第2章 群、环、体、域.

2.1 半群与群

1. 证明：封闭性 $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} x & y \\ 0 & x \end{pmatrix} = \begin{pmatrix} ax & ay+bx \\ 0 & ax \end{pmatrix}$.

令 $S = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \ a \neq 0,\ a, b \in C \right\}$，显然 S 非空.

首先 S 对于矩阵乘法封闭的.

由于矩阵乘法满足结合律，故 S 满足结合律.

对任意 $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in S$. 存在单位元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$，使得 $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$

由 $\begin{pmatrix} ax & ay+bx \\ 0 & ax \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 得 $x = a^{-1} = \frac{1}{a}$

$$y = \frac{-ba^{-1}}{a} = -\frac{b}{a^2}$$

故对任意 $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in S$，存在逆元 $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a^2} \\ 0 & \frac{1}{a} \end{pmatrix} \in S$.

因此 S 成群 □

2. 证明：显然 Z 非空，且二元运算 $\oplus$ 在 Z 上封闭.

1. 结合律：对 $(a\oplus b)\oplus c = (a+b-2)\oplus c = a+b-2+c-2$

$$= a+(b+c-2)-2 = a\oplus(b+c-2)$$

$$= a\oplus(b\oplus c)$$

2. 单位元存在为 $e=2$.

由 $\left.\begin{array}{l} a\oplus e = a+e-2 = a \\ e\oplus a = a. \end{array}\right\} \Rightarrow e=2.$

3. 逆元存在 $(4-a) = a^{-1} \in Z$

$\left.\begin{array}{l} a\oplus b = a+b-2 = 2 \\ b\oplus a = a+b-2 = 2 \end{array}\right\} \Rightarrow b = 4-a.$

故 $(Z, \oplus)$ 是群 □

3. 集合 $R\times R$ 上定义乘法 $(a,b)\cdot(c,d)=(ad+bc, bd)$.

$(R\times R,\cdot)$ 不成群. 因为 $\underset{\in R\times R}{(0,0)}$ 不存在逆元.

<1> $(R\times R,\cdot)$ 满足结合律 易证. $[(a,b)\cdot(c,d)](e,f)=(a,b)[(c,d)\cdot(e,f)]$

$=(adf+bcf+bde, bdf)$.

<2> $(R\times R,\cdot)$ 存在单位元 $(0,1)$ $\quad (a,b)\cdot(0,1)=(a,b)$

$(0,1)\cdot(a,b)=(a,b)$

<3> $(0,0)\in(R\times R)$ 不存在逆元.

□

4. 证明: 存在解 $ax=b \Rightarrow x=a^{-1}b$, $ya=b\Rightarrow y=ba^{-1}$.

假设方程 $ax=b$ 存在两个解 x_1 x_2.

则 $ax_1=b=ax_2$ 两边同时左乘 a^{-1} 得 $x_1=x_2$.

同理假设方程 $ya=b$ 存在两个解 y_1,y_2.

则 $y_1a=b=y_2a$ 两边同时右乘 a^{-1} 得 $y_1=y_2$

□

5. 证明: 由G是群. $a_1,a_2\cdots a_n\in G$.

故由 $(a_1a_2\cdots a_n)\cdot(a_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1})=e$ (G满足结合律)

$(a_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1})\cdot(a_1a_2\cdots a_n)=e$

群G的中元素的逆元唯一. 故 $(a_1a_2\cdots a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1}$ □

6. 证明: 由 $aba^{-1}=b \Rightarrow ab=ba$ 两边右乘 a

$ab=ba \Rightarrow aba^{-1}=b$ 两边右乘 a^{-1}.

□

7. 证明: 由 $aba^{-1}=b^n$. 得 $b=a^{-1}b^na$

故 $b^n=(a^{-1}b^na)^n=a^{-1}b^{n^2}a$

故 $b=a^{-1}b^na=a^{-1}(a^{-1}b^{n^2}a)a=a^{-2}b^{n^2}a^2$.

