

证明: 对任意  $x \in \mathbb{Z}$ , 分两种情况:

情况一: 若  $x = 2k (k \in \mathbb{Z})$  为偶数, 则  $f(\Delta x) = f(2k+1) = (2k+1) \bmod 2 = 1$ , 而  $\diamond f(x) = \diamond(2k \bmod 2) = \diamond 0 = 1 \bmod 2 = 1$ , 从而有  $f(\Delta x) = \diamond f(x)$ 。

情况二: 若  $x = 2k+1 (k \in \mathbb{Z})$  为奇数, 则  $f(\Delta x) = f(2k+2) = (2k+2) \bmod 2 = 0$ , 而  $\diamond f(x) = \diamond(2k+1 \bmod 2) = \diamond 1 = 0 \bmod 2 = 0$ , 从而也有  $f(\Delta x) = \diamond f(x)$ 。

这就是说, 对任意  $x \in \mathbb{Z}$ , 都有  $f(\Delta x) = \diamond f(x)$ , 从而  $f$  是同态。  $\square$

由于  $f(0) = 0, f(1) = 1$ , 所以  $f$  是满同态。又由于  $f(2) = f(0) = 0$ , 所以  $f$  不是单同态, 从而不是同构。

2.

(1)

证明: 对任意  $x, y \in L$ , 有:

$$\begin{aligned}
 f_a(x \vee y) &= (x \vee y) \wedge a && (f_a \text{ 定义}) \\
 &= (x \wedge a) \vee (y \wedge a) && (L \text{ 是分配格}) \\
 &= f_a(x) \vee f_a(y) && (f_a \text{ 定义}) \\
 f_a(x \wedge y) &= (x \wedge y) \wedge a && (f_a \text{ 定义}) \\
 &= (x \wedge y) \wedge (a \wedge a) && (a \wedge a = a) \\
 &= (x \wedge a) \wedge (y \wedge a) && (\text{交换律、结合律}) \\
 &= f_a(x) \wedge f_a(y) && (f_a \text{ 定义})
 \end{aligned}$$

这就证明了  $f_a$  是自同态。同理可证  $g_a$  是自同态。  $\square$

(2) 由幂集格定义知, 对任意  $x \in L$ ,  $x \in f_{\{1\}}(L)$  当且仅当  $x \subseteq \{1\}$  (充分性: 若  $x \subseteq \{1\}$ , 则  $x = x \cap \{1\} = f_{\{1\}}(x) \in f_{\{1\}}(L)$ 。必要性: 若  $x \in f_{\{1\}}(L)$ , 则  $x = f_{\{1\}}(y) = y \cap \{1\} \subseteq \{1\}$ )。从而  $f_{\{1\}}(L) = \{\emptyset, \{1\}\}$ ,  $f_{\{1\}}$  的同态像为  $\{\{\emptyset, \{1\}\}, \wedge, \vee\}$ 。

同理可知, 对任意  $x \in L$ ,  $x \in g_{\{1\}}(L)$  当且仅当  $\{1\} \subseteq x$ 。从而  $g_{\{1\}}(L) = \{\{1\}, \{0, 1\}, \{1, 2\}, \{0, 1, 2\}\}$ ,  $g_{\{1\}}$  的同态像为  $\{\{\{1\}, \{0, 1\}, \{1, 2\}, \{0, 1, 2\}\}, \wedge, \vee\}$ 。

3.

证明: 充分性。若  $G$  为素数, 则由 **Lagrange 定理**知,  $G$  没有非平凡的子群(从而也没有非平凡的正规子群), 所以  $G$  是单群。

必要性。设  $G$  为单群。任取  $G$  中一个非单位元  $a \in G$  (本题应假定  $G$  是非平凡的, 否则若  $G = \{e\}$ , 则  $G$  也是单群, 但  $|G| = 1$ , 不是素数), 则由于  $\langle a \rangle$  是  $G$  的正规子群(因为  $G$  是 Abel 群, 所以  $G$  的一切子群都是正规的), 且  $a$  不是单位元, 所以  $|\langle a \rangle| = |a| > 1$ ,  $\langle a \rangle \neq \{e\}$ 。由单群定义知, 必有  $\langle a \rangle = G$ 。从而  $G = \{a^k \mid k \in \mathbb{Z}\}$  是由  $a$  生成的循环群。下面证明  $G$  是素数阶的。

反设  $G$  不是素数阶的, 则分两种情况讨论。

情况一: 若  $G$  是无限阶的, 则  $a$  也是无限阶的, 从而  $a^2 \neq e, a^2 \neq a$ 。这就是说,  $\langle a^2 \rangle \neq G$  (因为  $a \notin \langle a^2 \rangle$ ) 且  $\langle a^2 \rangle \neq \{e\}$  (因为  $a^2 \in \langle a^2 \rangle$ ), 从而  $\langle a^2 \rangle$  是  $G$  的一个非平凡的正规子群, 这与  $G$  是单群矛盾。

情况二: 若  $G$  是有限阶的且  $|G|$  不是素数, 则存在  $k \mid |G|, 1 < k < |G|$ , 而  $1 < |\langle a^k \rangle| = |a^k| = \frac{|G|}{k} < |G|$ , 从而  $\langle a^k \rangle$  是  $G$  的一个非平凡的正规子群, 矛盾。  $\square$