抽象代数学题解

厦门大学数学系

几何代数教研室代数组编

编 者 的 话

本题解是根据N.贾柯勃逊著《抽象代数学》（卷1）基本概念所选的全部习题编写的，所用的符号、定理、公式都与该书一致。它是我们在教学过程中，为适应教学需要，更好地帮助同学较全面地理解全书服务的。

在编写出版过程中，得到系主任方德植教授及有关方面的热情支持和鼓励，特此致谢。本题解由几何代数教研室代数组杨锡安、佘明湍、杨照南、林大兴等同志编写。由于编者的水平有限，加上时间匆促，书中难免有不少缺点错误，恳请读者批评指正。

一九八〇年七月

目　录

引论：从集合论不，，，，自然数系

习 题 1

1．求证：对于各个n都有$n^+ \neq n$

〔证〕：令$N=\{n \mid n^+ \neq n$，n是自然数$\}$

首先，$1 \in N$，因为若$1 \in N$，即$1^+ = 1$，这就是说1的后继元素是1，也就是1是1的生成元素，这与Peano关于自然数公理iii）："自然数1无生成元"矛盾。所以N是含有1的自然数集合。

次设k是N中的任一元素，即$k^+ \neq k$．若$k^+ \in N$，即有$(k^+)^+ = k^+$，由Peano公理iv）："若$a^+ = b^+$，则$a = b$"得到$k^+ = k$，这与假设k是N中之元矛盾，$\therefore k^+ \in N$．再由Peano公理v）："自然数的每个集合，若它含有1，且含有这个集合每个元素的后继元素，则这集合含有一切自然数"知，N是自然数全体，即$n^+ \neq n$对所有自然数成立。

习 题 2

1．设$a>b$，$c>d$，求证：$a+c>b+d$，$ac>bd$．

〔证〕：设P表示自然数集合，a，b，c，$d \in P$．

（1）$\because a>b$，$\therefore$方程$a=b+x$对于x有在P中的解，即$\exists m \in P$使得$a=b+m$．$\therefore a+c=(b+m)+c=(b+c)+m \cdots (*)$

同样，$\because c>d$，$\therefore \exists n \in P$，使得$c=d+n$．

$\therefore b+c=b+(d+n)=(b+d)+n\cdots\cdots(**)$

由(*)知$a+c>b+c$.

由(**)知$b+c>b+d$.

再由传递性即得$a+c>b+d$.

(2) $\because a=b+m$, $\therefore ac=(b+m)c=bc+mc\cdots(*)'$

$\because c=d+n$. $\therefore bc=b(d+n)=bd+bn\cdots(**)'$

$\because m, n, b, c\in P$, $\therefore mc, bn\in P$.

$\therefore$由(*)′知$ac>bc$.

由(**)′知$bc>bd$.

再由传递性即得$ac>bd$.

习 题 3

1. 设$x>y$, 求证$-x<-y$.

〔证〕: 令$x=(\overline{a,\ b})$, $y=(\overline{c,\ d})$, $a, b, c, d\in P$.

$\because x>y$, 即$(\overline{a,\ b})>(\overline{c,\ d})$,

$\therefore a+d>b+c$, 由于在P中交换律成立

$\therefore d+a>c+b$. 即$(\overline{d,\ c})>(\overline{b,\ a})$

$\because(\overline{d,\ c})=-(\overline{c,\ d})$, $(\overline{b,\ a})=-(\overline{a,\ b})$.

$\therefore -(\overline{c,\ d})>-(\overline{a,\ b})$, 即$-y>-x$, 亦即$-x<-y$.

习 题 4

1. 整数的任一个非空集合S为下(上)有界的, 其意义是说: 对于S里的各个s, 有一个整数b(B)存在, 使$b\leqslant s$($B\geqslant s$). 求证: 这样的S含有一个最小(最大)元素.

