第5章 群参考答案

计算证明

1. 判断下列函数关系中哪些是函数？哪些是满射？哪些是单射？对于其中的每一个函数写出逆函数.

（1）$f_1 : \mathbb{Z}^+ \to \mathbb{Z}^+, \quad f_1(x) = x^2 + 1$；

（2）$f_2 : \mathbb{Z}^+ \cup \{0\} \to \mathbb{Q}, \quad f_2(x) = \dfrac{1}{x}$；

（3）$f_3 : 1, 2, 3 \to \alpha, \beta, \gamma, \quad f_3 = \{< 1, \alpha >, < 2, \beta >, < 3, \gamma >\}$

解　f_2 不是映射。f_1，f_3 是函数，其中 f_3 是满射，f_1，f_3 都是单射。

其中 f_1 不存在逆函数，f_3 的逆函数为$f_3^{-1} : \alpha, \beta, \gamma \to 1, 2, 3, \quad f_3^{-1} = \{< \alpha, 1 >, < \beta, 2 >, < \gamma, 3 >\}$

2. 给定实数域上的 n 阶方阵 $\mathbf{A}$ ，$\mathbf{T}$为实数域上的任意 n 阶方阵，证明：映射$f : \mathbf{T} \mapsto \mathbf{AT}$ 是单射当且仅当 $\det(\mathbf{A}) \neq 0$.

证明　充分性. 设 $\mathbf{T}_1$，$\mathbf{T}_2 \in \mathbb{R}^{n\times n}$，若 $\mathbf{AT}_1 = \mathbf{AT}_2$ ，则有 $\mathbf{A}(\mathbf{T}_1 - \mathbf{T}_2) = \mathbf{0}$. 由于 $\det(\mathbf{A}) \neq 0$，得到$\mathbf{A}$ 可逆，即存在逆矩阵 $\mathbf{A}^{-1}$。将上式两边同时左乘 $\mathbf{A}^{-1}$，得到 $\mathbf{T}_1 - \mathbf{T}_2 = \mathbf{0}$，即 $\mathbf{T}_1 = \mathbf{T}_2$. 故 f 为单射.

必要性. 反证. 假设 $\det(\mathbf{A}) = 0$，即 $\mathbf{A}$ 是奇异矩阵。存在方阵 $\mathbf{T}' \neq \mathbf{0}$，使得 $\mathbf{AT}' = \mathbf{0}$.令 $\mathbf{T}_1 = \mathbf{0}$，$\mathbf{T}_2 = \mathbf{T}'$，则有 $\mathbf{AT}_1 = \mathbf{AT}_2 = \mathbf{0}$. 而 $\mathbf{T}_1 \neq \mathbf{T}_2$，与 f 是单射矛盾，故 $\det(\mathbf{A}) \neq 0$. 证毕.

3. 给定任意集合 S，定义 2^S为所有 S 子集构成的集合，称为 S 的幂集（有时也记作 $\rho(S)$，如取 $S = \{1, 2\}$，则幂集 $2^S = \rho(S) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$），证明：

（1）$(2^S, \bigcup)$和$(2^S, \bigcap)$为半群；

（2）若对S 的子集定义运算$A\Delta B = (A\backslash B)\bigcup(B\backslash A)$，则$(2^S, \Delta)$ 为群. （明确：$A\backslash B = \{x|x \in A \wedge x \notin B\}$）

证明　（1）i. 封闭性：由幂集的定义易知，其中任意的元素的并和交一定在幂集中.

ii. 结合律：由集合并和交的运算满足结合律可知，对任意 $A, B, C \in 2^S$， $(A\bigcup B)\bigcup C = A\bigcup(B\bigcup C)$，$(A\bigcap B)\bigcap C = A\bigcap(B\bigcap C)$.

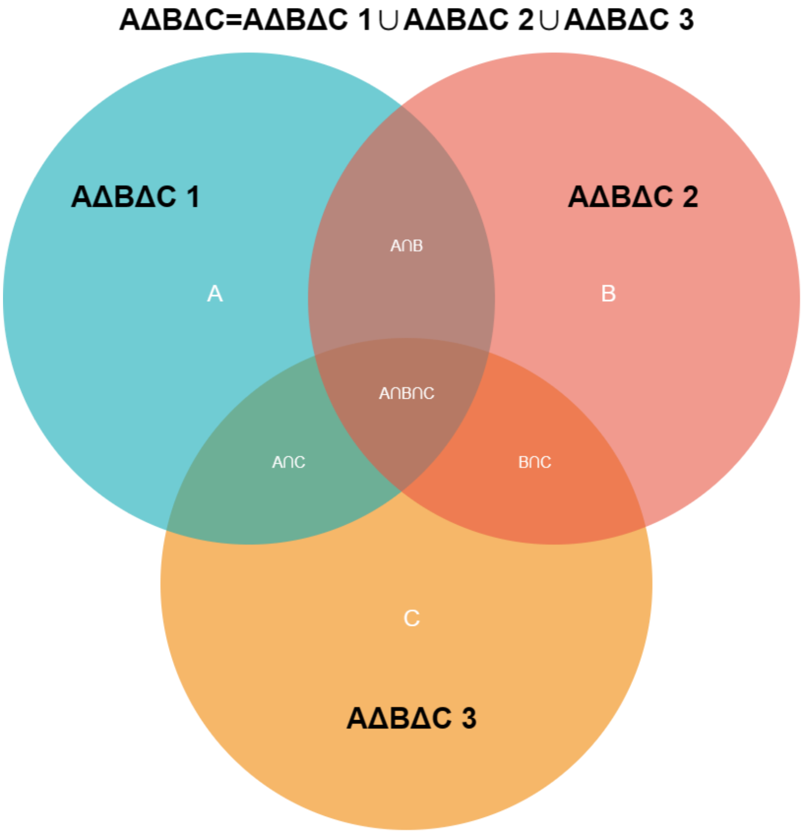
综上，$(2^S, \bigcup)$和$(2^S, \bigcap)$为半群. 证毕.

