3. 设有二元代数 $V=\langle\{a,b,c,d\};\cdot\rangle$，其中运算 · 由右表定义：

(1) 证明 V 是一循环独异点，并列出它的生成元；

(2) 如果 g 是生成元，将 V 的每一元素表示成 g 的幂；

(3) 列出 V 的所有幂等元；

(4) 证明 V 中每一个元素的某次乘方是幂等的.

·	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

4. 证明自然数集 N 对于运算 $x*y=\max\{x,y\}$ 构成一个半群. 它是独异点吗？

(1) 由表可得，V 是封闭的

$(a\cdot b)\cdot c = b\cdot c = d = a\cdot(b\cdot c) = a\cdot d$

$(b\cdot c)\cdot d = d\cdot d = c = b\cdot(c\cdot d) = b\cdot b$

$(a\cdot b)\cdot d = b\cdot d = a = a\cdot(b\cdot d) = a\cdot a$

$(a\cdot c)\cdot d = c\cdot d = b = a\cdot(c\cdot d) = a\cdot b$

$\Rightarrow$ V 是半群

单位元为 a $\Rightarrow$ V是独异点、

$c = b\cdot b$ ，$b = b$

$a = c\cdot c = b\cdot b\cdot b\cdot b$

$d = b\cdot c = b\cdot b\cdot b$

$\Rightarrow$ V 是循环独异点、生成元为 b

(2) $a = g^4$

$b = g$

$c = g^2$

$d = g^3$

(3) 幂等元为 a

(4) $b^4 = a$ 是幂等的

$c^2 = a$ 是幂等的

$a = a$ 是幂等的

$d^4 = d\cdot d\cdot c = d\cdot b = a$ 是幂等的

7. 证明在一个独异点中左可逆元（右可逆远）的集合形成一个子独异点.

左可逆元 a $\Rightarrow \exists\, a^{-1}$，$a^{-1}\cdot a = e$

设独异点 $\langle S,*\rangle$ ，左可逆元构成的集合 $\langle A,*\rangle$

① 显然 $\langle A,*\rangle$ 是可结合的 且 $A\subseteq S$

② 设 $\langle S,*\rangle$ 单位元为 e ，因为 $e\cdot e = e \Rightarrow e\in A$ ，e 也是A的单位元

③ 下面只需证明 A 对运算 $*$ 是封闭的

$\forall\, a,b\in A$， 有 $(b^{-1}*a^{-1})*(a*b) = b^{-1}*e*b = b^{-1}*b = e$

$\Rightarrow$ $a*b\in A$ $\Rightarrow$ A 对 $*$ 是封闭的

对于右可逆元同理可证

$\Rightarrow$ 一个独异点中左可逆元（右可逆元）的集合形成一个子独异点、

9. 试证明一独异点的所有可逆元素的集合，对于该独异点所具有的运算，能够构成群.

可逆元素 a：$\exists\, a^{-1}$，使 $a^{-1}\cdot a = a\cdot a^{-1} = e$

设独异点为 $\langle S;\cdot\rangle$，可逆元素的集合 $\langle A;\cdot\rangle$

① 单位元

设 $\langle S;\cdot\rangle$ 单位元为 e.

$e\cdot e = e \Rightarrow e \in A \Rightarrow e$ 为 $\langle A;\cdot\rangle$ 的单位元

② 结合性

$A \subseteq S$，S 对 $\cdot$ 可结合 $\Rightarrow$ A 对 $\cdot$ 可结合

③ 逆元：

$\forall a \in A$，有逆元 $a^{-1} \in S$，a^{-1} 逆元为 $a \Rightarrow a^{-1} \in A$

$\Rightarrow \forall a \in A$ 均有逆元 $a^{-1} \in A$

④ 封闭性

$\forall a, b \in A$. 有 $a\cdot a^{-1} = a^{-1}\cdot a = e$. $b\cdot b^{-1} = b^{-1}\cdot b = e$

$\Rightarrow (b^{-1}\cdot a^{-1})\cdot(ab) = b^{-1}\cdot e\cdot b = b^{-1}\cdot b = e$

$(ab)\cdot(b^{-1}\cdot a^{-1}) = a\cdot e\cdot a^{-1} = a\cdot a^{-1} = e$

$\Rightarrow$ A 对运算 $\cdot$ 封闭

$\Rightarrow$ 独异点可逆元素的集合对独异点的运算构成群

13. 试证明如果一个群的每一个元素都是它自己的逆远，则该群必是阿贝尔群.

设群 $\langle S;\cdot\rangle$

$\forall a \in S$. 有 $a\cdot a = e$

$\forall a, b \in S$，$a\cdot b = e\cdot a\cdot b\cdot e = b\cdot b\cdot a\cdot b\cdot a\cdot a$

$= b\cdot(b\cdot a\cdot b\cdot a)\cdot a = b\cdot e\cdot a = b\cdot a$

$\Rightarrow$ 该群可交换，是阿贝尔群

17. 试证明在一个有限群里，周期大于 2 的元素的个数一定是偶数.

