# The Radical Solutions of Algebraic Equation and Galois Theory

HIT

数学·统计学系列

# 代数方程的根式解及伽罗瓦理论

谢彦麟 编著

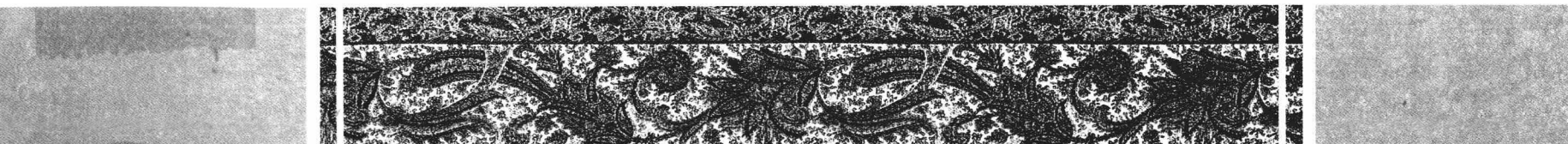
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

The Radical Solutions of Algebraic Equation and Galois Theory

# 代数方程的根式解及伽罗瓦理论

● 谢彦麟 编著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS



## 内容提要

本书是一位大学分析学教授在学习伽罗瓦理论时的心得体会,本书以还原历史的视角,以一元方程的求根公式讲起,配以大量简单例子帮助初学者通过自学掌握伽罗瓦理论这一抽象代数中的经典内容.

本书适合大学、中学师生及数学爱好者阅读.

**图书在版编目(CIP)数据**

代数方程的根式解及伽罗瓦理论/谢彦麟编著. —哈尔滨:哈尔滨工业大学出版社,2011.3

ISBN 978-7-5603-3233-8

Ⅰ.①代… Ⅱ.①谢… Ⅲ.①代数方程 Ⅳ.①O151.1

中国版本图书馆 CIP 数据核字(2011)第 038399 号

策划编辑 刘培杰 张永芹
责任编辑 张 瑞
策划编辑 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm×1092mm 1/16 印张 10.5 字数 194 千字
版 次 2011 年 3 月第 1 版 2011 年 3 月第 1 次印刷
书 号 ISBN 978-7-5603-3233-8
定 价 28.00 元

# 序言

有关代数方程的根式解问题，如至少五次方程不存在求根公式，圆规、直尺作图可能性与代数方程是否存在多层二次实根式有关，$p$ 等分圆的作法要先把 $2\cos\frac{2\pi}{p}$ 表示为多层二次实根式……这些问题与中学数学颇有关系. 作者作为中学生、大学生、中学教师时对这些问题就颇有兴趣，多次阅读参考文献[1][2]中对这些问题的论述（未用 Galois 理论基本定理），但颇为不解，有些论述似乎懂了，但几年前才发现有错误. “文革”后作者先读研究生，后于大学任教专攻分析，无暇再顾及代数方程. 退休后才有暇在约一年半时间内专攻代数方程根式解及 Galois 理论. 但建国后出版的有关书籍都以极为抽象的近世代数理论为基础论述 Galois 理论，作者亦无心解读. 唯幸找到一本使用文言文的旧书只以多项式理论为基础论述 Galois 理论，并详述与等分圆有关的单位根，以 Galois 群的不变式导出拉格朗日（Lagrange）预解方程从而得出三、四次方程求根公式等问题. 但此书颇难阅读，一个定理用文言文几字表述，不看证明就不知其义，且多个概念表述颇为模糊，条件亦不清楚，逻辑推理、条理不清，论证常有漏洞. 作者费九牛二虎之力终于从中理解了 Galois 群，Galois 理论基本定理之意义，结合参考文献[1]-[4]弄懂上述问题的推理论证及等分圆问题（可能性，

作法). 最后重新综合整理上述文献改正其中错误,草拟出拙文《Galois 理论学习总结》系统阐述上述问题及 Galois 理论,原只供自己日后欣赏. 近闻中学新教材(选修)有介绍代数方程的根式解及 Galois 理论,故再整理上述拙文为本书供哈尔滨工业大学出版社出版,以供中学教师参考. 书中对颇抽象的概念、定理的论述尽量详尽并多举例子说明以帮助读者理解. 对"文革"后高等代数教材删去的一些内容及数论等有关预备知识亦在正文或附录中补充,故只学过高等代数课程即可阅读本书. 但代数毕竟不是作者本行,本书难免有缺点、漏洞,不是之处唯望有关专家及读者指正.

