§4.群

- 群的基本概念
- 群的性质
- 群中元素的阶
- 循环群
- 置换群（*）
- 子群
- 陪集与拉格朗日(Lagrange)定理

§4.群

定义1.群(group)

设〈G, *〉是含幺半群。若G中每个元素都有逆元，即

$\forall g(g\in G\Rightarrow g^{-1}\in G)$，则称〈G, *〉为群。

注：•群就是每个元素都有逆元的含幺半群;

•验证一个代数系统是群，必须验证以下四点：

(1)封闭性;　(2)结合律;　(3)有幺元;　(4)有逆元。

例1. $\langle I,\times\rangle$， $\langle M_{n\times n}, \times\rangle$，$\langle N_m, \times_m\rangle$，$\langle 2^X, \cap\rangle$，$\langle P[x], \times\rangle$

是群吗？

例2. 〈I, +〉是一个群……

这里： I是整数集合，+是整数加法。

例3. 〈$M_{n\times n}$, +〉是一个群……

这里： $M_{n\times n}$是n×n实矩阵的全体，+是矩阵加法。

例4. $\langle N_m, +_m\rangle$ 是一个群……

这里：$N_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$, $+_m$定义如下

$\forall [i]_m, [j]_m \in N_m$, $[i]_m +_m [j]_m = [(i+j) \bmod m]_m$。

例5. $\langle 2^X, \oplus \rangle$ **是一个群……**

这里：X是一非空集合，2^X是X的幂集，⊕是集合的环和运算，即$A \oplus B=(A\cap B')\cup(B\cap A')$。

例6. $\langle P[x],+ \rangle$ **是一个群……**

这里：P[*x*]是实系数多项式的全体，+是多项式的加法。

群例子：1.设$G=\{a^n|n\in I\},a>0,a\neq 1$,则$\langle G,\times\rangle$是群。

2.设$G=\{a|a\in C\wedge a^n=1\wedge n\in I^+\}$,则$\langle G,\times\rangle$是群。

群例子： 3.设(G, $*$)是群，X={f | f:G $\to$G}，定义X上的运算Δ如下：

$\forall f,g\in X$， $\forall x\in G$, $(f\Delta g)(x)=f(x)*g(x)$。

则(X, Δ)是群。

定义2.交换群(Abel群 加群)。

设〈G,*〉是群。若*运算满足交换律，则称〈G,*〉是交换群。

例7.例2，例3，例4，例5，例6是交换群吗？

定义3.群的阶(rank)

设〈G,*〉是群。称G的势(基数)为群〈G,*〉的阶。

注：•群的阶反映群的大小；

•由定义3知有限群的阶就是G中元素的个数；无限群的阶是G的势；群的阶统一记为|G| 。

定理1.设〈G,*〉是群，|G|≥2 。则

(1)G中每个元素的逆元是唯一的;

(2)G中无零元。

[证]. (1)由于群有结合律，所以由§1定理2可知，逆元唯一；

(2)采用反证法：若零元$0\in G$，则对任何元素$g\in G$，都有

$$0 * g=g * 0=0 \qquad (1)$$

由于G是群，每个元都有逆元。设0的逆元为g_0，则有

$$0 * g_0=g_0 * 0=e \qquad (2)$$

e为群G的幺元。根据（1），特别地有

$$0 * g_0=g_0 * 0=0 \qquad (3)$$

由(2), (3)有　$e=0$

因而对群G的任何元g，都有　　$g=g * e=g * 0=0$

故此$|G|=1$，　因而与定理所给条件$|G|\geq 2$矛盾。

定理2. 设〈G,*〉是群。则 $\forall a,b\in G$，有

(1)反身律：$(a^{-1})^{-1}=a$；

(2)鞋袜律：$(a*b)^{-1} = b^{-1}*a^{-1}$。

[证]. (1)$\forall a \in G$， $(a^{-1})^{-1}=(a^{-1})^{-1}*e$

$=(a^{-1})^{-1}*(a^{-1}*a)$

$=((a^{-1})^{-1}*a^{-1})*a$ (结合律)

$=e*a$

$=a$ ；

(2) $\forall a,b \in G$，$(a*b)^{-1}$

$= (a*b)^{-1} * e$

$= (a*b)^{-1} * (a * b * b^{-1} * a^{-1})$ (结合律)

$= ((a*b)^{-1} * (a * b)) * (b^{-1} * a^{-1})$ (结合律)

$= e * (b^{-1} * a^{-1})$

$= b^{-1} * a^{-1}$。

定理3 设〈G,*〉是群，则*运算满足消去律。即

$\forall x,y,z \in G$,

$$x * y = x * z \Rightarrow y = z \text{；}$$

$$y * x = z * x \Rightarrow y = z \text{。}$$

[证]. 只证第一式。$\forall x,y,z\in G$,

$$y = e * y$$

$$= (x^{-1}*x)* y$$

$$= x^{-1}*(x* y) \qquad (结合律)$$

$$= x^{-1}*(x* z) \qquad (条件：x * y = x * z)$$

$$= (x^{-1}*x)* z \qquad (结合律)$$

$$= e* z$$

$$= z$$

例8. 〈G,o〉是一有限群。

这里：G={e,a,b,c}, o运算的运算表如右：

o	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

表1

(1)封闭性：由表1可得；

(2)结合律：留待后证；

(3)有幺元：**e**；

(4)有逆元：$e^{-1}=e$，$a^{-1}=a$，

$b^{-1}=b$，$c^{-1}=c$。

此群一般称为Klein 4-群，又称为几何群或运动群。

注：•Klein 日耳曼民族，几何学家，我国著名几何学家苏步青是他的晚年弟子。

定理4.在有限群〈G,*〉(设|G|=n)的*运算的运算表中，每一行(每一列)都与G中元素的自然顺序构成一个置换(双射)。即每个元素在每行(列)必出现一次且只出现一次。

注：●因此n阶有限群的运算表是由G中元素的 (n个行或n个列所形成的) n个置换所构成的。这个性质来源于群中每个元素都有逆元。

定理4.

