目　录

壹

预备知识

群是数学中的一个很重要的概念，群的理论现在已发展得很高深，它的应用也极广泛．它不仅对研究数学的其它分支是重要的，而且是研究某些自然科学学科，比如量子力学、光谱学、结晶学、原子物理、粒子物理等的有力武器．但是，群的理论并不是高深莫测的，体现群的要求的现象在我们的周围也可以找到．在本书中，我们将介绍一些这方面的例子．在这一部分中，我们先讲一些预备知识．

一、集　　合

集合这个概念直接反映了现实世界中常见的现象，它在数学中是不给予定义的概念．从直觉上来说，我们可以举出许多集合的例子：在一间屋子里，床、椅、桌、台灯、热水瓶、茶杯等合起来，是集合，可以叫做此屋中的“生活用具的集合”，椅、桌、台灯、笔、墨水瓶等合起来是集合，它们可以做为学习的用具，叫做“学习用具的集合”，把所有这些东西及其它用具合起来，叫做“用具的集合”．在我们身边还有许多其它集合，不胜枚举，以后也把集合简单地叫做“集”．

在数学中，1,2,3,…的全体是自然数的集合，以 N 作为标记；$0, \pm 1, \pm 2, \cdots$ 的全体是整数集合，以 Z 作为标记；当用 n 表示任

意给定的自然数，a 表示任意给定的整数时，$\frac{a}{n}$这种形式的所有的数的全体叫做有理数集合，以Q 作为标记；方程 $x^3-1=0$ 的三个根 $1, \omega=\frac{-1+\sqrt{3}i}{2}$，$\omega^2=\frac{-1-\sqrt{3}i}{2}$合起来叫做此方程解的集合，$1, \omega, \omega^2$ 叫做 1 的三次根，一般地 $x^n-1=0$（n 为自然数）的根叫做 1 的 n 次根.

由上面的例子可以看出，集合是由所谓元素构成的. 比如“生活用具的集合”以桌、椅等等作为它的元素；整数集合以 0，±1，±2 等等作为它的元素. 元素的个数可以是有限的，例如$x^3-1=0$的解集合，它的元素个数是 3；元素的个数也可以是无限的，例如自然数集合的元素个数就是无限的.

习惯上用大写英文字母，如 $E, M, A, \cdots$来表示集合；用小写英文字母 $a, b, c, x, \cdots$来表示元素. 为了用符号来表示“a 是 A 的元素”这句话，引用记号 $\in$，它表示“属于”的意思，这样，

$$a \in A$$

就表示“a 是 A 的元素”，或者说：“a 属于 A”，又用 $\notin$ 表示“不属于”，于是

$$b \notin A$$

就表示“b 不是 A 的元素”，或“b 不属于 A”.

为了表明一个集合 A 具有怎样的一些元素，常用如下的表示方式：

当 A 的元素的个数为有限的时候，A 具有元素 a, b, c, d, e 就表示为：

$$A=\{a, b, c, d, e\}.$$

当元素的个数为无限的时候，比如在全体自然数集合 N 的情形，可以写作

$$N=\{1, 2, 3, \cdots\},$$

在全体整数的集合Z的情形，可以写作

$$Z=\{0,\pm1,\pm2,\cdots\}.$$

请注意后面的点不可少，它表示无限的意思，这是一种象征手法.

还有许多不能这样逐一列出的情形，这时就采用下面的表示方式，例如可将全体有理数的集合Q表示为

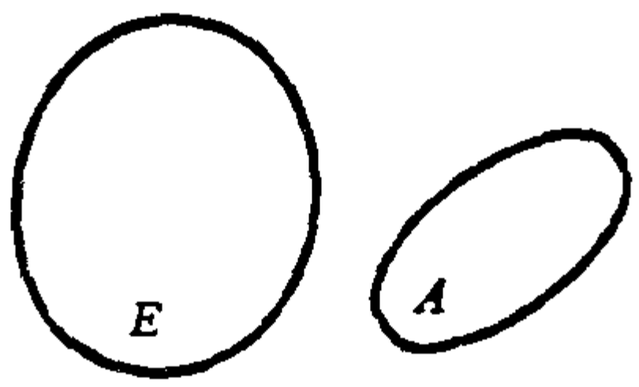
$$Q=\left\{\frac{a}{n}\middle|\forall n\in N,\ \forall a\in Z\right\},$$

花括号中的N就是上面所说的自然数的集合，Z是整数的集合；$\forall$的意思是“每一个”(或“所有的”)，所以$\frac{a}{n}$不只是一个数，而是任何有理数的表达式. 给定了a和n，就得到一个有理数；给定另一组a和n，又得另一个有理数，所以$Q=\left\{\frac{a}{n}\middle|\forall n\in N,\ \forall a\in Z\right\}$将所有的有理数概括无遗!

接着顺便谈一下实数系与复数系. 在中学我们已经知道，有理分数都可表示为循环小数；而非循环小数便是无理数，有理数与无理数的全体叫做实数系，记作R.

$a+bi$形式的数（这里$a,b\in R$，$i=\sqrt{-1}$)叫做复数. 复数的全体叫复数系，记作C.

为了形象化起见，还可用封闭的平面图形来表示集合，如右图所示. 这是示意图，也是一种象征手法.

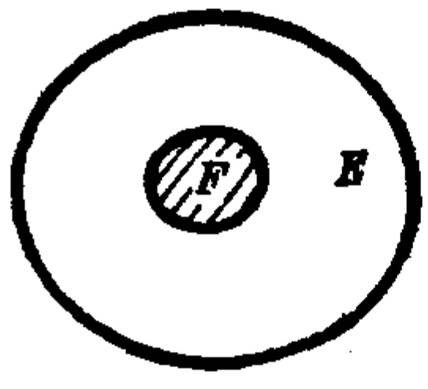


子集 从前面的例子可以看到，“学习用具的集合”的元素，包含在所有“用具集合”里面；自然数集合的元素包含在整数集合里面；而整数集合的元素又包含在有理数集合里面，等等. 换句话说，在上述三种情况中，前面的集合是后面的集合的一部分，从而就说前面的集合是后面的集合的子集. 概括地说：

一个集合F，如果它的一切元素都属于某个集合E，就说F是

E 的子集，写作 $F\subset E$，或 $E\supset F$. 从这里所说的条件可以看出，如果 $F\subset E$，那末当元素 $f\in F$ 时，必然有

$$f\in E.$$



$F\subset E$

请勿将$\subset$与$\in$这两个符号混淆.

一般地说，属于某个集合 A 的元素 a 都具有某种性质，此性质简略地用一个符号 P 来表示. 集合 A 就记作

$$A=\{a\mid \text{所有的 } a \text{ 具有 } P\}.$$

例如 $\rho=1,\omega,\omega^2$ 所具有的性质是，将它们代入 $x^3-1=0$ 中，都使左右两端相等，于是 $x^3-1=0$ 的解集合就记作

$$X=\{\rho\mid \rho \text{ 满足 } x^3-1=0\}.$$

不含有元素的集叫做空集，用符号$\varnothing$来表示. 例如，其平方等于 2 的有理数的集是空集. 又例如，平面几何中，三内角之和大于 180° 的三角形的集合就是平面三角形集合的空子集. 我们规定对于任意集合 E，有

$$\varnothing\subset E,$$

还可看到：

$$E\subset E.$$

集合的运算 在集合与集合之间可以建立一些特定的运算，主要的有以下几种：

（1）并 先看开始时举出的例子，在一个房间里生活用具有床、椅、桌、台灯、热水瓶、茶杯；学习用具有椅、桌、台灯、笔、墨水瓶，两类用具并在一起就是：床、椅、桌、台灯、热水瓶、茶杯、笔、墨水瓶，这里椅、桌、台灯是两种用具集合共有的，只取一次，这种把物品归并在一起的做法是集合的一种运算——“并”的实际背景，用数学术语来说：

设有 A 与 B 两个集合，所谓 A 与 B 的并，就是这样的元素组成

的集合，这些元素或者属于 A，或者属于 B. 用普通的话说，就是把 A 与 B 中的元素都取用无遗，但共同的只取一次. 对三个或三个以上的集合的并，可以依此类推，写法是

$$A\cup B,\ A\cup B\cup C,$$

$$\bigcup_{i=1}^{n} A_i(=A_1\cup A_2\cup A_3\cup\cdots\cup A_n),$$

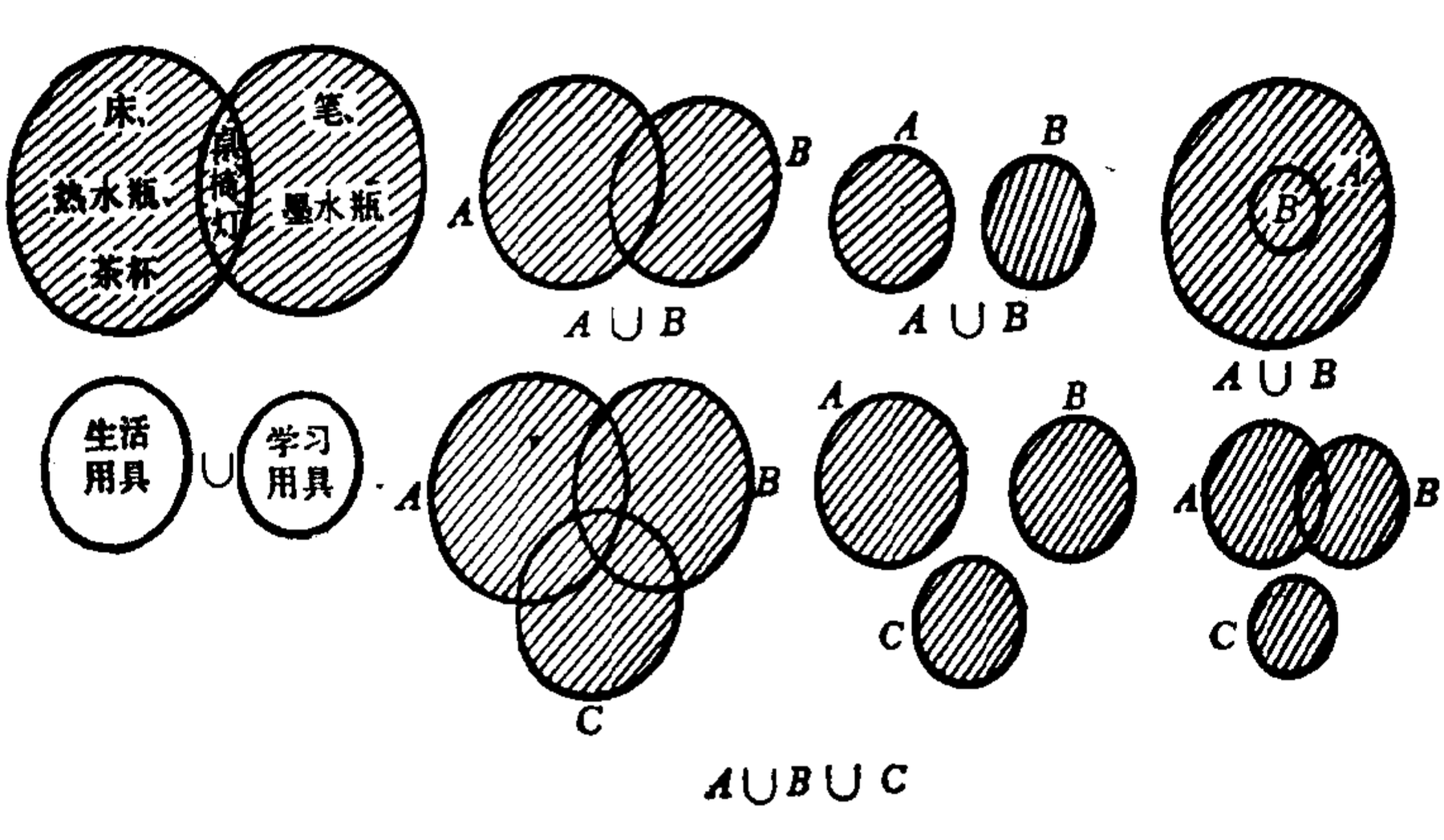
这里我们只限 n 为有限的情形.

从这里所说的条件可以看出，如果 $a\in A$, $b\in B$，那末

$$a\in A\cup B,\quad b\in A\cup B.$$

但是，如果 $c\in A\cup B$，那末，我们只能说，c 可能属于 A，可能属于 B，必然属于其中之一. 但究竟属于哪一个，或同时属于两个，还是不清楚的.

用图形来表示并的运算如下：



$A\cup B\cup C$

阴影部分表示并的结果

从所说并的意义来看，$A\cup B$ 与 $B\cup A$ 是一个意思. 用数学的术语来说，对于运算 $\cup$，A 与 B 的次序可以交换.

请注意，如果 $B\subset A$，那末 $B\cup A=A$；另外，

$$A \cup \varnothing = A.$$

（2）交　还是看前面的用具的集合．生活用具中的桌、椅、台灯与学习用具中的桌、椅、台灯是共同的，也就是生活用具的集合与学习用具的集合“相交”．在集合的运算中，所谓交的运算，就是以这样一类实际问题为背景的．

设有两个集合 A 与 B，所谓 A 与 B 的交就是这样的元素所组成的集合，这些元素既属于 A 同时又属于 B，写作 $A \cap B$．对三个或三个以上（这里只限于有限个）的集合，可以依此类推，

$$A \cap B \cap C, \quad \bigcap_{i=1}^{n} A_i (= A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n).$$

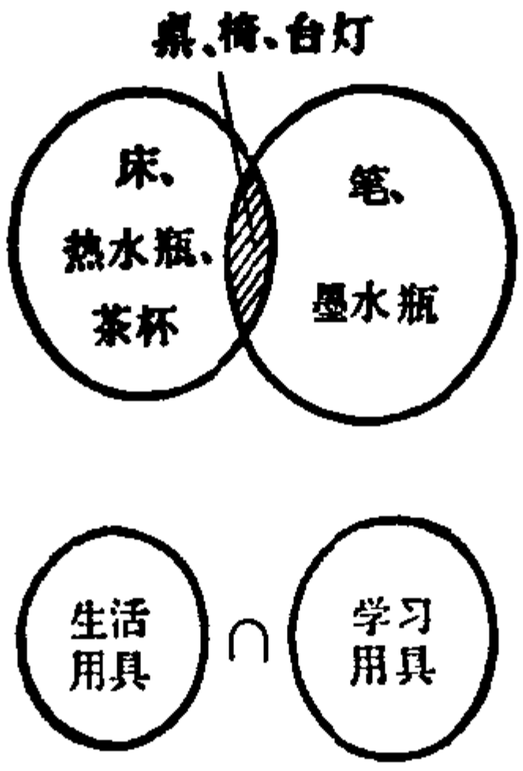
此处 n 为有限的自然数．

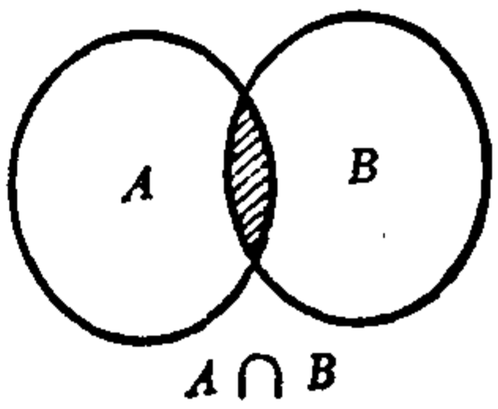
从这里所说的条件可以看出，如果 $c \in A \cap B$，那末必然有

$$c \in A \text{ 同时 } c \in B.$$

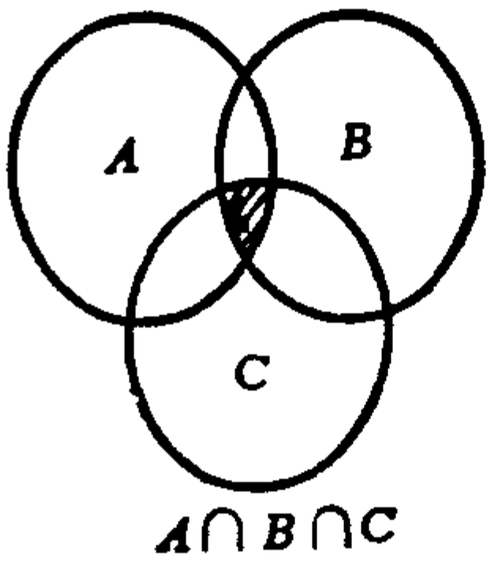
再从所说交的意义来看，$A \cap B$ 与 $B \cap A$ 是一个意思．用数学术语来说，对于运算 $\cap$，A 与 B 的次序可以交换．

用图来表示交的运算如下：





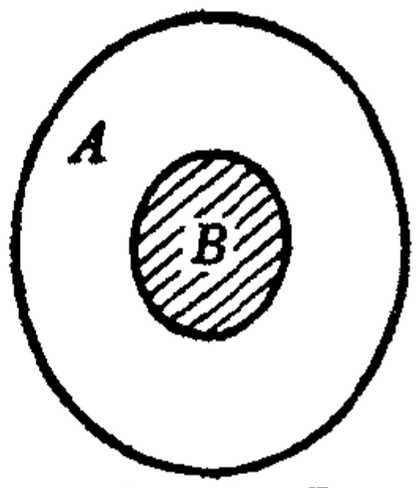
$A \cap B$



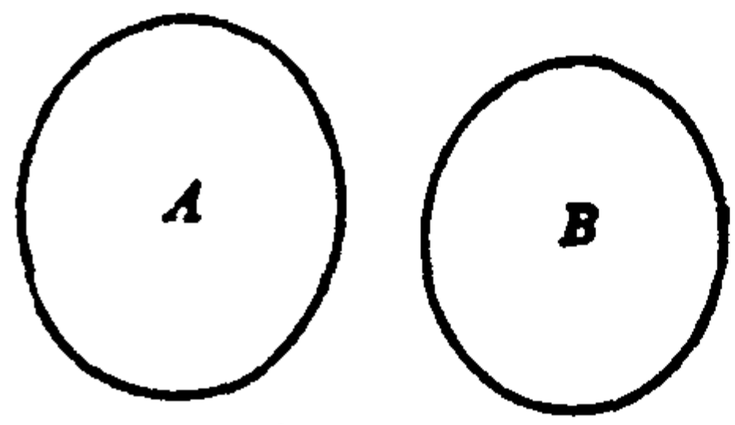
$A \cap B \cap C$

阴影部分表示交的结果

请注意，如果 $B \subset A$，那末 $A \cap B = B$，如果 $A \cap B = \varnothing$，那末 A 与 B 不相交．



$A \cap B = B$



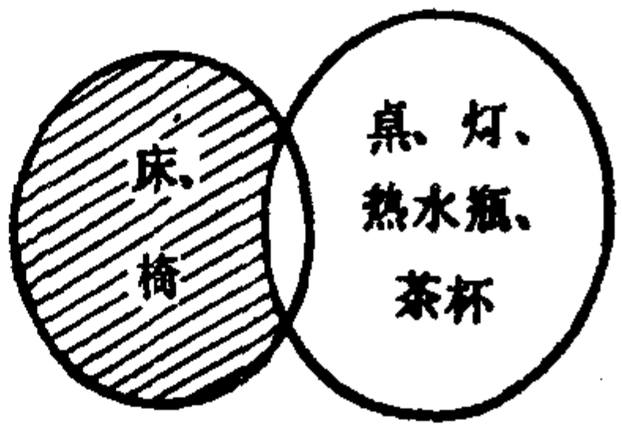
$A \cap B = \phi$

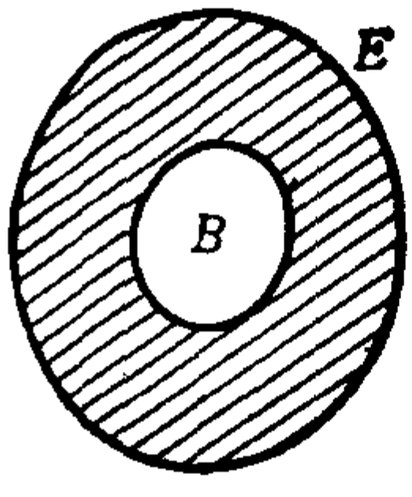
(3) 补 仍请看上述生活用具的例子. 如果将这些生活用具的集合记作 E, 而其中桌上的用物: 桌、台灯、热水瓶、茶杯作为子集 B, 那末在桌上用物的集合 B 之外再补上床、椅, 就构成此房中生活用具的集合 E.

用数学的语言来说, 就是:

设有集合 E 和它的子集 B, 所谓 B 对于 E 的补集就是这样一些元素 b 的集, 这些 b 属于 E, 但不属于 B, 即 $b \in E$, 且 $b \notin B$, 把补集写作 $C_E B$, 或简写作 CB. B 与 $C_E B$ 之间有关系: $B \cup C_E B = E$——这体现了补全的意思; 另有 $B \cap C_E B = \varnothing$——这体现了"要补全而成 E 的, 正是 B 中所缺的".

用图表示补的运算如下:





阴影部分表示 $C_E B$

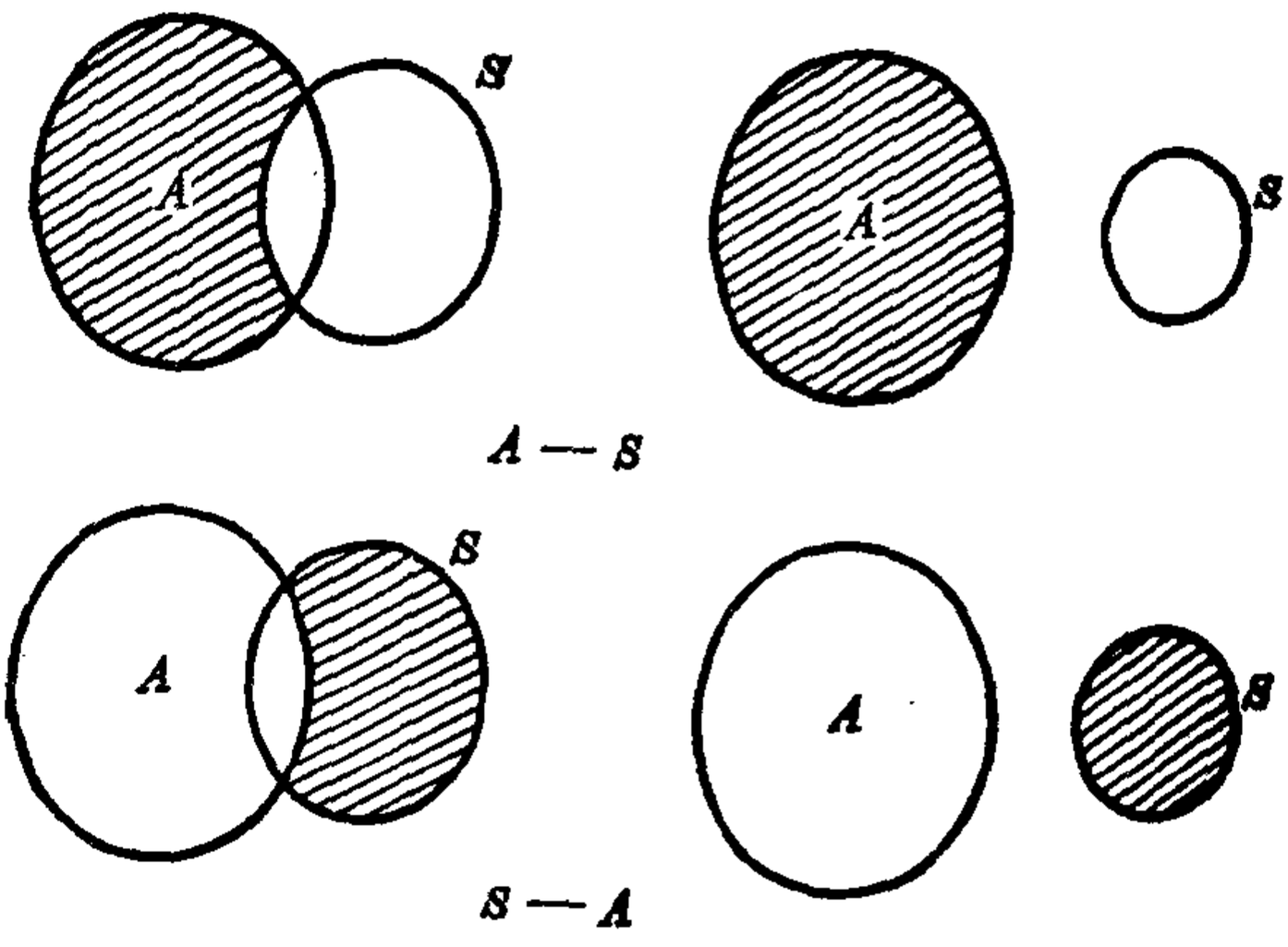
(4) 差 在上面生活用具的集合 E 与学习用具的集合 S 之间还可能有以下两种关系: (1)只属于生活用具集合, 不属于学习用具集合的物品: 床、热水瓶、茶杯; (2)只属于学习用具集合, 不属于生活用具集合的物品: 笔、墨水瓶. 在第一种情形, 床、热水瓶、

茶杯合在一起叫做生活用具集合对于学习用具集合的差；在第二种情形，笔、墨水瓶合在一起叫做学习用具集合对于生活用具集合的差.

在集合运算中，设有两个集合 A 与 S，所谓 A 对 S 的差集，是这样的元素组成的集，这些元素只属于 A 不属于 S，写作 $A-S$. 可以同样地定义 S 对 A 的差集 $S-A$.

显然 $A-S$ 与 $S-A$ 不是一回事，即对差运算来说，A 与 S 的次序不能交换.

用图表示差的运算如下：



阴影部分表示差

映射 设有集合 A, B，如果存在某个确定的规则，使 A 的每个元素 a 对应于 B 的某个确定的元素 b，这时，就说定义了由 A 到 B 的映射，映射通常用 f, g, φ, ψ 等表示，并记作

$$f: A \to B,$$

$b=f(a)$ 称为 a 在 f 下的象，A 称为 f 的定义域，当 a 取遍 A 的每个元素时，$f(a)$ 的全体叫做 f 的值域.

例 1 设 A 为 $Z=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$，$B=\{-1,$

1}，那末对应规则

$$\varphi:\begin{matrix}\text{凡偶数}\to 1\\ \text{凡奇数}\to -1\end{matrix}$$

给出一个 $Z\to B$ 的映射.

例 2 设 $Z=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$，$B=\{0,1,2,3,4,5,6\}$，对应规则为:

$$\varphi: z\in Z\longrightarrow z \text{ 被 } 7 \text{ 除所得余数}(\geqslant 0),$$

则 φ 给出了一个映射.

例 3 设 $A=X=\left\{\cdots,-2\pi,-\frac{3}{2}\pi,-\pi,-\frac{\pi}{2},0,\frac{\pi}{2},\pi,\frac{3}{2}\pi,2\pi,\cdots\right\}$，$B=\{1,i,-1,-i\}$，对应规则为

$$f: x\to \cos x+i\sin x,$$

则 f 确定了一个映射.

例 4 设 $A=R^+$(即大于零的实数)，$r\in R^+$，$B=R$（实数的全体)，对应规则为

$$\varphi: r\to \ln r,$$

则 φ 确定了一个映射.

设有定义域 A，值域 B. 对于 $a_1\neq a_2, a_1, a_2\in A$，有

$$f(a_1)\neq f(a_2),$$

而且对于每一个 $b\in B$，都存在 $a\in A$ 使 $f(a)=b$ 成立，这样的映射 f 就叫做一一对应的映射.

例如，在 $A=R, B=R$ 时，

$$f: x\to x+1 \quad (x\in R),$$

这映射是一一对应的.

现在请读者思考下面一些问题.

1. 在平面直角坐标系中，直线

$$y=x$$

可看作点的集合 L_0，点用实数的对 (x, y) 来表示. 按照前面所说的集合表示法，将 $y=x$ 看作一种性质，问可否将 L_0 写成

$$L_0=\{(x, y)\mid y=x,\quad x\in R\}.$$

2. 设有一些直线，在平面直角坐标系中由方程

$$l_c: y=x+c,\quad c=0, \pm1, \pm2, \pm3, \pm4, \pm5$$

给出，这些直线所成的集合记作 $\mathscr{L}$，问如何用一个式子来表达 $\mathscr{L}$？又

$$l_2\in\mathscr{L},$$

$$\{l_{-3}, l_5\}\subset\mathscr{L},$$

$$l_0\in\{l_0, l_1\}\cup\{l_1, l_2\},$$

$$l_1\subset\{l_0, l_1,\}\cap\{l_1, l_2\},$$

这里，例如 l_2, l_{-3} 各为

$$l_2: y=x+2,$$

$$l_{-3}: y=x-3.$$

这些写法，哪些是合理的？哪些是不合理的？

$$\{l_{-1}, l_2\}\cup\{l_0, l_{-1}, l_3\}=?$$

$$\{l_{-1}, l_2\}\cap\{l_0, l_{-1}, l_3\}=?$$

$$\{l_{-1}, l_{-3}\}\cap\{l_0, l_1, l_2\}=?$$

$$C_{\mathscr{L}}\{l_{-2}, l_{-1}, l_0, l_1, l_2\}=?$$

$$\{l_{-3}, l_{-1}, l_0, l_3\}-\{l_2, l_{-1}, l_5\}=?$$

$$\{l_2, l_{-1}, l_5\}-\{l_{-3}, l_{-2}, l_0, l_3\}=?$$

3. 在平面直角坐标系中，圆 O

$$x^2+y^2=1$$

与抛物线 P

$$y=x^2,$$

各可以看作平面上点的集合，它们的交也就是这两条曲线的交点的全体(如果有交点的话)，试写出 $O\cap P$.

4. 上文中已说过记号 Q,R,C 的意义，数字 0 是它们的元素，由 0 一个元素组成的子集便写成{0}，这写法对不对？从 Q,R,C 中各挖去{0}，用式子各应该怎样表达？

二、置　　换

读者一般都知道电话号码，同样几个数字，例如 1,2,3,4，其排列次序不同就代表不同的用户：1234 是用户甲，3142 就成为用户乙了．汽车牌照号码的情形是一样的，其他事物也有一个排列问题，譬如黄、紫、白三盆菊花装饰在花架上，黄紫白是一种装饰式样，白紫黄另是一种装饰式样，等等．

从实例来看，置换是什么：从号码 1 2 3 4 到 3 142 是一个替换过程，即

1　换成　3

2　换成　1

3　换成　4

4　换成　2

或写成下面的形式：

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

并把它叫做置换．

上面三种颜色菊花的排列式样也可写成置换形式

$$\begin{pmatrix} 黄 & 紫 & 白 \\ 白 & 紫 & 黄 \end{pmatrix}.$$

不过，一般地讲，我们在数学中都是把事物数字化或符号化，以便于运算，例如，我们不妨将黄菊花以 A 表示，紫菊花以 B 表示，白菊花以 C 表示，等等．

所以这个菊花置换的例子可写成

$$\begin{pmatrix} A\ B\ C \\ C\ B\ A \end{pmatrix}.$$

一般地讲，1，2，…，i，…，n 等 n 个数字的置换

$$\begin{pmatrix} 1\ \ 2 \cdots i \cdots n \\ a_1\ a_2 \cdots a_i \cdots a_n \end{pmatrix}$$

（这里 $a_1, a_2, \cdots, a_i, \cdots, a_n$ 各是 $1, 2, \cdots, i, \cdots, n$ 中的一个不相同的数）叫做 n 阶置换. 数字改为文字符号时，例如

$$\begin{pmatrix} A\ B\ C\ D\ E \\ E\ C\ A\ B\ \ D \end{pmatrix}$$

也是置换，它是五阶的.

现在来看 n 阶置换一共有多少个？

设 $a_1, a_2, \cdots, a_n$ 各是 $1, 2, \cdots, n$ 中不同的数，$b_1, b_2, \cdots, b_n$ 也各是 $1, 2, \cdots, n$ 中不同的数，而且各个 $a_i (i = 1, 2, \cdots, n)$ 与各个 b_i $(i = 1, 2, \cdots, n)$ 相互对应（即 a_1 对 $b_1, \cdots, a_i$ 对 $b_i, \cdots$）地来看不完全相同. 这样，$a_1, a_2 \cdots, a_n$；$b_1, b_2, \cdots, b_n$ 是 n 个自然数字的两个不同排列. 这两个不同排列对应两个不同的置换，即

$$a_1, a_2, \cdots, a_n \longrightarrow \begin{pmatrix} 1\ \ 2 \cdots n \\ a_1\ a_2 \cdots a_n \end{pmatrix}$$

$$b_1, b_2, \cdots, b_n \longrightarrow \begin{pmatrix} 1\ \ 2 \cdots n \\ b_1\ b_2 \cdots b_n \end{pmatrix}$$

因此，n 个自然数的排列个数，就是 n 阶置换的个数.

由于 n 个自然数字的排列一共有 $n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 = n!$ 个，所以 n 阶置换共有 $n!$ 个.

在下面的置换中：

$$\begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 4\ 1\ 2\ 5 \end{pmatrix}$$

数字替换的情况是：1 换成 3，3 换成 1，2 换成 4，4 换成 2，而 5 不

动. 只是两个数字互相调换位置，其他数字保持不变的置换叫做对换. 例如，

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

是一个对换，它只有 1,3 互换位置，我们把它简记为(1 3). 一般地，用(a b)表示只有 a,b 互换的置换.

在下面的置换中，

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

1 换成 3,3 换成 4,4 换成 2, 2 换成 1(5 不动)，这是 1,3,4,2 四个数字的轮流替换，叫做轮换，记作(1 3 4 2).

置换的乘法 假设有两个 n 阶置换

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ a_1 & a_2 & \cdots & a_i & \cdots & a_n \end{pmatrix}, \qquad \begin{pmatrix} a_1 & a_2 & \cdots & a_i & \cdots & a_n \\ b_1 & b_2 & \cdots & b_i & \cdots & b_n \end{pmatrix}$$

$a_1, a_2, \cdots, a_i \cdots, a_n; b_1, b_2, \cdots, b_i, \cdots, b_n$ 各是 1, 2, $\cdots$, i, $\cdots$, n 等数字中的一个数，而且各不相同，所谓这两个 n 阶置换的乘积

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ a_1 & a_2 & \cdots & a_i & \cdots & a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \cdots & a_i & \cdots & a_n \\ b_1 & b_2 & \cdots & b_i & \cdots & b_n \end{pmatrix}$$

是指，在左边的置换式中，1 换成 a_1，接着按右边的置换式将 a_1 换成 b_1，结果 1 换成 b_1；同样的道理，2换成 a_2，接着 a_2 换成 b_2，结果 2 换成 b_2；……；最后 n 换成 a_n，接着 a_n 换成 b_n，结果 n 换成 b_n. 这样，得到如下的置换

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ b_1 & b_2 & \cdots & b_i & \cdots & b_n \end{pmatrix}.$$

这里要说明一下，上面的第二个置换

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_i & \cdots & a_n \\ b_1 & b_2 & \cdots & b_i & \cdots & b_n \end{pmatrix}$$

在写法上比较特殊，实际上，它与把它的上行写成自然数顺序时的置换是一致的，看一个具体例子，就清楚了：

$$\begin{pmatrix} 3 & 5 & 1 & 4 & 2 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}\text{实际就是}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix},$$

因为上行的每个数字换成下行的什么数字，两个置换是一样的.

要注意，只是两个同阶的置换才能相乘，不同阶的不能相乘. 还要注意，在乘法中，两个置换的顺序一般是不可交换的，例如：

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

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

两个结果不一样.

但是，有一个叫做单位置换 I 的：

$$\begin{pmatrix} 1 & 2 \cdots & i & \cdots & n \\ 1 & 2 \cdots & i & \cdots & n \end{pmatrix} \text{ 或 } \begin{pmatrix} a_1 & a_2 \cdots & a_i & \cdots & a_n \\ a_1 & a_2 \cdots & a_i & \cdots & a_n \end{pmatrix}$$

($a_1, a_2, \cdots, a_i, \cdots, a_n$是 $1, 2, \cdots, i, \cdots, n$的一个排列)，将它从右边乘(以后简称作右乘)任一个同阶置换 σ，和将它从左边乘(简称作左乘)此同阶置换 σ，其结果总是相同的，都等于这个被乘的置换本身σ. 也就是$I\sigma=\sigma I=\sigma$. 由于 I 是其中任一符号都不变的置换，因而与其他任何置换相乘时也不至使后者中的符号改变.

逆置换 如果一个置换是

$$\begin{pmatrix} 1 & 2 \cdots & i & \cdots & n \\ a_1 & a_2 \cdots & a_i & \cdots & a_n \end{pmatrix}$$

那末它的逆置换就是将上行翻成下行，下行翻成上行的置换：

$$\begin{pmatrix} a_1 & a_2 \cdots & a_i & \cdots & a_n \\ 1 & 2 \cdots & i & \cdots & n \end{pmatrix},$$

这里 $a_1, a_2, \cdots, a_i \cdots, a_n$ 是 $1, 2 \cdots, i, \cdots, n$ 的一个排列. 某个置换

被它的逆置换左、右乘，其结果都等于单位置换，即

$$\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n\\ a_1 & a_2 & \cdots & a_i & \cdots & a_n\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \cdots & a_i & \cdots & a_n\\ 1 & 2 & \cdots & i & \cdots & n\end{pmatrix}=\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n\\ 1 & 2 & \cdots & i & \cdots & n\end{pmatrix},$$

$$\begin{pmatrix}a_1 & a_2 & \cdots & a_i & \cdots & a_n\\ 1 & 2 & \cdots & i & \cdots & n\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n\\ a_1 & a_2 & \cdots & a_i & \cdots & a_n\end{pmatrix}=\begin{pmatrix}a_1 & a_2 & \cdots & a_i & \cdots & a_n\\ a_1 & a_2 & \cdots & a_i & \cdots & a_n\end{pmatrix}.$$

后式的结果按照上面的说明就是单位置换，因为它将任何一个数换成它自己.

