第一章：群

1.1 第一节

1.1.1 第一题

写出正十二棱锥的旋转对称群的所有元素，这个群是循环群吗？

1.1.2 第二题

写出正六边形的对称群的所有元素，它的生成元是什么？生成元适合的关系有哪些？这个群的阶是多少？

1.1.3 第三题

写出正五边形的对称群的所有元素。

1.1.4 第四题

写出正四面体的旋转对称群的所有元素。

1.1.5 第五题

写出正方体的旋转对称群的所有元素。

1.1.6 第六题

写出$\mathbb{Z}_{15}$的单位群$\mathbb{Z}_{15}^*$的全部元素。

解：

$$\mathbb{Z}_{15}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\} \tag{1}$$

1.1.7 第七题

证明：$|\mathbb{Z}_p| = \varphi(p)$

证明：显然！

1.1.8 第八题

对于矩阵

$$A = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & \frac{2}{3} \\ -\frac{2}{3} & \frac{2}{3} & \frac{1}{3} \\ -\frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \end{pmatrix} \tag{2}$$

证明：$A \in \mathrm{SO}_3$，并找出旋转对称轴。

证明：容易验证$\det A = 1$且$A * A^T = I$。

$O(0,0,0)$显然为旋转不动点，令其另一非零旋转不动点为x，那么$Ax = x$，解得$x = (1, -1, 1)$，因此旋转对称轴为$(0,0,0)$和$(1,-1,1)$两点连线。

1.1.9 第九题

在S_5中，设

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} \tag{3}$$

求$\sigma_1\sigma_2$，$\sigma_2\sigma_1$，σ_1^{-1}，$\sigma_1\sigma_2\sigma_1^{-1}$。

写出σ_1和σ_2的轮换分解式和对换分解式，并说明σ_1和σ_2是奇置换还是偶置换。

解：容易求出

$$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}, \qquad \sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} \tag{4}$$

$$\sigma_1^{-1}=\begin{pmatrix}1&2&3&4&5\\2&4&1&5&3\end{pmatrix},\qquad \sigma_1\sigma_2\sigma_1^{-1}=\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix}\tag{5}$$

$$\sigma_1=(13542)=(12)(14)(15)(13),\qquad \sigma_2=(143)(25)=(13)(14)(25)\tag{6}$$

σ_1为偶置换，σ_2为奇置换。

1.1.10 第十题

r-轮换的奇偶性与r的奇偶性相反。

1.1.11 第十一题

写出A_3, A_4的所有元素。

解：

$$A_3=\{(1),(123),(132)\}\tag{7}$$

$$A_4=\{(1),(12)(34),(13)(24),(14)(23),(123),(132),(124),(142),(134),(143),(234),(243)\}\tag{8}$$

1.1.12 第十二题

证明：对于$\sigma=(i_1\cdots i_r)$，以及任意$\tau\in S_n$，成立

$$\tau\sigma\tau^{-1}=(\tau(i_1)\cdots\tau(i_r))\tag{9}$$

证明：任取$k\in\{1,\cdots,r\}$，注意到

$$(\tau\sigma\tau^{-1})(\tau(i_k))=\tau\sigma\tau^{-1}\tau(i_k)=\tau\sigma(i_k)=\tau(i_{k+1})\tag{10}$$

其中$i_{r+1}=r_1$，这说明$(\tau(i_1)\cdots\tau(i_r))$构成轮换。

任取$x\in\Omega\setminus\{i_1,\cdots,i_k\}$，那么$(\tau\sigma\tau^{-1})(x)=x$。

综上所述，$\tau\sigma\tau^{-1}=(\tau(i_1)\cdots\tau(i_r))$，原命题得证！

1.2 第二节

1.2.1 第一题

定义

$$k\mathbb{Z}=\{kn:n\in\mathbb{Z}\},\qquad k\in\mathbb{N}^*\tag{11}$$

证明：$(k\mathbb{Z},+)$为群$(\mathbb{Z},+)$的循环子群。

证明：显然$k\mathbb{Z}\subset\mathbb{Z}$。任取$a,b\in k\mathbb{Z}$，那么存在$m,n\in\mathbb{Z}$，使得成立$a=km,b=kn$，注意到

$$a-b=k(m-n)\in k\mathbb{Z}\tag{12}$$

因此$k\mathbb{Z}$为$\mathbb{Z}$的子群。

下面证明$k\mathbb{Z}=\langle k\rangle$，任取$a\in k\mathbb{Z}$，那么存在$n\in\mathbb{Z}$，使得成立$a=kn=nk$，因此$k\mathbb{Z}$为由$k$生成的循环群。

1.2.2 第二题

对于群$(G,*)$的子群H和K，定义

$$HK=\{h*k:h\in H,k\in K\}\tag{13}$$

证明：HK为子群当且仅当$HK=KH$。

证明：对于必要性，如果HK为子群，那么任取$h*k\in HK$，由于HK为子群，那么存在$h*k$的逆h_1*k_1，因此

$$h*k=(h_1*k_1)^{-1}=k_1^{-1}*h_1^{-1}\in KH\implies HK\subset KH\tag{14}$$

任取$k*h\in KH$，由于由于HK为子群，那么存在$h^{-1}*k^{-1}$的逆h_2*k_2，因此

$$k*h=(k*h)*(h^{-1}*k^{-1})*(h_2*k_2)=h_2*k_2\in HK\implies KH\subset HK\tag{15}$$

必要性得证！

对于充分性，如果$HK=KH$，那么任取$h_1*k_1,h_2*k_2\in HK$，存在$h_3*k_3,h_4*k_4\in HK$，使得成立$k_2^{-1}*h_2^{-1}=h_3*k_3,k_1*h_3=h_4*k_4$，于是

$$(h_1*k_1)*(h_2*k_2)^{-1}=(h_1*k_1)*(k_2^{-1}*h_2^{-1})=(h_1*k_1)*(h_3*k_3)=(h_1*h_4)*(k_4*k_3)\in HK \tag{16}$$

因此HK为子群，必要性得证！

1.2.3 第三题

在群$(\mathbb{C},+)$中，定义Gauss整数子群为$\langle 1,i\rangle$，其元素为?

解：$\langle 1,i\rangle=\mathbb{Z}^2$

1.2.4 第四题

1.2.5 第五题

证明：

$$S_n=\langle (12),(23),\cdots,(n-1\quad n)\rangle=\langle (12),(1\cdots n)\rangle \tag{17}$$

证明：已知

$$S_n=\langle (12),(13),\cdots,(1n)\rangle \tag{18}$$

记

$$S_n^{(1)}=\langle (12),(23),\cdots,(n-1\quad n)\rangle,\qquad S_n^{(2)}=\langle (12),(1\cdots n)\rangle \tag{19}$$

注意到，对于任意$a,b\in\mathbb{N}^*$

$$(ab)=(1a)(1b)(1a)\implies S_n^{(1)}\subset S_n \tag{20}$$

$$(1a)=(12)(23)\cdots(a-1\quad a)\cdots(23)(12)\implies S_n\subset S_n^{(1)} \tag{21}$$

$$(1\cdots n)=(12)(13)\cdots(1n)\implies S_n^{(2)}\subset S_n \tag{22}$$

$$(a\quad a+1)=(1\cdots n)^{a-1}(12)(1\cdots n)^{n-a+1}\implies S_n^{(1)}\subset S_n^{(2)} \tag{23}$$

因此

$$S_n^{(1)}=S_n^{(2)}=S_n \tag{24}$$

原命题得证！

1.2.6 第六题

证明：当$n\geq 3$时，成立

$$A_n=\langle (123),(124),\cdots,(12n)\rangle \tag{25}$$

证明：

1.2.7 第七题

在域$\mathbb{Q}$上行列式为1的2阶矩阵乘法群$\mathrm{SL}_2(\mathbb{Q})$中，设

$$A=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\qquad B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix} \tag{26}$$

证明：$|A|=4,|B|=3,|AB|=\infty$

证明：容易知道

$$A^2=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\qquad A^3=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\qquad A^4=\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{27}$$

$$B^2=\begin{pmatrix}-1&-1\\1&0\end{pmatrix},\qquad B^3=\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{28}$$

