

1, 试验证

(1) n 阶实正交矩阵的全体 $O_n(R) = \{A \in M_n(R) | A^T A = E\}$

关于矩阵的乘法运算构成群(称为正交群);

(2) n 阶酉矩阵的全体 $U_n(C) = \{A \in M_n(C) | \bar{A}^T A = E\}$

关于矩阵的乘法运算构成群(称为酉群),

其中 A^T 表示矩阵 A 的转置, $\bar{A}$ 表示矩阵 A 的共轭,

证明:

(1) 对属于 $O_n(R)$ 的任意 A, B , 都有 $(AB)^T(AB) = B^T A^T AB = E$, 即 AB 属于 $O_n(R)$

由于矩阵的乘法满足结合律,

从而对属于 $O_n(R)$ 的任意 A, B, C , 都有 $A(BC) = (AB)C$,

在 $O_n(R)$ 中存在单位元 E , 且对属于 $O_n(R)$ 的任意 A ,

存在有属于 $O_n(R)$ 的左逆元 A 使得 $A^T A = E$,

因此, 由群的定义知 $O_n(R)$ 关于矩阵的乘法运算构成群,

(2) 对属于 $U_n(C)$ 的任意 A, B ,

有 $(\bar{AB})^T(AB) = (\bar{A} \bar{B})^T(AB) = \bar{B}^T \bar{A}^T AB = E$, 即 AB 属于 $U_n(C)$,

显然, $U_n(C)$ 中元素关于矩阵的乘法满足结合律, 且在 $U_n(C)$ 中存在单位元 E ,

又对属于 $U_n(C)$ 的任意 A , 都存在有属于 $U_n(C)$ 的左逆元 $\bar{A}^T$, 使得 $\bar{A}^T A = E$,

故 $U_n(C)$ 关于矩阵的乘法运算构成群,

2, 设 $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

试证明 G 关于矩阵的乘法运算构成交换群,

证明: 令 $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, 则 $G = \{E, -E, A, B\}$, $AB = BA = -E$,

显然 G 中元素关于矩阵的乘法运算封闭, 且满足交换律和结合律,

E 为 G 中单位元, A 的逆元为 $-B = A$, B 的逆元为 B ,

因此, G 关于矩阵的乘法运算构成交换群,

3, 设 G 是群, 如果对于 G 中任意一个元素 a 都有 $a^{-1}=a$, 试证明 G 是交换群,

证明: 对属于群 G 的任意 a, b , 有 $a^{-1}=a, b^{-1}=b$, 从而 $ab=a^{-1}b^{-1}=(ba)^{-1}=ba$,
故 G 是交换群,

4, 试证明任意偶数阶有限群 G 必含有不等于 e 的元素 a , 使得 $a^2=e$,

证明: 反证, 若对属于群 G , 且不等于 e 的任意 a , 都有 $a^2 \neq e$,
则 a 与 a^{-1} 成对出现,

又因 $e=e^{-1}$, 从而 $|G|$ 为奇数, 这与 G 是偶数阶有限群矛盾,
故存在不等于 e 的 a 使得 $a^2=e$,

5, 正实数集合 R^+ 关于数的乘法运算是否是群?

非零整数集合 Z^* 关于数的乘法运算是否是群?

解: $\{R^+; \times\}$ 是群, $\{Z^*; \times\}$ 不是群, 因为 Z^* 中除 1 外其他元素都没有逆,

6, 设代数系统 $\{G; \bullet\}$ 满足以下条件:

(1) 运算“ $\bullet$ ”满足结合律: 即对属于群 G 的任意 a, b, c , 都有 $a \bullet (b \bullet c) = (a \bullet b) \bullet c$;

(2) G 中有右单位元: 即对属于群 G 的任意 a , 存在有属于群 G 的 e , 使得 $a \bullet e = a$;