谢彦麟

华南师范大学数学科学学院

# 目录

# 排列与置换

## 第一章

有 $n$ 个(互不相同)元素的集 $N$,不妨用各元素的序号记此集的元素,即

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

设集 $N$ 的任一排列为

$$(a_1,a_2,a_3,a_4,\cdots,a_n)$$

在行列式论中已定义此排列的反序数,现记为

$$\sigma(a_1,a_2,\cdots,a_n)$$

又定义了奇(偶)排列,并证明了:

**引理 1.1** 排列中对换任二元素必改变排列的奇、偶性.

**引理 1.2** 任一排列必可经若干次(含 0 次,即不必对换)对换变成标准排列

$$(1,2,\cdots,n)$$

反之亦然,且对换次数的奇偶性与此排列的奇偶性相同.

现再证:

**引理 1.3** 集 $N$ 的所有奇、偶排列个数相同,均为 $\frac{n!}{2}$.

**证** 设 $N$ 的所有偶排列集

$$\{(a_1,a_2,a_3,a_4,\cdots,a_n):2\mid\sigma(a_1,a_2,\cdots,a_n)\}$$

(其中记号 $p\mid q$ 表整数 $p$ 能整除整数 $q$).

在每个偶排列中对换开头二元素 $a_1,a_2$，由引理 1.1 知奇排列集

$$\{(a_2,a_1,a_3,a_4,\cdots,a_n):2\nmid\sigma(a_1,a_2,\cdots,a_n)\}$$

（其中记号 $p\nmid q$ 表整数 $p$ 不能整除整数 $q$）.

显然不同的偶排列经此对换得不同的奇排列；又任一奇排列

$$(b_1,b_2,b_3,b_4,\cdots,b_n)$$

必可由一个偶排列 $(b_2,b_1,b_3,b_4,\cdots,b_n)$ 对换开头二元素 $b_2,b_1$ 而得，故所有偶排列与所有奇排列有一一对应关系，其总个数相同，显然都等于 $\frac{n!}{2}$ 个.

设

$$N=\{a_1,a_2,\cdots,a_n\}$$

$(a_1,a_2,\cdots,a_n$ 为 $1,2,\cdots,n$ 的一排列），作一一映射

$$a_i\to b_i\quad(i=1,2,\cdots,n)$$

即把每个元素 $a_i$ 变成 $N$ 中某一元素 $b_i$（$b_i$ 可等于 $a_i$，即 $a_i$ 不变），$a_{i_1}\neq a_{i_2}$ 时 $b_{i_1}\neq b_{i_2}$（不同的 $a_i$ 变成不同的 $b_i$）. 则称此映射为 $N$ 的一个置换，记为

$$\begin{pmatrix}a_1,a_2,\cdots,a_n\\ b_1,b_2,\cdots,b_n\end{pmatrix}$$

显然 $(b_1,b_2,\cdots,b_n)$ 也是 $1,2,\cdots,n$ 的一个排列.

实际不妨取 $N$ 为标准排列 $(1,2,\cdots,n)$，则任一置换必可唯一地写成

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

例如

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

其中元素个数 $n$ 称此置换次数，此置换称 $n$ 次置换.

显然任一 $n$ 次置换对应唯一的（$n$ 个元素）排列 $(c_1,c_2,\cdots,c_n)$，反之任一（$n$ 个元素）排列 $(c_1,c_2,\cdots,c_n)$ 对应唯一的 $n$ 次置换，故 $n$ 次置换总数为 $n!$.

若 $N$ 的一个置换中有 $n-k(n-2\leqslant k\leqslant n)$ 个元素（不妨设为 $a_{k+1},a_{k+2},\cdots,a_n$）不变①，而其余元素有循环变换关系，即（不妨设）把 $a_1$ 变成 $a_2$，$a_2$ 变成 $a_3$，$a_3$ 变成 $a_4,\cdots,a_{k-1}$ 变成 $a_k$，最后的 $a_k$ 变成 $a_1$，亦即

$$\begin{pmatrix}a_1,a_2,a_3,\cdots,a_{k-1},a_k,a_{k+1},a_{k+2},\cdots,a_n\\ a_2,a_3,a_4,\cdots,a_k,\ a_1,a_{k+1},a_{k+2},\cdots,a_n\end{pmatrix}$$

则称此置换为 $a_1,a_2,\cdots,a_k$ 的轮换，特记为

$$(a_1,a_2,\cdots,a_k)$$

---

①当 $k=n$ 时无元素不变.

