\}.$$

(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

$$f(G)=G'.$$

(v) 设 H' 是 G' 的子群, 则 $f^{-1}(H')=\{a\in G\mid f(a)\in H'\}$ 是 G 的子群.

证: (i) 因为 $f(e)f(e)=f(e^2)=f(e)$, 两端同乘以 $f(e)^{-1}$ 得, $f(e)=e'$.

(ii) 因为 $f(a^{-1})f(a)=f(a^{-1}a)=f(e)=e'$, $f(a)f(a^{-1})=f(aa^{-1})=e'$, 所以 $f(a^{-1})=f(a)^{-1}$.

定理 6.3.3

设 f 是群 G 到群 G' 的一个同态, 则

(i) $f(e)=e'$, 即同态将单位元映射到单位元.

(ii) 对任意 $a\in G, f(a^{-1})=f(a)^{-1}$, 即将 a 的逆元映射到 $f(a)$ 的逆元.

(iii) $\ker f=\{a\in G\mid f(a)=e'\}$ 是 G 的子群, 且 f 是单同态的充要条件是

$$\ker f=\{e\}.$$

(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

$$f(G)=G'.$$

(v) 设 H' 是 G' 的子群, 则 $f^{-1}(H')=\{a\in G\mid f(a)\in H'\}$ 是 G 的子群.

证: (i) 因为 $f(e)f(e)=f(e^2)=f(e)$, 两端同乘以 $f(e)^{-1}$ 得, $f(e)=e'$.

(ii) 因为 $f(a^{-1})f(a)=f(a^{-1}a)=f(e)=e'$, $f(a)f(a^{-1})=f(aa^{-1})=e'$, 所以 $f(a^{-1})=f(a)^{-1}$.

(iii) 对任意 $a,b\in\ker f$, 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, $ab^{-1} \in \ker f$. 所以, $\ker f$ 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, $ab^{-1} \in \ker f = \{e\}$, 故 $a = b$. 因此, f 是单同态.

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

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

(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,

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

所以, $f(G)$ 是 G' 的子群, 且 f 是满同态的充要条件是 $f(G) = G'$.

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

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

(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,

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

所以, $f(G)$ 是 G' 的子群, 且 f 是满同态的充要条件是 $f(G) = G'$.

(v) 对任意 $a, b \in f^{-1}(H)$, 根据 (ii) 及 H' 为子群, 我们有

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in H' \text{ (因为 } H' \text{ 是子群).}$$

因此, $ab^{-1} \in f^{-1}(H')$. 所以, $f^{-1}(H')$ 是 G 的子群.

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

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

(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,

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

所以, $f(G)$ 是 G' 的子群, 且 f 是满同态的充要条件是 $f(G) = G'$.

(v) 对任意 $a, b \in f^{-1}(H)$, 根据 (ii) 及 H' 为子群, 我们有

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in H' \text{ (因为 } H' \text{ 是子群).}$$

因此, $ab^{-1} \in f^{-1}(H')$. 所以, $f^{-1}(H')$ 是 G 的子群.

注: $\ker f$ 叫作同态 f 的**核子群**, $f(G)$ 叫作**像子群**.

例 6.3.6 加群 $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ 到乘群 $G = \{\theta^k \mid \theta = e^{\frac{2\pi i}{n}}, k = 0, 1, 2, \cdots, n-1\}$ 的映射 $f: k \mapsto \theta^k$, 证明 f 是一个同构.

例 6.3.6 加群 $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ 到乘群 $G = \{\theta^k \mid \theta = e^{\frac{2\pi i}{n}}, k = 0, 1, 2, \cdots, n-1\}$ 的映射 $f: k \mapsto \theta^k$, 证明 f 是一个同构.

证：(1) f 是一一映射.

(a) 映射. $\forall\, x \in \mathbb{Z}/n\mathbb{Z}$, 有唯一的像 $f(x)$ 存在.

(b) 单射. 若 $x \neq y, f(x) \neq f(y)$.

(c) 满射. $\forall\, z \in G, \exists\, x \in \mathbb{Z}/n\mathbb{Z}$, 使得 $f(x) = z$, 至少有一个 x 存在.

