离 散 数 学 课 后 习 题 答 案 二（总 23 页）

习题

1. 列出关系 {□a，b，c，d □a，b，c，d □Z□且a □b □c □d □6} 中所有有序4元组。

解 {□a，b，c，d □a，b，c，d □Z□且a □b □c □d □6}

□{□1,1,1,6 □,□1,1,6,1 □,□1,6,1,1 □,□6,1,1,1 □,□1,1,2,3 □,□1,1,3,2 □,□1,2,1,3 □,□1,3,1,2 □,
□1,2,3,1 □,□1,3,2,1 □,□2,3,1,1 □,□3,2,1,1 □,□2,1,3,1 □,□3,1,2,1 □,□2,1,1,3 □,□3,1,1,2 □

2. 列出二维表所表示的多元关系中所有 5 元组。假设不增加新的 5 元组，找出二维表所有的主键码。

表 航班信息

航空公司	航班	登机口	目的地	起飞时间
Nadir	112	34	底特律	08:10
Acme	221	22	丹佛	08:17
Acme	122	33	安克雷奇	08:22
Acme	323	34	檀香山	08:30
Nadir	199	13	底特律	08:47
Acme	222	22	丹佛	09:10
Nadir	322	34	底特律	09:44

解 略

3. 当施用投影运算 □$_{2,3,5}$ 到有序 5 元组 □a，b，c，d □时你能得到什么？

解 略

4. 哪个投影运算用于除去一个 6 元组的第一、第二和第四个分量？

解 略

5. 给出分别施用投影运算 □$_{1,2,4}$ 和选择运算 □$_{航空公司= Nadir}$ 到二维表以后得到的表。

解 对航班信息二维表进行投影运算 □$_{2,3,5}$ 后得到的二维表

航班	登机口	起飞时间
112	34	08:10
221	22	08:17

122	33	08:22
323	34	08:30
199	13	08:47
222	22	09:10
322	34	09:44

对航班信息二维表进行选择运算$\square_{航空公司= \text{Nadir}}$ 后得到的二维表

航空公司	航班	登机口	目的地	起飞时间
Nadir	112	34	底特律	08:10
Nadir	199	13	底特律	08:47
Nadir	322	34	底特律	09:44

6. 把连接运算J_3用到 5 元组二维表和 8 元组二维表后所得二维表中有序多元组有多少个分量？

解 略

7. 构造把连接运算J_2用到二维表和二维表所得到的二维表。

表　零件供应商　　　　表 零件数量和颜色代码

供货商	零件号	项目
23	1092	1
23	1101	3
23	9048	4
31	4975	3
31	3477	2
32	6984	4
32	9191	2
33	1001	1

零件号	项目	数量	颜色代码
1001	1	14	8
1092	1	2	2
1101	3	1	1
3477	2	25	2
4975	3	6	2
6984	4	10	1
9048	4	12	2
9191	2	80	4

解　零件供应商二维表与零件数量和颜色代码二维表连接运算J_2结果

供货商	零件号	项目	数量	颜色代码
33	1001	1	14	8
23	1092	1	2	2

23	1101	3	1	1
31	3477	2	25	2
31	4975	3	6	2
32	6984	4	10	1
23	9048	4	12	2
32	9191	2	80	4