记

$$C=AB=\begin{pmatrix}1&1\\0&1\end{pmatrix} \tag{29}$$

那么由归纳法容易得到

$$C^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \tag{30}$$

于是

$$|A| = 4, |B| = 3, |AB| = \infty \tag{31}$$

1.2.8 第八题

证明：如果群$(G, *)$的每一个非单位元的阶均为2，那么$(G, *)$为Abel群。

证明：任取$a, b \in G$，那么

$$a * b = (a * b)^{-1} = b^{-1} * a^{-1} = b * a \tag{32}$$

因此$(G, *)$为Abel群。

1.2.9 第九题

证明：如果群$(G, *)$的阶为偶数，那么G存在2阶元。

证明：如果G不存在2阶元，那么对于任意元素$a \in G \setminus \{e\}$，$a^2 \neq e$，而存在$b \in G \setminus \{e\}$，使得$a * b = e$，因此使得互为逆元的元素成对出现，而由于群G的阶为偶数，那么$G \setminus \{e\}$的阶为奇数，矛盾！那么G存在2阶元。

1.2.10 第十题

Euler定理：对于$a, n \in \mathbb{N}^*$，如果$(a, n) = 1$，那么

$$a^{\varphi(n)} \equiv 1 \mod n \tag{33}$$

1.2.11 第十一题

求6阶循环群$G = \langle a \rangle$的所有子群。

证明：G的全部子群为

$$\langle e \rangle, \qquad \langle a \rangle, \qquad \langle a^2 \rangle, \qquad \langle a^3 \rangle \tag{34}$$

1.2.12 第十二题

求S_3的所有子群。

1.2.13 第十三题

求A_4的所有子群，并证明A_4没有6阶子群。

1.2.14 第十四题

证明：对于群G的有限子群H和K，成立

$$|HK| = \frac{|H||K|}{|H \cap K|} \tag{35}$$

证明：任取$a, b \in H \cap K$，那么$a, b \in H$且$a, b \in K$，因此$a * b^{-1} \in H$且$a * b^{-1} \in K$，于是$a * b^{-1} \in H \cap K$，进而$H \cap K < H$。

定义等价关系

$$a \sim b \iff a^{-1} * b \in H \cap K \tag{36}$$

那么

$$[H : H \cap K] = |H/\sim| \tag{37}$$

记$H/\sim = \{h_1, \cdots, h_r\}$，下面证明

$$HK = \bigsqcup_{k=1}^{r} h_k K \tag{38}$$

首先证明不交性，任取$i \neq j \in \{1, \cdots, r\}$，若$h_i K \cap h_j K \neq \varnothing$，令$a \in h_i K \cap h_j K$，那么$a \in h_i K$且$a \in h_j K$，于是存在$k_i, k_j \in K$，使得成立$a = h_i * k_i = h_j * k_j$，于是$h_i^{-1} * h_j = k_i * k_j^{-1} \in K$，因此$h_i^{-1} * h_j \in H \cap K$，进而$h_i \sim h_j$，矛盾！

其次证明等式，任取$h \in H, k \in K$，存在$i \in \{1, \cdots, r\}$，使得成立$h \sim h_i$，那么$h_i^{-1} * h \in H \cap K$，因此$h_i^{-1} * h \in K$，于是存在$k_h \in K$，使得成立$h = h_i * k_h$，于是$h * k = h_i * (k_h * k) \in h_i K$，于是$HK \subset \bigsqcup_{k=1}^{r} h_k K$。$HK \supset \bigsqcup_{k=1}^{r} h_k K$显然，于是$HK = \bigsqcup_{k=1}^{r} h_k K$。

由Lagrange定理

$$|HK| = |K||H/\sim| = |K|[H : H \cap K] = \frac{|H||K|}{|H \cap K|} \tag{39}$$

1.3 第三节

1.3.1 第一题

证明：

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \times) \tag{40}$$

证明：构造映射

$$\begin{aligned} \varphi :& \mathbb{R} \to \mathbb{R}^+ & (41) \\ & x \mapsto \mathrm{e}^x & (42) \end{aligned}$$

首先，证明φ为群同态态射。任取$x, y \in \mathbb{R}$，注意到

$$\varphi(x + y) = \mathrm{e}^{x+y} = \mathrm{e}^x \mathrm{e}^y = \varphi(x)\varphi(y) \tag{43}$$

因此φ为群同态态射。

其次，证明φ为双射。构造映射

$$\begin{aligned} \psi :& \mathbb{R}^+ \to \mathbb{R} & (44) \\ & x \mapsto \ln x & (45) \end{aligned}$$

注意到

$$\psi \circ \varphi = \varphi \circ \psi = \mathbb{1} \tag{46}$$

于是φ为双射。

综上所述，φ为群同构态射，因此$(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$。

1.3.2 第二题

在$\mathbb{Z}_9^*$中，$\overline{2}$的阶是多少？是否成立$(\mathbb{Z}_9^*, \times) \cong (\mathbb{Z}_6, +)$？

证明：

$$\mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\} \tag{47}$$

在$\mathbb{Z}_9^*$中，$|\overline{2}| = 6$，而在$\mathbb{Z}_6$中，$|\overline{2}| = 3$，因此$(\mathbb{Z}_9^*, \times) \ncong (\mathbb{Z}_6, +)$。

1.3.3 第三题

证明：

$$\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \tag{48}$$

证明：

$$\begin{aligned} \varphi :& \mathbb{Z}_8^* \to \mathbb{Z}_2 \times \mathbb{Z}_2 & (49) \\ & \overline{1} \mapsto (\overline{0}, \overline{0}) & (50) \\ & \overline{3} \mapsto (\overline{1}, \overline{0}) & (51) \\ & \overline{5} \mapsto (\overline{0}, \overline{1}) & (52) \\ & \overline{7} \mapsto (\overline{1}, \overline{1}) & (53) \end{aligned}$$

事实上，$\mathbb{Z}_8^*$为4阶非循环群，而4阶群仅有两个同构类$\mathbb{Z}_4$和$\mathbb{Z}_2 \times \mathbb{Z}_2$，因此$\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$。

1.3.4 第四题

1.3.5 第五题

证明：

$$D_3 \cong S_3 \tag{54}$$

证明：

$$D_n = \{\mathbb{1}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2 : \sigma^n = \tau^2 = \tau\sigma\tau\sigma = \mathbb{1}\} \tag{55}$$

$$S_n = (\mathscr{F}, \circ), \qquad \mathscr{F} = \{\sigma : \{1,2,3\} \to \{1,2,3\}\text{为双射}\} \tag{56}$$

构造映射

$$\sigma \mapsto (123), \qquad \tau \mapsto (12) \tag{57}$$

1.3.6 第六题

对于群G，证明：

$$\sigma : x \mapsto x^{-1} \text{ 是 } G \to G \text{ 的同构映射 } \iff G \text{ 是Able群} \tag{58}$$

证明：对于必要性，如果$\sigma : x \mapsto x^{-1}$是$G \to G$的同构映射，那么任取$x, y \in G$，成立$\sigma(x^{-1}y^{-1}) = \sigma(x^{-1})\sigma(y^{-1})$，于是$xy = yx$，因此$G$是Abel群。

对于充分性，如果G是Abel群，那么任取$x, y \in G$，成立

$$\sigma(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \sigma(x)\sigma(y) \tag{59}$$

于是σ为同态态射，而σ显然为双射，因此σ为同构映射。

1.3.7 第七题

1.3.8 第八题

证明：

$$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \tag{60}$$

证明：

$$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong (\mathbb{Z}_3 \times \mathbb{Z}_2) \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \tag{61}$$

1.3.9 第九题

下列四个24阶Abel群中，哪些是彼此同构的？

$$\mathbb{Z}_{24}, \qquad \mathbb{Z}_{12} \times \mathbb{Z}_2, \qquad \mathbb{Z}_6 \times \mathbb{Z}_4, \qquad \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3, \tag{62}$$

解：

$$\mathbb{Z}_{12} \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \ncong \mathbb{Z}_{24} \tag{63}$$

1.3.10 第十题

下列四个24阶非交换群中，哪些是彼此同构的？

$$D_{12}, \qquad D_4 \times \mathbb{Z}_3, \qquad A_4 \times \mathbb{Z}_2 \tag{64}$$