(2) $\forall\, x, y \in \mathbb{Z}/n\mathbb{Z}, f(x+y) = \theta^{x+y} = \theta^x \cdot \theta^y = f(x) \cdot f(y)$.

所以, 综上可知 f 是一个同构.

例 6.3.6 加群 $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ 到乘群 $G = \{\theta^k \mid \theta = e^{\frac{2\pi i}{n}}, k = 0, 1, 2, \cdots, n-1\}$ 的映射 $f: k \mapsto \theta^k$, 证明 f 是一个同构.

证：(1) f 是一一映射.

(a) 映射. $\forall\, x \in \mathbb{Z}/n\mathbb{Z}$, 有唯一的像 $f(x)$ 存在.

(b) 单射. 若 $x \neq y, f(x) \neq f(y)$.

(c) 满射. $\forall\, z \in G, \exists\, x \in \mathbb{Z}/n\mathbb{Z}$, 使得 $f(x) = z$, 至少有一个 x 存在.

(2) $\forall\, x, y \in \mathbb{Z}/n\mathbb{Z}, f(x+y) = \theta^{x+y} = \theta^x \cdot \theta^y = f(x) \cdot f(y)$.

所以, 综上可知 f 是一个同构.

例 6.3.7 设 a 是群 G 的一个元, 那么映射 $f: b \mapsto aba^{-1}$ 是 G 自同态.

例 6.3.6 加群 $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ 到乘群 $G = \{\theta^k \mid \theta = e^{\frac{2\pi i}{n}}, k = 0, 1, 2, \cdots, n-1\}$ 的映射 $f: k \mapsto \theta^k$, 证明 f 是一个同构.

证：(1) f 是一一映射.

(a) 映射. $\forall\, x \in \mathbb{Z}/n\mathbb{Z}$, 有唯一的像 $f(x)$ 存在.

(b) 单射. 若 $x \neq y, f(x) \neq f(y)$.

(c) 满射. $\forall\, z \in G, \exists\, x \in \mathbb{Z}/n\mathbb{Z}$, 使得 $f(x) = z$, 至少有一个 x 存在.

(2) $\forall\, x, y \in \mathbb{Z}/n\mathbb{Z}, f(x+y) = \theta^{x+y} = \theta^x \cdot \theta^y = f(x) \cdot f(y)$.

所以, 综上可知 f 是一个同构.

例 6.3.7 设 a 是群 G 的一个元, 那么映射 $f: b \mapsto aba^{-1}$ 是 G 自同态.

证：(1) 因为 G 是群, 由封闭性可知 $\forall\, b \in G, f(b) = aba^{-1} \in G$,

所以映射 f 是 G 到 G 的映射.

(2) 下证 f 是同态映射. 因为 $\forall\, b, c \in G$, 有

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

综上, 映射 $f: b \mapsto aba^{-1}$ 是 G 自同态.

直接构造同构并不容易. 通常先构造同态, 再借助于以下同态基本定理来诱导出同构映射.

定理 6.3.4

设 f 是群 G 到群 G' 的同态, 则 f 的核 $\ker f$ 是 G 的正规子群. 反过来, 如果 N 是 G 的正规子群, 则映射 $s : G \to G/N; a \mapsto aN$ 是核为 N 的 (自然) 同态.

直接构造同构并不容易. 通常先构造同态, 再借助于以下同态基本定理来诱导出同构映射.

定理 6.3.4

设 f 是群 G 到群 G' 的同态, 则 f 的核 $\ker f$ 是 G 的正规子群. 反过来, 如果 N 是 G 的正规子群, 则映射 $s: G \to G/N; a \mapsto aN$ 是核为 N 的 (自然) 同态.

证：由前面的定理 6.3.3 知, $\ker f \leq G$.

对任意的 $a \in G, b \in \ker f$, 我们有

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

所以 $aba^{-1} \in \ker f$. 故 $\ker f$ 是 G 的正规子群.

直接构造同构并不容易. 通常先构造同态, 再借助于以下同态基本定理来诱导出同构映射.

