

《离散数学》题库答案

(代数结构部分)

37、设 $A = \{2, 4, 6\}$, A 上的二元运算 $*$ 定义为: $a * b = \max \{a, b\}$, 则在独异点 $\langle A, * \rangle$ 中, 单位元是(), 零元是()。

答: 2, 6

38、设 $A = \{3, 6, 9\}$, A 上的二元运算 $*$ 定义为: $a * b = \min \{a, b\}$, 则在独异点 $\langle A, * \rangle$ 中, 单位元是(), 零元是();

答: 9, 3

(半群与群部分)

39、设 $\langle G, * \rangle$ 是一个群, 则

(1) 若 $a, b, x \in G$, $a * x = b$, 则 $x = ()$;

(2) 若 $a, b, x \in G$, $a * x = a * b$, 则 $x = ()$ 。

答: (1) $a^{-1} * b$ (2) b

40、设 a 是 12 阶群的生成元, 则 a^2 是()阶元素, a^3 是()阶元素。

答: 6, 4

41、代数系统 $\langle G, * \rangle$ 是一个群, 则 G 的等幂元是()。

答: 单位元

42、设 a 是 10 阶群的生成元, 则 a^4 是()阶元素, a^3 是()阶元素。

答: 5, 10

43、群 $\langle G, * \rangle$ 的等幂元是(), 有()个。

答: 单位元, 1

44、素数阶群一定是()群, 它的生成元是()。

答: 循环群, 任一非单位元

45、设 $\langle G, * \rangle$ 是一个群, $a, b, c \in G$, 则

(1) 若 $c * a = b$, 则 $c = ()$; (2) 若 $c * a = b * a$, 则 $c = ()$ 。

答: (1) $b * a^{-1}$ (2) b

46、 $\langle H, , * \rangle$ 是 $\langle G, , * \rangle$ 的子群的充分必要条件是()。

答: $\langle H, , * \rangle$ 是群 或 $\forall a, b \in G, a * b \in H, a^{-1} \in H$ 或 $\forall a, b \in G, a * b^{-1} \in H$

47、群 $\langle A, * \rangle$ 的等幂元有()个, 是(), 零元有()个。

答: 1, 单位元, 0

48、在一个群 $\langle G, * \rangle$ 中, 若 G 中的元素 a 的阶是 k , 则 a^{-1} 的阶是()。

答: k

49、在自然数集 N 上, 下列哪种运算是可结合的? ()

(1) $a * b = a - b$ (2) $a * b = \max \{a, b\}$ (3) $a * b = a + 2b$ (4) $a * b = |a - b|$

答: (2)

50、任意一个具有 2 个或以上元的半群, 它()。

(1) 不可能是群 (2) 不一定是群

(3) 一定是群 (4) 是交换群

答: (1)

51、6 阶有限群的任何子群一定不是 ()。

(1) 2 阶 (2) 3 阶 (3) 4 阶 (4) 6 阶

答: (3)

(半群与群部分)

19、求循环群 $C_{12} = \{e, a, a^2, \dots, a^{11}\}$ 中 $H = \{e, a^4, a^8\}$ 的所有右陪集。

解:

因为 $|C_{12}|=12$, $|H|=3$, 所以 H 的不同右陪集有 4 个: $H, \{a, a^5, a^9\}, \{a^2, a^6, a^{10}\}, \{a^3, a^7, a^{11}\}$ 。

20、求下列置换的运算:

解:

$$(1) \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$(2) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}^2$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

21、试求出 8 阶循环群的所有生成元和所有子群。

解:

设 G 是 8 阶循环群, a 是它的生成元。则 $G = \{e, a, a^2, \dots, a^7\}$ 。由于 a^k 是 G 的生成元的充分必要条件是 k 与 8 互素, 故 a, a^3, a^5, a^7 是 G 的所有生成元。

因为循环群的子群也是循环群, 且子群的阶数是 G 的阶数的因子, 故 G 的子群只能是 1 阶的、2 阶的、4 阶的或 8 阶的。因为 $|e|=1, |a|=|a^3|=|a^5|=8, |a^2|=|a^6|=4, |a^4|=2$, 且 G 的子群的生成元是该子群中 a 的最小正幂, 故 G 的所有子群除两个平凡子群外, 还有 $\{e, a^4\}, \{e, a^2, a^4, a^6\}$ 。

22、 I 上的二元运算 $*$ 定义为: $\forall a, b \in I, a*b = a+b-2$ 。试问 $\langle I, * \rangle$ 是循环群吗? 解:

$\langle I, * \rangle$ 是循环群。因为 $\langle I, * \rangle$ 是无限阶的循环群, 则它只有两个生成元。1 和 3 是它的两个生成元。因为 $a^n = na - 2(n-1)$, 故 $1^n = n - 2(n-1) = 2 - n$ 。从而对任一个 $k \in I, k = 2 - (2-k) = 1^{2-k}$, 故 1 是 $\langle I, * \rangle$ 的生成元。又因为 1 和 3 关于 $*$ 互为逆元, 故 3 也是 $\langle I, * \rangle$ 的生成元。

23、设 $\langle G, \cdot \rangle$ 是群, $a \in G$ 。令 $H = \{x \in G \mid a \cdot x = x \cdot a\}$ 。试证: H 是 G 的子群。

证明:

$\forall c, d \in H$, 则对 $\forall c, d \in HK, c \cdot a = a \cdot c, d \cdot a = a \cdot d$ 。故 $(c \cdot d) \cdot a = c \cdot (d \cdot a) = c \cdot (a \cdot d) = (c \cdot a) \cdot d = (a \cdot c) \cdot d = a \cdot (c \cdot d)$ 。从而 $c \cdot d \in H$ 。

由于 $c \cdot a = a \cdot c$, 且 $\cdot$ 满足消去律, 所以 $a \cdot c^{-1} = c^{-1} \cdot a$ 。故 $c^{-1} \in H$ 。

从而 H 是 G 的子群。

24、证明: 偶数阶群中阶为 2 的元素的个数一定是奇数。

证明:

设 $\langle G, \cdot \rangle$ 是偶数阶群, 则由于群的元素中阶为 1 的只有一个单位元, 阶大于 2 的元素是偶数个, 剩下的元素中都是阶为 2 的元素。故偶数阶群中阶为 2 的元素一定是奇数个。

