# 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 $A,B,C\in 2^S$，$(A\bigcup B)\bigcup C=A\bigcup(B\bigcup C)$，$(A\bigcap B)\bigcap C=A\bigcap(B\bigcap C)$.

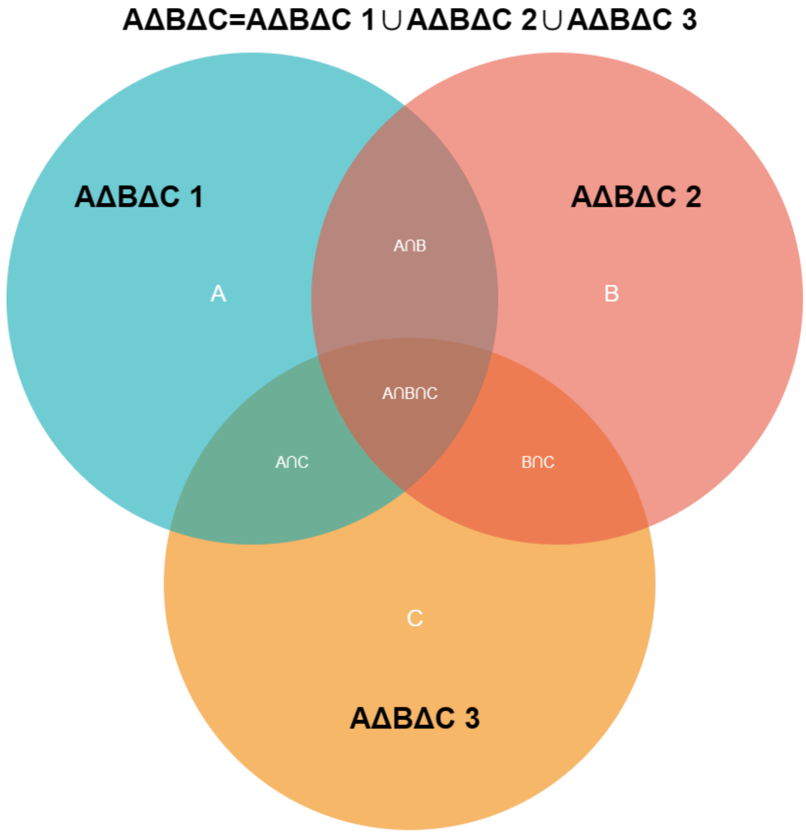
综上，$(2^S,\bigcup)$和$(2^S,\bigcap)$为半群. 证毕.

（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 $\forall A\in$　　，　　　　　　　　　　　　　　　　　　　　，说明存在逆元　　　　　.

[redacted]

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

（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）

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