定理 6.3.4

设 f 是群 G 到群 G' 的同态, 则 f 的核 $\ker f$ 是 G 的正规子群. 反过来, 如果 N 是 G 的正规子群, 则映射 $s: G \to G/N; a \mapsto aN$ 是核为 N 的 (自然) 同态.

证：由前面的定理 6.3.3 知, $\ker f \leq G$.

对任意的 $a \in G, b \in \ker f$, 我们有

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

所以 $aba^{-1} \in \ker f$. 故 $\ker f$ 是 G 的正规子群.

反过来, 设 N 是 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, $s(a) = N$ 的充要条件是 $a \in N$. 因此, s 是核为 N 的同态.

定理 6.3.5 (群同态基本定理)

设 f 是群 G 到群 G' 的同态, 则存在唯一的 $G/\ker f$ 到像子群 $f(G)$ 的同构 $\bar{f}: a\ker f \mapsto f(a)$ 使得 $f = i \circ \bar{f} \circ s$, 其中 s 是群 G 到群 $G/\ker f$ 的自然同态, $i: c \mapsto c$ 是 $f(G)$ 到 G' 的恒等同态, 即有以下的交换图:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s\downarrow & & \uparrow i \\ G/\ker f & \xrightarrow{\bar{f}} & f(G) \end{array}$$

定理 6.3.5 (群同态基本定理)

设 f 是群 G 到群 G' 的同态, 则存在唯一的 $G/\ker f$ 到像子群 $f(G)$ 的同构 $\bar{f}: a\ker f \mapsto f(a)$ 使得 $f = i \circ \bar{f} \circ s$, 其中 s 是群 G 到群 $G/\ker f$ 的自然同态, $i: c \mapsto c$ 是 $f(G)$ 到 G' 的恒等同态, 即有以下的交换图:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s\downarrow & & \uparrow i \\ G/\ker f & \xrightarrow{\bar{f}} & f(G) \end{array}$$

证: 首先, 证明存在性.

定理 6.3.5 (群同态基本定理)

设 f 是群 G 到群 G' 的同态, 则存在唯一的 $G/\ker f$ 到像子群 $f(G)$ 的同构 $\bar{f}: a\ker f \mapsto f(a)$ 使得 $f = i \circ \bar{f} \circ s$, 其中 s 是群 G 到群 $G/\ker f$ 的自然同态, $i: c \mapsto c$ 是 $f(G)$ 到 G' 的恒等同态, 即有以下的交换图:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s\downarrow & & \uparrow i \\ G/\ker f & \xrightarrow{\bar{f}} & f(G) \end{array}$$

证: 首先, 证明存在性.

根据定理 6.3.4, $\ker f$ 是 G 的正规子群, 所以存在商群 $G/\ker f$.

定理 6.3.5 (群同态基本定理)

设 f 是群 G 到群 G' 的同态, 则存在唯一的 $G/\ker f$ 到像子群 $f(G)$ 的同构 $\bar{f}: a\ker f \mapsto f(a)$ 使得 $f = i \circ \bar{f} \circ s$, 其中 s 是群 G 到群 $G/\ker f$ 的自然同态, $i: c \mapsto c$ 是 $f(G)$ 到 G' 的恒等同态, 即有以下的交换图:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s\downarrow & & \uparrow i \\ G/\ker f & \xrightarrow{\bar{f}} & f(G) \end{array}$$

证: 首先, 证明存在性.

根据定理 6.3.4, $\ker f$ 是 G 的正规子群, 所以存在商群 $G/\ker f$.

现在要证明: $\bar{f}: a\ker f \mapsto f(a)$ 是 $G/\ker f$ 到像子群 $f(G)$ 的同构.

(1) $\bar{f}$ 是映射, 即 "任一元素有唯一的像".

若 $a\ker f = b\ker f \Rightarrow b^{-1}a \in \ker f \Rightarrow f(b^{-1}a) = f(b^{-1})f(a) = e$,

所以 $f(a) = f(b)$, 所以像唯一.

(2) $\bar{f}$ 是单射, 即“不同的原像, 有不同的像”.