第 4 章：群、环、域

习题

1. 判断下列集合对所给的二元运算是否封闭。

（1）集合 $nZ=\{nz \mid z\in Z\}$ 关于普通加法和普通乘法运算，其中 n 是正整数。

（2）集合 $S=\{x \mid x=2n-1,\ n\in Z^{+}\}$ 关于普通加法和普通乘法运算。

（3）集合 $S=\{0,\ 1\}$ 关于普通加法和普通乘法运算。

（4）集合 $S=\{x \mid x=2^{n},\ n\in Z^{+}\}$ 关于普通加法和普通乘法运算。

（5）n 阶 $(n\ge 2)$ 实可逆矩阵集合 $M_n(R)$ 关于矩阵加法和矩阵乘法运算。

对于封闭的二元运算，判断它们是否满足交换律、结合律和分配律，并在存在的情况下求出它们的单位元、零元和所有可逆元素的逆元。

解 略

2. 判断下列集合对所给的二元运算是否封闭。

（1）正实数集合 R^{+} 和∗运算，其中∗运算定义为：

$$\forall a,\ b\in R^{+},\ a*b=a\cdot b-a-b$$

（2）$A=\{a_1,\ a_2,\ \ldots,\ a_n\},\ n\ge 2$。∗运算定义为：

$$\forall a,\ b\in A,\ a*b=b$$

对于封闭的二元运算，判断它们是否满足交换律、结合律和等幂律，并在存在的情况下求出它们的单位元、零元和所有可逆元素的逆元。

解（1）不封闭，例如：$0.5*0.5=0.5\cdot 0.5-0.5-0.5=-0.75\notin R^{+}$

（2）封闭。

不满足交换律：$\exists a,b\in A,\ a\ne b,\ a*b=b\ne a=b*a$

满足结合律：$\forall a,b\in A\ (a*b)*c=b*c=c,\ a*(b*c)=a*c=c$

满足等幂律：$\forall a\in A\ a*a=a$

$a_1,\ a_2,\ \ldots,\ a_n$ 都是左单位元，但无右单位元。

$a_1,\ a_2,\ \ldots,\ a_n$ 都是右零元，但无左零元。

因为无单位元，所以无逆元。

3. 设 $S = Q \times Q$，这里 Q 是有理数集合，$*$ 为 S 上的二元运算，$\forall \langle u, v \rangle, \langle x, y \rangle \in S$，

$$\langle u, v \rangle * \langle x, y \rangle = \langle ux, uy + v \rangle$$

（1）$*$ 运算在 S 上是否可交换、可结合是否为等幂的

（2）$*$ 运算是否有单位元、零元？如果有，请指出，并求 S 中所有可逆元素的逆元。

（3）$*$ 运算在 S 上是否满足消去律？

解 略

4. R 为实数集合，定义以下六个函数 $f_1, \ldots, f_6$。$\forall x, y \in R$ 有

$f_1(\langle x, y \rangle) = x + y$

$f_2(\langle x, y \rangle) = x - y$

$f_3(\langle x, y \rangle) = |x - y|$　　　　$f_4(\langle x, y \rangle) = xy$

$f_5(\langle x, y \rangle) = \min(x, y)$　　　　$f_6(\langle x, y \rangle) = \max(x, y)$

（1）指出哪些函数是 R 上的二元运算。

（2）若是 R 上的二元运算，说明是否是可交换的、可结合的、等幂的？

（3）若是 R 上的二元运算，在存在的情况下求出单位元、零元以及每个可逆元素的逆元。

（4）若是 R 上的二元运算，说明是否满足消去律。

解 略

5. 设 $G = \{1, 2, \ldots, 10\}$，问下面定义的运算 $*$ 在 G 上是否封闭对于封闭的二元运算，请说明运算是否满足交换律、结合律，并并在存在的情况下求出运算的单位元、零元和所有可逆元素的逆元。

（1）$x * y = \gcd(x, y)$，$\gcd(x, y)$ 表示 x 与 y 的最大公因数。

（2）$x * y = \mathrm{lcm}(x, y)$，$\mathrm{lcm}(x, y)$ 表示 x 与 y 的最小公倍数。

（3）$x * y =$ 大于等于 x 和 y 的最小整数。

（4）$x * y =$ 质数 p 的个数，其中 $x \le p \le y$。

解 （1）封闭。满足交换律，满足结合律，满足等幂律。无单位元，1 是零元。因为无单位元，所以无逆元。

（2）不封闭，例如：$3 * 5 = \mathrm{lcm}(3,5) = 15 \notin G$

（3）封闭。满足交换律，满足结合律，满足等幂律。1 是单位元，10 是零元。1 的逆元为 1，其他无逆元。

（4）封闭。不满足交换律，不满足结合律，不满足等幂律。无单位元，无零元。因为无单位元，所以无逆元

§半群与群

习题

1. 设 G 是所有形如

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$$

的矩阵组成的集合，$*$表示矩阵乘法。试问 $\langle G, *\rangle$是半群吗是有么半群吗这里 a_{11}、a_{12} 是实数。

解 任取 G 中的 2 个元素 $A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$、$B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix}$、

∵ $A * B = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} * \begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ 0 & 0 \end{pmatrix} \in G$

∴ $\langle G, *\rangle$是一个代数系统。且因为矩阵的乘法满足结合律，所以$\langle G, *\rangle$是半群。

又因为，只要 $a_{11}=1$，则

$$A * B = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} * \begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix} = B$$

对任何的 $B \in G$ 成立，即 $\begin{pmatrix} 1 & a_{12} \\ 0 & 0 \end{pmatrix}$是左单位元（不论 a_{12} 取什么值）。但右单位元不存在，因为不论 b_{11}，b_{12} 取什么值，

$$A * B = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} * \begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{11} \\ 0 & 0 \end{pmatrix} = B$$

