国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

中外物理学精品书系

经典系列 · 12

邓稼先学术讲义 III
——群论

重排本

邓稼先　著

北京大学出版社
PEKING UNIVERSITY PRESS

国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

中外物理学精品书系

经典系列·12

邓稼先学术讲义 III

——群论

重排本

邓稼先 著

北京大学出版社
PEKING UNIVERSITY PRESS

图书在版编目(CIP)数据

邓稼先学术讲义.3,群论:重排本/邓稼先著.—北京:北京大学出版社,2014.10
(中外物理学精品书系)
ISBN 978-7-301-24928-4

Ⅰ.①邓…　Ⅱ.①邓…　Ⅲ.①物理学　②群论　Ⅳ.①O4　②O152

中国版本图书馆 CIP 数据核字(2014)第 241925 号

书　　名:邓稼先学术讲义Ⅲ——群论(重排本)
著作责任者:邓稼先　著
责 任 编 辑:曾琬婷
标 准 书 号:ISBN 978-7-301-24928-4/O·1012
出 版 发 行:北京大学出版社
地　　址:北京市海淀区成府路 205 号　100871
网　　址:http://www.pup.cn
新 浪 微 博:@北京大学出版社
电 子 信 箱:zpup@pup.cn
电　　话:邮购部 62752015　发行部 62750672　编辑部 62767347　出版部 62754962
印 刷 者:北京中科印刷有限公司
经 销 者:新华书店
730 毫米×980 毫米　16 开本　18.75 印张　350 千字
2014 年 10 月第 1 版　2014 年 10 月第 1 次印刷
定　　价:56.00 元

“中外物理学精品书系”
编 委 会

序　　言

物理学是研究物质、能量以及它们之间相互作用的科学。她不仅是化学、生命、材料、信息、能源和环境等相关学科的基础，同时还是许多新兴学科和交叉学科的前沿。在科技发展日新月异和国际竞争日趋激烈的今天，物理学不仅囿于基础科学和技术应用研究的范畴，而且在社会发展与人类进步的历史进程中发挥着越来越关键的作用。

我们欣喜地看到，改革开放三十多年来，随着中国政治、经济、教育、文化等领域各项事业的持续稳定发展，我国物理学取得了跨越式的进步，做出了很多为世界瞩目的研究成果。今日的中国物理正在经历一个历史上少有的黄金时代。

在我国物理学科快速发展的背景下，近年来物理学相关书籍也呈现百花齐放的良好态势，在知识传承、学术交流、人才培养等方面发挥着无可替代的作用。从另一方面看，尽管国内各出版社相继推出了一些质量很高的物理教材和图书，但系统总结物理学各门类知识和发展，深入浅出地介绍其与现代科学技术之间的渊源，并针对不同层次的读者提供有价值的教材和研究参考，仍是我国科学传播与出版界面临的一个极富挑战性的课题。

为有力推动我国物理学研究、加快相关学科的建设与发展，特别是展现近年来中国物理学者的研究水平和成果，北京大学出版社在国家出版基金的支持下推出了"中外物理学精品书系"，试图对以上难题进行大胆的尝试和探索。该书系编委会集结了数十位来自内地和香港顶尖高校及科研院所的知名专家学者。他们都是目前该领域十分活跃的专家，确保了整套丛书的权威性和前瞻性。

这套书系内容丰富，涵盖面广，可读性强，其中既有对我国传统物理学发展的梳理和总结，也有对正在蓬勃发展的物理学前沿的全面展示；既引进和介绍了世界物理学研究的发展动态，也面向国际主流领域传播中国物理的优秀专著。可以说，"中外物理学精品书系"力图完整呈现近现代世界和中国物理