由 $b^{n^2}=(a^{-1}b^na)^{n^2}=a^{-1}b^{n^3}a$

故 $b=a^{-2}(a^{-1}b^{n^3}a)a^2=a^{-3}b^{n^3}a^3$ 迭代下去得

$b=a^{-i}b^{n^i}a^i$ 故 $a^ib a^{-i}=b^{n^i}$ □ ②

8. (2.1): $\begin{cases} na = a+a+\cdots+a & \forall n\in\mathbb{Z}^+ \\ 0\cdot a = 0 \\ (-n)a = n(-a) \end{cases}$

证明：对 $\forall a,b\in G$，$m,n\in\mathbb{Z}$.

$$\begin{cases} na+ma = (n+m)a \\ m(na) = (mn)a \\ n(a+b) = na+nb \end{cases}$$

(trivial). □

9. 证明：由于对 $\forall a,b\in G$，都有 $(ab)^2=a^2b^2$.

故 $abab=a^2b^2$ 两边同时左乘 a^{-1}，右乘 b^{-1} 得

$ba=ab$. 故对任意的 $a,b\in G$，都有 $ab=ba$

故 G 是交换群 □

10. 证明：(1) 由于 $a^2=e$ 故有 $a=a^{-1}$ (两边同时左乘 a^{-1})

(2) 由对 $\forall a,b\in G$，$ab\in G$ 故 $(ab)^2=e$

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

因此 G 是交换群 □

11. 证明：(1) 由 $(a^{n-1})\cdot a = a\cdot(a^{n-1}) = a^n = 1$ 故 $a^{-1}=a^{n-1}$

由 $b\cdot(b) = (b)\cdot b = 1$ 故 $b^{-1}=b$ □

(2). 由 $bab^{-1}=a^{-1} \Leftrightarrow ba=a^{-1}b \Leftrightarrow ab=ba^{-1}$

若 $ab=ba$ 则 $ba^{-1}=ba \Rightarrow a=a^{-1}=a^{n-1}$ 若 $n\geq 3$

$a\neq a^{n-1}$ 矛盾，故 $ab\neq ba$ □

(3) ① $(a^2b)a(a^2b)^{-1} = (a^2b)ab^{-1}a^{-2} = a^2bab^{-1}\cdot a^{-2} = a^2\cdot a^{-1}\cdot a^{-2}$
$= a^{-1}$

② $(a^2b)(a^2b) = a^2b\cdot \underline{b^{-1}ba}\cdot\underbrace{\underline{b^{-1}ba}\cdot\ \cdots\ \cdot\underline{b^{-1}ba}}_{j个}\cdot b$ (由(1) $b=b^{-1}$)

$= a^2\,bab^{-1}\cdot bab^{-1}\cdot\ \cdots\ \cdot bab^{-1}$

$= a^2\cdot\underbrace{\underline{(a^{-1})}\cdot\underline{(a^{-1})}\cdot\ \cdots\ \cdot\underline{(a^{-1})}}_{j个} = a^{2-j}$ □

(4). $ba^{2}b^{-1} = b\,\underbrace{\underline{ab^{-1}b}\cdot\underline{ab^{-1}b}\cdots\underline{ab^{-1}b}}_{2\text{个}}\cdot b^{-1}$

$= \underbrace{\underline{bab^{-1}}\cdot\underline{bab^{-1}}\cdots\underline{bab^{-1}}}_{2\text{个}}$

$= a^{-1}\cdot a^{-1}\cdots a^{-1} = a^{-2}$

故 $ba^{2} = a^{-2}b$

□

12. (1) $(\mathbb{Z},+)$ 是无限群，$(\mathbb{Z}/n\mathbb{Z},+)$ 是有限群. $\#(\mathbb{Z}/n\mathbb{Z},+) = n$.