设周期大于2的元素为 a，用 b^{-1} 代表元素b的逆元

设 $a^r=e$，r为满足式子的最小值 $\Rightarrow r>2$

有 $(a^{-1})^r=(a^r)^{-1}=e^{-1}=e$

若 $a^{-1}=a$，则 $a^2=a\cdot a^{-1}=e$ 与r的最小性矛盾

$\Rightarrow$有限群里周期大于2的元素个数一定是偶数

23. 设 $\langle H_1;*\rangle$ 和 $\langle H_2;*\rangle$ 是群 $\langle G;*\rangle$ 的子群，G 的子集 H_1*H_2 是否能构成 $\langle G;*\rangle$ 的子群？

不一定

考虑G为3个元素的对称群 S_3

$H_1=\{e,(1\ 2)\}$　$H_2=\{e,(1\ 3)\}$

$H_1*H_2=\{e,(1\ 3),(1\ 2),(1\ 3\ 2)\}$

$(1\ 3)*(1\ 2)=(1\ 2\ 3)\notin H_1*H_2$

封闭性不满足

$\Rightarrow H_1*H_2$ 不构成 $\langle G;*\rangle$ 的子群

25. 试证明循环群的子群也是循环群.

设循环群 $\langle S;\cdot\rangle$，生成元为 m

则 $\forall s\in S$，有 $s=m^k$

设循环群子群为 $\langle G;\cdot\rangle$

若 $m\in G$，则 $\langle G;\cdot\rangle$ 为循环群，生成元为m

若 $m\notin G$，若 $\langle G;\cdot\rangle$ 不为循环群，设 $\#G=n$

$G\subseteq S\Rightarrow G=\{m^{k_1},m^{k_2},\cdots m^{k_n}\}$

设 $d=\min\{k_1,k_2,\cdots k_n\}$

$k_i=a_id+b_i$，$i=1,2,\cdots n$，$0\le b_i<d$

$\langle G;\cdot\rangle$ 是群 $\Rightarrow$ 对于 m^d，有逆元 $m^{-d}\in G$

由封闭性

$(m^{-d})^{a_i} \cdot m^{a_i d+b} = m^b \in G$

与 d 的最小性矛盾

$\Rightarrow$ 所有循环群的子群也是循环群

29. 设 $\langle G;*\rangle$ 是一个群，$\langle \tilde{G};*\rangle$ 是 $\langle G;*\rangle$ 的一个子群，定义 G 的子集 H 为

$$H = \{a \mid a*\tilde{G} = \tilde{G}*a\}$$

试证明：(1) $\langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群；

(2) $\langle \tilde{G};*\rangle$ 是 $\langle H;*\rangle$ 的正规子群.

封闭性，结合性，单位元，逆元

(1) 设 G 的单位元为 e

$\Rightarrow e*\tilde{G} = \tilde{G}*e = \tilde{G} \Rightarrow e \in H$

H 为 G 的子集 $\Rightarrow e$ 为 H 的单位元

(2) H 为 G 的子集 $\Rightarrow$ H 对 $*$ 满足结合性

(3) 设 $a, b \in H$，$\tilde{G}$ 为 G 的子集

$a*b*\tilde{G} = a*(b*\tilde{G}) = a*\tilde{G}*b = (a*\tilde{G})*b = \tilde{G}*a*b$

$\Rightarrow$ H 对 $*$ 封闭

(4) 设 $a \in H$，a^{-1} 为 a 在 G 中的逆元

$a*\tilde{G} = \tilde{G}*a \Rightarrow a^{-1}*a*\tilde{G} = a^{-1}*\tilde{G}*a \Rightarrow \tilde{G} = a^{-1}*\tilde{G}*a$

$\Rightarrow \tilde{G}*a^{-1} = a^{-1}*\tilde{G} \Rightarrow a^{-1} \in H$

$\Rightarrow \langle H;*\rangle$ 是群

$H \subseteq G \Rightarrow \langle H;*\rangle$ 是 $\langle G;*\rangle$ 的子群

(2) 设 $g \in \tilde{G}$，由消去律 $g*\tilde{G} = \tilde{G}*g = \tilde{G}$

$\Rightarrow \tilde{G}$ 为 H 的子集 $\Rightarrow \langle \tilde{G};*\rangle$ 为 $\langle H;*\rangle$ 子群

$\forall h \in H$，$h*\tilde{G} = \tilde{G}*h$

$\Rightarrow \langle \tilde{G};*\rangle$ 是 $\langle H;*\rangle$ 正规子群