（2）i. 封闭性：由运算定义可知，$A\Delta B = (A\backslash B)\bigcup(B\backslash A) \subseteq A\bigcup B \in 2^S$.

ii. 结合律：对 $\forall A, B, C \in 2^S$，

$$(A\Delta B)\Delta C = (((A\backslash B)\bigcup(B\backslash A))\backslash C)\bigcup(C\backslash((A\backslash B)\bigcup(B\backslash A))) = ((A\backslash((B\backslash C)\bigcup(C\backslash B))\bigcup((C\backslash B)\bigcup(C\backslash B))\backslash A)) = A\Delta(B\Delta C)$$

（提示：可使用Venn图简化推导）



iii. 幺元：对$\forall A \in 2^S$，$A\Delta\varnothing = (A\backslash\varnothing)\bigcup(\varnothing\backslash A)\ = A\bigcup\varnothing\ = A$，说明存在幺元 $\varnothing$.

iv. 逆元：对 $\forall A \in 2^S$，$A\Delta A = (A\backslash A)\bigcup(A\backslash A)\ = \varnothing\bigcup\varnothing\ = \varnothing$，说明存在逆元 $A^{-1} = A$.

综上，$(2^S, \Delta)$ 为群. 证毕.

4. 设群中每个非幺元的阶为2，证明该群是Abel群.

证明 记群为 $(G.\cdot)$，$\forall a, b \in G$，$a \cdot b \in G$.

i. 若 $a \cdot b = e$，则$b = a^{-1}$，那么$a \cdot b = b \cdot a$.

ii. 若 $a \cdot b \neq e$，则$\mathrm{ord}(a \cdot b) = 2$，即$a \cdot b \cdot a \cdot b = e$，得到$a \cdot b \cdot = b^{-1} \cdot a^{-1}$. 而$\mathrm{ord}(a) = 2$，即$a \cdot a = e$，得到$a = a^{-1}$，同理 $b = b^{-1}$，代入得到$a \cdot b = b \cdot a$.

综上，$(G.\cdot)$ 为Abel群. 证毕.

5. 设H是$\mathbb{Z}$的子群，证明必定存在整数 m 使得$H = m\mathbb{Z}$.

证明 由$\mathbb{Z} =< 1 >$是循环群可知，子群 H 必定为循环群，故存在 $m \in \mathbb{Z}$ 使得 $H =< m >= m\mathbb{Z}$. （此时 m 可取满足 $1^m \in H$的非负最小值）证毕.

6. 证明群G不能写成两个真子群的并.

证明 假设群 G 可以写成两个真子群 A 和 B 的并，即 $G = A\bigcup B$. 由于 A 和 B 都是真子群，则 $A \neq \varnothing$，$B \neq \varnothing$，$A \neq G$，$B \neq G$. 则 $\exists\, a \in A \wedge a \notin B,\ b \notin A \wedge b \in B$，此时 $ab \notin A$(否则与$b \notin A$矛盾），同理有 $ab \notin B$，得到 $ab \notin G$，与群 G 的封闭性矛盾. 假设不成立. 证毕.

7. 设G是群，$a \in G$，$< a >$是 G 中唯一的二阶子群，证明对 $\forall x \in G$，有$ax = xa$.

证明 对 $\forall x\in G$ 展开讨论：i. 当 $x=a$ 时，显然有 $ax=xa=e$. ii. 当 $x\neq a$ 时，反设 $ax\neq xa \Leftrightarrow x^{-1}ax\neq a$. 而有 $(x^{-1}ax)(x^{-1}ax)=e$，且 $x^{-1}ax\neq e$（否则 $a=e$），说明$\mathrm{ord}(x^{-1}ax)=2$ 与$\langle a\rangle$是 G 中唯一二阶子群矛盾，故假设不成立.

综上，结论得证.