不可能对任何的 $A \in G$ 成立。

所以单位元不存在（事实上，若单位元存在，则左、右单位元都存在且相等还唯一），所以 $\langle G, *\rangle$不是有么半群。

2. 在正实数集合 R^+上定义运算$*$如下

$$a * b = \frac{a+b}{1+ab}$$

试问 $\langle R^+, *\rangle$是半群吗是有么半群吗

解 略

3. 在自然数集合 N 上定义运算 $\circ$和 $\cdot$如下：

$a \circ b = \max\{a, b\}$，　　　　$a \cdot b = \min\{a, b\}$

试问 $\langle N, \circ\rangle$和 $\langle N, \cdot\rangle$是半群吗是有么半群吗

解 略

4. 设□G，□□是半群，它有一个左零元□，令

G□ □{x □□□| x □G}

证明□G□，□□构成半群。

解 略

5. 在一个多于一个元素的有么半群中，证明一个右零元不可能有右逆元。

解 略

6. 设 G 是一个多于一个元素的集合，G^G 是 G 上所有函数组成的集合，证明有么半群□G^G，□□有多于一个的右零元，但没有左零元。这里□表示复合运算。

解 略

7. 设 Z 为整数集合，在 Z 上定义二元运算□如下：

x □y □x □y □2，□x，y □Z

问 Z 关于运算□能否构成群为什么

解 略

8. G □{ f (x) □ax □b |a □0，a，b □R}，证明□G，□□是群，这里□是复合运算。

解 略

9. 设 G □{r，1/r，1 □r，1/(1 □r)，(r □1)/r，r /(r □1)}，证明□G，□□是群，这里，运算 a □b 表示将 b 代换到 a 中 r 所在位置。

解 略

10. 设 A □{x |x □R □x □0，1}。在 A 上定义六个函数如下：

$f_1(x)$ □x　　$f_2(x)$ □x□

$f_3(x)$ □1 □x　　$f_4(x)$ □(1 □x)□

$f_5(x)$ □(x □1)x□　　$f_6(x)$ □x (x □1)□

令 G 为这六个函数构成的集合，□是复合运算。

（1）给出□G，□□的运算表。　　（2）验证□G，□□是群。

解 （1）□G，□□的运算表如下：

□	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3

f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

（2）从上运算表可以看出，运算具有封闭性，满足结合律，单位元为 f_1，每个元都有逆元，所以 $\langle G, \circ \rangle$ 构成群。

11. 在群 $\langle R, + \rangle$ 中计算下列元素的幂：

$0.5^2 = ?$　　　　$0.5^{10} = ?$

$0.5^0 = ?$　　　　$\sqrt{4}^2 = ?$

$\sqrt{4}^{10} = ?$　　　　$\sqrt{4}^0 = ?$

解　$0.5^2 = 1$　　　　$0.5^{10} = 5$

$0.5^0 = 0$　　　　$\sqrt{4}^2 = 4$

$\sqrt{4}^{10} = 20$　　　　$\sqrt{4}^0 = 0$

12 在群 $\langle G, \circ \rangle$ 中，证明

$$x^m \circ x^n = x^{m+n},\quad (x^m)^n = x^{m \times n},\quad \forall m, n \in Z$$

解 略

13. 设 $G = \{1, 2, 3, 4, 5, 6\}$，对于 G 上的二元运算“模7乘法 $\times_7$”：

$$i \times_7 j = (i \times j)(\mathrm{mod}\,7)$$

$\langle G, \times_7 \rangle$ 构成群。请

（1）给出 $\langle G, \times_7 \rangle$ 的运算表。　　　　（2）验证 $\langle G, \times_7 \rangle$ 构成群。

（3）给出每个元的次数。

解 略

14. 设 $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$，对于 G 上的二元运算“模15乘法 $\times_{15}$”：

$$i \times_{15} j = (i \times j)(\mathrm{mod}\,15)$$

请

（1）给出 $\langle G, \times_{15} \rangle$ 的运算表。　　　　（2）验证 $\langle G, \times_{15} \rangle$ 构成群。

（3）给出每个元的次数。

解（1）$\langle G, \circ_{15} \rangle$的运算表如下：

$\circ_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

（2）从上运算表可以看出，运算具有封闭性，满足结合律，单位元为“1”，每个元都有逆元（元素1，2，4，7，8，11，13，14的逆元分别是：1，8，4，13，2，11，7，14），所以$\langle G, \circ_{15} \rangle$构成群。