25、证明: 有限群中阶大于 2 的元素的个数一定是偶数。

证明:

设 $\langle G, \cdot \rangle$ 是有限群, 则 $\forall a \in G$, 有 $|a|=|a^{-1}|$ 。且当 a 阶大于 2 时, $a \neq a^{-1}$ 。故阶数大于 2 的元素成对出现, 从而其个数必为偶数。

26、试求 $\langle \mathbb{N}_6, +_6 \rangle$ 中每个元素的阶。

解:

0 是 $\langle \mathbb{N}_6, +_6 \rangle$ 中关于 $+_6$ 的单位元。则 $|0|=1$; $|1|=|5|=6$, $|2|=|4|=3$, $|3|=2$ 。

27、设 $\langle G, \cdot \rangle$ 是群, $a, b \in G$, $a \neq e$, 且 $a^4 \cdot b = b \cdot a^5$ 。试证 $a \cdot b \neq b \cdot a$ 。

证明:

用反证法证明。

假设 $a \cdot b = b \cdot a$ 。则 $a^4 \cdot b = a^3 \cdot (a \cdot b) = a^3 \cdot (b \cdot a) = (a^5 \cdot b) \cdot a$

$$= (a^2 \cdot (a \cdot b)) \cdot a = (a^2 \cdot (b \cdot a)) \cdot a = ((a^2 \cdot b) \cdot a) \cdot a = (a \cdot (a \cdot b)) \cdot (a \cdot a)$$

$$= (a \cdot (b \cdot a)) \cdot a^2 = ((a \cdot b) \cdot a) \cdot a^2 = ((b \cdot a) \cdot a) \cdot a^2 = (b \cdot a^2) \cdot a^2 \\ = b \cdot (a^2 \cdot a^2) = b \cdot a^4。$$

因为 $a^4 \cdot b = b \cdot a^5$, 所以 $b \cdot a^5 = b \cdot a^4$ 。由消去律得, $a=e$ 。

这与已知矛盾。

28、 I 上的二元运算 $*$ 定义为: $\forall a, b \in I$, $a*b=a+b-2$ 。试证: $\langle I, * \rangle$ 为群。

证明:

$$(1) \forall a, b, c \in I, (a*b)*c = (a*b)+c-2 = (a+b-2)+c-2 = a+b+c-4, a*(b*c)$$

$$= a+(b*c)-2 = a+(b+c-2)-2 = a+b+c-4。故 (a*b)*c = a*(b*c), 从而*满足结合律。$$

$$(2) 记 e=2。对 \forall a \in I, a*2=a+2-2=a=2+a-2=2*a。故 e=2 是 I 关于运算*的单位元。$$

$$(3) 对 \forall a \in I, 因为 a*(4-a)=a+4-a-2=2=e=4-a+a-2=(4-a)*a。故 4-a 是 a 关于运算*的逆元。$$

综上所述, $\langle I, * \rangle$ 为群。

29、设 $\langle S, \cdot \rangle$ 为半群, $a \in S$ 。令 $S_a = \{a^i \mid i \in I_+\}$ 。试证 $\langle S_a, \cdot \rangle$ 是 $\langle S, \cdot \rangle$ 的子半群。

证明:

$\forall b, c \in S_a$, 则存在 $k, l \in I_+$, 使得 $b=a^k, c=a^l$ 。从而 $b \cdot c = a^k \cdot a^l = a^{k+l}$ 。因为 $k+l \in I_+$, 所以 $b \cdot c \in S_a$, 即 S_a 关于运算 $\cdot$ 封闭。故 $\langle S_a, \cdot \rangle$ 是 $\langle S, \cdot \rangle$ 的子半群。

30、单位元有惟一逆元。

证明:

设 $\langle G, * \rangle$ 是一个群, e 是关于运算 $*$ 的单位元。

若 e_1, e_2 都是 e 的逆元, 即 $e_1*e=e$ 且 $e_2*e=e$ 。

因为 e 是关于运算 $*$ 的单位元, 所以 $e_1=e_1*e=e=e_2*e=e_2$ 。

即单位元有惟一逆元。

31、设 e 和 0 是关于 A 上二元运算 $*$ 的单位元和零元, 如果 $|A|>1$, 则 $e \neq 0$ 。

证明:

用反证法证明。假设 $e=0$ 。

对 A 的任一元素 a , 因为 e 和 0 是 A 上关于二元运算 $*$ 的单位元和零元, 则 $a=a*e=a*0=0$ 。即 A 的所有元素都等于 0 , 这与已知条件 $|A|>1$ 矛盾。

从而假设错误。即 $e \neq 0$ 。

32、证明在元素不少于两个的群中不存在零元。

证明: (用反证法证明)

设在素不少于两个的群 $\langle G, * \rangle$ 中存在零元 θ 。对 $\forall a \in G$, 由零元的定义有 $a*\theta=\theta$ 。

$\therefore \langle G, * \rangle$ 是群, $\therefore$ 关于 $*$ 消去律成立。 $\therefore a=e$ 。即 G 中只有一个元素, 这与 $|G| \geq 2$ 矛盾。故在元素不少于两个的群中不存在零元。

33、证明在一个群中单位元是惟一的。

证明:

设 e_1, e_2 都是群 $\langle G, * \rangle$ 的单位元。 则 $e_1=e_1*e_2=e_2$ 。

所以单位元是惟一的。

34、设 a 是一个群 $\langle G, * \rangle$ 的生成元, 则 a^{-1} 也是它的生成元。

证明:

$\forall x \in G$, 因为 a 是 $\langle G, * \rangle$ 的生成元, 所以存在整数 k , 使得 $x=a^k$ 。

故 $x=((a^k)^{-1})^{-1}=((a^{-1})^k)^{-1}=(a^{-1})^{-k}$ 。从而 a^{-1} 也是 $\langle G, * \rangle$ 的生成元。

35、在一个偶数阶群中一定存在一个 2 阶元素。

证明:

群中的每一个元素的阶均不为 0 且单位元是其中惟一的阶为 1 的元素。因为任一阶大于 2 的元素和它的逆元的阶相等。且当一个元素的阶大于 2 时, 其逆元和它本身不相等。故阶大于 2 的元素是成对的。从而阶为 1 的元素与阶大于 2 的元素个数之和是奇数。