称 $k$ 为此轮换阶数,此轮换称为 $k$ 阶轮换. 当然此轮换亦可记为$(a_2,a_3,\cdots,a_k,a_1)$,$(a_3,\cdots,a_k,a_1,a_2),\cdots$.

元素 $a_i$ 与 $a_j$ 的对换是其特例,即二阶轮换$(a_i,a_j)$.

对排列$(a_1,a_2,\cdots,a_n)$ 进行置换$\begin{pmatrix}1,2,\cdots,n\\c_1,c_2,\cdots,c_n\end{pmatrix}$ 所得排列,记为

$$(a_1,a_2,\cdots,a_n)\begin{pmatrix}1,2,\cdots,n\\c_1,c_2,\cdots,c_n\end{pmatrix}$$

如

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

对 $N$ 先进行置换 $\sigma_1$,再进行置换 $\sigma_2$ 所得结果(又得一个置换)称之为置换 $\sigma_1$ 与置换 $\sigma_2$ 之积,记为 $\sigma_1\sigma_2$.

但有些书记为 $\sigma_2\sigma_1$. 相应把排列$(a_1,a_2,\cdots,a_n)$ 进行置换$\begin{pmatrix}1,2,\cdots,n\\c_1,c_2,\cdots,c_n\end{pmatrix}$,所得排列记为

$$\begin{pmatrix}1,2,\cdots,n\\c_1,c_2,\cdots,c_n\end{pmatrix}(a_1,a_2,\cdots,a_n)$$

如

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

(实际可直接写出结果).

**注意** 置换的乘法不适合交换律. 如

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

但

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

**定理 1.1** 除置换$\begin{pmatrix}1,2,\cdots,n\\1,2,\cdots,n\end{pmatrix}$(即各元素都不变)外,任一置换必可分解为若干($k$)个无公元素的轮换(即任二轮换中的元素互不相同,当 $k=1$ 时此置换就是一个轮换)之积,且此分解式是唯一的(不计各轮换因式的次序).

其道理很简单,可用例子说明:

设有置换

$$\begin{pmatrix}1,2,3,4,5,6,7,8,9,10\\3,5,4,1,2,6,8,10,7,9\end{pmatrix}$$

从上行第一个数 1 开始,由 1 变成 3,3 变成 4,4 变成 1,得一个轮换(1,3,4);

再从上行未取的第一数2开始，由2变成5，5变成2，又得一个轮换(2,5)；

上行未取的第一数6不变；

上行随后未取第一数7，由7变成8，8变成10，10变成9，9变成7，又得一轮换(7,8,10,9).

上行10个数已取尽，于是原置换分解为

$$(1,3,4)(2,5)(7,8,10,9)$$

显然三个轮换因式的次序可任意调换，即两两无公共元素的轮换适合乘法交换律.

此定理提供了表示置换的简式.

**定义 1.1** 在置换

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

中若排列

$$(c_1, c_2, \cdots, c_n)$$

为偶(奇)排列，则称此置换为偶(奇)置换.

恒等置换 I 是偶置换.

由引理1.3知，$n$ 次偶、奇置换总数均为 $\frac{n!}{2}$ 个.

**引理 1.4** 偶(奇)置换必可分解为偶(奇)数个对换之积.

**证** 从引理1.2知，标准排列$(1,2,\cdots,n)$经偶(奇)数次对换变成偶(奇)排列$(c_1,c_2,\cdots,c_n)$. 于是此偶(奇)置换为此偶(奇)数个对换之积.

**推论 1** 奇(偶)置换改变(不改变)排列的奇偶性，反之亦然.

**推论 2** 两偶置换之积，两奇置换之积为偶置换；奇置换与偶置换之积，偶置换与奇置换之积为奇置换.

**推论 3** 若干个置换之积，若其中奇置换个数为偶(奇)数，则此积为偶(奇)置换.

**引理 1.5** 偶(奇)阶轮换是奇(偶)置换.

**证** 易见

$$(a_1, a_2, \cdots, a_k) = (a_1, a_2)(a_1, a_3)\cdots(a_1, a_k)$$

即为 $k-1$ 个对换之积，于是偶(奇)数 $k$ 阶轮换为奇(偶)数次对换之积，但由引理1.1知对换改变排列之奇偶性，故为奇置换，再据上述推论3知所述轮换是奇(偶)置换.