（3）元素1，2，4，7，8，11，13，14的次数分别是：1，4，2，4，4，2，4，2。

习题

1. 设$\langle G, \circ \rangle$是群，若$\forall x \in G$有$x^2 = e$，证明$\langle G, \circ \rangle$为交换群。

解 略

2. 设$\langle G, \circ \rangle$是群，证明G是交换群的充分必要条件是$\forall a, b \in G$有$(a \circ b)^2 = a^2 \circ b^2$。

解 必要性：如果G是交换群，$\forall a, b \in G$有$(a \circ b)^2 = a^2 \circ b^2$是显然的。

充分性：根据$(a \circ b)^2 = a^2 \circ b^2$得$a \circ b \circ a \circ b = a \circ a \circ b \circ b$，再由消去律得$b \circ a = a \circ b$，即交换律成立，所以$G$是交换群。

3. 设$\langle G, \circ \rangle$是群，并且对任意的$a, b \in G$都有$(a \circ b)^3 = a^3 \circ b^3$，$(a \circ b)^5 = a^5 \circ b^5$，证明$G$是交换群。

解 略

4. 设$\langle G, \circ \rangle$是有限半群，且满足消去律，证明G是群。

解 对于$\forall a \in G$，考虑集合

$$G_a = \{a, a^2, a^3, \cdots, a^m, \cdots\}$$

由封闭性可知$G_a \subseteq G$。又由于G是有限集，所以G_a也是有限集。故必有$n, k \geq 0$，使得

$$a^n = a^{n+k}$$

$\forall b$ 有

$$a^n \circ b = a^{n+k} \circ b$$

由消去律可得

$$b = a^k \circ b$$

这表明 a^k 是左单位元，同理可证它是右单位元，所以 a^k 是单位元。又因为

$$a^{k-1} \circ a = a \circ a^{k-1} = a^k = e$$

所以，a 有逆元 a^{k-1}。因此，$\langle G, \circ \rangle$ 是群。

5. 设 $\langle G, \circ \rangle$ 是群，a，b，$c \in G$，证明

$$|a \circ b \circ c| = |b \circ c \circ a| = |c \circ a \circ b|$$

略

6. 设 $\langle G, \circ \rangle$ 是群，a，$b \in G$ 且 $a \circ b = b \circ a$。如果 $|a| = n$，$|b| = m$ 且 n 与 m 互质，证明 $|a \circ b| = n \cdot m$。

解 略

7. 证明循环群一定是交换群，举例说明交换群不一定是循环群。

解 略

8. 证明由 1 的 n 次复根的全体所组成的集合在复数乘法下构成一个 n 阶循环群。

解 由代数的知识可知，1 的 n 次复根的全体所组成的集合为

$$G = \{e^{\frac{2k\pi}{n}i} \mid k = 0,1,2,\ldots,n-1\}$$

$\forall e^{\frac{2p\pi}{n}i}, e^{\frac{2q\pi}{n}i} \in G, p,q \in \{0,1,2,\ldots,n-1\}$，有 $e^{\frac{2p\pi}{n}i} \cdot e^{\frac{2q\pi}{n}i} = e^{\frac{2(p+q)\pi}{n}i}$。若 $p+q < n$，则 $e^{\frac{2(p+q)\pi}{n}i} \in G$；若 $p+q \geq n$，则存在 $k \in \{0,1,2,\ldots,n-1\}$，使得 $p+q = n+k$，而 $e^{\frac{2(p+q)\pi}{n}i} = e^{\frac{2(n+k)\pi}{n}i} = e^{\frac{2k\pi}{n}i} \in G$。因此 G 关于数的乘法是封闭的。故 $\langle G, \cdot \rangle$ 是代数系统。

数的乘法运算满足结合律。故 $\langle G, \cdot \rangle$ 是半群。

因为 $\forall e^{\frac{2k\pi}{n}i} \in G$，有 $1 \cdot e^{\frac{2k\pi}{n}i} = e^{\frac{2k\pi}{n}i} \cdot 1 = e^{\frac{2(k+0)\pi}{n}i} = e^{\frac{2k\pi}{n}i}$，所以 $1 = e^{\frac{2\cdot 0\pi}{n}i}$ 是 G 的幺元。故 $\langle G, \cdot \rangle$ 是有幺半群。