1.3.11 第十一题

证明：当n为奇数时，成立

$$D_{2n} \cong D_n \times \mathbb{Z}_2 \tag{65}$$

1.3.12 第十二题

证明：当n为奇数时，成立

$$O_n \cong SO_n \times \{I, -I\} \cong SO_n \times \mathbb{Z}_2 \tag{66}$$

1.4 第四节

1.4.1 第一题

定义群映射

$$
\begin{aligned}
f: & (\mathbb{R},+) \to (\mathbb{C}\setminus\{0\},\times) && (67)\\
& x \mapsto \mathrm{e}^{2\pi i x} && (68)
\end{aligned}
$$

证明：f是群同态映射，并求$\mathrm{Ker}\ f$和$\mathrm{Im}\ f$。

证明：显然f是定义良好的。任取$x,y\in\mathbb{R}$，那么$f(x+y)=\mathrm{e}^{2\pi i(x+y)}=\mathrm{e}^{2\pi ix}\mathrm{e}^{2\pi iy}=f(x)f(y)$，因此$f$是群同态映射。

$$
\mathrm{Ker}\ f=\{x\in\mathbb{R}:f(x)=1\}=\{x\in\mathbb{R}:\mathrm{e}^{2\pi ix}=1\}=\mathbb{Z} \quad (69)
$$

$$
\mathrm{Im}\ f=\{f(x):x\in\mathbb{R}\}=\{\mathrm{e}^{2\pi ix}:x\in\mathbb{R}\}=\partial\mathbb{D} \quad (70)
$$

其中$\mathbb{D}=\{z\in\mathbb{C}:|z|<1\}$。

1.4.2 第二题

定义群映射

$$
\begin{aligned}
f: & (\mathbb{C}\setminus\{0\},\times) \to (\mathbb{C}\setminus\{0\},\times) && (71)\\
& z \mapsto \frac{z}{|z|} && (72)
\end{aligned}
$$

证明：f是群同态映射，并求$\mathrm{Ker}\ f$和$\mathrm{Im}\ f$。

证明：显然f是定义良好的。任取$z,w\in\mathbb{C}\setminus\{0\}$，注意到$f(zw)=\dfrac{zw}{|zw|}=\dfrac{z}{|z|}\dfrac{w}{|w|}=f(z)f(w)$，因此$f$是群同态映射。

$$
\mathrm{Ker}\ f=\{x\in\mathbb{C}\setminus\{0\}:f(x)=1\}=\{x\in\mathbb{C}\setminus\{0\}:z/|z|=1\}=\mathbb{R}^+ \quad (73)
$$

$$
\mathrm{Im}\ f=\{f(x):x\in\mathbb{C}\setminus\{0\}\}=\{z/|z|:x\in\mathbb{C}\setminus\{0\}\}=\{z\in\mathbb{C}:|z|=1\} \quad (74)
$$

1.4.3 第三题

定义群映射

$$
\begin{aligned}
f: & \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}\setminus\{0\} && (75)\\
& A \mapsto \det(A) && (76)
\end{aligned}
$$

证明：f是群同态映射，并求$\mathrm{Ker}\ f$和$\mathrm{Im}\ f$。依此进一步证明：$\mathrm{SL}_n(\mathbb{F})\lhd\mathrm{GL}_n(\mathbb{F})$，且$\mathrm{SL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F})\cong\mathbb{F}\setminus\{0\}$。

证明：显然f是定义良好的。任取$A,B\in\mathrm{GL}_n(\mathbb{F})$，注意到$f(AB)=\det(AB)=\det(A)\det(B)=f(A)f(B)$，因此$f$是群同态映射。

$$
\mathrm{Ker}\ f=\{A\in\mathrm{GL}_n(\mathbb{F}):f(A)=1\}=\{A\in\mathrm{GL}_n(\mathbb{F}):\det(A)=1\}=\mathrm{SL}_n(\mathbb{F}) \quad (77)
$$

$$
\mathrm{Im}\ f=\{f(A):A\in\mathrm{GL}_n(\mathbb{F})\}=\{\det(A):A\in\mathrm{GL}_n(\mathbb{F})\}=\mathbb{F}\setminus\{0\} \quad (78)
$$

由第一同构定理，$\mathrm{SL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F})\cong\mathbb{F}\setminus\{0\}$。$\mathrm{SL}_n(\mathbb{F})\lhd\mathrm{GL}_n(\mathbb{F})$是显然的。

1.4.4 第四题

定义

$$
\begin{aligned}
G&=\{f:\mathbb{R}\to\mathbb{R},x\mapsto ax+b:a,b\in\mathbb{R},a\neq 0\},\\
H&=\{f:\mathbb{R}\to\mathbb{R},x\mapsto x+c:c\in\mathbb{R}\}
\end{aligned} \quad (79)
$$

证明：$(G,\circ)$为群，且$G/H\cong\mathbb{R}\setminus\{0\}$，同时$H\lhd G$。

证明：$(G,\circ)$为群是基于如下事实

$$
\begin{aligned}
& cx+d\circ ax+b=c(ax+b)+d=(ac)x+(bc+d), && (80)\\
& ax+b\circ x=x\circ ax+b=ax+b, && (81)\\
& \frac{x-b}{a}\circ ax+b=ax+b\circ\frac{x-b}{a}=x, && (82)\\
& (ex+f\circ cx+d)\circ ax+b=ex+f\circ(cx+d\circ ax+b)=(ace)x+(bce+de+f) && (83)
\end{aligned}
$$

$H\lhd G$是基于如下事实

$$
\frac{x-b}{a}\circ x+c\circ ax+b=x+\frac{a}{c} \quad (84)
$$

构造映射

$$\begin{aligned} f : & G \to \mathbb{R} \setminus \{0\} && (85)\\ & kx+b \mapsto k && (86)\end{aligned}$$

任取$k_1x+b_1, k_2x+b_2 \in G$，注意到
$f(k_1x+b_1 \circ k_2x+b_2) = f((k_1k_2)x+(k_1b_2+b_1)) = k_1k_2 = f(k_1x+b_1)f(k_2x+b_2)$，因此$f$为群同态映射，而显然$\operatorname{Ker} f = H, \operatorname{Im} f = \mathbb{R} \setminus \{0\}$，由群同构定理，$G/H \cong \mathbb{R} \setminus \{0\}$。

1.4.5 第五题

证明：

$$\mathbb{R}/\mathbb{Z} \cong \partial\mathbb{D} \tag{87}$$

证明：我们先来考察一下此同构的动机，可以容易看到

$$\begin{aligned} \mathbb{R}/\mathbb{Z} &= \{x+\mathbb{Z} : x \in \mathbb{R}\} = \{x+\mathbb{Z} : x \in [0,1)\},\\ \partial\mathbb{D} &= \{z \in \mathbb{C} : |z| = 1\} = \{\mathrm{e}^{2\pi ix} : x \in [0,1)\}\end{aligned} \tag{88}$$

因此我们可以构造群同构态射

$$\begin{aligned} \varphi : & \mathbb{R}/\mathbb{Z} \to \partial\mathbb{D} && (89)\\ & x+\mathbb{Z} \mapsto \mathrm{e}^{2\pi ix} && (90)\end{aligned}$$

我们也可以这样构造群同态映射

$$\begin{aligned} \psi : & \mathbb{R} \to \mathbb{C} \setminus \{0\} && (91)\\ & x \mapsto \mathrm{e}^{2\pi ix} && (92)\end{aligned}$$

注意到

$$\begin{aligned} \operatorname{Ker} \psi &= \{x \in \mathbb{R} : f(x) = 1\} = \{x \in \mathbb{R} : \mathrm{e}^{2\pi ix} = 1\} = \mathbb{Z},\\ \operatorname{Im} \psi &= \{\psi(x) : x \in \mathbb{R}\} = \{\mathrm{e}^{2\pi ix} : x \in \mathbb{R}\} = \partial\mathbb{D}\end{aligned} \tag{93}$$

由同构定理，$\mathbb{R}/\mathbb{Z} \cong \partial\mathbb{D}$。

1.4.6 第六题

证明：

$$(\mathbb{C} \setminus \{0\})/\mathbb{R}^+ \cong \partial\mathbb{D} \tag{94}$$

其中$\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$。

证明：

方法一：构造映射

$$\begin{aligned} f : & (\mathbb{C} \setminus \{0\}, \times) \to (\mathbb{C} \setminus \{0\}, \times) && (95)\\ & z \mapsto \frac{z}{|z|} && (96)\end{aligned}$$

显然f是定义良好的。任取$z, w \in \mathbb{C} \setminus \{0\}$，注意到$f(zw) = \dfrac{zw}{|zw|} = \dfrac{z}{|z|}\dfrac{w}{|w|} = f(z)f(w)$，因此$f$是群同态映射。

$$\operatorname{Ker} f = \{x \in \mathbb{C} \setminus \{0\} : f(x) = 1\} = \{x \in \mathbb{C} \setminus \{0\} : z/|z| = 1\} = \mathbb{R}^+ \tag{97}$$

$$\operatorname{Im} f = \{f(x) : x \in \mathbb{C} \setminus \{0\}\} = \{z/|z| : x \in \mathbb{C} \setminus \{0\}\} = \{z \in \mathbb{C} : |z| = 1\} \tag{98}$$

由群同构定理

$$(\mathbb{C} \setminus \{0\})/\mathbb{R}^+ \cong \partial\mathbb{D} \tag{99}$$

方法二：构造映射

$$\begin{aligned} \varphi : & (\mathbb{C} \setminus \{0\})/\mathbb{R}^+ \to \partial\mathbb{D} && (100)\\ & \rho\mathrm{e}^{i\theta}\mathbb{R}^+ \mapsto \mathrm{e}^{i\theta} && (101)\end{aligned}$$

首先考察此映射的定义良好性。任取$\rho, \varrho \in \mathbb{R}^+$以及$\theta, \vartheta \in \mathbb{R}$，满足$\rho\mathrm{e}^{i\theta}\mathbb{R}^+ = \varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+$，因此$\theta \equiv \vartheta \mod 2\pi$，进而$\varphi(\rho\mathrm{e}^{i\theta}\mathbb{R}^+) = \mathrm{e}^{i\theta} = \mathrm{e}^{i\vartheta} = \varphi(\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+)$，于是$\varphi$是定义良好的。

其次证明φ为群同态映射。任取$\rho, \varrho \in \mathbb{R}^+$以及$\theta, \vartheta \in \mathbb{R}$，注意到

$$\varphi((\rho\mathrm{e}^{i\theta}\mathbb{R}^+)(\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+)) = \varphi(\rho\varrho\mathrm{e}^{i(\theta+\vartheta)}\mathbb{R}^+) = \mathrm{e}^{i(\theta+\vartheta)} = \mathrm{e}^{i\theta}\mathrm{e}^{i\vartheta} = \varphi(\rho\mathrm{e}^{i\theta}\mathbb{R}^+)\varphi(\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+) \tag{102}$$

因此φ为群同态映射。

最后证明φ为双射。任取$\rho, \varrho \in \mathbb{R}^+$以及$\theta, \vartheta \in \mathbb{R}$，注意到

$$\begin{aligned} & \varphi(\rho e^{i\theta}\mathbb{R}^+) = \varphi(\varrho e^{i\vartheta}\mathbb{R}^+) && (103) \\ \implies & e^{i\theta} = e^{i\vartheta} && (104) \\ \implies & e^{i\theta}\mathbb{R}^+ = e^{i\vartheta}\mathbb{R}^+ && (105) \\ \implies & \rho e^{i\theta}\mathbb{R}^+ = \varrho e^{i\vartheta}\mathbb{R}^+, && (106) \\ & && (107) \\ & \varphi(e^{i\theta}\mathbb{R}^+) = e^{i\theta} && (108) \end{aligned}$$

因此φ为双射。

综合以上三点

$$(\mathbb{C} \setminus \{0\})/\mathbb{R}^+ \cong \partial\mathbb{D} \tag{109}$$

1.4.7 第七题

证明：

$$G \times \{e\} \lhd G \times H, \qquad G \times H/G \times \{e\} \cong H \tag{110}$$

证明：构造群同态映射

$$\begin{aligned} \varphi : & G \times H \to H && (111) \\ & (g, h) \mapsto h && (112) \end{aligned}$$

注意到$\mathrm{Ker}\,\varphi = G \times \{e\}, \mathrm{Im}\,\varphi = H$，因此原命题得证！

1.4.8 第八题

证明：

$$H, K < G, \quad G \cong H \times K \implies H \lhd G, \quad G/H \cong K \tag{113}$$

证明：由于$G \cong H \times K$，那么存在同态双射$\varphi \times \psi : G \to H \times K$为$h * k \mapsto (h, k)$，因此对于任意$a, b \in G$，成立

$$\begin{aligned} & (\varphi(a * b), \psi(a * b)) && (114) \\ = & (\varphi \times \psi)(a * b) && (115) \\ = & (\varphi \times \psi)(a) * (\varphi \times \psi)(b) && (116) \\ = & (\varphi(a), \psi(a)) * (\varphi(b), \psi(b)) && (117) \\ = & (\varphi(a) * \varphi(b), \psi(a) * \psi(b)) && (118) \end{aligned}$$

因此$\varphi(a * b) = \varphi(a) * \varphi(b)$且$\psi(a * b) = \psi(a) * \psi(b)$，于是$\varphi : G \to H$和$\psi : G \to K$为同态态射。容易知道$\mathrm{Ker}\,\psi = H$，因此$H \lhd G$且$G/H \cong K$。

1.4.9 第九题

求D_3和D_4的换位子群。

1.4.10 第十题

证明：

$$[D_{2n-1}, D_{2n-1}] = \{\sigma^i : 0 \leq i \leq 2n-2\} \tag{119}$$

$$[D_{2n}, D_{2n}] = \{\sigma^{2i} : 0 \leq i \leq n-1\} \tag{120}$$

证明：

$$\sigma^i\tau^j\sigma^s\tau^t(\sigma^i\tau^j)^{-1}(\sigma^s\tau^t)^{-1} = \begin{cases} \mathbb{1}, & (j,t) = (0,0) \\ \sigma^{-2s}, & (j,t) = (1,0) \\ \sigma^{2i}, & (j,t) = (0,1) \\ \sigma^{2i-2s}, & (j,t) = (1,1) \end{cases} \tag{121}$$

因此

$$[D_n, D_n] = \{\sigma^{2i} : n \in \mathbb{N}^*\} \tag{122}$$

1.4.11 第十一题

求S_4的换位子群。

1.4.12 第十二题

求S_n的换位子群。

1.4.13 第十三题

证明：当$n \geq 5$时，成立$A_n' = A$。

1.4.14 第十四题

写出S_4的导群列。

1.4.15 第十五题

证明：如果置换群G含有奇置换，那么G存在指数为2的子群。

1.4.16 第十六题

1.4.16.1 第一问

对于满的群同态映射$\varphi: G \to H$，证明：如果$J < H$，那么$\mathrm{Ker}\, \varphi \subset \varphi^{-1}(J) < G$。

1.4.16.2 第二问

对于满的群同态映射$\varphi: G \to H$，定义映射

$$\Phi : \{J : J < H\} \to \{K : \mathrm{Ker}\, \varphi \subset K < G\} \tag{123}$$
$$J \mapsto \varphi^{-1}(J) \tag{124}$$

证明：Φ为双射。

1.4.17 第十七题

证明：当$n \geq 5$时，A_n为单群。

1.4.18 第十八题

半直积：称群G为正规子群N和子群H的半直积，且记作$G = N \rtimes H$，如果满足如下命题之一。

1. $G = NH$，且$N \cap H = \{e\}$。
2. $G/N \cong H$

1.4.19 第十九题

证明：当$n \geq 3$时，S_n为A_n与$\langle (12) \rangle$的半直积。

1.5 第五节

1.5.1 第一题

定义映射

$$\varphi : \mathbb{Z} \times \mathbb{R} \to \mathbb{R} \tag{125}$$
$$(n, x) \mapsto n + x \tag{126}$$

证明：φ为群$(\mathbb{Z}, +)$关于$\mathbb{R}$的作用。

证明：注意到

$$\begin{gathered} \varphi(0, x) = 0 + x = x \\ \varphi(m+n, x) = (m+n) + x = m + (n+x) = \varphi(m, \varphi(n, x)) \end{gathered} \tag{127}$$

1.5.2 第二题

定义映射

$$\varphi : \mathbb{Z} \times \mathbb{R} \to \mathbb{R} \tag{128}$$
$$(n, x) \mapsto (-1)^n x \tag{129}$$

证明：φ为群$(\mathbb{Z}, +)$关于$\mathbb{R}$的作用。

证明：注意到

$$\begin{gathered} \varphi(0, x) = (-1)^0 x = x \\ \varphi(m+n, x) = (-1)^{m+n} x = (-1)^m((-1)^n x) = \varphi(m, \varphi(n, x)) \end{gathered} \tag{130}$$

1.5.3 第三题

证明：映射$\varphi(x) = x^{-1}$为Abel群G的自同构映射。

证明：注意到

$$\begin{gathered} \varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y) \\ \varphi \circ \varphi = \mathbb{1} \end{gathered} \tag{131}$$

1.5.4 第四题

求$\mathrm{GL}_n(\mathbb{F})$的中心。

解：

$$\mathrm{Z}(\mathrm{GL}_n(\mathbb{F})) = \{M \in \mathrm{GL}_n(\mathbb{F}) : AM = MA, \forall A \in \mathrm{GL}_n(\mathbb{F})\} = \{\lambda I_n : \lambda \in \mathbb{F}\} \tag{132}$$

1.5.5 第五题

对于$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_n(\mathbb{C})$，定义Möbius变换

$$\mu_{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} : \overline{\mathbb{C}} \to \overline{\mathbb{C}} \tag{133}$$
$$z \mapsto \frac{az+b}{cz+d} \tag{134}$$

1.5.5.1 第一问

记$\mathcal{MT} = \{\mu_M : M \in \mathrm{GL}_n(\mathbb{F})\}$，证明：$M$关于复合运算构成群。

证明：注意到

$$\mu_A \circ \mu_B = \mu_{AB}, \qquad \mu_{\lambda M} = \mu_M \tag{135}$$

因此

$$\mu_I \circ \mu_M = \mu_M \circ \mu_I = \mu_M \tag{136}$$
$$\mu_{M^{-1}} \circ \mu_M = \mu_M \circ \mu_{M^{-1}} = \mu_I \tag{137}$$
$$(\mu_A \circ \mu_B) \circ \mu_C = \mu_A \circ (\mu_B \circ \mu_C) = \mu_{ABC} \tag{138}$$

进而$\mathcal{MT}$构成群。

1.5.5.2 第二问

证明：$\mathrm{GL}_n(\mathbb{C})/\mathrm{Z}(\mathrm{GL_n}(\mathbb{C})) \cong \mathcal{MT}$

证明：定义映射

$$\varphi : \mathrm{GL}_n(\mathbb{C}) \to \mathcal{MT} \tag{139}$$
$$M \mapsto \mu_M \tag{140}$$

注意到

$$\varphi(AB) = \mu_{AB} = \mu_A \circ \mu_B = \varphi(A) \circ \varphi(B) \tag{141}$$

从而φ为群同态映射。而

$$\mathrm{Ker}\, \varphi = \{M \in \mathrm{GL}_n(\mathbb{C}) : \mu_M = \mu_I\} = \{\lambda I : \lambda \in \mathbb{C}\} = \mathrm{Z}(\mathrm{GL_n}(\mathbb{C})) \tag{142}$$
$$\mathrm{Im}\, \varphi = \mathcal{MT} \tag{143}$$

进而由同构定理，成立$\mathrm{GL}_n(\mathbb{C})/\mathrm{Z}(\mathrm{GL}_\mathrm{n}(\mathbb{C}))\cong\mathcal{MT}$。

1.5.6 第六题

证明：$G/\mathrm{Z}(G)$为循环群$\iff G$为Abel群

证明：由于$G/\mathrm{Z}(G)\cong\mathrm{Inn}(G)$，只需证明$\mathrm{Inn}(G)$为循环群$\iff G$为Abel群。

我们来证明

$$\mathrm{Inn}(G)\text{ is cyclic}\iff\mathrm{Inn}(G)\text{ is trivial}\iff G\text{ is abelian}\tag{144}$$

如果G是Abel群，那么对于任意$g\in G$，$\gamma_g=\mathbb{1}_G$，因此$\mathrm{Inn}(G)=\{\mathbb{1}_G\}$为平凡群。

如果$\mathrm{Inn}(G)=\{\mathbb{1}_G\}$为平凡群，那么显然$\mathrm{Inn}(G)=\{\mathbb{1}_G\}\cong\mathbb{Z}_1$为循环群。

如果$\mathrm{Inn}(G)$为循环群，那么存在$g_0\in G$，使得对于任意$g\in G$，存在$n\in\mathbb{Z}$，使得成立$\gamma_g=\underbrace{\gamma_{g_0}\circ\cdots\circ\gamma_{g_0}}_{n\text{ times}}$，因此对于任意$g\in G$，成立$g*g*g^{-1}=g_0^n*g*g_0^{-n}$。取$g=g_0$，可得$g*g_0=g_0*g$，因此$\gamma_{g_0}=\mathbb{1}_G$，于是对于任意$g\in G$，$\gamma_g=\mathbb{1}_G$，因此$\mathrm{Inn}(G)=\{\mathbb{1}_G\}$为平凡群。

如果$\mathrm{Inn}(G)=\{\mathbb{1}_G\}$为平凡群，那么对于任意$g\in G$，$\varphi(g)=\gamma_g=\mathbb{1}_G$，因此对于任意$g\in G$，成立$\gamma_g(g)=g$，于是

$$g^{-1}*g*g=g\implies g*g=g*g\tag{145}$$

进而G是交换的。

1.5.7 第七题

证明：

$$\mathrm{Z}(D_{2n-1})=\{\mathbb{1}\},\qquad\mathrm{Z}(D_{2n})=\{\mathbb{1},\sigma^n\}\tag{146}$$

1.6 第六节

1.6.0 引理

证明：对于素数p,q，如果$(p,q)=1$，且$(p^m-1)!<q^n$，那么p^mq^n阶群不为单群，其中$m,n\in\mathbb{N}^*$。

证明：设群$|G|=p^mq^n$，由Sylow第三定理，G至多存在p^k个Sylow p-子群，其中$0\le k\le m$。

如果G仅存在1个Sylow p-子群，那么该子群为非平凡正规子群。

如果G存在p^k个Sylow p-子群，其中$1\le k\le m$，设为$\Omega=\{P_i\}_{i=1}^{p^k}$，考虑$G$在$\Omega$上的共轭作用$(x,P_i)=xP_ix^{-1}$，诱导群同态$\Psi:G\to S_{p^k},\quad x\mapsto\psi_x$，其中$\psi_x:S_{p^k}\to S_{p^k},\quad P_i\mapsto xP_ix^{-1}$。由群同构定理，$G/\mathrm{Ker}\ \Psi\cong\mathrm{Im}\ \Psi$。由于$\mathrm{Im}\Psi<S_{p^k}$，因此$|\mathrm{Im}\Psi|\le p^k!$。如果$\mathrm{Ker}\ \Psi=\{e\}$，那么$|\mathrm{Im}\Psi|=|G|/|\mathrm{Ker}\Psi|=|G|=p^mq^n>p^m!\ge p^k!$，矛盾！如果$\mathrm{Ker}\ \Psi=G$，那么对于任意$x\in G$，$\psi_x=\mathbb{1}$，因此$xP_1=P_1x$，于是$P_1\triangleleft G$。由Sylow第二定理，$G$仅存在1个Sylow p-子群，矛盾！进而$\mathrm{Ker}\ \Psi$为G的非平凡正规子群。

综上所述，G存在非正规子群，因此G不为单群。

1.6.1 第一题

证明：不存在阶为148的单群。

证明：

$$148=2^2\times47,\qquad(2^2-1)!<47\tag{147}$$

1.6.2 第二题

证明：不存在阶为36的单群。

证明：

$$36=2^2\times3^2,\qquad(2^2-1)!<3^2\tag{148}$$

1.6.3 第三题

证明：不存在阶为56的单群。

证明：

$$56 = 2^3 \times 7 \tag{149}$$

设$|G| = 56$，那么由Sylow第三定理，G存在1个或8个Sylow 7子群。

如果G仅存在1个Sylow 7-子群，那么该子群为非平凡正规子群。

如果G存在8个Sylow 7-子群，那么

1.6.4 第四题

证明：不存在阶为30的单群。

1.6.5 第五题

证明：6阶群或为$\mathbb{Z}_6$，或为D_3。

1.6.6 第六题

证明：10阶群的结构。

1.6.7 第七题

证明：15阶群的结构。

1.6.8 第八题

证明：35阶群的结构。

1.6.9 第九题

证明：21阶群的结构。

1.6.10 第十题

证明：对于素数p, q，如果$q > p$且$p \nmid q-1$，那么pq阶群为$\mathbb{Z}_{pq}$。

证明：设$|G| = pq$，那么由Sylow定理，G存在且仅存在唯一p阶子群H，存在且存在唯一q阶子群K，那么$H, K \lhd G$，且$H \cap K = \{e\}$。

设$H = \{a^i : 0 \leq i < p\}$，$K = \{b^j : 0 \leq j < q\}$。注意到$a^i b^j = a^k b^l \implies a^{i-k} = b^{l-j} \in H \cap K = \{e\}$，因此$i = k, j = l$，那么$G = \{a^i b^j : 0 \leq i < p, 0 \leq j < q\}$。

由于$K \lhd G$，那么$aKa^{-1} = K$，因此定义$\varphi(x) = axa^{-1}$，因此$\varphi \in \mathrm{Aut}(K) \cong \mathbb{Z}_{q-1}$，因此$\varphi^{q-1} = \mathbb{1}$。而$\varphi^p(x) = a^p x a^{-p} = x$，因此$\varphi^p = \mathbb{1}$。因为$p \nmid q-1$，因此$\varphi = \mathbb{1}$，进而$ab = ba$，进而$G \cong \mathbb{Z}_{pq}$。

第二章：环

2.1 第一节

2.1.1 第一题

对于域F，令$S=\left\{\begin{pmatrix} a & 0 \\ 0 & 0\end{pmatrix}:a\in F\right\}$，证明：$S$为$M_n(F)$的子环。

证明：显然！

2.1.2 第二题

证明：有限整环为域。

证明：对于有限整环R，任取$r\in R\setminus\{0\}$，考虑$rR\subset R$。如果$|rR|<|R|$，那么存在互异元素$a,b\in R$，使得成立$ar=br$。由消去律，$a=b$，矛盾！因此$|rR|=|R|$，那么$rR=R$。注意到$1\in R=rR$，那么存在$s\in R$，使得成立$rs=sr=1$，进而R为域。

2.1.3 第三题

证明：$R=\left\{\begin{pmatrix} a & b \\ -\overline{b} & \overline{a}\end{pmatrix}:a,b\in\mathbb{C}\right\}$为除环。

证明：显然$(H,+)$为交换群。

乘法单位元为$\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$，乘法结合律、分配律显然，

注意到

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a}\end{pmatrix}\begin{pmatrix} c & d \\ -\overline{d} & \overline{c}\end{pmatrix}=\begin{pmatrix} ac-b\overline{d} & ad+b\overline{c} \\ -\overline{ad}-\overline{b}c & \overline{ac}-\overline{b}d\end{pmatrix} \tag{150}$$

因此

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a}\end{pmatrix}\begin{pmatrix} \frac{\overline{a}}{|a|^2+|b^2|} & -\frac{b}{|a|^2+|b^2|} \\ \frac{\overline{b}}{|a|^2+|b^2|} & \frac{a}{|a|^2+|b^2|}\end{pmatrix}=\begin{pmatrix} \frac{\overline{a}}{|a|^2+|b^2|} & -\frac{b}{|a|^2+|b^2|} \\ \frac{\overline{b}}{|a|^2+|b^2|} & \frac{a}{|a|^2+|b^2|}\end{pmatrix}\begin{pmatrix} a & b \\ -\overline{b} & \overline{a}\end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} \tag{151}$$

2.1.4 第四题

证明：对于幺环R的理想I，成立$1\in I\iff I=R$。

证明：显然！

2.1.5 第五题

证明：证明：域没有非平凡理想。

证明：如果R为域，任取R的非零理想I，那么存在$r\in I\setminus\{0\}$，而R为域，因此$1=r^{-1}r\in I$，那么$I=R$，进而R仅存在平凡理想。

2.1.6 第六题

证明：如果交换幺环R没有非平凡理想，那么R为域。

证明：反证，如果R不为域，那么存在$r_0\in R\setminus\{0\}$，使得对于任意$r\in R$，成立$r_0\cdot r\neq 1$。考虑主理想(r_0)，由条件假设，$1\notin(r_0)$，因此$\{0\}\subsetneq(r_0)\subsetneq R$，进而$R$存在非平凡理想$(r_0)$，矛盾！从而$R$为域。

2.1.7 第七题

对于交换环R的理想I，定义$\mathrm{rad}\ I=\{r\in R:\exists n\in\mathbb{N}^*,r^n\in I\}$，证明：$\mathrm{rad}\ I$为环$R$的理想。

证明：首先，任取$a,b\in\mathrm{rad}\ I$，那么存在$m,n\in\mathbb{N}^*$，使得$a^m,b^n\in I$，注意到

$$(a-b)^{m+n}=\sum_{k=0}^{m+n}C_{m+n}^k a^k b^{m+n-k}\in I \tag{152}$$

因此$a-b\in\mathrm{rad}\ I$，进而$(\mathrm{rad}\ I,+)$为子群。

其次，任取$r \in R$，注意到

$$(ra)^n = r^n a^n \in I \tag{153}$$

因此$ra \in \text{rad } I$，进而$\text{rad } I$为理想。

2.1.8 第八题

证明：对于幺环R，如果$a \in R$存在$n \in \mathbb{N}^*$，使得成立$a^n = 0$，那么存在b，使得成立$(1-a)b = b(1-a) = 1$。

证明：注意到

$$\frac{1}{1-a} = \sum_{m=0}^{\infty} a^m \tag{154}$$

因此

$$1 = (1-a)\sum_{m=0}^{\infty} a^m = (1-a)\sum_{m=0}^{n} a^m \tag{155}$$

2.1.9 第九题

证明：对于交换环R，集合$\text{rad } 0 = \{r \in R : \exists n \in \mathbb{N}^*, r^n = 0\}$为环$R$的理想。

证明：见2.1.7

2.1.10 第十题

证明：对于除环D，$M_n(D)$为单环。

2.2 第二节

2.2.1 第一题

证明：$R \cong \mathbb{H}$，其中

$$R = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\} \tag{156}$$

证明：构造映射

$$\begin{aligned} \varphi : \quad & \mathbb{H} \longrightarrow R \\ a + bi + cj + dk & \longmapsto \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \end{aligned} \tag{157}$$

注意到

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{158}$$

$$\begin{aligned}
&\varphi((a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k)) && (159)\\
=&\varphi((a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k) && (160)\\
=&\begin{pmatrix} (a_1 + a_2) + (b_1 + b_2)i & (c_1 + c_2) + (d_1 + d_2)i \\ -(c_1 + c_2) + (d_1 + d_2)i & (a_1 + a_2) - (b_1 + b_2)i \end{pmatrix} && (161)\\
=&\begin{pmatrix} a_1 + b_1 i & c_1 + d_1 i \\ -c_1 + d_1 i & a_1 - b_1 i \end{pmatrix} + \begin{pmatrix} a_2 + b_2 i & c_2 + d_2 i \\ -c_2 + d_2 i & a_2 - b_2 i \end{pmatrix} && (162)\\
=&\varphi(a_1 + b_1 i + c_1 j + d_1 k) + \varphi(a_2 + b_2 i + c_2 j + d_2 k) && (163)
\end{aligned}$$

$$\begin{aligned}
&\varphi((a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)) && (164)\\
=&\varphi((a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2)i && (165)\\
&+ (a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2)j + (-b_2 c_1 + b_1 c_2 + d_2 d_1 + a_1 + d_2)k) && (166)\\
=&\begin{pmatrix} \begin{pmatrix} (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) \\ +(a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2)i \end{pmatrix} & \begin{pmatrix} (a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2) \\ +(-b_2 c_1 + b_1 c_2 + d_2 d_1 + a_1 + d_2)i \end{pmatrix} \\ \begin{pmatrix} -(a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2) \\ +(-b_2 c_1 + b_1 c_2 + d_2 d_1 + a_1 + d_2)i \end{pmatrix} & \begin{pmatrix} (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) \\ -(a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2)i \end{pmatrix} \end{pmatrix} && (167)\\
=&\begin{pmatrix} a_1 + b_1 i & c_1 + d_1 i \\ -c_1 + d_1 i & a_1 - b_1 i \end{pmatrix}\begin{pmatrix} a_2 + b_2 i & c_2 + d_2 i \\ -c_2 + d_2 i & a_2 - b_2 i \end{pmatrix} && (168)\\
=&\varphi(a_1 + b_1 i + c_1 j + d_1 k)\varphi(a_2 + b_2 i + c_2 j + d_2 k) && (169)
\end{aligned}$$

因此φ为环同态映射。

而显然φ为双射，因此$R \cong \mathbb{H}$。

2.2.2 第二题

2.2.2.1 第一问

证明：对于满的环同态映射$\varphi : R \to S$，如果I为R的理想，那么$\varphi(I)$为S的理想。

证明：任取$a, b \in I$，那么$a - b \in I$，进而

$$\varphi(a) - \varphi(b) = \varphi(a - b) \in \varphi(I) \tag{170}$$

任取$r \in R$，那么$ar, ra \in I$，进而

$$\varphi(r)\varphi(a) = \varphi(ra) \in \varphi(I), \qquad \varphi(a)\varphi(r) = \varphi(ar) \in \varphi(I) \tag{171}$$

因此$\varphi(I)$为S的理想。

2.2.2.2 第二问

证明：对于满的环同态映射$\varphi : R \to S$，如果I为S的理想，那么$\varphi^{-1}(I)$为R的理想，且$\mathrm{Ker}\ \varphi \subset \varphi^{-1}(I)$。

证明：任取$a, b \in \varphi^{-1}(I)$，那么

$$\varphi(a - b) = \varphi(a) - \varphi(b) \in I \implies a - b \in \varphi^{-1}(I) \tag{172}$$

任取$r \in R$，那么$\varphi(a)\varphi(r), \varphi(r)\varphi(a) \in I$，进而

$$\varphi(ar) = \varphi(a)\varphi(r) \in I, \qquad \varphi(ra) = \varphi(r)\varphi(a) \in I \implies ar, ra \in \varphi^{-1}(I) \tag{173}$$

因此$\varphi^{-1}(I)$为R的理想。而$\{0\} \subset I$，因此$\mathrm{Ker}\ \varphi \subset \varphi^{-1}(I)$。

2.2.3 第三题

求解如下同余方程：

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases} \tag{174}$$

解：注意到

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 0 \mod 5 \\ x \equiv 0 \mod 7 \end{cases} \iff x \equiv 70 \mod 105 \tag{175}$$

$$\begin{cases} x \equiv 0 \mod 3 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 7 \end{cases} \iff x \equiv 21 \mod 105 \tag{176}$$

$$\begin{cases} x \equiv 0 \mod 3 \\ x \equiv 0 \mod 5 \\ x \equiv 1 \mod 7 \end{cases} \iff x \equiv 15 \mod 105 \tag{177}$$

因此

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases} \iff x \equiv 23 \mod 105 \tag{178}$$

2.2.4 第四题

2.2.4.1 第一问

求方程$x^2 = 1$在$\mathbb{Z}_{35}$中的根。

解：

$$\overline{1}, \qquad \overline{6}, \qquad \overline{29}, \qquad \overline{34} \tag{179}$$

2.2.4.2 第二问

求方程$x^2=4$在$\mathbb{Z}_{35}$中的根。

解：

$$\overline{2},\qquad \overline{13},\qquad \overline{22},\qquad \overline{33} \tag{180}$$

2.2.5 第五题

2.2.5.1 第一问

证明：方程$x^2=2$在$\mathbb{Z}_{35}$中不存在根。

2.2.5.2 第二问

证明：方程$x^2=3$在$\mathbb{Z}_{35}$中不存在根。

2.3 第三节

2.3.1 第一题

证明：域F上一元多项式环$F[x]$的理想为主理想，其中非(0)主理想可以由首一多项式生成。

证明：取$F[x]$的理想I，如果$I=\{0\}$为平凡理想，那么$I=(0)$。如果$I\neq\{0\}$，那么取I中次数最小的非零首一多项式$g(x)$。对于任意$f(x)\in I$，作带余除法，成立$f(x)=g(x)q(x)+r(x)$，其中$\deg(r(x))<\deg(g(x))$。注意到$r(x)=f(x)-g(x)q(x)\in I$，因此$r(x)=0$，进而$f(x)=g(x)q(x)$。由$f(x)$的任意性，$I=(g(x))$。

2.3.2 第二题

证明：对于非零交换幺环R，如果S为R的子环，P为R的素理想，那么$S\cap P$为S的素理想。

证明：首先证明$S\cap P$为S的理想，任取$x\in S\cap P$，以及$s\in S$，成立

$$xs\in S, xs\in P\implies xs\in S\cap P \tag{181}$$

于是$S\cap P$为S的理想。而$P\neq S$，于是$1\notin P$，但是$1\in S$，因此$S\cap P\neq S$。任取$x,y\in S$，注意到

$$xy\in S\cap P\implies xy\in P\implies x\in P\text{或}y\in P\implies xy\in S\cap P\text{或}xy\in S\cap P \tag{182}$$

2.3.3 第三题

证明：

$$\operatorname{Spec}\mathbb{Z}/(30)=\{(2)/(30),(3)/(30),(5)/(30)\} \tag{183}$$

证明：如下集合函数为双射。

$$\begin{aligned}\Phi:\{I\supset(30)\text{ 为 }\mathbb{Z}\text{ 的素理想}\}&\longrightarrow\operatorname{Spec}\mathbb{Z}/(30)\\ I&\longmapsto I/(30)\end{aligned} \tag{184}$$

而满足$I\supset(30)$的$\mathbb{Z}$的素理想仅为$I=(2),(3),(5)$，因此

$$\operatorname{Spec}\mathbb{Z}/(30)=\{(2)/(30),(3)/(30),(5)/(30)\} \tag{185}$$

2.3.4 第四题

证明：对于域F，如果$p(x)$为$F[x]$的不可约多项式，那么$F[x]/(p(x))$为域。

证明：$F[x]/(p(x))$为域$\iff$ $(p(x))$为$F[x]$的极大理想。任取$F[x]$的理想$I\supsetneq(p(x))$，由于$F[x]$为主理想整环，那么存在$f(x)$，使得成立

$$I=(f(x))\implies p(x)\in(f(x))\implies f(x)\mid p(x)\implies f(x)=c\text{或}f(x)=ap(x)\implies I=F[x]\text{或}I=(p(x)) \tag{186}$$

因此$(p(x))$为$F[x]$的极大理想，进而$F[x]/(p(x))$为域。

2.3.5 第五题

证明：对于域F，如果$f(x)$为$F[x]$的可约多项式，那么$F[x]/(f(x))$存在非平凡零因子。

证明：这几乎是显然的。

$$f(x)=f_1(x)f_2(x)\implies(f_1(x)+(f(x)))(f_2(x)+(f(x)))=f_1(x)f_2(x)+(f(x))=f(x)+(f(x))=(f(x)) \tag{187}$$