[证]. 只证关于第$i(1\leq i \leq n)$行结论成立。 设

$$G=\{a_1(=e), a_2,\ldots, a_n\}$$

构造自然映射 f_i:$G\to G$ 使得

对任何的$a\in G$， $f_i(a)=a_i * a$

为此，只须证明f_i是一双射函数即可。

①后者唯一：

$\forall a_j, a_k \in G$， $a_j = a_k$

$\Rightarrow a_i * a_j = a_i * a_k$

$\Rightarrow f_i(a_j) = f_i(a_k)$ ；

②单射：

$\forall a_j, a_k \in G$， $f_i(a_j) = f_i(a_k)$

$\Rightarrow a_i * a_j = a_i * a_k$

$\Rightarrow a_j = a_k$ (消去律)；

……

③满射：$\forall a_j \in G$,根据群有逆元及运算封闭性知,

$\exists a_k = a_i^{-1} * a_j \in G$,使得

$f_i(a_k) = a_i * a_k$

$= a_i * (a_i^{-1} * a_j)$

$= (a_i * a_i^{-1}) * a_j$ (结合律)

$= e * a_j$

$= a_j$ 。

定义4.元素的乘幂

设〈G,*〉是群。G中元素乘幂的定义在半群定义的基础上，增补如下： $\forall x \in G$，

$$x^0 = e \quad ;$$

$$x^{-n} = (x^{-1})^n \quad (\forall n \in N)\text{。}$$

注：•将半群中元素的乘幂（在自然数N范围内进行）扩展到群中元素的乘幂是在整数I范围内进行。

•同样可以由归纳法证明，当指数为整数时，指数定律在群中成立。即任取 $x \in G$， $\forall m,n \in I$，有

(1) $x^m * x^n = x^{m+n} = x^n * x^m$；

(2) $(x^m)^n = x^{mn} = (x^n)^m$；

•证明时，固定整数m，对正整数n使用归纳法，当n是负整数时，就变成x^{-1}的正整数指数运算。

例9.在〈I,+〉群中，取$1\in I$，有

$1^0=0$, $1^n=n$； $1^{-1}=-1$, $1^{-n}=-n$； $1^n+1^{-n}=n-n=0$ ……

例10.设X是由方程$x^4=1$的4个根组成的集合，

即　$X=\{1,-1,i,-i\}$，其中$i=\sqrt{-1}$。

设×是复数乘法，其运算表如表2 。

×	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

表2

由表2可知：

$1^1=1, 1^2=1, 1^3=1, 1^4=1, \ldots$；

$(-1)^1=-1, (-1)^2=1, (-1)^3=-1, (-1)^4=1, (-1)^5=-1, \ldots$；

$(i)^1=i, (i)^2=-1, (i)^3=-i, (i)^4=1, (i)^5=i, \ldots$；

$(-i)^1=-i, (-i)^2=-1, (-i)^3=i, (-i)^4=1, (-i)^5=-i, \ldots$。

注：•本例各元素乘幂的结果中，4次乘幂的结果是1，为群的幺元；而这正好说明它们都是四次方程$x^4=1$的根；

•群的元素乘幂回归幺元是群的元素一个比较普遍的现象；它在寻找群的子群，元素的求逆，元素性质的探讨等方面都有着广泛的作用。

定义5.元素的阶(rank)

设〈G,*〉是群。$\forall g \in G$，称

$k=\min\{m:m\in N\backslash\{0\}\wedge g^m=e\}$为元素g的阶；若这样的k不存在，则称g的阶为无穷。

注：
- 元素g的阶k是使$g^m=e$成立的最小正整数；
- 由于元素的自乘幂是一次一次乘的，因此这个无穷只能是可数无穷；
- 由定义5可知，么元是群中唯一的一个一阶元素；
- 群的阶和群中元素的阶这样两个阶的概念，这是两个根本不同的概念。

例11.在Klein 4-群〈G, o〉中，幺元e的阶为1；其它元素a,b,c的阶均为2；

在例9的群〈I,+〉中，幺元0的阶为1；其他元素的阶均为无穷；

在例10的群〈X,*〉中，幺元1的阶为1；-1的阶为2；
i和-i的阶均为4。

定理5. 设〈G,*〉是群。 $\forall g \in G$，

(1)若g的阶为n，则 $g^1, g^2, \ldots, g^n(=e)$ 互不相同；

(2)若g的阶为无穷，则 $g^0 (=e), g^1, g^2, \ldots, g^n, \ldots$ 互不相同。

[证].采用反证法。

(1)否则，设有$g^i = g^j$ $(1\le i<j \le n)$，于是有

$$g^{j-i} = g^{j+(-i)}$$

$= g^j * g^{-i}$ (指数律)

$= g^i * g^{-i}$ (反证假设： $g^i = g^j$)

$=e$

即有$1\le j-i<n$，使$g^{j-i} = e$。这与g的阶为n，具有最小性，矛盾。故有$g^1,g^2,\ldots,g^n$互不相同。

例12.在例10的群〈X,*〉中,

元素i的阶为4, 所以有i^1,i^2,i^3,i^4互不相同；

-i的阶也为4，所以$(-i)^1, (-i)^2,(-i)^3 ,(-i)^4$也互不相同。

定理6. 设〈G,*〉是群。$\forall g \in G$，g与g^{-1}有相同的阶。

[证].分两种情况来证：

(1)设g的阶有限，为n。从而$g^n=e$。由于

$$(g^{-1})^n = (g^n)^{-1} \quad (\text{指数律})$$

$$= e^{-1} \quad (g^n=e)$$

$$= e$$

这说明g^{-1}的阶也是有限的，故可设其阶为m，于是有$(g^{-1})^m=e$ 。

从而由阶定义的最小性知$m \le n$；

……

其次，又由于

$g^m = ((g^{-1})^m)^{-1}$ (指数律)

$= e^{-1}$ $((g^{-1})^m = e)$

$= e$

从而由阶定义的最小性知 $n \le m$；

于是(由≤的反对称性)有$n=m$，即g和g^{-1}的阶相同。

(2)设g的阶无穷，则g^{-1}的阶也必是无穷的。否则， 设g^{-1}的阶是有限的，为m，从而$(g^{-1})^m=e$ 。

于是 $g^m=(\ (g^{-1})^m\ )^{-1}$ (指数律)

$= e^{-1}$ $((g^{-1})^m =e)$

$= e$

这说明g的阶也是有限的，故与g的阶为无穷矛盾。因此当g的阶是无穷时， g^{-1}的阶也是无穷的。

由(1)和(2)知， g和g^{-1}有相同的阶。

例13.在例10的群〈X,*〉中,元素i和-i互为逆元，

i和-i的阶均为4，相同。

定理7. 设〈G,*〉是群。 $\forall g \in G$

(1)若g的阶有限，设其为k，从而$g^k=e$ 。则

(1.1)$\forall m \in N$, $g^m = e \Leftrightarrow k \mid m$ ；

(1.2)$\forall m,n \in N$, $g^m = g^n \Leftrightarrow k \mid m-n$ ；

(2)若g的阶无限，则 $\forall m,n \in N$, $g^m = g^n \Rightarrow m=n$ 。

[证].(1)(1.1)先证$\Rightarrow$)：

若g^m＝e，则必有$k \mid m$ 。否则$k \nmid m$ ，于是，由带余除法，可设 $m=kq+r$ $(0< r< k)$，故可得 $r=m-kq$，从而

$$
\begin{aligned}
g^r &= g^{m-kq} \\
&= g^{m+(-kq)} \\
&= g^m * (g^k)^{-q} && \text{(指数律)} \\
&= e * (e)^{-q} && (g^m = e,\ g^k = e) \\
&= e * e \\
&= e
\end{aligned}
$$

故与g的阶为k，具有最小性，矛盾。

(1.1)次证$\Leftarrow$):

