离散数学作业 Solution set 18

Problem 1

对以下各小题给定的群 G_1 和 G_2，以及 $f: G_1 \to G_2$，说明 f 是否为群 G_1 到 G_2 的同态，如果是，说明是否为单同态、满同态和同构。求同态像 $f(G_1)$。

(1) $G_1 = \langle Z, + \rangle$, $G_2 = \langle R^*, \cdot \rangle$, 其中 R^* 为非零实数集合，+ 和 $\cdot$ 分别表示数的加法和乘法。

$$f: Z \to R^*, f(x) = \begin{cases} 1 & x \text{ 是偶数} \\ -1 & x \text{ 是奇数} \end{cases}$$

(2) $G_1 = \langle Z, + \rangle$, $G_2 = \langle A, \cdot \rangle$, 其中 + 和 $\cdot$ 分别表示数的加法和乘法, $A = \{x | x \in C \wedge |x| = 1\}$, 其中 C 为复数集合。

$$f: Z \to A, f(x) = \cos x + i \sin x$$

解:

(1) 是同态，不是单同态，也不是满同态。$f(G_1) = \{-1, 1\}$

(2) 是同态，是单同态，不是满同态。$f(G_1) = \{\cos x + i \sin x | x \in \mathbb{Z}\}$

Problem 2

令 G, G' 为群，函数 $f: G \to G'$ 是一个群同态。证明:

(1) $\ker f = \{x \in G | f(x) = e\}$ 是 G 的子群

(2) $\mathrm{img}\ f = \{x \in G' | \exists g \in G, f(g) = x\}$ 是 G' 的子群

解:

(1) 首先 $e \in \ker f$，$\ker f$ 非空。任取 $a, b \in \ker f$，我们有 $f(ab^{-1}) = f(a)f(b)^{-1} = e \in \ker f$，所以 $\ker f = \{x \in G | f(x) = e\}$ 是 G 的子群

(2) 首先 $e \in \mathrm{img}\ f$，$\mathrm{img}\ f$ 非空。任取 $a, b \in \mathrm{img}\ f$，则存在 $g, h \in G$，使得 $f(g) = a, f(h) = b$。则 $ab^{-1} = f(g)f(h^{-1}) = f(gh^{-1}) \in \mathrm{img}\ f$，所以 $\mathrm{img}\ f = \{x \in G' | \exists g \in G, f(g) = x\}$ 是 G' 的子群

Problem 3

设 G_1 为循环群，f 是群 G_1 到 G_2 的同态，证明 $f(G_1)$ 也是循环群。

解:

设 $G_1 =< a >$, $f : G_1 \to G_2$ 为群同态。易见 $f(G_1)$ 为群, 对任意 $y \in f(G_1)$, 存在 $a^i \in G_1$，使得

$$y = f(a^i) = (f(a))^i$$

故 $f(G_1) =< f(a) >$.

Problem 4

设 ϕ 是群 G 到 $G^{'}$ 的同构映射，$a \in G$，证明：a 的阶和 $\phi(a)$ 的阶相等。

解:

注意到 $\phi(a)^{|a|} = \phi(a^a) = \phi(e) = e$，则有 $|\phi(a)| \mid |a|$。因为 ϕ 为同构，故 ϕ^{-1} 为 G' 到 G 的同构，因此 $|a| \mid |\phi(a)|$。得证。

Problem 5

证明：三阶群必为循环群.

证明:

任意不为单位元的元素阶均不等于 1 且整除 3，故只能为 3。因此任意不为单位元的元素均生成整个群，故为循环群。

Problem 6

我们记 n 阶循环群为 C_n，欧拉函数 $\phi(m)$ 定义为与 m 互素且不大于 m 的正整数的个数，考虑以下三个事实

对正整数 m，欧拉函数的结果 $\phi(m)$ 为 C_m 的生成元的个数

C_n 的每个元素均生成 C_n 的一个子群

C_n 的每个子群均是一个循环群 C_m，且 $m \mid n$

证明著名的公式

$$\sum_{m>0, m|n} \phi(m) = n$$

证明：左边为 C_n 的所有子群的生成元的数量，右边为 C_n 中元素的数量。我们知道 C_n 中每个元素均能生成一个循环子群，故得证。
严格地，对任意 $m \mid n$，C_n 中恰好存在 $\phi(m)$ 个可以生成 m 阶循环子群的元素。因为 $m \mid n$，$C_n =< a >$ 恰有一个 m 阶子群 $< a^{n/m} >$。其有 $\phi(m)$ 个生成元，均属于 C_n。故 $\sum_{m>0,m|n} \phi(m) \leq n \wedge \sum_{m>0,m|n} \phi(m) \geq n$。
得证。

Problem 7

设 p 是素数，证明每一个 p 阶群都是循环群，且以每一个非单位元的元素作为它的生成元。
证明：
设 G 为 p 阶群，可知 $|G| \geq 2$。对任意 $m \neq e \in G$ 我们有 $|m| \mid p$，即 $|m| = p$。则 $G =< m >$。得证。

Problem 8

证明：循环群一定是阿贝尔群。

证明:

设 G = <a> 是循环群. $\forall a^i, a^j \in < a >$，有 $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$，得证。

Problem 9

设 G 为群, a 是 G 中给定元素, a 的正规化子 $N(a)$ 表示 G 中与 a 可交换的元素构成的集合，即 $N(a) = \{x | x \in G \wedge xa = ax\}$. 证明: $N(a)$ 是 G 的子群.

证明:

1. $ea = ae$, $e \in N(a) \neq \emptyset$,
2. $\forall x, y \in N(a)$, 则 $ax = xa, ay = ya$.
3. $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$, 所以 $xy \in N(a)$

由 $ax = xa$, 得 $x^{-1}axx^{-1} = x^{-1}xax^{-1}$, $x^{-1}ae = eax^{-1}$, 即 $x^{-1}a = ax^{-1}$, 所以 $x^{-1} \in N(a)$。根据判定定理，$N(a)$ 是 G 的子群.