有了置换乘法的概念之后，就可以谈置换分解成对换之积的问题. 可以证明，任何一个置换都可分解成若干个对换之积. 例如

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 2 & 6 & 5\end{pmatrix}$$

是下面对换的积：(13)(14)(12)(56)，即

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 2 & 1 & 4 & 5 & 6\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 2 & 3 & 1 & 5 & 6\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 1 & 3 & 4 & 5 & 6\end{pmatrix}\cdot\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 1 & 2 & 3 & 4 & 6 & 5\end{pmatrix}.$$

又如

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

是积(12)(14)(13)(5). 其中(5)表示数 5 不变，它可以不写出，即积是(12)(14)(13)，只须记住这是五阶置换，还原成置换写法时，要把 5→5 写出.

这里顺便谈一下对换之逆的问题. 实际上，可以验证

(12)之逆即(21)，(或(12))，

(13)(24)之逆即(24)(13)，

(14)(23)(56)之逆即(56)(23)(14).

依此类推，所以一般地讲，

$(ab)(cd)\cdots(xy)(zw)$之逆即$(zw)(xy)\cdots(cd)(ab)$.

值得注意的是，一个置换分解为对换的乘积时，分解的方式不是唯一的，比如

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(13)(12)=(23)(13),$$

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(23)=(13)(23)(12).$$

但是有一个性质在分解时保持不变，那就是对换个数的奇偶性不变. 也就是说，同一个置换不可能既分解成偶数个对换的积，又分解成奇数个对换的积. 这个结论的证明我们在下面给出. 有了这个结论，我们就可以给出奇置换和偶置换的概念了. 当一个置换分解成对换的乘积时，如果对换的个数是奇数，那末这个置换叫做奇置换，如果对换的个数是偶数，那末叫做偶置换. 比如单位置换 $\begin{pmatrix}1&2\cdots i\cdots n\\1&2\cdots i\cdots n\end{pmatrix}$ 是没有经过对换的置换，也就是可以将排列 123 $\cdots i\cdots n$ 看成未曾施以对换，从而对换的个数为 0；0 是偶数，所以单位置换是偶置换.

现在我们来证明上面提到的那个结论. 证明的过程较长，但证明的方法可能对多数读者说是没有接触过的，因此读者不妨读一下，如果感到有困难，也可以跳过去不读.

首先，作一个 n 个符号 $a_1, a_2, \cdots, a_n$ 的表示式

$$\begin{aligned}\Phi=&(a_1-a_2)(a_1-a_3)\cdots(a_1-a_i)\cdots(a_1-a_j)\cdots(a_1-a_n)\\&(a_2-a_3)\cdots(a_2-a_i)\cdots(a_2-a_j)\cdots(a_2-a_n)\\&\cdots\cdots\cdots\cdots\cdots\cdots\\&(a_i-a_{i+1})\cdots(a_i-a_j)\cdots(a_i-a_n)\\&\cdots\cdots\cdots\\&(a_j-a_{j+1})\cdots(a_j-a_n)\\&\cdots\cdots\\&(a_{n-1}-a_n).\end{aligned}$$

现在将对换$(a_i\ a_j)$作用在Φ上，即将Φ中的a_i换成a_j，a_j换成a_i，看看结果如何？

（1）在表示式Φ的$n\cdot(n-1)/2$个线性(一次)因子的连乘积中，由于对换$(a_i\ a_j)$的作用，线性因子(a_i-a_j)变成(a_j-a_i)，即$-(a_i-a_j)$，所以Φ变号.

（2）对$k=1,2,\cdots,i-1$，(a_k-a_i)与(a_k-a_j)，由于对换$(a_i\ a_j)$的作用，各变成(a_k-a_j)与(a_k-a_i)，也就是说，Φ只改变相应两线性因子的位置，但不变号.

（3）对$l=j+1,j+2,\cdots,n-1$，(a_j-a_l)与(a_i-a_l)，由于对换$(a_i\ a_j)$的作用，各变成(a_i-a_l)与(a_j-a_l)，Φ也是只改变相应两线性因子的位置，不变号.

（4）对$m=i+1,i+2,\cdots,j-1$，(a_i-a_m)，(a_m-a_j)由于对换$(a_i\ a_j)$的作用各变成(a_j-a_m)，(a_m-a_i)，前者是(a_m-a_j)的反号，即$-(a_m-a_j)$；后者是(a_i-a_m)的反号，即$-(a_i-a_m)$，这两个带负号的线性因子相乘，结果与原来两线性因子相乘一样，所以Φ的正负号不受影响.

在$(a_i\ a_j)$的作用下，Φ中受影响的就是这四种线性因子，而结果只有情况(1)影响Φ的正负号，但Φ的绝对值不变，所以对Φ作对换一次，就改变一次Φ的正负号.

现在假设有一置换π既能表示成偶数个对换的积，又能表示成奇数个对换的积：

$$\pi=(b_1\ b_2)(b_3\ b_4)\cdots(b_{n-1}\ b_n)\qquad\text{偶数个因子}$$

$$\pi=(d_1\ d_2)(d_3\ d_4)\cdots(d_{m-1}\ d_m)\qquad\text{奇数个因子}$$

$b_1,b_2,\cdots,b_n,d_1,d_2,\cdots,d_m$中可能有相同的数字，对相同的只取一次，不相同的照样写下来，得

$$c_1,c_2,\cdots,c_s.$$

对$c_1,c_2,\cdots,c_s$这些符号作表示式Φ，

$$\Phi=(c_1-c_2)(c_1-c_3)\cdots(c_1-c_s)(c_2-c_3)\cdots(c_2-c_s)\cdots(c_{s-1}-c_s).$$

再把置换 π 作用到 Φ 上.

把表示成偶数个对换之积的置换 π 作用在 Φ 上，按照上面的说明，结果 Φ 的正负号改变偶数次，实际上等于不变号，即 Φ 仍保持为 Φ.

把表示成奇数个对换之积的置换 π 作用在 Φ 上，按照上面的说明，结果 Φ 的正负号改变奇数次，实际上等于变号一次，即 Φ 变为 $-\Phi$.

同一置换 π 作用在 Φ 上却产生两个不同的结果，这是一矛盾，因而同一置换不可能既表示成偶数个对换之积，又表示成奇数个对换之积.

下面我们来证明置换中另一个结果，即：n 阶置换中偶置换的个数与奇置换的个数相等.

设 n 个符号 $a_1,\cdots,a_n$ 的所有偶置换各为

$$\pi_1,\pi_2,\cdots,\pi_m,$$

它们各不相同，在它们的右边乘任意的对换，比如 (a_1,a_2)，则都变为奇置换

$$\pi_1(a_1\ a_2),\pi_2(a_1\ a_2),\cdots,\pi_m(a_1\ a_2).$$

它们也各不相同，因为，如果有一对相同，例如 $\pi_1(a_1\ a_2)=\pi_2(a_1\ a_2)$，则再在两端右边乘 $(a_1\ a_2)$，

$$\pi_1(a_1\ a_2)(a_1\ a_2)=\pi_2(a_1\ a_2)(a_1\ a_2),$$

因为 $(a_1\ a_2)(a_1\ a_2)=I$，这意味着 $\pi_1=\pi_2$，这结果与 $\pi_1,\pi_2,\cdots,\pi_m$ 各不相同的假设不合.

现在要验证偶置换的个数 m 与奇置换的个数 l 相等，先假设不相等，例如 $m>l$，由于

$$\pi_1(a_1\ a_2),\pi_2(a_1\ a_2),\cdots,\pi_m(a_1\ a_2)$$

都是奇置换，且全不相同. 而奇置换的个数 l 是 n 阶置换中全部

奇置换的个数，所有$\pi_i(a_1\ a_2)$也应在这l个奇置换中，但$\pi_i(a_1\ a_2)$的个数m竟超出全部奇置换的个数l，是不合理的，所以$m>l$的假设不成立，同样$l>m$也不合理，所以只能$m=l$，但n阶置换共有$n!$个，所以

$$m=l=\frac{n!}{2}.$$

现在请读者考虑下面的问题：

1. $\begin{pmatrix}1&2&3&4&5\\3&2&4&5&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\5&4&1&3&2\end{pmatrix}=?$

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

2. 求

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

的逆置换.

3. 请验证

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

表示成对换之积的一种形式是(13)(14)(12)(15).

4. 试验证(51)(53)(54)(52)与(25)(21)(23)(24)同是$\begin{pmatrix}1&2&3&4&5\\3&5&4&2&1\end{pmatrix}$分解成两种形式的偶数个对换之积.

5. 已知1的三次根是$x_1=1, x_2=\omega,\ x_3=\omega^2$，作此三根的表示式

$$\varphi=x_1^2+x_2^2+x_3^2.$$

以(x_1x_2)与(x_2x_3)作用于φ，问φ的值变不变？

作另外一个表示式

$$\psi=x_1+2x_2+3x_3$$

以$(x_1\ x_2\ x_3)$作用ψ，问ψ的值变不变？

三、剩　余　类

大家都知道，以7为除数，除7，14，21，…，都可除尽，即得余数为0；除8，15，22，…，都得余数为1；除9，16，23，…，都得余数为2；以此类推．在被除数为负整数的情况，例如以7除-1，得商数-1，余数为6；除-2，得商数-1，余数为5，等等．由此可得到同余的概念．

所谓两个整数l，k按模m同余，是指l，k被m除所得的余数相等，记作

$$l\equiv k \pmod m.$$

如果l，k按模m不同余，就记作

$$l\not\equiv k \pmod m.$$

请读者自行验算下列三条性质．

1. $l\equiv l \pmod m$；

2. 如果$l\equiv k \pmod m$，那末$k\equiv l \pmod m$；

3. 如果$l\equiv k \pmod m$，$k\equiv n \pmod m$，那末

$$l\equiv n \pmod m.$$

现在讲一下关于同余的一个基本定理：

1. 如果l与k按模m同余，那末必有$l-k$能被m整除，反过来也正确．

事实上：$l=q_1m+r_1$；$k=q_2m+r_2$，q_1，q_2为整商数，r_1，r_2为余数，两式相减得

$$l-k=q_1m-q_2m+r_1-r_2,$$

$$l-k=(q_1-q_2)m+(r_1-r_2).$$

但因 $r_1=r_2$(由 l 与 k 按模 m 同余),所以

$$l-k=(q_1-q_2)m,$$

即 $l-k$ 能被 m 整除.

根据这个定理就可以证明:

2. 如果 $a_1\equiv b_1 \pmod m$, $a_2\equiv b_2 \pmod m$,那末

$$a_1+a_2\equiv b_1+b_2 \pmod m$$

事实上,由 $a_1\equiv b_1 \pmod m$ 得 $\quad a_1-b_1=mq_1$,

由 $a_2\equiv b_2 \pmod m$ 得 $\quad a_2-b_2=mq_2$,

相加得 $\quad a_1+a_2-b_1-b_2=m(q_1+q_2)$

即 $\quad a_1+a_2\equiv b_1+b_2 \pmod m$.

利用同余的概念,我们可以把整数系 Z 按模 m 分类. 即固定一个自然数 m 为除数,去除每一个整数,把余数相同的作为一类,这样共有 m 类,它们是:

余数为 0 的类(记作[0]):…, $-2m$, $-m$, 0, m, $2m$, …

余数为 1 的类(记作[1]):…, $-2m+1$, $-m+1$, 1, $m+1$, $2m+1$, …

……

余数为 $m-1$ 的类(记作[$m-1$]), …, $-m-1$, -1, $m-1$, $2m-1$, $3m-1$, …

容易看出,每一个整数一定属于某一确定的类;每一类中的任意两个数一定模 m 同余;取自任意两个不同类中的整数一定模 m 不同余. 这 m 个类[0],[1],…, [$m-1$]叫做模 m 的剩余类. 0, 1, …, $m-1$ 是模 m 剩余类的代表元,在剩余类中的每一个数都可以作为代表元,即如果 $a\in[c]$,那末$[a]=[c]$.

由此可以规定,两个剩余类相加,就是各代表元相加. 例如 $[a]+[b]=[a+b]$, $[a]+[0]=[a+0]=[a]$.

四、内部的规律

大家知道，在整数系里对两个整数可以进行加法，结果仍在整数系里；在平面矢量集合中对两矢量可以进行矢量加法的运算，其结果仍是矢量，等等．这些运算都是在一定的集合内部的各元素间进行的，而其结果又不出这相应的集合，所以这里所遵循的规律是内部的规律，而数量乘矢量就不是内部的规律的作用，因数量属于数的集合，而矢量属于矢量的集合，数乘不是在同一集合内部进行的．

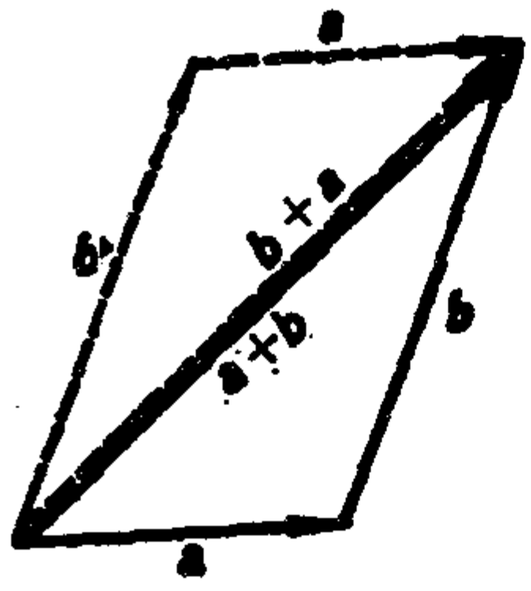
在各个特定集合内，加法、乘法、矢量加法，接连施行某个手续等等，都可以作为内部的规律．在很多书中把这些叫做代数运算，用记号 $*$ 或 $\circ$ 来表示．

I．集合 A 的任意元素 a,b 如果适合下面的等式：

$$a*b=b*a,$$

就说此集合的元素对 $*$ 是可交换的，或说交换律成立．

在实数域 R，有理数域 Q 里，对于加法、乘法，交换律成立；这是众所周知的．在自由矢量的集合中，对于矢量加法，交换律成立，这可以从右图看出．



在模 m 的剩余类集合中，各剩余类对于加法交换律成立．

因为按规定，$[a]+[b]=[a+b]$，

$$[b]+[a]=[b+a],$$

因数的加法满足交换律，$a+b$ 与 $b+a$ 相等，所以 $[a+b]=[b+a]$，从而

$$[a]+[b]=[b]+[a].$$

即剩余类对于加法交换律成立.

但是,交换律不成立的情形也是不胜枚举的,例如:

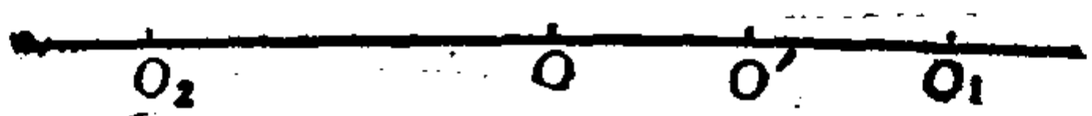
(1) 在 n 阶置换的集合中,对于置换乘法交换律一般不成立,这在(壹二)中已经谈到.

(2) 在自由矢量的集合中,对矢量的乘法,即所谓叉乘,交换律不成立:

$$\boldsymbol{a}\times\boldsymbol{b}\neq\boldsymbol{b}\times\boldsymbol{a},$$

这是因为 $\boldsymbol{a}\times\boldsymbol{b}=-\boldsymbol{b}\times\boldsymbol{a}$ 的缘故.

(3) 在平面几何中,令 α 为"在直线上关于点 O 取对称的象",β 为"在此直线上关于另一点 O' 取对称象",$*$为接连进行取对称象的手续,$\alpha*\beta$ 表示先作 β,接着将 β 的结果再作 α,请看图上标志的点



先说明一下,什么是在"直线上关于点 O 取对称的象". 例如,将 O_1 关于 O 取对称的象,就是先取线段 O_1O,再在 O 的另一侧取长度与 O_1O 的长度相等的线段 OO_2,点 O_2 就是点 O_1 关于 O 的对称的象,又如将点 O 取关于 O 的对称的象,即对 O 作 α. 记为 αO (同样可说明 βO). 这时线段 OO 缩为一点,长度是零,O 关于 O 的对称的象就是 O 本身,所以 $\alpha O=O$. 根据以上的说明,并注意到 $OO'=O'O, OO_1=OO_2$,

$$(\beta*\alpha)O=\beta O=O_1,$$

$$(\alpha*\beta)O=\alpha O_1=O_2.$$

所以 $\alpha*\beta\neq\beta*\alpha$,即作为变换,元素 α,β 对 $*$ 是不可交换的.

II. 在集合 A 中,a,b,c 为它的任意三个元素,如果对于$*$,下面的式子成立:

$$(a*b)*c=a*(b*c),$$

就说此集合的元素间对于代数运算 * 是可结合的，或运算 * 满足结合律.

在有理数系 Q，实数系 R 里，对于加法、乘法，结合律都成立. 在平面的矢量集合里，对矢量的加法，结合律成立. 在集合的运算里，对并、交，结合律成立. 对剩余类的加法，结合律也成立. 这些读者都可自行验证.

还可以验证，对置换乘法，结合律成立.

事实上，设有 n 阶置换

$$A=\begin{pmatrix}1 & 2 & \cdots & n\\ a_1 & a_2 & \cdots & a_n\end{pmatrix},\quad B=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ b_1 & b_2 & \cdots & b_n\end{pmatrix},$$

$$C=\begin{pmatrix}b_1 & b_2 & \cdots & b_n\\ c_1 & c_2 & \cdots & c_n\end{pmatrix}$$

对于 B,C 的写法，我们在前面已作过说明，所以要写成那样，是为了便于做乘法. 这样

$$(AB)C=\left[\begin{pmatrix}1 & 2 & \cdots & n\\ a_1 & a_2 & \cdots & a_n\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ b_1 & b_2 & \cdots & b_n\end{pmatrix}\right]\cdot\begin{pmatrix}b_1 & b_2 & \cdots & b_n\\ c_1 & c_2 & \cdots & c_n\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & \cdots & n\\ b_1 & b_2 & \cdots & b_n\end{pmatrix}\begin{pmatrix}b_1 & b_2 & \cdots & b_n\\ c_1 & c_2 & \cdots & c_n\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & \cdots & n\\ c_1 & c_2 & \cdots & c_n\end{pmatrix},$$

$$A(BC)=\begin{pmatrix}1 & 2 & \cdots & n\\ a_1 & a_2 & \cdots & a_n\end{pmatrix}\left[\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ b_1 & b_2 & \cdots & b_n\end{pmatrix}\cdot\begin{pmatrix}b_1 & b_2 & \cdots & b_n\\ c_1 & c_2 & \cdots & c_n\end{pmatrix}\right]$$

$$=\begin{pmatrix}1 & 2 & \cdots & n\\ a_1 & a_2 & \cdots & a_n\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ c_1 & c_2 & \cdots & c_n\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & \cdots & n\\ c_1 & c_2 & \cdots & c_n\end{pmatrix}.$$

但是结合律不成立的事例也是不少的，请看

(1) 在实数系里，对于将两数之和除以 $n(n>1)$ 的运算，结合律不成立：

$$\frac{\frac{a+b}{n}+c}{n}=\frac{a+b+nc}{n^2},\quad \frac{a+\frac{b+c}{n}}{n}=\frac{na+b+c}{n^2};$$

此二式的结果一般是不等的，所以结合律不成立.

(2) 在三维矢量的集合里，任意三个矢量对于矢量积，结合律一般不成立(这里不予证明)：

$$(\boldsymbol{a}\times\boldsymbol{b})\times\boldsymbol{c}\neq\boldsymbol{a}\times(\boldsymbol{b}\times\boldsymbol{c}).$$

在今后我们将遇到不少的代数运算，随着群的研究的展开，代数运算的重要性将愈来愈被读者所理解.

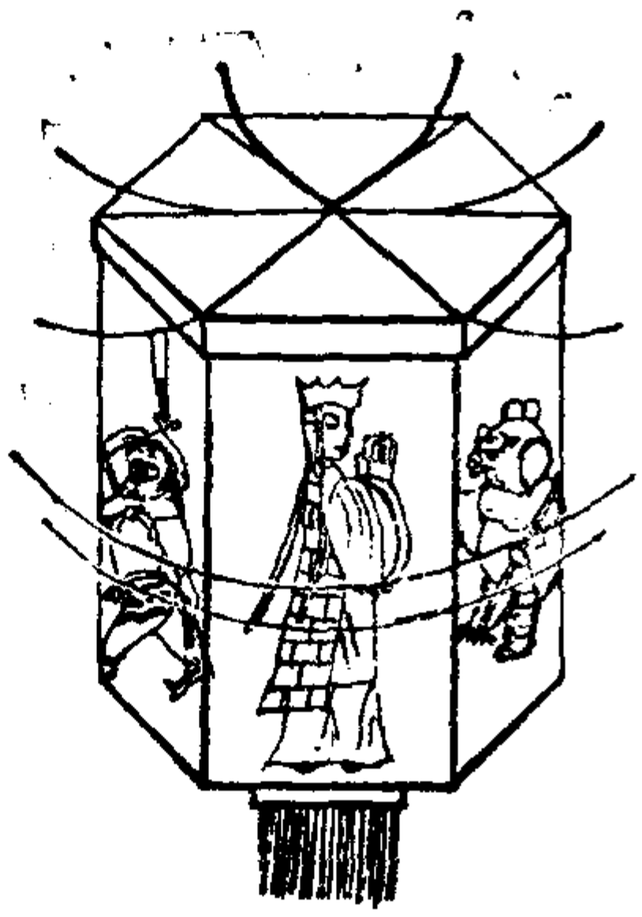
贰

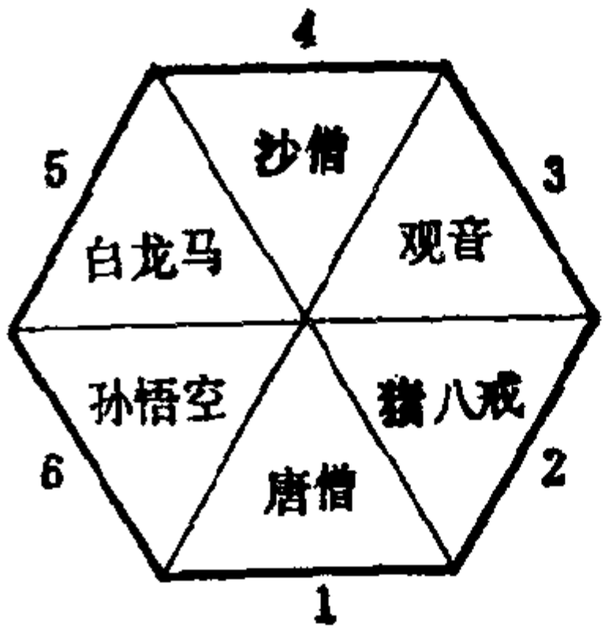
从走马灯谈起

——群与群的例子

一、走马灯里有数学问题吗?

中国人喜爱元宵节，这一天晚上五色缤纷的彩灯给人们带来欢乐，特别是走马灯，这种精致的艺术品显示出中国人民的聪明智慧，正六边形柱体的宫灯内，在点燃灯芯后，就依次转动着六幅人物或风景图片，走马灯能绕轮轴转动，有其物理原因，这是毋须多说的，但是有没有数学问题呢？下面我们来作些分析.





假设走马灯内是“去西天取经”的人物和他们的支持者的图片，(1)唐僧，(2)猪八戒，(3)观音，(4)沙僧，(5)白龙马，(6)孙悟空，如图所示，各就各位.

以反时钟方向绕中心O转动60°的角(在这里将转60°及它

的倍数的转动看作是有意义的转动. 不计其他的转动). 这个运动以 φ 来表示, φ 把唐僧从 1 号位转到 2 号位; 把猪八戒从 2 号位转到 3 号位, ……. 所以在这个问题里, 绕中心 O 转动 60° 的角, 相当于置换

$$\varphi:\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}$$

顺便说一下, $\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}$ 这种形式的置换, 就是前面曾说到的轮换(1 2 3 4 5 6).

再转动一个 60° 的角, 即两次施行 φ, 到本节末就会看到接连施行 φ 是一代数运算, 两次施行 φ 即 $\varphi*\varphi$, 简写作 $\varphi\varphi=\varphi^2$, 得

$$\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{pmatrix}.$$

即两次施行 φ 的结果, 唐僧从第一位转到第三位, 猪八戒从第二位转到第四位, ……, 以下类推.

又可看到, 例如 $\varphi^2,\varphi,\varphi^3$ 可以按下述方式结合: (1) $(\varphi^2*\varphi)*\varphi^3$; (2) $\varphi^2*(\varphi*\varphi^3)$. 按照(壹四)中所说, 对置换乘法结合律成立, 所以 $(\varphi^2*\varphi)*\varphi^3=\varphi^2*(\varphi*\varphi^3)$.

不难看出

$$\begin{pmatrix}1&2&3&4&5&6\\5&6&1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\5&6&1&2&3&4\end{pmatrix},$$

即 $\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$ 是原位不动的转动, 即转 $0°=0\cdot60°$ 的角, 它不影响其他的转动.

最后, 如果在 φ^2 后继续施行四次 φ, 即 φ^4, 得

$$\begin{pmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$$

这样，在 φ^2 以后施行 φ^4：$\varphi^2*\varphi^4$，各个人物都回到原位.

从走马灯我们可以得到以下几点启示：（1）如果保持反时钟方向每次转 60° 角，即施行 φ，那末不论转多少次，在某位总不外乎上述六个人物出现. 改用置换的术语，即有六个置换：

$$\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{pmatrix},$$

$$\begin{pmatrix}1&2&3&4&5&6\\4&5&6&1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5&6\\5&6&1&2&3&4\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5&6\\6&1&2&3&4&5\end{pmatrix},$$

其中任意两个按置换乘法相乘，其结果终不出这六个之外，因而置换乘法是这里的代数运算.

（2）三个转动相继施行，可以有两种结合方式，其结果相同，即例如前面的 $(\varphi^2*\varphi)*\varphi^3=\varphi^2*(\varphi*\varphi^3)$.

（3）有一种实际上不变位的转动，例如 0°，360°，720°等等，它不影响其它转动，如同化学中的中性元素一样.

（4）有一种转动，就有一种返回到原位的转动，例如前面提到的 φ^2，它的返回到原位的转动是 φ^4，相应的置换表示是

$$\varphi^2:\begin{pmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{pmatrix},\quad \varphi^4:\begin{pmatrix}1&2&3&4&5&6\\5&6&1&2&3&4\end{pmatrix};$$

我们就以走马灯的转动作为前导，引出群的概念，并检验一些群的例子.

二、群 的 定 义

假定 G 是具有有限个或无限个元素的集合，在 G 的元素间给出了一个代数运算 $*$（加、乘或其他），使得

1）如果 $a\in G, b\in G$，那末必有 $c\in G$，使

$$a*b=c,$$

以后 $a*b$ 简写为 ab. 这个要求叫做封闭性.

2) 对 G 的任意三个元素 a, b, c, 成立

$$(ab)c = a(bc).$$

这叫做 G 的任意三元素满足结合律.

3) 存在一个元素 $e \in G$, 使得

$$ae = a, \quad ea = a,$$

e 叫做中性元素(在乘法中叫单位元素, 在加法中叫零元).

4) 对每个元素 $a \in G$, 存在一个 $a^{-1} \in G$, 使得

$$aa^{-1} = e, \quad a^{-1}a = e,$$

a^{-1} 叫做 a 的逆元, 或对称元.

这时, 就说集合 G 关于代数运算*是一个群.

事实上, 这个中性元素是唯一的. 因为, 如果有另一个 e', 也使 $e'a = a, a \in G$, 那末 $e'a = a = ea$. 根据群的元素有逆元素的性质, 设 a 的逆元素为 a^{-1}, 那末

$$e'aa^{-1} = eaa^{-1},$$

$$e'e = ee$$

即

$$e' = e.$$

于是, e 与 e' 是同一个中性元素.

同样可以证明, 每个元素 a 的逆元 a^{-1} 也是唯一的. 事实上, 设有 a 的另一逆元 a_1^{-1}, 那末

$$aa^{-1} = e = aa_1^{-1},$$

$$a^{-1}aa^{-1} = a^{-1}aa_1^{-1},$$

$$a^{-1} = a_1^{-1}.$$

由此可见 a^{-1} 与 a_1^{-1} 是相同的. 所以每个元素 a 的逆元素 a^{-1} 是唯一的.

群里元素的个数简称做元数, 或群的阶. 元数为无限的叫做无限群, 元数为有限的叫做有限群.

以上这四个性质对群来说是不可少的，谈到群时就要逐一验证这四个性质是否成立.

前节讲到的走马灯绕中轴的旋转，即正六角形绕中心每次转60°，那里提到的四点启示，都适合以上四点要求，所以可以粗略地讲：走马灯的每次转 60° 的旋转做成群，或者给这个群一个外号：走马灯群，尽管可能不合乎科学习惯，但也许还能加深印象吧！

群 G 的一部分元素所成的子集 A 和子集 B 之间按群的代数运算的积 $A*B$，以后简写作 AB，在 A,B 为有限的情形，AB 是这样的集合：它的元素是 A 的各元素 a_i（在左边）与 B 的各元素 b_j（在右边）按代数运算 $*$ 的积 a_i*b_j，以后简记作 a_ib_j，而 $B*A$ 即 BA 则是由 b_k*a_l，即 $b_ka_l(b_k\in B, a_l\in A)$ 所组成的集合，a_ib_j, b_ja_i 一般是不相同的. 用表格列出各元素的 A 与 B 积如下（其中并不排除有重合的）：

左边 A\右边 B	b_1	b_2	$\cdots$	b_i	$\cdots$	b_m
a_1	a_1b_1	a_1b_2	$\cdots$	a_1b_i	$\cdots$	a_1b_m
a_2	a_2b_1	a_2b_2	$\cdots$	a_2b_i	$\cdots$	a_2b_m
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	a_ib_1	a_ib_2	$\cdots$	a_ib_i	$\cdots$	a_ib_m
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	a_nb_1	a_nb_2	$\cdots$	a_nb_i	$\cdots$	a_nb_m

$=AB.$

关于 BA，情况是相似的，只须注意各个 b_k 在左边，各个 a_l 在右边，即可.

如果 A 只含一个元素 a，则 $AB=aB=\{ab_1, ab_2, \cdots, ab_m\}$，$BA=Ba=\{b_1a, b_2a, \cdots, b_ma\}$，如果 B 只含一个元素 b，则以此类推即得结果. 去掉有限这个条件，在一般的情形，用公式表示就是

$$AB=\{ab\mid a\in A, b\in B\}$$

与

$$BA=\{ba\mid a\in A, b\in B\}.$$

可以验算：$(A\cup B)C=AC\cup BC$，例如 $A=\{a_1,a_2\}$，$B=\{b_1,b_2,b_3\}$，$C=\{c\}$. $A\cup B=\{a_1,a_2,b_1,b_2,b_3\}$，$(A\cup B)C=\{a_1c,a_2c,b_1c,b_2c,b_3c\}=\{a_1c,a_2c\}\cup\{b_1c,b_2c,b_3c\}=AC\cup BC$.

三、群 的 例 子

I. 元素为数或函数的群

(1) 整数系Z对加法构成群，它是无限群.

我们从中学代数已知，在整数系 Z，即在全体整数中，有(任意)整数 a，同时也有$-a$，以及 0.

1) 封闭性成立是显然的；

2) 结合律，成立也是显然的. 因为数的加法满结合律，例如 $a,-b,c\in Z$，则

$$a+[(-b)+c]=[a+(-b)]+c.$$

3) 中性元素为数 0.

4) 元素 a 的逆元为$-a$；$-a$ 又叫做 a 的负元.

(2) 有理数系Q对加法构成群，它是无限群.

(3) 实数系R对加法构成群，它是无限群.

(4) 复数系C对加法构成群，它是无限群.

(2)—(4)的验证十分简单，读者可自己进行.

(5) 所有偶数 $2m$ 的集合 M，$m\in Z$，对于数的加法构成群，它是无限群.

1) 封闭性. 设任意两个偶数：$2p$，$2q$，$p,q\in Z$，则 $2p+2q=2(p+q)$，$p+q\in Z$，所以 $2p+2q\in M$.

2) 结合律由数的加法满足结合律得到.

3) 中性元素为 0.

4) 每个元 $2p$ 的逆元存在，它是$-2p$.

这样所有偶数 $2m$ 的集合就构成一个加法群.

(6) 正有理数集 Q^+ 对乘法构成群,它是无限群.

封闭性和结合律是显然的. 中性元素是 1. 因为 Q^+ 的每个元素 $a=\frac{p}{q}>0, p, q\in N$, 所以 $\frac{1}{a}\left(=\frac{q}{p}\right)$ 存在且大于 0, 即 a 的逆元存在.

(7) 正实数集 R^+ 对乘法构成群,它是无限群.

(8) 从有理数系中去掉 0 所成的集, 记作 $Q'=Q-\{0\}$. 这个集对乘法构成群. 请读者注意,如果不去掉 0,"每个元存在逆元"的这个关于乘法群的要求能否被满足?同时由此还请读者注意,消去律并非在任何情况下总能成立, 即由 $ab=ac$, 并不总能推出 $b=c$. 因为例如 $4\cdot 0=3\cdot 0$, 但$4\neq 3$.

(9) 从实数系 R 中去掉零的集合, 同上面相仿记作 $R'=R-\{0\}$,这个集合对乘法构成群,它是无限群.

(10) 从复数系 C 中去掉零的集合记作$C'=C-\{0\}$, 这个集合对乘法构成群,它是无限群.

((7)—(10)的验证法与(6)相似,请读者自行验证)

(11) 模为 1 的复数集 C_1 对乘法构成群,它是无限群. 用指数形式来表示复数

$$z=\rho e^{i\varphi}$$

ρ 为模,φ 为辐角,i 为虚数单位,模为 1 的复数为

$$z=e^{i\varphi}.$$

φ 可取任意实数,所以 z 的个数是无限的.

1) 封闭性. 设有

$$z_1=e^{i\varphi_1},\quad z_2=e^{i\varphi_2},\quad z_3=e^{i\varphi_3},$$

那末有

$$z_1z_2=e^{i\varphi_1}\cdot e^{i\varphi_2}=e^{i\varphi_1+i\varphi_2}=e^{i(\varphi_1+\varphi_2)}.$$

这仍然是模为 1 的复数.

2) 结合律成立.

$$(z_1 \cdot z_2) \cdot z_3 = e^{i(\varphi_1+\varphi_2)} \cdot e^{i\varphi_3} = e^{i(\varphi_1+\varphi_2+\varphi_3)},$$

$$z_1 \cdot (z_2 \cdot z_3) = e^{i\varphi_1} \cdot (e^{i(\varphi_2+\varphi_3)}) = e^{i(\varphi_1+\varphi_2+\varphi_3)}.$$

3) 中性元显然为 $1 = e^{i0} = e^0$.

4) 任意元的逆元存在，设 $z = e^{i\varphi}$，那末逆元为 $z^{-1} = e^{-i\varphi} = e^{i(-\varphi)}$，因为 $z \cdot z^{-1} = e^{i\varphi} \cdot e^{-i\varphi} = e^{i(\varphi-\varphi)} = e^0 = 1$.

根据以上四点，所以说模为 1 的复数对乘法构成群.

(12) 1 的三次根：$1, \omega, \omega^2$ 对乘法构成群，它的元数为 3. 验证它构成群，只要记住 $\omega = \dfrac{-1+\sqrt{3}\,i}{2}$，$\omega^3 = 1$. 为清楚起见，我们把验算的结果用表格的形式写出来：

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

也就是说，把 $1, \omega, \omega^2$ 分别依次写在最上面一行和最左一列，把两个元素相乘的结果写在这两个元素所在行和列的交叉处，比如 $\omega^2 \cdot \omega$ 的结果就是 ω^2 所在的行和 ω 所在的列的交叉处的 1. 读者可以自己想一想，怎么从表上看出群的 4 条性质都是满足的.

一般，对群的元素进行运算的结果用如上这样的表格表示时，这种表叫做群的乘法表.

(13) 数 1 与 -1 对数的乘法构成群.

因为 $1 \cdot 1 = 1, (-1) \cdot 1 = -1, (-1)(-1) = 1$，所以封闭性成立. 结合律因数的乘法满足结合律而成立. 中性元素为 1. 任一元的逆元为各自元素本身，即 1 的逆元是 1，-1 的逆元是 -1.

(14) 以代换为代数运算的一种群.

设有四个函数:以下规定 $x\neq0$,

$e(x)=x$,假设这是原始的函数;

$f(x)=\dfrac{1}{x}$,这是原始函数的倒数函数;

$g(x)=-x$,这是原始函数的负函数;

$h(x)=-\dfrac{1}{x}$,这是原始函数的负倒数函数.