若$k \mid m$，则$m=kq$。于是

$$g^m = g^{kq}$$

$$=(g^k)^q \qquad \text{(指数律)}$$

$$=e^q \qquad (g^k=e\ )$$

$$=e$$

(1.2) $g^m = g^n$

$\Leftrightarrow g^m * g^{-n} = g^n * g^{-n}$

$\Leftrightarrow g^{m+(-n)} = g^{n+(-n)}$ (指数律)

$\Leftrightarrow g^{m-n} = e$ ($g^0=e$)

$\Leftrightarrow k \mid m-n$ (根据(1.1))

(2)若g的阶无限，则

$$g^m = g^n$$

$$\Rightarrow g^m * g^{-n} = g^n * g^{-n}$$

$$\Rightarrow g^{m+(-n)} = g^{n+(-n)}$$ (指数律)

$$\Rightarrow g^{m-n} = e$$ ($g^0=e$)

$$\Rightarrow m-n=0$$ (g的阶无限，只有$g^0=e$)

$$\Rightarrow m=n$$

例14.在例10的群〈X,*〉 中,

元素-1的阶是2,所以

$(-1)^2=1$, $(-1)^4=1$, $(-1)^6=1$,… , $(-1)^{2n}=1$, …;

元素i的阶是4,所以

$(i)^4=1$,$(i)^8=1$, $(i)^{12}=1$, …, $(i)^{4n}=1$, …;

元素-i的阶是4,所以

$(-i)^4=1$, $(-i)^8=1$,$(-i)^{12}=1$, …, $(-i)^{4n}=1$,…。

定理8.有限群中每个元素的阶都是有限的。设〈G,*〉是有限群，|G|＝n，则G中每个元素的阶≤n。

[证].对任一元素$g \in G$，设其阶为m，则由定理5知

$g^1, g^2, \ldots, g^m$这m个元素互不相同；

由群的封闭性知它们同时都在G中；因此有$m \le n$。

所以群G中每个元素的阶$\le n$。

例15.在例8的Klein 4-群〈G, o〉中，么元e的阶为1，其他元素a,b,c的阶均为2，均小于群的阶4；

在例10的群〈X,*〉 中,么元1的阶为1，-1的阶为2， i和-i的阶均为4，均小于等于群的阶4 。

定义6.循环群(cyclic group)

设〈G,*〉是群。若存在着元素 $g_0 \in G$，使得

$$(\forall g \in G)(\exists n \in I)(g = g_0^{\,n})$$

则称〈G, *〉为循环群；同时称 g_0 是该循环群的生成元(generating element)。并且将〈G, *〉记作(g_0)。

例16.群〈I,+〉是循环群。

在群〈I,+〉中取 1∈I，由于$0=1^0$,$n=1^n$,$-n=(-1)^n=(1^{-1})^n=1^{-n}$，故I中的每个元素都可表示成1的整数次幂。由循环群的定义知〈I,+〉是循环群，1是该循环群的生成元。

例17.群〈N_m,$+_m$〉是循环群。

在群〈N_m,$+_m$〉中，取$[1]_m \in N_m$，由于$[0]_m=([1]_m)^0$, $[i]_m= ([1]_m)^i$，故N_m中的每个元素都可表示成$[1]_m$的整数次幂。由循环群的定义知〈N_m,$+_m$〉是循环群, $[1]_m$是该循环群的生成元。

定理9. 设〈G,*〉是循环群， |G|＝n 。那么

(1)g_0是生成元$\Leftrightarrow$ g_0^{-1}是生成元；

(2)g_0是生成元$\Leftrightarrow$ g_0的阶是n 。

[证]. (1) g_0是生成元

$\Leftrightarrow (\forall g\in G)(\exists k\in I)(g=g_0^{k})$

$\Leftrightarrow (\forall g\in G)(\exists k\in I)(g=(g_0^{-1})^{-k})$ （指数律）

$\Leftrightarrow (\forall g\in G)(\exists m\in I)(g=(g_0^{-1})^{m})$ （这里：$m= - k$）

$\Leftrightarrow$ g_0^{-1}是生成元；

(2) 由于$|G|=n$， $\langle G,*\rangle$是有限群，由定理8可知$g_0\in G$的阶有限，不妨设其为m，并且$m\leq n$。

先证$\Leftarrow$)： 若g_0的阶是n，则构造集合

$$S=\{e, g_0, g_0^2, \ldots, g_0^{n-1}\},$$

根据定理5可知$|S|=n$，并且由群的封闭性知$S\subseteq G$，因此由 $|G|=n$ 可知有 $S=G$。

从而，g_0是生成元。

次证⇒)：构造集合

$$S=\{e, g_0, g_0^2, \ldots, g_0^{m-1}\}$$

根据定理5可知$|S|=m$，并且由群的封闭性知$S\subseteq G$ 。

又对任何$g\in G$，由于g_0是生成元，故存在着整数k，

使得$g=g_0^k$ 。而g_0的阶是m，则有$g_0^m = e$；根据带余除法，有

$k=qm+r \quad (0\le r<m)$,

……

从而　$g=g_0^k$

$=g_0^{qm+r}$

$=(g_0^m)^q * g_0^r$　　　　(指数律)

$=e^q * g_0^r$　　　　(因：$g^0m = e$)

$=e*g_0^r$　　　　(因：$e^q = e$)

$=g_0^r$

$\in S$　　　　(因：$0\le r<m$)

故 $G\subseteq S$；

从而 $S= G$,于是　$m= |S|=|G|=n$，　即g_0的阶是n 。

定理10. 设〈G,*〉是循环群， g_0是生成元。

(1)若g_0的阶为m，则〈G,*〉与〈N_m, $+_m$〉同构；

(2)若g_0的阶为无穷，则〈G,* 〉与 〈I,+〉同构。

[证]. (1)由条件及定理9知

$G=\{e, g_0, g_0^2, \ldots, g_0^{m-1}\}$,

$N_m=\{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$,

定义自然映射 $h: G \to N_m$，

$\forall g_0^k \in G$

$h(g_0^k) = [k]_m$,

由双射函数的定义知h是双射函数。

……

$\forall\, g_0^{\,i}$、$g_0^{\,j} \in G$

由于 $h(g_0^{\,i} * g_0^{\,j}) = h(g_0^{(i+j) \bmod m})$

$$= [(i+j) \bmod m]_m$$

$$= [i]_m +_m [j]_m$$

$$= h(g_0^{\,i}) +_m h(g_0^{\,j})$$

故h满足同态公式。

由同构的定义知h是从〈G,*〉到〈N_m, $+_m$〉的同构函数，即〈G,*〉和〈N_m, $+_m$〉同构。

(2)由于g_0的阶为无穷，故根据定理5的(2)有

$$e(=g_0^0),\ g_0,\ g_0^2, \ldots, g_0^n, \ldots \qquad ①$$

互不相同。

根据定理6，g_0和g_0^{-1}有相同的阶，故与上同理可得

$$g_0^{-1}, g_0^{-2}, \ldots, g_0^{-n}, \ldots \qquad ②$$

互不相同。

……

另外①与②中任何一对元素g_0^i和g_0^{-j}互不相同。否则有

$i \geq 0, j>0$(故有$i+j>0$),使得$g_0^i = g_0^{-j}$， 于是

$$g_0^{i+j} = g_0^i * g_0^j = g_0^{-j} * g_0^j = e$$

这说明g_0的阶有限，与g_0的阶为无穷矛盾。

于是有

$$G = \{\ldots, g_0^{-n}, \ldots, g_0^{-2}, g_0^{-1}, e, g_0, g_0^2, \ldots, g_0^n, \ldots\}$$

……

定义自然映射 $h:G\rightarrow I$， $h(g_0^k)=k$ 。

$\forall k\in I$有原象$g_0^k\in G$，使$h(g_0^k)=k$ 。故h是满射的。

若$h(g_0^i)=h(g_0^j)$, 即$i=j$，则有$g_0^i=g_0^j$ ，即h是单射的。

于是，由双射函数的定义可知h是双射函数。

$$h(g_0^i*g_0^j)=h(g_0^{i+j})=i+j=h(g_0^i)+h(g_0^j)$$

故h满足同态公式。

由同构的定义知h是从〈G,*〉到〈I,+〉的同构函数，即〈G,*〉和〈I,+〉同构。

定理11. 循环群一定是交换群。

[证].仿§3定理2可证。

定义7.置换群(permutation group)

设所有n次置换构成的集合为S_n，$A \subseteq S_n$, $A \neq \varnothing$, $\diamond$是置换的合成运算。若〈A, ◇〉构成群，则称〈A, ◇〉为一(n次)置换群。

例18.设在三维空间有一矩形方框如图1所示。四个顶点分别标记为1,2,3,4。 用这些标记来表示矩形方框的运动。

将方框的运动用置换的方式表示：

令 e:不动 (在平面内绕原点旋转360°)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

a:绕横轴旋转180 °(上下翻转)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

b: 绕纵轴旋转180 °(左右翻转)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

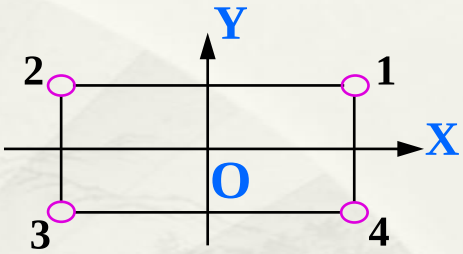

图1

c:在平面内绕原点旋转180°

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

令A={e,a,b,c}， ◇为置换的合成运算。

下面用置换的合成来定义旋转的复合运动。

a ◇ b意味着先旋转a再旋转b。于是得到A上的置换合成表如下：

例如

$$a \diamond b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = c$$

◇	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

表3

由表3知，这正是 在前面例8所讲的Klein 4-群。

由于置换的合成运算◇就是关系的合成运算o，故◇运算满足结合律。这正好回答了前面例8所遗留的问题。

由于Klein 4-群〈A, ◇〉是由几何形刚体在空间的运动所产生的，这正是 把它称为几何群、运动群的原因。

另外由表3明显得知，这个置换群还是一个交换群。

注：•在例18中可以看到刚体在空间的运动可以由4次置换来描述；但并不是任何4次置换都表示刚体在空间中的运动。如在例18中，置换 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$

就不代表任何刚体运动。

•由于4个元素的置换应有4!= 24个，而在例18中只取了其中的4个置换，没有取完，所以$A \subset S_4$。

定理12.n个元素的非空集合X上的所有n次置换构成的集合S_n，在置换的合成运算$\diamond$下构成一置换群〈S_n,$\diamond$〉。 称为n次对称群(group of symmetry),简记为S_n 。

[证].

(1)封闭性：因为任意两个n次置换P_i，P_j的合成$P_i \diamond P_j$仍为一个n次置换，且结果唯一， 即

$$\forall P_i, P_j, P_i \in S_n \wedge P_j \in S_n \Rightarrow P_i \diamond P_j \in S_n ;$$

(2)结合律：置换的合成运算◇满足结合律；

(3)有幺元；关于◇运算的幺元是n次恒等置换I，即

$$\exists I\in S_n, \forall P\in S_n, I\diamond P=P\diamond I=P$$

(4)有逆元；由于任一n次置换P的逆置换P^{-1}仍是一n次置换，即$P^{-1}\in S_n$，故S_n中任一元素P都有逆元P^{-1}，即

$$\forall P\in S_n, \exists P^{-1}\in S_n, P\diamond P^{-1}=P^{-1}\diamond P=I。$$

例19. 此例讨论一个由所有置换构成的群。为了简单起见，取X=｛1,2,3｝，3个元素的置换有3！=6个。

$$S_3=\{\sigma_1, \sigma_2,\sigma_3, \sigma_4, \sigma_5, \sigma_6\}=\{e, \tau, \sigma^2\tau, \sigma\tau, \sigma, \sigma^2\}$$

用轮换的形式写出来是

$$\sigma_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}=(1)=e=\sigma^3=\tau^2 \qquad \sigma_4=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}=(23)=\sigma\tau$$

$$\sigma_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}=(12)=\tau \qquad \sigma_5=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=(123)=\sigma$$

$$\sigma_3=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}=(13)=\sigma^2\tau \qquad \boldsymbol{\sigma_6=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}=(132)=\sigma^2}$$

其运算表如下：

$\diamond$	e	τ	$\sigma^2\tau$	$\sigma\tau$	σ	σ^2
e	e	τ	$\sigma^2\tau$	$\sigma\tau$	σ	σ^2
τ	τ	e	σ	σ^2	$\sigma^2\tau$	$\sigma\tau$
$\sigma^2\tau$	$\sigma^2\tau$	σ^2	e	σ	$\sigma\tau$	τ
$\sigma\tau$	$\sigma\tau$	σ	σ^2	e	τ	$\sigma^2\tau$
σ	σ	$\sigma\tau$	τ	$\sigma^2\tau$	σ^2	e
σ^2	σ^2	$\sigma^2\tau$	$\sigma\tau$	τ	e	σ

表4

由表4知

(1) $\diamond$是S_3上的二元运算,具有封闭性；

(2) 置换的合成运算◇满足结合律；

(3) e是关于◇运算的幺元；

(4) $e, \tau, \sigma^2\tau, \sigma\tau$ 的逆元是其本身； σ, σ^2互为逆元。

由群的定义可知〈S_3,◇〉是群，因而是置换群。 称其为三次六阶对称群。由表4易知其不是交换群，因而它是最小的非交换群。

〈S_3,◇〉实际上可看作是由两个较小的置换群〈H_1,◇〉和〈H_2,◇〉的乘积得到的，这里： $H_1=\{e, \tau\}$， $H_2=\{e, \sigma, \sigma^2\}$ 。这就引出了子群及Lagrange定理，还有群的构造等问题。

定理13.（Cayley定理）任何n阶有限群〈G,*〉都与一n次置换群同构。

[证].设|G|＝n，G=｛a_1(=e),a_2,…,a_n｝。

则令A=｛P_1,P_2,…,P_n｝，其中：

$$P_i=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 * a_i & a_2 * a_i & \cdots & a_n * a_i \end{pmatrix} \qquad (1 \le i \le n)$$

显然P_1,P_2,…,P_n是*运算的运算表中n个列置换，由本节定理4知，它们是n个互不相同的n次置换，即|A|＝n 。◇是置换的合成运算，则：

(一)〈A,◇〉是一n次置换群

(1)封闭性：对任何P_i，$P_j \in A$，对应着$a_i, a_j \in G$，由群〈G,*〉的封闭性知，存在着$a_k \in G$，使 $a_i * a_j = a_k$。而a_k对应着列置换$P_k \in A$。于是对任何$x \in G$，都有

$$(P_i \diamond P_j)(x) = P_j(P_i(x)) = (x * a_i) * a_j = x * (a_i * a_j) = x * a_k = P_k(x)$$

所以 $P_i \diamond P_j = P_k \in A$。

故合成运算◇关于置换集合A封闭；

(2)结合律：置换的合成运算$\diamond$满足结合律；

(3)有幺元； $P_1 \in A$是关于$\diamond$运算的幺元；

因为，对任何$P_i \in A$,都有 对任何$x \in G$，都有

$$(P_1 \diamond P_i)(x)=P_i(P_1(x))=(x*a_1)*a_i=x*(a_1*a_i)=x*(e*a_i)=x*a_i=P_i(x)$$

$$(P_i \diamond P_1)(x)=P_1(P_i(x))=(x*a_i)*a_1=x*(a_i*a_1)=x*(a_i*e)=x*a_i=P_i(x)$$

所以 $P_1 \diamond P_i=P_i= P_i \diamond P_1$

故$P_1 \in A$是关于$\diamond$运算的幺元；

(4)有逆元；对任何$P_i \in A$，对应着$a_i \in G$，由群(G,*〉有逆元知，存在着$a_j \in G$，使$a_i^{-1} = a_j$。而a_j对应着列置换$P_j \in A$。于是对任何$x \in G$，都有

$$(P_i \diamond P_j)(x)=P_j(P_i(x))=(x*a_i)*a_j=x*(a_i*a_j)=x*e=x*a_1=P_1(x)$$

$$(P_j \diamond P_i)(x)=P_i(P_j(x))=(x*a_j)*a_i=x*(a_j*a_i)=x*e=x*a_1=P_1(x)$$

所以 $P_i \diamond P_j=P_1 = P_j \diamond P_i$

故$P_i^{-1} = P_j \in A$是P_i关于◇运算的逆元；

由群的定义知〈A,◇〉是群。因此〈A,◇〉是n次置换群。

(二)群〈G,∗〉与n次置换群〈A,◇〉同构

定义自然映射 $h:G\rightarrow A$

对任何$a_i\in G$， $h(a_i)= P_i$

(1)h是双射函数：由定义显然；

(2)h满足同态公式：

对任何$a_i,a_j\in G$，由群〈G,∗〉的封闭性知，

存在着$a_k\in G$，**使** $a_i*a_j = a_k$ **，。。。**

于是　对任何$x \in G$，都有

$$h(a_i*a_j)(x)=h(a_k)(x)$$
$$= P_k(x)$$
$$=x*a_k$$
$$=x*(a_i*a_j)$$
$$=(x*a_i)*a_j$$
$$=P_j(P_i(x))$$
$$=(P_i \diamond P_j)(x)$$
$$=(h(a_i)\diamond h(a_j))(x)$$

所以　$h(a_i*a_j)=h(a_i)\diamond h(a_j)$；　因此〈G,*〉与〈A,◇〉同构。

定义8.子群(subgroup)

若群〈G,∗〉的子代数系统〈S,∗〉也是群，则称〈S,∗〉是〈G,∗〉的子群。

注：•验证子群，除了验证子代数系统的

(1)$S \subseteq G$ ；　　　　(2)$S \neq \varnothing$ ；

(3) *运算关于S封闭；

还应该验证

(4) 有幺元(并与群G 中的幺元重合)；

(5) 有逆元(并与群G 中的同一元的逆元重合)　；

而结合律则不须验证，因为根据本章§1定理3可知，遗传。

•群〈S,*〉是群〈G,*〉的子群， 简记为$S<G$ ；

定理14.设〈G,∗〉是群， $S \subseteq G$ 且$S \neq \varnothing$ 。那么

〈S,∗)是〈G,∗〉的子群⇔

$$\left.\begin{array}{l}(1)\text{封闭性：}\forall a \forall b(a \in S \wedge b \in S \Rightarrow a*b \in S) \\ (2)\text{有逆元：}\forall a(a \in S \Rightarrow a^{-1} \in S)\end{array}\right\} \quad (*)$$

[证].先证$\Rightarrow$):

由于〈S,$*$〉是〈G,$*$〉的子群，故〈S,$*$〉是群。因而

(1)有封闭性：$\forall a \forall b(a \in S \wedge b \in S \Rightarrow a*b \in S)$

这就证明了条件(*) (1)；

(2)有幺元：暂设其为e_s；

(3)有逆元：即对任何$a \in S$，都存在着$b \in S$，使

$$b*a = a*b = e_s \quad ;$$

……

下面来证两点，即条件(*) (2) ：

(a) e_s =e，即子群〈 S,*〉的幺元e_s与大群〈G,*〉的幺元e重合；从而说明e∈S。

(b) b= a^{-1}，即任一元素a∈S在子群〈S,*〉中的逆元b与其在大群〈G,*〉中的逆元a^{-1}重合；从而说明a^{-1}∈S，

……

首先，由于$e_s, e\in G$，因此有

$e_s*e = e_s$ (因e是群〈G,*〉的幺元)

$e_s*e_s = e_s$ (因e_s是群〈S,*〉的幺元)

故有 $e_s*e_s = e_s*e$

于是由群〈G,*) 的消去律可得

$e_s =e$ ；

……

其次 $b=b*e$

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

$=(b*a)*a^{-1}$（结合律）

$=e*a^{-1}$ （b是a在子群〈S,*)中的逆元且$e_s=e$）

$=a^{-1}$ ；

次证$\Leftarrow$)：只需验证〈S,$*$〉是群即可

(1)封闭性：条件($*$) (1)保证；

(2)结合律：遗传；

(3)有幺元：由于$S\neq\varnothing$，故必至少有某一元素$a_0\in S$，于是由条件($*$) (2)有$a_0^{-1}\in S$，从而由条件($*$) (1)有

$$e=a_0*a_0^{-1}\in S \quad ;$$

(4)有逆元：条件($*$) (2)保证；

故〈S,$*$〉是群；所以〈S,$*$〉是〈G,$*$〉的子群。

定理15.设$\langle G,*\rangle$是群， $S\subseteq G$ 且$S\neq\varnothing$ 。那么

$\langle S,*\rangle$是$\langle G,*\rangle$的子群$\Leftrightarrow$

(混合)封闭性：$\forall a\forall b(a\in S\wedge b\in S\Rightarrow a*b^{-1}\in S)$ (**)