科学发展的全貌,是一部目前国内为数不多的兼具学术价值和阅读乐趣的经典物理丛书。

"中外物理学精品书系"另一个突出特点是,在把西方物理的精华要义"请进来"的同时,也将我国近现代物理的优秀成果"送出去"。物理学科在世界范围内的重要性不言而喻,引进和翻译世界物理的经典著作和前沿动态,可以满足当前国内物理教学和科研工作的迫切需求。另一方面,改革开放几十年来,我国的物理学研究取得了长足发展,一大批具有较高学术价值的著作相继问世。这套丛书首次将一些中国物理学者的优秀论著以英文版的形式直接推向国际相关研究的主流领域,使世界对中国物理学的过去和现状有更多的深入了解,不仅充分展示出中国物理学研究和积累的"硬实力",也向世界主动传播我国科技文化领域不断创新的"软实力",对全面提升中国科学、教育和文化领域的国际形象起到重要的促进作用。

值得一提的是,"中外物理学精品书系"还对中国近现代物理学科的经典著作进行了全面收录。20 世纪以来,中国物理界诞生了很多经典作品,但当时大都分散出版,如今很多代表性的作品已经淹没在浩瀚的图书海洋中,读者们对这些论著也都是"只闻其声,未见其真"。该书系的编者们在这方面下了很大工夫,对中国物理学科不同时期、不同分支的经典著作进行了系统的整理和收录。这项工作具有非常重要的学术意义和社会价值,不仅可以很好地保护和传承我国物理学的经典文献,充分发挥其应有的传世育人的作用,更能使广大物理学人和青年学子切身体会我国物理学研究的发展脉络和优良传统,真正领悟到老一辈科学家严谨求实、追求卓越、博大精深的治学之美。

温家宝总理在 2006 年中国科学技术大会上指出,"加强基础研究是提升国家创新能力、积累智力资本的重要途径,是我国跻身世界科技强国的必要条件"。中国的发展在于创新,而基础研究正是一切创新的根本和源泉。我相信,这套"中外物理学精品书系"的出版,不仅可以使所有热爱和研究物理学的人们从中获取思维的启迪、智力的挑战和阅读的乐趣,也将进一步推动其他相关基础科学更好更快地发展,为我国今后的科技创新和社会进步做出应有的贡献。

"中外物理学精品书系"编委会　主任

中国科学院院士,北京大学教授

王恩哥

2010 年 5 月于燕园

目　录

第 1 章　群论的基本概念

§1.1　集　　合

集合是元的组合，它们并不需要有外加的结构或性质. 现列出一些有用的符号：

$a\in S$，表示 a 属于 S（a 是集合 S 的一个元）.

$a\notin S$，表示 a 不属于 S（a 不是集合 S 的一个元）.

$S=S'$，表示集合 S 和 S' 含有同样的元.

$A\subset S$（A 包含在 S 内）：集合 A 中的每一个元属于集合 S. 也可写成 $S\supset A$（图 1-1），A 称为 S 的子集合. 若 $S\subset S'$，且 $S'\subset S$，则 $S=S'$.

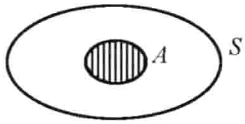

图　1-1

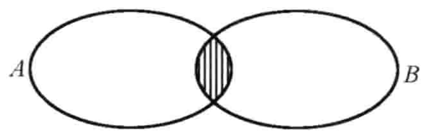

图　1-2

$A\cap B$（A 和 B 的交集）：所有既属于 A 又属于 B 的元的集（图 1-2）.

$A\cup B$（A 和 B 的并集）：属于 A 或属于 B 或属于两者的所有元的集（图1-3）.

$A-B$：把集合 A 中的元扣除掉那些属于集合 B 的元所剩下元的集合就是 $A-B$（图 1-4）.

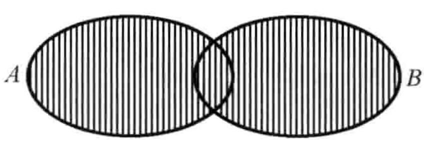

图　1-3

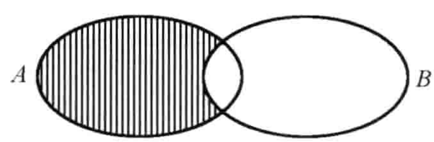

图　1-4

$\varnothing$：空集合（不含有任何元）. 若 $A\cap B=\varnothing$，表示 A 和 B 没有任何共同的元，A 和 B 称之为分离集合或不相交集合.

若 $A\subset S$，${}_{S}A$ 为由 S 中所有不属于 A 的元组成的集合，称之为 S 中子集 A 的补集或余集.

§1.2　映射和变换

S 和 S' 是两个集合. 若对于任何一个元 $x\in S$，对应有一个元 $x'\in S'$，我们就说在映射 M 作用下，集合 S 映入集合 S'. x' 称为在映射 M 作用下 x 的象. 用符号表示：

$$x \xrightarrow{M} x' \quad 或 \quad x' = Mx. \tag{1.1}$$

若 $S=S'$，我们就说在映射 M 作用下，集合 S 映入它本身. 在本节中，我们仅限于讨论集合映入它本身. 至于一个集合映入另一个集合，道理也是相同的. 例如：若有一个集合含有三个元 a,b,c，可以有映射 M，即

$$M = \begin{Bmatrix} a \to b \\ b \to a \\ c \to c \end{Bmatrix}. \tag{1.2}$$

另一个映射 M' 可能是

$$M' = \begin{Bmatrix} a \to a \\ b \to a \\ c \to a \end{Bmatrix}. \tag{1.3}$$

若集合含有无穷多个元，或连续元，我们可以把映射 M 看成函数关系. 例如，在 X 轴上的点集，映射 M 可以是

$$x \xrightarrow{M} x' = x + a \quad 或 \quad x' = Mx = x + a,$$

亦即 X 轴上每一点向右移 a 个单位，即得到它的象点，这种映射称之为平移.

若对于每一个元 $x\in S$，有 $Mx=M'x$，则两个映射 M 和 M' 称为恒等的. 反之，若 $M=M'$，则 $Mx=M'x$ 对于所有元 $x\in S$ 都是成立的. 单位映射 E 的定义是把集合中的元映入它本身，即 $Ex=x$. 若 $x'=Mx$，$x''=M'x'$，则

$$x'' = M'x' = M'(Mx), \tag{1.4a}$$

即

$$x'' = M'Mx. \tag{1.4b}$$

换句话说，映射满足结合律.

从方程(1.2)和(1.3)可以看出映射 $M'M$ 表示

$$\begin{Bmatrix} a \to b \to a \\ b \to a \to a \\ c \to c \to a \end{Bmatrix} = \begin{Bmatrix} a \to a \\ b \to a \\ c \to a \end{Bmatrix}. \tag{1.5a}$$

如果我们把映射作用顺序颠倒过来，则 MM' 表示

$$\begin{Bmatrix} a \to a \to b \\ b \to a \to b \\ c \to a \to b \end{Bmatrix} = \begin{Bmatrix} a \to b \\ b \to b \\ c \to b \end{Bmatrix}, \tag{1.5b}$$

亦即 $MM' \neq M'M$. 换句话说,映射不满足交换律.

一一映射(或称之为变换)的意思是集合中的两个不同元在一一映射作用下没有相同的象,即元 x' 是一个(仅是一个)元 x 的象. 在(1.2)式中 M 是一一映射,而 M' 就不是一一映射. 给定一个一一映射,我们可以找到一个逆映射. 于是,如果映射 M 将 x 映入 x', $x'=Mx$,它的逆映射 M^{-1} 就将 x' 映入 x, $x=M^{-1}x'$. 因此, $x'=Mx=MM^{-1}x'$,从而

$$MM^{-1} = E. \tag{1.6a}$$

而且 $x=M^{-1}x'=M^{-1}Mx$,于是

$$M^{-1}M = E. \tag{1.6b}$$

例如,映射

$$M = \begin{Bmatrix} a \to b \\ b \to a \\ c \to c \end{Bmatrix}$$

的逆映射是

$$M^{-1} = \begin{Bmatrix} a \to b \\ b \to a \\ c \to c \end{Bmatrix}.$$

在这种情况下,映射 M 的逆映射就是它本身,即 $M=M^{-1}$.

对于在方程(1.4a)中的映射 M 和 M',我们有

$$x = M^{-1}x', \quad x' = M'^{-1}x'', \quad x = M^{-1}M'^{-1}x'',$$

而从方程(1.4b),得到

$$x = (M'M)^{-1}x'',$$

于是

$$(M'M)^{-1} = M^{-1}M'^{-1}, \tag{1.7}$$

即两个映射之积的逆映射是运算顺序颠倒过来的逆映射之积.

对于集合含有有限元的映射的例子,参见映射(1.2)和(1.3)式. 对于连续点集的映射,上面曾举过 X 轴平移的例子,下面再举一例,即直线的射影变换. 在 X 轴的点的射影变换的意思是

$$x \to x'; \quad x' = \frac{ax+b}{cx+d}, \text{其中} \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \neq 0. \tag{1.8}$$

我们可以很容易证明在一直线上的四个点的交比

$$\frac{(x_1 - x_2)/(x_3 - x_2)}{(x_1 - x_4)/(x_3 - x_4)} \tag{1.9}$$

经过射影变换是不变的，即四个象点的交比仍保持上述形式.

§1.3 群的概念

一个群 G 是一个集合，它的元可以通过封闭乘积运算联系起来. 所谓封闭乘积运算是指如果 $a, b \in G$，则 $ab \in G$(即乘积运算具有封闭性). 这种集合还满足：

(1) $a(bc) = (ab)c$(满足结合律)；

(2) 有一个单位元 e，对于所有 $a \in G$，有 $ea = a$；

(3) 对于每一个元 $a \in G$，有一个逆元 a^{-1}，使得 $a^{-1}a = e$.

首先，应注意这里所谓乘积运算并不一定是普通的乘法运算. 当讨论到有理数(零除外)集合，它们之间的乘积是乘法运算，则此集合组成一个群. 当讨论到整数(正数，负数，零都包括在内)，它们之间的乘积是加法运算，此集合也组成一个群. 对于不同的群，乘积运算有不同的含义.

其次，注意在这个定义中，我们仅要求左边的单位元 e 和左边的逆元. 按照群的定义，我们也可证明 e 也是右边的单位元($ae = a$)，a^{-1} 也是右边的逆元($aa^{-1} = e$).

我们注意到因为 $a^{-1} \in G$，它也有一个逆元 $(a^{-1})^{-1}$，按照第(3)条 $(a^{-1})^{-1}a^{-1} = e$，按照第(2)，(3)条 $ea = a$，$a^{-1}a = e$，有

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1}.$$

将上式两端从左边乘以 $(a^{-1})^{-1}$，得

$$(a^{-1})^{-1}a^{-1}aa^{-1} = (a^{-1})^{-1}a^{-1},$$

而 $(a^{-1})^{-1}a^{-1} = e$，于是

$$(a^{-1})^{-1}a^{-1}aa^{-1} = eaa^{-1} = e.$$

按照第(1)，(2)条 $aa^{-1} \in G$，$eaa^{-1} = aa^{-1}$，于是

$$aa^{-1} = e. \tag{1.10}$$

因为 $a^{-1} \in G$，按照第(2)条

$$ea^{-1} = a^{-1}.$$

将上式两端从左边乘以 a，且应用方程(1.10)，得

$$aea^{-1} = aa^{-1} = e.$$

再将上式两端从右边乘以 a，且应用第(3)条，得

$$aea^{-1}a = ea = a. \tag{1.11}$$

但按照第(2)，(3)条 $a^{-1}a = e$，$ee = e$，得

$$aea^{-1}a = aee = ae.$$

代入方程(1.11)，得

$$ae = a. \tag{1.12}$$

方程(1.10)和(1.12)说明 a^{-1} 也是右边的逆元,e 也是右边的单位元.

如果对于任何元 $a,b\in G$,且 $ab=ba$,则群 G 称为阿贝尔(Abel)群.

具有 g 个元的群称之为 g 阶的群.

若 $a,b\in G$,则按照群的定义,有

$$(ab)^{-1}ab = e.$$

将上式两端从右边乘以 b^{-1},则

$$(ab)^{-1}abb^{-1} = eb^{-1} = b^{-1},$$

而 $bb^{-1}=e,(ab)^{-1}abb^{-1}=(ab)^{-1}ae=(ab)^{-1}a$,于是

$$(ab)^{-1}a = b^{-1}.$$

再将上式两端从右边乘以 a^{-1},由于 $aa^{-1}=e$,得

$$(ab)^{-1} = b^{-1}a^{-1}, \tag{1.13}$$

即一个群的两元之积的逆元等于乘积顺序颠倒过来的逆元之积.

如果 $a,b,c\in G$,且

$$ab = ac,$$

将上式两端从左边乘以 a^{-1},即 $a^{-1}ab=a^{-1}ac$,由于 $a^{-1}a=e$,得

$$b = c.$$

换句话说,如果 $a,b,c\in G$,且 $ab=ac$,即可得 $b=c$.

如果 $a\in G,a^2=aa$,同样 a 的 n 次幂积表示

$$a^n = \underbrace{a\cdot a\cdot \cdots \cdot a}_{n\text{个}a}.$$

我们用 a^0 表示单位元 e,即

$$a^{-1}a = aa^{-1} = e = a^0.$$

我们还可以定义 a 的负 m 次幂积,即

$$a^{-m} = (a^{-1})^m = (a^m)^{-1},$$

其中最后一步是应用方程(1.13)的结果.如果元 a 的所有幂积都是不相同的,则 a 称为具有无穷阶;如果不是这种情况,我们找到两个整数 r 和 $s(r>s)$,使得

$$a^r = a^s.$$

乘以 a^{-s},我们有

$$a^{r-s} = e \quad (r>s, r-s>0).$$

如果 n 是最小的正整数,使得 a^n 是单位元,即

$$a^n = e, \quad n>0; \tag{1.14}$$

以及如果 $a^k=e,k>0$,则 $k\geqslant n$,我们就说 a 的阶是 n.

如果 a 的阶是 n,则所有元

$$e = a^0, a^1, a^2, \cdots, a^{n-1} \tag{1.15}$$

都是不相同的(因为如果 $a^r=a^s$,则 $a^{r-s}=l$,且 $r-s<n$,那么这就和 n 是最小的正整数,使得 $a^n=e$ 相矛盾). 于是,元 a 的每一个幂积都要是(1.15)式中的一个元,因为任何整数 k 均可写成

$$k = sn + t, \quad 0 \leqslant t < n,$$

从而

$$a^k = a^{sn+t} = (a^n)^s a^t = e^s a^t = a^t.$$

从这个推论中可以看出,如果 $a^k=e$(即 $t=0$),则 k 是 n 的整数倍.

1阶的群就只含有一个元 e: $ee=e$.

2阶的群含有两个不同的元 e,a,于是 $aa=a^2$ 不可能是 a,因为 $a^2=a$ 就表示 $a=e$,因此 $a^2=e$,亦即 a 就是它自己的逆元 a^{-1}. 下面列出2阶的群的具体例子:

整数{1,−1}是一种2阶的群,如果把元的乘积看成是算术乘积($e=1,a=-1$). 整数{0,1}也是一种2阶的群,如果我们把元的乘积看成是模为2的加法(即两个数的和大于或等于2时,则把2扣去),则

$$0+0=0, \quad 0+1=1+0=0, \quad 1+1=0.$$

在这种情况下,$e=0,a=1$.

再有一种2阶的群就是两个数的排列

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},$$

上式的意思就是在 $e=\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ 中,$1\to1,2\to2$,在 $a=\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ 中,$1\to2,2\to1$,于是

$$a^2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e.$$

上述三个例子就是2阶抽象群的三种不同的具体实现. 这三种群都有相同的结构,它们被称为是同构的.

如果有两个群 G 和 G',元 $a,b\in G$ 和元 $a',b'\in G'$ 之间有一一对应关系,使得在这种对应之下元之间的关系保持不变,即 $(a\cdot b)'=(a'\times b')$,其中群 G 的乘积运算用“·”来表示,群 G' 的乘积运算用“×”来表示,那么{G·}群和{G'×}群就称为是同构的,或群 G 同构映射入群 G',简称群 G 同构于群 G'. 这种映射就称之为同构映射(为简单起见,在不会引起混淆的情况下就把 G 中两元之积表示成 ab,把 G' 中两元之积表示成 $a'b'$).

如果群是同构的,尽管群的具体实现不同(就像上面所举出的三个例子那样),但是抽象群是相同的. 同构于抽象群的具体群就称为此抽象群的实现(或具体实现).

我们还可以定义一种所谓等价关系(用“≡”来表示). 集合中的元 $a,b,c,\cdots$ 满足以下关系:

(1) $a \equiv a$(自反性);

(2) 如果 $a \equiv b$,则 $b \equiv a$(对称性);

(3) 如果 $a \equiv b, b \equiv c$,则 $a \equiv c$(可递性).

这些元 $a,b,c,\cdots$ 就称为具有等价关系.集合中满足等价关系的元组成等价类,或简称类.同构群就满足等价关系,亦即群 G 和它本身是同构的;如果群 G 同构于群 G',则群 G' 也同构于群 G;如果群 G 同构于群 G',而群 G' 又同构于群 G'',则群 G 就同构于群 G''.

3 阶的群含有三个不同的元 e,a,b. ab 不能等于 a,也不能等于 b,因为 $ab=a$ 就表示 $b=e$,$ab=b$ 就表示 $a=e$,从而 $a=e$ 或 $b=e$ 就和 e,a,b 是三个不同元这一事实相矛盾,所以 $ab=e$. 同样,$aa=a$ 也表示 $a=e$,因此 aa 只能等于 e 或等于 b. 但如果 $aa=e$,则

$$(aa)b = a(ab) = eb = b.$$

而 $ab=e$,所以 $a(ab)=ae=a$,从上式就可得到

$$a = b,$$

这又和 a,b 是不同的元相矛盾,所以 aa 不能等于 e,aa 只能等于 b. 同样,$bb=a$. 所以 3 阶的群的三个不同的元是 $e,a,a^2=b$ 或 $e,b,b^2=a$. 我们可以把 3 阶的群的三个不同的元写成 $\{e,a,a^2\}$. 而 $a^3(ab)=e$. 这是 3 阶的群的唯一的可能性. 3 阶的抽象群的一个简单的具体实现是 $x^3-1=0$ 的三个根,它们的乘积就是复数的普通乘积.

一个群 G 的元是 $\{e,a,a^2,\cdots,a^{n-1}\}$,那么群 G 就叫做 n 阶的循环群,3 阶的群只可能是 3 阶的循环群,它是循环群的一种特例. 循环群显然是阿贝尔群.

设 g 阶的群 G 的元是 $\{a_1=e,a_2,\cdots,a_g\}$,若 $\{b_1,b_2,\cdots,b_n\}$ 是 G 中数目最少的不同的元,使得 G 中任一元 $a_i(i=1,2,\cdots,g)$ 等于 $\{b_1,b_2,\cdots,b_n\}$ 彼此之间的乘积,其中可能包括它们的幂积,那么 $\{b_1,b_2,\cdots,b_n\}$ 就叫做形成群 G 的基,或称为 G 的生成元,也可说 $\{b_1,b_2,\cdots,b_n\}$ 生成群 G. 例如,循环群 $\{e,a,a^2,\cdots,a^{n-1}\}$ 的基显然就是 a.

下面我们列出群表,把群的元列成方阵,方阵中第 n 行和第 m 列是群中第 n 个元和第 m 个元的乘积. 例如,2 阶群的群表是

	e	a
e	$e^2=e$	$ea=a$
a	$ae=a$	$a^2=e$

或简化为

	e	a
e	e	a
a	a	e

3 阶群的群表是

	e	a	$b(=a^2)$
e	$e^2=e$	$ea=a$	$eb=b$
a	$ae=a$	$a^2=b$	$ab=e$
b	$be=b$	$ba=e$	$b^2=a$

或简化为

	e	a	$b(=a^2)$
e	e	a	b
a	a	b	e
b	b	e	a

从上表可以看出,群表中所列出的元对于主对角线是对称的,这仅对于阿贝尔群才成立.而 2 阶的群和 3 阶的群都只能是循环群,而循环群是阿贝尔群.另外,在每一行(或每一列)中,群的所有的元只出现一次,且仅出现一次,这是因为群表中所列出的元都是两个元的乘积.如果出现两次 $ab=ac$,则 $b=c$,而 b 和 c 是不同的元,不可能有 $ab=ac$ 的情况.

4 阶的抽象群有两种不同的结构(见 §1.4).

(1)

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

$a^2=b$, $ab=c=a^3$,
$a^4=b^2=e$.

这是 4 阶的循环群$\{e,a,a^2,a^3\}$,$a^4=e$.

(2)

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

$a^2=b^2=c^2=e$,
$ab=c$, $ac=b$, $bc=a$.

这种群叫做 4-群,通常用符号 V 来表示.从群表可以看出,所列出的元对于主对角线也都是对称的,这两种群也都是阿贝尔群.更高阶的群不一定都是阿贝尔群.在 6 阶的群中,我们可以发现第一个非阿贝尔群,例如三个数目的排列就是非阿贝尔群.

在上表中,我们看到 4-群的元$\{e,a\}$本身就形成一个群($ee=e,ea=ae=a,aa=e$),$\{e,b\}$和$\{e,c\}$也是如此.

G 群中一组元的集合 H,即 $H\subset G$,如果满足以下两个条件:

(1) H 中任何两元的乘积仍属于 H;

(2) 如果 $a\in H$,则 $a^{-1}\in H$,

则 H 称为 G 的子群.

任何子群 H 本身也是一个群,这是因为 H 中的元也属于群 G,它们自然满足结合律.而且 $a,a^{-1}\in H$,$aa^{-1}=e$ 也属于 H.任何群 G 都有两个平凡子群,即单位

元 e 是一个子群，以及整个群 G 是它本身的子群. 这两个平凡子群又叫做假子群，其他的子群有时叫做真子群. 正如以上所述，4-群有子群 $\{e,a\}$，同样还有同构子群 $\{e,b\}$ 和 $\{e,c\}$. 此外，在任何群 G 中，$\{e,a,a^2,\cdots,a^{n-1}\}$（其中 $a\in G$，n 是 G 的阶）是 G 的阿贝尔子群.

对于含有限个元的群（即有限群）来说，子群的两个条件只有第(1)条就够了. 在这种情况下，对于 $a\in H$，就有 a 的幂积，例如 a^{n-1}（也属于 H）使得 $aa^{n-1}=a^n=e$，即 $a^{-1}=a^{n-1}\in H$. 换句话说，第(2)个条件是第(1)个条件的结果. 但这里必须指出，并不是所有的群都只含有限个元，有的群含有无限多个元，而且有的群的元还是连续的，这就是所谓无限群和连续群. 例如，集合 G 的元是整数，把加法运算作为它们之间的乘积（$e=0$，$a^{-1}=-a$，a 是整数），这样的集合 G 就是无限阶的（阿贝尔）群. 对于无限群来说，子群的两个条件都需要. 例如，我们讨论正整数集合，把加法运算作为它们之间的乘积，那么它们满足第一个条件，但不满足第二个条件，因此正整数就不是整数的子群.

定理 1-1　令 $H\subset G$，群 H 是群 G 的子群的充要条件是，对于所有的 a 和 $b\in H$，有 $ab^{-1}\in H$.