以函数代换作为代数运算*. 即,例如

$$h(x)*f(x)[\text{或 }hf(x)]=h\left(\frac{1}{x}\right)=-\frac{1}{\frac{1}{x}}=-x,\text{等等.}$$

为验证*的封闭性,我们把所有二个元的乘积写出来:

$ee(x)=e(x)$;

$ef(x)=e\left(\dfrac{1}{x}\right)=\dfrac{1}{x}=f(x)$;　　$fe(x)=f(x)$;

$eg(x)=e(-x)=-x=g(x)$;　　$ge(x)=g(x)$;

$eh(x)=e\left(-\dfrac{1}{x}\right)=-\dfrac{1}{x}=h(x)$;　　$he(x)=h(x)$;

$gf(x)=g\left(\dfrac{1}{x}\right)=-\dfrac{1}{x}=h(x)$;

$fg(x)=f(-x)=\dfrac{1}{-x}=-\dfrac{1}{x}=h(x)$;

$fh(x)=f\left(-\dfrac{1}{x}\right)=\dfrac{1}{-\frac{1}{x}}=-x=g(x)$;

$hf(x)=h\left(\dfrac{1}{x}\right)=-\dfrac{1}{\frac{1}{x}}=-x=g(x)$;

$gh(x)=g\left(-\dfrac{1}{x}\right)=-\left(-\dfrac{1}{x}\right)=\dfrac{1}{x}=f(x)$;

$hg(x)=h(-x)=-\left(-\dfrac{1}{x}\right)=\dfrac{1}{x}=g(x)$;

$$ff(x)=f\left(\frac{1}{x}\right)=\frac{1}{\frac{1}{x}}=x=e(x);$$

$$gg(x)=g(-x)=-(-x)=x=e(x);$$

$$hh(x)=h\left(-\frac{1}{x}\right)=-\frac{1}{-\frac{1}{x}}=-(-x)=x=e(x);$$

由上面的验算中可以看出 $e(x)$是中性元素，每一个元素的逆元素是它本身．读者可自行验证结合律成立．因此这四个函数关于代换构成群．这个群有很有趣的几何意义，我们将在(18)中说明．

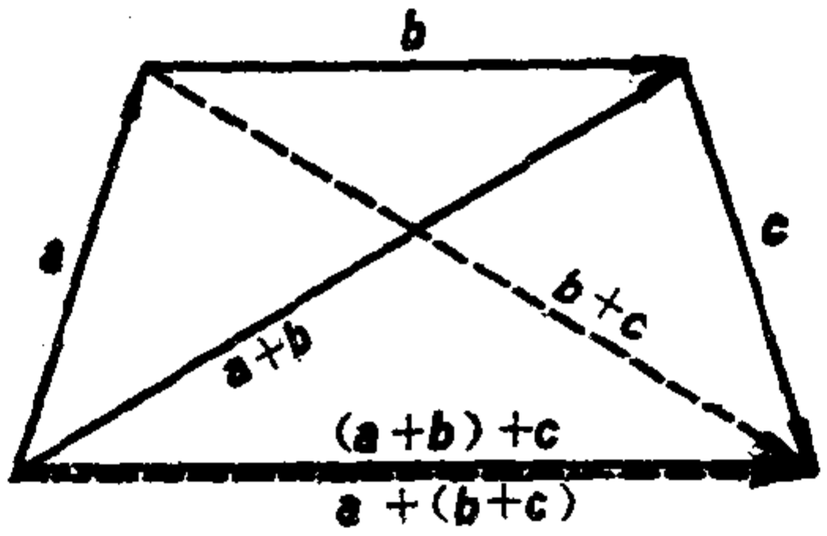
由上面的验算我们还可以看出这个代数运算*是交换的．

II．几何中的群

(15) 三维空间里矢量的集合对矢量加法构成群

1) 封闭性是显然的．因为任意两个矢量的和仍为矢量；

2) 对矢量加法结合律成立，看下图即知

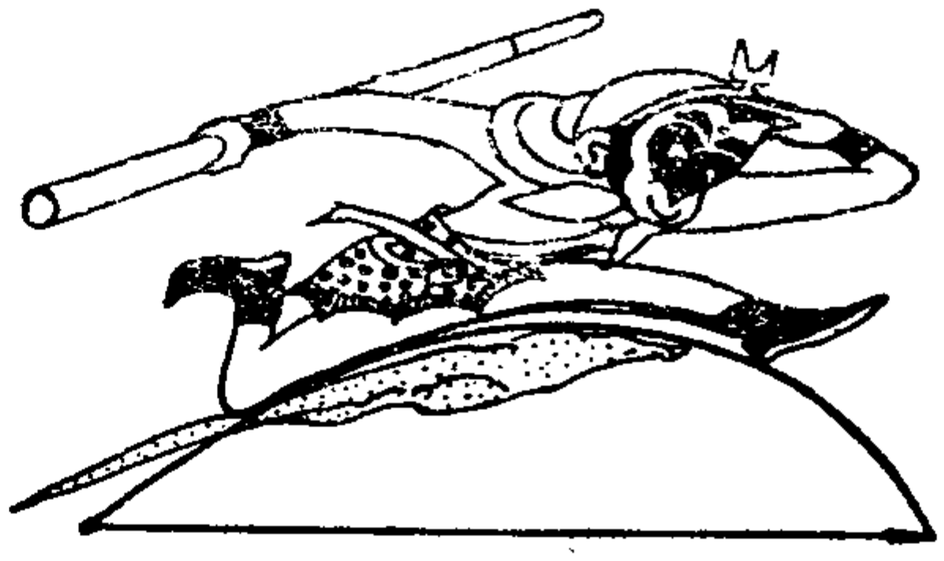


此图说明 $(a+b)+c=a+(b+c)$

3) 中性元为零矢量 0；

4) 任一个元 a 的逆元为 $-a$；

这里读者不妨把思路放开一点，考虑一句俗话："孙悟空的本领大，一个跟斗十万八千里，再大，也翻不出如来佛的手掌心．"这句话是在炫耀一个人可以控制另一个人的能力时常用的，将它从数学上改造一下，即如果把如来佛的手掌看作广阔无垠的平面(即无限的平面)，孙悟空的跟斗是从平面一点到另一点的矢量(不计



翻到空中的那段弧)，大小任意，包括原地不动的零矢量，方向任意，翻的次数任意. 所说的矢量都在平面内(即如来佛的手心里)，它们的和也在平面内，即对加法运算是封闭的. 由此可见，从上面那句话就可构造平面矢量对矢量加法的群.

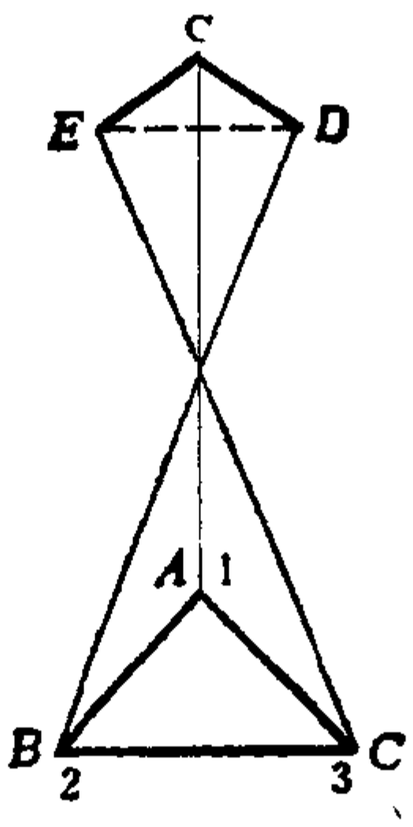
(16) 正三角形的运动群

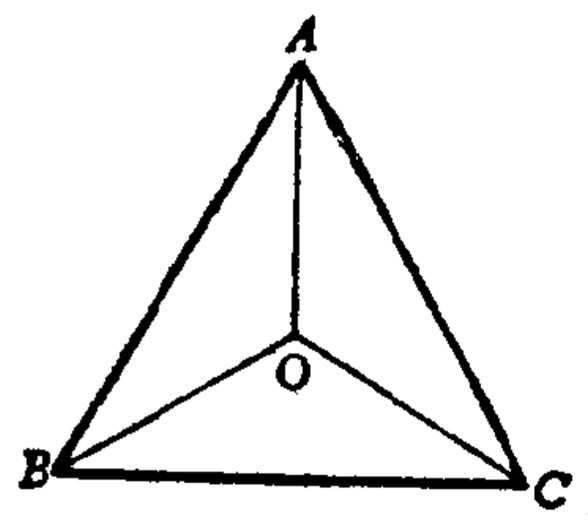
打一个比喻，一个放小鼓的活动的三脚支撑架，地上的落脚点 No. 1, No. 2, No. 3 是固定的，联成正三角形，但究竟是哪个脚(假定给支脚以不同的名称如 A、B、C)落在哪个点上却是随意的，这样就产生了不同的支架方法:(下面的记法，如 $2A$，表示 A 脚落在 No. 2 点上，等等)

$$(1A, 2B, 3C);\ (2A, 1B, 3C);\ (3A, 1B, 2C);$$

$$(1A, 3B, 2C);\ (2A, 3B, 1C);\ (3A, 2B, 1C).$$

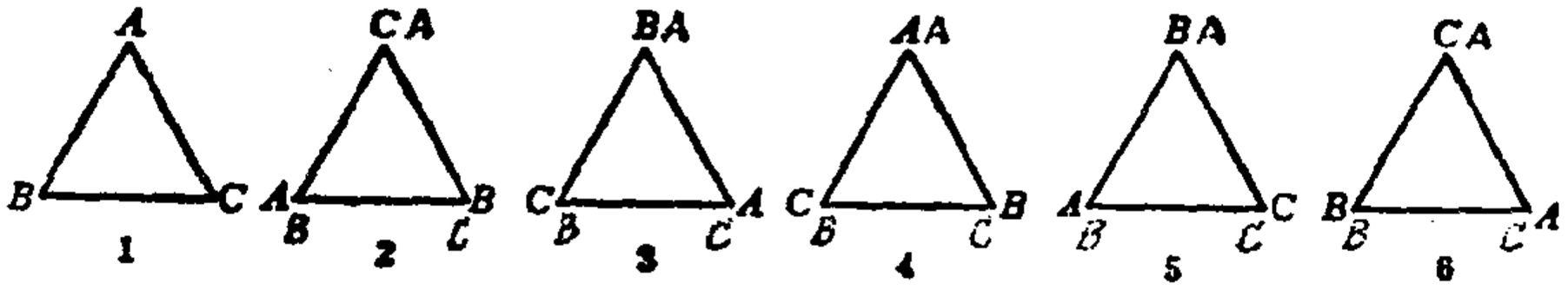
从几何上来看就有下面的类似物.





设有一个正三角形 $\triangle ABC$(请注意顶点 A, B, C 的放置地位)，它的

中心为 O，所谓正三角形的运动就是只变更三角形的顶点与边的相对位置，但不改变 $\triangle ABC$ 所占空间的运动．即是说，在原来的顶点位置和边的位置，可以有如下的几种情形：



每个角的大小，每条边的长短都不变，以虚点写的字母表示原顶点．与三脚支架中地面上点编号 No. 1, No. 2, No. 3 一样，这样就必然要有如下几种运动：

1）在平面内绕中心 O 反时钟方向旋转 120°和 240°．转 120°时 A 换成 C，C 换成 B，B 换成 A，即情形 1 换成情形 2，据上面所说的换法，可用置换表示成

$$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},$$

转 240°时，$A\to B, B\to C, C\to A$，置换表示是

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}.$$

2）以 AO, BO，CO 为轴各转 180°．关于 AO 轴转 180°的运动，这是在三维空间里转动，其结果是 $A\to A, B\to C, C\to B$，即情形 1 换成情形 4．用置换来表示，即

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix},$$

关于 BO 和 CO 各转 180°的运动，其结果分别为 $B\to B$，$A\to C, C\to A$ 和 $C\to C, A\to B, B\to A$，即

$$\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \text{ 和 } \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.$$

3）完全不动：$A\to A, B\to B, C\to C$，用置换来表示

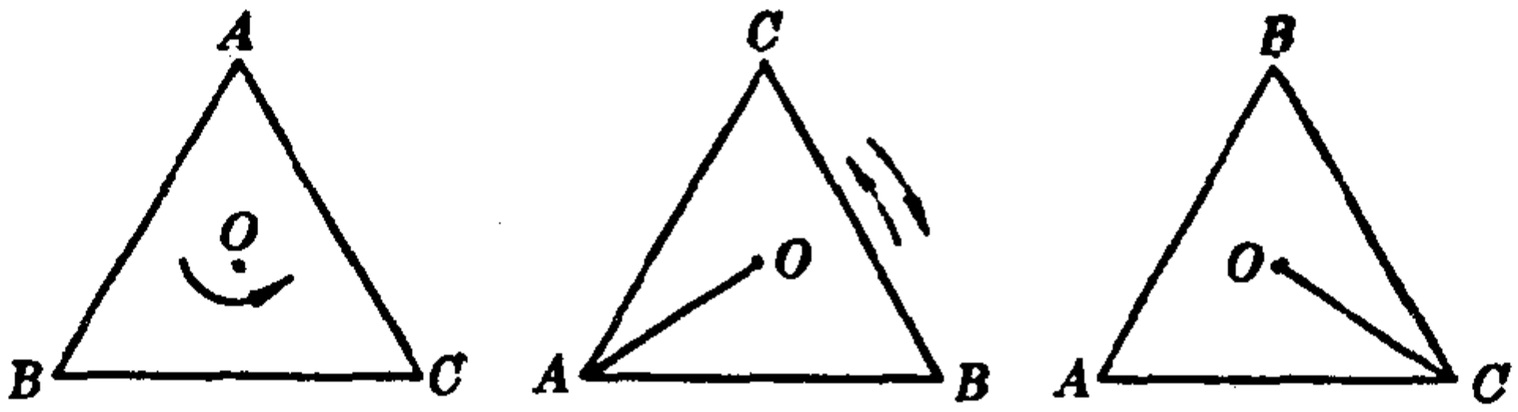
$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}.$$

显然这是中性元素.

现在来看两次运动的结果：

$$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

这是先将正三角形$\triangle ABC$从原位绕中心O反时钟方向转120°一次，再绕轴AO在空间转180°一次，结果如同原图绕CO轴转180°，请看图：



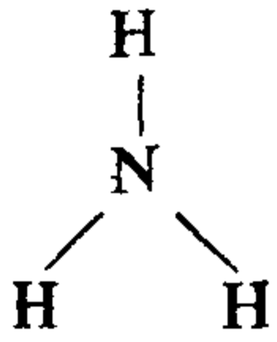
这样的正三角形运动的元素共有六个，即

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},$$

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}.$$

按照置换乘法(或上述运动)，它们构成群.

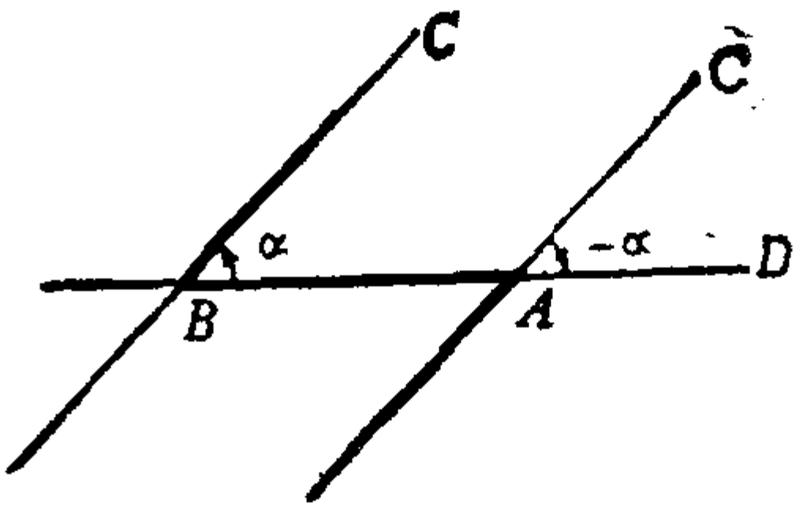
从正三角形运动可看到，氨NH_3分子结构式



(N实际在纸面之上)保持原来位置的运动，请读者自己考虑它的

运动情况.

但是,要提请读者注意,在平面上的一切旋转并不构成群,请看下面的例子.

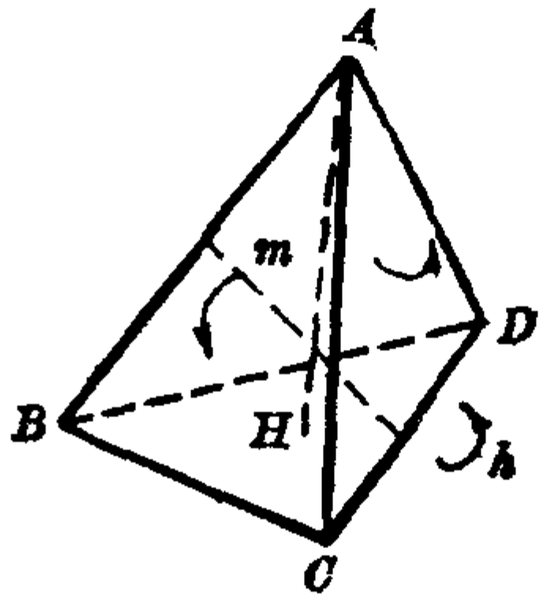


设有一活动卡尺,(AB 为活动槽,槽中有活动钮)它处于CAD的状态. 先将卡尺收拢,也就是将 CA 以活动钮所在的支点 A 为轴心绕它转一个角度 $-\alpha$,而使 CA 与 DA 重合. 尺的另一支 DA 始终不动,然后(此时将活动钮从支点 A 顺着 DA 移到后面的 B 点.)使CB绕B点转一个角度 α,再使活动卡尺的两支分开,卡尺便呈图中 $\mathbf{C}BD$($\mathbf{C}$ 即C,为了表示位置不同,故写作 $\mathbf{C}$)的状态,那末从 C 到 $\mathbf{C}$ 是一平移,如果将连接进行旋转作为这里的运算$*$,旋转记作 R,平移记作 T. 使 CA 与 DA 重合的旋转是 $R(CA,-\alpha)$,使卡尺张开的旋转是 $R(\mathbf{C}B,\alpha)$,从 C 到 $\mathbf{C}$ 的平移是 T;那末先作旋转 $R(CA,-\alpha)$,再作旋转 $R(\mathbf{C}B,\alpha)$,

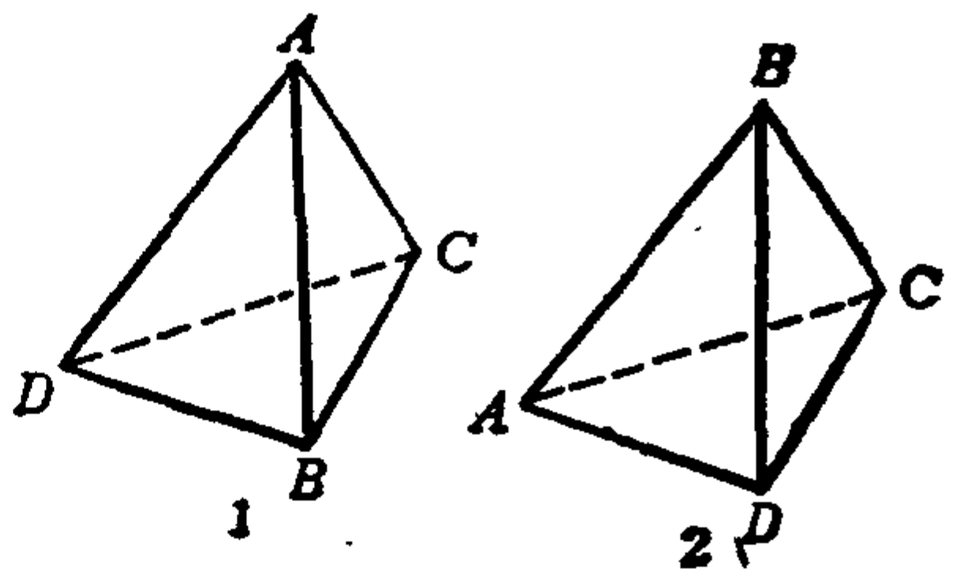
$$R(CA,-\alpha)*R(\mathbf{C}B,\alpha)=T.$$

由此可见这样的两次旋转,结果是平移,而不是旋转. 一般地,平面上两次旋转的结果,可能不是旋转,封闭性不能成立,所以平面上一切旋转不构成群. 但是由上面所说可以猜到平面的旋转与平移却可以构成群.

(17) 正四面体运动的群



所说的正四面体运动,是这样一种运动,它只改变顶点、面、棱的相对位置,但不改变它所占的空间.也就是经过运动,要在原来的顶点、棱、面位置出现下列情形. 例如,(1) 顶点 A 不动,而底面的正三角形$\triangle BCD$ 转动:D换到 B 的位置,B 换到 C 的位置,C换



到 D 的位置，即原图换成情形 1；（2）两对顶点的位置相互对调，即原图中顶点 A,B 对调，C,D 对调，即换成情形 2，A,D；B,C 对调，A,C；B,D 对调的情形可以类推；（3）最后是原图不动．（在(15)中已将平面三角形的运动作了较详细的分析，这里对正四面体的分析就比较概括一些；因为可以从平面三角形类推到正四面体，同时读者也可以用硬纸做成正四面体来分析，关键是要掌握下面所说的三种类型的运动．）

正四面体的运动有下面的三种方式：

1）将高 AH 作为旋转轴，绕它按图示方向转 120°，240°，以图示方向为正向，得到两个运动，这就是上面说到情形 1.

$$h_1=\begin{pmatrix} A & B & C & D \\ A & D & B & C \end{pmatrix},\qquad h_1^2=\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}.$$

分别以高 BH_2, CH_3, DH_4 为轴而转动．例如以 BH_2 为转轴按 A 到 C，C 到 D，D 到 A 方向转 120°，240°，得到

$$h_2=\begin{pmatrix} A & B & C & D \\ C & B & D & A \end{pmatrix},\qquad h_2^2=\begin{pmatrix} A & B & C & D \\ D & B & A & C \end{pmatrix}.$$

类似地还有 $h_3=\begin{pmatrix} A & B & C & D \\ D & A & C & B \end{pmatrix}$，$h_3^2=\begin{pmatrix} A & B & C & D \\ B & D & C & A \end{pmatrix}$，

$$h_4=\begin{pmatrix} A & B & C & D \\ B & C & A & D \end{pmatrix},\qquad h_4^2=\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix},$$

h_1^2 即是先作一次 h_1，再作一次 h_1：$h_1 * h_1 = h_1^2$，余类推．可以看到

$h_1^3, h_2^3, h_3^3, h_4^3 = e$，即还原.

2) 以对棱中点的联结线作为轴. 例如绕其中一轴按 A 到 B，B 到 A，C 到 D，D 到 C 方向作 180° 的旋转，结果就是上面说到的情形 2. 这里有三个运动.

$$m_1=\begin{pmatrix} A\ B\ C\ D \\ B\ A\ D\ C \end{pmatrix},\quad m_2=\begin{pmatrix} A\ B\ C\ D \\ C\ D\ A\ B \end{pmatrix},$$

$$m_3=\begin{pmatrix} A\ B\ C\ D \\ D\ C\ B\ A \end{pmatrix};$$

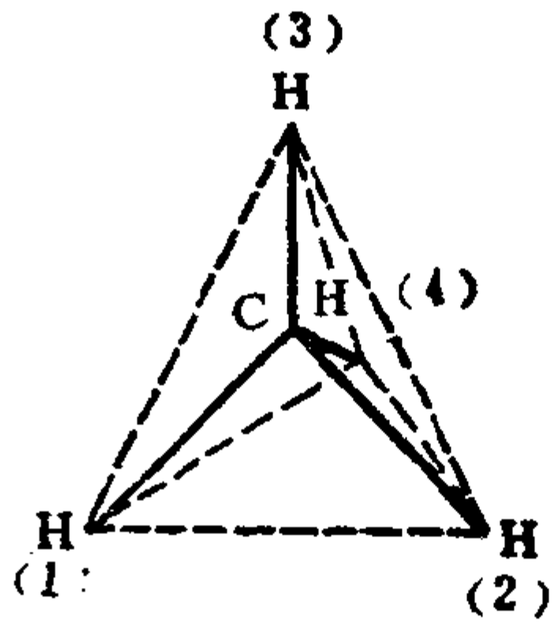
可以看到 $m_1^2, m_2^2, m_3^2 = e$.

3) 完全不动

$$e=\begin{pmatrix} A\ B\ C\ D \\ A\ B\ C\ D \end{pmatrix}$$

这里以置换乘法作为运算，上述 12 个元素构成群，例如：$h_3 \cdot m_1 = h_2, m_3 \cdot h_3 = h_4$ 等等，即封闭性成立；由于置换乘法满足结合律，所以结合律成立是不言自明的；中性元即是 3) 中的 e；至于每个元素存在逆元素，可请读者自行证明. 读者到后面就会看到，这实际上是四阶交代群.

从正四面体运动可以推测到甲烷 CH_4 分子结构式保持原来位置的运动，请读者自己考虑它的具体情况；这时须注意 CH_4 分子结构式的运动群是置换群 S_4（见例22），而不是交代群 A_4（见例23）. 因为例如它允许有奇置换(12)，即关于平面 $\overset{(3)}{H}\ C\ \overset{(4)}{H}$ 的镜面反射.



(18) 抛物线上的群

我们知道抛物线的方程式为

$$y^2=2px,$$

其中 p 为焦距，现将此方程式改变形式：令 $p=2a$，那末

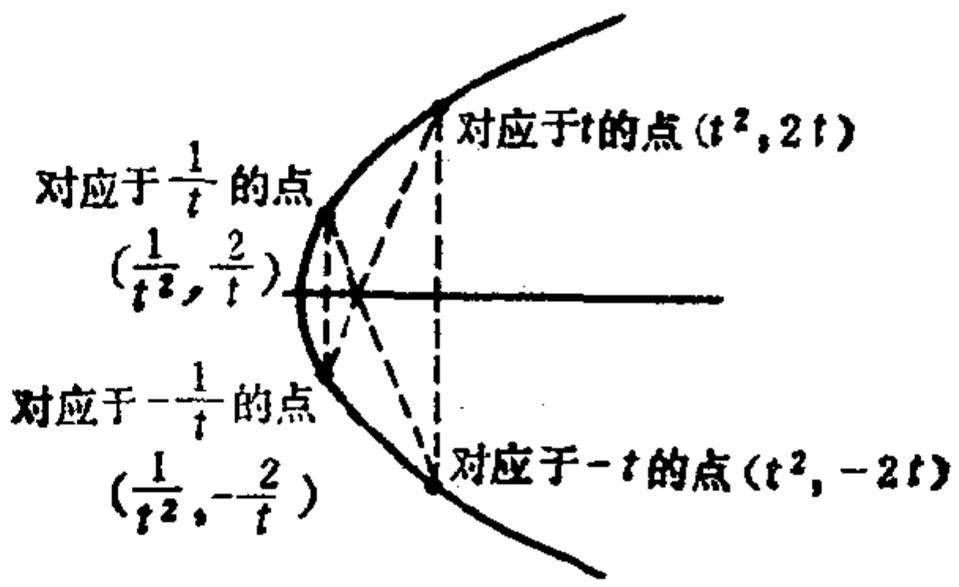
$$y^2=4ax.$$

如果令 x 任取某个实数值 b，将此 b 写作 $b=at^2\ (t\neq 0)$，这是可能的，于是 $y^2=4a^2t^2$. 现在就利用 t 作为参数，看抛物线上的有关的点 $(at^2,2at)$.

不妨取 $a=1$，这时 $y^2=4t^2$，规定

当　　$t>0$ 时，$y>0$，

当　　$t<0$ 时，$y<0$.



于是，例如给定一个 $t>0$，由于 $a=1$，就可得到一个确定的 $b=t^2$，这样，得到对应于给定 t 的点 $(t^2,2t)$. 作出四个函数：

$$e(t)=t,\quad f(t)=\frac{1}{t},$$

$$g(t)=-t,\quad h(t)=-\frac{1}{t}.$$

按照前面所说，这四个函数对代换构成群. 对给定的 t，在抛物线上找出对应于 t 的一个点，即 $(t^2,2t)$，相当于在抛物线 $y^2=4x$ 上给出了函数 $e(t)=t$. 将此点与焦点联结，延长，与抛物线交于另一点即 $\left(\frac{1}{t^2},\frac{-2}{t}\right)$，这一点的参数就是对应第一点的参数的负倒数，相当于在抛物线 $y^2=4x$ 上给出函数 $h(t)$，又如果从此点作轴的

垂线，延长与抛物线交于第三点，即$\left(\frac{1}{t^2}, \frac{2}{t}\right)$；此第三点参数就是对应第一点参数的倒数，相当于给出了 $f(t)$. 至此，第四点 $(t^2, -2t)$也就不难找到了. 给出另一个异于 t 的 t'，又可重复同样的过程，因此有人把例(14)中的群叫做抛物线上的群.

III 其他元素的群

(19) 按模(大于 1 的整数)m 的剩余类的集对剩余类加法构成群，它的元数为 m.

在模 m剩余类$[0], [1], \cdots, [m-1]$的集合中，定义剩余类的加法为它们代表元相加，即

$$[a]+[b]=[a+b].$$

从形式上看，$[a+b]$也是模 m的一个剩余类，好象加法封闭性是成立的. 但这里必须注意，如果当$[a], [b]$的代表元改变时，它们的和也变了，那末封闭性是不是成立呢？因此要求证明当 $a_1 \in [a]$，$b_1 \in [b]$时，$[a_1+b_1]=[a+b]$. 根据剩余类的定义，也就是要证明当 $a_1 \equiv a (\mathrm{mod} m)$，$b_1 \equiv b (\mathrm{mod} m)$时，$a_1+b_1 \equiv a+b (\mathrm{mod}\, m)$. 而这一点在(壹三)中已经证明了. 因此剩余类加法的封闭性成立.

中性元素为$[0]$类.

逆元素也是显然的，因为 $a+(-a)=0$，所以$[a]$的逆元素是$[-a]$或$[m-a]$.

结合律的验证如下：因为

$$([a]+[b])+[c]=[a+b]+[c]=[a+b+c],$$

$$[a]+([b]+[c])=[a]+[b+c]=[a+b+c],$$

所以

$$([a]+[b])+[c]=[a]+([b]+[c]).$$

(20) 一元群

例如，在实数系里数 1 对乘法构成一元群，数 0 对加法构成一

元群.

又如,设有一个集合 Ω,取这个集合与其本身的交得

$$\Omega \cap \Omega = \Omega.$$

如果将取交$\cap$看成运算*，那末上式表明由 Ω 构成的集合$\{\Omega\}$关于$\cap$构成群. 因为封闭性和结合律是显然的,中性元素是Ω 本身,而 Ω 的逆元素也是 Ω 本身. 即$\{\Omega\}$构成一元群.

(21) 仿照例**(12)**用列表法来构造四个元素间运算*的结果.

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

从这个表可以看出:1) 对任意两个元素进行运算的结果都属于这个集合,即

$$ab=c, ba=c, ac=b, cb=a, bc=a, cb=a, ca=b \in \{e, a, b, c\};$$

所以封闭性成立.

2) 结合律显然成立,例如: $(ab)c=c\cdot c=e, a(bc)=a\cdot a=e$;

3) 单位元 e 已在表上说明;

4) 每个元素是它自身的逆元素.

因此 e, a, b, c 对表中规定的运算构成群,而且是可交换的.

这个群叫做克莱因(Klein)四元群.

(22) 置换群　n 阶置换共有$n!$个,这$n!$个 n 阶置换的全体包含了所有可能的 n 阶置换. 这样,两个 n 阶置换

$$\begin{pmatrix} 1 & 2\cdots n \\ a_1 & a_2\cdots a_n \end{pmatrix}, \begin{pmatrix} 1 & 2\cdots n \\ b_1 & b_2\cdots b_n \end{pmatrix}$$

(其中 $a_1, a_2, \cdots, a_n$ 为 $1, 2, \cdots, n$ 中各不相同的一个数，$b_1, b_2, \cdots, b_n$ 也是这样)相乘时结果还是一个 n 阶置换，这在壹中已谈到，所以封闭性成立，

中性元为

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix};$$

一个元$\begin{pmatrix} 1 & 2 \cdots n \\ a_1 & a_2 \cdots a_n \end{pmatrix}$的逆元为$\begin{pmatrix} a_1 & a_2 \cdots a_n \\ 1 & 2 \cdots n \end{pmatrix}$.

结合律成立在(壹四)中已证明过.

所有 $n!$ 个 n 阶置换的全体对置换乘法适合群的四个要求，所以这 $n!$ 个 n 阶置换对置换乘法构成群，它又叫做 n 阶对称群，并记作 S_n.

(23) 交代群 在 $n!$ 个 n 阶置换中，有一半，即 $n!/2$ 个是偶置换，另一半是奇置换. 由偶置换的定义，它是偶数个对换的积，因此，如果有两偶置换，以 a, b 表示:

$$a = \underbrace{(a_1 a_2) \cdots (a_i a_k)}_{2m \text{ 个}}$$

$$b = \underbrace{(b_1 b_2) \cdots (b_j b_k)}_{2l \text{ 个}}$$

$m, l \in N$，因此，

$$ab = \underbrace{(a_1 a_2) \cdots (a_i a_k)\,(b_1 b_2) \cdots (b_j b_k)}_{2m+2l \text{ 个}}$$

$2m+2l$ 为偶数，所以 a, b 的积仍为偶置换，如果相邻两对换可以相消，那末留下的还是偶数个对换，这样，积仍为偶置换，这说明封闭性成立.

中性元是

$$\begin{pmatrix} 1 & 2 \cdots n \\ 1 & 2 \cdots n \end{pmatrix},$$

它可以是0个对换之积，所以是偶置换.

至于存在逆元，只要看一个例子就够了. 设偶置换表示成对换之积为

$$(a_1a_2)(a_3a_4)(a_5a_6)(a_7a_8),$$

那末由(壹二)中的说明可知其逆置换为

$$(a_7a_8)(a_5a_6)(a_3a_4)(a_1a_2),$$

后者同样为偶置换.

由于对置换乘法结合律成立，所以 n 阶偶置换的集对置换乘法满足结合律.

这样，所有 n 阶偶置换的集构成群，它叫做 n 阶交代群，记作 A_n.

例如，三阶交代群 A_3 的元为

$$e,(12)(13),(13)(12).$$

又如四阶交代群 A_4 的 $4!/2=12$ 个元素为

$$e,(12)(13),(13)(12),$$
$$(23)(24),(24)(23),(31)(34),(34)(31),$$
$$(41)(42),(42)(41),(12)(34),(13)(24),(14)(23).$$

(24) 系数为实数，满秩的 $m\times m$ 矩阵(所谓满秩矩阵，就是它的行列式不为零)的集合对矩阵乘法构成群.

1) 封闭性. 设有两个 $m\times m$ 矩阵

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & & a_{mm} \end{pmatrix},\quad B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mm} \end{pmatrix}$$

其中 a_{ij},b_{ij} 是实数，$i,j=1,2,\cdots,m$. 行列式 $|A|,|B|$ 不等于零.

A 乘以 B 的积 AB 为

$$AB=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mm} \end{pmatrix}$$

$$=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mm} \end{pmatrix}=C$$

这里要确定的是 C; 它的元素是

$$c_{ik}=\sum_{j=1}^{m}a_{ij}\cdot b_{jk}=a_{i1}b_{1k}+a_{i2}b_{2k}+\cdots+a_{im}b_{mk},$$

$$i,k=1,2,\cdots,m$$

即矩阵 C 中在第 i 行， k 列的元素等于矩阵 A 中第 i 行的各元素与 B 中第 k 列的对应元素的乘积的和. 可见 c_{ik} 仍为实数. 又因 A,B 都是满秩的，即行列式 $|A|,|B|\neq 0$, 所以 $|C|=|AB|=|A|\cdot|B|\neq 0$，这样 C 也是满秩的，于是封闭性成立. 但一般地 $AB\neq BA$.

2) 中性元为

$$e=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

即对角线上都是 1, 其他的位置上均为 0 的 $m\times m$ 矩阵.

3) 矩阵 A

$$[A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix}$$

的逆矩阵为

$$A^{-1}=\begin{pmatrix} \frac{A_{11}}{D} & \frac{A_{21}}{D} & \cdots & \frac{A_{m1}}{D} \\ \frac{A_{12}}{D} & \frac{A_{22}}{D} & \cdots & \frac{A_{m2}}{D} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \frac{A_{1m}}{D} & \frac{A_{2m}}{D} & \cdots & \frac{A_{mm}}{D} \end{pmatrix}$$

其中D是矩阵A的行列式，由于A为满秩，$D\neq 0$，而A_{ik}则为行列式：

$$A_{ik}=\begin{pmatrix} a_{11} & \cdots & a_{1,k-1} & a_{1k} & \cdots & a_{1,k+1} & \cdots & a_{1m} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{i-1,1} & \cdots & a_{i-1,k-1} & a_{i-1,k} & \cdots & a_{i-1,k+1} & \cdots & a_{i-1,m} \\ 0 & \cdots & 0 & 1 & \cdots & 0 & \cdots & 0 \\ a_{i+1,1} & \cdots & a_{i-1,k-1} & a_{i+1,k} & \cdots & a_{i+1,k+1} & \cdots & a_{i+1,m} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{m,1} & \cdots & a_{m,k-1} & a_{m,k} & \cdots & a_{m,k+1} & \cdots & a_{mm} \end{pmatrix}$$

它叫做a_{ik}的$m-1$阶代数余子式，这样，矩阵A的逆矩阵存在.