[证]. 证明：定理15条件(**)$\Leftrightarrow$定理14条件(*)

先证$\Rightarrow$)：

(1)有逆元：由于$S \neq \varnothing$，故必至少有某一元素$a_0 \in S$，于是重复有$a_0 \in S$，从而由条件(**) 有 $e=a_0*a_0^{-1} \in S$

因此，对任何$a \in S$，由于$e \in S$已证，故由条件(**) 有

$$a^{-1} = e*a^{-1} \in S$$

这样，定理14条件(*)(2)得证；

(2)封闭性：对任何$a,b\in S$，由已证(1)有逆元有$b^{-1}\in S$,从而由条件(**) 有 $a*b=a*(b^{-1})^{-1}\in S$

故定理14条件(*)(1)得证。

次证$\Leftarrow$)：对任何$a,b\in S$，根据定理14条件(*)(2)有逆元有$b^{-1}\in S$,再根据定理14条件(*)(1)封闭性有

$$a*b^{-1}\in S$$

故条件(**) (混合)封闭性得证。

定理16.设〈G,∗〉是有限群，|G|＝n，$S\subseteq G$且$S\neq\varnothing$。那么〈S,∗〉是〈G,∗〉的子群⇔

封闭性：$\forall a\forall b(a\in S\wedge b\in S\Rightarrow a*b\in S)$ (***)

[证].先证⇒)：由于〈S,∗〉是〈G,∗〉的子群，故〈S,∗〉是群，因而具有封闭性：$\forall a\forall b(a\in S\wedge b\in S\Rightarrow a*b\in S)$

这就证明了条件(***)。

次证$\Leftarrow$)：只需验证〈 S,$*$〉是群即可

(1)封闭性：条件(***) 保证；

(2)结合律：遗传；

(3)有幺元：由于$S\neq\varnothing$，故必至少有某一元素$a_0\in S$，由$S\subseteq G$知$a_0\in G$；由$|G|=n$，根据定理8知a_0的阶有限，设其为k，$k\leq n$，则有$a_0^k = e$，于是由已证之封闭性有

$$e=a_0^k\in S \quad ;$$

………

(4)有逆元：对任何$a\in S$，由$S\subseteq G$知$a\in G$；由$|G|=n$，根据定理8知a的阶有限，设其为m，$m\le n$，则有$a^m=e$；

① $m=1, a=e, a^{-1}=e$,

② $m>1$,于是由已证之封闭性有$a^{m-1}\in S$，从而有

$a*a^{m-1}=a^m=e$， $a^{m-1}*a=a^m=e$；

所以 $a^{-1}=a^{m-1}\in S$；

故〈S,∗〉是群；所以〈S,∗〉是〈G,∗〉的子群。

例20.平凡子群。

设〈G,*〉是群，则〈{e},*〉和〈G,*〉是〈G,*〉的两个子群。由于每个群都有这样的子群，且这两个子群对问题的研究价值不大。故称这两个子群是〈G,*〉的平凡子群。

例21.循环群的子群是循环群。即若〈G,∗〉是循环群且〈S,∗〉是〈G,∗〉的子群，则〈S,∗〉是循环群。

[证].由子群的定义知〈S,∗〉是群。下证〈S,∗〉是循环群。

设g_0是〈G,∗〉的生成元，于是由$S \subseteq G$ 知S中的每个元素都可表示成g_0^n， $n \in I$。设m是S诸元素中方次最小的正方幂。下证g_0^m是S的生成元。

任取$x \in S$，则有$k \in I$ 使$x=g_0^k$ 。根据带余除法，

有 $k=qm+r \quad (0 \le r < m)$

于是有 $g_0^r = g_0^{k-qm}$

$= g_0^k * (g_0^m)^{-q}$ (指数律)

由于$g_0^k = x \in S$、$g_0^m \in S$ ，有$(g_0^m)^{-q} \in S$，故由群〈 S,*〉的封闭性可得$g_0^r \in S$ 。

而m是S中诸元素的最小正方幂，故有r=0。即有

$$x = g_0^k = g_0^{qm} = (g_0^m)^q$$

即g_0^m是〈S,*〉的生成元。

于是由循环群的定义知〈S,*〉是循环群。

例22. 设〈G,∗〉是群。令

$$S = \{c : c \in G \wedge (\forall g \in G)(c*g=g*c)\}$$

则〈S,∗〉是〈G,∗〉的子群。

称此子群〈S,∗〉是群〈G,∗〉的中心。

[证]. (1)$S \subseteq G$ ： 由S的定义显然；

(2)$S \neq \varnothing$：有幺元$e \in G$，使得$(\forall g \in G)(e*g=g*e)$，故有 $e \in S$；

(3)(混合)封闭性：$\forall a\forall b(a\in S\wedge b\in S\Rightarrow a*b^{-1}\in S)$

对于任何的$a,b\in S$，则有$a,b\in G$，且对任何$g\in G$， $a*g=g*a$，$b*g=g*b$，

对后一等式左右两边，前后同乘$b^{-1}\in G$，得到$g*b^{-1} = b^{-1}*g$ 即 $b^{-1}*g =g*b^{-1}$，

因此有$a*b^{-1}\in G$，使得 对任何$g\in G$

$(a*b^{-1}) *g = a*(b^{-1}*g)$ (结合律)

$= a*(g*b^{-1})$ $(b^{-1}*g =g*b^{-1})$

$= (a*g)*b^{-1}$ (结合律)

$= (g*a)*b^{-1}$ $(a*g=g*a)$

$= g*(a*b^{-1})$ (结合律)因此 $a*b^{-1}\in S$；

所以，根据定理15可知，〈S,∗〉是〈G,∗〉的子群。

子群例子：

*陪集和Lagrange定理

定义9.陪集(coset)

设〈G,$*$〉是群，〈H,$*$〉是〈G,$*$〉的子群。对于任何元素$a\in G$，

(1)由a所确定的H在G中的左陪集(left coset)定义为

$$aH=\{a*h:h\in H\}$$

(2)由a所确定的H在G中的右陪集(right coset)定义为

$$Ha=\{h*a:h\in H\}$$

称元素a是左陪集aH及右陪集Ha的代表元素，简称代表元。

陪集例子：

例23.已知〈 $S_3,\diamond$〉是三次六阶置换群。其中

$$S_3=\{(1),(12),(13),(23),(123),(132)\}$$

〈 $H_1,\diamond$〉是〈$S_3,\diamond$〉的子群，其中$H_1=\{(1),(12)\}=\{e,\tau\}$，

则H_1的左陪集：

$(1)H_1$,$(12)H_1$；$(13)H_1$,$(132)H_1$ ；$(23)H_1$,$(123)H_1$ ；

H_1的右陪集：

$H_1(1)$, $H_1(12)$；$H_1(13)$, $H_1(123)$；$H_1(23)$, $H_1(132)$ ；

注：•$e \in H$，因为〈$H,\diamond$〉是子群；$a=a*e \in aH$， $a=e*a \in Ha$，代表元在它所代表的陪集之中；

•一般地，$aH \neq Ha$，例如，在上例中

$$(123)H_1=\{(23),(123)\}\neq\{(13),(123)\}=H_1(123)$$

•如果$(\forall a \in G)(aH=Ha)$，则称〈 $H,*$〉是〈 $G,*$〉的**正规子群**或**不变子群**，记为$H \lhd G$。

定理17.设〈 H,*〉是群〈 G,*〉的子群。令

$$\left.\begin{array}{l}(1)S_l=\{aH: a\in G\} \\ (2)S_r=\{Ha: a\in G\}\end{array}\right\}(此表示去掉重复元素\ )$$

则S_l，S_r均是G的划分。

[证].只证S_l构成G上的划分。

为证S_l是G的划分，根据划分的定义，应证明如下两点：

(a) $\bigcup_{aH\in S_l} aH=G$；

(b)$(\forall a\in G)(\forall b\in G)(aH=bH \vee aH \cap bH=\varnothing)$；

先证(a) $\bigcup_{aH\in S_l} aH = G$；

对于任何$aH\in S_l$，都有$a\in G$，$H\subseteq G$，从而由群 (G,*)的封闭性得到 $aH\subseteq G$，故此，由并是包含关系的上确界可得 $\bigcup_{aH\in S_l} aH \subseteq G$；

又对于任何的$a\in G$，有 $a\in aH\subseteq \bigcup_{aH\in S_l} aH$，故有 $G\subseteq \bigcup_{aH\in S_l} aH$；

所以，由包含关系的反对称性，得到 $\bigcup_{aH\in S_l} aH = G$；

次证(b) $(\forall a\in G)(\forall b\in G)(aH=bH \vee aH\cap bH=\varnothing)$；

对任何$a,b\in G$，若$aH\cap bH=\varnothing$，则问题已证；否则若$aH\cap bH\neq\varnothing$，则必至少有一元素$x_0\in aH\cap bH$，从而

$x_0\in aH\cap bH$

$\Rightarrow x_0\in aH \wedge x_0\in bH$

$\Rightarrow x_0=a*h_1 \wedge x_0=b*h_2$ (这里$h_1, h_2\in H$)

$\Rightarrow a*h_1=b*h_2$

$\Rightarrow$ **$a=b*h_2*h_1^{-1} \wedge b=a*h_1*h_2^{-1}$ (*)**

下面 来证：$aH=bH$。为此，要分证：

① $aH\subseteq bH$； ② $bH\subseteq aH$；

只证①；

对任何元素y，

$y \in aH$

$\Rightarrow y = a * h'$ (这里$h' \in H$)

$\Rightarrow y = b * h_2 * h_1^{-1} * h'$ (由(*)： $a = b * h_2 * h_1^{-1}$)

$\Rightarrow y = b * h''$ (由H的封闭性： $h'' = h_2 * h_1^{-1} * h' \in H$)

$\Rightarrow y \in bH$

所以 $aH \subseteq bH$；

所以，由包含关系的反对称性， 得到

$aH = bH$ 。

所以，左陪集全体S_l是G的一个划分。

定理18.设〈H,*〉是群〈G,*〉的子群。则有

(1) $(\forall a\in G)(|aH|=|H|)$；

(2) $(\forall a\in G)(|Ha|=|H|)$；

[证].只证(1)

建立自然映射 $f: H\to aH$ 使得

对任何$h\in H$， $f(h)=a*h$

于是

①后者唯一：由$*$运算的结果唯一性可得；

②满射：对任何 $y\in aH$，有$x = h\in H$，使得$y = a*h$，于是，

有 $f(x)= f(h)=a*h = y$ ；

③单射： $f(h_1)= f(h_2)$

$\Rightarrow a*h_1 = a*h_2$

$\Rightarrow h_1= h_2$ （群有消去律）。

定理19.群〈 G,∗〉的子群〈 H,∗〉的不同左陪集的个数等于它的不同右陪集的个数。即

$$|S_l| = |S_r| 。$$

[证].建立映射 $f: S_r \to S_l$ 使得

对任何 $Ha \in S_r$， $f(Ha)=a^{-1}H$

于是

(1)后者唯一：对任何$Ha,Hb\in S_r$，若$Ha=Hb$，须证：$f(Ha)=f(Hb)$，即要证：$a^{-1}H = b^{-1}H$；

为此，要分证：

① $a^{-1}H \subseteq b^{-1}H$；

② $b^{-1}H \subseteq a^{-1}H$；

只证①；

对任何元素y， $y \in a^{-1}H$

$\Rightarrow y = a^{-1} * h_1$ (这里$h_1 \in H$)

$\Rightarrow y^{-1} = (a^{-1} * h_1)^{-1}$

$= h_1^{-1} * a$ (鞋袜律，反身律)

$\Rightarrow y^{-1} \in Ha$ (因为群有逆元故$h_1^{-1} \in H$)

$\Rightarrow y^{-1} \in Hb$ (条件$Ha=Hb$)

$\Rightarrow y^{-1} = h_2 * b$ (这里$h_2 \in H$)

$\Rightarrow y = (y^{-1})^{-1}$ (反身律)

$= (h_2 * b)^{-1}$

$= b^{-1} * h_2^{-1}$ (鞋袜律)

$\Rightarrow y \in b^{-1}H$ (因为群有逆元故$h_2^{-1} \in H$)

所以 $a^{-1}H \subseteq b^{-1}H$； 由包含关系的反对称性， 得到 $a^{-1}H = b^{-1}H$ 。

(2) 满射：对任何 $aH\in S_l$，有$Ha^{-1}\in S_r$，使得

$f(Ha^{-1})= (a^{-1})^{-1}H = aH$；

(3)单射：对任何$Ha,Hb\in S_r$，若$f(Ha)= f(Hb)$，即

有 $a^{-1}H = b^{-1}H$，须证： $Ha=Hb$；

为此，要分证：

① $Ha\subseteq Hb$；

② $Hb\subseteq Ha$；

只证①；

对任何元素y， $y \in Ha$

$$\Rightarrow y = h_1 * a \qquad (这里h_1 \in H)$$

$$\Rightarrow y^{-1} = (h_1 * a)^{-1}$$

$$= a^{-1} * h_1^{-1} \qquad (鞋袜律)$$

$$\Rightarrow y^{-1} \in a^{-1}H \qquad (因为群有逆元故h_1^{-1} \in H)$$

$$\Rightarrow y^{-1} \in b^{-1}H \qquad (条件a^{-1}H = b^{-1}H)$$

$$\Rightarrow y^{-1} = b^{-1} * h_2 \qquad (这里h_2 \in H)$$

$$\Rightarrow y = (y^{-1})^{-1} \qquad (反身律)$$

$$= (b^{-1} * h_2)^{-1}$$

$$= h_2^{-1} * b \qquad (鞋袜律，反身律)$$

$$\Rightarrow y \in Hb \qquad (因为群有逆元故h_2^{-1} \in H)$$

所以 $Ha \subseteq Hb$；由包含关系的反对称性， 得到 $Ha = Hb$ 。

注：• 实际上已经证明了：　$Ha = Hb \Leftrightarrow a^{-1}H = b^{-1}H$；

在(1)后者唯一中　证明的是：　$Ha = Hb \Rightarrow a^{-1}H = b^{-1}H$；

在(3)单射中　证明的是：　$a^{-1}H = b^{-1}H \Rightarrow Ha = Hb$；

•因此　实际上也可得到：$aH= bH \Leftrightarrow Ha^{-1} =Hb^{-1}$；

因为　$aH= bH \Leftrightarrow (a^{-1})^{-1}H = (b^{-1})^{-1}H$

$\Leftrightarrow Ha^{-1} =Hb^{-1}$　(利用$Ha = Hb \Leftrightarrow a^{-1}H = b^{-1}H$)。

