

第...次作业
 张旭辉
 2012205036
 计算机组

1. 解:
 已知 G 的阶为 p^2 , 其中 p 为素数
 对 g, g_2 , ~~显然 (g, g_2) 不一定为 e , $(g, g_2)^2 = g^2 \cdot g_2^2$ 不一定为 e , 故只能是 $(g, g_2)^{p^2} = e$~~
 因此 g, g_2 阶为 p^2 .

2. 证:
 已知 G 是循环群, 不妨设 $\langle g \rangle = G$, 即 g 为生成元,
 $g \in G$
 由题可知, H 是 G 的正规子群, 则 $G/H = \{g^i H \mid 0 \leq i < n\}$
 若证 G/H 是循环群, 只需说明 G/H 至少有一个生成元.
 $\therefore G = \langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$
 $\therefore (g, H)^2 = eH \in G/H$
 $(g, H)' = g, H \in G/H$
 $(g, H)^2 = (g, H) \cdot (g, H) = g^2 \cdot H \in G/H$
 $(g, H)^3 = (g, H) \cdot (g, H)^2 = g^3 \cdot H \in G/H$
 \vdots
 $(g, H)^i = \underbrace{(g, H) \cdots (g, H)}_{i \uparrow} = g^i H \in G/H$
 故 $G/H = \langle g, H \rangle$
 得证.

3. 证:
 $\therefore G$ 是循环群, $\forall a, b \in G$ 有 $\phi(ab) = \phi(a)\phi(b)$
 $\forall g \in G$ 且存在 $k \in \mathbb{Z}$ 使得 $g = g^k$, 有 $\phi(g) = \phi(g^k) = \phi(g) \cdots \phi(g)$
 $= \phi(g)^k$
 $\therefore \phi(G)$ 是循环群.
 $\therefore G$ 是交换群, 且 $\forall a, b \in G$ 有 $\phi(ab) = \phi(a)\phi(b)$
 G 是交换群, 故 $ab = ba$
 $\therefore \phi(b)\phi(a) = \phi(ba) = \phi(ab) = \phi(a)\phi(b)$
 $\therefore \phi(G)$ 是交换群.

4. 证:
 $\therefore p$ 和 q 是素数, G 阶为 p^2
 故对 $\forall g \in G$, 阶为 $1, p, q$ 或 p^2
 假设 $g_1, g_2 \in G$, 且 g_1 的阶为 p, g_2 的阶为 q , 题已证得
 g_1, g_2 的阶为 p, q , 即为群的阶
 $\therefore g_1, g_2$ 为 G 的一个生成元
 $\therefore G$ 是循环群.