因为该群的阶是偶数, 从而它一定有阶为 2 的元素。

36、代数系统 $\langle G, * \rangle$ 是一个群, 则 G 除单位元以外无其它等幂元。

证明:

设 e 是该群的单位元。若 a 是 $\langle G, * \rangle$ 的等幂元, 即 $a*a=a$ 。

因为 $a*e=a$, 所以 $a*a=a*e$ 。由于运算 $*$ 满足消去律, 所以 $a=e$ 。

即 G 除单位元以外无其它等幂元。

37、设 $\langle G, * \rangle$ 是一个群, 则对于 $a, b \in G$, 必有唯一的 $x \in G$, 使得 $a*x=b$ 。

证明:

因为 $a^{-1}*b \in G$, 且 $a*(a^{-1}*b)=(a*a^{-1})*b=e*b=b$, 所以对于 $a, b \in G$, 必有 $x \in G$, 使得 $a*x=b$ 。

若 x_1, x_2 都满足要求。即 $a*x_1=b$ 且 $a*x_2=b$ 。故 $a*x_1=a*x_2$ 。

由于 $*$ 满足消去律, 故 $x_1=x_2$ 。

从而对于 $a, b \in G$, 必有唯一的 $x \in G$, 使得 $a*x=b$ 。

38、设半群 $\langle S, \cdot \rangle$ 中消去律成立, 则 $\langle S, \cdot \rangle$ 是可交换半群当且仅当 $\forall a, b \in S, (a \cdot b)^2 = a^2 \cdot b^2$ 。

证明:

$$\Rightarrow \forall a, b \in S, (a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = ((a \cdot b) \cdot a) \cdot b \\ = (a \cdot (a \cdot b)) \cdot b = ((a \cdot a) \cdot b) \cdot b = (a \cdot a) \cdot (b \cdot b) = a^2 \cdot b^2;$$

$$\Leftarrow \forall a, b \in S, \text{因为 } (a \cdot b)^2 = a^2 \cdot b^2, \text{所以 } (a \cdot b) \cdot (a \cdot b) = (a \cdot a) \cdot (b \cdot b). \text{故 } a \cdot ((b \cdot a) \cdot b) = a \cdot (a \cdot (b \cdot b)).$$

由于 $\cdot$ 满足消去律, 所以 $(b \cdot a) \cdot b = a \cdot (b \cdot b)$, 即 $(b \cdot a) \cdot b = (a \cdot b) \cdot b$. 从而 $a \cdot b = b \cdot a$. 故 $\cdot$ 满足交换律。

39、设群 $\langle G, * \rangle$ 除单位元外每个元素的阶均为 2, 则 $\langle G, * \rangle$ 是交换群。

证明:

对任一 $a \in G$, 由已知可得 $a * a = e$, 即 $a^{-1} = a$.

对任一 $a, b \in G$, 因为 $a * b = (a * b)^{-1} = b^{-1} * a^{-1} = b * a$, 所以运算 $*$ 满足交换律。

从而 $\langle G, * \rangle$ 是交换群。

40、设 $*$ 是集合 A 上可结合的二元运算, 且 $\forall a, b \in A$, 若 $a * b = b * a$, 则 $a = b$. 试证明:

(1) $\forall a \in A, a * a = a$, 即 a 是等幂元;

(2) $\forall a, b \in A, a * b * a = a$;

(3) $\forall a, b, c \in A, a * b * c = a * c$.

证明:

(1) $\forall a \in A$, 记 $b = a * a$. 因为 $*$ 是可结合的, 故有 $b * a = (a * a) * a = a * (a * a) = a * b$. 由已知条件可得 $a = a * a$.

(2) $\forall a, b \in A$, 因为由 (1), $a * (a * b * a) = (a * a) * (b * a) = a * (b * a)$,

$$(a * b * a) * a = (a * b) * (a * a) = (a * b) * a = a * (b * a).$$

故 $a * (a * b * a) = (a * b * a) * a$, 从而 $a * b * a = a$.

(3) $\forall a, b, c \in A, (a * b * c) * (a * c) = ((a * b * c) * a) * c = (a * (b * c) * a) * c$

且 $(a * c) * (a * b * c) = a * (c * (a * b * c)) = a * (c * (a * b) * c)$.

由 (2) 可知 $a * (b * c) * a = a$ 且 $c * (a * b) * c = c$,

$$\text{故 } (a * b * c) * (a * c) = (a * (b * c) * a) * c = a * c$$

$$\text{且 } (a * c) * (a * b * c) = a * (c * (a * b) * c) = a * c,$$

$$\text{即 } (a * b * c) * (a * c) = (a * c) * (a * b * c).$$

从而由已知条件知, $a * b * c = a * c$.

41、设 $\langle G, \cdot \rangle$ 是群, 作 $f: G \rightarrow G, a \mapsto a^{-1}$. 证明: f 是 G 的自同构 $\Leftrightarrow G$ 是交换群。

证明:

$$\Rightarrow \text{设 } f \text{ 是 } G \text{ 的自同构. 对 } \forall a, b \in G, a \cdot b = (b^{-1} \cdot a^{-1})^{-1} = (f(b) \cdot f(a))^{-1} = (f(b \cdot a))^{-1} = ((b \cdot a)^{-1})^{-1} = b \cdot a.$$

故运算 $\cdot$ 满足交换律, 即 G 是可交换群。

$$\Leftarrow \text{因为当 } a \neq b \text{ 时, } a^{-1} \neq b^{-1}, \text{ 即 } f(a) \neq f(b), \text{ 故 } f \text{ 是 } G \text{ 到 } G \text{ 中的一个单一函数. 又对 } \forall a \in G, \text{ 有 } f(a^{-1}) = (a^{-1})^{-1} = a.$$

故 f 是 G 到 G 上的满函数. 从而 f 是 G 到 G 上的自同构。

对 $\forall a, b \in G$, 因为 G 是可交换群, 故 $f(a \cdot b) = (a \cdot b)^{-1} = (b \cdot a)^{-1} = a^{-1} \cdot b^{-1} = f(a) \cdot f(b)$. 故 f 满足同态方程。