**推论** 在置换用轮换因式之积的表示式中若偶阶轮换因式个数为偶(奇)数，则此置换为偶(奇)置换，反之亦然.

# 置换群

## 第二章

**定理 2.1** $n$ 次置换的乘法适合结合律：即对任何三个 $n$ 次置换 $\sigma_1,\sigma_2,\sigma_3$ 有

$$(\sigma_1\sigma_2)\sigma_3=\sigma_1(\sigma_2\sigma_3)$$

**证** 若 $\sigma_1$ 把元素 $a_{n_1}$ 变成元素 $a_{m_1}$，$\sigma_2$ 把元素 $a_{m_1}$ 变成元素 $a_{p_1}$，$\sigma_3$ 把元素 $a_{p_1}$ 变成元素 $a_{q_1}$，则 $\sigma_1\sigma_2$ 把元素 $a_{n_1}$ 变成元素 $a_{p_1}$，再由上述知 $(\sigma_1\sigma_2)\sigma_3$ 把元素 $a_{n_1}$ 变成元素 $a_{q_1}$；又由上述知 $\sigma_2\sigma_3$ 把元素 $a_{m_1}$ 变成元素 $a_{q_1}$，于是 $\sigma_1(\sigma_2\sigma_3)$ 亦把元素 $a_{n_1}$ 变成元素 $a_{q_1}$. 因 $a_{n_1}$ 可代表 $N$ 中任一元素，故定理结论得证.

同样置换乘法结合律可推广到任一个置换之积（即可任意添加括号，但不能改变各置换因式的次序）.

称置换

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

为单位置换（或恒等置换），即使各元素不变，特记为 $I$.

一般

$$\begin{pmatrix}a_1,a_2,\cdots,a_n\\a_1,a_2,\cdots,a_n\end{pmatrix}=I$$

显然

$$\sigma I = I\sigma = \sigma$$

易见 $I$ 为左(右) 乘任一置换使之不变的唯一置换.

设 $n$ 次置换

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

称置换

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

为 $\sigma$ 的逆置换,记为 $\sigma^{-1}$,则有 $\sigma^{-1} = \sigma'$.

显然 $\sigma$ 为 $\sigma'$ 的逆置换,称二置换为互逆置换.

一般

$$\begin{pmatrix} a_1, a_2, \cdots, a_n \\ b_1, b_2, \cdots, b_n \end{pmatrix}^{-1} = \begin{pmatrix} b_1, b_2, \cdots, b_n \\ a_1, a_2, \cdots, a_n \end{pmatrix}$$

显然

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = I$$

且 $\sigma^{-1}$ 为左乘(右乘)$\sigma$ 使积为 $I$ 的唯一置换.

**引理 2.1** $\sigma$ 与 $\sigma^{-1}$ 有相同奇偶性.

**证** 显然 $I$ 是偶置换,据 $\sigma\sigma^{-1} = I$ 及引理 1.4 推论 2 知本引理成立(用反证法).

由于在 $N = \{1,2,\cdots,n\}$ 的所有置换中可定义乘法运算,它适合结合律,又存在单位置换 $I$(使对任一置换 $\sigma$ 适合 $\sigma I = I\sigma = \sigma$),对任一置换 $\sigma$ 存在唯一逆置换 $\sigma^{-1}$(使 $\sigma\sigma^{-1} = \sigma^{-1}\sigma = I$). 即对所有 $n$ 次置换的乘法运算适合群的定义,故所有 $n$ 次置换之集对其乘法运算为一个群,称之为 $n$ 次对称群,记之为 $S_n$.

因单位置换 $I$ 为偶置换,任两偶置换之积为偶置换,任何偶置换之逆置换亦为偶置换. 故所有 $n$ 次偶置换组成之集对其乘法运算为一个群,称之为 $n$ 次交代群,记之为 $A_n$.

只含($n$ 次) 单位置换之集 $\{I\}$,易见对其乘法运算为一个群($I \cdot I = I$, $I^{-1} = I$),称之为 $n$ 次单位置换群,或 $n$ 次恒等置换群.

因二次置换只有 $I$ 及(1,2),易见二次群只有

$$\{I\}, S_2 = \{I, (1,2)\}$$

一般情况,若由一些(部分或全部)$n$ 次置换所组成的置换集对置换乘法符合群的定义(即集的任二置换之积为集的置换,集含单位置换,集的任一置换之逆置换亦为集的置换),则称此置换集为一个($n$ 次) 置换群,群的所有置换个数 $q$ 称为此群的阶数,又称此群为 $q$ 阶群.

如$\{I\}$的阶数为1;对称群$S_n$及交代群$A_n$的阶数分别为$n!$及$\frac{n!}{2}$.

同样记(置换$\sigma$的$k$次幂)

$$\underbrace{\sigma\sigma\cdots\sigma}_{k个}=\sigma^k$$

同样定义任何置换$\sigma$的零次幂为单位置换$I$

$$\sigma^0=I$$

易见对任何$k_1,k_2\in\mathbf{N}(\mathbf{N}=\mathbf{Z}^+\cup\{0\}$——按现行中学课本规定)有

$$\sigma^{k_1}\sigma^{k_2}=\sigma^{k_1+k_2}$$

$$(\sigma^{k_1})^{k_2}=\sigma^{k_1k_2}$$

从而$\sigma$的幂适合乘法交换律.

又对任何自然数$k$(含0)有

$$I^k=I$$

显然对轮换的幂有

$$(a_1,a_2,\cdots,a_k)^2=\begin{pmatrix}a_1,a_2,\cdots,a_{k-2},a_{k-1},a_k\\a_3,a_4,\cdots,a_k,\ a_1,\ a_2\end{pmatrix}$$

$$(a_1,a_2,\cdots,a_k)^3=\begin{pmatrix}a_1,a_2,\cdots,a_{k-3},a_{k-2},a_{k-1},a_k\\a_4,a_5,\cdots,a_k,\ a_1,\ a_2,\ a_3\end{pmatrix}$$

$$\vdots$$

$$(a_1,a_2,\cdots,a_k)^{k-2}=\begin{pmatrix}a_1,\ a_2,a_3,a_4,\cdots,a_k\\a_{k-1},a_k,a_1,a_2,\cdots,a_{k-2}\end{pmatrix}$$

$$(a_1,a_2,\cdots,a_k)^{k-1}=\begin{pmatrix}a_1,a_2,a_3,\cdots,a_k\\a_k,a_1,a_2,\cdots,a_{k-1}\end{pmatrix}=(a_1,a_k,a_{k-1},\cdots,a_3,a_2)$$

$$(a_1,a_2,\cdots,a_k)^k=I$$

$$(a_1,a_2,\cdots,a_k)^{mk}=I\quad(m\in\mathbf{Z}^+)$$

$$(a_1,a_2,\cdots,a_k)^{mk+r}=(a_1,a_2,\cdots,a_k)^r\quad(m\in\mathbf{Z}^+,r=0,1,2,\cdots,k-1)$$

易见

$$(a_1,a_2,\cdots,a_k)^r\quad(r=0,1,2,\cdots,k-1)$$

的逆元

$$((a_1,a_2,\cdots,a_k)^r)^{-1}=(a_1,a_2,\cdots,a_k)^{k-r}$$

**定理2.2** 对任何置换$\sigma$,必存在唯一正整数$m$,使

$$\sigma^m=I$$

且$m$为使"$\sigma$的幂等于$I$"的最小次数.

**证** 当$\sigma=I$,取$m=1$即可.当$\sigma\neq I$,把$\sigma$分解为若干个两两无公共元素的轮换因式之积,取各轮换因式阶数之最小公倍数$m$(若$\sigma$就是一个轮换,则取

$m$ 为此轮换阶数). 易见 $\sigma^m = I$.

再证 $m$ 为使 $\sigma$ 的幂等于 $I$ 的最小次数:对小于 $m$ 的正整数 $m'$,因 $m'$ 必然至少不是某轮换因式阶数 $p$ 的倍数,由上述各轮换幂的公式知,$\sigma^{m'}$(导到此轮换的 $m'$ 次幂)必不能使此轮换中各元素不变,于是 $\sigma^{m'} \neq I$.

**定理 2.3** 设定理 2.2 中所述 $n$ 次置换 $\sigma$ 及正整数 $m$,则 $\sigma$ 的所有自然数次幂只有如下 $m$ 个互不相同的置换:

$$\sigma, \sigma^2, \sigma^3, \cdots, \sigma^{m-1}, \sigma^m = \sigma^0 = I \tag{2.1}$$

它们组成一个置换群,称为由 $\sigma$ 生成的($n$ 次 $m$ 阶)循环置换群(或简称循环群),称 $\sigma$ 为此循环置换群的生成元.

**证** 对任何自然数 $p$,对除数 $m$ 作带余除法得

$$p = qm + r \quad (q \in \mathbf{N}, r = 0, 1, 2, \cdots, m-1)$$

从而

$$\sigma^p = \sigma^{qm+r} = (\sigma^m)^q \sigma^r = I^q \sigma^r = I\sigma^r = \sigma^r$$

即 $\sigma$ 的所有幂都在式(2.1)内.

再证式(2.1)内任二置换不等:

否则有 $r_1, r_2 \in \{0, 1, 2, \cdots, m-1\}$,不妨设 $r_1 < r_2$,使

$$\sigma^{r_1} = \sigma^{r_2}$$

即

$$\sigma^{r_1} = \sigma^{r_1} \sigma^{r_2 - r_1}$$

两边左乘 $\sigma^{m-r_1}$ 得

$$I = \sigma^{r_2 - r_1}$$

但

$$0 < r_2 - r_1 \leqslant r_2 < m$$

这与 $m$ 为"使 $\sigma$ 的幂等于 $I$" 的最小次数矛盾.

又因式(2.1)中有单位置换 $I$,其内任二置换 $\sigma^{r_1}$ 与 $\sigma^{r_2}$ 之积 $\sigma^{r_1+r_2}$ 仍(可化)为式(2.1)内的置换,对其内任一置换 $\sigma^r (r = 0, 1, 2, \cdots, m-1)$,易见有逆置换 $\sigma^{m-r}$ 在式(2.1)内,故式(2.1)组成一个置换群.

特例:$k$ 阶轮换 $\sigma$ 为 $k$ 阶循环置换群的生成元,且 $\sigma^k = I$.

类似有:

**定理 2.4** 若一 $n$ 次置换集内可进行乘法运算,则此置换集为一个置换群.

**证** 只要再证此集含单位置换且对集内任一置换 $\sigma$,在此集存在逆置换 $\sigma^{-1}$:由定理 2.2 知存在最小正整数 $m$,使 $\sigma^m = I$,由假设知此集含 $\sigma^m = I$;又易见 $\sigma\sigma^{m-1} = \sigma^{m-1}\sigma = I$,于是此集又含 $\sigma^{m-1} = \sigma^{-1}$. 故此置换集为一置换群.

**例 1** 设 5 次置换

$$\sigma = (1, 2, 3)(4, 5)$$

则因 3,2 之最小公倍数为 6,$\sigma$ 生成 6 阶循环群:

$$\sigma = (1,2,3)(4,5)$$
$$\sigma^2 = (1,3,2)$$
$$\sigma^3 = (4,5)$$
$$\sigma^4 = (1,2,3)$$
$$\sigma^5 = (1,3,2)(4,5)$$
$$\sigma^6 = I$$

**例 2** 设 6 阶轮换

$$\sigma = (1,2,3,4,5,6)$$

则

$$\sigma = (1,2,3,4,5,6)$$
$$\sigma^2 = (1,3,5)(2,4,6)$$
$$\sigma^3 = (1,4)(2,5)(3,6)$$
$$\sigma^4 = (1,5,3)(2,6,4)$$
$$\sigma^5 = (1,6,5,4,3,2)$$
$$\sigma^6 = I$$

这 6 个置换组成 6 阶循环群.

**例 3** 设 5 阶轮换

$$\sigma = (1,2,3,4,5)$$

则由 $\sigma$ 产生 5 阶循环群:

$$\{(1,2,3,4,5),(1,3,5,2,4),(1,4,2,5,3),(1,5,4,3,2),I\}$$

**定义 2.1** 若两个 $n$ 次置换群 $S_1, S_2$ 有(作为置换集)$S_1 \subset S_2$,则称 $S_1$ 是 $S_2$ 的子群.

易见任何 $n$ 次置换群是 $S_n$ 的子群,$\{I\}$ 是任何 $n$ 次置换群的子群.