8. 设 G 为交换群，幺元为 e. 定义 G 中的扭元为满足 $g^n=e(n\in\mathbb{Z}^+)$ 的元素 g，扭元集合为 $G_{tor}=\{g\in G|\exists n\in\mathbb{Z}^+,g^n=e\}$. 证明 G_{tor} 是 G 的正规子群.

证明 先证：$G_{tor}\leq G$. 由扭元的定义易知 $e\in G_{tor}$，则 G_{tor} 非空. 对 $\forall g_1,g_2\in G_{tor}(g_1^{n_1}=g_2^{n_2}=e)$，有 $(g_1g_2^{-1})^{n_1n_2}=e$，即$g_1g_2^{-1}\in G_{tor}$. $G_{tor}\leq G$ 得证.

再证：$G_{tor}\lhd G$. 由 G 为交换群易知$G_{tor}\lhd G$成立，证毕.

9. 设 G 是一个群，$N\lhd G$，$H<G$，$HN=\{hn|h\in H,n\in N\}$（符号表示的含义与教材保持一致）. 证明 H 与 HN/N 之间存在满同态映射.

证明 1）先证：HN是群 .

i. 封闭性：由 HN 的构造易知封闭性成立.

ii. 结合律：对 $\forall h_1,h_2,h_3\in H,n_1,n_2,n_3\in N$，$[(h_1n_1)(h_2n_2)](h_3n_3)=h_1n_1h_2n_2h_3n_3=h_1n_1(h_2n_2h_3n_3)=(h_1n_1)[(h_2n_2)(h_3n_3)]$.

iii. 幺元：记 G 的幺元为 e，取 $h_0=e$, $n_0=e$，易知 $h_0n_0=e$，此时对$\forall hn\in HN$，$(hn)h_0n_0=hn$. 存在幺元 且幺元为 e .

iv.逆元：对 $\forall hn\in HN$，由H为群可知，$\exists h'=h^{-1}\in H$，则 $(hn)(h'n')=hnh'n'=(hnh^{-1})n'$， 由 $N\lhd G$ 可知：$hnh^{-1}=n_1\in N$，只需取 $n'=n_1^{-1}$，得到$(hn)(h'n')=n_1n_1^{-1}=e$. 说明存在逆元.

2）再证：$N\lhd HN$.

只需证：$\forall n,n'\in N$，$h\in H$，$(hn)n'(hn)^{-1}\in N$. 而 $(hn)n'(hn)^{-1}=hnn'n^{-1}h^{-1}=hn''h^{-1}$. 由 $N\lhd G$，有 $\forall n\in N,g\in G$，$gng^{-1}\in N$.又 $H<G$，有 $\forall h\in H$，$h\in G$. 则 $hn''h^{-1}\in N$，即 $N\lhd HN$ 得证.

则 HN/N 是HN 对 N 的商群.

3）最后证：群 H 与 HN/N 之间存在满同态映射.

定义映射 φ：$H\to HN/N,\ h\mapsto hnN\ \Leftrightarrow\ h\mapsto hN$（其中 $nN=\{nn'|n'\in N\}=N$）. 由定义和配集的性质等，易知 φ 是良定的.

对 $\forall hN\in HN/N$，$\exists h\in H$，$\varphi(h)=hN$. 说明 φ 是满射.

对 $\forall h_1,h_2\in H$，有 $\varphi(h_1\cdot h_2)=(h_1\cdot h_2)N=h_1N*h_2N=\varphi(h_1)*\varphi(h_2)$. 说明 φ 是同态映射.

综上，H 与 HN/N 之间存在 φ：$H\to HN/N,\ h\mapsto hN$满同态映射. 证毕.

10. 在DES分组对称加密算法的设计中，首先对分组的明文执行初始置换，初始置换是通过IP置换矩阵实现的. IP的定义如下:

$$IP = \begin{bmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \\ 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 \\ 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{bmatrix}$$

（1）查阅资料，对IP置换的含义进行说明；

（2）对分组后得到的64 bit数据：507239AA7EA3B82E，进行IP置换后得到的数据（同样使用十六进制表示）；

（3）求IP置换的逆元IP^{-1}（以同样的矩阵的形式给出）；

（4）*(选做，不算分)考虑C/C++编程实现对数据的分组和初始置换等.

解　（1）对应比特位的置换，……（说清楚初始置换的基本内涵即可）

（2）1357902468FEDCBA

（3）

$$IP^{-1} = \begin{bmatrix} 40 & 8 & 48 & 16 & 56 & 24 & 64 & 32 \\ 39 & 7 & 47 & 15 & 55 & 23 & 63 & 31 \\ 38 & 6 & 46 & 14 & 54 & 22 & 62 & 30 \\ 37 & 5 & 45 & 13 & 53 & 21 & 61 & 29 \\ 36 & 4 & 44 & 12 & 52 & 20 & 60 & 28 \\ 35 & 3 & 43 & 11 & 51 & 19 & 59 & 27 \\ 34 & 2 & 42 & 10 & 50 & 18 & 58 & 26 \\ 33 & 1 & 41 & 9 & 49 & 17 & 57 & 25 \end{bmatrix}$$