2.3.6 第六题

构造含4个元素的有限域。

2.3.7 第七题

构造含9个元素的有限域。

2.3.8 第八题

构造含8个元素的有限域。

解：由于$\mathbb{Z}_2$为2阶域，那么取$\mathbb{Z}_2[x]$中的3次不可约多项式x^3+x+1，因此$\mathbb{Z}_2[x]/(x^3+x+1)$为8阶有限域，其中对于任意$f(x)\in\mathbb{Z}_2[x]/(x^3+x+1)$，存在且存在唯一$a_0,a_1,a_3\in\mathbb{Z}_2$，使得成立

$$f(x)=a_0+a_1x+a_2x^2+(x^3+x+1) \tag{188}$$

2.3.9 第九题

证明：$4\mathbb{Z}$为$2\mathbb{Z}$的极大理想，但是$2\mathbb{Z}/4\mathbb{Z}$不为域。

证明：取$2\mathbb{Z}$的理想$I\supset 4\mathbb{Z}$，而4的素因子仅有2，那么$I=4\mathbb{Z}$或$I=2\mathbb{Z}$，进而$4\mathbb{Z}$为$2\mathbb{Z}$的极大理想。

注意到

$$(2+4\mathbb{Z})(2+4\mathbb{Z})=4+4\mathbb{Z}=4\mathbb{Z} \tag{189}$$

因此$2\mathbb{Z}/4\mathbb{Z}$不为域。

2.4 第四节

2.4.1 第一题

证明：对于任意$m,n\in\mathbb{Z}$，$m+ni$为代数整数。

证明：令

$$f(x)=x^2-2mx+(m^2+n^2) \tag{190}$$

于是

$$f(m+ni)=0 \tag{191}$$

2.4.2 第二题

证明：$\sqrt{2}+\sqrt{3}$为代数数，并求$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上的极小多项式。

证明：注意到

$$\begin{aligned}
x&=\sqrt{2}+\sqrt{3} &(192)\\
\Longrightarrow (x-\sqrt{2})^3&=3 &(193)\\
\Longleftrightarrow x^2-1&=2\sqrt{2}x &(194)\\
\Longrightarrow (x^2-1)^2&=8x^2 &(195)\\
\Longleftrightarrow x^4-10x^2+1&=0 &(196)
\end{aligned}$$

因此$\sqrt{2}+\sqrt{3}$为整系数方程x^4-10x^2+1的根，因此$\sqrt{2}+\sqrt{3}$为代数数，且

$$x^4-10x^2+1=(x+(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}+\sqrt{3}))(x+(\sqrt{3}-\sqrt{2}))(x+(\sqrt{2}-\sqrt{3})) \tag{197}$$

因此x^4-10x^2+1为$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上的极小多项式。

2.4.3 第三题

设$t\in\mathbb{C}$为$f(x)=x^3-x+1$的根，在代数数域$\mathbb{Q}[t]$中求

$$(5t^2+3t-1)(2t^2-2t+6),\qquad (3t^2-t+2)^{-1} \tag{198}$$

解：由于$t^3=t-1$，那么

$$
\begin{aligned}
(5t^2+3t-1)(2t^2-2t+6) =&10x^4-4x^3+22x^2+20x-6 && (199)\\
=&10t(t-1)-4(t-1)+22t^2+20t-6 && (200)\\
=&32t^2+6t-2 && (201)
\end{aligned}
$$

令

$$
\begin{aligned}
& (3t^2-t+2)(at^2+bt+c)=1 && (202)\\
\iff & 3at^4+(3b-a)t^3+(2a-b+3c)t^2+(2b-c)t+(2c-1)=0 && (203)\\
\iff & 3at(t-1)+(3b-a)(t-1)+(2a-b+3c)t^2+(2b-c)t+(2c-1)=0 && (204)\\
\iff & (5a-b+3c)t^2+(-4a+5b-c)t+(a-3b+2c-1)=0 && (205)\\
\iff & \begin{cases} 5a-b+3c=0 \\ -4a+5b-c=0 \\ a-3b+2c=1 \end{cases} && (206)\\
\iff & a=-\frac{2}{7}, b=-\frac{1}{7}, c=\frac{3}{7} && (207)
\end{aligned}
$$

因此

$$
(3t^2-t+2)^{-1}=(-2t^2-t+3)/7 \tag{208}
$$

2.4.4 第四题

由于$f(x)=x^3+2x^2+x+3$为$\mathbb{Z}_4[x]$中的基本不可约多项式，那么$\mathbb{Z}_4[x]/(f(x))$为Galois环$\mathrm{GR}(2^2,3)$。

2.4.4.1 第一问

证明：$\mathbb{Z}_4[x]/(f(x))$不为整环。

证明：由于

$$
2x+1 \notin (f(x)), \qquad 2x^2-2x+3 \notin (f(x)) \tag{209}
$$

但是

$$
(2x+1)(2x^2-2x+3)=4x \tag{210}
$$

2.4.4.2 第二问

求$x+(f(x))$在$\mathbb{Z}_4[x]/(f(x))$的单位群中的阶。

证明：

$$
\begin{aligned}
x^1 &= x && (211)\\
x^2 &= x^2 && (212)\\
x^3 &= 2x^2+3x+1 && (213)\\
x^4 &= 3x^2+3x+2 && (214)\\
x^5 &= x^2+3x+3 && (215)\\
x^6 &= x^2+2x+1 && (216)\\
x^7 &= 1 && (217)
\end{aligned}
$$

2.6 第六节

2.6.1 第一题

对于$\mathbb{Z}[\sqrt{5}i]=\{a+b\sqrt{5}i : a,b\in\mathbb{Z}\}$，定义范数$\|a+b\sqrt{5}i\|=a^2+5b^2$。

2.6.1.1 第一问

证明：

$$
a+b\sqrt{5}i \text{ 为 } \mathbb{Z}[\sqrt{5}i] \text{ 的单位} \quad \iff \quad \|a+b\sqrt{5}i\|=1 \tag{218}
$$

证明：

$$
\begin{aligned}
& a+b\sqrt{5}i \text{ 为 } \mathbb{Z}[\sqrt{5}i] \text{ 的单位} && (219)\\
\iff & \text{存在 } c,d\in\mathbb{Z},\text{ 使得成立 } (a+b\sqrt{5}i)(c+d\sqrt{5}i)=1 && (220)\\
\iff & \text{存在 } c,d\in\mathbb{Z},\text{ 使得成立 } (ac-5bd-1)+(ad+bc)\sqrt{5}i=0 && (221)\\
\iff & \text{存在 } c,d\in\mathbb{Z},\text{ 使得成立 } ac-5bd=1 \text{ 且 } ad+bc=0 && (222)\\
\iff & \text{存在 } c,d\in\mathbb{Z},\text{ 使得成立 } c=\frac{a}{a^2+5b^2} \text{ 且 } d=\frac{-b}{a^2+5b^2} && (223)\\
\iff & a^2+5b^2 \mid a \text{ 且 } a^2+5b^2 \mid b && (224)\\
\iff & a^2+5b^2=1 && (225)\\
\iff & \|a+b\sqrt{5}i\|=1 && (226)
\end{aligned}
$$

2.6.1.2 第二问

证明：

$$\|a+b\sqrt{5}i\|=9 \implies a+b\sqrt{5}i \text{ 为 } \mathbb{Z}[\sqrt{5}i] \text{ 的不可约元} \tag{227}$$

证明：

$$\|a+b\sqrt{5}i\|=9 \iff a+5b^2=9 \implies b^2\le\frac{9}{5} \implies |b|=0,1 \implies (|a|,|b|)=(3,0),(2,1) \tag{228}$$

任取$a+b\sqrt{5}i$的因子$c+d\sqrt{5}i$，那么

$$\frac{a+b\sqrt{5}i}{c+d\sqrt{5}i}=\frac{ac+5bd}{c^2+5d^2}+\frac{bc-ad}{c^2+5d^2}\sqrt{5}i\in\mathbb{Z}[\sqrt{5}i] \tag{229}$$

因此

$$c^2+5d^2 \mid ac+5bd, \qquad c^2+5d^2 \mid bc-ad \tag{230}$$

当$(a,b)=(3,0)$时，成立

$$c^2+5d^2 \mid 3c, \qquad c^2+5d^2 \mid 3d \tag{231}$$

2.6.1.3 第三问

证明：3和$2\pm\sqrt{5}i$不为$\mathbb{Z}[\sqrt{5}i]$的素元。

2.6.1.4 第四问

证明：$\mathbb{Z}[\sqrt{5}i]$不为唯一因子分解整环。