**定理 2.5** 置换群 $G$ 的阶数 $p$ 必为其子群 $G'$ 的阶数 $p'$ 的整数倍. 此倍数记为 $[G:G']$,$[G:G'] = \dfrac{p}{p'}$.

**证** 若 $p' = p$,结论显然,下设 $p' < p$,又设

$$G' = \{\sigma_1, \sigma_2, \cdots, \sigma_{p'}\}$$

因 $p' < p$,群 $G$ 内必有不属于 $G'$ 的置换 $\tau_2$,从而含置换

$$\sigma_1\tau_2, \sigma_2\tau_2, \cdots, \sigma_{p'}\tau_2 \tag{2.2}$$

上述 $p'$ 个置换互不相同(否则如 $\sigma_1\tau_2 = \sigma_2\tau_2$,两边右乘 $\tau_2^{-1}$ 得 $\sigma_1 = \sigma_2$,矛盾). 且其中任一置换不与 $G'$ 中任一置换相同(否则如 $\sigma_1\tau_2 = \sigma_2$,则 $\tau_2 = \sigma_1^{-1}\sigma_2$,因群 $G'$ 含 $\sigma_1, \sigma_2$,必含逆置换 $\sigma_1^{-1}$,从而又含 $\sigma_1^{-1}\sigma_2 = \tau_2$,与前述矛盾).

若除 $G'$ 及式(2.2)中置换外 $G$ 再无其他置换,则 $p = 2p'$,结论得证. 若 $G$ 尚

有其他置换，在其中取置换 $\tau_3$，从而 $G$ 又含置换

$$\sigma_1\tau_3,\sigma_2\tau_3,\cdots,\sigma_{p'}\tau_3 \tag{2.3}$$

同样式(2.3)中各置换互不相同，且其任一置换不与 $G'$ 中的置换相同. 再证式(2.3)中任一置换不与式(2.2)中任一置换相同：否则如 $\sigma_3\tau_3=\sigma_2\tau_2$，则

$$\tau_3=\sigma_3^{-1}(\sigma_2\tau_2)$$

即

$$\tau_3=(\sigma_3^{-1}\sigma_2)\tau_2$$

但 $\sigma_3^{-1}\sigma_2$ 为 $G'$ 的置换，故 $\tau_3$ 为式(2.2)中的置换，这与假设 $G$ 尚有在 $G'$ 及式(2.2)中的置换之外的置换 $\tau_3$ 矛盾.

若除 $G'$ 及式(2.2)，式(2.3)中的置换外 $G$ 不含其他置换，则 $p=3p'$，命题得证. 否则继续作同样论证，因 $G$ 的置换个数 $p$ 有限，故必到某一步取尽 $G$ 的所有置换，即 $G$ 的所有置换排成下表：

$$\begin{array}{c}\sigma_1,\quad \sigma_2,\quad \cdots,\sigma_{p'}\\ \sigma_1\tau_2,\sigma_2\tau_2,\cdots,\sigma_{p'}\tau_2\\ \sigma_1\tau_3,\sigma_2\tau_3,\cdots,\sigma_{p'}\tau_3\\ \vdots\\ \sigma_1\tau_m,\sigma_2\tau_m,\cdots,\sigma_{p'}\tau_m\end{array}$$

从而 $p=mp'$，定理证毕.

**定理 2.6** 设有 $k$ 阶循环置换群

$$G=\{\sigma,\sigma^2,\cdots,\sigma^{k-1},I\}\quad(\sigma^k=I)$$

又设正整数 $m$ 与 $k$ 的最大公约数(记为)$(k,m)=d$，设 $\frac{k}{d}=k'$，则置换集

$$G'=\{\sigma^m,(\sigma^m)^2,\cdots,(\sigma^m)^{k'}\}=\{\sigma^m,\sigma^{2m},\cdots,\sigma^{k'm}\}$$

为 $k'$ 阶循环置换群，且为 $G$ 的子群.

**证** 设

$$\frac{m}{d}=m'$$

求得

$$(\sigma^m)^{k'}=\sigma^{\frac{mk}{d}}=\sigma^{m'k}=(\sigma^k)^{m'}=I^{m'}=I$$

再对任何小于 $k'$ 的正整数 $k''$，证 $(\sigma^m)^{k''}\neq I$：否则若 $(\sigma^m)^{k''}=I$，即 $\sigma^{mk''}=I$，因 $k$ 为以 $\sigma$ 为生成元的循环群之阶数，故 $mk''$ 除以 $k$ 所得余数 $r=0$(否则 $\sigma^{mk''}=\sigma^r\neq I$). 于是

$$mk''=pk\quad(p\in\mathbf{Z}^+)$$

两边除以 $d$ 得

$$m'k''=pk'$$