离散数学（2023）作业 20 - 循环群与群同构

离散数学教学组

Problem 1

证明：三阶群必为循环群。

答案： 任意不为单位元的元素的阶均不等于 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 2

证明：循环群一定是交换群。

答案： 设 $G = \langle a \rangle$ 是循环群。$\forall a^i, a^j \in \langle a \rangle$，有 $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$，得证。

Problem 3

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。

答案： 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 $G = \langle m \rangle$，得证。

Problem 4

考虑整数加群 $(\mathbb{Z}, +)$ 的循环子群 $\langle a \rangle$ 和 $\langle b \rangle$，其中 a, b 分别是两个循环群的生成元，则 $\langle a \rangle$ 是 $\langle b \rangle$ 的子群当且仅当 $b \mid a$。

答案：

- 充分性：由 $b \mid a$ 得，存在一整数 k，使得 $a = k * b$。对于任意 $\langle a \rangle$ 中的元素 a^i，我们有 $a^i = (kb)^i = (k^i)(b^i)$。由于 b^i 是 $\langle b \rangle$ 中的元素，我们只需证明 k^i 也是 $\langle b \rangle$ 中的元素。将 $a = k * b$ 代入 k^i 中，我们有 $k^i = \left(\frac{a}{b}\right)^i = \frac{a^i}{b^i}$。由于 a^i 和 b^i 都是 $\langle a \rangle$ 中的元素，且 $\langle a \rangle$ 是一个子群，所以它们的商 $\frac{a^i}{b^i}$ 也是 $\langle a \rangle$ 中的元素。因此，k^i 是 $\langle b \rangle$ 中的元素。
- 必要性：由 $\langle a \rangle$ 是 $\langle b \rangle$ 的子群，对任意 $\langle a \rangle$ 中元素 a^i, a^j，则 $a^i, a^j \in \langle b \rangle$。令 $j = i + 1$，则存在整数 p, q，满足 $a^i = b^p a^{(i+1)} = b^q$。两边分别做商，得 $a = b^{(q-p)} = b + b + \cdots + b$($q$-$b$ 个 b 相加)=$(q-p) * b$。令 $r = q - p$，由 p 和 q 为整数，r 为整数，即存在整数 r，使得 $a = r * b$，所以 $b \mid a$。

Problem 5

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。

答案： 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 6

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

答案： 设 $G_1 = \langle a \rangle$，$f : G_1 \to G_2$ 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 $f(G_1) = \langle f(a) \rangle$。

Problem 7

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。

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

答案：

1. 是同态，不是单同态，也不是满同态。
2. 是同态，是单同态，不是满同态。

Problem 8

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

答案：

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

Problem 9

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：

1. 对正整数 m，欧拉函数的结果 $\phi(m)$ 为 C_m 的生成元的个数
2. C_n 的每个元素均生成 C_n 的一个子群
3. C_n 的每个子群均是一个循环群 C_m，且 $m \mid n$

证明公式
$$\sum_{m>0, m|n} \phi(m) = n$$

答案： 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 $\langle a^{n/m} \rangle$。其有 $\phi(m)$ 个生成元，均属于 C_n。故 $\sum_{m>0,m|n} \phi(m) \le n \wedge \sum_{m>0,m|n} \phi(m) \ge n$，得证。

Problem 10

证明：整数加群 Z **不与**有理数加群 Q 同构。

答案： 假设同构，则存在双射 $f : Z \to Q$ 满足同态性质。令有理数 $p/q = f(1)$，我们有 $f(-1) = -p/q$。则对任意 $k \in Q$，均存在整数 z，使得 $k = f(z) = z \times (p/q)$。即存在 z' 使得 $|z||p/q| = |(1/2q)| < |p/q|$。矛盾，得证。