若 $a\ker f \neq b\ker f \Rightarrow b^{-1}a \notin \ker f \Rightarrow f(b^{-1}a) = f(b^{-1})f(a) \neq e$,

所以 $f(a) \neq f(b)$.

(3) $\bar{f}$ 是满射. 对任意的 $c \in f(G)$, 存在 $a \in G$ 使得 $f(a) = c$.

从而, $\bar{f}(a\ker f) = f(a) = c$. 即 $a\ker f$ 是 c 的原像.

(4) 保持同态, 即 $\bar{f}$ 是 $G/\ker f$ 到 $f(G)$ 的同态映射.

对任意的 $a\ker f, b\ker f \in G/\ker f$, 有

$$\bar{f}((a\ker f)(b\ker f)) = \bar{f}((ab)\ker f) = f(ab) = f(a)f(b) = \bar{f}(a\ker f)\bar{f}(b\ker f).$$

综上, $\bar{f}$ 是同构. 并且, 有 $f = i \circ \bar{f} \circ s$. 因为

$$i \circ \bar{f} \circ s(a) = i(\bar{f}(s(a))) = i(\bar{f}(a\ker f)) = i(f(a)) = f(a), a \in G.$$

(2) $\bar{f}$ 是单射, 即“不同的原像, 有不同的像”.

若 $a\ker f \neq b\ker f \Rightarrow b^{-1}a \notin \ker f \Rightarrow f(b^{-1}a) = f(b^{-1})f(a) \neq e$,

所以 $f(a) \neq f(b)$.

(3) $\bar{f}$ 是满射. 对任意的 $c \in f(G)$, 存在 $a \in G$ 使得 $f(a) = c$.

从而, $\bar{f}(a\ker f) = f(a) = c$. 即 $a\ker f$ 是 c 的原像.

(4) 保持同态, 即 $\bar{f}$ 是 $G/\ker f$ 到 $f(G)$ 的同态映射.

对任意的 $a\ker f, b\ker f \in G/\ker f$, 有

$$\bar{f}((a\ker f)(b\ker f)) = \bar{f}((ab)\ker f) = f(ab) = f(a)f(b) = \bar{f}(a\ker f)\bar{f}(b\ker f).$$

综上, $\bar{f}$ 是同构. 并且, 有 $f = i \circ \bar{f} \circ s$. 因为

$$i \circ \bar{f} \circ s(a) = i(\bar{f}(s(a))) = i(\bar{f}(a\ker f)) = i(f(a)) = f(a), a \in G.$$

最后证明唯一性.

假如还有同构 $g : G/\ker f \to f(G)$ 使得 $f = i \circ g \circ s$,

则对任意 $a\ker f \in G/\ker f$, 我们有

$$g(a\ker f) = i(g(s(a))) = (i \circ g \circ s)(a) = f(a) = \bar{f}(a\ker f), \text{即 } g = \bar{f}.$$

例 6.3.8　设 f 是群 $\mathbb{Z}$ 到群

$$G =< a >= \{a^n \mid 0 \leq n < 3, a^3 = 1\} = \{1, a, a^2\}$$

的同态, $f : n \mapsto a^n$. 我们有 $\mathbb{Z}/\ker f \cong < a >$.

具体来说, f 是群 $\mathbb{Z}$ 到群

$$G =< a >= \{a^n \mid 0 \leq n < 3, a^3 = 1\} = \{1, a, a^2\}$$

的同态, 有 $\ker f = 3\mathbb{Z}$,

则 $\mathbb{Z}/\ker f = \mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$,

等价于 $G =< a >= \{a^n \mid 0 \leq n < 3, a^3 = 1\} = \{1, a, a^2\}$.

本课作业

1. 群 $U_4 = \{1, -1, i, -i\}$ 的下列子集是否构成群 U_4 的子群?

(1) $\{1, -1\}$;

(2) $\{i, -i\}$;

(3) $\{1, i\}$;

(4) $\{1, -i\}$.

2. 证明 $SL_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$ 的正规子群.

3. 整数加群 $\mathbb{Z}$ 与偶数加群 $2\mathbb{Z}$ 同构.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn