抽象代数

ABSTRACT ALGEBRA

杨胜良 吴德军 杨 琳 编著

兰州大学出版社
LANZHOU UNIVERSITY PRESS

抽象代数

ABSTRACT ALGEBRA

杨胜良 吴德军 杨 琳 编著

东南大学出版社
SOUTHEAST UNIVERSITY PRESS

图书在版编目（CIP）数据

抽象代数 / 杨胜良，吴德军，杨琳编著. -- 兰州 : 兰州大学出版社，2015.12
ISBN 978-7-311-04881-5

Ⅰ. ①抽… Ⅱ. ①杨… ②吴… ③杨… Ⅲ. ①抽象代数 Ⅳ. ①0153

中国版本图书馆CIP数据核字(2016)第020641号

策划编辑 张爱民
责任编辑 郝可伟
封面设计 郇 海

书 名 抽象代数
作 者 杨胜良 吴德军 杨 琳 编著
出版发行 兰州大学出版社 （地址:兰州市天水南路222号 730000）
电 话 0931-8912613(总编办公室) 0931-8617156(营销中心)
0931-8914298(读者服务部)
网 址 http://www.onbook.com.cn
电子信箱 press@lzu.edu.cn
印 刷 兰州万易印务有限责任公司
开 本 710 mm×1020 mm 1/16
印 张 14.75
字 数 220千
版 次 2016年3月第1版
印 次 2016年3月第1次印刷
书 号 ISBN 978-7-311-04881-5
定 价 32.00元

前　言

抽象代数是数学专业研究生的一门基础课. 自2004年起，我们在兰州理工大学理学院为数学系研究生开设“抽象代数”学位课程，本书是在讲稿基础上反复修改整理而成的，凝聚了作者及同事们所积累的丰富教学经验. 本书注重讲述传统的基础知识，同时也力图使读者能够对抽象代数的主要思想方法有所体会. 本书是抽象代数的基础教材，主要介绍群、环、域、模四个基本的代数结构以及范畴的初步知识. 全书共分五章. 第一章介绍群的基本概念. 第二章介绍环论基础. 第三章介绍域的扩张和有限域. 第四章介绍模论基础知识. 第五章介绍范畴的基础理论. 习题是本书的一个重要组成部分. 要掌握抽象代数的理论和方法，必须做一定量的习题. 本书每一章附有足够数量的习题，其中多数是基础性的，也有少数是比较难的. 读者可以选择一部分来完成.

在本书的编写过程中，得到了兰州理工大学理学院很多老师和研究生的大力支持和帮助，在此谨致谢意. 本书的出版得到了兰州理工大学研究生重点学位课程建设计划资助，在此作者表示衷心感谢.

本书第一章和第三章由杨胜良编写，第二章由杨琳编写，第四章和第五章由吴德军编写，最后由杨胜良对全书进行统稿. 限于作者水平，书中难免有错误或不妥之处，恳请读者批评指正.

杨胜良　吴德军　杨琳

2016年2月于兰州理工大学

目　录

第一章 群

本章介绍群论基础知识.

§ 1.1 集合与映射

集合与映射是数学中的两个基本概念. 本节简要介绍集合与映射的基础知识, 顺便引入本书常用的符号.

所谓集合就是指作为整体来讨论的一些事物，组成集合的各个事物叫作这个集合的元素. 我们用大写拉丁字母$A, B, C, \cdots$来表示集合，用小写拉丁字母$a, b, c, \cdots$来表示集合的元素. 当a是集合A的元素时，记为$a \in A$, 读作a属于A. 当a不是集合A的元素时，记为$a \notin A$，读作a不属于A. 我们约定用$\mathbb{C}$表示全体复数组成的集合；$\mathbb{R}$表示全体实数组成的集合；$\mathbb{Q}$表示全体有理数组成的集合；$\mathbb{Z}$表示全体整数组成的集合；$\mathbb{N}$表示全体自然数（即非负整数）组成的集合. 不包含任何元素的集合叫作空集，记作$\emptyset$.

