离散数学

Discrete Mathematics

吴梅红

厦门大学计算机科学系

E-mail: wmh@xmu.edu.cn



6.4 群的直积与同态

- 群的积代数就是群的直积。

定义 6.11 设$<G_1, *>$, $<G_2, \circ>$是群, 在 $G_1 \times G_2$上定义运算 $\cdot$ 如下: $\forall <a_1, b_1>, <a_2, b_2> \in G_1 \times G_2$,

$$<a_1, b_1> \cdot <a_2, b_2> = < a_1 * a_2 , b_1 \circ b_2 >,$$

则 $G_1 \times G_2$ 关于$\cdot$ 运算构成群, 称为$G_1 \times G_2$的直积。

例 6.20 设 $G_1 = <Z_6, \oplus>$, $G_2 = <Z, +>$,

则 $G_1 \times G_2 = <Z_6 \times Z, *>$, 且有

$$<4, 5> * <3, -6> = <4 \oplus 3, 5 + (-6)> = <1, -1>,$$

$$<2, 6>^3 = <2 \oplus 2 \oplus 2, 6 + 6 + 6> = <0, 18>。$$

定义 6.12 设$<G_1, *>$, $<G_2, \circ>$是群, $f: G_1 \to G_2$,

如果 $\forall a, b \in G_1$, 都有

$$f(a * b) = f(a) \circ f(b)$$

成立, 则称 f 是G_1到G_2的同态映射, 简称同态。

- 如果同态映射f 是单射, 称为单同态;
- 如果是满射, 则称为满同态;
- 如果是双射, 则称为同构。

例 6.21 (1) 设 $G = \langle Z, +\rangle$, $f : Z \to Z$, $f(x) = kx$,

其中k为整数, 那么$\forall\ a, b \in Z$, 有

$$f(a + b) = k(a + b) = ka + kb = f(a) + f(b),$$

因此, f为G的自同态。

- 当$k = 0$时, f 将所有元素映射到单位元, 称为零同态;
- 当$k = \pm 1$时, f 为双射, 是同构;
- 而对于其他的整数k, f 是单同态。∎

例 6.21(2)设$G = \langle Z_n, \oplus \rangle$, $\oplus$为模n加法, $f_p: Z_n \to Z_n$,

$f_p(x) = (px) \bmod n$, $p = 0, 1, \ldots, n-1$, 则 $\forall\, a, b \in Z_n$, 有

$$f_p(a \oplus b) = (p(a \oplus b)) \bmod n = (pa \oplus pb)) \bmod n$$

$$= (pa) \bmod n \oplus (pb) \bmod n = f_p(a) \oplus f_p(b)。$$

f 为自同态。例如n = 6, $G = \langle Z_n, \oplus \rangle$有6个自同态如下:

$f_0 = \{\langle 0, 0\rangle, \langle 1, 0\rangle, \langle 2, 0\rangle, \langle 3, 0\rangle, \langle 4, 0\rangle, \langle 5, 0\rangle\}$;

$f_1 = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 4, 4\rangle, \langle 5, 5\rangle\}$;

$f_2 = \{\langle 0, 0\rangle, \langle 1, 2\rangle, \langle 2, 4\rangle, \langle 3, 0\rangle, \langle 4, 2\rangle, \langle 5, 4\rangle\}$;

$f_3 = \{\langle 0, 0\rangle, \langle 1, 3\rangle, \langle 2, 0\rangle, \langle 3, 3\rangle, \langle 4, 0\rangle, \langle 5, 3\rangle\}$;

$f_4 = \{\langle 0, 0\rangle, \langle 1, 4\rangle, \langle 2, 2\rangle, \langle 3, 0\rangle, \langle 4, 4\rangle, \langle 5, 2\rangle\}$;

$f_5 = \{\langle 0, 0\rangle, \langle 1, 5\rangle, \langle 2, 4\rangle, \langle 3, 3\rangle, \langle 4, 2\rangle, \langle 5, 1\rangle\} \cong f_1$。

例 6.21(3) 设$G_1 = \langle Z, +\rangle$, $G_2 = \langle Z_n, \oplus\rangle$, $f: Z \rightarrow Z_n$,

$f(x) = (x) \bmod n$, 则 $\forall a, b \in Z$, 有

$$f(a + b) = (a \oplus b) \bmod n$$

$$= (a) \bmod n \oplus (b) \bmod n$$

$$= f(a) \oplus f(b)。$$

f 是G_1 到 G_2 的满同态。 $\blacksquare$

例 6.21(4) 设$G_1 = \langle R, +\rangle$, $G_2 = \langle R^*, \cdot\rangle$, $f: R \rightarrow R^*$,

$f(x) = e^x$, 则 $\forall a, b \in R$, 有

$$f(a + b) = e^{a+b} = e^a \cdot e^b$$

$$= f(a) \cdot f(b)$$

f 为G_1 到 G_2 的单同态。 $\blacksquare$

定理 6.10 设f 是群G_1到G_2的同态映射, 则

(1) $f(e_1) = e_2$, 其中e_1和 e_2分别是G_1和G_2的单位元。

证明(1) $f(e_1)f(e_1) = f(e_1e_1) = f(e_1) = f(e_1)e_2$,

由消去律得 $f(e_1) = e_2$。

(2) $\forall x \in G_1$, $f(x^{-1}) = f(x)^{-1}$。

证明(2) $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_1) = e_2$,

$f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2$。故 $f(x^{-1}) = f(x)^{-1}$。

(3) 设$H \le G_1$, 那么 $f(H) \le G_2$。

证 $e_2 \in f(H)$, $f(H)$非空。$\forall a, b \in f(H)$, $\exists$对应的$x, y \in H$,

使得 $f(x) = a$, $f(y) = b$, $xy^{-1} \in H$,

从而有 $ab^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$, 即$f(H) \le G_2$。

例 6.22 设$G_1 = <Q^*, \bullet>$, $G_2 = <Q, +>$,

则不存在G_1到 G_2的同构。 其中$Q^* = Q - \{0\}$。

证 假设 存在同构, $f : Q^* \to Q$,

则 $f(1) = 0$。

由此得 $f(-1) + f(-1) = f((-1)(-1)) = f(1) = 0$。

于是有 $2f(-1) = 0$, $f(-1) = 0$

与f 是双射矛盾。