〔证〕: 先证任一非空的上有界的整数集S必含有最大元素. 假定S_+表示S中全部正整数的集合。当$S_+\neq\varnothing$, 考察集

合

$H=\{h \mid h \geqslant s_+$，$s_+$是$S_+$的任意元素$\}$

∵S上有界，所以S_+也上有界∴存在正整数h_1，对于S_+中的任意元素s_+，都有$h_1 \geqslant s_+$，∴$h_1 \in H$，故H是非空的自然数的集合，根据关于自然数的性质（O_4），H有最小的h_0存在，使得对任意的$h \in H$，都有$h \geqslant h_0$。此时，显然有$h_0 \in S_+$，因为若$h_0 \in S^+$，则对所有的$s_+ \in S_+$，都有$s_+ < h_0$。

于是$s_+ \leqslant h_0 + (-1)$．而$h_0 + (-1) < h_0$．这与h_0最小的假定矛盾．

∵$S_+ \subseteq S$，∴$h_0 \in S$．h_0就是S的最大元素。

当$S_+ = \varnothing$时，若$O \in S$，显然O就是S的最大元素

若$O \notin S$．考察集合

$S' = \{-s \mid s$为S的元素$\}$∵对于任意$s \in S$，都有$s < o$

∴$-s > o$．即S'是正整数（自然数）集合，由关于自然数的性质（O_4），S'有最小数$-s_0$，对于S'中任一元素$-s$，都有

$$-s \geqslant -s_0$$

∴$s_0 \geqslant s$，即s_0是S中的最大元素。

再证任一非空的下有界的整数集合S必含有最小元素。设s_1是S的一个下界，则对任意的$s \in S$都有$s_1 \leqslant s$，∴$-s_1 \geqslant -s$．∴$-s_1$是集合$S' = \{-s \mid s$是S的元素$\}$的上界，据前面所证，S'含有最大元素$-s_0$。即对S'中任一元素$-s$，都有$-s \leqslant -s_0$，∴$s \geqslant s_0$，即s_0是集合S的最小元素。

2．若$x \geqslant 0$，则命$|x| = x$，但若$x < 0$，则命$|x| = -x$，求证

$$|xy| = |x|\,|y| \qquad |x+y| \leqslant |x| + |y|$$

〔证〕：先证第一式．1）若x，y有一为0，等式显然成立．因两边都是零。

2）若x、y异号，不妨设$x>0$，$y<0$．则$xy<0$于是$|xy|=-(xy)$．而$|x|=x$．$|y|=-y$.得$|x||y|=x(-y)=-(xy)$．等式成立。

3）若x、y同号，则$xy>0$．$|xy|=xy$.

分两种情形，都是正数时，$|x|=x$，$|y|=y$，得$|x||y|=xy$。都是负数时，$|x|=-x$、$|y|=-y$.得$|x||y|=(-x)(-y)=xy$．等式也成立。

再证第二式，1）若x、y异号，不妨设$|x|\geqslant|y|$．则$|x+y|\leqslant|x|$，于是$|x+y|\leqslant|x|+|y|$．

2）若x、y同号，分两种情形，都是正数时，

$|x+y|=x+y=|x|+|y|$

都是负数时，$|x+y|=-(x+y)=(-x)+(-y)=|x|+|y|$．

习 题 5

1．求证：q与r是唯一的

〔证〕：设$a=bq_1+r_1$，$0\leqslant r_1<|b|$．

又$a=bq_2+r_2$，$0\leqslant r_2<|b|$．

则 $bq_1+r_1=bq_2+r_2$．于是$b(q_1-q_2)=r_2-r_1$，得$|b(q_1-q_2)|=|r_2-r_1|$

若$q_1-q_2\neq 0$，则左边$|b(q_1-q_2)|=|b||q_1-q_2|\geqslant|b|$而右边$|r_2-r_1|<|b|$，此不可能．

故必$q_1-q_2=0$．由$b(q_1-q_2)=r_2-r_1$，得$r_2-r_1=0$．即$q_1=q_2$，$r_1=r_2$。

第一章　半群及群

习　题　6

1．在整数的集合里定义二元合成$f(x,y)=x+y^2$，求作所有导出的四元合成。

解：由$N(n)=\frac{(2n-2)!}{n!\,(n-1)!}$得$N(4)=5$，记$(xy)=x+y^2$所导出的五种四元合成为

$((a_1a_2)a_3)a_4=((a_1+a_2^2)a_3)a_4=(a_1+a_2^2+a_3^3)a_4=a_1+a_2^2+a_3^2+a_4^2$；