通常给出一个集合的方法有两种: 一种是列举法，即列出一个集合的全部元素；另一种是描述法，即指出一个集合的元素的特征性质. 例如, $L_m = \{0, 1, 2, \cdots, m-1\}$就是用列举法给出了小于正整数$m$的所有非负整数的集合，而$\mathbb{C} = \{a + b\mathrm{i} | a, b \in \mathbb{R}, \mathrm{i}^2 = -1\}$就是用描述法给出了全体复数的集合.

一个集合A所包含元素的个数记作$|A|$，叫作A的基数. 当$|A|$为一个有限数时，称A 为有限集，否则，称A为无限集.

如果集合A的每个元素都是集合B的元素，那么就说A是B的子集，记作$A \subseteq B$，或$B \supseteq A$. 如果A是B的子集而且B也是A的子集，那么就说A与B相等，记作$A = B$. 如果A是B的子集, 但$A \neq B$，那么就说A是B的真子集，记作$A \subset B$.

设A, B是两个集合，A与B的并、交、差分别定义为:

$$A \cup B = \{x | x \in A \text{ 或} x \in B\},$$

$$A \cap B = \{x | x \in A \text{ 且} x \in B\},$$

$$A - B = \{x | x \in A \text{ 但} x \notin B\}.$$

而A与B的笛卡儿积定义为：

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

所谓从集合A到集合B的一个映射σ，是指一个对应法则，使得A中每个元素a都有B中一个唯一确定的元素b与它对应. 从集合A到集合B的一个映射σ 也叫作定义在A上而在B中取值的一个函数.

我们用

$$\sigma : A \longrightarrow B$$

表示σ是从集合A到集合B的一个映射. 如果在映射σ下，A中的元素a与B中的元素b对应，记作$b = \sigma(a)$，或$\sigma : a \longmapsto b$. 此时把b叫作a在映射σ下的像，而把a叫作b 在映射σ下的一个原像. 设$A' \subseteq A$而$B' \subseteq B$，把B的子集$\sigma(A') = \{\sigma(a) | a \in A'\}$叫作$A'$在映射$\sigma$下的像，而把$A$的子集$\sigma^{-1}(B') = \{a \in A | \sigma(a) \in B'\}$叫作$B'$在映射$\sigma$下的完全原像. 特别地，$\sigma(A)$叫作映射$\sigma$的像. 如果$\sigma(A) = B$，就称$\sigma$是$A$到$B$ 的一个满射. 如果在映射σ下，A中任意两个不同元素的像也一定不同，即对任意$a_1, a_2 \in A$, 当$a_1 \neq a_2$时, 必定有$\sigma(a_1) \neq \sigma(a_2)$, 就称$\sigma$是$A$到$B$的一个单射. 既是单射又是满射的映射叫作双射. 双射也叫作一一对应. 如果存在一个一一对应$\sigma : A \longrightarrow B$，就称集合$A$与集合$B$是等势的, 记作$|A| = |B|$.

设$\sigma : A \longrightarrow B$ 与$\tau : B \longrightarrow C$ 是两个映射，则对任意$a \in A$，由

$$\phi(a) = \tau(\sigma(a))$$

确定的映射$\phi : A \longrightarrow C$ 叫作σ与τ的合成，这个合成映射记为$\phi = \tau \circ \sigma$. 可以证明，一个映射$\sigma : A \longrightarrow B$是一一对应的充分必要条件是存在另一个映

射$\tau : B \longrightarrow A$，使得$\tau\sigma = i_A$且$\sigma\tau = i_B$，这里$i_A$表示集合$A$上的恒定映射，即$i_A : A \longrightarrow A$，对任意$a \in A$, $i_A(a) = a$. 在这种情况下，我们称映射σ是可逆的，而且把τ叫作σ的逆映射，记为$\tau = \sigma^{-1}$.