定义10. 指数（exponent）

子群〈 H,∗〉关于群〈 G,∗〉的不同左陪集(或右陪集)的个数(或势)称为群〈 G,∗〉关于子群〈 H,∗〉 的指数。记为 $|G/H|$ 。

注：•根据定义有 $|G/H| = |S_l| = |S_r|$ ；

定理20.拉格朗日(Lagrange)定理

设〈 H,∗〉是有限群〈 G,∗〉的子群。则有

$|G| = |G/H|\cdot|H|$ （或 $|G/H|=|G|/|H|$ ）。

[证].由于〈 G,∗〉是有限群，故指数|G/H|是有限的(分类个数不会超过总元素个数)，故可设|G/H| =k 。

于是，由定理17，有k个元$a_1, a_2, \ldots, a_k \in G$，使得

$G= a_1H \cup a_2H \cup \ldots \cup a_kH$ 并且 $a_iH \cap a_jH= \varnothing$ $(1 \leq i \neq j \leq k)$

从而有

$$|G| = |a_1H| + |a_2H| + \ldots + |a_kH|$$

$$= \underbrace{|H| + |H| + \ldots + |H|}_{k个} \qquad (定理18\ (\forall a \in G)(|aH|=|H|))$$

$$=k \cdot |H|$$

$$=|G/H| \cdot |H|\ 。$$

注：•在定理的证明中， 用的是左陪集；根据定理19，用右陪集一样可证得拉氏定理。

•根据拉氏定理显然可得:

①子群的阶一定整除大群的阶；即$|H| \mid |G|$

因此，寻找子群，只须寻找以大群阶的因子为阶数的子群;

②左陪集的个数一定整除大群的阶；即$|S_l| \mid |G|$；

右陪集的个数一定整除大群的阶；即$|S_r| \mid |G|$；

大群关于子群的指数一定整除大群的阶；即$|G/H| \mid |G|$；

即，左陪集的个数、右陪集的个数、指数都是大群阶的因子。

例24. 在例23中三次对称群S_3的阶是6,故S_3的非平凡子群是：

2阶群 $H_1=\{(1),(12)\}=\{e,\tau\}$

3阶群 $H_2=\{(1), (123), (132)\}=\{e, \sigma, \sigma^2\}$

H_1(不同)的左陪集为三个：$\{(1),(12)\}=\{e,\tau\}$,

$\{(13),(132)\}=\{\sigma^2\tau , \sigma^2\}$, $\{(23),(123)\}=\{\sigma\tau , \sigma\}$

H_1(不同)的右陪集为三个：$\{(1),(12)\}=\{e,\tau\}$,

$\{(13),(123)\}=\{\sigma^2\tau , \sigma\}$, $\{(23),(132)\}=\{\sigma\tau , \sigma^2\}$

H_2(不同)的左陪集为二个：

$$\{(1),(123)\ ,(132)\} = \{e,\ \sigma,\ \sigma^2\}\ ,\qquad \{(12),(13),(23)\} = \{\tau, \sigma^2\tau\ ,\ \sigma\tau\}$$

H_2(不同)的右陪集为二个：

$$\{(1),(123)\ ,(132)\} = \{e,\ \sigma,\ \sigma^2\}\ ,\qquad \{(12),(13),(23)\} = \{\tau, \sigma^2\tau\ ,\ \sigma\tau\}$$

因此 $2\times3=6, 3\times2=6$ 所以，满足拉氏定理。

注：•三次对称群S_3的2阶子群还有：$H_1' = \{(1),(13)\} = \{e,\ \sigma^2\tau\}$，
$H_1'' = \{(1),(23)\} = \{e,\ \sigma\tau\}$；

•子群〈$H_2, \diamond$〉显然是群〈$S_3, \diamond$〉的正规子群，记为$H_2 \lhd S_3$。

推论1.素数阶群的子群只有两个，即两个平凡子群。

[证].设〈G,∗〉是有限群，|G|=p。由于p是素数，故p的因子只能是1和p。因此由Lagrange定理知，素数阶群的子群只能是1阶子群和它本身，即两个平凡子群：〈{e},∗〉和〈G,∗〉。

推论2.在有限群中，每个元素的阶都是群的阶的因子。

[证].设〈G,$*$〉是有限群，|G| =n。对任何元素$g \in G$，由定理8知，g的阶有限，故可设g的阶为m，且有$m \le n$。令$S=\{e, g, g^2, \ldots, g^{m-1}\}$，由定理5知S中元素互不相同，因此|S| = m；$*$运算关于S是封闭的，根据定理16知〈S,$*$〉是群〈G,$*$〉的子群，且是循环子群。由Lagrange定理知，m | n。故每个元素的阶是群的阶的因子。

推论3.每个素数阶群都是循环群。

[证].设〈G,$*$〉是有限群，|G| =p， p是素数。由于p>1，故必有元素g$\in$G且g$\neq$e。由定理8知， g的阶有限，故可设g的阶为m，且有$1<m\leq p$ (若m=1，则g=e，矛盾)。令$S=\{e, g, g^2, \ldots, g^{m-1}\}$, 由定理5知S中元素互不相同，因此|S| = m； $*$运算关于S是封闭的，根据定理16知〈S,$*$〉是群〈G,$*$〉的子群，且是循环子群。由Lagrange定理知， m | p，由p是素数及$m\neq1$知m=p，于是有G=S，故群〈G,$*$〉是循环群，而元素g正好是这个群的生成元。

注：●实际上证明了：素数阶群的每个非幺的元素都是这个群的生成元，它们的阶都相同，全都等于群的阶。

推论4.四阶不同构的群只有两个，一个是4阶循环群，一个是Klein 4一群。

[证].在四阶群中，若有一个元素的阶为4，则该群就是4阶循环群(参见表5)；

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

表5 4阶循环群

o	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

表6 Klein4一群

若没有4阶元素，由推论2知除幺元外，每个元素的阶只能是2。而除幺元外，每个元素的阶为2的群就是Klein4一群(参见表6) 。

从同构的意义上来说，四阶群只有两个，一个是4阶循环群，一个是Klein4一群。