4) 结合律可以从矩阵乘法的定义推得. 以3×3矩阵为例

$$\left[\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}\right]\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}$$

$$=\begin{pmatrix} \sum_{i=1}^{3} a_{1i}b_{i1} & \sum_{i=1}^{3} a_{1i}b_{i2} & \sum_{i=1}^{3} a_{1i}b_{i3} \\ \sum_{i=1}^{3} a_{2i}b_{i1} & \sum_{i=1}^{3} a_{2i}b_{i2} & \sum_{i=1}^{3} c_{2i}b_{i3} \\ \sum_{i=1}^{3} a_{3i}b_{i1} & \sum_{i=1}^{3} a_{3i}b_{i2} & \sum_{i=1}^{3} a_{3i}b_{i3} \end{pmatrix}\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}$$

$$=\begin{pmatrix} \sum\limits_{i,j=1}^{3} a_{1i}b_{ij}c_{j1} & \sum\limits_{i,j=1}^{3} a_{1i}b_{ij}c_{j2} & \sum\limits_{i,j=1}^{3} a_{1i}b_{ij}c_{j3} \\ \sum\limits_{i,j=1}^{3} a_{2i}b_{ij}c_{j1} & \sum\limits_{i,j=1}^{3} a_{2i}b_{ij}c_{j2} & \sum\limits_{i,j=1}^{3} a_{2i}b_{ij}c_{j3} \\ \sum\limits_{i,j=1}^{3} a_{3i}b_{ij}c_{j1} & \sum\limits_{i,j=1}^{3} a_{3i}b_{ij}c_{j2} & \sum\limits_{i,j=1}^{3} a_{3i}b_{ij}c_{j3} \end{pmatrix}, \tag{1}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}\left[\begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}\right]$$

$$=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}\begin{pmatrix} \sum\limits_{j=1}^{3} b_{1j}c_{j1} & \sum\limits_{j=1}^{3} b_{1j}c_{j2} & \sum\limits_{j=1}^{3} b_{1j}c_{j3} \\ \sum\limits_{j=1}^{3} b_{2j}c_{j1} & \sum\limits_{j=1}^{3} b_{2j}c_{j2} & \sum\limits_{j=1}^{3} b_{2j}c_{j3} \\ \sum\limits_{j=1}^{3} b_{3j}c_{j1} & \sum\limits_{j=1}^{3} b_{3j}c_{j2} & \sum\limits_{j=1}^{3} b_{3j}c_{j3} \end{pmatrix}$$

$$=\begin{pmatrix} \sum\limits_{i,j=1}^{3} a_{1i}b_{ij}c_{j1} & \sum\limits_{i,j=1}^{3} a_{1i}b_{ij}c_{j2} & \sum\limits_{i,j=1}^{3} a_{1i}b_{ij}c_{j3} \\ \sum\limits_{i,j=1}^{3} a_{2i}b_{ij}c_{j1} & \sum\limits_{i,j=1}^{3} a_{2i}b_{ij}c_{j2} & \sum\limits_{i,j=1}^{3} a_{2i}b_{ij}c_{j3} \\ \sum\limits_{i,j=1}^{3} a_{3i}b_{ij}c_{j1} & \sum\limits_{i,j=1}^{3} a_{3i}b_{ij}c_{j2} & \sum\limits_{i,j=1}^{3} a_{3i}b_{ij}c_{j3} \end{pmatrix}. \tag{2}$$

(1)=(2)，所以对于 3×3 矩阵结合律成立；不难推广到一般情形.

(25) 设 z 为复数，a,b,c,d 为任意实数，且满足行列式 $\begin{vmatrix} a & b \\ c & d \end{vmatrix}=ad-bc\neq0$，则在复数系里，分式线性函数

$$f(z)=\frac{az+b}{cz+d},$$ 当 $c\neq0$ 时；令 $f\left(-\frac{d}{c}\right)=\infty, f(\infty)=\frac{a}{c}$,

这些分式线性函数的全体 L 对代换运算构成群.

现验证如下:设有两个满足上述条件的 f,g:

$$f(z)=\frac{az+b}{cz+d}\in L,$$

$$g(z)=\frac{a'z+b'}{c'z+d'}\in L,$$

以代换运算作为运算,

$$g*f(z)=\frac{a'\dfrac{az+b}{cz+d}+b'}{c'\dfrac{az+b}{cz+d}+d'}$$

$$=\frac{(a'a+cb')z+(a'b+b'd)}{(c'a+cd')z+(c'b+d'd)},$$

这里行列式

$$\begin{vmatrix} a'a+cb' & a'b+b'd \\ c'a+cd' & c'b+d'd \end{vmatrix}$$

就是行列式 $\begin{vmatrix} a & b \\ c & d \end{vmatrix}=(ad-bc)\neq 0$ 与 $\begin{vmatrix} a' & b' \\ c' & d' \end{vmatrix}=(a'd'-b'c')\neq 0$ 的积,所以不等于 0. $g*f$ 同样是分式线性函数,系数亦为实数,且行列式不等于 0,所以封闭性成立.

单位元是 $e(z)=z$.

关于 $f(z)=\dfrac{az+b}{cz+d}$ 的逆元,可以令

$$a'a+cb'=1,\quad a'b+b'd=0$$

$$c'a+cd'=0,\quad c'b+d'd=1.$$

得到

$$a'=\frac{d}{ad-bc},\qquad b'=\frac{-b}{ad-bc},$$

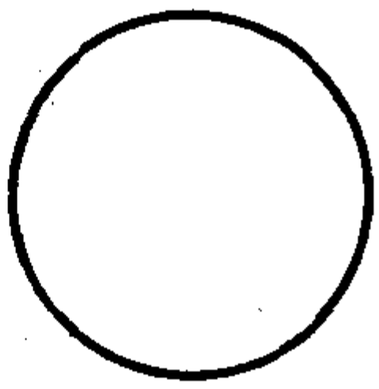
$$c'=\frac{-c}{ad-bc},\qquad d'=\frac{a}{ad-bc}.$$

所以, $f^{-1}(z)=\dfrac{dz-b}{-cz+a}$;再用代换可以验证 $f*f^{-1}=f^{-1}*f$,即每个

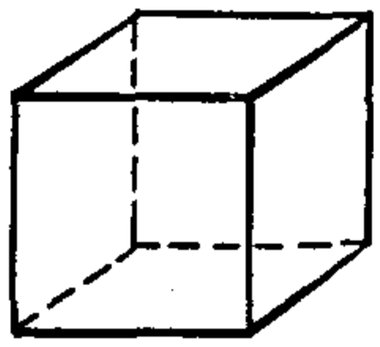
元素 f 的逆元存在.

关于结合律成立，读者不难自己验证.

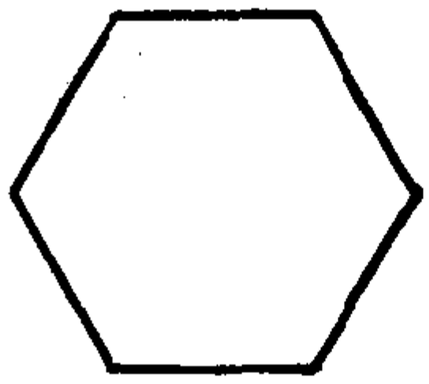
1. 请读者考虑，对下面的图形，如果要求位置不变，有几种运动形式，是否构成群.



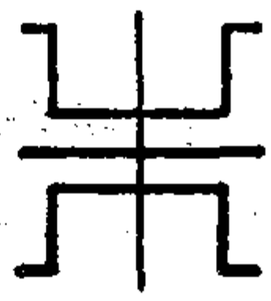
圆



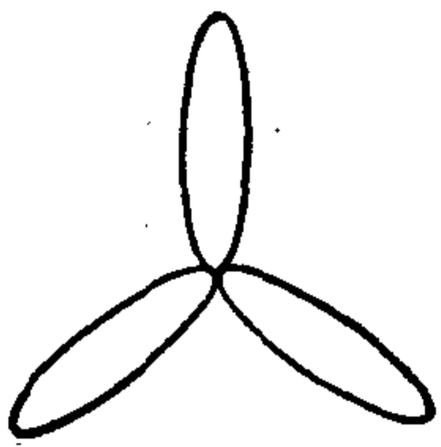
正六面体



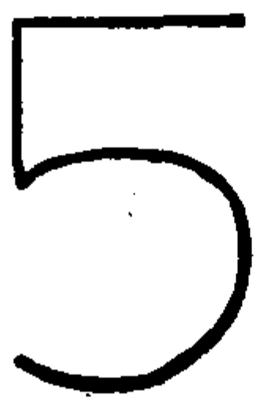
正六边形



寿字对称图形



三叶玫瑰



2. 请读者回头看(壹四)中的Ⅰ，例(3). 那里分别关于直线上 O, O' 两定点取对称 α, β；并将 α, β 看成变换. “接连做”这种手续作为运算$\circ$. 由 α, β 两元素生成无限多个元素：$\alpha, \beta, \alpha\circ\alpha, \beta\circ\beta, \alpha\circ\beta, \beta\circ\alpha, \alpha\circ\beta\circ\alpha, \beta\circ\alpha\circ\beta, \alpha\circ\beta\circ\alpha\circ\beta, \cdots$等等. 它们也是变换. 将此直线上任一定点 A 关于 O, O' 作上述各变换，“接连做”作为运算，试验证，这些元素的集合能否构成一无限的不可交换群？

提示：$\alpha\circ\alpha, \beta\circ\beta$ 均为中性元素 e.

四、两个概念

现在将前面已经遇到的两个概念提出来，阐述一下.

循环群 循环群是这样的群，它的每个元素都是某个固定元

素的某次幂，例如走马灯群的元素就是下列轮换

$$a=\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}$$

的某次幂. $x^3=1$ 的根$1,\omega,\omega^2$的群，它的各元素是元素$\omega=\dfrac{-1+3i}{2}$的某次幂. 在这里我们也可以说循环群是由某一个固定元素生成的.

对于有限循环群来说，它的元素取一定次数的幂又回到原来的元素，通俗的讲可说它的幂是周而复始的，所以有限循环群的每个元素必有一“周期”，设 a 是群的一个任意元，使

$$a^p=e$$

的最小自然数 p 叫做元素 a 的周期. 例如 $x^3=1$ 的根的群，它的元素 ω,ω^2 都有周期 3，又如 e，(123)，(132)这个三阶交代群中，(123)，(132)的周期都为 3. 但并不是每个元素的周期都相同，例如，在走马灯群中，$\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}$的周期为6，而$\begin{pmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{pmatrix}$的周期为 3，等等.

请读者验证(贰三)中例 19 的群，即模 m 剩余类的群，对剩余类加法，是否构成循环群？这里请注意，定义中“元素的幂”要以“元素的倍数”来代替，而中性元是被 m 除余数为 0 的类.

有限群的元素都有周期，因为若无周期，则随着幂指数的增长，元数也增长而无止境，这与有限性相矛盾. 但它与循环群不同，一般的有限群不是由一个元素生成的，例如上节中的克莱因群，尽管它的每个元素都有周期 2，但不是由一个元素生成的，为此要引入生成元这个概念如下.

一个群可以只由若干个元素按规定的代数运算而产生，即所谓生成，这种生成群的元素，叫生成元. 例如(1)克莱因四元素群

可由 a,b 生成，因为 $a^2=b^2=e, ab=c$，也可由 a,c 或 b,c 生成.

(2)三次对称群 S_3: $e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, b=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, d=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, f=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$是由 a,c 生成的，因为 $b=a^2, d=ca, f=ac, e=ab$. (3)整数对加法的群可由数 2,3 生成. 例如，因逆运算是可行的，所以 $3-2=1$，又有 $2+2=4, 2+3=5, \cdots, 2-3=-1$ 等等. (4)有理数对乘法的群可由所有素数生成；等等. 后一例较复杂，但仍然是可验证的，例如，取素数 2,3,5,7,11,…以至无穷无尽的素数，则$\frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}\cdots$存在，$2\cdot\frac{1}{2}=1$存在，$1\times2=2$存在，$2\times\frac{1}{11}=\frac{2}{11}$存在，等等.

交换群 如果群的任意两个元素对代数运算是可交换的，即

$$a*b=b*a \text{ 或 } ab=ba,$$

那末，这样的群就叫做交换群，或阿贝尔群.

2 阶对称群是交换的，因它的元素为

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

所以可交换性是不难验证的. 但 $n\geqslant3$ 时，n 阶对称群就是不可交换的了. 3 阶交代群是可交换的，它的元素是:

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, (123), (132),$$

其可交换性也是可直接验证的. 但 $n\geqslant4$ 时，n 阶交代群 A_n 就是不可交换的了. 因而 n 阶对称群 S_n 当然不可交换. 满秩的 $m\times m$ 矩阵的群对矩阵乘法构成不可交换的群.

请读者验证，前面例子中，还有哪些群是不可交换的.

下面简略地介绍一下群的概念的起源.

早在 18 世纪，拉格朗日(Lagrange)就发现了置换在用根式解高次代数方程中有重要的作用，现代有些学者说他自发地应用了置换群的思想来求代数方程的根式解. 后来经过罗菲(Ruffin)与阿贝尔(Abel)的工作，直到伽罗华(Galois)于 1830 年充分自觉地运用了群的思想来研究代数方程的根式解，并取得了辉煌的成就(这个问题本书最后一节要讲到)，而群这个术语就是由伽罗华首先引进数学的，那段时期主要是研究置换群，因而是有限群，1870 年约当(Jordan)发表了关于置换群的基本著作，详尽地阐述了伽罗华的思想.

另一方面，不依赖于伽罗华的理论，在几何园地里由于出现了多种独立的几何体系：欧几里德几何，罗巴切夫斯基几何，黎曼几何和射影几何，为了研究它们之间的联系与亲缘关系，德国数学家克莱因(Klein)于公元 1872 年在他的著名演说《埃尔兰特纲领》中利用变换群的概念，奠定了几何分类的基础，这是群的概念与理论的第二个来源.

最后，欧拉(Euler)于 1761 年关于除幂所得余数的文章与高斯于 1801 年关于双重二次型的文章，成为群的概念与理论的第三个源泉.

在 19 世纪末，从具体群的研究过渡到抽象群的研究，这时开始认为群的基础性质在于群的运算，而不在于某种具体的元素(如置换等等)，于是各种各样的群就从理论上被统一起来了.

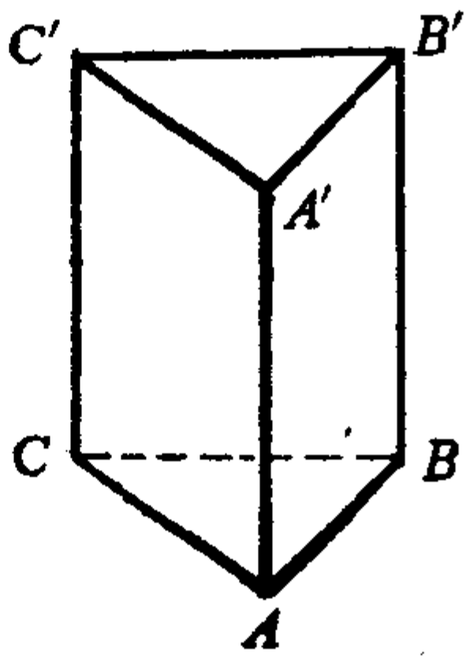
正如本书一开始所讲，现在群论已是数学中的一个很大很活跃的学科，它的应用也极为广泛，不仅在数学本身，如在方程式论，拓扑学，微分方程式论等等方面有许多应用，而且在其他学科，如晶格分类，量子力学等方面也有极其重要的应用.

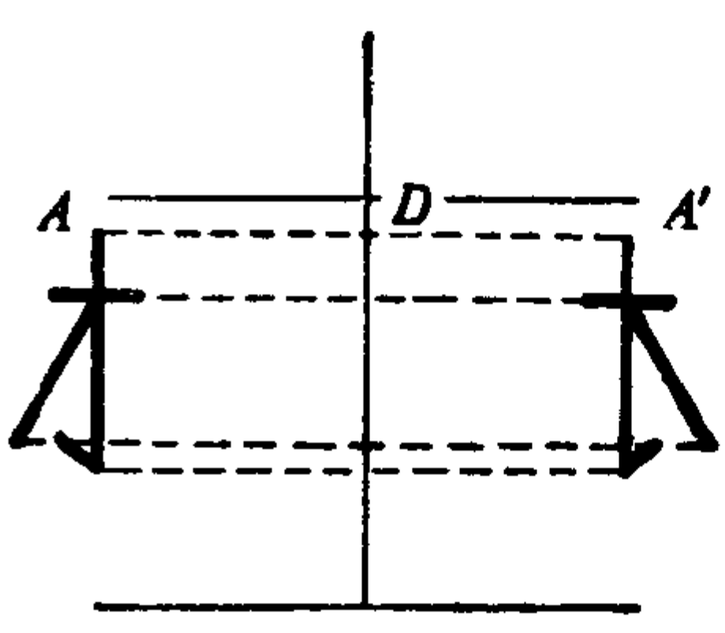
叁

万花筒里的数学

——群的知识的深化

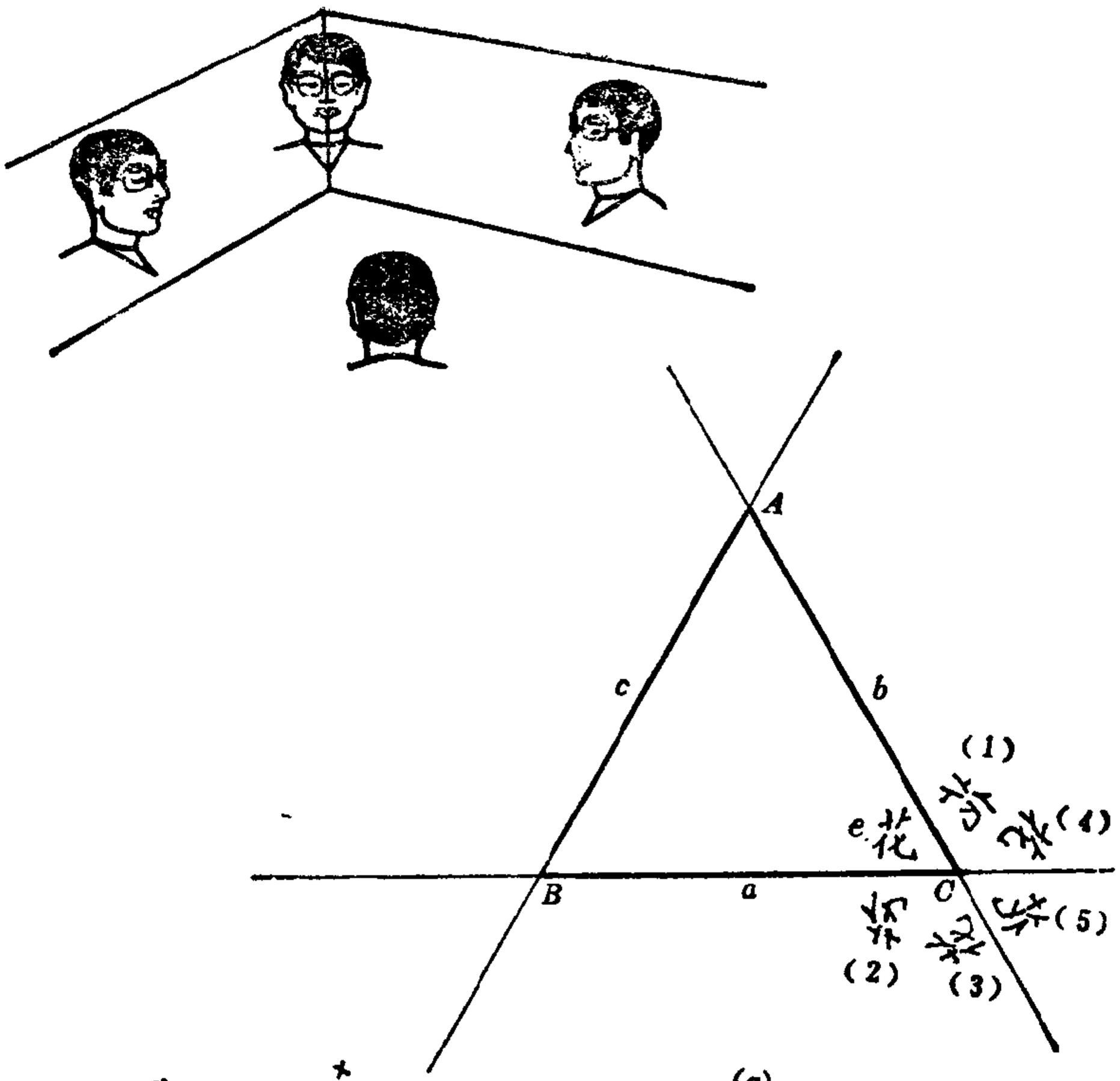
万花筒是少年喜爱的玩具. 它的结构是一个三棱柱，侧面是三块同样大小的长方形反光镜，底面是一块正三角形的毛玻璃，上面放了彩色小玻璃碴(见图). 不停地转动棱柱，从上底往下底看，可看到千变万化的花样，所以人们把它叫做万花筒.



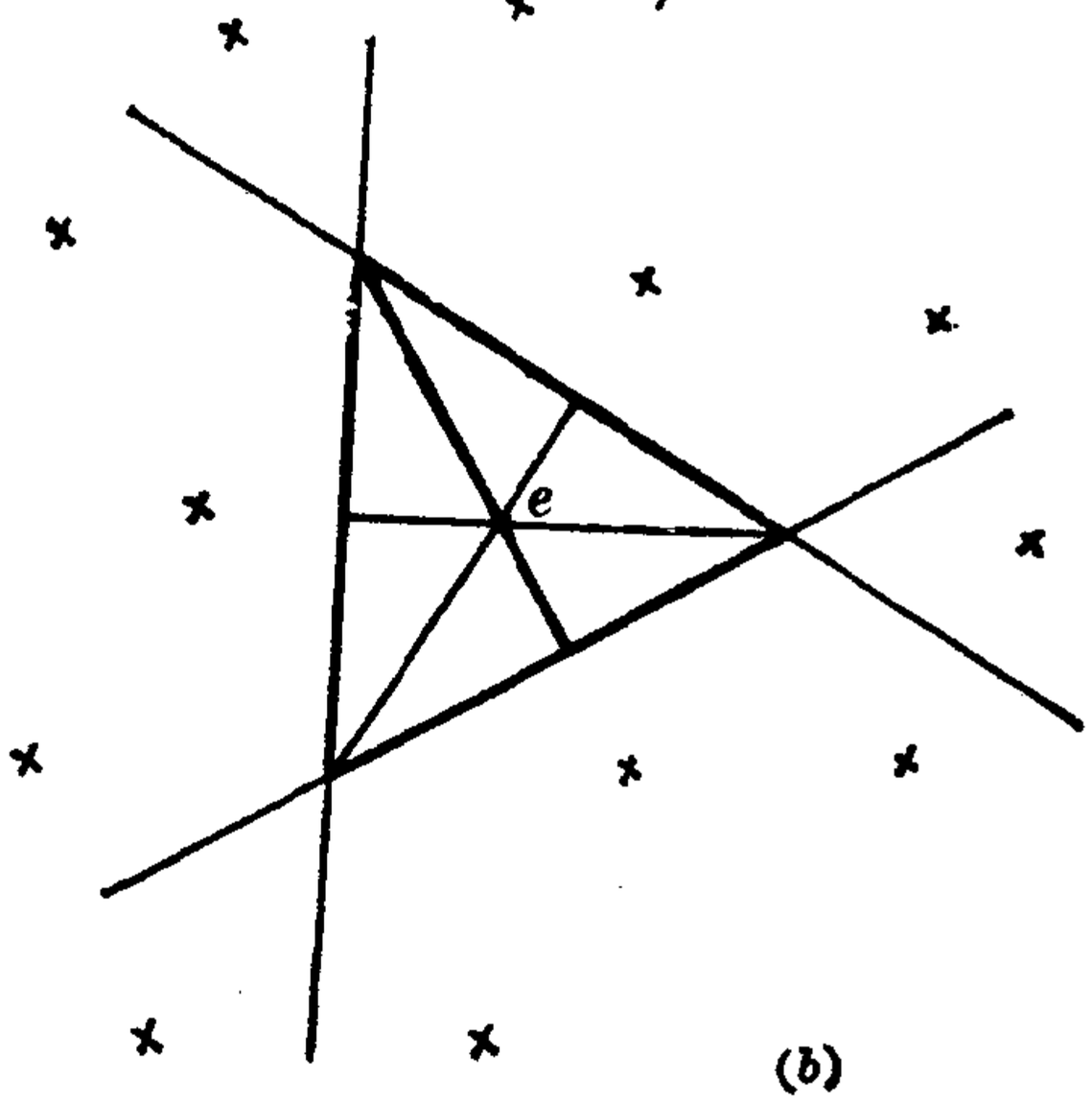


在说明千变万化的花样之所以产生以前，先讲一个与数学和物理有关的概念：镜面反射. 设有一个平面反光镜，垂直地放在水平面上；在镜前放一个图样，例如“才”字，将它的每一点垂直地投射到镜面上，例如A垂直地投射到镜面的D点，延长AD，取$DA'=AD$，那末A'就是A在镜中的象；对其他的点也照此进行，就得到“才”字在镜中的象. 如图所示.

如果将一个东西放在两个平面反光镜之间，例如放在一个角形区域里，那末情况就比刚才所说的要复杂许多，现在来看一个例



(a)



(b)

子. 请看上页第一图，因有了上面的说明，此立体图便一望可知，不须详说了.

现在就来分析万花筒里的数学. 按照实际，万花筒的底部是正三角形，即各个内角为 60°.

上图(*a*)是万花筒镜面反射的示意图. $\triangle ABC$ 是正三角形. a,b,c 是平面反射镜. e 处的“花”是原始实物，其他的“花”或“·”乃是经过镜面反射的象. 但尽管这样，图中的“花”“·”并不能表示象的全部. 我们所关心的是右下方顶点 C 近傍的情景，并对它进行分析.

将原始实物的“花”看作不变的镜面反射的象，即中性元素 e 的象：e(花)＝花. 对镜面 a,b 作反射，这种行为简单地用 a,b 来表示. a 作用于“花”，得 a(花)，即图中的象(2). b 作用于“花”，得 b“花”，即象(1). 对 a(花)再作镜面反射 a：aa(花)，就还原为“花”；同样 bb(花)也还原为“花”. 所以，将 a,b 这两个镜面反射看作元素时，它们的逆元素适合下式

$$aa^{-1}=a^{-1}a=aa=e;\quad bb^{-1}=b^{-1}b=bb=e.$$

将 a(花)作镜面反射 b，ba(花)，它的象是(4). 将 b(花)作镜面反射 a，ab(花)，它的象是(3). (4)与(3) 是不同的象，所以 ab(花)$\neq ba$(花)，即把镜面反射 a,b 看作元素. 镜面反射的连续施行看作运算(看作广义的乘法)

$$ab\neq ba.$$

这说明，这种乘法是不满足交换律的.

从上面的说明可以看到，以镜面反射 a,b 作为元素，由它们可以产生如下全部 6 种元素

$$e,\ a,\ b,\ ab,\ ba,\ aba=bab.$$

后面三个元素的逆元分别是：$(ab)^{-1}=ba$，$(ba)^{-1}=ab$，$(aba)^{-1}=aba=bab$.

结合律成立，请读者自行验证.

这样，在C的附近一隅，上述六个镜面反射作为元素正好形成一个群，它们的象聚集一起如花朵那样.

同时我们看到在这个群里还包含二个较小的群，它们分别是：$\{e,a\}$或$\{e,b\}$.

在$\triangle ABC$中原始实物的位置不同，姿式不同，花的象也就不同. 请看图(b)，在那里实物放在中心，它与图(a)又是一种不同景色. 万花筒底面的小玻璃碴五颜六色，形状各异，形成的象如同群花并艳，繁星点点. 称为万花筒是名不虚传的.

从上面的分析，我们可以给这种群一个外号，叫做万花筒群，想还合适吧！

一、子　　群

在这一章里开始曾说到万花筒里的群；一个小群$\{e, a\}$包含在一个较大的群中，下面就给小群下一个数学定义.

子群　群G的子群B是G的一部分，它对G内定义的代数运算也满足对于群的四项要求.

在(贰二)的例子中：

整数系Z对加法的群，是有理数系Q对加法的群的子群；而Q又是实数系R对加法的群的子群.

去掉零的有理数系$Q'=Q-\{0\}$对乘法的群，是去掉零的实数系$R'=R-\{0\}$对乘法的群的子群.

n阶交代群A_n是n阶对称群S_n的子群.

这里要说明两点：在G的子群B中定义的代数运算要和(母)群G的代数运算是一样的. 其次，群G总有子群，因为，中性元对相应的代数运算构成群，且属于G；G本身属于G，对相应的代数

运算当然构成群. 这是G的两个特殊的子群. 以后谈到子群，一般都是指真子群，即$B\subset G, B\neq\{e\}$. 还要注意，G的中性元与B的中性元是一致的，因为如果B的中性元为e'，那末根据e'的中性，就有

$$e'\cdot e'=e',$$

以e'的逆元e'^{-1}乘上式，得

$$e'\cdot e'\cdot e'^{-1}=e,$$

所以

$$e'=e.$$

这就说明，B的中性元就是G的中性元.

二、群的同态

这是一个很重要的概念，为了很好地理解这个概念，我们先从下面几个例子入手.

例1 设整数系$\cdots,-3,-2,-1,0,1,2,3,\cdots$，在其中定义了加法运算作为代数运算，这样得到整数加法群. 又设有$+1$与-1两个数，在其中定义了乘法作为代数运算，这是二元乘法群. 如果有映射φ，使得：

凡奇数　　对应于　-1

凡偶数　　对应于　$+1$

偶数$+$偶数$=$偶数　对应于　$(+1)\cdot(+1)=+1$

奇数$+$奇数$=$偶数　对应于　$(-1)\cdot(-1)=+1$

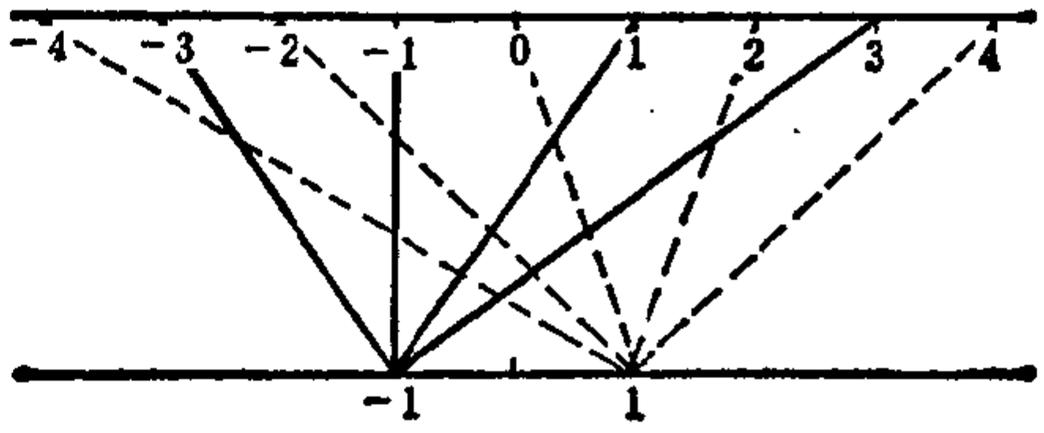
奇数$+$偶数$=$奇数　对应于　$(-1)\cdot(+1)=-1$

偶数$+$奇数$=$奇数　对应于　$(+1)\cdot(-1)=-1$

这就是说，整数系中的每个数，或对应于$+1$，或对应于-1，其次，整数系中任何一对数按照加法结合，它们经过映射φ的象就按照数的乘法结合，结合的结果也满足对应关系. 而且前者的中性元0，对应于后者的中性元1，前者中任意元素的逆元对应

于后者中该元素的象的逆元，例如，$2m(m\in Z)$的逆元为$-2m$对应于$+1$的逆元$+1$；$2m+1$的逆元$-(2m+1)$对应于-1的逆元-1；而且$(2m+1)+[-(2m+1)]=0\longmapsto(-1)\cdot(-1)=+1$.

这是无穷多元对应于一个元的映射，如下图所示：



例2 设有n阶对称群，又有$+1$与-1两个数作成的二元乘法群，还有映射φ，使得

凡偶置换　对应于　$+1$

凡奇置换　对应于　-1

置换乘法以*表示：

偶置换*偶置换＝偶置换　对应于　$(+1)\cdot(+1)=+1$

奇置换*奇置换＝偶置换　对应于　$(-1)\cdot(-1)=+1$

(因为在奇置换*奇置换中，前者对换的个数为奇数，后者对换的个数亦为奇数，在*中对换个数相加，奇数＋奇数＝偶数，即便消去，也是成对的，结果仍为偶数，所以得上面的等式).

偶置换*奇置换＝奇置换　　对应于　　$(+1)\cdot(-1)=-1$,

奇置换*偶置换＝奇置换　　对应于　　$(-1)\cdot(+1)=-1$,

中性元$\begin{pmatrix}1 & 2\cdots n\\ 1 & 2\cdots n\end{pmatrix}$为偶置换　对应于　　$+1$.

偶置换的逆元为偶置换；奇置换的逆元为奇置换(因$(a_1\ a_1')\cdot(b_1\ b_1')(c_1\ c_1')$的逆元为$(c_1\ c_1')(b_1\ b_1')(a_1\ a_1')$)，而它们各自对应的$+1$，$-1$的逆元，正是$+1$，或$-1$自身，这里的$\varphi$是多元对应于一个元的映射.

从上面两个例子我们可以看到一些共同的东西，将它们加以概括，就可以形成一些普遍的要求：

设有群 G，其中的代数运算为$*$，又有群 G'，其中的代数运算为$\circ$，如果存在映射 φ，使对 G 的每个元素 a，有 G' 的一个完全确定的元素 a' 与之对应，并且从

$$\varphi:\ a\to a',\ \ b\to b'$$

可以推得

$$\varphi:\ a*b\to a'\circ b',$$

或写成

$$\varphi(a*b)=\varphi(a)\circ\varphi(b)=a'\circ b',$$

那末，φ 就叫做群 G 到 G' 的同态映射.

由定义和前两个例子看出群的同态是一个映射，而且是一个保持群的运算的映射.

请注意，同态映射并不要求一一对应，例如上面两个例子就是这样.

如果上述同态映射是一一对应的，即除了要满足对同态的要求外，还要求群 G 的一个 a 对应群 G' 的一个且只一个 a'，群 G' 的一个 a' 也对应一个且只一个 a，那末就说 φ 是从群 G 到 G' 的同构映射；而 G 则与 G' 同构.

例如，整数按模 4 的剩余类有四个元，即[0]类(被 4 除，余数为 0)，[1]类(被 4 除，余数为 1)，[2]类(被 4 除，余数为 2)，[3]类(被 4 除，余数为 3). 这四个元对加法构成群 G.

又，$1, i=\sqrt{-1}, i^2=1, i^3=-i\ (i^4=1)$，这四个元素对复数乘法构成循环群 G'. 设 G 到 G' 的映射 φ 为：

$$\begin{aligned}\varphi:\ & 1\to[0]\\ & i\to[1]\\ & i^2\to[2]\\ & i^3\to[3]\end{aligned}$$

φ 是保持运算的，例如

$$\varphi:\ i^2\cdot i^3=i\longrightarrow[2]+[3]=[1],$$

因此 φ 是一个同态，又因 φ 是一一对应的，所以 φ 是同构映射，G 与 G' 为同构.

再如，设关于数的乘法的复数群 $C'=C-\{0\}$，其中元素是 $a+bi$ ($a,b\in R$, a,b 不同时为零). 又 M' 为形如

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

的满秩矩阵的全体，它对于矩阵乘法构成群. 设 C' 到 M' 的映射 φ 为

$$\varphi:\ a+bi\to\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

任意两个复数 $a+bi, c+di$ 相乘，有

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i,$$

它们的象的乘积

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{pmatrix},$$

它恰好是 $(a+bi)(c+di)$ 的象，即

$$\varphi[(a+bi)(c+di)]=\varphi(a+bi)\varphi(c+di).$$

此外，不同的复数对应不同的矩阵，即是一对一的，所以 φ 是同构映射.

同态、同构的概念很重要. 如果 G 与 G' 同构，那末通过同构就可从 G 的一些性质看到 G' 的相应性质. 这就无怪乎苏联的群论学者 Каргаполов 与 Мерзляков 形象地说，同构映射犹如拷贝，同一部小说的不同版本等等.

前面我们讲的是群的同态与同构，对于一般集合，也可以有这些概念，因为后面要用到，现在就来叙述一下. 设 φ 是集合 M 到

M' 的一个映射，在 M 中定义了运算 $*$，在 M' 中定义了运算 $\circ$. 如果对 M 中的任意 a, b，有

$$\varphi(a*b) = \varphi(a) \circ \varphi(b),$$

则称 φ 是 M 到 M' 的一个同态.

由此不难叙述从集合 M 到集合 M' 的同构映射，这时只要附加映射是一一对应的即可.

请读者说明:

(1) 贰三中，小鼓三脚活动架之下三脚落点与上三支撑点之间有同构关系. (下三脚落点的正三角形对保持平面位置的运动作成群，已作了说明. 对上三支撑点的正三角形也作相似的处理).

(2) 把取常用对数看作从 R^+ 到 R 的映射 φ

$$\varphi:\ a \to \log a,\ \ \forall a \in R^+$$

对于 $x, y \in R^+$，则

$$\log(xy) = \log x + \log y.$$

请说明这是一同构映射.

三、再谈群的同态

从同态的概念可以引出不少新问题，现在来介绍一些主要的.

(1) 将群 G 同态地映射(φ)到群 G'，则 G 的中性元对应于 G' 的中性元，G 的每个元的逆元对应于 G' 的相应元的逆元.

实际上，设 e 为 G 的中性元，$x \in G$，那末

$$\varphi(e*x) = \varphi(x) = \varphi(e) \circ \varphi(x)$$

按照同态要求，$\varphi(e), \varphi(x) \in G'$；设 G' 的中性元为 e'，那末

$$e' \circ \varphi(x) = \varphi(x).$$

将上下两式对比就可知 $\varphi(e) = e'$.

同理

$$\varphi(x^{-1}*x)=\varphi(e)=\varphi(x^{-1})\circ\varphi(x).$$

而 $\varphi(e)$为 G' 的中性元，所以 $\varphi(x^{-1})$为 $\varphi(x)$的逆元. 例如(贰二)中例二之单位置换对应群{−1，1}中的 1，奇置换的逆元为奇置换，对应于−1 的逆元 −1.

(2) 如果群 G(代数运算为$*$)同态地映射(φ)到具有代数运算$\circ$的集合 G' 上，即 G' 的每个元素都是G 的元素的同态象，那末 G' 也是一个群. 这是因为

对于 $a',b'\in G'$，由假设存在 $a,b\in G$，使 $\varphi(a)=a'$，$\varphi(b)=b'$. 按照集合间同态的要求，

$$\varphi(a*b)=\varphi(a)\circ\varphi(b)=a'\circ b',$$

因$a*b\in G$，所以$a'\circ b'\in G'$，即封闭性成立.

其次，设 e 是G 的中性元，则 $\varphi(e)=e'$ 是 G' 的中性元. 因为对于任意 $a'\in G$，由假设存在 $a\in G$，使 $\varphi(a)=a'$，再由同态要求，

$$a'=\varphi(a)=\varphi(e*a)=\varphi(e)\circ\varphi(a)=\varphi(e)\circ a'.$$

再有，$a'\in G$ 的逆元是 $\varphi(a^{-1})$. 因为

$$e'=\varphi(a*a^{-1})=\varphi(a)\circ\varphi(a^{-1})=a'\circ\varphi(a^{-1}).$$

最后验证结合律成立.

设 $a',b',c'\in G'$，它们分别是 $a,b,c\in G$ 的象，即 $\varphi(a)=a'$，$\varphi(b)=b'$，$\varphi(c)=c'$. 因为 φ 是同态，所以

$$(a*b)*c\to\varphi(a*b)\circ\varphi(c)=(\varphi(a)\circ\varphi(b))\circ\varphi(c)=(a'\circ b')\circ c'$$

$$a*(b*c)\to\varphi(a)\circ\varphi(b*c)=\varphi(a)\circ(\varphi(b)\circ\varphi(c))=a'\circ(b'\circ c')$$

由于G 中结合律成立，$(a*b)*c=a*(b*c)$，所以同态象也相等，即

$$(a'\circ b')\circ c'=a'(b'\circ c').$$

因而 G' 构成群. (贰二)中例 1 可以作为这个论断的例子.

读者可以验证，在同态映射下，可交换性也是保持的，但有些性质可能消失，这就是前面提到的苏联群论学者 Кapраполов 和 Мерзляков 说的，同态犹如记忆，重要的记住了，细节忘了，见后

面换位子群一节中的说明.

(3) 一个群G同态地映射(φ)到群G', G中与G'的中性元相对应的所有元的集N,叫做在同态映射φ下G的核,它构成群G的子群.

这是因为设a,b是N的任意两个元素,那末根据同态的要求,

$$\varphi(a*b)=\varphi(a)\circ\varphi(b)=e'\circ e'=e',$$

这里e'是G'的中性元.上式表明$a*b$属于N,即封闭性成立.又,

$$e'=\varphi(a*a^{-1})=\varphi(a)\circ\varphi(a^{-1})=e'\circ\varphi(a^{-1}),$$

所以$\varphi(a^{-1})=e'$,即a的逆元a^{-1}属于N. 所以N构成G的子群.

例如,我们在满秩的2×2实矩阵全体

$$M_2=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle|\ a,b,c,d\in R, ad-bc\neq0\right\}$$

关于矩阵乘法的群和实数集$R'=R-\{0\}$间建立一个映射φ,使

$$\varphi:\ \begin{pmatrix}a & b\\ c & d\end{pmatrix}\to\begin{vmatrix}a & b\\ c & d\end{vmatrix},$$

即把$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$对应于一个非零实数. 根据(貳)中关于满秩$m\times m$矩阵对乘法构成群的说明,这个映射是一个同态. 这样,对应于行列式为1的所有2×2矩阵

$$\begin{pmatrix}x & y\\ z & w\end{pmatrix}$$

($xw-yz=1$)就是这个群的核.

显然这个核构成群. 因为,设核的两个元是

$$A=\begin{pmatrix}x & y\\ z & w\end{pmatrix},\qquad B=\begin{pmatrix}u, & v\\ s, & t\end{pmatrix}$$

那末与AB(矩阵之积)对应的实数是相应行列式的积$|A|\cdot|B|$,它的值$1\cdot1=1$, 所以AB属于核,其他的要求也是不难验证的.

(4) --个有限的 n 元群必然同构于 n 阶对称群的一个子群.

现在证明这个论断如下:

假设 n 元有限群 G 的 n 个不同元素原始排列成下面的式样:

$$x_1,\ x_2,\ \cdots,\ x_n,$$

并且认定这种排列相当于足标数字原始排列 $1,2,\cdots,n$, 这是按自然数次序的排列.

用 $x_1,x_2,\cdots,x_n$ 中任意一个元素, 例如用 x_i, 逐个从右边乘 $x_1,x_2,\cdots,x_n$, 得 $x_1x_i,x_2x_i,\cdots,x_nx_i$. 由于 $x_1,x_2,\cdots,x_i,\ \cdots,\ x_n$ 都是 G 的元, 所以 $x_1x_i,x_2x_i,\cdots,x_nx_i$ 必然属于 G, 并且它们互不相同, 因为, 否则, 例如 $x_1x_i=x_2x_i$, 两端右乘 x_i^{-1}, 则 $x_1=x_2$, 这与原假设矛盾. 这样, $x_1x_i,x_2x_i,\cdots,x_nx_i$ 就是 $x_1,x_2,\cdots,x_n$ 的一个重新排列. 于是可以说 x_i 所对应的置换为:

$$\begin{pmatrix} x_1 & \cdots & x_n \\ x_1x_i & \cdots & x_nx_i \end{pmatrix},$$

写作

$$\varphi:\ x_i\to\begin{pmatrix} x_1 & \cdots & x_n \\ x_1x_i & \cdots & x_nx_i \end{pmatrix}. \tag{1}$$

同理

$$x_j\to\begin{pmatrix} x_1 & \cdots & x_n \\ x_1x_j & \cdots & x_nx_j \end{pmatrix}, \tag{2}$$

$$x_ix_j\to\begin{pmatrix} x_1 & \cdots & x_n \\ x_1x_ix_j & \cdots & x_nx_ix_j \end{pmatrix}, \tag{3}$$

为了证明本定理, 须要证明群 $G=\{x_1,\cdots,x_n\}$ 与上述置换的集 B 同构, 从而 B 是 n 阶对称群 S_n 的一个子群.

现证明

$$\varphi(x_ix_j)=\varphi(x_i)\varphi(x_j),$$

且为一同构.

事实上, 在(1)的置换中 x_1 换为 x_1x_i. 在(2)的置换之上行中

找 x_1x_i，这必然存在，因为 x_1x_i 是 $x_1,\cdots,x_n$ 中的一个元素(群的封闭性)，(2)的置换的下行所对应的就是 $x_1x_ix_j$，它也是 $x_1,\cdots,x_n$ 中的某个元素. 于是 x_1 换为 $x_1x_ix_j$. 这种手续实际就是(1)，(2)中置换相乘的一个步骤，它对应着(3)的置换的第一列. 依此逐个进行下去，就得到(3). 于是，在(1)，(2)，(3)的条件下

$$\varphi(x_ix_j)=\begin{pmatrix} x_1 & \cdots & x_n \\ x_1x_ix_j & \cdots & x_nx_ix_j \end{pmatrix}=\varphi(x_i)\varphi(x_j)$$

$$=\begin{pmatrix} x_1 & \cdots & x_n \\ x_1x_i & \cdots & x_nx_i \end{pmatrix}\begin{pmatrix} x_1 & \cdots & x_n \\ x_1x_j & \cdots & x_nx_j \end{pmatrix},$$

于是，φ 是同态.

G 的单位元对应于$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}$；$x_i^{-1}$ 对应于

$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_1x_i & x_2x_i & \cdots & x_nx_i \end{pmatrix}$的逆，这显然存在. 至于结合律也是显然的，$B$ 的封闭性由 G 的封闭性推得，所以 B 是 S_n 的一个子群.

不难看出，不同的 x_i 对应不同的置换，反之也一样，所以它又是同构.

以前面讲到的克莱因群为例，来看它所对应的置换的群，令

$$e=x_1,\quad a=x_2,\quad b=x_3,\quad c=x_4.$$

以中性元右乘所有四个元素，得

$$e,\quad a,\quad b,\quad c$$

对应的置换为

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

以 a 右乘所有四个元素得

$$a,\quad a\cdot a=e,\quad b\cdot a=c,\quad c\cdot a=b.$$

所对应的置换为

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

以 b 右乘原始排列的四个元素，得 c，b，a，e，所对应的置换为

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

最后用 c 右乘 e，a，b，c 得 c，b，a，e，所对应的置换为

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

这样克莱因群所对应的置换的群的元为

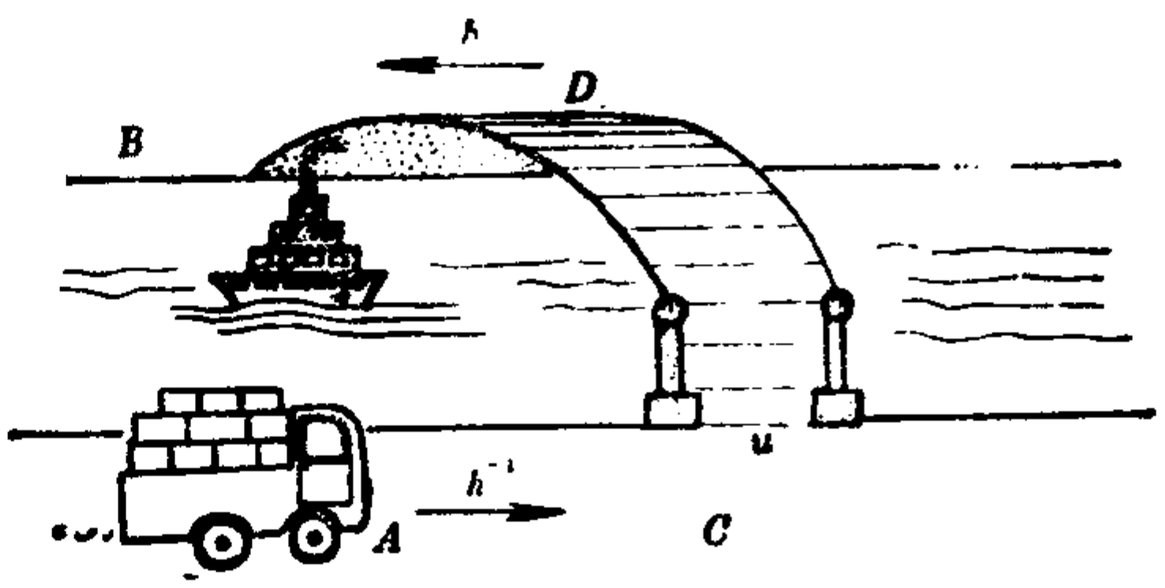
$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\ \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},$$

它是 4 阶对称群的一个子群.

读者试做与 $1,\omega,\omega^2$ 相对应的置换的群.

四、共轭、共轭元素

先来看一个实际的事例.



设有一条河，C、D 两点间建有公路桥；A、B两点间设有大驳船. 一运货汽车从 A 到 B 有二种选择，一种走水路，路途较近，但

等船花费时间，且上下船麻烦；另一种走陆路，从 A 到 C，在 C 过桥到 D，最后到 B，路远，但直接，费时也不多．设从 A 到 C 走陆路的动作记作 h^{-1}，从 C 到 D 过桥记作 u，再从 D 到 B 走陆路，记作 h（从 $A\to C$ 与从 $C\to D$，距离一样，但方向相反）．如果从 A 到 B 渡船的动作记作 s，那末，从效果看

$$h^{-1}uh=s.$$

类似的现象，请读者自己思索，现在来谈一个与此相象的数学概念，即共轭概念．

设有群 G，所谓 G 的一个元素 y 共轭于 $x\in G$，是指存在一个元素 $a\in G$，使得

$$y=a^{-1}xa,$$

有时也将此说成：用 a 将 x 变形．

现在来看两个例子．

例 1　在 4 阶对称群中，置换

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

与置换

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

共轭．因为可以找到

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

使得

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

例 2　满秩的 2×2 矩阵

$$\begin{pmatrix}19&24\\-11&-14\end{pmatrix}$$

与矩阵

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

共轭，因为可找到

$$a=\begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix},$$

使得

$$\begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}=\begin{pmatrix} 19 & 24 \\ -11 & -14 \end{pmatrix},$$

这里

$$\begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}^{-1}=\begin{pmatrix} -3 & 2 \\ \frac{5}{2} & -\frac{3}{2} \end{pmatrix}.$$

可以看出，当 y 与 x 共轭时，x 与 y 共轭，因为由 $y=x^{-1}xa$，得

$$x=aya^{-1},$$

或写作

$$x=(a^{-1})^{-1}y(a^{-1}).$$

例如在例 2 中，

$$\begin{pmatrix} 19 & 24 \\ -11 & -14 \end{pmatrix} \text{ 与 } \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

共轭时，后者也与前者共轭，这时只需将 a 等于

$$\begin{pmatrix} -3 & 2 \\ \frac{5}{2} & -\frac{3}{2} \end{pmatrix}$$

a^{-1} 等于 $\begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}$即可.

从共轭的定义与上面两个例子可以看到：

(1) x 与自己共轭，这是因为 $e^{-1}x\ e=x$.

(2) y 共轭于 x 时，x 也共轭于y，这在上面已经说明了.

(3) 如果 x 与 y 共轭，y 与 z 共轭，那末 x 与 z 共轭，事实上：

$$a^{-1}ya=x,$$

$$b^{-1}zb=y,$$

以后式代入前式，得

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

根据结合律：

$$a^{-1}b^{-1}zba=x$$

即

$$(ba)^{-1}z(ba)=x$$

这里 $a^{-1}b^{-1}=(ba)^{-1}$，因为 $ba(a^{-1}b^{-1})=baa^{-1}b^{-1}=e$.

还要注意，二元素之积 ab, ba 共轭，因为，

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

e 是一很特殊的元素，它只与自己共轭，因为对任何 a，都有 $a^{-1}ea=e$.

最后，与 x 共轭的元素 z，有与 x 相同的周期. 这是因为，如果 x 的周期为 p，那末，由于

$$a^{-1}xa=z,\quad x^p=e,$$

取 z 的 p 次幂，则

$$(a^{-1}xa)^p=z^p,$$

$$\underbrace{a^{-1}xa}\cdot\underbrace{a^{-1}xa}\cdot\underbrace{a^{-1}xa}\cdots\underbrace{a^{-1}xa}=z^p,$$

$$a^{-1}\cdot\underbrace{x\cdot x\cdots x}_{p\text{个}}a=z^p,$$

即

$$a^{-1}x^pa=z^p,$$

$$a^{-1}ea=z^p \qquad e=z^p$$

这表示 z 的周期$\leqslant p$. 如果 z 的周期为 $p_1<p$，则

$$(a^{-1}xa)^{p_1}=z^{p_1},$$

$$a^{-1}x^{p_1}a=e,$$

$$x^{p_1}=aea^{-1}=e.$$

这不可能，因 $p_1<p$，x^{p_1} 不能等于 e. 所以 $p_1=p$. 即 z 的周期也是 p，但逆命题不成立，即是说，周期相同的两个元素并不一定共轭.

于是，把相互共轭的元素归并到一起，就组成一类，叫做共轭元素系，因而在一个群 G 中，就按照共轭的关系划分成各个共轭元素系. 同一个系中的元素相互共轭，不同系的元素互不共轭，所以各个不同的共轭元素系之间没有共同的元素. 以 K_0，K_1，…，K_i 表示各个不同的共轭元素系：以 $k_0, k_1, \cdots, k_i$ 表示各个系的元素的个数，在有限的情形，以 n 表示 G 的元数，那末

$$n=k_0+k_1+\cdots+k_i.$$

有一类特殊的共轭元素系. 它的元素与群 G 中任何一个元素都可交换，即设 x 为这样的元素，$\forall a\in G$，有

$$ax=xa,$$

或
$$a^{-1}xa=x.$$

这样的 x 叫做 G 中的中心元或不变元，即是说，用 G 中的任意元素将 x 变形时，结果等于它自己. 这种中心元总是存在的，例如 e 就与任何元素 x 可交换. 一中心元单独组成共轭系. e 就单独组成共轭系. 这是特殊的共轭系.

群 G 中所有中心元的集合 I 叫做 G 的中心，以后将证明 I 是 G 的一个子群.

五、找共轭元素的一种方法

共轭这个概念很重要，在这里对有限群的情形谈谈找共轭元素的一种方法，前面讲到群的图表表示法，在我们所说的方法中可以利用这个方法.

假设群G按照下表所示的办法运算（列的元素左乘行的元素）：

列/行	e	a	b	c	…	x	y	z
e								
a								
b								u
c								
…								
x								u
y								
z								

列中的一个元素x与行中的一个元素b结合，得u，即$xb=u$。再从列中查b，从b向右看，寻找有无与b结合得u的，结果在c垂直向下有u，即$bc=u$，因而

$$xb=bc,$$

所以$b^{-1}xb=c$，这表示x与c共轭.

这种利用群的乘法表找共轭元素的方法，是比较方便的．再有，前面说过共轭的元素有相同的周期，因此周期不同的元素必然不共轭，但周期相同的元素也并不一定共轭，还要进一步检验.

根据上述原则，我们来求正四面体运动群的共轭系．在正四面体运动的群里，h类型元素的周期为3，m类型的元素的周期为2，所以h类型的元素与m类型的元素肯定不共轭，但h类型的各元素可能共轭，m类型的元素也可能共轭，经过检验，得下表：

$h_1m_2=m_2h_3$	$m_2^{-1}h_1m_2=h_3$,
$h_1m_3=m_3h_4$	$m_3^{-1}h_1m_3=h_4$,
$h_3m_1=m_1h_4$	$m_1^{-1}h_3m_1=h_4$,
$h_2m_3=m_3h_3$	$m_3^{-1}h_2m_3=h_3$,
$h_2m_2=m_2h_4$	$m_2^{-1}h_2m_2=h_4$
……	……

$$m_1h_1=h_1m_2 \qquad h_1^{-1}m_1h_1=m_2,$$
$$m_2h_1^2=h_1^2m_1 \qquad (h^2)^{-1}m_2h_1^2=m_1,$$
$$m_3h_1=h_1m_1 \qquad h_1^{-1}m_3h_1=m_1,$$
$$m_2h_1=h_1m_3 \qquad h_1^{-1}m_2h_1=m_3,$$
$$\cdots\cdots \qquad \cdots\cdots$$
$$h_1^2m_1=m_1h_2^2 \qquad m_1^{-1}h_1^2m_1=h_2^2,$$
$$h_1^2m_2=m_2h_3^2 \qquad m_2^{-1}h_1^2m_2=h_3^2,$$
$$h_1^2m_3=m_3h_4^2 \qquad m_3^{-1}h_1^2m_3=h_4^2,$$
$$h_2^2m_3=m_3h_3^2 \qquad m_3^{-1}h_2^2m_3=h_3^2,$$
$$h_3^2m_1=m_1h_4^2 \qquad m_1^{-1}h_3^2m_1=h_4^2,$$

这说明，h^1 类型各元素相互共轭；h^2 类型各元素相互共轭；m 类型各元素也相互共轭，m 类型各元素与 h 类型各元素或 h^2 类型各元素均不共轭，因周期明显地不同，但 h 类型元素与 h^2 类型元素尽管周期相同，也不共轭.

于是，正四面体运动的群便划分成下面的四个共轭系：

$$e;\{m_1,m_2,m_3\},\{h_1,h_2,h_3,h_4\},\ \{h_1^2,h_2^2,h_3^2,h_4^2\}.$$

在这种分法中，上面关于元数的公式成立：

$$n=1+3+4+4.$$

由这个结果还可看到，各个共轭系的元数恰是群 G 的元数的因数，在本例中：

$$n=12=1\cdot3\cdot4.$$

六、共 轭 子 群

先回顾一下(贰二)中讲到的群的子集（元数为有限的）的积 AB，当 A(或 B)只含一个元素 a(或 b)时，

$$AB=aB=\{ab_1,ab_2,\cdots,ab_m\},BA=Ba=\{b_1a,b_2a,\cdots,b_ma\}.$$

现在来看群G的子群B. 设B的各个不同的元素为

$$a_1, a_2, \cdots, a_m.$$

用G的元素将B变形: $g^{-1}Bg$, 就是用g将各个a_i变形为

$$g^{-1}a_1g, g^{-1}a_2g, \cdots, g^{-1}a_mg.$$

将经此变形后的各元素的集合记作$K=g^{-1}Bg$.

读者可以验证, 当$i\neq j$时, $g^{-1}a_ig\neq g^{-1}a_jg$, 而且$K$是群$G$的一个子群. 因为设$g^{-1}a_1g, g^{-1}a_2g\in K$, 则

$$(g^{-1}a_1g)(g^{-1}a_2g)=g^{-1}a_1gg^{-1}a_2g=g^{-1}a_1a_2g,$$

因为$a_1a_2\in B$, 所以$g^{-1}a_1a_2g\in K$. 另外K中$g^{-1}a_1g$的逆元求法如下:

$$(g^{-1}a_1g)(g^{-1}xg)=e,$$

$$g^{-1}a_1xg=e,$$

因e只与自己共轭, 所以$a_1x=e, x=a_1^{-1}$.

即$g^{-1}a_1^{-1}g$为$g^{-1}a_1g$的逆元. 所以K构成子群.

从上面所说, 我们可以定义共轭子群如下: 所谓子群B共轭于子群K, 是指存在G的元素g, 使

$$g^{-1}Bg=K.$$

如果两个子群B与K是共轭的, 那末它们的元数相等.

设有群G的子群H, 如果对于所有的$g\in G$, H满足以下的条件:

$$g^{-1}Hg=H, \text{或 } Hg=gH,$$

即H与它自身共轭, 那末这样的子群H叫做G的正规子群. 由此可见与正规子群共轭的子群, 与此正规子群等同. 即正规子群与自己共轭.

请注意, 在正规子群H中, $gH=Hg$这个表达式只说明, 对任何的$g\in G$, 有$h_1, h_2\in H$, 使得

$$gh_1=h_2g,$$

但并不要求$h_1=h_2$.

现在不难证明群G的中心I构成G的子群，且为正规子群了.

因为，设$a_1, a_2 \in I, x \in G$

$$a_1 x = x a_1, a_2 x = x a_2,$$

$$a_1 a_2 x = a_1 x a_2 = x a_1 a_2,$$

这说明$a_1 a_2 \in I$.

任意的$a \in I$的逆元a^{-1}也属于I. 因为从$ax = xa$推出 $x = a^{-1}xa$，从后者又可推出$xa^{-1} = a^{-1}x$，这说明a^{-1}也是中心元.

所以中心I是G的一个子群，且从$a = x^{-1}ax$， $a \in I$, $x \in G$可看出，I是正规子群. 但正规子群并不一定是中心.

例如，在系数为实数的满秩$n \times n$矩阵乘法群G中，形如

$$\begin{pmatrix} a & & & 0 \\ & a & & \\ & & a & \\ 0 & & & \ddots \\ & & & & a \end{pmatrix}$$

的矩阵，即主对角线上的元素均为任意的同一个实数$a \neq 0$，其它的元素都是零的矩阵的集合，是G的中心. 显然中心愈大，与其他元素可交换的元素愈多，反之则愈少，最小的中心是只由中性元素组成的群，这样的群只有e可以和其他元素交换. 如果$I = G$，那么G就成交换群了，它是G中最大的中心.

如果我们所处理的是同态映射的核，即前面提到的子群N，那末设$g \in G$，便有

$$g^{-1} N g = N.$$

这是因为，根据同态映射的要求，在同态φ下，$\forall a \in N$，对任意的$g \in G$，

$$\begin{aligned} \varphi(g^{-1}ag) = \varphi(g^{-1})\varphi(ag) &= \varphi(g^{-1})\varphi(a)\varphi(g) \\ &= \varphi(g^{-1})e'\varphi(g) \\ &= \varphi(g^{-1})\varphi(g) = e', \end{aligned}$$

所以$g^{-1}ag \in N$. 因为a为任意的，便有

$$g^{-1}Ng\subset N,\text{即}\quad Ng\subset gN. \tag{1}$$

但由于 g 是任意的，所以对同一个 g，下式

$$(g^{-1})^{-1}N(g^{-1})=gNg^{-1}\subset N$$

也成立，这就是说

$$gN\subset Ng. \tag{2}$$

结合(1),(2)得

$$gN=Ng,$$

即

$$N=g^{-1}Ng.$$

这表明同态映射 φ 下的核是正规子群.

正规子群是一个很重要的概念，现在再来看几个例子

1) n 阶对称群 $S_n(n\neq 4)$ 含有唯一的真($\neq S_n$, $\{e\}$)正规子群，它是 n 阶交代群 A_n.

2) 在 4 阶交代群 A_4 中，下列四个元素

$$e,(12)(34),(13)(24),(14)(23)$$

构成 A_4 的正规子群，它们就是(贰三)中例(17)之正四面体运动中绕对棱中点联线转 180° 的运动.

3) 可交换的加法群的子群，可交换的乘法群的子群都是正规子群.

4) 满秩的 2×2 矩阵，

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

其系数为实数，对矩阵乘法构成群 G. 其中行列式 $\begin{vmatrix} e & f \\ g & h \end{vmatrix}=1$ 的所有 2×2 矩阵是其正规子群 N.

这是因为，设 x，y 是这样的两个矩阵，即末行列式 $|xy|=|x|\cdot|y|=1\cdot 1=1$.

又设 $g\in G$，则 $|g^{-1}xg|=|g^{-1}|\cdot|x|\cdot|g|=|g^{-1}||g||x|=1\cdot 1=1$. 所以 $g^{-1}xg\in N$，而 $x\in N$ 为任意的，即

$$g^{-1}Ng=N.$$

七、群 G 按子群 B 划分为陪集系

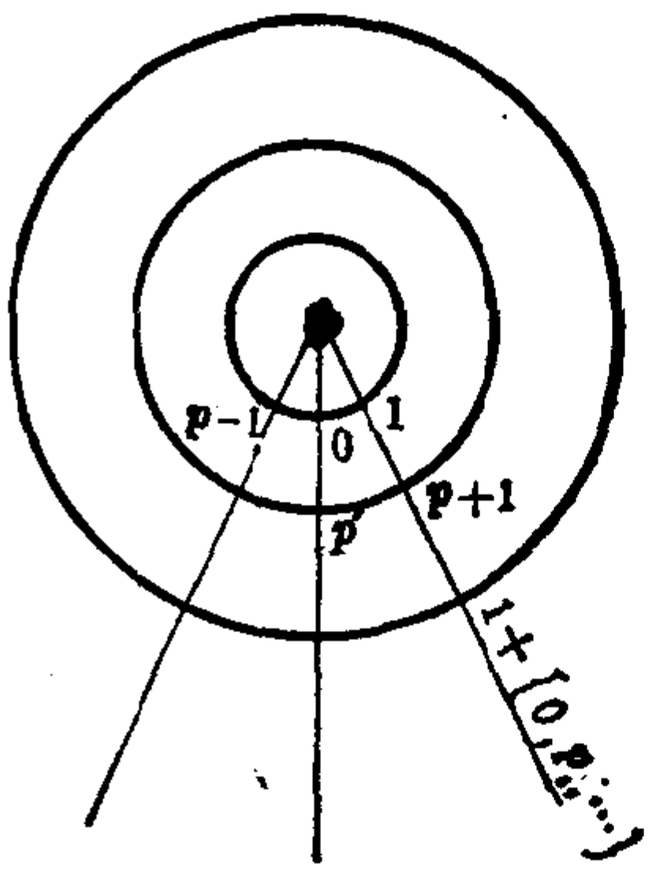
现在来看一个与日常生活相似的现象.

已知整数系 Z 对加法构成群. Z 对某一素数 $p>2$ 分成剩余类:

$$[0]:\ (\cdots -2p,-p,0,p,2p,\cdots).$$
$$[1]:\ (\cdots -2p+1,-p+1,1,p+1,2p+1,\cdots),$$
$$[2]:\ (\cdots -2p+1,-p+2,2,p+2,2p+2,\cdots),$$
$$\cdots$$
$$[p-1]:\ (\cdots -1,p-1,2p-1,\cdots).$$

从[0]到[$p-1$]各类中抽出一个代表，例如，$0,1,2,\cdots,p-1$.

现在假设开一个圆桌会议，共 $p(>2)$ 个席位，由于 $p(>2)$ 为素数，当然为奇数. 各个剩余类派代表参加，它们假设就是 $0,1,\cdots,p-1$. 代表到齐就坐，[0]类是一个群坐主位；其他各剩余类依次反时针方向坐在 $1,2,\cdots,p-1$ 位，这样就犹如 0 为主席，其他的为陪席一样.



下面就讲群 G 按子群 B 划分为陪集系的问题.

假设群 B 是群 G 的真子群，$a\in G$. 我们将 aB 叫做 G 之元素 a 按 B (或mod$B$)的左陪集； Ba 叫做 G 之元素 a 按 B (或mod$B$)的

右陪集；a叫做左陪集(右陪集)的代表元.

这里谈一下，哪些元素有资格做陪集的代表元的问题？首先，aB 中的任一元素都可作为代表元. 因为如果 $a_1\in aB$，那末 $u\in B$，$a_1=au$，$a_1B=auB=aB$(因 $u\in B$，$uB=B$). 其次，只有 aB 中的元素才能作为它的左(右)陪集的代表. 因为设 $a_1B=aB$，那末由于 $e\in B$，所以 $a_1\in aB$. 因此，$a_1=au$，$u\in B$.

B 本身也是 G 按 B 的左(右)陪集，这时代表元可选为 e，因为 $eB=B$，$Be=B$.

下面谈一下一个重要论断：

两个左(右)陪集 a_1B，a_2B，要么完全等同，要么无共同元.

这是因为，如果 $x\in a_1B\cap a_2B$，即 x 为 a_1B 与 a_2B 的共同元素，那末 $x=a_1u_1=a_2u_2$，其中 u_1，$u_2\in B$，这样，$a_1u_1B=a_2u_2B$ 而 u_1B，$u_2B=B$，所以 $a_1B=a_2B$. 这说明，只要 a_1B，a_2B 有共同元，两陪集就等同，两个不同的陪集一定无共同元.

根据上面的断语和关于代表元的说明，就可将群 G 按 B (或 mod$B$) 划分成左陪集系：

$$G=aB\cup bB\cup cB\cup\cdots=\bigcup_{x\in L}xB.$$

这里 aB，bB，cB，…两两不相交，L 表示各左代表元 a，b，…的集合.

于此还要介绍一下，在某些专门著作中也将上式写成

$$G=aB+bB+cB+\cdots=\sum_{x\in L}xB,$$

这里 $+$、Σ 就是上式并 $\cup$ 的意思，而不是和的意思. 本书采用后一写法.

同样，群 G 可按 B 划分成右陪集系：

$$G=B+Bg+\cdots=\sum_{y\in R}By,$$

这里 R 表示右代表元的集合.

这里，我们要说明，一个集合 U 的 U^{-1}，是指：

$$U^{-1}=\{u^{-1}\mid \forall u\in U\}.$$

因此当 U 为群 G 的子群时，因 $u\in U, u^{-1}\in U, (u^{-1})^{-1}\in U$，所以 $U^{-1}=U$. 当然有 $G^{-1}=G$.

设 $g\in G$，陪集 $gU=\{gu_i\mid u_i\in U\}$ 的 $(gU)^{-1}$ 就是 $\{(gu_i)^{-1}\mid u_i\in U\}=\{u_i^{-1}g^{-1}\mid u_i\in U\}=U^{-1}g^{-1}$.

如果 U, V 是两个集，它们的并 $U\cup V$ 的 $(U\cup V)^{-1}$ 按照定义就是

$$\{u_i^{-1}\mid u_i\in U\}\cup\{v_j^{-1}\mid v_j\in V\}.$$

这样两个陪集 g_1U, g_2U 的并 $g_1U\cup g_2U$ 的 $(g_1U\cup g_2U)^{-1}$ 就是

$$\begin{aligned}&\{(g_1u_i)^{-1}\mid u_i\in U\}\cup\{(g_2u_i)^{-1}\mid u_i\in U\}\\&=\{u_i^{-1}g_1^{-1}\mid u_i\in U\}\cup\{u_i^{-1}g_2^{-1}\mid u_i\in U\}\\&=U^{-1}g_1^{-1}\cup U^{-1}g_2^{-1}.\end{aligned}$$

再将 G 按 B 划分成左陪集系的表达式按照 G 中的代数运算取逆，得到

$$G=G^{-1}=\left(\sum_{x\in L}xB\right)^{-1}=\sum_{x^{-1}\in R}B^{-1}x^{-1}=\sum_{x^{-1}\in R}Bx^{-1}=\sum_{x^{-1}=y\in R}By.$$

上式由第三节到第四节是由刚才的说明得到的，由第四节到第五节则是显然的. 由此可知，G 按 B 划分成左陪集的个数与右陪集的个数是相等的，把这个数叫做子群 B 在群 G 中的指数，以 $|G:B|$ 来表示.

设 G 为有限群，从群 G 按 B 分成陪集系的表达式可知：

$$|G:B|=\frac{n}{k},$$

其中 n 为 G 的元数，k 是 B 的元数，不难看出：

$$n=|G:e|,$$

这个结果叫做拉格朗日定理.

现在可以转过来讲群 G 按正规子群 N 划分为陪集系的问题

了.

$$G=eN+aN+bN+\cdots+kN.$$

这里 $e,a,b,\cdots,k$ 为代表元,但因 N 为正规子群, $eN=Ne$, $aN=Na, bN=Nb,\cdots,kN=Nk$, 所以又有

$$G=Ne+Na+Nb+\cdots+Nk.$$

这就是说, G 按正规子群 N 划分成左陪集系与右陪集系是一回事.

例如, n 阶对称群 S_n 可按 n 阶交代群 A_n 分划为两个陪集系, 一个是 n 阶交代群 A_n 本身, 另一个是 S_n 中的 任一奇置换 π_0 与 A_n 的积, 即

$$S_n=A_n+\pi_0A_n.$$

显然, $|S_n:A_n|=2$.

这里要强调三点:

1. G 的按正规子群 N 的分解式中 $aN,bN,\cdots$(或 $aB, bB,\cdots,$) 任意两陪集间都无共同元.

2. $aN,bN,\cdots$各自内部, 各元素按照前面所说意义, 可找到共轭元.

3. 按前面所说, N 在 G 中的指数为 $|G:N|$.

利用群 G 的元数是其子群 B 的元数之倍数的关系, 可以说, 元数为素数 p 的群 G 必为循环群. 这是因为, 设 $a(\neq e)\in G$. 那末 a 的周期 β 有限: $a^\beta=e$. 因而 $a,a^2,\cdots,a^\beta$ 形成一子群 B, 则 β 为 G 的元数 p 的因子, 但 p 为素数, 所以, $\beta=p$ 或 1, 后者不可能, 因为 $a\neq e$. 所以 $\beta=p$, 这说明元数为素数 p 的群 G 必为循环群.

八、商　　群

上节已经说到群 G 按正规子群 N 划分为陪集系

$$G=eN+aN+bN+\cdots+xN,$$

可以验证 $eN, aN, bN, \cdots, xN$ 构成群. 这是因为:

1) $(aN)(bN)$[即$\{(ah_i)(bh_j), h_i, h_j \in N\}$]

$=\{ah_i bh_j, h_i, h_j \in N\}$(按群的结合律)

$=\{abh_k h_j, h_k, h_j \in N\}$(按群的结合律与$N$的正规性)

$=\{abh_e, h_e \in N\}$(N 为子群, $h_k h_j = h_e$)

$=(ab)N$,

因 $ab \in G$, 所以 abN 必属于某一确定的陪集系. 同理

2) $((aN)(bN))(cN) = (abN)cN = abNcN = abcN$,

$(aN)((bN)(cN)) = (aN)(bcN) = abcNN = abcN$.

这上下两式相等, 即结合律成立.

3) $(eN)(aN) = eaN = aN$,

$(aN)(eN) = aeN = aN$,

即 eN 为中性元.

4) $(aN)(a^{-1}N) = aa^{-1}N = eN$; 同样$(a^{-1}N)(aN) = eN$, 即 aN 的逆元为 $a^{-1}N$.

关于群的四个要求都得到满足, 所以 $eN, aN, bN, \cdots, xN$构成群, 叫做商群, 并写成:

$$G/N.$$

不难看出, 群G按正规子群N的商群的元数, 就是正规子群N在群G中的指数.

从上面证明的过程可以看出, 两个陪集按某个代数运算结合时代表元同时按此代数运算结合, 结果依代表元结合的结果为转移, 所以代表元起着重要的作用, 因而商群的元素有另一种写法:

$$e, a, b, \cdots, x \quad (\mathrm{mod}N)$$

请注意这里的$(\mathrm{mod}N)$不可少.

商群是在群的基础上产生的新的群, 从群的发展来看, 它是一个跃进, 从其作用来看, 许多重要的理论将由此得以建立, 因此要

请读者注意.

商群的例子.

在六之例 3 中,四阶交代群 A_4 之正规子群 N 为:

$$e,(12)(34),(13)(24),(14)(23).$$

将 A_4 按 N 划分为陪集系. 显然划分中有 eN, 取 $(123)\notin N$, 作陪集 $(123)N$. 在 $(123)N$ 的元素中不含 (132). 于是就以 (132) 作代表元,构成陪集 $(132)N$. $(132)N$ 与 $(123)N$ 中无公共元素. 因只要有一公共元素,两陪集就重合,但 (132) 不含于 $(123)N$ 中, 故不能重合,而且无公共元素. 于是

$$A_4=eN+(123)N+(132)N.$$

所成的商群为

$$eN,(123)N,(132)N,$$

或换种写法:

$$e,(123),(132)\quad(\mathrm{mod}N).$$

这个商群也可以写成

$$eN,(142)N,(124)N$$

或

$$eN,(243)N,(234)N.$$

因为代表元是可以在所属的某陪集内任取的. 例如 $(142)N$ 与 $(123)N$ 为同一陪集, 实际上 $(142)\ (12)\ (34)=(134)$; 而 $(123)(14)(23)=(134)$,两陪集有一元素相重,两陪集重合. 同理 $(142)N$ 也与 $(243)N$ 为同一陪集.