设A是一个非空集合. $A \times A$ 的一个子集R叫作集合A上的一个二元关系. 当$(a,b) \in R$时，就说a与b有关系R，记作aRb；当$(a,b) \notin R$时，就说a与b没有关系R，记作$a\bar{R}b$. 集合A上的一个二元关系$\sim$叫作一个等价关系，如果它满足以下三个条件:

(1) 自反性：$a \sim a$对所有$a \in A$;

(2) 对称性：从$a \sim b$推出$b \sim a$;

(3) 传递性：从$a \sim b$和$b \sim c$推出$a \sim c$.

设$\sim$是集合A上的一个等价关系, 对任意$a \in A$定义$\bar{a} = \{x \in A | x \sim a\}$, 称之为一个等价类.

一个非空集合A的一组非空子集$A_i (i \in I)$叫作A的一个划分，如果$\bigcup_{i\in I} A_i = A$而且$i \neq j$ 时$A_i \cap A_j = \emptyset$. 容易证明，若$\sim$是集合A上的一个等价关系，则全体等价类构成A的一个划分.

设m为一个正整数. 在整数集合$\mathbb{Z}$中规定：两个数a与b有模m同余关系$\sim$，当且仅当$m|(a-b)$. 容易验证，$\sim$是集合$\mathbb{Z}$的一个等价关系，由此等价关系导出的划分为

$$\mathbb{Z}_m = \{\bar{j} | j \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{m-1}\},$$

其中$\bar{j} = \{km + j | k \in \mathbb{Z}\}$, $j = 0, 1, 2, \cdots, m-1$.

§ 1.2 群的概念

设S是一个非空集合. 映射$\sigma : S \times S \to S$叫作集合$S$上的一个二元运算. 定义了一个二元运算的非空集合，通常叫作群胚. 二元运算通常称为乘法，即对任意$x, y \in S$，将$\sigma((x,y))$ 记作$x \cdot y$或xy，简称为x与y的积. 若对任意$x, y, z \in S$，总有$(xy)z = x(yz)$，则称这个乘法满足结合律，或者说这个乘法是结合的. 若对任意$x, y \in S$，总有$xy = yx$，则称这个乘法满足交换律，或者说这个乘法是交换的. 若存在$e \in S$，使得对任意$x \in S$，总有$ex = x$, 则

称e为左单位元；若存在$e' \in S$，使得对任意$x \in S$，总有$xe' = x$，则称e'为右单位元；若e既是左单位元又是右单位元，则称e为单位元. 如果群胚S的乘法满足结合律，则称S为半群. 若半群S含有单位元，则称S为幺半群.

例 1.2.1 数域F上的关于字母z的多项式的集合按照乘法运算构成一个幺半群.

例 1.2.2 数域F上2阶方阵的集合按照矩阵的乘法运算构成一个幺半群.

定义 1.2.1 设G是一个非空集合，G上有一个乘法运算"$\cdot$"，若满足以下三条，就称集合G关于这个乘法构成群，或称$(G, \cdot)$是群，简称G是群：

(1) 乘法满足结合律，即$\forall x, y, z \in G$，$(xy)z = x(yz)$；

(2) 有单位元，即$\exists\, e \in G$，$\forall x \in G$，$xe = ex$；

(3) 每个元素有逆元，即$\forall x \in G$，$\exists\, x^{-1} \in G$，$xx^{-1} = x^{-1}x = e$.

如果一个群G的乘法运算是交换的，则称G是一个交换群或阿贝尔群. 若一个群G中的元素是有限的，即$|G| < \infty$，则称G是一个有限群，否则就称G是一个无限群. G的基数$|G|$叫作群G 的阶.

例 1.2.3 图形的对称群. 设Ω是一个几何图形，Ω到它自身的一个(几何)运动叫作Ω的一个对称. 若Ω的所有对称构成的集合为S_Ω，S_Ω上的二元运算就是对称的合成，即对任意两个对称f, g，$g \circ f$表示对Ω先做运动f然后跟着做运动g. 显然，两个对称的合成也是一个对称；保持不动的运动即恒等对称就是合成运算的单位元；而对称f 的逆f^{-1}就是与f相反的运动. 所以，一个几何图形Ω的所有对称的集合S_Ω关于对称的合成运算构成一个群，称之为Ω的对称群.

例 1.2.4 正三角形的对称群(图1.2.1).

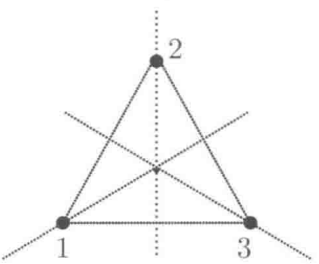

图1.2.1

正三角形的对称群为$D_3^* = \{e, f, f^2, t_1, t_2, t_3\}$，其中$e$为恒等对称，$f$是绕中心沿逆时针方向旋转$\frac{2\pi}{3}$，$f^2$是绕中心沿逆时针方向旋转$\frac{4\pi}{3}$，$t_1$是关于过中心和顶点1的对称轴的反射，$t_2$是关于过中心和顶点2的对称轴的反射，$t_3$是关于过中心和顶点3的对称轴的反射.

例 1.2.5 正方形的对称群(图1.2.2).

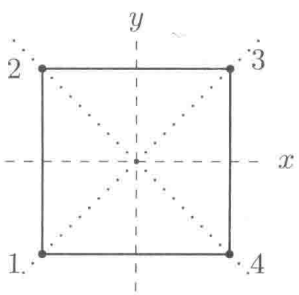

图1.2.2

正方形的对称群为$D_4^* = \{e, f, f^2, f^3, t_{1,3}, t_y, t_{2,4}, t_x\}$，其中$e$为恒等对称，$f$是绕中心沿逆时针方向旋转$\frac{\pi}{2}$，$f^2$是绕中心沿逆时针方向旋转$\pi$，$f^3$ 是绕中心沿逆时针方向旋转$\frac{3\pi}{2}$，$t_{1,3}$是关于过顶点1和顶点3的对称轴的反射，t_y是关于y轴的反射，$t_{2,4}$是关于过顶点2和顶点4的对称轴的反射，t_x是关于x轴的反射.

例 1.2.6 设$B_4 = \{e, a, b, c\}$，乘法表为

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

可以验证$(B_4, \cdot)$是一个交换群，通常叫作Klein 四元群，简称四元群.

例 1.2.7 设m为一个给定的正整数. 令L_m为所有$< m$的非负整数所组成的集合，即

$$L_m = \{0, 1, 2, \cdots, m-1\}.$$

那么，L_m关于模m的加法运算构成一个m阶群. 特别地，当$n=4$时，$(L_4,+)$的加法表为

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

可以看到，$(B_4,\cdot)$的乘法表与$(L_4,+)$的加法表有很大差异.

定理 1.2.1 设G是任意群，那么

(1) G中单位元e是唯一的；

(2) 对任意$x\in G$，x的逆元x^{-1}是唯一的.

证明 (1) 如果e'也是单位元，则$e=ee'=e'$.

(2) 如果x'也是x的逆元，那么$x'x=xx'=e$，所以$x^{-1}=ex^{-1}=(x'x)x^{-1}=x'(xx^{-1})=x'e=x'$.

定理 1.2.2 设G是任意群，那么G中以下结论成立:

(1) 设$a,b,c\in G$. 若$ab=ac$，则$b=c$；

(2) 对任意$a,b\in G$，$(ab)^{-1}=b^{-1}a^{-1}$；

(3) 对任意$a\in G$，$(a^{-1})^{-1}=a$；

(4) 对任意$a,b\in G$，方程$ax=b$和$ya=b$均在G中有唯一解：$x=a^{-1}b$，$y=ba^{-1}$.

证明 (1) 若$ab=ac$，则$b=eb=(a^{-1}a)b=a^{-1}(ab)=a^{-1}(ac)=(a^{-1}a)c=ec=c$.

(2) 由$(ab)(b^{-1}a^{-1})=a((bb^{-1})a^{-1})=a(ea^{-1})=aa^{-1}=e$，所以$(ab)^{-1}=b^{-1}a^{-1}$.