(3) G 中每个元素有右逆元: 即对属于群 G 的任意 a , 存在有属于群 G 的 b ,
使得 $a \bullet b = e$,

试证明 G 关于运算“ $\bullet$ ”是群,

证明: 只需证明右单位元也是左单位元, 右逆元也是左逆元,

(1) 由条件(3), 对属于群 G 的任意 a , 存在有属于群 G 的 b , 使得 $a \bullet b = e$,

同时也存在有属于群 G 的 c , 使得 $b \bullet c = e$,

所以 $ea = e(ae) = eabc = e(ab)c = (ee)c = ec = (ab)c = a(bc) = ae = a$,

(2) 由条件(3), 对于属于群 G 的任意 a , 存在有属于群 G 的 b , 使得 $b \bullet c = e$,

所以 $ba = (ba)e = (ba)(bc) = b(ab)c = bc = e = ab$,

从而 C 关于运算“ $\bullet$ ”是群,

7, 在半群 G 中, 若对属于群 G 的任意 a, b , 方程 $ax=b$ 和 $ya=b$ 在 G 中都有解, 试证明 G 是群,

证明: 只需证明 G 中存在右单位元, G 中任意元素都有右逆元,

设方程 $ax=a$ 的解为 e , 则对属于群 G 的任意 b , 方程 $ya=b$ 有解, 设为 c ,

则有 $be=cae=ca=b$, 即 e 是 G 的右单位元,

对属于群 G 的任意 $b, bx=e$ 有解, 即 b 有右逆元, 因此 G 是群,

8, 设 $G=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{C}, a \neq 0\right\}$

说明 G 关于矩阵的乘法运算是否构成群(这里 $\mathbb{C}$ 表示复数域),

解: 不构成群(无单位元),

9, 试举例说明满足以下条件的代数系统 $\{G; \bullet\}$ 不是群:

(1) 运算“ $\bullet$ ”满足结合律: 即对属于群 G 的任意 a, b, c , 有 $a \bullet (b \bullet c) = (a \bullet b) \bullet c$

(2) G 中有左单位元: 即对属于群 G 的任意 a , 存在有属于群 G 的 e , 有 $e \bullet a = a$

(3) 每个元素有右逆元: 对属于群 G 的任意 a , 存在有属于群 G 的 b , 使得 $a \bullet b = e$

解: 反例: $G=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{C}, a \neq 0\right\}$, 有左单位元 $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$, c 属于 $\mathbb{C}$,

$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 有右逆元为 $\begin{pmatrix} \frac{1}{a} & \frac{c}{a} \\ 0 & 0 \end{pmatrix}$, 但是 $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$ 不是右单位元, c 属于 $\mathbb{C}$,

故 G 不构成群,

10, 设 G 是有限群, 证明 G 中满足 $a^3=e$ 的元素 a 的个数是奇数,

证明: 令 $S=\{x \in G \mid x^3=e\}$, 由于 G 是有限群, 所以 S 为有限集,

又因为 $e^3=e$, 所以 e 属于 S , 从而 S 不是空集,

如果另外有不等于 e 的 x , 使得 $x^3=e$, 则 $(x^{-1})^3=e$,

因 $x \neq e$, 所以 $x \neq x^{-1}$, 这说明 S 中的非单位元总是成对出现,

又因为 $e^{-1}=e$, 所以 G 中使等式 $x^3=e$ 成立的元素 x 的个数是奇数,

习题 1 判断下列代数系统是否为半群、有单位元的半群、群、交换群

- (1) 整数集合关于数的乘法运算；
- (2) 偶数集合关于数的乘法运算；
- (3) 三阶严格上三角形矩阵集合关于矩阵的乘法运算；
- (4) 集合 A 上所有变换集合关于变换的合成运算；
- (5) 正整数集合关于运算 $m \circ n = m^n$ ；
- (6) Z_n 关于剩余类乘法运算；
- (7) 正整数集合关于运算 $m \circ n = m$ ，

解: (1) 有单位元的交换半群，因为 2 没有逆元，所以不是群，

(2) 无单位元的交换半群，所以不是群，

(3) 无单位元的非交换半群，所以不是群，

(4) 有单位元的非交换半群，不是群，

(5) 因为该运算不满足结合律，所以不是半群，

(6) 有单位元的交换半群，但是 $\bar{0}$ 没有逆元，因此不是群，

(7) 无单位元的非交换半群，因此不是群，

习题 2 试证明有理数集合关于运算 $a \circ b = a + b + ab$ 是有单位元的交换半群，

证明: 由 $a \circ b = a + b + ab = b \circ a$

$$(a \circ b) \circ c = (a + b + ab) \circ c = a + b + ab + c + ac + bc + abc$$

$$a \circ (b \circ c) = a \circ (b + c + bc) = a + b + c + bc + ab + ac + abc$$

可知此运算满足交换律和结合律，显然 $0 \circ a = a \circ 0 = a$ ，因此 0 是单位元，

但是 $(-1) \circ b = -1 \neq 0$ ，即 -1 没有逆元，

因此，有理数集合关于运算 $a \circ b = a + b + ab$ 是有单位元的交换半群，但不是群，

习题 3 设 $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}, a \neq 0 \right\}$, 证明 G 关于矩阵的乘法运算是群,