(2) D_6 不是交换群. $(\mathbb{Z}/6\mathbb{Z},+)$ 是交换群.
(见习题11(2))

(3). $\mu_n = \{e^{\frac{2k\pi i}{n}} \mid k=1,2,\dots n\}$

$\mu_4 = \{1,-1,i,-i\}$ $\quad \mathbb{Z}/4\mathbb{Z} = \{\bar0,\bar1,\bar2,\bar3\}$

定义: $\varphi:\ \mathbb{Z}/4\mathbb{Z} \longrightarrow \mu_4$

$\bar0 \longmapsto 1$ 单位元		$\bar0 \longmapsto 1$
$\bar1 \longmapsto i$		$\bar1 \longmapsto -i$
$\bar2 \longmapsto -1$		$\bar2 \longmapsto -1$
$\bar3 \longmapsto -i$		$\bar3 \longmapsto i$

显然 φ 为双射. 易验证 φ 保持运算 故 $(\mathbb{Z}/4\mathbb{Z},+) \cong \mu_4$. □

(4). $(\mathbb{Z}/5\mathbb{Z})^{\times} = \{\bar1,\bar2,\bar3,\bar4\}$

定义: $\varphi: (\mathbb{Z}/5\mathbb{Z})^{\times} \longrightarrow \mu_4$

$\bar1 \longmapsto 1$ 单位元

$\bar2 \longmapsto i$

$\bar3 \longmapsto -i$

$\bar4 \longmapsto -1$

显然 φ 为双射. 易验证 φ 保持运算 故 $(\mathbb{Z}/5\mathbb{Z})^{\times} \cong \mu_4$ □

13. 证明：由 $\varphi: G \longrightarrow G$
$x \longmapsto x^{-1} \quad (\forall x \in G)$

显然是双射.[可以证一下]

$\Rightarrow$ 若 G 为交换群. $\varphi(x_1x_2) = (x_1x_2)^{-1} = x_2^{-1}x_1^{-1} = x_1^{-1}x_2^{-1} = \varphi(x_1)\varphi(x_2)$.

故 φ 保持运算. φ 为同构映射.

$\Leftarrow$ 若 φ 为同构映射，则对 $\forall x_1, x_2 \in G$, 有.

$x_1x_2 = \varphi(x_1^{-1})\varphi(x_2^{-1}) = \varphi(x_1^{-1}x_2^{-1}) = \cancel{\varphi(}(x_1^{-1}x_2^{-1})^{-1} = x_2x_1$

故 G 为交换群. □

14. 证明：设群 G 为偶数阶群 $\#G = |G| = 2n \quad n \geq 1$.

若 G 中不含有偶数元素 $a \neq e$, 满足 $a^2 = e$, 即 G 中不含有元素 $a \neq e$. $a = a^{-1}$.

若在 G 中除去单位元 $\#(G \setminus \{e\}) = 2n-1$ 为奇数

但在 $G \setminus \{e\}$ 中任意元素如 a, 均有其逆元 $a^{-1} \neq a$. 两两配对, (a, a^{-1})

在 $G \setminus \{e\}$ 中应有偶数个元素，矛盾.

故 G 中必有元素 $a \neq e$, 满足 $a^2 = e$ □

15. 证明 (与14题相合)

若 $n > 2$, 则对任意 G 中的 n 阶元素 a, $\quad a \neq a^{-1}$ (否则 a 的阶为2)

a^{-1} 亦为 n 阶元素，故 G 中阶为 n 的元素成对出现，个数是偶数 □

2.2 环

1、证明：归纳法.

当n=1时，$(a+b)^1 = \binom{n}{1}a + \binom{n}{0}b = a+b$.

假设当n=m时，等式成立，即 $(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k}$.

现证明当n=m+1时等式成立.

$$(a+b)^{m+1} = (a+b)^m(a+b) = \left[\sum_{k=0}^{m}\binom{m}{k}a^k b^{m-k}\right]\cdot a+b$$

$$= \sum_{k=0}^{m}\binom{m}{k}a^{k+1}b^{m-k} + \sum_{k=0}^{m}\binom{m}{k}a^k b^{m+1-k}$$

$$= \sum_{k=1}^{m+1}\binom{m}{k-1}a^k b^{m+1-k} + a^0 b^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^k b^{m+1-k}$$

$$= a^{m+1} + b^{m+1} + \sum_{k=1}^{m}\left[\binom{m}{k-1}+\binom{m}{k}\right]a^k b^{m+1-k}$$

$$= \sum_{k=0}^{m+1}\binom{m+1}{k}a^k b^{m+1-k}$$

□

得证.