(3) 由$a^{-1}a=e$，$a^{-1}(a^{-1})^{-1}=e$以及逆元的唯一性，得$(a^{-1})^{-1}=a$.

(4) 由$a(a^{-1}b)=(aa^{-1})b=eb=b$，得$x=a^{-1}b$是方程$ax=b$的一个解. 根据(1)，这样的解是唯一的.

设G是任意群，a是G中任意元，n是一个正整数. 我们规定：$a^0=e$，$a^n=aa\cdots a$为n个a的积，$a^{-n}=(a^{-1})^n$. 容易证明以下结论.

定理 1.2.3 设G是任意群，那么G中以下结论成立:

(1) 若$a \in G$, m, n 是任意整数，则$a^m a^n = a^{m+n}$;

(2) 若$a \in G$, m, n 是任意整数，则$(a^m)^n = a^{mn}$;

(3) 对任意$a, b \in G$，若$ab = ba$，则$(ab)^n = a^n b^n$.

如果把一个交换群G的运算用加法+表示，单位元用0表示，一个元素a的逆元就叫作负元且记为$-a$，通常称$(G, +)$为加群. 在加群中，元素a的n幂次就记为倍数na.

定义 1.2.2 设G是任意群，H是G的一个非空子集. 若H关于G的乘法运算构成一个群，那么就称H为G的一个子群，记作$H \leq G$. 若群G的子群H不等于G，就称H为G的一个真子群，记作$H < G$.

定理 1.2.4 设G是一个群，H是G的一个非空子集，那么以下条件是等价的:

(1) H为G的一个子群;

(2) 对任意$a, b \in H$，有$ab \in H$，而且对任意$a \in H$，有$a^{-1} \in H$;

(3) 对任意$a, b \in H$，有$ab^{-1} \in H$.

证明 (1) $\Rightarrow$ (2)和(2) $\Rightarrow$ (3) 是显然的. 下证(3) $\Rightarrow$ (1).

假定对任意$a, b \in H$，有$ab^{-1} \in H$. 由H是G的一个非空子集，至少存在一个$a \in H$，于是有$e = aa^{-1} \in H$. 因此，对任意$a \in H$, 有$a^{-1} = ea^{-1} \in H$. 因此，对任意$a, b \in H$，有$b^{-1} \in H$，$ab = a(b^{-1})^{-1} \in H$. 所以，$H$关于$G$的乘法运算是封闭的. 由定义1.2.1以及定义1.2.2，H为G的一个子群.

定义 1.2.3 设G是一个群，M是G的一个非空子集. 群G的包含M的最小子群称为由M在G中生成的子群，记作$\langle M \rangle$.

任意群G都有子群. 例如，G本身和由单位元生成的子群$\langle e \rangle$就是G的两个子群. 这两个子群叫作平凡子群.

例 1.2.8 整数集合$\mathbb{Z}$关于加法运算构成一个无限群$(\mathbb{Z}, +)$. $H = \{nk | k \in \mathbb{Z}\}$是整数加群$(\mathbb{Z}, +)$的一个子群，其中$n$是取定的一个自然数.

§ 1.3 置换群

设$N=\{1,2,\cdots,n\}$，N到N的一个双射叫作一个n次置换，所有的n次置换的集合S_n关于置换的合成运算构成的群叫作n次对称群. 对称群S_n的每个子群都叫作n个元素的置换群. 设$\sigma\in S_n$, σ可以表示为：

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n)\end{pmatrix}.$$

例如，设σ是一个7次置换: $\sigma(1)=4$，$\sigma(2)=2$，$\sigma(3)=7$，$\sigma(4)=1$，$\sigma(5)=3$，$\sigma(6)=6$，$\sigma(7)=5$，则σ可以表示为：

$$\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 4 & 2 & 7 & 1 & 3 & 6 & 5\end{pmatrix}.$$

例 1.3.1 3次对称群S_3 的6个元素为:

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

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

S_3中的乘法为映射的合成运算，例如

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

这里表示先作σ_6的置换，然后作σ_5的置换. 而$G_1=\{\sigma_1,\sigma_2,\sigma_3\}$, $G_2=\{\sigma_1,\sigma_4\}$, $G_3=\{\sigma_1,\sigma_5\}$, $G_4=\{\sigma_1,\sigma_6\}$都是$S_3$ 的子群，从而都是3次置换群.