证明: 对属于集合 $\mathbb{R}$ 的任意 a, b , 且 a, b 都不为 0,

$$\text{有 } \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} \in G$$

即 G 关于矩阵的乘法运算是代数系统,

矩阵乘法运算的结合律在 G 中也成立,

二阶单位矩阵是 G 的单位元, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a^{-1} \end{pmatrix}$ 属于 G

因此 G 关于矩阵的乘法运算是群,

习题 4 证明集合 $A = \{2^n \mid n \in \mathbb{Z}\}$ 关于数的乘法运算是交换群,

证明: 显然数的乘法运算是集合 A 的运算, A 的单位元为 $2^0 = 1$, 2^n 的逆元为 2^{-n}

又因数的乘法运算满足结合律和交换律, 故集合 A 关于数的乘法运算是交换群

习题 5 证明代数系统 $\{Z_p^*; \cdot\}$ 是交换群, 其中 p 是素数, $Z_p^* = Z_p - \{\bar{0}\}$,

证明: 对属于 Z_p^* 的任意 $\bar{a}$, 有 $\bar{1}\bar{a} = \bar{a}$, 即 $\bar{1}$ 是 Z_p^* 的左单位元,

因为 $\bar{a}$ 属于 Z_p^* , 所以 a 与 p 互素, 进而存在整数 s, t , 使得 $sa + tp = 1$,

因此 $\bar{s}\bar{a} = \bar{s}\bar{a} + \bar{t}\bar{p} = \overline{sa + tp} = \bar{1}$, 即 $\bar{a}$ 有左逆元,

另外, 代数系统 Z_p^* 上的乘法运算满足结合律和交换律, 因而 $\{Z_p^*; \cdot\}$ 是交换群,

习题 6 在群 $\{Z_7^*; \cdot\}$ 中, 求解方程 $\bar{5}x = \bar{2}, y\bar{2} = \bar{3}$,

解: 先求 $\bar{5}$ 的逆元, 再将 $\bar{5}$ 的逆元与 $\bar{2}$ 相乘即可, $x = (\bar{5})^{-1}\bar{2} = \bar{3}\bar{2} = \bar{6}$,

同样可得 $y = \bar{3}(\bar{2})^{-1} = \bar{3}\bar{4} = \bar{5}$,

习题 7 设 $G = \{(a, b) | a, b \in \mathbb{Z}_5, b \neq \bar{0}\}$, 规定 $(a, b) \cdot (c, d) = (ad + bc, bd)$,

试证明 $\{G; \cdot\}$ 是交换群,

证明: 若 b, d 都不为 $\bar{0}$, 则由 $\mathbb{Z}_5 - \{\bar{0}\}$ 关于乘法运算是群可知 $bd \neq \bar{0}$,

因此, $\{G; \cdot\}$ 是代数系统,

由 $((a, b) \cdot (c, d)) \cdot (s, t) = (ad + bc, bd) \cdot (s, t) = (adt + bct + bds, bdt)$,

$(a, b) \cdot ((c, d) \cdot (s, t)) = (a, b) \cdot (ct + ds, dt) = (adt + bct + bds, bdt)$,

可知 $\{G; \cdot\}$ 是交换半群

若 $(a, b) \cdot (c, d) = (ad + bc, bd) = (a, b)$, 则 $d = \bar{1}, c = \bar{0}$, 即 $(\bar{0}, \bar{1})$ 是右单位元,

若 b 不等于 $\bar{0}$, 则存在不等于 $\bar{0}$ 的 d , 使得 $bd = \bar{1}$,

从而 $(a, b) \cdot (-ad^2, d) = (ad - bad^2, bd) = (\bar{0}, \bar{1})$, 即 (a, b) 有右逆元,

综上, $\{G; \cdot\}$ 是交换群,

习题 8 设 G 是群, 证明 $G \times G$ 关于运算 $(a, b) \cdot (c, d) = (ac, bd)$ 是群,

其中 a, b, c, d 都属于 G ,

证明: 设 e 是 G 的单位元, 则 (e, e) 是 $G \times G$ 的单位元, (a^{-1}, b^{-1}) 是 (a, b) 的逆元,

由 $((a, b) \cdot (c, d)) \cdot (e, f) = (ac, bd) \cdot (e, f) = (ace, bdf)$,

$(a, b) \cdot ((c, d) \cdot (e, f)) = (a, b) \cdot (ce, df) = (ace, bdf)$,

知 $G \times G$ 的运算满足结合律, 因此 $G \times G$ 是群

习题 9 试证明有限半群 G 是群的充分必要条件是 G 中消去律成立,

证明: 必要性, 在 G 中, 若 $ax = ay$, 则两端左乘 a 的逆元得 $x = y$,

同样的, 由 $xa = ya$ 可以推得 $x = y$, 即在 G 中消去律成立,

充分性, 设半群 G 含有 n 个元素 $a_1, a_2, \dots, a_n$,

用元素 a_i 左乘 G 的每个元素得 $a_i a_1, a_i a_2, \dots, a_i a_n$,

因为在 G 中消去律成立, 所以这 n 个元素互不相同,

从而存在属于集合 $\{1, 2, \dots, n\}$ 的某个 k 使得 $a_j = a_i a_k$, 即方程 $a_j = a_i x$ 有解,

同理可证方程 $a_j = ya_i$ 有解, 所以 G 是群,

注：以上结论对无限群不成立，

例如自然数关于加法运算是半群，且消去律成立，但不是群，

习题 10 $R^2=\{(x,y)|x,y\in R\}$ 是平面上点的集合，

对属于集合 A 的任意 a,b ，有 R^2 上平移变换 $\tau_{a,b}:(x,y)\rightarrow(x+a,y+b)$ ，

试证明 $G=\{\tau_{a,b}|a,b\in R\}$ 关于变换的乘法运算是群(这个群称为平移变换群)，

证明：因为 $\tau_{a,b}\tau_{c,d}=\tau_{a+c,b+d}$ 及变换的合成运算满足结合律，

所以 G 关于变换的乘法运算是半群，

显然， $\tau_{0,0}$ 是单位元， $\tau_{-a,-b}$ 是 $\tau_{a,b}$ 的逆元，因此， G 关于变换的乘法运算是群

习题 11 对属于集合 R 的任意 a,b ，令 $\tau_{a,b}:R\rightarrow R, x\rightarrow ax+b$ ，

试证明 $G=\{\tau_{a,b}|a,b\in R, a\neq 0\}$ 关于变换的乘法运算是群，

证明：因为 $\tau_{a,b}\tau_{c,d}=\tau_{ac,ad+b}$ ，及变换的合成运算满足结合律，

所以 G 关于变换的乘法运算是半群

显然， $\tau_{1,0}$ 是单位元， $\tau_{a^{-1},-ba^{-1}}$ 是 $\tau_{a,b}$ 的逆元，

因此， G 关于变换的乘法运算是群，

习题 12 设 G 是有单位元的半群， $U(G)$ 是 G 的所有可逆元构成的集合，

试证明 $U(G)$ 是群，

证明：因为 G 的单位元是可逆元，所以 $U(G)$ 是非空集合，

因为 G 是半群，所以 $U(G)$ 的元素满足结合律，

对属于集合 $U(G)$ 的任意 a,b ，有 a^{-1} 属于 $U(G)$ ， ab 属于 $U(G)$ ，

因此 $U(G)$ 是群，称为 G 的单位群，

习题 13 $\{Z_n; \cdot\}$ 是有单位元的半群，则 $U(Z_n)$ 关于剩余类乘法运算是交换群，

分别求 $U(Z_5)$ 和 $U(Z_6)$ 的元素

解： $U(Z_5)=Z_5-\{\bar{0}\}$ ， $U(Z_6)=\{\bar{1}, \bar{5}\}$ ，

习题 14 请将下列 4 阶群运算表补充完整，

	e	a	b	c
e				
a	a	e		
b				
c				e

当一个群为有限群时，它的元素的运算关系可以通过运算表给出，例如含有 3 个元素的剩余类加法群 Z_3 ，表中的左上角表示运算，表的第一行和第一列列出所有元素，并用第一列的各个元素去和第一行的各个元素运算，一般地，第一行和第一列列出的元素的次序相同

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

解: 注意到 $ae=a$ ，根据群的消去律可知 e 是单位元，从而可以计算出运算表的第一行、第一列元素，仍然根据群的消去律可知表中在一行(列)中的元素都不相同，那么 $ab=b$ 或 c ，若 $ab=b$ ，则 $a=e$ ，矛盾，所以 $ab=c, ac=b$ ，进而可知 $bc=a, ba=c, ca=b, bb=e, cb=a$ ，

习题 15 请将下面 5 阶交换群的运算表补充完整

	e	a	b	c	d
e					
a		b			
b				e	
c					
d	d				

解: 仿照习题 14 可得

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c