2. 证明：由 $a(b-c)+ac = a(b-c+c) = ab$ 两边同时减 ac

得 $\Rightarrow$ $a(b-c) = ab-ac$

由 $(b-c)a + ca = (b-c+c)a = ba$ 两边同时减 ca.

得 $\Rightarrow$ $(b-c)a = ba-ca$

3. 证明：若 a 可逆，则存在 $b\in R$，$b\neq 0$，使得 $ab=ba=1$

$\Leftrightarrow$ 存在 $b\neq 0 \in R$，使得 $(-a)\cdot(-b) = (-b)\cdot(-a) = 1$

$\Leftrightarrow$ $-a$ 可逆.

$\Leftarrow$ 由 $-a$ 可逆，则 $-(-a)$ 可逆，故 a 可逆 □

4. 证明：Q, R, C 关于数的加法和乘法构成有单位交换环.

利用定义证明即可. 〈1〉 Q, R, C 交换群.

[（显然 Q, R, C）非空] 〈2〉 关于乘法结合律

〈3〉 分配律.

〈4〉 单位元 1.

〈5〉 交换律显然.

$Q^{\times} = Q\setminus\{0\}$

$R^{\times} = R\setminus\{0\}$

$C^{\times} = C\setminus\{0\}$.

5. 证明：$\mathbb{Z}/n\mathbb{Z}$ 是模 n 剩余类环，单位元 $\bar{1}$，零元 $\bar{0}$，且是交换环.

乘法单位群是模 n 的简化剩余类集 $(\mathbb{Z}/n\mathbb{Z})^{\times}$ 构成的乘法群.

证明：〈1〉由例 2.1.4. $\mathbb{Z}/n\mathbb{Z}$ 是加法交换群

〈2〉 乘法结合律 $(\bar{a}\cdot\bar{b})\cdot\bar{c} = \bar{a}\cdot(\bar{b}\cdot\bar{c})$

〈3〉 乘法对加法的分配律.

〈4〉 单位元 $\bar{1}$，零元 $\bar{0}$，交换环 $\bar{a}\cdot\bar{b} = \bar{b}\cdot\bar{a}$.

由例 2.2.7 其乘法单位群是模 n 的简化剩余类集 $(\mathbb{Z}/n\mathbb{Z})^{\times}$ 构成的乘法群.

6. 证明：反证. 若 a 是左零因子，则存在 $b\neq 0$，$b\in R$.

使得 $a\cdot b = 0$ 则 $a^{-1}\cdot a\cdot b = 0 \Rightarrow b = 0$ 矛盾

同理 a 不是右零因子

□

7. 证明：~~⇒ 若 |A|~~ 注：$M = M(n, K)$ 不是交换环.

⇒ 若 $|A|\neq 0$，则 A 是可逆矩阵. $A\cdot A^{-1} = A^{-1}\cdot A = E$

故 A 是可逆元，由第 6 题 A 不是右（左）零因子，故 A 不是零因子，矛盾.

故 $|A| = 0$

⇐ 由 $|A| = 0$，故 $A = (\alpha_1\ \alpha_2 \cdots \alpha_n)$ 的列向量组线性相关.

即存在 $k_1\ k_2 \cdots k_n$ 不全为 0，使得 $(\alpha_1\ \alpha_2 \cdots \alpha_n)\begin{pmatrix}k_1\\k_2\\ \vdots \\k_n\end{pmatrix} = 0$.

$$A\cdot\begin{pmatrix}k_1 & k_1 & \cdots & k_1\\ k_2 & k_2 & \cdots & k_2\\ \vdots & \vdots & & \vdots\\ k_n & k_n & \cdots & k_n\end{pmatrix} = 0\ (矩阵)$$ 故 A 是左零因子

同理 考虑 A 的行向量组，可得 A 是右零因子，故 A 是零因子

□

法②
利用 $AX = 0$ 有非零解 齐次线性方程组 来证.

8: $(Z;\oplus,\odot)$ 不构成环.