现在来看稍为复杂点的例子:

假设有循环群 $G=\{a\}$, 它的元数为两个不同的素因数的积 $n=pq$,那末它有两个真子群

$$e,a^p,a^{2p},\cdots a^{(q-1)p};\tag{1}$$

$$e,a^q,a^{2q},\cdots,a^{(p-1)q}.\tag{2}$$

把(1)写作$\{a^p\}$，把(2)写作$\{a^q\}$，由于$a^i\cdot a^k=a^{i+k}=a^{k+i}=a^k\cdot a^i$，它们是可交换的子群，所以$\{a^p\}$，$\{a^q\}$ 都是真的正规子群，它们的元数分别为 q，p.

将G按$\{a^p\}$划分为陪集系，得

$$G=e\{a^p\}+a\{a^p\}+\cdots+a^{p-1}\{a^p\}.$$

再将G按$\{a^q\}$划分为陪集系，得

$$G=e\{a^q\}+a\{a^q\}+\cdots+a^{q-1}\{a^q\}.$$

这样，由于正规子群不同，G根据它们所划分的陪集系不同，商群也就不同，两个不同的商群记作 $G/\{a^p\}$，$G/\{a^q\}$.

商群 $G/\{a^p\}$的元素为

$$e,a,\cdots,a^{p-1}\pmod{\{a^p\}}.$$

对此商群，可以验证如下. 其中任意两个元素的积 $a^la^m(\mathrm{mod}\{a^p\})$ $(0\leqslant l,m\leqslant p-1)$，即 $a^{l+m}(\mathrm{mod}\{a^p\})$，总属于一个确定的陪集 $a^r\{a^p\}$. 这是因为 $l+m=bp+r$，$r=0,1,\cdots,p-1$，于是，$a^{l+m}=a^{bp+r}=(a^p)^b\cdot a^r$. 由于$(a^p)^b$属于$\{a^p\}$. 即属于以 e 为代表的陪集系，所以$(a^p)^ba^r(\mathrm{mod}\{a^p\})=a^r(\mathrm{mod}\{a^p\})$. 这样，$a^r$ 确是代表元 $e,a,a^2,\cdots,a^p$ 中的一个元素，因此封闭性成立，其他的三个要求，同样可以验证，是成立的.

这个商群的元数为 p，而商群 $G/\{a^q\}$的元数则为 q.

随着 $p>q$ 或 $p<q$，而说商群 $G/\{a^p\}$比 $G/\{a^q\}$小或大.

对于以上所说的各点，我们现在就可以用一个关于同态的定理来做一个小结了.

按照前面所说的定义，群G中的元素凡经过同态映射φ而映射到群G'的中性元素e'的，构成G的核N，它又是正规子群.

将群G按正规子群N分成陪集系：$eN,aN,bN,\cdots,lN,e,a,b,\cdots,l$ 为G的元素，$eN,aN,bN,\cdots,lN$ 构成商群 G/N.

设有一个同态映射 ψ，将群G同态地映到群 Γ 上. 于是，群 I

的一个元素 a，在群 G 中有一组原象．如果这些原象之一为 x，那末这组原象就是陪集 xN，$N\subset G$ 为同态 ψ 的核．事实上，既然 ψ 为同态映射，所以核 N 存在．设 e_1 为 Γ 的中性元，u 为 N 的任一元素，那末 xu 为 xN 的元素，按同态的要求，因为 $\psi(u)=e_1\in\Gamma$，

$$\psi(xu)=\psi(x)\psi(u)=\psi(x)=a,$$

所以 xN 中的任意元素与 $xe=x$ 同样为 Γ 的某个元素 a 的原象，即 xN 为 a 的一组原象．

按 79、81 页的说明可知，如果 $b\neq a, b\in\Gamma$，则所对应的陪集不与 xN 相交，因而 Γ 的元素与 G 按 N 的陪集是一一对应的．

群 Γ 与 G 按同态映射的核 N 的商群 G/N 同构．

现在就来叙述这一个关于同态的定理．

每一个群 G 到另一个群 Γ 的同态映射 φ 的核为正规子群 $N\subset G$．反过来，对群 G 的每一个正规子群 N，存在一个 G 到它按 N 的商群 G/N 上的同态映射 φ，它的核是 N．设 G 按正规子群 N 划分为陪集系，将 G 的每个元素对应于某个相应的陪集，就得到这个同态映射 φ．

如果 ψ 是群 G 到群 Γ 上的任意同态映射，那末 Γ 的每个元素在 ψ 下的一组原象是 G 按 ψ 的核 N 划分的陪集系中的某个陪集，而且 Γ（作为 G 在 ψ 下的象）同构于 G 按照核 N 的商群 G/N．

从这个定理又可推得，如果要 G 到 Γ 的同态映射 φ 是同构的，就必须使这个映射 φ 的核只由一个中性元素所组成，而且只需这一条件就够了．

这是因为，每个陪集只有一个元素：$x\{e\}$；Γ 的每个元素只与 G 按 $\{e\}$ 的商群 $G/\{e\}\cong G$ 的一个元素对应．

为了扩大知识面，下面再谈一下同构定理，只叙述这个定理而不作证明．读者了解有这回事就行，所以不作较透澈的说明．

在（壹）中已介绍了两个集合的积，现在，设群 G 有两个子群

A, B. 它们的积 AB, BA 的意义与集合的积是类似的，我们说子群 A, B 的积是可换的：

$$AB=BA,$$

是指对 A 中的任意元素 a'，与 B 中的任意元素 b' 的积 $a'b'$（一般地说 a', b' 不可交换，即 $a'b' \neq b'a'$），有 B 中的元素 b'' 与 A 中的元素 a''，使得

$$a'b' = b''a''$$

成立（这 b'', a'' 不一定分别等于 b', a'），否则 A, B 就是不可换的.

例如对在 S_3 中的两个子群

$$A: \quad a_1=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \quad a_2=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \quad e$$

$$B: \quad b_1=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \quad e,$$

有 $AB=BA$. 这是可以验证的，例如

在 AB 中有 $a_1b_1=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$,

$$a_2b_1=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix};$$

在 BA 中有 $b_1a_1=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$,

$$b_1a_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix};$$

因而

$$a_1b_1=b_1a_2, \quad a_2b_1=b_1a_1, \text{ 等等，其余不一一列举.}$$

但对 S_3 中的另两个子群

$$C: \quad c_1=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \ e,$$

$$D:\qquad d_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ e;$$

$CD\neq DC$，这表示 D,C 不可换. 因为

$$CD:\ c_1e=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$c_1d_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

$$DC:\ d_1e=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},$$

$$d_1c_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$

在 DC 中找不到 $x\in D,y\in C$，使 $xy=c_1d_1$；在 CD 中也找不到 u，v，使 $uv=d_1c_1$.

其次，可将子群 $A\subset G$ 的每个元素，与子群 $B\subset G$ 的每个元素相结合而生成子群 $\{A,B\}$（即对每个 $a',a''\in A$ 与 $b',b''\in B$，$a'b'$，$b''a''$ 等所组成的子群）. 例如上面的例子中 $\{A,B\}$ 为：

$$e,a_1,a_2,b_1,a_1b_1=b_1a_2,a_2b_1=b_1a_1$$

在这个子群里，A,B 可换，有 $AB=\{A,B\}$，但是在上例 C,D 的情形 C,D 不可换，CD 只含于 $\{C,D\}$，而不能等于 $\{C,D\}$.

现在就来叙述同构定理.

设 A 和 B 是群 G 的两个子群，A 是子群 $\{A,B\}$ 的正规子群，则这两个子群的交 $A\cap B$ 是 B 的正规子群，且商群

$$\frac{\{A,B\}}{A}\cong\frac{B}{A\cap B},$$

$\cong$ 表示同构.

在上例中，A 是 $\{A,B\}$ 的正规子群，$A\cap B=\{e\}$ 当然是 B 的正规子群，另一方面，A 在 $\{A,B\}$ 中的指数为 2，$A\cap B$ 在 B 中的指数为 2，从这里就可窥测到同构关系，读者可试求出上式两端的

元素.

九、单　　群

一个群，如果除了它自身和中性元以外，没有真的正规子群，就叫做单群；否则就叫做复群.

元数为素数的群是单群，因为按照群的元素 n，正规子群元数 k 与指数 i 的关系的定理 $n=ki$，n 必须是 k 的倍数，但这里 n 是素数，无真的因子，它所具有的因子只 n 与 1 两个，因此，要么 $n=k, i=1$，要么 $k=1$，$i=n$. 这说明 G 只有它本身与 e 作为正规子群. 特别，在可交换群的情形，当 G 为循环群，且元数为素数时，它是单群，例如

$$e,(1\ 2\ 3),(1\ 3\ 2)$$

是单群.

请读者注意，元素为复合数并不能说明一个群 G 必是复群，在(肆)中将要证明，交代群 A_5 的元数为 60，但它是单群，尽管 60 为复合数.

区别一个群是单群还是复群，也是很重要的，它对判别群是否可解与在 5 次以上代数方程是否可用其系数经过有限次有理运算来解时起着主要的作用.

十、换 位 子 群

在(叁四)里曾谈到共轭元素

$$a^{-1}ba=c.$$

如果能找到一个元素 k，使得 $c=bk$，从而

$$a^{-1}ba=bk,$$

即

$$b^{-1}a^{-1}ba=k,$$

那么 k① 就叫做 b 与 a 的换位元素，也就是 b 与 k 的积，可使 b 变成此积的共轭元素，若从 $ba=abk$ 来看，即 ab 右乘以 k，可使它变换位置，得 ba，这就是“换位”二字的由来.

群 G 中换位元素总是存在的，例如在上式中令 $b=a$，则

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

因为 G 总会有中性元 e 的，所以至少存在一个对任意一对元素 a,a 的换位元素 e.

假设群 G 有换位元素如下(这里且看有限情形)：

$$k_0=e,k_1,k_2,\cdots,k_l.$$

按照 G 中的运算，将这些 k_i 作一切可能的结合(两个换位元素的积可能不是换位元素)，得到各种可能的结果，例如

k_i $(i=0,1,\cdots,l)$

k_ik_j $(i,j=0,1,\cdots,l$，并且包括 $i=j)$

$k_ik_jk_m$ $(i,j,m=0,1,\cdots,l$，包括 $i=j=m)$

… … …

$k_0k_1k_2\cdots k_l$

再找出它们各自的逆元素，例如

$$k_i=a_i^{-1}b_i^{-1}a_ib_i,\quad k_i^{-1}=b_i^{-1}a_i^{-1}b_ia_i;$$

$$k_j=a_j^{-1}b_j^{-1}a_jb_j,\quad k_j^{-1}=b_j^{-1}a_j^{-1}b_ja_j;$$

$$k_ik_j=a_i^{-1}b_i^{-1}a_ib_ia_j^{-1}b_j^{-1}a_jb_j,$$

那末

$$(k_ik_j)^{-1}=k_j^{-1}k_i^{-1}=b_j^{-1}a_j^{-1}b_ja_j\cdot b_i^{-1}a_i^{-1}b_ia_i,$$

所有这些元素都属于 G，将它们归并到一起，其中可能有相同的，则取一次，可以看出这里也包括 e. 所有这些元素构成一个群，

① 有些书里也记作

$$b^{-1}a^{-1}ba=[b,a]$$

叫做群G的换位子群，以K来表示. 如果K只包含一个e，这就说明G的所有元都是可交换的，K愈大，可交换的元愈少，与群G的中心恰相反.

现在来谈下面两个性质.

1. 一个子群G的换位子群K是正规子群.

如果能证得$gK=Kg, \forall g\in G$，就证明了K是正规子群. 而要证$gK=Kg$，就得证明K的元素的共轭元素也属于K.

现在假设$k=a^{-1}b^{-1}ab, k\in K, a, b\in G$.

取k的共轭元素

$$g^{-1}kg=g^{-1}a^{-1}b^{-1}abg=g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}ag^{-1}bg$$

$$=(g^{-1}ag)^{-1}(g^{-1}bg)^{-1}(g^{-1}ag)(g^{-1}bg),$$

这说明k的共轭元素也呈换位元的形式，所以$g^{-1}kg$属于换位子群K.

再看K的任意元素

$$\lambda=k_1k_2\cdots k_t,$$

这里k_i是换位元素，取其共轭元素

$$g^{-1}\lambda g=g^{-1}k_1gg^{-1}k_2g\cdots g^{-1}k_tg$$

$$=(g^{-1}k_1g)(g^{-1}k_2g)\cdots(g^{-1}k_tg),$$

右边的每个$(g^{-1}k_ig)$按上段的证明为换位元素，属于K，因而$g^{-1}\lambda g\in K$. 这样，K的每个元素的共轭元素同时属于K，这说明K是正规子群.

2. 如果群G的正规子群N含有换位子群K，那末商群G/N是可交换群.

这是因为，已知

$$K\subset N\subset G,$$

将G按N划分为陪集系

$$G=eN+aN+bN+\cdots+mN$$

设 $k\in K$ 使 $ab=bak$.

因为 $k\in K\subset N$，所以按代表元的选法，

$$eN=kN=N.$$

又

$$aNbN=abN,$$

$$abN=bakN=baN=bNaN\text{（因为 }k\in N\text{）}.$$

即

$$(aN)(bN)=(bN)(aN).$$

这说明，G/N 为交换群.

一个群 G，尽管它本身可能不可交换，但对其换位子群 K 取商群 G/K，则是可交换的，所以换位子群有特殊的意义. 我们已知，G 到其商群的映射是同态 φ，上面的论断说明，在正规子群包含换位子群的条件下，经过同态 φ，不可交换性丧失了，也就是所谓同态在一定条件下具有忘性.

换位子群的例子.

已知四阶对称群 S_4 的元素为:

e, (234), (314), (412), (132),

(243), (341), (421), (123),

(12)(14), (13)(24), (14)(23),

(12), (1234), (1432), (24)(13),

(1243), (1342), (14)(23),

(34), (1324), (1423),

它的换位子群是四阶交代群 A_4:

e, (234), (314), (412), (132),

(243), (341), (421), (123),

(12)(34), (13)(24), (14)(23).

不难验证，例如 (234), (314)的换位元素是

$(234)^{-1}(314)^{-1}(234)(314)=(243)(134)(234)(314)=$
$(13)(24)$，而$(13)(24)\in A_4$.

读者自行验证，群

e，(1234)，$(13)(24)$，(1432)，$(12)(34)$，
(24)，$(14)(23)$，(13)

中，

$$e,(13)(24)$$

为它的换位子群.

请读者回头看(叁八) 商群之例. A_4 的换位子群(也是正规子群)是 $N=\{e,(12)(34),(14)(32),(13)(24)\}$. A_4 对 N 的商群 $eN,(123)N,(132)N$ 是可交换的.

十一、群 的 表 示

这里讲的群的表示，就是群的元素用方阵(在一般理论书籍中是说用线性变换来表示，但限于本书所提供的预备知识，我们只说它的特例—方阵)来表示. 它的用处很大，但因为须要较多其它方面的知识，这里只能点到即止.

先谈一个具体的问题.

我们已知 S_3 的元素是

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad b=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

$$c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad d=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad f=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

现在作如下的对应关系

$$e\to\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\ (1),\quad a\to\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\ (2),\quad b\to\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\ (3),$$

$$c\to\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}(4),\quad d\to\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}(5),\quad f\to\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}(6).$$

解释一下，例如(2)中置换 a 把 1 换为 2，对应的方阵表明把单位方阵$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$中第一列换为第二列(或者说，把第二列放在第一列的位置上)； a 把 2 换为3，对应的方阵表明将单位方阵第二列换为第三列；a 把 3 换为 1，对应的方阵表明将单位方阵第三列换为第一列；……等等，可以验证这种对应关系满足同态映射的要求，因而是同态映射 φ，例如

$$b=a^2\to\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\text{同(3)}$$

$$f=ac\to\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\text{同(6)}$$

由于 φ 是同态映射，a,b,c,d,e,f 构成群，所以在 φ 下的方阵的集合也是群.

这样，设给定两个群：n 元的群 G 与 m 元的方阵群 Γ，$m\leqslant n$. 如果在 G 与 Γ 之间存在一个同态映射 D，那末就说方阵群 Γ 是群 G 的表示. 于是，设 a,b 为 G 的任意元，e 为 G 的中性元，就有

$$D(ab)=D(a)D(b),\tag{1}$$

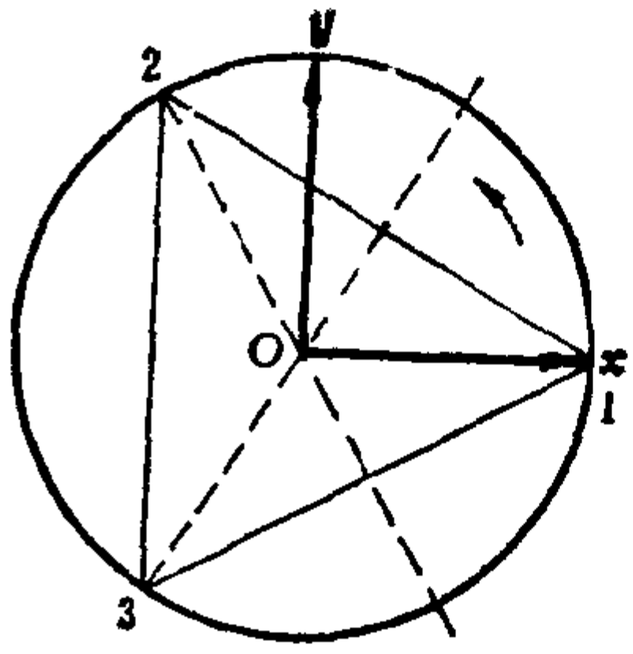
$$D(ae)=D(a)=D(a)D(e),\tag{2}$$

$$D(aa^{-1})=D(e)=D(a)D(a^{-1}).\tag{3}$$

所以，G 的中性元映为 Γ 的中性元，G 的一个元素的逆元映为 Γ 中相应元素的逆元，(3)中的 $D(a^{-1})$ 可写为 $D^{-1}(a)$.

群的表示并非唯一的，上面所说的 S_3 还可以有如下的表示.

在单位圆内内接一个等边三角形，如图所示．Ox, Oy 为轴，令 x 为Ox上的单位矢量，y 为Oy 上的单位矢量．三角形的三个顶点分别为 1, 2, 3.



显然，S_3 中的 e 就使此三角形保持原位，从而整个圆不动，x，y 也不动.

$a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$就是此正三角形围绕中心$O$ 按箭头方向转120°，则 1 转到 2，2 转到 3，3 转到 1. 因为此图为刚体，与三角形旋转的同时，矢量 x 的矢端坐标由(1, 0)转到(cos 120°, sin 120°)；矢量 y 的矢端坐标由 (0, 1) 转到 (cos(90°+120°), sin(90°+120°)) =(−sin 120°, cos 120°)．于是，可以建立下列的对应

$$a\to\begin{pmatrix}\cos 120^\circ, -\sin 120^\circ\\ \sin 120^\circ, \quad \cos 120^\circ\end{pmatrix}=\begin{pmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix},$$

此方阵中的第一、二列即分别为 x, y 旋转 120°后的坐标.

$c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ 就是此三角形以 Ox 为轴转 180°，或叫镜面反射，使 2 换为 3，3 换为 2，这时矢量 $x=(1,0)$不动，矢量$y=(0,1)$变成(0, −1)于是可以建立下列的对应：

$$c\to\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

这里方阵中的第一、二列是经所说镜面反射后 x、y 的坐标.

再看 $f=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ 就是正三角形绕 $3O$ 轴的镜面反射，由

a 的情况可见，x 的坐标由(1,0)换为$(\cos 120°, \sin 120°)$，而 y 的坐标则换为$(\cos 30°, \sin 30°)=\left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right)$，因而又可以建立对应关系

$$f\to\begin{pmatrix}\cos 120 & \cos 30\\ \sin 120 & \sin 30\end{pmatrix}=\begin{pmatrix}-\frac{1}{2} & \frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & \frac{1}{2}\end{pmatrix}.$$

余下的三种对应关系请读者自己去建立.

可以验证，所建立的对应关系是同态对应，因而所说的方阵是 S_3 的另一种表示，例如

$$ac=f\to\begin{pmatrix}\cos 120° & -\sin 120°\\ \sin 120° & \cos 120°\end{pmatrix}\begin{pmatrix}\cos 120° & \cos 30°\\ \sin 120° & \sin 30°\end{pmatrix}$$

$$=\begin{pmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}-\frac{1}{2} & \frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & \frac{1}{2}\end{pmatrix}.$$

如果将 1 看作 1×1 的方阵(1)，我们也可以使 S_3 的所有元素 e, a, b, c, d, f 对应于 1，这也是一种同态，因而也是 S_3 的一种表示.

如果将 $+1$ 与 -1 看作 1×1 方阵(1)，(-1)，还可以将 S_3 中的偶置换对应于 $+1$，奇置换对应于 -1，这又是一种同态，因而也是 S_3 的一种表示，这二个例子解释了定义中的 $m\leqslant n$.

设有与 Γ 中的方阵同阶的满秩方阵 X，使得

$$X^{-1}D(g)X=D'(g), \forall g\in G$$

成立，(X^{-1} 是 X 的逆元)，就说这两表示 D, D' 是等价的.

例如，设 X 为$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$，其逆亦为

$$X^{-1}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$

那末

$$X^{-1}D(c)X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=D'(c),$$

$$X^{-1}D(a)X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

$$=\begin{pmatrix}-\frac{1}{2} & \frac{\sqrt{3}}{2}\\ -\frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix}=D'(a),$$

因其他的 b,df,e 都由 a,c 生成，所以 $D'(b),D'(d),D'(f),D'(e)$ 都由 $D'(a),D'(c)$ 生成，请读者自己去完成.

在代数学中，一个 $n\times n$ 方阵 $A=(a_{ij})$ 的主对角线(从左上角至右下角)上各元素的和即

$$a_{11}+a_{22}+\cdots+a_{nn}$$

是所谓 A 的迹，记作 $\mathrm{tr}(A)$，表示 $D(g)$ 的迹

$$\mathrm{tr}(D(g))$$

叫做群之元素 g 的表示的特征标.

有一个定理说明，等价的表示有同样的特征标. 对这个定理不再给予证明，看上面的例子就很清楚了:

$D(c)$ 与 $D'(c)$ 的特征标同为 $1-1=0,-1+1=0$,

$D(a)$ 与 $D'(a)$ 的特征标同为 $-\frac{1}{2}-\frac{1}{2}=-1,-\frac{1}{2}-\frac{1}{2}=-1$,

等等.

用以上的叙述可以做氨 NH_3 的群表示，同时这又说明，群的表示理论在固体物理、量子力学，以及微分方程中有重要的应用，

请有兴趣的读者在学好数学基础课以后作深入的学习与研究.

十二、几 个 定 理

首先要说明，前面讲到有限群G的子群B的元数k可以整除G的元数n:$n/k=i$，其中i为B在G中的指数. 但是，倒过来的说法并不成立. 群G的元数n可以被某个数i所整除，然而它并不一定有元数为i的子群，现在就请看下面的一个例子.

设有三个元素:$a=(12)(34)$,$b=(123)$,$c=(13)(24)$,由这三个元素生成交代群A_4. A_4有12个元素. 它有二元子群$\{e,a\}$或$\{e,c\}$;有三元子群$\{e,b,b^2\}$. 但无六元子群. 请读者逐一试之.

不过，如果我们把元数的因子限制为素数的幂，情况就会改变. 还是上面的例子，可以看出12的素因数为2，3，它恰有2元子群与3元子群，还有$2^2=4$元子群.

下面的定理说明了这个现象.

定理1 如果p是素数，又如果p^m(m为自然数)小于群G的元数n且整除n,那末G至少有一个真子群,它的元数被p^m整除.

我们不证明这个定理.

由此定理还可以得出下面两个推论:

推论1 如果p^m整除群G的元数n，那末此群G至少有一个p^m元子群.

因为根据上面的定理，群G有一真子群B，B的元数能被p^m整除,显然,B的元数少于G的元数n，再对B应用上面的定理,B也有真子群Γ,它的元数被p^m整除,Γ的元数少于B的元数,一直进行下去,最后必得一个元数为p^m的子群$\Gamma_{,m}$.

推论2 如果p为素数,整除群G的元素n,那末,G有元数为p的子群.

这是当然的，因为在定理中可令 $m=1$，再根据推论 1，就得到此推论 2.

定理 2 如果 p 为素数，自然数 $m>1$，那末元数为 p^m 的群 G 必有元数为 p^l（自然数 $l<m$）的正规子群.

我们不证此定理.

例如，下面的由正四边形旋转与对换 B、D 两顶点所成的群 G 有 $2^3=8$ 个元素.

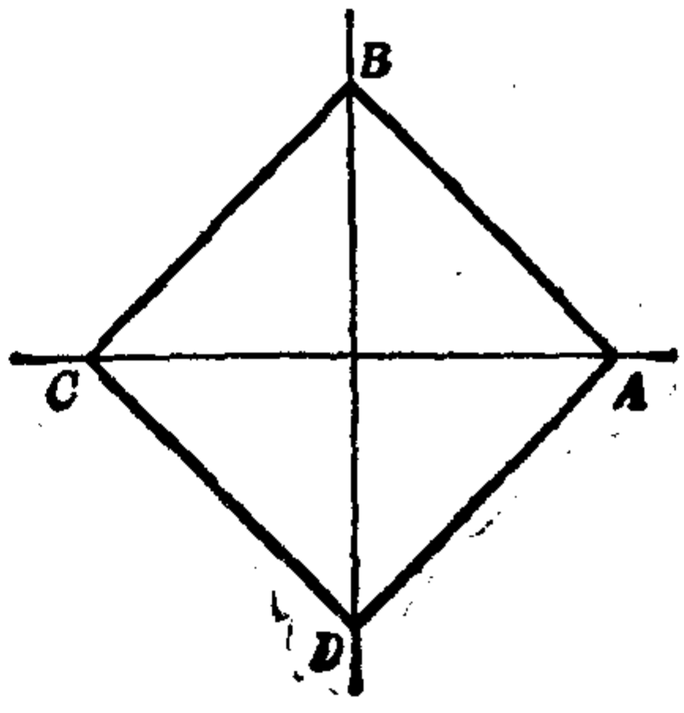
$$e,\ a=\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix},\ b=\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix},$$

显然，$a^4=e, b^2=e, b^{-1}ab=a^3$. 因而其他的五个元素为：

$$a^2, a^3, ab(=ba^3), ba(=a^3b), a^2b(=ba).$$

它有 $2^1=2$ 元正规子群：e, a^2；

还有 $2^2=4$ 元的正规子群：e, a, a^2, a^3.



肆

“八大锤”的联想

——正二十面体运动群及其他

爱好古典小说的读者，想必喜爱《岳传》中八大锤的故事.

锤是一立体形，它可以有各种各样的形状，正二十面体是其中一种形式.

这里我们感兴趣的是正二十面体，它的运动的群是 60 元群，而且是单群，这是一很有意义的数学事实. 与正二十面体运动的群同构的群是五阶交代群 A_5. 它在证明五次以上的一般代数方程不能用根式来解的问题中起到关键作用.

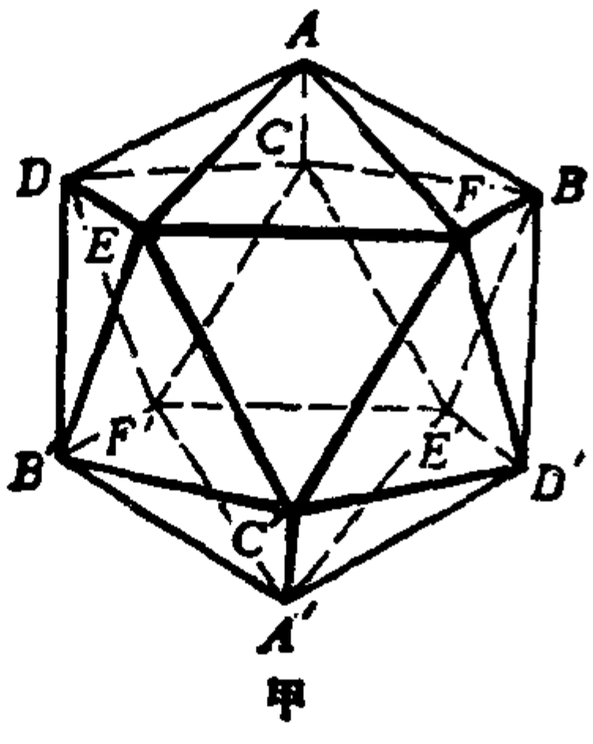
下面就先说明正二十面体的运动构成 60 元群，关于它是单群这个性质不予证明，而对 A_5 为单群则给以较详细的证明.

一、正二十面体运动群

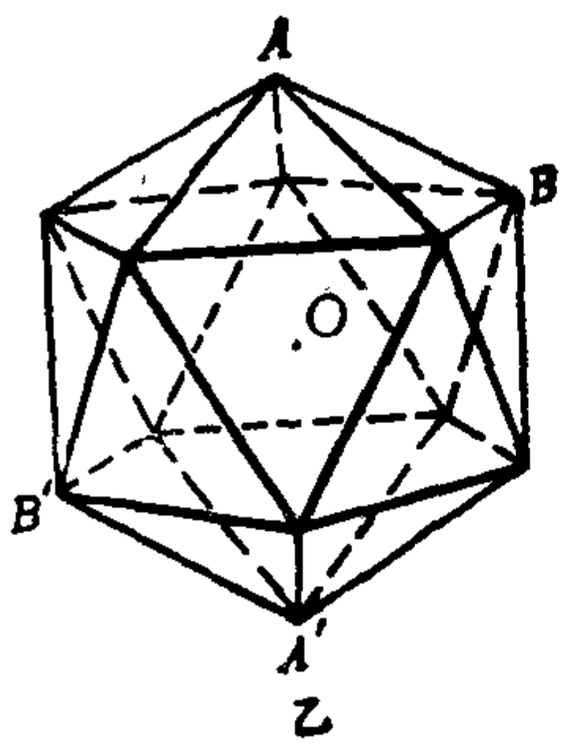
——元数为复合数的单群

现在来考察正二十面体的运动，如同关于正四面体的运动一样，正二十面体的运动是不改变它所占空间的运动，即各个顶点、棱、面的位置，经运动后仍为顶点、棱、面的位置，所变更的只是它们的标号，正二十面体的运动，只能是下面的四种：

(1) 全然不动的运动



甲



乙

$$e=\begin{pmatrix} A & B & C & D & E & F & A' & B' & C' & D' & E' & F' \\ A & B & C & D & E & F & A' & B' & C' & D' & E' & F' \end{pmatrix}.$$

(2) 以穿过 AA'(在乙图中以重黑点表示)的线段为轴每次顺着一固定方向转 $(360\div 5=)72^\circ$ 的运动，将它记作V_A. 同样，还有分别以穿过 BB', CC', DD', EE', FF' 的线段为轴顺着各自固定方向每次转 72° 的运动，分别记作 V_B, V_C, V_D, V_E, V_F.

围绕 AA' 转 72°，就使

$A\to A,\ B\to C,\ \cdots, D\to E,\ E\to F,\ F\to B,$

$A'\to A',\ B'\to C',\ \cdots, D'\to E',\ E'\to F',\ F'\to B'.$

即

$$V_A=\begin{pmatrix} A & B & C & D & E & F & A' & B' & C' & D' & E' & F' \\ A & C & D & E & F & B & A' & C' & D' & E' & F' & B' \end{pmatrix}.$$

作两次绕 AA' 的72° 的运动，即 $V_A * V_A=(V_A)^2$:

$$(V_A)^2=\begin{pmatrix} A & B & C & D & E & F & A' & B' & C' & D' & E' & F' \\ A & D & E & F & B & C & A' & D' & E' & F' & B' & C' \end{pmatrix}.$$

由此推得

$$(V_A)^4=\begin{pmatrix} A & B & C & D & E & F & A' & B' & C' & D' & E' & F' \\ A & F & B & C & D & E & A' & F' & B' & C' & D' & E' \end{pmatrix}.$$

可以看出，$(V_A)^5$ 回到原位，即相当于不动，这样，e，V_A，$(V_A)^2$，$(V_A)^3, (V_A)^4$ 形成一五元循环子群，记作$\{(V_A)\}$，现将这类子群叫

做(V)类型的子群. $\{(V_B)\},\{(V_C)\},\{(V_D)\},\{(V_E)\}$, $\{(V_F)\}$都是(V)类型子群.

所以,如果暂不计全然不动的运动(或$(V_A)^5$等),那末因为(V)类型的子群共有 6 个,每个子群中的运动为 4 个,那末(V) 类型的运动共有

$$4\times6=24\text{ 个.}$$

(3) 以此正二十面体的两个对棱中心的联线为轴, 绕此轴按确定方向转 180° 的旋转,例如绕 $AB,A'B'$ 中点 (在图乙中用×表示)联线转 180°的运动,这运动将 $A,B;A',B'$ 两对点对换,即$(AB)(A'B')$,由于共有 $AB,A'B';AC,A'C';AD$, $A'D';AE,A'E'$; $AF,A'F';BC,B'C';BF,B'F';BD',B'D;CD,C'D';C'F,CF';DE,D'E';C'E,E'C;DF',D'F;EB',E'B;EF,E'F'$ 等 15 对对边, 就有 15 个中点联线.如果暂不计全然不动的运动(包括两次转180°的运动),那末绕中线转 180° 的运动. 对于每一对对边只有 1 个运动, 15 个对边就共有

$$1\times15=15$$

个运动. 如果将绕 AB, $A'B'$ 中点联线为轴的运动记作 M_{AB}, 那末用置换表示此 M_{AB},就是

$$M_{AB}=\begin{pmatrix}A & B & C & D & E & F & A' & B' & C' & D' & E' & F'\\ B & A & F & D' & E' & C & B' & A' & F' & D & E & C'\end{pmatrix}$$

$$=(AB)(CF)(DD')(EE')(F'C')(A'B'),$$

$(M_{AB})^2$ 又回复到原位,相当于不动. 这样,e, M_{AB} 形成一个二元子群,记作$\{(M_{AB})\}$. 这类子群叫做(M)类型的子群,其他的可以照此类推.

(4) 以两相对面的三角形中心联线为轴. 顺确定方向转 120°; 240° 的旋转,由于相对面的三角形有 $\triangle ABC$, $\triangle A'B'C'$; $\triangle ADC$, $\triangle A'D'C';\triangle ABF,\triangle A'B'F';\triangle ADE,\triangle A'D'E';\triangle AEF,\triangle A'E'F';$

$\triangle BCE', \triangle B'C'E; \triangle BFD', \triangle B'F'D; \triangle CF'E', \triangle C'EF; \triangle CDF'; \triangle C'D'F; \triangle EB'D, \triangle E'BD'$等十对三角形，每一对三角形在不计全然不动的运动(包括转 360° 的运动)时，只有转 120°，240° 的运动两个，所有这十对三角形共有

$$2\times 10=20$$

个运动.

将$\triangle ABC, \triangle A'B'C'$ 中心联线为轴的运动记作 C_{ABC}，它的置换表示就是

$$C_{ABC}=\begin{pmatrix} A & B & C & D & E & F & A' & B' & C' & D' & E' & F' \\ B & C & A & F & D' & E' & B' & C' & A' & F' & D & E \end{pmatrix},$$

$$(C_{ABC})^2=\begin{pmatrix} A & B & C & D & E & F & A' & B' & C' & D' & E' & F' \\ C & A & B & E' & F' & D & C' & A' & B' & E & F & D' \end{pmatrix}.$$

$(C_{ABC})^3$又回到原位，即相当于不动，其他的可以照此类推.

这样，$e, (C_{ABC}), (C_{ABC})^2$ 形成一个三元子群，记作$\{(C_{ABC})\}$.

这类子群叫做(C)类型子群.

于是全然不动，$(V), (M), (C)$四个类型合起共有

$$1+24+15+20=60$$

种运动.

现在来看$(V), (M), (C)$三个类型的子群间的关系.

以(M_{AB})使(V_A)变形得

$$(M_{AB})^{-1}(V_A)(M_{AB})=(V_B),$$

即(V_A)与(V_B)其轭. 同样可证

$$(M_{AB})^{-1}(V_A)^i(M_{AB})=(V_B)^i \qquad (i=2,3,4)$$

即$(V_A)^i$ 与$(V_B)^i$ 共轭. 同时由于$\{(V_A)\}$与$\{(V_B)\}$除 e 以外元素都以 5 为周期，所以$\{(V_A)\}$与$\{(V_B)\}$共轭，用上面同样的方法，可以证得$\{(V_C)\}, \{(V_D)\}, \{(V_E)\}, \{(V_F)\}$ 等五元子群都相互共轭，所以组成共轭系.

