第二次作业

Log Creative

2023 年 9 月 26 日

1. (a) 解：是。$Z_5 = \{0, 1, 2, 3, 4\}$，则

   封闭性 若 $a, b \in Z_5$，则 $((a+b) \bmod 5) \in Z_5$；

   结合律 $(a+b)+c \bmod 5 = a+(b+c) \bmod 5$；

   单位元 0 是群的单位元，$a+0 \equiv a \pmod 5$；

   逆元 每个元素都有逆元：$0+0 \equiv 0 \pmod 5$; $1+4 \equiv 0 \pmod 5$; $2+3 \equiv 0 \pmod 5$; $3+2 \equiv 0 \pmod 5$；$4+1 \equiv 0 \pmod 5$。

   所以 $(Z_5, + \bmod 5)$ 是一个群。

   生成元 而 $g = 3$ 是它的一个生成元：

i	1	2	3	4	5
$g^i \bmod 5$	3	1	4	2	0

   所以 $(Z_5, + \bmod 5)$ 是一个循环群。

   (b) 解：不是。$Z_8^* = \{1, 3, 5, 7\}$，则：

   封闭性 $1 \times x \equiv x \pmod 8 \in Z_8^*$；$3 \times 5 \equiv 7 \pmod 8, 3 \times 7 \equiv 5 \pmod 8, 5 \times 7 \equiv 7 \pmod 8$；

   结合律 $(a \times b) \times c \equiv a \times (b \times c) \pmod 8$；

   单位元 1 是群的单位元，$a \times 1 \equiv a \pmod 8$；

   逆元 每个元素都有逆元：$1 \times 1 \equiv 1 \pmod 8, 3 \times 3 \equiv 1 \pmod 8, 5 \times 5 \equiv 1 \pmod 8, 7 \times 7 \equiv 1 \pmod 8$。

   所以 $(Z_8^*, \times \bmod 8)$ 是一个群。

   生成元 而它的任何一个元素都不是它的生成元：$\{1\}, \{1, 3\}, \{1, 5\}, \{1, 7\}$ 都是它的生成子群。

   所以 $(Z_8^*, \times \bmod 8)$ 不是循环群。

2. 解：由于循环群的性质：$h \circ h^{q-1} = h^q = e$，以及循环群的封闭性性质，$h^{q-1} \in G$，所以 h^{q-1} 是 h 的逆元。

   为了求出 h^{q-1}，可以考虑使用平方相乘法，逐步求出 $h, h^2, \cdots, h^{2^k}$ $(k = \lfloor \log_2(q-1) \rfloor)$，而 $q-1 = (a_k a_{k-1} \cdots a_0)_2$ 表示为二进制形式，那么

   $$h^{q-1} = (h^{2^k})^{a_k} \cdot (h^{2^{k-1}})^{a_{k-1}} \cdot \cdots \cdot h^{a_0}$$

   可以在 $O(\log_2(q-1))$ 时间内求出。

3. 解：$(Z_{13}, + \bmod 13)$ 是满足条件的 13 阶循环群。

   封闭性 若 $a, b \in Z_{13}$，则 $((a+b) \bmod 13) \in Z_{13}$；

结合律 $(a+b)+c \bmod 13 = a+(b+c) \bmod 13$;

单位元 0 是群的单位元，$a+0 \equiv a \pmod{13}$;

逆元 每个元素 $x \in Z_{13}$ 都有逆元 $(13-x) \in Z_{13}$，$x+(13-x) \equiv 0 \pmod{13}$。

所以 $(Z_{13}, + \bmod 13)$ 是一个群。

生成元 $g=5$ 是它的一个生成元。

g	1	2	3	4	5	6	7	8	9	10	11	12	13
$g^i \bmod 13$	5	10	2	7	12	4	9	1	6	11	3	8	0