$\forall e^{\frac{2k\pi}{n}i} \in G$，存在 $e^{\frac{2(n-k)\pi}{n}i} \in G$，使得

$e^{\frac{2k\pi}{n}i} \cdot e^{\frac{2(n-k)\pi}{n}i} = e^{\frac{2(n-k)\pi}{n}i} \cdot e^{\frac{2k\pi}{n}i} = e^{2\pi i} = 1$，所以 $e^{\frac{2k\pi}{n}i}$ 的逆元存在。故 $\langle G, \cdot \rangle$ 是群。

因为 $e^{\frac{2k\pi}{n}i} = [e^{\frac{2\pi}{n}i}]^k$，故 $e^{\frac{2\pi}{n}i}$ 是群 G 的一个生成元，因此 G 是循环群。

9. 5、6、14、15 的循环群的生成元分别有多少个？

设 是阶数为 5 的循环群的生成元，因在比 5 小的正整数中有且仅有 2，3，4 与 5 互质，所以 a^2， a^3， a^4 也是生成元，因此生成元个数为 4。

设 a 是阶数为 6 的循环群的生成元，因在比 6 小的正整数中有且仅有 5 与 6 互质，所以 a^5 也是生成元，因此生成元个数为 2。

设 a 是阶数为 14 的循环群的生成元，因在比 14 小的正整数中有且仅有 3，5，9，11，13 与 14 互质，所以 a^3， a^5， a^9 a^{11} a^{13} 也是生成元，因此生成元个数为 6。

设 a 是阶数为 15 的循环群的生成元，因在比 15 小的正整数中有且仅有 2，4，8，11，13，14 与 15 互质，所以 a^2， a^4， a^8 a^{11} a^{13} a^{14} 也是生成元，因此生成元个数为 7。

10. 设 $G=\{1, 5, 7, 11\}$，对于 G 上的二元运算“模12 乘法 $\otimes_{12}$”：

$$i \otimes_{12} j = (i \times j)(\mathrm{mod}\, 12)$$

（1）证明 $\langle G, \otimes_{12} \rangle$ 构成群。　　（2）求 G 中每个元素的次数。

（3） $\langle G, \otimes_{12} \rangle$ 是循环群吗？

习题

1. 给出群 $\langle Z_8, +_8 \rangle$ 的全部子群。

解 两个非平凡子群是：$\{0, 2, 4, 6\}$ 和 $\{0, 4\}$，两个平凡子群是：Z_8 和 $\{0\}$。

2. 设 $G=\{1, 5, 7, 11\}$，对 G 上的二元运算“模12 乘法 $\otimes_{12}$”：

$$i \otimes_{12} j = (i \times j)(\mathrm{mod}\, 12)$$

$\langle G, \otimes_{12} \rangle$ 构成群，请求出 $\langle G, \otimes_{12} \rangle$ 的所有子群。

解 略

3. 设 $\langle G, \circ \rangle$ 是群， H 是其子群，任给 $a \in H$，令

$$aHa^{-1} = \{a \circ h \circ a^{-1} \mid h \in H\}$$

证明 aHa^{-1} 是 G 的子群（称为H 的共轭子群）

解 略

4. 设 $\langle G, \circ \rangle$ 是群， H 和 K 是其子群，证明HK 和 KH 是 $\langle G, \circ \rangle$ 的子群当且仅当 $HK = KH$，其中

$HK = \{h \circ k \mid h \in H \wedge k \in K\}$　　　$KH = \{k \circ h \mid k \in K \wedge h \in H\}$

5. 设 $\langle G, \circ \rangle$ 是群，H 是G的子集，证明H是G的子群当且仅当 $H^2 \subseteq H$，$H^{-1} \subseteq H$，这里

$$H^2 = \{h_1 \circ h_2 \mid h_1, h_2 \in H\} \qquad H^{-1} = \{h^{-1} \mid h \in H\}$$

证（1）因为H是G的子集，根据 H^2，H^{-1} 的定义，显然有：$H^2 \subseteq H, H^{-1} \subseteq H$　又因为H中任意元素h可以写成 $e \circ h$，所以 $H \subseteq H^2$，还因为H中任意元素h可以写成 $(h^{-1})^{-1}$，所以 $H \subseteq H^{-1}$，因此

$$H^2 = H, \quad H^{-1} = H$$

（2）$\forall h_1, h_2 \in H$，因为 $H^2 \subseteq H$，$H^{-1} \subseteq H$，所以

$$h_1 \circ h_2^{-1} = h_1 \circ h_3 = h_4 \in H$$

由子群的判定定理知，H 是G的子群。

6. 某一通讯编码的码字 $x = (x_1, x_2, \cdots, x_7)$，其中 x_1，x_2，x_3 和 x_4 为数据位，x_5，x_6 和 x_7 为校验位（x_1，x_2，$\cdots$，x_7 都是 0 或 1），并且满足

$$x_5 = x_1 \oplus_2 x_2 \oplus_2 x_3 \qquad x_6 = x_1 \oplus_2 x_2 \oplus_2 x_4 \qquad x_7 = x_1 \oplus_2 x_3 \oplus_2 x_4$$