$(a_1(a_2a_3))a_4=(a_1(a_2+a_3^2))a_4=(a_1+a_2+a_3^2)a_4$

$=a_1+a_2^2+a_4^2+2a_2a_3^2+a_3^4$；

$(a_1a_2)(a_3a_4)=(a_1+a_2^2)(a_3+a_4^2)=a_1+a_2^2+(a_3+a_4^2)^2=a_1+a_2^2+a_3^2+2a_3a_4^2+a_4^4$

$a_1(a_2(a_3a_4))=a_1(a_2(a_3+a_4^2))=a_1(a_2+(a_3+a_4^2)^2)$

$=a_1(a_2+a_3^2+2a_3a_4^2+a_4^4)$

$=a_1+(a_2+a_3^2+2a_3a_4^2+a_4^4)^2=a_1+a_2^2+2a_2a_3^2$

$+4a_2a_3a_4^2+a_3^4+2a_2a_4^4+4a_3^3a_4^2+6a_3^2a_4^4+4a_3a_4^6+a_4^8$

$a_1((a_2a_3)a_4)=a_1((a_2+a_3^2)a_4)=a_1(a_2+a_3^2+a_4^4)$

$=a_1+(a_2+a_3^2+a_4^2)^2=a_1+a_2^2+2a_2a_3^2+2a_2a_4^2+a_3^4+2a_3^2a_4^2+a_4^4$。

2．对于一个给定的二元合成，我们可以用归纳法定义n个元素的简单积为a_iu或va_i，这里u为$a_2,\cdots,a_n$的简单积，v为$a_1,\cdots,a_{n-1}$的简单积，证明：$\geqslant 2^r$个元素的任一个积

可看作r个元素（它们自身也是积）的简单积。

〔证〕：对r施行数学归纳法：

当r＝1时，≥2个元素的任一个积，由给定的二元合成结果是一个元素，所以它可看为一个元素的简单积，命题成立。

设为r＝k时，命题成立：即≥2^k个元素的任意一个积可看作k个元素的简单积，现证对r＝k＋1命题成立。≥2^{k+1}个元素的任意一个积由合成最后结果总可表为u·v。因为元素的个数≥2^{k+1}，所以u，v中至少有一个(不妨设u)所含元素的个数≥2^k，由归纳法假设，u可表示为k个元素的简单积，把v中所含元素全体看作一个简单积，所以≥2^{k+1}个元素的任意一个积可看作k＋1个简单积，所以对于任意自然数r，命题成立。

习 题 7

1．命G为实数二维组（a，b）的全体，其中a≠0，如果G里的合成由公式

$$(a,b)(c,d)=(ac,bc+d)$$

来定义，验证：G是一个群。

〔证〕1）．设(a，b)，(c，d)∈G，∵a≠0，c≠0 ∴ac≠0，且bc＋d也是实数，∴(a，b)(c,d)＝(ac，bc＋d)∈G

2）〔(a,b)(c,d)〕(e,f)＝(ac,bc＋d)(e,f)

＝(ace,bce＋de＋f)

(a,b)〔(c,d)(e,f)〕＝(a,b)(ce,de＋f)

＝(ace,bce＋de＋f)

$\therefore$〔(a,b)(c,d)〕(e,f)=(a,b)〔(c,d)(e,f)〕。

3)(1,0)为G的恒等元，$\because$(1,0)(a,b)

=(a,b)(1,0)=(a,b)

4)$(a,b)^{-1}=(a^{-1},-ba^{-1})\in G$，$\because a\neq 0$，$\therefore a^{-1}$有意义。

$(a,b)(a^{-1},-ba^{-1})=(1,0),(a^{-1},-ba^{-1})(a,b)$

=(1,-b+b)=(1,0)故G成群。

习 题 8

1．设半群的元素e适合$e^2=e$，这元素叫做同势元素（或幂等元素。）证明：群里的同势元素是e=1，

〔证〕：设e是群G的同势元素，则

$$e^2=e.$$

$\because e\in G$，$\therefore$存在$e^{-1}\in G$，把上式同右乘e^{-1}，则得

$e^2e^{-1}=ee^{-1}=1$，而$e^2e^{-1}=e$

$\therefore e=1$。

2．求证半群G如果具有下列性质，则成为群：

(i)G有一个右恒等元l_r，(ii)G的每个元a对于l_r有一个右逆元。

〔证〕：对任意的$a\in G$，由(ii)，存在$b\in G$使得$ab=l_r$，现要证b对于l_r也是a的左逆元，即$ba=l_r$

$bab=b(ab)=bl_r=b$

$\because b\in G$，$\therefore$存在$c\in G$，使得$bc=l_r$，把上式两边同右乘c得

$babc=ba(bc)=bal_r=ba=bc=l_r$

即 $ba=l_r$……(*)

再证右恒等元l_r也是左恒等元，即$l_ra=a$。

$\because l_r a = (ab)a = a(ba) = al_r = a$。

$\therefore l_r = 1$，由（*）知b是a的右逆元又是左逆元，$\therefore$b是a的逆元，$\therefore$G成群。

3．设G为半群，且对于元素a与b，方程$ax = b$及$ya = b$都可解，证明：G是一个群。

〔证〕：设$e \in G$是方程$ax = a$的解，即$ae = a$

对于G中的任意元b，方程$ya = b$在G中有解。

$yae = (ya)e = be$

$yae = y(ae) = ya = b$。$\therefore be = b$

即e是G的右恒等元。

又，方程$ax = e$在G中有解，$\therefore$群G中的任意元a关于右恒等元e都有右逆元，由第2题知G成群。

4．如果相消律在一个有限半群里成立，证明：这半群是一个群。

〔证〕：令$G = \{a_1, a_2, \cdots, a_n\}$（其中$a_i$各不相同）是一个有限半群，任取$a \in G$，作集合$G_1 = \{aa_1, aa_2, \cdots, aa_n\}$，显然$G_1$中的每个元素都是G中的元素，而且当$i \neq j$时，$aa_i \neq aa_j$。因如果$aa_i = aa_j$，由相消律成立即得$a_i = a_j$，这与假设矛盾。$\therefore G = G_1$

于是G中的任一元素都可表为$b = a_j$即方程$ax = b$在G中有解。同理可证$ya = b$在G中也可解。

由第3题知G成群。

习 题 9

1．验证：形状如（1，b）的二维组的子集合构成习题7的第1题里所述的群的一个子群。

〔证〕：令H＝｛（1，b）｜b是实数｝。

1）（1，b）（1，c）＝（1，b＋c）∈H。

2）(1,0)∈H，(1,0)(1，b)＝(1，b)(1,0)＝(1，b)。

3）$(1,b)^{-1}=(1,-b)\in H$。$(1,b)(1,-b)=(1,-b)(1,b)=(1,0)$，故H为G的子群。

2．求证：群G的一个子集合H成为一个子群的充要条件是a与b属于H时，$ab^{-1}\in H$。

〔证〕：必要性：设H是群G的子群，若a，b∈H，则$b^{-1}\in H$

$\therefore ab^{-1}\in H$。

充分性：i）若b∈H，则$1=bb^{-1}\in H$.ii）1，b∈H

则$b^{-1}=1b^{-1}\in H$，iii）若a，b∈H，则$b^{-1}\in H$

$\therefore a(b^{-1})^{-1}=ab\in H$。故H为G的子群。

3．求证：群的任一个有限子半群必为一个子群（参看习题8第4题）

〔证〕：设H是群G的一个有限子半群，因相消律在G里成立，所以在H里也成立。由习题8第4题知H成群，即H是G的一个子群。

4．设以A表示G的各子群H的任一个集合，求证：交$\bigcap_A H$是一个子群。

〔证〕：设a、b∈$\bigcap_A H$则a、b属于各个H，∵各个H都是G的子群，$\therefore ab^{-1}$∈各个H.$\therefore ab^{-1}\in\bigcap_A H$，故$\bigcap_A$是G的一个子群。