从而 f 是 G 的自同构。

42、若群 $\langle G, * \rangle$ 的子群 $\langle H, * \rangle$ 满足 $|G| = 2|H|$, 则 $\langle H, * \rangle$ 一定是群 $\langle G, * \rangle$ 的正规子群。

证明:

由已知可知, G 关于 H 有两个不同的左陪集 H, H_1 和两个不同的右陪集 H, H_2 。因为 $H \cap H_1 = \Phi$ 且 $H \cup H_1 = G$, $H \cap H_2 = \Phi$ 且 $H \cup H_2 = G$, 故 $H_1 = G - H = H_2$ 。

对 $\forall a \in G$, 若 $a \in H$, 则 $aH = H, Ha = H$ 。否则因为 $a \in G - H$, 故 $aH \neq H, Ha \neq H$ 。从而 $aH = Ha = G - H$ 。故 H 是 G 的不变子群。

43、设 H 和 K 都是 G 的不变子群。证明: $H \cap K$ 也是 G 的不变子群。

证明:

因为 H 和 K 都是 G 的不变子群, 所以 $H \cap K$ 是 G 的子群。对 $\forall a \in G, h \in H \cap K$, 有 $a \cdot h \cdot a^{-1} \in a \cdot H \cdot a^{-1}, h \cdot a^{-1} \in a \cdot K \cdot a^{-1}$ 。因为 H 和 K 都是 G 的不变子群, 所以 $a \cdot h \cdot a^{-1} \in H$ 且 $a \cdot h \cdot a^{-1} \in K$ 。从而 $a \cdot h \cdot a^{-1} \in H \cap K$ 。故 $H \cap K$ 是 G 的不变子群。

44、设群 G 的中心为 $C(G) = \{a \in G \mid \forall x \in G, a \cdot x = x \cdot a\}$ 。证明 $C(G)$ 是 G 的不变子群。

证明:

先证 $C(G)$ 是 G 的子群。

$\forall a, b \in C(G)$, 对 $\forall x \in G$, 有 $a \cdot x = x \cdot a, b \cdot x = x \cdot b$ 。故 $(a \cdot b) \cdot x = a \cdot (b \cdot x) = a \cdot (x \cdot b) = (a \cdot x) \cdot b = (x \cdot a) \cdot b = x \cdot (a \cdot b)$, $a^{-1} \cdot x = x \cdot a^{-1}$ 。从而 $a \cdot b, a^{-1} \in C(G)$ 。故 $C(G)$ 是 G 的子群。

再证 $C(G)$ 是 G 的不变子群。

对 $\forall a \in G, \forall h \in C(G)$, 记 $b = a \cdot h \cdot a^{-1}$ 。下证 $b \in C(G)$ 。因为 $h \in C(G)$, 所以 $b = (a \cdot h) \cdot a^{-1} = (h \cdot a) \cdot a^{-1} = h \cdot (a \cdot a^{-1}) = h \in C(G)$ 。

故 $C(G)$ 是 G 的不变子群。

45、设 $\langle G, \cdot \rangle$ 是没有非平凡子群的有限群。试证: G 是平凡群或质数阶的循环群。

证明:

若 G 是平凡群, 则结论显然成立。

否则设 $\langle G, \cdot \rangle$ 的阶为 n 。任取 $a \in G$ 且 $a \neq e$, 记 $H = \langle a \rangle$ (由 a 生成的 G 的子群)。显然 $H \neq \{e\}$, 且 G 没有非平凡子群, 故 $H = G$ 。从而 G 一定是循环群, 且 a 是 G 的生成元。

若 n 是合数, 则存在大于 1 的整数 k, m , 使得 $n = mk$ 。记 $H = \{e, a^k, (a^k)^2, \dots, (a^k)^{m-1}\}$, 易证 H 是 G 的子群, 但 $1 < |H| = m < n$, 故 H 是 G 的非平凡子群。这与已知矛盾。从而 n 是质数。

故 G 是质数阶的循环群。

综上所述, G 是平凡群或质数阶的循环群。

46、设 H 和 K 都是 G 的有限子群, 且 $|H|$ 与 $|K|$ 互质。试证: $H \cap K = \{e\}$ 。

证明:

用反证法证明。

若 $H \cap K \neq \{e\}$ 。则 $H \cap K$ 是一个元素个数大于 1 的有限集。

先证 $H \cap K$ 也是 G 的子群, 从而也是 H 和 K 的子群。

$\forall a, b \in H \cap K$, 则 $a, b \in H$ 且 $a, b \in K$ 。因为 H 和 K 都是 G 的子群, 故 $a \cdot b, a^{-1} \in H$ 且 $a \cdot b, a^{-1} \in K$ 。从而 $a \cdot b \in H \cap K, a^{-1} \in H \cap K$ 。故 $H \cap K$ 是 G 的子群, 从而也是 H 和 K 的子群。

由拉格朗日定理可知, $|H \cap K|$ 是 $|H|$ 和 $|K|$ 的因子, 这与已知矛盾。

47、素数阶循环群的每个非单位元都是生成元。

证明：

设 $\langle G, * \rangle$ 是 p 阶循环群， p 是素数。

对 G 中任一非单位元 a 。设 a 的阶为 k ，则 $k \neq 1$ 。

由拉格朗日定理， k 是 p 的正因子。因为 p 是素数，故 $k=p$ 。即 a 的阶就是 p ，即群 G 的阶。故 a 是 G 的生成元。

48、若 $\langle S, \bullet \rangle$ 是可交换独异点， T 为 S 中所有等幂元的集合，则 $\langle T, \bullet \rangle$ 是 $\langle S, \bullet \rangle$ 的子独异点。

证明：

$\because e \bullet e = e, \therefore e \in T$ ，即 T 是 S 的非空子集。

$\forall a, b \in T, \because \langle S, \bullet \rangle$ 是可交换独异点，

$\therefore (a \bullet b) \bullet (a \bullet b) = ((a \bullet b) \bullet a) \bullet b$

$= (a \bullet (b \bullet a)) \bullet b = (a \bullet (a \bullet b)) \bullet b$

$= ((a \bullet a) \bullet b) \bullet b = (a \bullet a) \bullet (b \bullet b)$

$= a \bullet b$ ，即 $a \bullet b \in T$ 。

故 $\langle T, \bullet \rangle$ 是 $\langle S, \bullet \rangle$ 的子独异点。

49、设 $\langle G, \bullet \rangle$ 是群，且 $a \in G$ 的阶为 n ， $k \in I$ ，则 $|a^k| = \frac{n}{(k, n)}$ ，其中 (k, n) 为 k 和 n 的最大公因子。