设$\sigma\in S_n$，若存在$x\in N$ 以及正整数k 使得$x,\sigma(x),\sigma^2(x),\cdots,\sigma^{k-1}(x)$互不相同且$\sigma^k(x)=x$，而当$y\in N-\{x,\sigma(x),\sigma^2(x),\cdots,\sigma^{k-1}(x)\}$ 时，$\sigma(y)=y$，则称置换σ为一个长为k的轮换，或k–轮换，记作

$$\sigma=(x,\sigma(x),\sigma^2(x),\cdots,\sigma^{k-1}(x)).$$

例如，设σ是一个7次置换: $\sigma(1)=4$, $\sigma(2)=2$, $\sigma(3)=7$, $\sigma(4)=3$, $\sigma(5)=5$, $\sigma(6)=6$, $\sigma(7)=1$, 则σ是一个4–轮换，且可以表示为$\sigma=(1437)$. 长为1的轮换即1–轮换就是恒等置换. 长度为2的轮换(ij)叫作对换.

每个置换都可以表示成互不相交的轮换的乘积. 例如, 设σ是一个7次置换: $\sigma(1)=4$, $\sigma(2)=2$, $\sigma(3)=7$, $\sigma(4)=1$, $\sigma(5)=3$, $\sigma(6)=6$, $\sigma(7)=5$, 则σ可以表示为$\sigma=(14)(2)(375)(6)$. 这样的表示不是唯一的，如σ还可以表示为$\sigma=(41)(2)(6)(537)$. 我们规定，每个轮换必须将最小的元素写在首位，轮换按首位数字从小到大排列，这样每个置换都可以唯一地表示成互不相交的轮换的乘积，这种表示叫作置换的标准轮换分解. 例如，上面的置换σ的标准轮换分解为$\sigma=(14)(2)(375)(6)$. 3次对称群S_3的6个元素的标准轮换分解为：

$$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=(1)(2)(3),\ \sigma_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(123),$$

$$\sigma_3=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132),\ \sigma_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(1)(23),$$

$$\sigma_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(13)(2),\ \sigma_6=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12)(3).$$

例 1.3.2 4次对称群S_4的元素的两种表示：

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=(1)(2)(3)(4);\ \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=(12)(3)(4);$$

$$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}=(13)(2)(4);\ \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}=(14)(2)(3);$$

$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}=(1)(23)(4);\ \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}=(1)(24)(3);$$

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(1)(2)(43);\ \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=(123)(4);$$

$$\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=(132)(4);\ \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=(124)(3);$$

$$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}=(142)(3);\quad\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}=(134)(2);$$

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}=(143)(2);\quad\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}=(1)(234);$$

$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}=(1)(243);\quad\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1234);$$

$$\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}=(1243);\quad\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}=(1324);$$

$$\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}=(1342);\quad\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}=(1423);$$

$$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=(1432);\quad\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(12)(34);$$

$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(13)(24);\quad\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(14)(23).$$

根据以上讨论和例题，我们可以得到以下定理.

定理 1.3.1 每个置换都可以分解成互不相交的轮换之积，而且除了轮换的次序以及1–轮换的多少外，这种分解是唯一的.

定理 1.3.2 每个置换α都可以分解成一些的对换之积，而且对换的个数的奇偶性是唯一确定的.

证明 容易验证

$$(i_1i_2\cdots i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2),$$

即一个r–轮换能分解成$r-1$个对换的乘积. 每个置换α都可以分解成互不相交的轮换之积，进而就可以分解成一些对换之积.

假定置换α是s个长度分别为$r_1,r_2,\cdots,r_s$的互不相交的轮换的乘积. 我们规定

$$N(\alpha)=(r_1-1)+(r_2-1)+\cdots+(r_s-1).$$