5．设a是群G的任一个元素，求证：与a可交换的元素的集合G(a)是G的一个子群。

〔证〕：记G(a)＝｛b｜a为G中一固定元素，b∈G，ab＝ba｝.则1∈G(a)∵1a＝a1＝a。∴G(a)非空。

设b，$c\in G(a)$，则$ba=ab$，$ca=ac$。

$(bc)\cdot a=b(ca)=b(ac)=(ba)c=(ab)c=a(bc)$

$\therefore bc\in G(a)$

对于$b\in G(a)$，$\because ab=ba$，$\therefore b^{-1}abb^{-1}=b^{-1}bab^{-1}$

即得$b^{-1}a=ab^{-1}$，$\therefore b^{-1}\in G(a)$。

故G(a)是G的一个子群。

习 题 10

1．设$x\to x'$是一个同构，求证：1的象$1'$是第二个群的恒等元素，并且$(a^{-1})'=(a')^{-1}$。

〔证〕：设a是第一个群的任一个元素，它在同构映射下的象为a'。由同构关系有$(1\cdot a)'=1'a'$，而$(1\cdot a)'=a'$。

$$\therefore 1'a'=a'.$$

同理可证 $a'1'=a'$。$\therefore 1'$是第二个群的恒等元素。

$\because a'(a^{-1})'=(a\cdot a^{-1})'=1'$，$(a^{-1})'a'=(a^{-1}\cdot a)'=1'$

$\therefore (a^{-1})'=(a')^{-1}$。

2．映照$\theta\to e^{i\theta}$是否为R+到由绝对值为1的复数组成的乘法群上的一个同构呢？

〔证〕：这个映照不是同构映照。

$\because \theta\neq\theta+2k\pi, k=\pm1,\pm2,\cdots$，而$e^{i\theta}=e^{i(\theta+2k\pi)}$

即$\theta\to e^{i\theta}$不是1—1的。

习 题 11

1．设$\alpha=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$，$\beta=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}$

计算$\alpha\beta$，$\beta\alpha$，及α^{-1}。

〔解〕$\alpha\beta=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}$

$\beta\alpha=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}$

$\alpha^{-1}=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$

2．写出S_3的元素，并作出这个群的乘法表。

〔解〕：S_3的元素有$3!=6$个：

$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$，$\sigma_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$，$\sigma_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$，

$\sigma_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$，$\sigma_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$，$\sigma_6=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$，

它的乘法表如下：

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

3．验证下列变换成一个变换群：

$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$，$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$，$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$。

〔证〕：这三个变换就是上题中的σ_1，σ_4，σ_5，令$H=\{\sigma_1,\sigma_4,\sigma_5\}$由乘法表知$\sigma_1\sigma_1=\sigma_1\in H$，$\sigma_4\sigma_4=\sigma_5\in H$，$\sigma_5\sigma_5=\sigma_4\in H$。

$\sigma_1\sigma_4=\sigma_4\in H$，$\sigma_1\sigma_5=\sigma_5\in H$，$\sigma_4\sigma_5=\sigma_1\in H$。

∴H中任意二个元素的乘积仍为H的元素。

σ_1 是H的恒等元素：$\sigma_1\sigma_4=\sigma_4\sigma_1=\sigma_4$，$\sigma_1\sigma_5=\sigma_5\sigma_1=\sigma_5$，$\sigma_1^{-1}=\sigma_1\in H$。$\sigma_4^{-1}=\sigma_5\in H$。$\sigma_5^{-1}=\sigma_4\in H$

∴H成变换群。

4．§6里那些个例子是变换群？

答：例8与例9中所述的群是变换群。

5．验证由法则$x\to ax+b$，$a\neq 0$给出直线的变换的集合成一个变换群。证明这个群与习题7第1题里给出的群是同构的。

〔证〕：记变换 $x\to ax+b$ 为 $\sigma_{(a,b)}$，令 $T=\{\sigma_{(a,b)}\mid x\sigma_{(a,b)}=ax+b\}$

∵映照 $x\to ax+b$ 显然是映上的且1－1的。

∴T是1－1变换的集合。又因

(i) 任取 $\sigma_{(a,b)}$，$\sigma_{(c,d)}\in T$。则

$$x(\sigma_{(a,b)}\sigma_{(c,d)})=(ax+b)\sigma_{(c,d)}=c(ax+b)+d=acx+bc+d=x\sigma_{(ac,bc+d)}$$

∴$\sigma_{(a,b)}\sigma_{(c,d)}=\sigma_{(ac,bc+d)}\in T$。

(ii) $\sigma_{(1,0)}$ 是T中的恒等元素：$\sigma_{(1,0)}\sigma_{(a,b)}=\sigma_{(a,b)}\sigma_{(1,0)}=\sigma_{(a,b)}$

(iii) $\sigma_{(a^{-1},-a^{-1}b)}\in T$ 是 $\sigma_{(a,b)}$ 的逆元素：

$\sigma_{(a^{-1},-a^{-1}b)}\sigma_{(a,b)}=\sigma_{(a,b)}\sigma_{(a^{-1},-a^{-1}b)}=\sigma_{(1,0)}$ 故T为变换群。