证明：

记 $p = \frac{n}{(k, n)}, q = \frac{k}{(k, n)}, |a^k| = m$ 。由 n 和 p 的定义，显然有 $(a^k)^p = e$ 。故 $m \leq p$ 且 $m|p$ 。

又由于 $a^{km} = e$ ，所以由定理5.2.5知， $n|km$ 。即 $p|qm$ 。但 p 和 q 互质，故 $p|m$ 。

由于 p 和 m 都是正整数，所以 $p=m$ 。即 $|a^k| = \frac{n}{(k, n)}$ 。

50、设 $\langle G, \bullet \rangle$ 是有限群， $|G|=n$ ，则 $\forall a \in G, |a| \leq n$ 。

证明：

$\forall a \in G$ ，由封闭性及 $|G|=n$ 可知 $a, a^2, \dots, a^n, a^{n+1}$ 中必有相同的元素，不妨设为 $a^k = a^m, k < m$ 。由消去律得 $a^{m-k} = e$ 。从而 $|a| \leq m-k \leq n$ 。

51、设 $G = \langle a \rangle$ ，若 G 为无限群，则 G 只有两个生成元 a 和 a^{-1} ；

证明：

$\forall b \in G = \langle a \rangle$ ，则 $\exists n \in I$ ，使 $b = a^n$ 。故 $b = (a^{-n})^{-1} = (a^{-1})^{-n}$ ，从而 a^{-1} 也是 G 的生成元。

若 c 是 G 的生成元，则 $\exists k, m \in I$ ，分别满足 $c = a^k$ 和 $a = c^m$ 。从而 $c = (c^m)^k = c^{mk}$ 。若 $km \neq 1$ ，则由消去律可知 c 的阶是有限的，这与 $|G|$ 无限矛盾。从而 $km=1$ ，即 $k=1, m=1$ 或 $k=-1, m=-1$ 。故 $c=a$ 或 $c=a^{-1}$ 。

从而 G 只有两个生成元 a 和 a^{-1} 。

52、设 $G = \langle a \rangle$ ， $\{e\} \neq H \leq G$ ， a^m 是 H 中 a 的最小正幂，则

(1) $H = \langle a^m \rangle$ ；

(2) 若 G 为无限群，则 H 也是无限群；

证明:

(1) $\forall b \in H, \exists k \in \mathbb{I}$, 使得 $b = a^k$ 。令 $k = mq + r, 0 \leq r < m$ 。

则 $a^r = a^{k-mq} = a^k \bullet a^{-mq} = b \bullet (a^m)^{-q}$ 。

因为 $b, a^m \in H$, 且 $H \leq G$, 所以 $a^r \in H$ 。

由于 $0 \leq r < m$, 且 a^m 是 H 中 a 的最小正幂, 故 $r=0$, 即 $k=mq$ 。

从而 $b = (a^m)^q$ 。故 a^m 是 H 的生成元。

(2) 因为 $\{e\} \neq H$, 故 H 的生成元为 a^m ($m \neq 0$)。因为 G 是无限群, 所以 a 的阶是无限的, 从而 a^m 的阶也是无限的, 故 H 也是无限群。

53、设 $G = \langle a \rangle, |G| = n$, 则对于 n 的每一正因子 d , 有且仅有一个 d 阶子群。因此 n 阶循环群的子群的个数恰为 n 的正因子数。

证明:

$\Rightarrow$ 对 n 的每一正因子 d , 令 $k = \frac{n}{d}, b = a^k, H = \{e, b, b^2, \dots, b^{d-1}\}$ 。

因为 $|a| = n$, 所以 $b^d = (a^k)^d = a^{kd} = a^n = e$ 且 $|b| = d$ 。

从而 H 中的元素是两两不同的, 易证 $H \leq G$ 。

故 $|H| = d$ 。所以是 G 的一个 d 阶子群。

设 H_1 是 G 的任一 d 阶子群。则由定理 5.4.4 知, $H_1 = \langle a^m \rangle$, 其中 a^m 是 H_1 中 a 的最小正幂, 且 $|H| = \frac{n}{m}$ 。

因为 $|H| = d$, 所以 $m = \frac{n}{d} = k$, 即 $H = H_1$ 。从而 H 是 G 的惟一 d 阶子群。

$\Leftarrow$ 设 H 是 G 的惟一的 d 阶子群。若 $d=1$, 则结论显然成立。否则 $H = \langle a^m \rangle$, 其中 a^m 是 H 中 a 的最小正幂。

由定理 5.4.4 知, $d = \frac{n}{m}$ 。故 d 是 n 的一个正因子。

54、设 h 是从群 $\langle G_1, * \rangle$ 到 $\langle G_2, \bullet \rangle$ 的群同态, G_1 和 G_2 的单位元分别为 e_1 和 e_2 , 则

(1) $h(e_1) = e_2$;

(2) $\forall a \in G_1, h(a^{-1}) = h(a)^{-1}$;

(3) 若 $H \leq G_1$, 则 $h(H) \leq G_2$;

(4) 若 h 为单一同态, 则 $\forall a \in G_1, |h(a)| = |a|$ 。

证明:

(1) 因为 $h(e_1) \bullet h(e_1) = h(e_1 \bullet e_1) = h(e_1) = e_2 \bullet h(e_1)$, 所以 $h(e_1) = e_2$ 。

(2) $\forall a \in G_1, h(a) \bullet h(a^{-1}) = h(a \bullet a^{-1}) = h(e_1) = e_2$,

$h(a^{-1}) \bullet h(a) = h(a^{-1} \bullet a) = h(e_1) = e_2$, 故 $h(a^{-1}) = h(a)^{-1}$ 。

(3) $\forall c, d \in h(H), \exists a, b \in H$, 使得 $c = h(a), d = h(b)$ 。故 $c \bullet d = h(a) \bullet h(b)$