又以(M_{AB})使(C_{ABC})变形，得

$$(M_{AB})^{-1}(C_{ABC})(M_{AB})=(C_{BAF}),$$

而C_{ABC}与C_{BAF}同以3为周期，所以C_{ABC}与C_{BAF}共轭．用与上段同样的方法可以证得$\{(C_{ABC})\},\{(C_{BAF})\},\{(C_{BDC})\}$…10个三元子群相互共轭，所以组成共轭元素系．

最后，以(V_A)使(M_{AB})变形．得

$$(V_A)^{-1}(M_{AB})(V_A)=(M_{AF}),$$

而M_{AB}与M_{AF}同以2为周期，所以(M_{AB})与(M_{AF})共轭．同样可得，$\{(M_{AB})\},\{(M_{AF})\},\{(M_{AC})\}$，…等15个二元子群相互共轭，形成共轭元素系．

要证明正二十面体的群为单群，必须证明它不含真的正规子群，现在假设它有真的正规子群，如果导出矛盾，就表明有真的正规子群的假设不成立，正二十面体的群为单群就得到证明．证明的过程这里就略去了．现在只证$n\geqslant 5$时交代群A_n——其中包含60元的A_5——为单群，也就行了．

$n\geqslant 5$时，交代群A_n是单群，特别是A_5为单群，由于它在后面有用，我们将这个结论证明一下．为简单起见，这里假定$n=5$，$n>5$的情形与此相似．

设N是A_5的一个正规子群，它不是$\{e\}$，因此在N中至少存在一个偶置换$\pi\neq e$，后者可以分解成轮换，或对换的积，且出现在一个轮换或对换中的符号，与另一个中的不同，因此它们不外乎有以下几种形式

$$\pi=(i_0\ i_1\ i_2\ i_3\ i_4), \tag{1}$$

$$\pi=(i_0\ i_1\ i_2), \tag{2}$$

$$\pi=(i_0\ i_1)(i_2\ i_3), \tag{3}$$

i_0,i_1,i_2,i_3,i_4是互不相同的符号，它们可以各是1,2,3,4,5中的一个数，以上三种情形（包括它们的积）穷尽了A_5中所有偶置换所

能分解成的形式.

由于假定N是正规子群,所以对每个偶置换 p, $p\pi p^{-1}$ 属于N, 从而 $p\pi p^{-1}\pi^{-1}$ 也属于 N. 对于上述三种形式的 π,我们选择 p 的形式如下:

$$1)\quad p=(i_1\ i_2\ i_3)$$

$$2)\quad p=(i_1\ i_2\ i_3)$$

$$3)\quad p=(i_1\ i_2\ i_4)$$

以 1)对(1),2)对(2),3)对(3),作 $\alpha=p\pi p^{-1}\pi^{-1}$,分别得

$$\alpha=(i_0\ i_2\ i_3), \qquad [1]$$

$$\alpha=(i_0\ i_3)(i_1\ i_2), \qquad [2]$$

$$\alpha=(i_1\ i_2\ i_3\ i_0\ i_4), \qquad [3]$$

这说明,如果在N中存在形式(1)的置换 π, 那末也存在形式[1]的置换;如果存在(2)形式的置换,那末也存在形式[2]的置换;如果存在形式[3]的置换,那末也存在形式[3]的置换,综合对比可见,(1),(2),(3)([1],[2],[3])可以由此及彼,相互导出与共存.

把(3)或[2]的形式写成$(j_1j_2)(j_3j_4)$, 这里 j_1,j_2,j_3,j_4 各不相同.

假设$(k_1\ k_2)(k_3\ k_4)\in A_5$,其中 k_1,k_2,k_3,k_4 各不相同, 我们来看置换

$$\beta=\begin{pmatrix}k_1 & k_2 & k_3 & k_4\\ j_1 & j_2 & j_3 & j_4\end{pmatrix}$$

上行的各个 $k_i(i=1,2,3,4,)$,与下行的 j_i 各不相同,可以算出

$$\beta=(j_1\ j_2)(j_3\ j_4)\beta^{-1}=(k_1\ k_2)(k_3\ k_4),$$

如果以φ表示 $\beta(j_1\ j_2)$,又得

$$\varphi(j_1\ j_2)(j_3\ j_4)\varphi^{-1}=\beta(j_1\ j_2)(j_1\ j_2)(j_3\ j_4)(j_1\ j_2)\beta^{-1}$$
$$=\beta(j_1\ j_2)(j_3\ j_4)\beta^{-1},$$

于是

$$\varphi(j_1\ j_2)(j_3\ j_4)\varphi^{-1}=(k_1\ k_2)(k_3\ k_4),$$

β 与 φ 相差一个因子——对换 $(j_1\ j_2)$，因此奇偶性不同，一个为偶置换，另一个必然是奇置换，我们令其中的偶置换为 γ，即

$$\gamma=\beta,\quad \text{当 } \beta \text{ 为偶时,}$$

$$\gamma=\varphi,\quad \text{当 } \varphi \text{ 为偶时.}$$

按照刚才的证明结果，得

$$\gamma(j_1, j_2)(j_3\ j_4)\gamma^{-1}=(k_1\ k_2)(k_3\ k_4).$$

因为 $(j_1\ j_2)(j_3\ j_4)\in N$，而 $\gamma\in A_5$，按照开始时的假设 N 为 A_5 中的一个正规子群，所以 $\gamma(j_1\ j_2)(j_3\ j_4)\gamma^{-1}=(k_1\ k_2)(k_3\ k_4)\in N$. 由此可见在 A_5 的正规子群 N 中包含了一切其中四个符号无一相同(即 $j_1\ j_2\ j_3\ j_4$ 各不相同)的两对换之积.

再来看看符号有重复的两个对换之积，它们可以写成 $(j_1\ j_2)\cdot(j_1\ j_3)$ 的形式. 除 $j_1\ j_2\ j_3$ 外还有两个不同的符号 l_1, l_2，于是置换 $(j_1\ j_2)(l_1\ l_2)$，$(l_1\ l_2)(j_1\ j_3)$ 是符号无一相同的两个置换，按刚才所证，属于 N，但是

$$(j_1\ j_2)(l_1\ l_2)\cdot(l_1\ l_2)(j_1\ j_3)=(j_1\ j_2)(j_1\ j_3),$$

这说明 $(j_1\ j_2)(j_1\ j_3)$ 也属于 N. 于是 N 中包含了任意两个对换之积，从而包含了任意偶数个对换的积.

综合以上所说可知正规子群 N 包含了一切偶置换，这样 $N=A_5$.

这说明 A_5 的正规子群 N 既然不是 $\{e\}$，就是 A_5 本身，也就是 A_5 无真正的正规子群.

二、群的理论在解代数方程中的应用

这一节的目的是要说明，群具有很大的威力，即它在解代数方程的问题中有极其重要的应用．而方程理论本身并不是此文的目的．由于这里涉及的理论相当艰深，要在这本小册子中作面面俱到的叙述是有困难的，所以只作一些粗浅的介绍，能说明群的威力就可以了．

我们已经知道二次方程的求解公式，当首项系数为 1 时，$f(x)=x^2+bx+c=0$ 的求解公式是

$$x=\frac{-b\pm\sqrt{b^2-4c}}{2},$$

这就是说，二次代数方程的解可以用它的系数经过有限次加、减、乘、除与开根号的运算而求得．

三次方程有解的公式，这里略谈一下求三次方程之根的卡尔当公式．

设三次方程为

$$f(x)=x^3+ax^2+bx+c=0, \tag{1}$$

作代换

$$x=y-\frac{a}{3},$$

得

$$y^3+py+q=0 \tag{2}$$

（这里 $p=-\frac{a^2}{3}+b$，$q=\frac{2a^3}{27}-\frac{ab}{3}+c$），(2)的一个根由下面的公式表示：

$$y_0=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

这个 y_0 是对方程的系数经过有限次有理运算与开根号运算得到的，当然下一步还要进行计算，才能得到原三次方程(1)的解，但所有步骤都是对系数进行有限次有理运算与开根号运算得到的.

四次代数方程也有求根公式，即是说它们的解都可以通过对方程的系数进行有限次有理运算与开根号运算来求得，试看下面求解的简要过程.

设四次方程为

$$f(x)=x^4+ax^3+bx^2+cx+d=0, \tag{1}$$

以 $x=y-\frac{a}{4}$ 代入，(1)化为

$$y^4+py^2+qy+r=0 \tag{2}$$

利用参数 α 把(2)化为下列等式

$$\left(y^2+\frac{p}{2}+\alpha\right)^2-\left[2\alpha y^2-qy+\left(\alpha^2+p\alpha-r+\frac{p^2}{4}\right)\right]=0 \tag{3}$$

选择参数 $\alpha=\alpha_0$，使(3)的方括号中的多项式有二重根 $\frac{q}{4\alpha_0}$，则 (3) 变成

$$\left(y^2+\frac{p}{2}+\alpha_0\right)^2-2\alpha_0\left(y-\frac{q}{4\alpha_0}\right)^2=0,$$

于是

$$y^2-\sqrt{2\alpha_0}\,y+\left(\frac{p}{2}+\alpha_0+\frac{q}{2\sqrt{2\alpha_0}}\right)=0,$$

$$y^2+\sqrt{2\alpha_0}\,y+\left(\frac{p}{2}+\alpha_0-\frac{q}{2\sqrt{2\alpha_0}}\right)=0.$$

求得 y，也即得到 x.

但五次与五次以上的代数方程没有求根的公式，即不能用根

式来解，为什么？这就是下文所要逐步说明的，在那里明显地反映出群的威力.

[1] 关于代数方程可否用根式来解的问题涉及许多方面，首先，对一个 n 次代数方程：

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n=0 \tag{1}$$

来说，它的系数 $1, a_1, a_2, \cdots, a_n$ 在什么数的范围里，是一个重要的问题，所以有必要先介绍一下数域的概念.

所谓一个数域，就是这样的数的集合，它既是数对于乘法的群，这时规定数 0 不计在此乘法群之内；又是数对于加法的群，这时数 0 是它的中性元素；并且数的乘法对加法的分配律成立.

这样，全体有理数集合构成有理数域，记作 Q；全体实数的集合构成实数域，记作 R；全体复数的集合构成复数域，记作 C，但全体整数不构成数域，因为整数对于乘法不构成群.

设 a, b 为任意有理数，以 $a+b\sqrt{5}$ 为元素的集合，记作

$$Q(\sqrt{5})=\{a+b\sqrt{5}\mid a, b\in Q\},$$

在[2]中可看到，$Q(\sqrt{5})$ 是数域. 任一数域都包含有理数域 Q，即 Q 是最小的数域.

有了数域的概念，我们就可以说，方程的系数在什么数的范围里了. 例如，方程 $x^2+3x+4=0$ 的系数在有理数域 Q 里；而方程 $x^3+3^{\frac{1}{2}}=0$ 的系数就不在 Q 里，而是在实数域 R 里.

不仅如此，正如前面所说，系数在什么数域里之所以重要，还因为它与该方程的解有关. 例如，方程

$$x^2-4x+2=0$$

的系数：$a=1, b=-4, c=2$ 在 Q 中，它的解可以经过已知的著名公式来表示：

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}=\frac{4\pm\sqrt{(-4)^2-4\cdot1\cdot2}}{2\cdot1}=\frac{4\pm2\sqrt{2}}{2}$$

$$=2\pm\sqrt{2},$$

这就是说，$x^2-4x+2=0$ 的解可以经过对在 Q 中的系数 1，-4，2 进行有限次加、减、乘、除与开根号运算来表达.

这样，我们就可以叙述，什么是方程可以用根式来解的问题了.

如果方程(1)的系数属于某个数域 F，对这些系数进行有限次加、减、乘、除(除数非零)和开根号运算，就能求得此方程的根，则说此方程在 F 上可以用根式来解，否则便是不能用根式来解.

今后，我们把方程 (1) 的系数所在的域叫做方程 $f(x)$ 的基本域.

[2] 代数学基本定理说明：每个 n 个次代数方程

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0 \tag{1}$$

在复数域 C 里恰有 n 个根(重根按重数计算)；这里 $a_1,\cdots,a_n$ 是复数，当然其中可能有实数，有理数，乃至整数.

假设上述代数方程(1) 的 n 个根为 $x_1,x_2,\cdots,x_n$，其中可能有实数，但是我们笼统地都把它们叫做复数根，于是

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n). \tag{2}$$

这就叫做 $f(x)$ 在复数域里可以分解成一次因子的积. 例如

$$f(x)=x^3-7x+6,$$

它的系数 $1,0,-7,6\in Q$，它的根为 $1,2,-3\in Q$. 因此在 Q 上就已有

$$f(x)=(x-1)(x-2)(x+3).$$

所以这个方程在 Q 上可以分解成一次因子的积，当然在 C 上也就分解成一次因子的积了.

然而，对 $f(x)=x^2-5$ 就不能说它在 Q 中可以分解成一次因子的积，因为，在

$$f(x)=x^2-5=(x-\sqrt{5})(x+\sqrt{5})$$

的一次因子中，数 $\sqrt{5}$ 不属于 Q.

这就给人们一个启示，如果在Q中加进$\sqrt{5}$，那末，在这个新的范围里，x^2-5是不是可以分解因式了呢？这个想法有道理，但不完整，问题是，加进$\sqrt{5}$以后，要将Q扩大为一个新的数域，因为只有在域中才能进行加、减、乘、除等运算，而结果仍不出数域之外．现在就来谈谈如何构造这个数域，将$\sqrt{5}$加进Q，与Q中的所有数及$\sqrt{5}$本身一起，反复做数的乘法群的运算和加法群的运算，就可构成新的数域，即前面提到的$Q(\sqrt{5})=\{a+b\sqrt{5}\mid a,b\in Q\}$．因为可以验证在$Q(\sqrt{5})=\{a+b\sqrt{5}\mid a,b\in Q\}$中对于加、减、乘、除(除数不为零)是封闭的，所以$Q(\sqrt{5})$构成数域，叫做在$Q$中添加$\sqrt{5}$而成的数域，又因为一切有理数可以由1产生：$1+1=2$，$1+2=3$，$(1+1)\div(1+1+1)=\frac{2}{3}$等等，所以又可将$\alpha+\beta\sqrt{5}$写成如下形式

$$\alpha\cdot 1+\beta\sqrt{5}=\alpha+\beta\sqrt{5},$$

其中$\alpha,\beta\in Q$，且是任意的，叫做这个表示式中的系数，当$\beta=0$时，就是一切有理数α；当$\alpha=0,\beta=1$时，就是所加进去的$\sqrt{5}$，这样新的数域就构成了，并写作$Q(\sqrt{5})$，叫做Q包含$\sqrt{5}$的扩域．可以验证所有$\alpha+\beta\sqrt{5}$形式的数满足对于域的所有要求，因为，就乘法群来看，设下面的$\alpha,\beta,\gamma,\mu,\eta,\xi$属于$Q$，则$(\alpha+\beta\sqrt{5})(\gamma+\mu\sqrt{5})=(\alpha\gamma+5\beta\mu)+(\alpha\mu+\beta\gamma)\sqrt{5}$，它仍是$\alpha+\beta\sqrt{5}$形式的数，数1是此群的中性元素；$\alpha+\beta\sqrt{5}\neq 0$的逆元为

$$\frac{1}{\alpha+\beta\sqrt{5}}=\frac{\alpha-\beta\sqrt{5}}{\alpha^2-5\beta^2}=\frac{\alpha}{\alpha^2-5\beta^2}+\frac{(-\beta)\sqrt{5}}{\alpha^2-5\beta^2},$$

这仍是$\alpha+\beta\sqrt{5}$形式的数；因为$\alpha+\beta\sqrt{5}$为实数，所以结合律成立；关于乘法对加法的分配律成立，也是因为这里讲的都是实数，而在实数范围里分配律是成立的，所以

$$[(\alpha+\beta\sqrt{5})+(\gamma+\mu\sqrt{5})](\eta+\xi\sqrt{5})$$
$$=(\alpha+\beta\sqrt{5})(\eta+\xi\sqrt{5})+\gamma+(\mu\sqrt{5})(\eta+\xi\sqrt{5})$$

是显然的. 至于$Q(\sqrt{5})$也满足数对于加法群的要求，是不难验证的，例如

$$(\alpha+\beta\sqrt{5})+(\gamma+\mu\sqrt{5})=(\alpha+\gamma)+(\beta+\mu)\sqrt{5},$$

仍是$\alpha+\beta\sqrt{5}$形式的数. 0为零元素，$\alpha+\beta\sqrt{5}$的逆元为$-\alpha-\beta\sqrt{5}$等等；关于结合律成立请读者亲自一试.

再看一个例子，设方程

$$f(x)=x^4-2x^2-3=(x^2-3)(x^2+1)=0,$$

这里(x^2-3)在Q里不能再分解因子，将此方程的一个根$\sqrt{3}$加进Q，作成域$Q(\sqrt{3})$，则x^2-3在$Q(\sqrt{3})$上可以分解成下面因式的积

$$(x-\sqrt{3})(x+\sqrt{3}).$$

但在$Q(\sqrt{3})$上(x^2+1)仍不能分解成一次因式之积，所以再将$x^2+1=0$的一个根i加进$Q(\sqrt{3})$，形成新的数域$Q(\sqrt{3})(i)$，或记作$Q(\sqrt{3},i)$，则x^2+1就可以分解成一次因式的积了：

$$(x+i)(x-i).$$

$Q(\sqrt{3})$叫做Q与$Q(\sqrt{3},i)$的中间域.

现在来看$Q(\sqrt{3},i)$中元素的表达形式，我们知道，当把$\sqrt{3}$加进Q时，$Q(\sqrt{3})$的元素用Q上的系数表示成

$$a+b\sqrt{3}.$$

但当i加进$Q(\sqrt{3})$后，$Q(\sqrt{3},i)$的元素以$Q(\sqrt{3})$中的数为系数时就表示成

$$\begin{aligned}&(c+d\sqrt{3})(a+b\sqrt{3})+(e+f\sqrt{3})i\\&=(ac+3bd)+(cb+ad)\sqrt{3}+ei+f\sqrt{3}\,i.\end{aligned}$$

这里$(c+d\sqrt{3})$，$(e+f\sqrt{3})$均为$Q(\sqrt{3})$上的元素，而$a,b,c,d,e,f\in Q$，所以等式的右边又表示$Q(\sqrt{3},i)$的元素以Q上的数为系数的表现形式，只须注意$ac+3bd,cb+ad,e,f\in Q$. 事实上，令$ac+3bd=\delta\in Q$，$bc+ad=\sigma\in Q$，则上式化简为

$$\delta+\sigma\sqrt{3}+ei+f\sqrt{3}\,i.$$

正如不久前的分析一样,在$Q(\sqrt{3},i)$中有有理数,无理数$\sqrt{3}$,虚数i,无理数$\sqrt{3}$与虚数i的积,所以$Q(\sqrt{3},i)$中的数可表示成

$$\delta+\sigma\sqrt{3}+ei+f\sqrt{3}\,i,$$

$$\delta,\ \sigma,\ e,\ f\in Q,$$

它将$Q(\sqrt{3},i)$的数概括无遗.

现在可以进行归纳了,设方程

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0$$

的基本域为F,在它的n个根中无重根(或者说n个根都不相同),那末可以将这n个根$x_1,x_2,\cdots,x_n$加进F中去,将F扩大成一个新的域,叫做分裂域,并记作$F(x_1,x_2,\cdots,x_n)$,这时$F(x)$在$F(x_1,\cdots,x_n)$上就能分解成一次因式的积了.

[3] 现在来建立方程$f(x)$的珈罗华群,它是方程可否用根式来解的关键,先看下面的方程

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n=0. \tag{1}$$

它的根设为$x_1,x_2,\cdots,x_n$,并假设无重根,将x_1代入方程,得

$$f(x_1)=x_1^n+a_1x_1^{n-1}+\cdots+a_n=0, \tag{2}$$

将x_1换为x_2,又得

$$f(x_2)=x_2^n+a_1x_2^{n-1}+\cdots a_n=0, \tag{3}$$

如此等等,这就难免使人们产生一个联想:可不可以建立一个变换s,以它作用于(2)时,系数($\in F$)都不变,右边的零也不变,而根则变为同一方程的另一个根,如果能找到这种变换,解决我们的问题就前进一步.

现在来建立这种变换.

假设已知数域K,建立一个将K一一对应地映射到自身上的变换s(后面将看到这样的s是存在的),这个s将K中的元素的和

映射为相应的象的和，将元素的积映射为相应的象的积，也就是，如果 a, b 是 K 的任意两个元素，那末，用记号 a^s 表示这种变换作用于 a，同时也表明 a 在 s 下的象，则按照上面所说

$$(a+b)^s = a^s + b^s,$$

$$(ab)^s = a^s \cdot b^s,$$

而 $a^s, b^s \in K$ 分别为 a, b 在 s 下的象，并且还要满足如下的条件：

1) 对每个元素 $a \in K$，$a^s \in K$ 是唯一确定的；

2) 如果 $a \neq b$，那末 $a^s \neq b^s$；

3) 对每个元素 $b \in K$，可以找到 $a \in K$，使得 $a^s = b$.

下面证明，这样的变换作成一个群，运算是接连施行这种变换，设有 s, t, u 三个这种变换.

显然，对任意的 $a \in K$，先作变换 s，则 $a^s \in K$，再作 t，两次变换记作 st，$(a^s)^t = a^{st}$，因 $a^s \in K$，所以 $(a^s)^t \in K$，于是，对一个元素 $a \in K$ 来说，st 也是有意义的变换.

再看 $a^{(st)u} = (a^{st})^u = ((a^s)^t)^u$，

$$a^{s(tu)} = (a^s)^{(tu)} = ((a^s)^t)^u,$$

这样，对一个元素 $a \in K$ 来说，$(st)u = s(tu)$.

此外，还有

$$(a+b)^{st} = ((a+b)^s)^t = (a^s + b^s)^t = a^{st} + b^{st};$$

$$(ab)^{st} = (a^s b^s)^t = a^{st} b^{st};$$

由于 s, t 都是满足上述条件的变换，以及 $a, b \in K$，所以 $a^s, b^s, a^{st}, b^{st} \in K$，对 $(a+b)$，(ab) 施行 $(st)u$ 与 $s(tu)$ 得同样结果，可以象对一个元素那样验证，请读者自行验证，这些结果说明，所定义的变换对运算来说是封闭的，且结合律成立.

在所定义的变换中有一个使所有的元素都不变的变换 e：

$$a^e = a, \quad a \in K,$$

它是中性元，符合所列举的条件.

对所定义的每个变换 s，还可以定义它的逆变换 s^{-1}：

$$ss^{-1}=s^{-1}s=e,$$

即

$$(a^s)^{s^{-1}}=a;\quad (a^{s^{-1}})^s=a.$$

按照上面的条件3)：$a^s=b$；同样，对每个 a，存在 b'，使得 $a=(b')^{s^{-1}}$. 但 $a^s=b$，而 $a^s=((b')^{s^{-1}})^s=(b')^{s^{-1}s}=(b')^e=b'$，由于条件2) $b'=b$，这说明变换 s, s^{-1} 是一一对应的.

还可以验证：若 $a^s=b, c^s=d$，则 $a=b^{s^{-1}}, c=d^{s^{-1}}$；$(b+d)^{s^{-1}}=(a^s+c^s)^{s^{-1}}=(a+c)^{ss^{-1}}=a+c=b^{s^{-1}}+d^{s^{-1}}$，$(bd)^{s^{-1}}=(a^sc^s)^{s^{-1}}=(ac)^{ss^{-1}}=ac=b^{s^{-1}}d^{s^{-1}}$.

所以，s 的逆变换 s^{-1} 也满足所说条件.

上面定义的变换叫做域 K 的自同构，并且域 K 的所有的自同构作成一个群 $\mathscr{G}$.

每个数域 K 都包含有理数域 Q，易于证明 K 的任一自同构，作用于任一有理数时，使此有理数保持不变，从而使 Q 一一对应地映射到自身.

只须证明，在此自同构作用下，1保持为 1，0 保持为 0 即可.

事实上，按照关于自同构的要求：

$$(1\cdot b)^s=b^s=1^s\cdot b^s.$$

这说明，1^s 为 1 在自同构 s 下的象域中的中性元素，但是象域就是有理数域本身(因为自同构 s 把一个域映射为自身)，所以中性元 1 在 s 下的 1^s 就是 1，即

$$1^s=1.$$

再看

$$(0+b)^s=b^s=0^s+b^s,$$

由此可见 0^s 在象域中是零元，但象域也是有理数域，所以 0^s 即普通的 0，

$$0^s = 0.$$

其他的结果都可由这两结果推出，请读者自行推证.

[4] 现在回到方程 $f(x)$ 的基本域 F 的情形.

设上面提到的域 K 是基本域 F 的分裂域 $F(x_1, x_2, \cdots, x_n)$. 如果在 $K = F(x_1, x_2, \cdots, x_n)$ 上的自同构群的某些自同构 s 使域 F 中所有元素保持不变，即对任意的 $a \in F$，有

$$a^s = a,$$

那末，所有这样的自同构 s 显然构成前面所说的群 $\mathscr{G}$ 的一个子群，这个子群叫做多项式 $f(x)$ 或代数方程 $f(x) = 0$ 的珈罗华群，记作 $\mathscr{G}(K, F)$.

这样，设

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

是域 F 上的任意方程，它在 $F(x_1, x_2, \cdots, x_n)$ 上的一个根设为 α_1，则

$$\alpha_1^n + a_1 \alpha_1^{n-1} + \cdots + a_n = 0.$$

以 $s \in \mathscr{G}(K, F)$ 作用于上式，则

$$(\alpha_1^s)^n + a_1 (\alpha_1^s)^{n-1} + \cdots + a_n = 0.$$

这是因为按照 s 的性质，它使 F 中的数 $a_i (i = 0, \cdots, n)$ 保持不变，包括使 0 保持不变，而 α_1 变为 α_1^s. 如果 $\alpha_1^s = \alpha_k$，则由上式可知 $\alpha_1^s = \alpha_k$ 也是所设方程的根.

于是，珈罗华群中的任意自同构 s 将 F 上的一个代数方程的根变为同一方程的根. 当 $\alpha_1^s = \alpha_k$ 时，α_k 叫做与 α_1 共轭.

由此可见，$\mathscr{G}(K, F)$ 中的自同构 s 作用于所属方程的根上时，只把这个根变为那个根，也就是只将此方程的各个根重新排列，因而自同构 s 相当于一个置换（由此可见，[3]中提到的 s 是存在的），于是：

任意一个无重根的方程的珈罗华群 $\mathscr{G}(K, F)$ 可以被看作是一

个置换群.

由于 n 个根(也就是 n 个元素)的排列为 $n!$ 个,所以珈罗华群的元素至多为 $n!$ 个.

为什么说"至多为 $n!$ 个",这是因为有些置换并不在 $\mathscr{G}(K,F)$ 内,例如,方程

$$f(x)=x^2-3x+4=0,$$

它的两个根是 $x_1=1, x_2=-4$. 这里 $F=Q$,那末,因为 $1,-4\in Q$,按照珈罗华群的要求,任意置换 $s\in\mathscr{G}(K,Q)$ 作用于 x_1,x_2,应保持其不变,又因为只可能有两个置换($n!=2!=2\cdot1=2$):

$$e=\begin{pmatrix}1&2\\1&2\end{pmatrix},\qquad s=\begin{pmatrix}1&2\\2&1\end{pmatrix}.$$

其中能保持 $x_1=1, x_2=-4$ 不变的置换只有 e,这就是说,$f(x)$ 的珈罗华群 $\mathscr{G}(K,Q)$ 只由一个元素组成: $\{e\}$,它的元数 <2.

现在按珈罗华群的定义与上面的说明,来看一个例子,通过观察,估计有关方程的珈罗华群.

例 1 $f(x)=x^2+2x+2=0$ 的两个根为

$$x_1=-1+i,\quad x_2=-1-i.$$

这里 $F=Q$,而 $x_1, x_2\notin Q$. 所以 $\mathscr{G}(K,Q)$ 中的任意置换 s,除 e 外,作用于 x_1,x_2,都要使它们改变,但是,因为总共只有 $n!=2!=2$ 个置换

$$e=\begin{pmatrix}1&2\\1&2\end{pmatrix},\qquad s=\begin{pmatrix}1&2\\2&1\end{pmatrix},$$

后者作用于 x_1,x_2 而使 x_1,x_2 对换,既然使它们改变,因而 $\begin{pmatrix}1&2\\2&1\end{pmatrix}\in\mathscr{G}(K,Q)$,而 $\mathscr{G}(K,Q)$ 必须包含中性元素,即 $e\in\mathscr{G}(K,Q)$,否则便不成其为群,所以 $f(x)$ 的 $\mathscr{G}(K,Q)$ 的元素为

$$\begin{pmatrix}1&2\\1&2\end{pmatrix},\quad\begin{pmatrix}1&2\\2&1\end{pmatrix}.$$

[5] 但是，求一个方程的珈罗华群远比上例要复杂. 对上面的例子所以能通过观察来估计，只是因为它的次数是 2，根的情况不复杂，才能做到，根的情况稍为复杂一点，就不容易观察到方程的珈罗华群，因此，为了求出珈罗华群，还要借助下面与珈罗华群有关的两个事实.

先看一个例子，已知三次方程

$$x^3+px+q=0,\quad p,q\in F,$$

设它的根是x_1, x_2, x_3，作函数

$$\varphi=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2.$$

在三次对称群 S_3 的一切元素作用下，φ 保持不变(参看壹中置换一节的思考题)，于是它是根的对称函数. 另一方面，根据韦达定理：

$$x_1+x_2+x_3=0,$$

$$x_1x_2+x_2x_3+x_3x_1=p,$$

$$x_1x_2x_3=-q,$$

经计算可得

$$\varphi=-4p^3-27q^2\in F.$$

这说明，以三次方程 $x^3+px+q=0$ 的三个根作成的函数 $\varphi=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$ 在 S_3 的所有元素作用下不改变其值. 虽然我们现在还未能判定 $x^3+px+q=0$ 的珈罗华群是什么，但是从关于珈罗华群的元数的那一段论述中可见，此方程的珈罗华群$\mathscr{G}(K,F)\subseteq S_3$("$\subseteq$"表示左边包含于或等于右边)，既然 S_3的所有元素(即置换)保持 φ 不变，那末作为S_3 之子群的$\mathscr{G}(K,F)$的元素当然也保持 φ 不变，按照珈罗华群的性质：$\varphi\in F$.

于是，我们所要说明的第一个事实是：

设方程 $f(x)$的基本域为 F，它的珈罗华群为$\mathscr{G}(K,\ F)$. 以 $f(x)$的 n 个根作有理函数 φ，φ 的系数属于 F，如果$\mathscr{G}(K,\ F)$作用

于 φ，而使 φ 的函数值保持不变，那末 φ 的值便属于 F.

作为上述事实的反面，如果 $\mathscr{G}(K,F)$ 作用于 φ 而使 φ 的函数值改变，那末 φ 的值就不能属于 F.

第二个事实是：

设以方程 $f(x)$ 的根作一有理函数 φ，φ 的系数在 F 中，如果 φ 的值等于 F 中的一个数，那末它在 $\mathscr{G}(K,F)$ 的所有置换的作用下不改变其函数值.

对于这个事实可作如下的解释，因为按题设 φ 是根的有理函数，φ 的系数属于 F，φ 的值等于 F 中的一个数，按照对群 $\mathscr{G}(K,F)$ 的要求，φ 的值在 $\mathscr{G}(K,F)$ 的所有置换的作用下保持不变.

这件事的反面是：如果 φ 的值不是 F 中的量，那末它在 $\mathscr{G}(K,F)$ 的置换作用下要改变其函数值.

这两个事实很重要，它可以帮助我们找出方程的珈罗华群 $\mathscr{G}(K,F)$.

现在再看上面的例子，在那里说过 $x^2+2x+2=0$ 的两个根是 $x_1=-1+i$，$x_2=-1-i$.

作根的有理函数

$$\varphi=x_1+3x_2=-4-2i,$$

这个函数的值不在 $F=Q$ 中，所以 $\mathscr{G}(K,F)$ 的置换应该改变其值，现在不谈 e，只看 $s=(12)$，它作用于 φ，确实改变其值：

$$\varphi^s=x_2+3x_1=-4+2i.$$

所以 $s=(12)$ 属于 $\mathscr{G}(K,F)$，$e\in\mathscr{G}(K,F)$，所以要找的群 $\mathscr{G}(K,F)=\{e,(12)\}$，因 S_2 一共只有两个元素，即 $e,(12)$.

要注意，如果只作 $\varphi=x_1+x_2=-2\in Q$，行不行？答复是，这不足以解决问题，因为在 $\varphi=x_1+x_2=-2$ 中，i 消失了，反映不出根及以根作其他有理函数的情况，所以作根的有理函数时，只作其对称函数是不够的.

例 2　$f(x)=x^3+x^2+x+1=0$ 的三个根为

$$x_1=-1,\ x_2=+i,\ x_3=-i.$$

这个例子比上面的例子复杂，因为它既有属于 $F=Q$ 的 $x_1=-1$，又有不属于 F 的根 $x_2, x_3=\pm i$. 这样，所要求的珈罗华群应该满足两个条件：(1)使 x_1 不变，(2)使 x_2，x_3 或由它们作成的函数(系数在 $F=Q$ 中)改变. 设由 x_2, x_3 作成的函数 φ 为：

$$\varphi=x_2+2x_3=i-2i=-i,$$

可能作为 $\mathscr{G}(K,F)$ 之元素的置换为：

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad s_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad s_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$

$$s_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad s_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad s_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

以 s_1, s_2, s_3, s_4, s_5 作用于 φ，都使它改变函数值，但同时又使 $x_1=-1$ 保持不变的只有 $s_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$，因为很明显，$s_3$ 中要改变的数字不涉及 1；而 s_1, s_2, s_4, s_5 都涉及 1 的变化，不满足上面所说的两个条件，因而不属于 $\mathscr{G}(K,F)$，所以在此题中

$$\mathscr{G}(K,F)=\{e,(2\ \ 3)\}.$$

例 3　已知：

$$f(x)=x^3-7x+7=0,$$

求它的 $\mathscr{G}(K,F)$.

此题较复杂，因为求根时要计算较复杂的公式，但按照本段开始时曾用到的式子

$$(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2,$$

将它两边开平方根得有理函数

$$\delta=(x_1-x_2)(x_2-x_3)(x_3-x_1).$$

按照那里所讲的计算 $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$ 的公式

$$-4p^3-27q^2,$$

则

$$\delta=\sqrt{-4p^3-27q^2}.$$

以 $p=-7, q=7$ 代入，得$\delta=\sqrt{49}=\pm 7$，± 7 在$F=Q$ 中，使 $\mathscr{G}(K, F)$的置换作用于 δ，应使其保持不变，但在上面所说的 S_3 的六个置换中，使 δ 保持不变的，除 e 以外，只有

$$s_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad s_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

所以 $\mathscr{G}(K, F)=\{e, (123), (132)\}$.

一般的 n 次方程

$$x^n+ax^{n-1}+bx^{n-1}\cdots+c=0$$

(这里文字$a, b, \cdots, c$是相互独立的，即一个文字不与其它的文字有关系)的珈罗华群$\mathscr{G}(K, F)$是对称群 S_n. 对这个结论这里不予证明.

[6] 如果用方程$f(x)$的根 $x_1, x_2, \cdots, x_n$ 作有理函数 ψ，当$f(x)$的珈罗华群$\mathscr{G}(K, F)$的某些置换作用于这个有理函数 ψ 时，ψ 保持不变，那末这些置换作成$\mathscr{G}(K, F)$的子群H，因为，设使 ψ 保持不变的置换为:

$$s_1=e, s_2, \cdots, s_k,$$

作用于 ψ，例如

$$(\psi)^{s_1}=\psi,$$

因而

$$(\psi^{s_2})^{s_i}=\psi^{s_i}=\psi.$$

设s_i^{-1} 为 s_i 的逆置换，则

$$(\psi^{s_i})^{s_i^{-1}}=(\psi)^{s_i^{-1}}=\psi^{s_is_i^{-1}}=\psi^e=\psi,$$

所以 s_i^{-1} 属于使 ψ 保持不变的置换；等等. 可见这些置换构成$\mathscr{G}(K, F)$的子群.

例 4 方程 $f(x)=x^3-5=0$，它的三个根是

$$x_1=5^{\frac{1}{3}},\quad x_2=5^{\frac{1}{3}}\omega,\quad x_3=5^{\frac{1}{3}}\omega^2$$

其中ω是1的异于1立方根之一，作这三个根的函数，可以看到此方程在Q中的珈罗华群$\mathscr{G}(K,F)$为

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

再作根的有理函数

$$\omega=\frac{x_2}{x_1}=\frac{x_3}{x_2},$$

使ω的值保持不变的变换，除e外，为(123)，(132)．因而这三个置换构成$\mathscr{G}(K,F)$的子群：

$$H=\{e,(123),(132)\}.$$

将$\omega=\frac{x_2}{x_1}=\frac{x_3}{x_2}$加进$F=Q$后，得扩域$Q(\omega)$．由于$x_1\omega=x_2$，$x_3=x_2\omega$，可以看到，在扩域$Q(\omega)$上$f(x)$的珈罗华群，恰是$H=\{e,(123),(132)\}$，进一步将$5^{\frac{1}{3}}$加进$Q(\omega)$，得$Q(\omega,5^{\frac{1}{3}})=K$，于是相应的珈罗华群就变为$\{e\}$了．

另一方面，如果所作的有理函数为

$$\psi=x_1=5^{\frac{1}{3}}.$$

那末使ψ保持不变的置换，除e以外，只有(2 3)，因而$H'=\{e,(2\ 3)\}$.