记

令 $\sigma_{(a,b)}\to(a,b)=\sigma'_{(a,b)}$

这个对应显然是1－1且映上的。

$\because \sigma(a,b)\sigma(c,d)=\sigma(ac,bc+d)$

$\therefore (\sigma(a,b)\sigma(c,d))'=\sigma'(ac,bc+d)=(ac,bc+d)$

而$\sigma'(a,b)\sigma(c,d)=(a,b)\cdot(c,d)=(ac,bc+d)$

$\therefore (\sigma(a,b)\sigma(c,d))'=\sigma'(a,b)\sigma'(c,d)$

∴这个对应是同构对应。

即变换群T与实数二维组(a,b)，$a\neq 0$对于给定合成法所构成的群同构

6．验证由(x、y)→(x+a，0)所定义的平面上变换的全体关于积合成组成群。它是一个变换群吗?

〔证〕记变换(x，y)→(x+a，0)为σ_a，令G={σ_a | a为实数}任取σ_a，$\sigma_b\in G$。

$(x,y)(\sigma_a\sigma_b)=(x+a,0)\sigma_b=(x+a+b,0)=(x,y)\sigma_{a+b}$

$\therefore \sigma_a\sigma_b=\sigma_{a+b}\in G$。

σ_0是G中的恒等元：$\sigma_0\sigma_a=\sigma_a\sigma_0=\sigma_a$

$\sigma_{-a}\in G$是σ_a的逆元：$\sigma_{-a}\sigma_a=\sigma_a\sigma_{-a}=\sigma_0$

又，变换的乘积当然满足结合律，故G成群。

但因(x,y)→(x+a,o)不是平面上映上的1－1的变换，故G不是一个变换群。

习 题 12

1．写出S_3的正则实现

〔解〕：依习题11第2题里的记号，并把σ_i简记为i。i=1，2，…6则S_3的(右)正则实现为：

$\sigma_1\to\sigma_{1r}=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$，$\sigma_2\to\sigma_{2r}=\begin{pmatrix}1&2&3&4&5&6\\2&1&5&6&3&4\end{pmatrix}$

$\sigma_3 \to \sigma_{3r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$, $\sigma_4 \to \sigma_{4r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix}$

$\sigma_5 \to \sigma_{5r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}$, $\sigma_6 \to \sigma_{6r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

习 题 13

1．把12阶循环群的子群列成一表

〔解〕：设〔a〕是12阶循环群，$a^{12} = 1$

则〔a〕的子群共有$d(12) = 6$个，它们是：

〔a〕，〔a^2〕，〔a^3〕，〔a^4〕，〔a^6〕，〔a^{12}〕$= \{1\}$。

2．令$Z = 〔a〕$是r（$< \infty$）阶循环群，求证：a^m的阶是$〔m, r〕/m = r/(m, r)$。

〔证〕：令$d = (m, r)$表示m，r的最大公约数，于是有

$$m = dm_1, \quad r = dr_1, \quad (m_1, r_1) = 1.$$

$\because (a^m)^{r/(m,r)} = (a^m)^{\frac{r}{d}} = (a^r)^{m_1} = 1^{m_1} = 1$

又假设s是使$(a^m)^s = 1$的任意正整数，则

由$a^{ms} = 1$有$r \mid ms$。$\therefore dr_1 \mid dm_1 s$，$r_1 \mid m_1 s$。

$\because (r_1, m_1) = 1$。$\therefore r_1 \mid s$，即$\frac{r}{d} \mid s$。

$\therefore \frac{r}{d}$是使得$(a^m)^s = 1$最小的正整数，$\therefore a^m$的阶为$\frac{r}{d} = \frac{r}{(m, r)}$

又$\because 〔m, r〕$表示m与r的最小公倍数，而$mr = 〔m, r〕 \cdot (m, r)$，

$\therefore \frac{〔m, r〕}{m} = \frac{r}{(m, r)}$是$a^m$的阶。

3．求证：r阶循环群恰含有$\phi(r)$个生成元素，这里$\phi(r)$（欧拉(Euler)的ϕ函数）表示$< r$而与r互质（亦