$= h(a * b)$ 。因为 $H \leq G_1$, 所以 $a * b \in H$, 故 $c \bullet d \in h(H)$ 。又 $c^{-1} = (h(a))^{-1} = h(a^{-1})$ 且 $a^{-1} \in H$, 故 $c^{-1} \in h(H)$ 。

由定理 5.3.2 知 $h(H) \leq G_2$ 。

(4) 若 $|a| = n$, 则 $a^n = e_1$ 。故 $(h(a))^n = h(a^n) = h(e_1) = e_2$ 。从而 $h(a)$ 的阶也有限, 且 $|h(a)| \leq n$ 。

设 $|h(a)|=m$, 则 $h(a^m) = (h(a))^m = h(e_1) = e_2$ 。因为 h 是单一同态, 所以 $a^m = e_1$ 。即 $|a| \leq m$ 。
故 $|h(a)| = |a|$ 。

若 a 的阶是无限的, 则类似于上述证明过程可以得出, $h(a)$ 的阶也是无限的。

故结论成立。

55、有限群 G 的每个元素的阶均能整除 G 的阶。

证明:

设 $|G|=n$, $\forall a \in G$, 则 $|a|=m$ 。令 $H = \{e, a, a^2, \dots, a^{m-1}\}$ 。

则 H 是 G 的子群且 $|H|=m$ 。由 Lagrange 定理知 $|H|$ 能整除 $|G|$, 故 a 的阶能整除 G 的阶。

56、证明: 在同构意义下, 只有两个四阶群, 且都是循环群。

证明:

在 4 阶群 G 中, 由 Lagrange 定理知, G 中的元素的阶只能是 1, 2 或 4。阶为 1 的元素恰有一个, 就是单位元 e 。

若 G 有一个 4 阶元素, 不妨设为 a , 则 $G = \langle a \rangle$, 即 G 是循环群, 从而是可交换群。

若 G 没有 4 阶元素, 则除单位元 e 外, G 的其余 3 个阶均为 2。不妨记为 a, b, c 。因为 a, b, c 的阶均为 2, 故 $a^{-1}=a, b^{-1}=b, c^{-1}=c$ 。从而 $a \bullet b \neq a, a \bullet b \neq b, a \bullet b \neq e$, 故 $a \bullet b = c$ 。同理可得 $a \bullet c = c \bullet a = b, c \bullet b = b \bullet c = a, b \bullet a = c$ 。

57、在一个群 $\langle G, * \rangle$ 中, 若 G 中的元素 a 的阶是 k , 即 $|a|=k$, 则 a^{-1} 的阶也是 k 。

证明:

因为 $|a|=k$, 所以 $a^k = e$ 。即 $(a^{-1})^k = (a^k)^{-1} = e$ 。

从而 a^{-1} 的阶是有限的, 且 $|a^{-1}| \leq k$ 。

同理可证, a 的阶小于等于 $|a^{-1}|$ 。

故 a^{-1} 的阶也是 k 。

58、在一个群 $\langle G, * \rangle$ 中, 若 A 和 B 都是 G 的子群。若 $A \cup B = G$, 则 $A=G$ 或 $B=G$ 。

证明:

用反证法证明。

若 $A \neq G$ 且 $B \neq G$, 则有 $a \in A, a \notin B$ 且 $b \in B, b \notin A$ 。因为 A, B 都是 G 的子群, 故 $a, b \in G$, 从而 $a*b \in G$ 。

因为 $a \in A$, 所以 $a^{-1} \in A$ 。若 $a*b \in A$, 则 $b = a^{-1} * (a*b) \in A$, 这与 $a \notin B$ 矛盾。从而 $a*b \notin A$ 。

同理可证 $a*b \notin B$ 。

综合可得 $a*b \notin A \cup B = G$, 这与已知矛盾。从而假设错误, 得证 $A=G$ 或 $B=G$ 。

59、设 e 是奇数阶交换群 $\langle G, * \rangle$ 的单位元, 则 G 的所有元素之积为 e 。

证明:

设 $G = \langle \{e, a_1, a_2, \dots, a_{2n}\}, * \rangle$, n 为正整数。

因为 G 的阶数为奇数 $2n+1$, 所以由拉格朗日定理知 G 中不存在 2 阶元素, 即除了单位元 e 以外, G 的所有元素的阶都大于 2。故对 G 中的任一非单位元 a , 它的逆元 a^{-1} 不是它本身, 且 G 中不同的元素有不同的逆元。

由此可见, G 中的 $2n$ 个非单位元构成互为逆元的 n 对元素。因为 G 是交换群, 故 G 的所有元素之积可变为

成单位元和 n 对互为逆元的元素之积的积, 从而结果为 e 。

60、设 $S=Q \times Q$, Q 为有理数集合, $*$ 为 S 上的二元运算: 对任意 $(a, b), (c, d) \in S$, 有

$$(a, b) * (c, d) = (ac, ad+b),$$

求出 S 关于二元运算 $*$ 的单位元, 以及当 $a \neq 0$ 时, (a, b) 关于 $*$ 的逆元。

解:

设 S 关于 $*$ 的单位元为 (a, b) 。根据 $*$ 和单位元的定义, 对 $\forall (x, y) \in S$, 有

$$(a, b) * (x, y) = (ax, ay+b) = (x, y), \quad (x, y) * (a, b) = (ax, xb+y) = (x, y)。$$

即 $ax=x, ay+b=y, xb+y=y$ 对 $\forall x, y \in Q$ 都成立。解得 $a=1, b=0$ 。

所以 S 关于 $*$ 的单位元为 $(1, 0)$ 。

当 $a \neq 0$ 时, 设 (a, b) 关于 $*$ 的逆元为 (c, d) 。根据逆元的定义, 有

$$(a, b) * (c, d) = (ac, ad+b) = (1, 0)$$

$$(c, d) * (a, b) = (ac, cb+d) = (1, 0)$$

即 $ac=1, ad+b=0, cb+d=0$ 。解得 $c=\frac{1}{a}, d=-\frac{b}{a}$ 。

所以 (a, b) 关于 $*$ 的逆元为 $(\frac{1}{a}, -\frac{b}{a})$ 。

61、设 $\langle G, * \rangle$ 是一个群, H, K 是其子群。定义 G 上的关系 R : 对任意 $a, b \in G$, $aRb \Leftrightarrow$ 存在 $h \in H, k \in K$, 使得 $b=h*a*k$, 则 R 是 G 上的等价关系。