将$\varphi=x_1=5^{\frac{1}{3}}$加进$Q$，得扩域$Q(5^{\frac{1}{3}})$．这样，在$Q(5^{\frac{1}{3}})$上的珈罗华群就是$H'=\{e,(2\ 3)\}$

将上面的具体结果抽象成下面的命题．

设给定一个方程$f(x)=0$，它的系数属于数域F，相应的珈罗华群为$\mathscr{G}(K,F)$，如果我们把经$\mathscr{G}(K,F)$的子群H作用后保持不变的方程的根的有理函数ψ加进域F，使域F扩充为域$F(\psi)$，则相应的珈罗华群就收缩为H．这样一步一步地把方程的根的有理函数加进系数域F中去，相应的珈罗华群就逐步缩小为$\{e\}$，这时候方程在扩充后的域中是可以分解因式的，于是方程在这个域上

有根，问题是这个根是否可用根式来表示，换句话说，所添加的根的有理函数 ψ 是否可用根式来表示，下段将说明，如果相应的群 H 是元数为素数的循环群，这是可能的.

[7] 现在就紧接着上段，来谈谈解决我们的问题中又一个重要步骤.

先谈一下元数为素数 p 的循环群，它就是由如下形式的轮换.

$$s=\begin{pmatrix}1 & 2 & \cdots & p-1 & p\\ 2 & 3 & \cdots & p & 1\end{pmatrix} \text{ 即 } (1\ 2\ 3\ \cdots\ (p-1)\ p)$$

产生的循环群，其中 p 为素数，这个循环群的元数显然是素数 p.

$s=(1\ 2\ \cdots\ (p-1)\ p)$ 的周期为 p: $s^p=e$, 又

$$s=(1\ 2\cdots(p-1)\ p)=(1\ 2)(1\ 3)\cdots(1\ (p-1))(1\ p),$$

其中对换的个数为 $p-1$，在 p 为大于 2 的素数时 $p-1$ 显然为偶数，所以 s 为偶置换，它的各次幂自然也是偶置换.

其次，要谈一下与元数为素数的循环群有关的一个重要结果.

一个 p（p 为素数）次代数方程 $f(x)=0$，如果在基本域 F 中加进 1 的 p 次原根后的扩域 F' 上，它的珈罗华群 $\mathcal{G}(K,F')$ 是元数为素数 p 的循环群，那末它在 F' 中可用根指数小于或等于 p 的根式来解.

现在对这个结果作一些说明，先引进一个概念：

方程 $$x^p-1=0$$

有 p 个根，叫做 1 的 p 次根，现在来看这些 p 次根是什么样的？我们知道，上式可以写成复数形式

$$z^p-1=0,\ \text{或}\ z^p=1,$$

令 $z=r(\cos\alpha+i\sin\alpha)$，于是

$$z^p=r^p(\cos\alpha+i\sin\alpha)^p.$$

按照棣美弗公式 $(\cos\alpha+i\sin\alpha)^p=\cos p\alpha+i\sin p\alpha$，得

$$z^p=r^p(\cos\alpha+i\sin\alpha)^p=r^p(\cos p\alpha+i\sin p\alpha).$$

因为 1 可写成 $1^p(\cos 0+i\sin 0)$的形式，所以

$$r^p=1^p, \text{即 } r=1, \cos p\alpha+i\sin p\alpha=\cos 0+i\sin 0,$$

即
$$p\alpha=0+2k\pi, \qquad \alpha=\frac{2k\pi}{p}.$$

给 k 以 $0,1,\cdots,p-1$ 等数值，即得 1 的 p 个 p 次根：

$$\cos\frac{2k\pi}{p}+i\sin\frac{2k\pi}{p}, \quad k=0,1,\cdots,p-1.$$

一般地讲，设 m 为自然数，在

$$x^m-1=0$$

的 m 个根中，只有 m 次自乘才能等于 1 的那些 m 次根，叫做 1 的 m 次原根. 因此在我们的问题 $x^p-1=0$ 中，记其一个原根（例如 $\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$）为 ρ，则可以验证，1 的所有 p 个 p 次根为

$$1,\rho,\rho^2,\cdots,\rho^{p-1}.$$

例如 1 的三次原根为 ω,ω^2，而它的三次根是

$$1,\rho=\omega,\rho^2=\omega^2; \quad \text{或} \quad 1,\rho=\omega^2,\rho^2=(\omega^2)^2=\omega.$$

1 的四次原根为 $i,-i$，而它的四次根是

$$1,\rho=-i,\rho^2=(-i)^2=-1,\rho^3=(-i)^3=i;$$

或
$$1,\rho=i,\rho^2=(i)^2=-1,\rho^3=(i)^3=-i.$$

因为已知(素数) p 次方程 $f(x)=0$ 在 F' 上的珈罗华群$\mathcal{G}(K,F')$是元数为素数 p 的循环群，那末它是由轮换

$$s=(1\ 2\cdots p)$$

生成的 p 个置换的群，显然 $s^p=e$.

利用 $1,\rho,\rho^2,\cdots,\rho^{p-1}$ 作线性方程组如下：

$$\begin{aligned}
&x_1+x_2+\cdots+x_p=a_0,\\
&x_1+\rho x_2+\rho^2x_3+\cdots+\rho^{p-1}x_p=a_1,\\
&\cdots\cdots\cdots\\
&x_1+\rho^kx_2+\rho^{2k}x_3+\cdots+\rho^{(p-1)k}x_p=a_k,
\end{aligned} \tag{1}$$

$$\cdots\cdots\cdots$$

$$x_1+\rho^p x_2+\rho^{2p}x_3+\cdots+\rho^{(p-1)p}x_p=a_{p-1},$$

这里 $x_1,x_2,\cdots,x_p$ 为 p 次方程 $f(x)=0$ 的 p 个根.

显然,(1)的第一式就是 p 次方程 $f(x)=0$ 的展开式中 x^{p-1} 项的系数的负数. 至于其余的 a_k 是什么,下面就给予说明.

对(1)作轮换 $s\in\mathscr{G}(K,F')$, 这时第一式显然不变, 现在看其他各式的变化情况,例如,以 s 作用于

$$x_1+\rho^k x_2+\rho^{2k}x_3+\cdots+\rho^{(p-1)k}x_p=a_k,$$

这时此式左边变成:

$$x_2+\rho^k x_3+\rho^{2k}x_4+\cdots+\rho^{(p-2)k}x_{p-1}+\rho^{(p-1)k}x_1.$$

这是因为在 F' 上,按照珈罗华群的性质, ρ 在 s 的作用下保持不变(见[6],例4),所变更的只是 $x_i(i=1,2,\cdots,p)$.

然而用 ρ^{-k} 乘 a_k 的等式,也会得同样的结果:

$$\rho^{-k}x_1+\rho^{-k}\rho^k x_2+\rho^{-k}\rho^{2k}x_3+\cdots+\rho^{-k}\rho^{(p-1)k}x_p=\rho^{-k}a_k,$$

化简, 得

$$\rho^{-k}x_1+x_2+\rho^k x_3+\cdots+\rho^{(p-2)k}x_p=\rho^{-k}a_k.$$

这里因为(注意 $\rho^p=1$)

$$\rho^{(p-1)k}x_1=\rho^{pk}\cdot\rho^{-k}x_1=(\rho^p)^k\cdot\rho^{-k}x_1=(1)^k\cdot\rho^{-k}x_1=\rho^{-k}x_1.$$

于是 s 将 a_k 变成 $\rho^{-k}a_k$.

现在作 a_k 的 p 次幂 $a_k^p=u$. 以 s 作用于 u,得

$$(x_2+\rho^k x_3+\cdots+\rho^{(p-1)k}x_p)(x_2+\rho^k x_3+\cdots+\rho^{(p-1)k}x_p)\cdots$$

$$(x_2+\rho^k x_3+\cdots+\rho^{(p-1)k}x_p)$$

(共 p 个因式)

这相当于

$$(\rho^{-k}a_k)(\rho^{-k}a_k)\cdots(\rho^{-k}a_k)=(\rho^{-k}\cdot a_k)^p=(\rho^{-k})^p a_k^p=a_k^p,$$

(共 p 个因式)

也就是说,以置换 s 作用于 a_k^p,保持 a_k^p 不变.

由于 k 是任意的,所以 s 不改变所有的 a_k^p, 即不改变 a_0^p,a_1^p,

$\cdots, a_k^p, \cdots, a_{p-1}^p$，又由于 $f(x)=0$ 的珈罗华群的所有 p 个元素都是由 s 生成的，所以珈罗华群$\mathscr{G}(K, F')$的一切元素不改变每一个 a_k^p. 这样每个 a_k^p 的值必为 F' 中的某个数 u_k，于是a_k是u_k的 p 次根，即 $a_1, \cdots, a_{p-1}$ 是 F' 中相应的数的 p 次根：$\sqrt[p]{u_1}, \cdots, \sqrt[p]{u^p{}_{-1}}$. 同时由本段上面的说明，已知 1 的 p 次根为：

$$\rho=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p};\ \rho^l=\cos l\frac{2\pi}{p}+i\sin l\frac{2\pi}{p};$$

（l 为 $1, \cdots, p-1$中的数）.

(1)的线性方程组是由 ρ 与 a_k 来表示的，解这个线性方程组，就得到$x_1, x_2, \cdots, x_p$的解，这个解是由$a_0, a_1=\sqrt[p]{u_1}, \cdots, a_{p-1}=\sqrt[p]{u_{p-1}}$与$\rho, \cdots, \rho^{p-1}$来表示的，所以可以用根式来解，而且根指数$\leqslant p$.

下面就对一个具体例子，应用上面的说法，以引导出判别方程可否用根式来解的结果.

设方程 $f(x)=x^4-x^2+1=0$. 由于 $x^4-x^2+1=(x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1)$，$\sqrt{3}\notin Q$，所以在 Q 上 $f(x)$不可能分解因式，它的四个根为

$$x_1=\frac{\sqrt{3}+i}{2},\ x_2=\frac{\sqrt{3}-i}{2},\ x_3=-\frac{\sqrt{3}+i}{2},\ x_4=-\frac{\sqrt{3}-i}{2}.$$

可以算得，$f(x)=x^4-x^2+1=0$ 在 $F=Q$ 上的珈罗华群 $\mathscr{G}(K, F)$为

$$\{e, (12)(34), (13)(24), (14)(23)\}.$$

作根的有理函数

$$x_1+x_2=\sqrt{3},\qquad x_3+x_4=-\sqrt{3},$$

保持这两个函数不变的置换为 e，$(12)(34)$，将$\sqrt{3}$ 加进 Q，得 $Q(\sqrt{3})$，使在$Q(\sqrt{3})$上$\mathscr{G}(K, F)$退化为正规子群：

$$H_1=\{e, (12)(34)\}.$$

再作根的有理函数：

$$\psi_1=x_1x_4=-\left(\frac{\sqrt{3}+i}{2}\right)^2;\qquad \psi_2=x_3x_2=-\left(\frac{\sqrt{3}-i}{2}\right)^2;$$

保持此两函数不变的群$\mathscr{G}(K,F)$中的置换为 e 与(14)(23).

利用 x_1x_4, x_2x_3 作辅助函数

$$y^2+\psi_1=y^2+x_1x_4=0,\quad y^2+\psi_2=y^2+x_2x_3=0;$$

ψ_1,ψ_2 不在 Q 中,也不在$Q(\sqrt{3})$中,所以对换 ψ_1, ψ_2 时就要改变其值, 因而这个新方程在$Q(\sqrt{3})$ 上的珈罗华群 Γ 为 $\{e,(\psi_1,\psi_2)\}$. 这里(ψ_1,ψ_2)即 ψ_1 与 ψ_2 对换.

这个Γ恰与$\mathscr{G}(K,F)/H_1$——$\{e,(14)(23)\}(\mathrm{mod}H_1)$同构. Γ 是元数为素数的循环群,是可用根式来解的,而这两辅助函数与原方程等价,所以原方程可以用根式来解.

将 x_1x_4 (x_2x_3) 的值 $-\left(\frac{\sqrt{3}+i}{2}\right)^2\left(-\left(\frac{\sqrt{3}-i}{2}\right)^2\right)$, 加进$Q(\sqrt{3})$,得$Q(\sqrt{3},i)$,$H_1$ 即退化为$\{e\}$,这时原方程在$Q(\sqrt{3},i)$上可用根式来解.

从这个关于方程可用根式来解的例子, 我们得到一个很有启发性的图式: 当此方程可用根式来解时,有

$$\mathscr{G}(K,F)\supset H_1(\text{正规子群})\supset e;$$

$$\frac{\mathscr{G}(K,F)\text{的元数}}{H_1\text{的元数}}=2,\text{素数},\quad \frac{H_1\text{的元数}}{\{e\}\text{的元数}}=2,\ \text{素数};$$

辅助函数的群Γ同构于商群$\mathscr{G}(K,F)/H_1$.

有了这些,就可以谈论可解群与方程可否用根式来解的问题了.

[8] 先说一下最大正规子群的概念:

一个群G的所谓真正最大正规子群 H, 是这样的正规子群 $H\subset G, H\neq\{e\}$,它不包含在任何一个更大的真正正规子群之中.

现在讲可解群:

设有群G, G 有真正的最大正规子群 H_1, H_1 又有真正的最大正规子群 H_2,…如此类推,经有限步以后得到 H_{n-1} 的最大正规子

群 $H_n=\{e\}$. 这样就有一个子群的序列

$$G\supset H_1\supset H_2\cdots\supset H_{n-1}\supset H_n=\{e\},$$

这里H_i为$H_{i-1}(1\leqslant i\leqslant n)$的正规子群,再作商群的序列

$$G/H_1,\ H_1/H_2,\ \cdots,\ H_{n-2}/H_{n-1},H_{n-1}/H_n;$$

分别得指数

$$u_1,\ u_2,\ \cdots,\ u_{n-1},\ u_n;$$

这叫做合成因子.

如果合成因子都是素数,就说群G是可解的;否则就是不可解的.

如果一个代数方程对域F的珈罗华群$\mathscr{G}(K,F)$是可解群,那末此方程可以相对于F用根式来解.

例如,一般四次方程,它在F中的珈罗华群$\mathscr{G}(K,F)$为四次对称群S_4. S_4的元数为$4!=24$. (如果是具体的四次方程,其珈罗华群可能是S_4的子群.) 而S_4有最大正规子群为偶置换所成的群,即交代群A_4,$H_1=A_4$,A_4的元数为12. A_4又有最大正规子群H_2

$$H_2=\{e,(12)(34),(13)(24),(14)(23)\},$$

H_2的元数为4. H_2又有最大正规子群$H_3=\{e,(12)(34)\}$. (或$\{e,(13)(24)\}$,或$\{e,(14)(23)\}$). H_3的元数为2. H_3有唯一的正规子群$H_4=\{e\}$,所以得到子群序列:

$$\mathscr{G}(K,F)=S_4\supset H_1\supset H_2\supset H_3\supset H_4=\{e\};$$

H_i是$H_{i-1}(1\leqslant i\leqslant 4)$的正规子群. 相应的合成因子是

$$2,\ 3,\ 2,\ 2;$$

它们都是素数(S_4为可解群),所以四次方程的群是可解群,从而四次方程在F中可用根式来解,这在开始时已经说明.

又例如,一般的五次代数方程

$$f(x)=x^5+a_1x^4+\cdots+a_5=0,$$

其中文字 a_1, a_2, a_3, a_4, a_5 属于某个 F，且相互独立.

此方程的珈罗华群$\mathscr{G}(K,\ F)$是对称群 S_5，S_5 的元数是 120. 它的最大正规子群为交代群 A_5，即 $H_1 = A_5$，A_5 的元数为 60，但是如上节所说，A_5 为单群，因此，相应的子群序列为

$$\mathscr{G}(K,F) = S_5 \supset A_5 \supset \{e\}.$$

相应的合成因子为

$$120/60 = 2, \qquad 60/1 = 60;$$

60 不是素数，所以群$\mathscr{G}(K,F)$是不可解群. 相应的一般五次代数方程在 F 中不可用根式来解，从而五次以上的一般代数方程也不可用根式来解.

利用珈罗华群的理论还可证明，一般不能用圆规与直尺三等分一个任意角的问题.

有了此节冗长的说明，关于群的巨大威力就无须再说什么了.

从理论上证明五次以上的一般代数方程不能用根式来解，是阿贝尔、珈罗华，特别是珈罗华的功绩，正因为如此，为了纪念他而将上面所说的那个群叫做珈罗华群.

附　录

为了说明壹到叁及肆一中有关理论的应用，现引用下文作为一综合例题，以供读者参考。

群在九层镂空球中的应用

我国象牙雕或玉雕九层镂空球是一种极其精致、美丽的工艺品，它表现了我国劳动人民的高度智慧和高超技艺．不仅如此，如果我们对它从数学的角度作些规定，那么从这种球里面还可看到一个群，这些规定是：

1．假定九个球都是同心球；

2．任何一个球的运动都是独立的，即任何一个球的运动，都不影响在它里面或外面的球的运动．

3．假定九个球面上的花色都是(1)元宝形、(2)心形、(3)菱形、(4)梅花、(5)星形、(6)圆形，每个球上各有一个；并且今后就按上述次序编号．这六个花色位于以球心 O 为轴心的三维笛卡尔坐标系的横轴、纵轴、竖轴与球面的交点上．这些交点就以 1、2、3、4、5、6 来标记．

4．以最外层球不动，作为定位球．任何一层球的运动，都以它面上的任一个花色对准定位球的某一个花色(不一定相同)，才算合乎要求的运动．

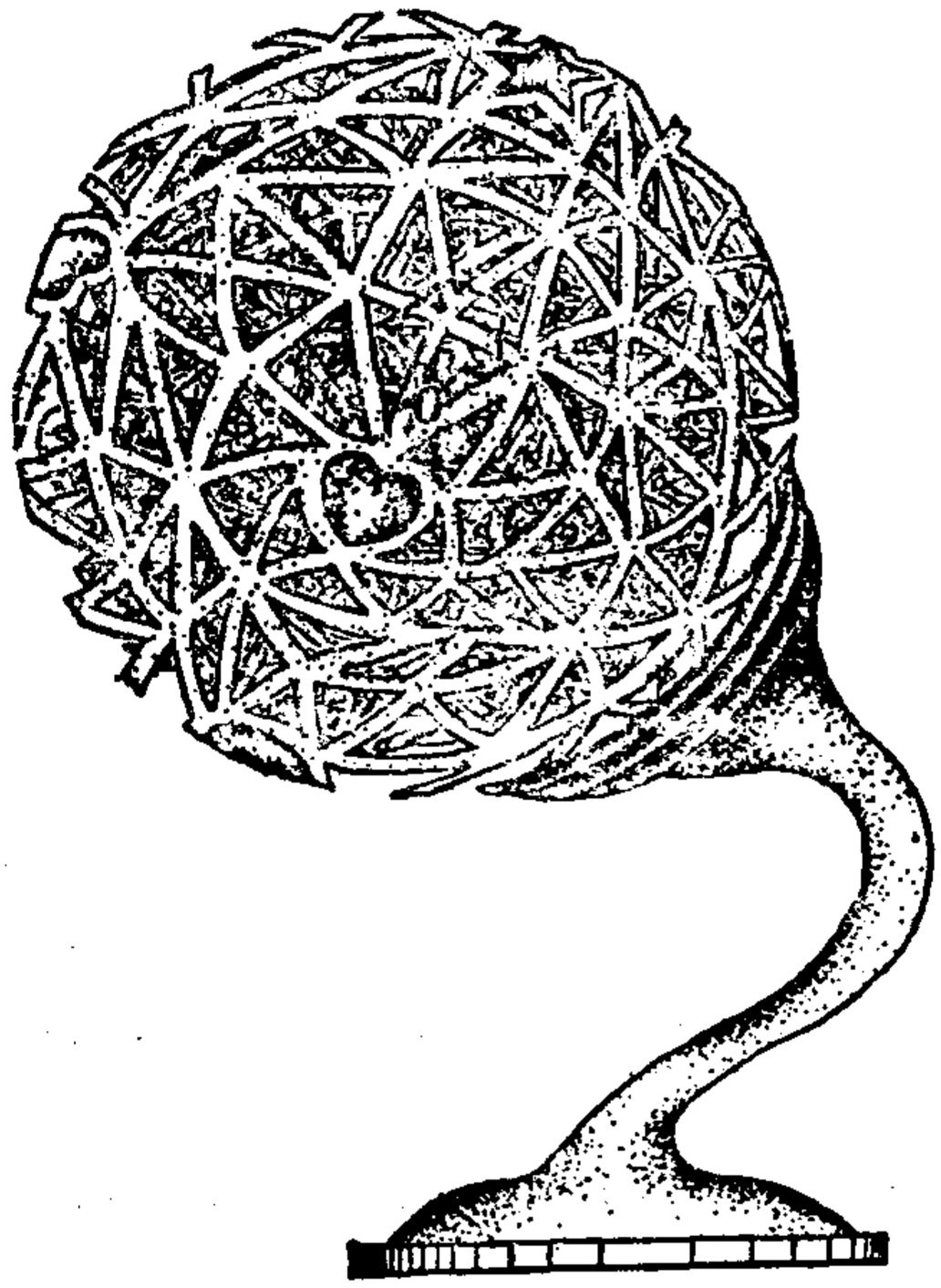
作图中每一个球的三个大圆的弦，以连接 1、2；2、3；3、4；4、1；5、2；2、6；6、4；4、5；1、6；6、3；3、5；5、1；这样就得到正八面体．

按照上面的规定，九层球的每一层球的运动，就是正八面体的运动；按照一般的数学书的说法，可以证明，它们是：

以 5、6；1、3；2、4 的联线为轴的转动，这种转动每次转 90°，得到三个子群：

(1){(1 2 3 4)}；(2){(2 6 4 5)}；(3){(5 3 6 1)}．它们是环循群，元数都为 4．以相对的棱边 35、16；15、63；12、34；23、14；54、26；46、25 之中

本文曾以蚓深署名在《教材通讯》1985 年第一期上发表．



点联线为轴，各作 180°的转动，得到六个子群；

(1){(35) (61) (24)}；(2){(15) (63) (24)}；(3){(12) (34) (56)}；

(4){(23) (14) (56)}；(5){(54) (26) (13)}；(6){(46) (25) (13)}；

它们是环循群，元数都是 2.

以相对的正三角形△235，△146；△236，△154； △125， △346； △126，△345 的中心之联线为轴每次作 120°的旋转，得 4 个子群：

(1){(253) (614)}；(2){(236) (415)}；(3){(346) (251)}；

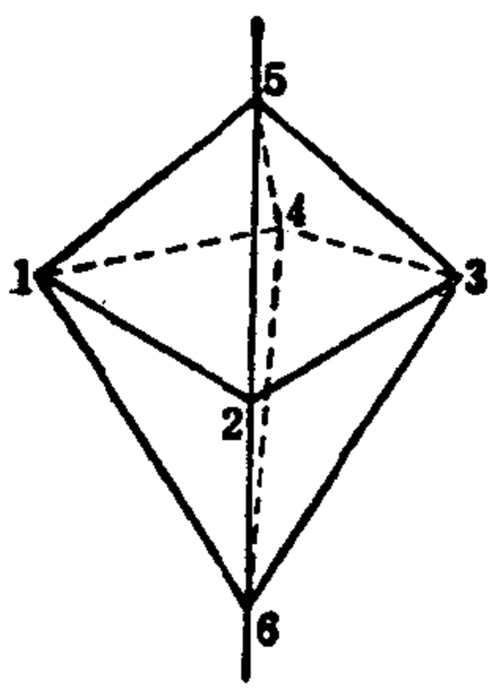
(4){(612) (345)}；

它们也是环循群，元数是 3.

在任一层球面上. 上述三种子群一起结合而成群，这个群的元数 $24=2^3\cdot 3$. 2 为素数，按照97页的定理与推论，元数为$n=ap^m$的群，其中 p 为素数 $a\not\equiv 0(\mathrm{mod}p)$，$m$为自然数，必有 p^m 元子群，本题里 $n=24, a=3, p=2, m=3$. 所以，这个群至少有一个 $2^3=8$ 元子群，可以验证，它是：

$$\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}=\mathrm{e},(13)(24),(24)(56),(13)(56),$$

$$(12)(34)(56),(14)(23)(56),(1234),(1432).$$



它有由偶置换组成的 12 元子群:

$$e,(13)(24),(24)(56),(13)(56),(253)(614),(236)(415),$$
$$(346)(251),(612)(345),(352)(641),$$
$$(632)(514),(152)(643),(543)(216),(a)$$

至于它有 4 元子群、2 元子群则是很明显的.

现在将各层球上的运动相结合,例如:

第一层球的运动(因它是定位的,始终不动)$\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$;

第二层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\2&3&4&1&5&6\end{pmatrix}$;

第三层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\1&6&3&5&2&4\end{pmatrix}$;

第四层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\5&4&6&2&1&3\end{pmatrix}$;

第五层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\3&5&1&6&2&4\end{pmatrix}$;

第六层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$;

第七层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\4&5&2&6&3&1\end{pmatrix}$;

第八层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\3&4&1&2&5&6\end{pmatrix}$;

第九层球的运动 $\begin{pmatrix}1&2&3&4&5&6\\4&1&2&3&5&6\end{pmatrix}$;

可以将这种结合看作是九层球的一个运动,但这样的写法很烦琐,为了简化

写法，引进下列的记号来代替它：

$$\begin{array}{|cccccc|}
\hline
1 & 2 & 3 & 4 & 5 & 6 \\
2 & 3 & 4 & 1 & 5 & 6 \\
1 & 6 & 3 & 5 & 2 & 4 \\
5 & 4 & 6 & 2 & 1 & 3 \\
3 & 5 & 1 & 6 & 2 & 4 \\
1 & 2 & 3 & 4 & 5 & 6 \\
4 & 5 & 2 & 6 & 3 & 1 \\
3 & 4 & 1 & 2 & 5 & 6 \\
4 & 1 & 2 & 3 & 5 & 6 \\
\hline
\end{array}, \qquad (1)$$

即是说，把各层之置换的第一行都省略掉，由第一行的自然顺序排列 123456 统一代行九个置换的第一行的任务．并将这种记号姑且叫做 9 层 6 次置换．

这种多层的置换的乘法，实际上就是置换乘法，例如：

$$\begin{array}{|cccccc|}
\hline
1 & 2 & 3 & 4 & 5 & 6 \\
2 & 3 & 4 & 1 & 5 & 6 \\
1 & 6 & 3 & 5 & 2 & 4 \\
5 & 4 & 6 & 2 & 1 & 3 \\
3 & 5 & 1 & 6 & 2 & 4 \\
1 & 2 & 3 & 4 & 5 & 6 \\
4 & 5 & 2 & 6 & 3 & 1 \\
3 & 4 & 1 & 2 & 5 & 6 \\
4 & 1 & 2 & 3 & 5 & 6 \\
\hline
\end{array}
\cdot
\begin{array}{|cccccc|}
\hline
1 & 2 & 3 & 4 & 5 & 6 \\
5 & 2 & 6 & 4 & 3 & 1 \\
4 & 3 & 2 & 1 & 6 & 5 \\
2 & 5 & 4 & 6 & 1 & 3 \\
2 & 6 & 4 & 5 & 3 & 1 \\
1 & 6 & 3 & 5 & 4 & 2 \\
4 & 1 & 2 & 3 & 5 & 6 \\
2 & 1 & 4 & 3 & 6 & 5 \\
2 & 3 & 4 & 1 & 5 & 6 \\
\hline
\end{array}, \qquad (2)$$

乘法是：将左边第一、二行作为一个置换与右边第一、二行作为一置换相乘：

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 3 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & 1 \end{pmatrix};$$

接着右边第一、三行作为一置换与右边第一、三行作为一置换相乘

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 5 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix};$$

依此类推，结果得

$$\begin{array}{|cccccc|}
\hline
(1)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(2)\ 2 & 6 & 4 & 5 & 3 & 1 \\
(3)\ 4 & 5 & 2 & 6 & 3 & 1 \\
(4)\ 1 & 6 & 3 & 5 & 2 & 4 \\
(5)\ 4 & 3 & 2 & 1 & 6 & 5 \\
(6)\ 1 & 6 & 3 & 5 & 4 & 2 \\
(7)\ 3 & 5 & 1 & 6 & 2 & 4 \\
(8)\ 4 & 3 & 2 & 1 & 6 & 5 \\
(9)\ 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
\end{array}. \qquad (3)$$

这仍是一9层6次置换. 多层置换的好处就在于,经过它可以一眼看穿, 与定位球上每个花色相对的在各层球上是什么花色, 例如, 上面这9层置换表示与定位球上4号即梅花对应的.第二层球是星形,第三层球是圆,第四层球是星形,第五层球是元宝,第六层球是星形,第七层球是圆,第八层球是元宝,第九层球是梅花等等. 可以看到不变的9层6次置换,即中性元是

$$\begin{array}{|cccccc|}
\hline
(1)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(2)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(3)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(4)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(5)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(6)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(7)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(8)\ 1 & 2 & 3 & 4 & 5 & 6 \\
(9)\ 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
\end{array} = \mathbf{e}. \qquad (4)$$

九层球上的9层6次置换(这种元素)的集合，关于9层置换乘法是封闭的，满足结合律,且存在每个元的逆元. 因而九层球上的9层6次置换元素的集合对于它的乘法构成一有限群 $\Gamma_{9,6}$. 此群的元数为$24^8=2^{24}\cdot 3^8=1100,7531,4176$. 即九层镂空球共有一千一百亿七千五百三十一万四千一百七十六种状态,可以说是千姿百态,令人叹为观止.

多层的置换例如在大型交响乐队分层次排坐位中也可应用.

如果将置换写成对换、轮换之积的形式，多层置换的写法还可简化. 这时第一行的自然顺序排列可以不必写出,于是(1)可以写作

$$\begin{matrix}(2)\\(3)\\(4)\\(5)\\(6)\\(7)\\(8)\\(9)\end{matrix}\left|\begin{matrix}(1234)\\(2645)\\(15)\,(24)\,(36)\\(13)\,(25)\,(46)\\e_6\\(146)\,(253)\\(13)\,(24)\\(1432)\end{matrix}\right| \tag{5}$$

其中 e_i 是 i 层的中性元. 于是9层6次置换乘法,例如(2)可写作:

$$\begin{matrix}(2)\\(3)\\(4)\\(5)\\(6)\\(7)\\(8)\\(9)\end{matrix}\left|\begin{matrix}(1234)\\(2645)\\(15)\,(24)\,(36)\\(13)\,(25)\,(46)\\e_6\\(146)\,(253)\\(13)\,(24)\\(1432)\end{matrix}\right|\cdot\left|\begin{matrix}1536)\\(14)\,(23)\,(56)\\(125)\,(346)\\(126)\,(345)\\(26)\,(45)\\(1432)\\(12)\,(34)\,(56)\\(1234)\end{matrix}\right|=\left|\begin{matrix}(126)\,(345)\\(146)\,(253)\\(2645)\\(14)\,(23)\,(56)\\(26)\,(45)\\(13)\,(25)\,(46)\\(14)\,(23)\,(56)\\e_9\end{matrix}\right|, \tag{6}$$

此式左边第一、二两记号内同一行按置换乘法相乘,而得右边的同一行中的置换. 这种写法在计算9层6次置换的乘法时确实比(2)的写法简单. 但不如(2)、(3)那样可一眼看穿对应情况.

上面说到的群 $\Gamma_{9,6}$ 实际上是一个更大的群的子群. 现在就暂时把九层镂空球上的群放在一边,来看这个更大的群.

设已给定象上面那样的9层6次置换的集合:除第一层作为定位的标志以外,从第二层至第九层,每一层的所有6次置换组成一对称群 S_6,它的元素的个数为

$$6!=720.$$

将每一层的各个置换与其他各层的各个置换做各种可能的结合,则所有9层6次置换的个数为

$$720^8.$$

这 720^8 个9层6次置换作为元素组成一有限群 $S_{9,6}$,上面说的9层镂空球上的群 $\Gamma_{9,6}$ 就是 $S_{9,6}$ 的子群.

在普通的置换情形,有奇置换与偶置换之分,9层6次置换的情形就比较复杂. 但是我们仍然可以对此做一些探索. 现在就尝试着引进下面的三

个概念. 请注意第一层不运动，是定位的，不计其奇偶性. 犹如置换中第一行的作用.

9层6次全偶置换，是指每一层都是偶置换，这里包括 e，见(4)

9层6次全奇置换，是指每一层都是奇置换；

9层6次奇偶混合置换，是指各层既可以是奇置换又可以是偶置换，并且必然是两者兼有.

可以看到，在这9层6次置换的群 $S_{9,6}$ 里，9层6次全偶置换的个数为：360^8

这些9层6次全偶置换的全体对所定义的9层6次置换乘法是封闭的，且满足其他三个要求，因而构成9层6次置换群 $S_{9,6}$ 的 360^8 元子群.

在九层镂空球上的群 $\Gamma_{9,6}$ 也有类似的情况. 例如 $\Gamma_{9,6}$ 的9层全偶置换的全体就是由上面(a)式的偶置换在第二层至第九层上各种可能结合所构成的，它是 $\Gamma_{9,6}$ 的子群，共有元数

$$12^8=429981696.$$

$S_{9,6}$ 的9层6次全奇置换的个数同样是 360^8.

$S_{9,6}$ 的9层6次奇偶混合置换的个数是

$$720^8-2.360^8.$$

对这些9层6次奇偶混合置换又可以进行分类，例如

第二层奇，其余为偶的一类；

.....

第二、五层奇，其余为偶的一类；等等. 这些类的数目为几？现进行计算.

假设置换为奇以 -1 代表，置换为偶以 1 代表. 每一层为 -1 或为 1，只有两种可能的选择，现在有8层来进行这种选择，因而可供选择的总数是

$$2^8=256.$$

这256种类型中包括9层6次全偶置换的全体(作为一种类型)，将后者记作

$$E[1,1,1,1,1,1,1,1];$$

也包括9层6次全奇置换的全体(作为一种类型)，将此九层全奇置换的全体记作

$$O[-1,-1,-1,-1,-1,-1,-1,-1].$$

9层6次奇偶混合置换，例如上面提到的两个类型元素的全体分别记作

$$M[1,-1,1,1,1,1,1,1]$$

$$M[1,-1,1,1,-1,1,1,1],$$

$M[1,-1,1,1,-1,1,1,1]$中所含同类元素的个数是

$$360^2\times 360^6=360^8,$$

其他每一类九层奇偶混合置换的元素的个数也是

$$360^k\times 360^{(8-k)}=360^8,$$

这里k为含奇置换的层数

可以验证$E[1,1,1,1,1,1,1,1,1]$不仅是9层6次置换群$S_{9,6}$的一个子群，而且还是一个正规子群.

如果将$S_{9,6}$就$E[1,1,1,1,1,1,1,1,1]$(以后简记作E)分为陪集系

$$S_{9,6}=E+x(-1,-1,-1,-1,-1,-1,-1,-1)E+\sum_{\substack{i,j=+1,-1\\ j=2,3,\cdots,9}} y(\cdots i_j\cdots)E \tag{7}$$

这里$x(-1,-1,-1,-1,-1,-1,-1,-1,)$为$O[-1,-1,-1,-1,-1,-1,-1,-1,-1]$中的任意元素；$y(\cdots i_j\cdots)$，$i_j=+1,-1$，$j=2,3,\cdots 9$，为9层奇偶混合置换的某一确定类型中的任意元素，但不是全奇，也不是全偶.

在这个分解式(7)中，E在$S_{9,6}$中的指数为256.

令每一个奇偶类型中的任一元素都对应于表示这类型的记号，例如

$$\varphi: y[1,1,-1,-1,1,1,1,-1)\mapsto[1,1,-1,-1,1,1,1,-1],$$

并定义类型记号间的乘法是：右边记号中各个位号上的数字与左边记号中相应位号上的数字按普通的数的乘法相乘，例如

$$[1,1,-1,-1,1,1,1,-1]\cdot[-1,-1,1,1,-1,-1,-1,1]=$$
$$=[1\cdot(-1),1\cdot(-1),(-1)\cdot 1,(-1)\cdot 1,1\cdot(-1),1\cdot(-1),1\cdot(-1),$$
$$(-1)\cdot 1]$$
$$=[-1,-1,-1,-1,-1,-1,-1,-1]$$

可以看出映射φ是同态映射，9层置换在同态映射φ下的像：

$$[i_2,i_3,\cdots,i_9]$$
$$i_k=-1\ \text{或}\ 1,k=2,3,\cdots,9,$$

按规定的运算组成一个群，它的单位元是

$$[1,1,1,1,1,1,1,1],$$

每一元素是它自己的逆元. 这个群的元素(除单位元外)的阶均为2.

这个群与二元群$\{-1,1\}$类似，在某种意义上，可说是$\{-1,1\}$的推广.

上面的探讨很不成熟，望读者批评指正.

在写这本小书时参考或取材于下列各书：

张禾瑞、郝炳新：《高等代数》第一版，人民教育出版社.

园正造：《群论》，第君绛译，商务印书馆.

王湘浩，谢邦杰：《高等代数》，高等教育出版社.

比索等：《普通数学》第一卷，邓应生译，高等教育出版社.

奎耐：《高等数学基本教程》第一卷，胡作玄，郭书春译，高等教育出版社.

L. R. Lieber：《伽罗华与群论》.

E. J. Budden：《*The Fascination of Croups*》Cambridge university Press, 1978.

W. Burnside：《*Theory of Groups of Finite order*》Dover Publ ication Inc. 1955.

H. Boerher：《*Darstellungen Von Gruppen*》Springer Verlag, 1955.

R. Kochendorffer：《*Lebrbuch der Gruppentheorie*》Akademische Verlagsgesellschaft, 1966.

V. Specht：《*Gruppentheorie*》Springer Verlag, 1956.

M. Hall：《*The Theory of Groups*》Macmillan Company.

P. Dubreil M. L. Dubreil-Jacotion

《*Lecons d'algebre moderne*》Dunod, 1961.

А. Г. Курош：«Теория Групп» изд. «Hayka» 1967.

L. E. Dickson：《*Modern Algebraic Theories*》

M. M. Postnikov：《*Foundation of Galois Theory*》

[General Information]
书名=漫话群
作者=邓应生编
页数=137
SS号=10068993
出版日期=

目录
正文