事实上，如果 H 是 G 的子群，a 和 $b\in H$，按照第(2)条，a^{-1} 和 $b^{-1}\in H$，而按照第(1)条自然就得到 $ab^{-1}\in H$.

反之，对于所有 a 和 $b\in H$，有 $ab^{-1}\in H$，那么 $aa^{-1}=e\in H$，亦即单位元 $e\in H$. 既然单位元 $e\in H$，$a\in H$，于是 $ea^{-1}=a^{-1}\in H$，亦即 a^{-1} 也属于 H. 同样，b^{-1} 也属于 H. 既然 a 和 $b^{-1}\in H$，于是 $a(b^{-1})^{-1}=ab\in H$. 这就是说子群的两个条件都得到满足，H 是 G 的子群.

定理 1-2　如果 G 是 n 阶的群，其元是 $e,a_2,a_3,\cdots,a_n$，那么对于任何 i，在序列

$$ea_i,\ a_2a_i,\ a_3a_i,\ \cdots,\ a_na_i$$

或序列

$$a_ie,\ a_ia_2,\ a_ia_3,\ \cdots,\ a_ia_n$$

中，G 的每一个元出现一次而且仅出现一次.

事实上，如果某一个元出现两次，我们要有 $a_ra_i=a_sa_i$，即 $a_r=a_s$，这跟 a_r 和 a_s 是 G 的两个不同的元相矛盾. 换句话说，G 的任何一个元在上述序列中只能出现一次.

这点在讨论群表时已指出过，在群表的每一行（或每一列）中，群的所有元出现一次且仅出现一次. 这种现象就是这个定理的必然结果.

§1.4　对称群的一些性质

n 个数排列所形成的群叫做对称群 S_n. 因为 n 个数有 $n!$ 种排列，所以 S_n 的阶

为 $n!$. S_n 的元可以表示为

$$\Pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}, \tag{1.16a}$$

其中$(a_1,a_2,a_3,\cdots,a_n)$表示$(1,2,3,\cdots,n)$的某种排列，即把 i 换成 $a_i(i=1,2,3,\cdots,n)$. 当然，我们也没有理由一定要把上行的数按顺序排起来，也可写成

$$\Pi = \begin{pmatrix} 2 & 1 & 3 & \cdots & n \\ a_2 & a_1 & a_3 & \cdots & a_n \end{pmatrix},$$

或为了更普遍一些，我们写成

$$\Pi = \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ a_{b_1} & a_{b_2} & a_{b_3} & \cdots & a_{b_n} \end{pmatrix}. \tag{1.16b}$$

上面三种写法都是表示同一个排列，单位排列元是

$$e = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}. \tag{1.17}$$

例如，三个数的排列是

$$\Pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

在 Π_1 中，$1\to2,2\to1,3\to3$；在 Π_2 中，$1\to1,2\to3,3\to2$. 我们可以定义 Π_1 和 Π_2 的乘积，$\Pi_1\Pi_2$ 其意思是 $1\to1\to2,2\to3\to3,3\to2\to1$. 而 $\Pi_2\Pi_1$ 的意思是 $1\to2\to3,2\to1\to1,3\to3\to2$. 所以

$$\Pi_1\Pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$\Pi_2\Pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

即 $\Pi_1\Pi_2\neq\Pi_2\Pi_1$. 所以，排列的乘积并不满足交换律. 一般来讲，如果有 n 个数排列

$$\Pi_1 = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix},$$

则根据方程(1.16b)，有

$$\Pi_1\Pi_2 = \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ a_{b_1} & a_{b_2} & a_{b_3} & \cdots & a_{b_n} \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_{b_1} & a_{b_2} & a_{b_3} & \cdots & a_{b_n} \end{pmatrix} \tag{1.18a}$$

和

$$\Pi_2\Pi_1 = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_{a_1} & b_{a_2} & b_{a_3} & \cdots & b_{a_n} \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ b_{a_1} & b_{a_2} & b_{a_3} & \cdots & b_{a_n} \end{pmatrix}. \tag{1.18b}$$