证明:

$\forall a \in G$, 因为 H, K 是 G 的子群, 所以 $e \in H$ 且 $e \in K$ 。令 $h=k=e$, 则 $a=e*a*a=h*e*k$, 从而 aRa 。即 R 是自反的。

$\forall a, b \in G$, 若 aRb , 则存在 $h \in H, k \in K$, 使得 $b=h*a*k$ 。因为 H, K 是 G 的子群, 所以 $h^{-1} \in H$ 且 $k^{-1} \in K$ 。故 $a=h^{-1}*a*k^{-1}$, 从而 bRa 。即 R 是对称的。

$\forall a, b, c \in G$, 若 aRb, bRc , 则存在 $h, g \in H, k, l \in K$, 使得 $b=h*a*k, c=g*b*l$ 。所以 $c=g*b*l=g*(h*a*k)*l=(g*h)*a*(k*l)$ 。因为 H, K 是 G 的子群, 所以 $g*h \in H$ 且 $k*l \in K$ 。从而 aRc 。即 R 是传递的。

综上所述, R 是 G 上的等价关系。

62、设 H 是 G 的子群, 则下列条件等价:

- (1) H 是 G 的不变子群;
- (2) $\forall a \in G, a \bullet H \bullet a^{-1} \subseteq H$;
- (3) $\forall a \in G, a^{-1} \bullet H \bullet a \subseteq H$;
- (4) $\forall a \in G, \forall h \in G, a \bullet h \bullet a^{-1} \subseteq H$ 。

证明:

(1) $\Rightarrow$ (2) $\forall a \in G$, 则对 $h \in H$, 令 $h_1=a \bullet h \bullet a^{-1}$, 因为 $a \bullet h \in a \bullet H$ 且 $H \bullet a=a \bullet H$, 所以 $\exists h_2 \in H$, 使得 $a \bullet h=h_2 \bullet a$ 。故 $h_1=(h_2 \bullet a) \bullet a^{-1}=h_2 \in H$ 。故 $a \bullet H \bullet a^{-1} \subseteq H$ 。

(2) $\Rightarrow$ (3) $\forall a \in G$, 对 $h \in H$, 令 $h_1=a^{-1} \bullet h \bullet a$, 则 $(h_1)^{-1}=a \bullet h^{-1} \bullet a^{-1}$ 。因为 $h^{-1} \in H$, 所以 $(h_1)^{-1}=a \bullet h^{-1} \bullet a^{-1}$

$\in a \bullet H \bullet a^{-1}$ 。由 (2) 可知 $(h_1)^{-1} \in H$, 从而 $h_1 \in H$ 。故 $a^{-1} \bullet H \bullet a \subseteq H$ 。

(3) $\Rightarrow$ (4) 类似于 (2) $\Rightarrow$ (3) 的证明。

(4) $\Rightarrow$ (1) $\forall a \in G$, 对 $\forall b \in a \bullet H$, 则 $\exists h \in H$, 使得 $b = a \bullet h$ 。故 $b = (a \bullet h) \bullet (a^{-1} \bullet a) = (a \bullet h \bullet a^{-1}) \bullet a$ 。

由于 $a \bullet h \bullet a^{-1} \in H$, 所以 $b \in H \bullet a$ 。即 $a \bullet H \subseteq H \bullet a$ 。

反之对 $\forall b \in H \bullet a$, 则 $\exists h \in H$, 使得 $b = h \bullet a$ 。故 $b = (a \bullet a^{-1}) \bullet (h \bullet a) = a \bullet (a^{-1} \bullet h \bullet a) = a \bullet (a^{-1} \bullet h \bullet (a^{-1})^{-1})$ 。

由于 $a^{-1} \bullet h \bullet (a^{-1})^{-1} \in H$, 所以 $b \in a \bullet H$ 。即 $H \bullet a \subseteq a \bullet H$ 。

即 $H \bullet a = a \bullet H$ 。从而 H 是 G 的不变子群。

63、在半群 $\langle G, * \rangle$ 中, 若对 $\forall a, b \in G$, 方程 $a * x = b$ 和 $y * a = b$ 都有惟一解, 则 $\langle G, * \rangle$ 是一个群。

证明:

任意取定 $a \in G$, 记方程 $a * x = a$ 的惟一解为 e_R 。即 $a * e_R = a$ 。

下证 e_R 为关于运算 $*$ 的右单位元。

对 $\forall b \in G$, 记方程 $y * a = b$ 的惟一解为 y 。

$\because \langle G, * \rangle$ 是半群, $\therefore$ 运算 $*$ 满足结合律。

$\therefore b * e_R = (y * a) * e_R = y * (a * e_R) = y * a = b$ 。

类似地, 记方程 $y * a = a$ 的惟一解为 e_L 。即 $e_L * a = a$ 。

下证 e_L 为关于运算 $*$ 的左单位元。

对 $\forall b \in G$, 记方程 $a * x = b$ 的惟一解为 x 。

$\because \langle G, * \rangle$ 是半群, $\therefore$ 运算 $*$ 满足结合律。

$\therefore e_L * b = e_L * (a * x) = (e_L * a) * x = a * x = b$ 。

从而在半群 $\langle G, * \rangle$ 中, 关于运算 $*$ 存在单位元, 记为 e 。

现证 G 中每个元素关于运算 $*$ 存在逆元。

对 $\forall b \in G$, 记 c 为方程 $b * x = e$ 的惟一解。下证 c 为 b 关于运算的逆元。记 $d = c * b$ 。则 $b * d = (b * c) * b = e * b = b$ 。

$\because b * e = b$, 且方程 $b * x = b$ 有惟一解, $\therefore d = e$ 。

$\therefore b * c = c * b = e$ 。从而 c 为 b 关于运算的逆元。

综上所述, $\langle G, * \rangle$ 是一个群。

64、设 $\langle G, * \rangle$ 是群, H 和 K 都是 G 的子群, 令 $HK = \{h * s \mid s \in K, h \in H\}$, $KH = \{s * h \mid s \in K, h \in H\}$, $\langle HK, * \rangle$, $\langle KH, * \rangle$ 是 G 的子群的充分必要条件是 $HK = KH$ 。