这里 $\oplus_2$ 是模 2 加法。设 H 是所有这样的码字构成的集合。在 H 上定义二元运算如下：

$$\forall x, y \in H, \ x \circ y = (x_1 \oplus_2 y_1, x_2 \oplus_2 y_2, \cdots, x_7 \oplus_2 y_7)$$

证明 $\langle H, \circ \rangle$ 构成群，且是 $\langle G, \circ \rangle$ 的子群，其中G是长度为 7 的位串构成的集合。

解　略

7. 设 $G = \langle a \rangle$ 是循环群，$H = \langle a^s \rangle$ 和 $K = \langle a^t \rangle$ 是它的两个子群。证明 $H \cap K = \langle a^u \rangle$，这里 $u = [s, t]$ 是s和t的最小公倍数。

解　$\forall a^l \in H \cap K$，则根据定理，l 应是s的倍数，也应是t的倍数，从而 l 应是s和t的最小公倍数 $u = \mathrm{lcm}(s, t)$ 的倍数，所以 $a^l \in \langle a^u \rangle$。

$\forall a^l \in \langle a^u \rangle$，则 l 应是s和t的最小公倍数 $u = \mathrm{lcm}(s, t)$ 的倍数，从而 l 是s的倍数，也是t的倍数，所以 $a^l \in H$，$a^l \in K$，即 $a^l \in H \cap K$。

8. 设 5 阶置换为

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

计算 $\sigma\tau$，$\tau\sigma$，σ^{-1}，$\sigma^{-1}\tau\sigma$，$\tau^{-1}\sigma\tau$。

解　略

9. 设 $S = \{1, 2, 3, 4\}$，写出S上的所有 4 元置换。

解　略

10. 4 元对称群 S_4 的运算表，求出单位元，每个元的逆元，每个元的次数以及它的所有子群

陪集与商群

习题

1. 集合 $Z_{20} = \{0, 1, 2, \cdots, 19\}$ 在“模20加法 $+_{20}$”下构成群。设H是由元素5生成的 Z_{20} 的子群。

（1）求H的每个元素及其次数。 （2）求H在 Z_{20} 中的所有左陪集。

解（1）$H = \{0, 5, 10, 15\}$，$0, 5, 10, 15$ 的次数分别为：1，4，2，4。

（2）H在 Z_{20} 中的所有左陪集如下：

$H = \{0, 5, 10, 15\}$，$1H = \{1, 6, 11, 16\}$，$2H = \{2, 7, 12, 17\}$

$3H = \{3, 8, 13, 18\}$，$4H = \{4, 9, 14, 19\}$

2. 求12阶循环群 $G = \{e, a, a^2, a^3, a^4, \cdots, a^{11}\}$ 的子群 $H = \{e, a^4, a^8\}$ 在G中的所有左陪集。

解 所有左陪集如下：

$H = \{e, a^4, a^8\}$，$aH = \{a, a^5, a^9\}$，$a^2H = \{a^2, a^6, a^{10}\}$

3. 设H是群 $\langle G, \cdot \rangle$ 的子群，证明H的所有不同左陪集（右陪集）中有且仅又一个在 $\cdot$ 下构成 $\langle G, \cdot \rangle$ 的子群。

解 略

4. 证明6阶群必含有3次元。

解 略

5. 证明偶数阶群必含2次元。

解 设 $\langle G, \cdot \rangle$ 是偶数阶群，若它无二次元，则对G中的非单位元a，有

$$a \neq a^{-1}$$

所以，G中的元素，除单位元外，其他都是成对出现的，所以G中的元素是偶数个，矛盾。故偶数阶群必含2次元。

6. 证明在有限群中次数大于2的元素的个数必定是偶数。

解 略

7. 设 $\langle G, \cdot \rangle$ 是一个阶数为p的有限群，其中p是质数，证明G是循环群并求它的所有子群。

解 略

8. 设H和K分别是群 $\langle G, \cdot \rangle$ 的r，s阶子群，若r，s互质，证明 $H \cap K = \{e\}$。