考虑 Z 的 $\oplus$ ~~群~~ 不构成群. 因为 Z 中除了 ± 1 外, 不存在加法的逆元. □

9: 显然 S 为非空集合.

(1) S 对 $+$ 成交换群.

(1) $[(a,b)+(c,d)]+(e,f)=(a,b)+[(c,d)+(e,f)]$

(2) 单位元 $(0,0)$

(3) 逆元 $(-a,-b)$

(4) 交换律 $(a,b)+(c,d)=(c,d)+(a,b)$.

(2) 乘法结合律 $[(a,b)\cdot(c,d)](e,f)=(a,b)\cdot[(c,d)\cdot(e,f)]$

(3) 分配律 易证明 trivial

(4) 单位元. $(1,0)$

故 $(S,+,\cdot)$ 是有单位环 □

10. R 是有单位交换环. 故 R 非空. $a\oplus b\in R$, $a\odot b\in R$.

(1) R 对 $\oplus$ 成交换群.

(1) $(a\oplus b)\oplus c = a+b+c-1-1 = a\oplus(b\oplus c)$

(2) ~~单位元~~ (零元): 1 (环 R 中的单位元)

$a\oplus 1 = 1\oplus a = a$

(3) 逆元 (负元): $1+1-a$ ~~$=1\oplus 1-a=-a$~~ ~~$=2\cdot 1-a$~~ ~~[逆环是 $2-a$] 有区别~~

$a\oplus b=b\oplus a=a+b-1=1 \Rightarrow b=1+1-a$.

(4) 交换律 显然.

(2) 乘法结合律 $(a\odot b)\odot c = a\odot(b\odot c)$ 易证明

(3) 乘法对加法分配律. $(a\oplus b)\odot c=(a\odot c)\oplus(b\odot c)$

$c\odot(a\oplus b)=(c\odot a)\oplus(c\odot b)$

(4) 单位元: 0 (R 中的零元)

$a\odot b=b\odot a=a+b-ab=a \Rightarrow b=0$

(5) 交换律: $a\odot b=b\odot a=a+b-ab$ ($\because R$ 是交换环) □

故 $(R;\oplus,\odot)$ 是有单位交换环

11: 若 a 不是 R 的一个左零因子, 则 $ab\neq 0$. 且有 $(ab)\cdot a=0$ 故 a 是 R 的一个右零因子.

若 $ab=0$ 则 a 是 R 的一个左零因子 □

2.3 体和域

1. 证明：（类似例 2.3.1） $F = Q[\sqrt{d}]$

首先要证 F 对加法和乘法都封闭，对任意 $a, b, c, e \in Q$.

有：$(a+b\sqrt{d}) + (c+e\sqrt{d}) = (a+c) + (b+e)\sqrt{d} \in Q[\sqrt{d}]$

$(a+b\sqrt{d})(c+e\sqrt{d}) = (ac+bed) + (ae+bc)\sqrt{d} \in Q[\sqrt{d}]$

复数的加法和乘法限制在 F 上仍是二元运算，显然 F 中加法结合律，交换律，乘法交换律，结合律以及加法和乘法间的分配律都自然成立.

且 $0, 1 \in F$，$-(a+b\sqrt{d}) = -a + (-b)\sqrt{d} \in F$.

当有理数 a, b 不全为 0 时，可验证 $a^2 - db^2 \neq 0$，于是

$$(a+b\sqrt{d})^{-1} = \frac{a-b\sqrt{d}}{a^2-db^2} = \underbrace{\frac{a}{a^2-db^2}}_{\in Q} + \underbrace{\frac{-b}{a^2-db^2}}_{\in Q}\sqrt{d} \in Q[\sqrt{d}]$$

~~在 G=~~

故 $Q[\sqrt{d}]$ 是一个域 □

2. 证明：Q_8 非空，且对矩阵乘法封闭.

$I^2 = J^2 = K^2 = -E$

$IJ = K = -JI$

$JK = I = -KJ$

$KI = J = -IK$

(1) 故 Q_8 对矩阵乘法满足结合律

(2) 单位元：E

(3) 存在逆元：

$-I^2 = -J^2 = -K^2 = E$. □