证明:

$\Rightarrow HK$ 是 G 的子群。 $\forall c \in HK$, 则 $c^{-1} \in HK$, 故存在 $a \in H, b \in K$, 使得 $c^{-1} = a \bullet b$ 。因为 $c = (a \bullet b)^{-1} = b^{-1} \bullet a^{-1}$ 。

因为 H 和 K 都是 G 的子群, 所以 $a^{-1} \in H, b^{-1} \in K$, 即 $c \in KH$ 。从而 $HK \subseteq KH$ 。 $\forall c \in KH$, 则存在 $a \in H, b \in K$, 使得 $c = b \bullet a$ 。因为 $c = (a^{-1} \bullet b^{-1})^{-1}$ 。因为 H 和 K 都是 G 的子群, 所以 $a^{-1} \in H, b^{-1} \in K$, 即 $a^{-1} \bullet b^{-1} \in HK$ 。因为 HK 是 G 的子群, 所以 $c = (a^{-1} \bullet b^{-1})^{-1} \in HK$ 。从而 $KH \subseteq HK$ 。

故 $HK = KH$ 。

$\Leftarrow HK = KH$ 。对 $\forall c, d \in HK$, 有 $a_1, a_2 \in H, b_1, b_2 \in K$, 使得 $c = a_1 \bullet b_1, d = a_2 \bullet b_2$ 。则 $c \bullet d = (a_1 \bullet b_1) \bullet (a_2 \bullet b_2) = ((a_1 \bullet b_1) \bullet a_2) \bullet b_2 = (a_1 \bullet (b_1 \bullet a_2)) \bullet b_2$ 。因为 $b_1 \bullet a_2 \in KH = HK$, 所以存在 $a_3 \in H, b_3 \in K$, 使得 $b_1 \bullet a_2 = a_3 \bullet b_3$ 。从而 $c \bullet d = (a_1 \bullet (b_1 \bullet a_2)) \bullet b_2 = (a_1 \bullet (a_3 \bullet b_3)) \bullet b_2 = (a_1 \bullet a_3) \bullet (b_3 \bullet b_2)$ 。因为 H 和 K 都是

G 的子群, 故 $a_1 \cdot a_3 \in H$, $b_3 \cdot b_2 \in K$ 。从而 $c \cdot d \in HK$ 。

又 $c^{-1} = (a_1 \cdot b_1)^{-1} = b_1^{-1} \cdot a_1^{-1}$ 。因为 H 和 K 都是 G 的子群, 故 $a_1^{-1} \in H$, $b_1^{-1} \in K$ 。从而 $c^{-1} \in KH$ 。因为 $HK = KH$, 所以 $c^{-1} \in HK$ 。

综上所述, HK 是 G 的子群。

65、设 H 和 K 都是 G 的不变子群。证明: HK 也是 G 的不变子群。

证明:

先证 HK 是 G 的子群。

对 $\forall a \in HK$, 有 $h \in H, k \in K$, 使得 $a = h \cdot k$ 。因为 $a = h \cdot k = (h \cdot k \cdot h^{-1}) \cdot h$, 且 K 是 G 的不变子群, 所以 $h \cdot k \cdot h^{-1} \in K$ 。故 $a \in KH$ 。从而 $HK \subseteq KH$ 。

同理可证, $KH \subseteq HK$ 。

故 $HK = KH$ 。从而 HK 是 G 的子群。

下证 HK 是 G 的不变子群。

对 $\forall a \in G, b \in HK$, 有 $h \in H, k \in K$, 使得 $b = h \cdot k$ 。故 $a \cdot b \cdot a^{-1} = a \cdot (h \cdot k) \cdot a^{-1} = (a \cdot h \cdot a^{-1}) \cdot (a \cdot k \cdot a^{-1})$ 。因为 H 和 K 都是 G 的不变子群, 所以 $a \cdot h \cdot a^{-1} \in H$ 且 $a \cdot k \cdot a^{-1} \in K$ 。从而 $a \cdot b \cdot a^{-1} \in HK$ 。故 HK 是 G 的不变子群。

66、设 $\langle G, * \rangle$ 为群, $a, b, c \in G$ 。若 $a*b = c*b*a, a*c = c*a, b*c = c*b$, 且 a, b 的阶分别为 m, n , 则 c 的阶整除 m 与 n 的最大公因子 (m, n) 。

证明:

设 c 的阶为 k 。在 $a*b = c*b*a$ 两边同时右乘 b^{n-1} , 再由 $a*b = c*b*a$ 得

$$\begin{aligned} a*b^n &= (c*b*a)*b^{n-1} = (c*b)*(a*b)*b^{n-2} = (c*b)*(c*b*a)*b^{n-2} \\ &= (c*b)^2*a*b^{n-2} = (c*b)^2*(a*b)*b^{n-3} = (c*b)^2*(c*b*a)*b^{n-3} \\ &= (c*b)^3*a*b^{n-3} = \dots = (c*b)^n*a, \end{aligned}$$

再由 $b*c = c*b$ 及 b 的阶为 n 得

$$a = a*b^n = (c*b)^n*a = (c^n*b^n)*a = c^n*a,$$

所以 $c^n = e$ 。故由元素阶的定义有 $k|n$ 。

由 $a*b = c*b*a, a*c = c*a, b*c = c*b$ 得 $a*b = b*a*c$, 两边同时左乘 a^{m-1} , 再由 $a*b = b*a*c$ 得

$$\begin{aligned} a^m*b &= a^{m-1}*(b*a*c) = a^{m-2}*(a*b)*(a*c) = a^{m-2}*(b*a*c)*(a*c) \\ &= a^{m-2}*b*(a*c)^2 = a^{m-3}*(a*b)*(a*c)^2 = a^{m-3}*(b*a*c)*(a*c)^2 \\ &= a^{m-3}*b*(a*c)^3 = \dots = b*(a*c)^m, \end{aligned}$$

再由 $a*c = c*a$ 及 a 的阶为 m 得

$$b = a^m*b = b*(a*c)^m = b*a^m*c^m = b*c^m,$$

所以 $c^m = e$ 。故由元素阶的定义有 $k|m$ 。

由此可见, k 是 m 和 n 的公因子, 从而能整除 m 和 n 的最大公因子 (m, n) 。