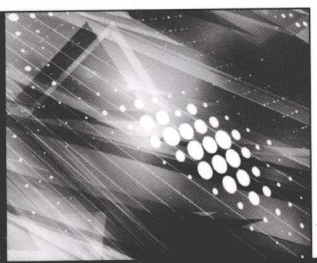
高　等　学　校　教　材

抽象代数



◆ 大连理工大学数学科学学院
◆ 王　颖　南基洙　编著

高等教育出版社
HIGHER EDUCATION PRESS

高等学校教材

抽象代数

Chouxiang Daishu

大连理工大学数学科学学院
王　颖　南基洙　编著

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

内容提要

本书介绍了抽象代数学中最基本的内容，共4章。第一章介绍了等价关系、分类和代数系统等预备知识，第二章至第四章则分别介绍了群、环、域和伽罗瓦(Galois)理论等。在每一章的末尾，还简述了一些有趣的史料和有关数学家的传记。

本书可作为高等学校数学类专业本科高年级学生及研究生的教材，也可作为相关技术人员的参考用书。

图书在版编目（CIP）数据

抽象代数/王颖，南基洙编著．--北京：高等教育出版社，2013.2

ISBN 978-7-04-034759-3

Ⅰ.①抽… Ⅱ.①王…②南… Ⅲ.①抽象代数-高等学校-教材 Ⅳ.①O153

中国版本图书馆 CIP 数据核字(2013)第001491号

策划编辑 张晓丽	责任编辑 张彦云	封面设计 李卫青	版式设计 杜微言
插图绘制 黄建英	责任校对 张小镝	责任印制 毛斯璐	

出版发行	高等教育出版社	咨询电话	400-810-0598
社　　址	北京市西城区德外大街4号	网　　址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印　　刷	三河市杨庄长鸣印刷装订厂	网上订购	http://www.landraco.com
开　　本	787mm×960mm　1/16		http://www.landraco.com.cn
印　　张	10.25	版　　次	2013年2月第1版
字　　数	180千字	印　　次	2013年2月第1次印刷
购书热线	010-58581118	定　　价	16.70元

物 料 号　34759-00

前　言

抽象代数学是以有运算的集合(即代数系统)作为其研究对象的一门基础性数学学科。它在数学发展中占据着非常重要的地位。近年来,随着物理学、化学、计算机以及数字信息技术的飞速发展,抽象代数学的知识和技巧也越来越多地应用于这些相关科学领域。例如,群论应用于物理学和晶体化学,环与域应用于编码和信息技术领域等。

本书是作者在近几年讲授抽象代数(或近世代数)讲稿的基础上整理而形成的。作者在大连理工大学为数学类专业本科高年级学生和非数学类专业研究生多次讲授这门课程。写本书的初衷是想以尽可能直观、简洁和初等的语言,向学生较系统地介绍抽象代数学的基本思想、方法和技巧,以使学生初步了解和掌握抽象代数学研究的问题、使用的方法和技巧,为学生进一步学习代数学和其他学科奠定基础。

本书包含了抽象代数学中最基本的内容:第一章预备知识,介绍了学习抽象代数学的基本知识,如映射、等价关系、分类和代数系统等;第二章群,介绍了群、子群、正规子群和商群等,同时还着重强调了群在集合上的作用在研究群结构方面所起的作用,并以此为工具介绍了西罗(Sylow)定理和有限交换群的结构定理;第三章环,介绍了环、子环、理想、商环等,同时以多项式环为例,系统地讨论了环的唯一分解性等性质;第四章域,介绍了域和域的扩张理论,并较详细地介绍了伽罗瓦(Galois)基本定理及其应用。此外,在每一章后,我们还简单介绍了与该章有关的一点史料和某些重要数学家的生平。

根据我们的教学经验,完成本书全部内容的教学需要大约60学时。

在此我们对在本书的编辑出版过程中提出宝贵修改意见的审稿专家及编辑表示衷心感谢。由于作者水平有限,书中难免存在不少缺点和错误,敬请读者斧正。

王　颖　南基洙

2012年9月于大连理工大学创新园

目　录

第一章　预备知识

抽象代数的研究对象是有运算的集合，即代数系统. 确切地说，一个代数系统，是指由一个集合和定义在该集合中的一种或多种运算构成的一个系统. 在本章中我们先简单回顾与代数系统相关的集合和映射等概念，然后再引入代数系统的概念，并对其性质作一简单介绍.

第 1 节　集合与映射

我们首先简单回顾集合的相关概念，以及集合的一些运算性质，并给出剩余类集合及集合的笛卡儿积等概念.

我们称一些研究对象组成的总体为集合，构成集合的对象称为集合的元素. 令 A 是一个集合，若对象 a 属于 A，则用 $a\in A$ 表示；反之，若对象 a 不属于 A，那么用 $a\notin A$ 表示.

我们熟知的全体自然数就构成一个集合，以符号 $\mathbf{N}$ 表示；全体整数也构成一个集合，以符号 $\mathbf{Z}$ 表示. 类似地，全体有理数、实数和复数均构成集合，分别用 $\mathbf{Q}$，$\mathbf{R}$ 和 $\mathbf{C}$ 表示.

令 A 和 B 是两个集合. 若对于任意 $a\in A$ 都有 $a\in B$，则称集合 A 是集合 B 的子集合，记为 $A\subseteq B$ 或记为 $B\supseteq A$，读作 A 含于 B 或 B 包含 A. 特别地，如果 $A\subseteq B$ 并且 $B\subseteq A$，那么称集合 A 和 B 相等，记为 $A=B$.

我们规定不包含任何元素的集合为空集，并记为 $\varnothing$. 显然，$\varnothing$ 是任何集合的子集合，即对于任意的集合 A 都有 $\varnothing\subseteq A$.

代数学研究的一个根本目标就是对所研究的对象进行有目的的分类. 对于集合，可以给出一种最简单的分类：按集合中所含元素的个数分类. 如果一个集合含有有限多个元素，则称其为有限集. 否则，称其为无限集.

我们熟知的 $\mathbf{N}$，$\mathbf{Z}$，$\mathbf{Q}$，$\mathbf{R}$ 和 $\mathbf{C}$ 都是无限集. 当然，我们可以非常容易地写出一些有限集：$\{1,2,3\}$，$\{a_1,a_2,\cdots,a_n\}$，$\{x\mid -2\leqslant x\leqslant 3,x\in\mathbf{Z}\}$ 和{春，夏，秋，冬}等等. 另外，如果我们按“余数”考虑整数集合，则可以定义一些更有意思的、后文经常用到的无限集和有限集.

例如，如果我们对整数按被 3 除的余数进行考察的话，则有

(1) 被 3 除余数是 0 的整数集合的子集合为$\{0,\pm 3,\pm 6,\pm 9,\cdots\}$；

(2) 被 3 除余数是 1 的整数集合的子集合为$\{\cdots,-5,-2,1,4,7,\cdots\}$；

(3) 被3除余数是2的整数集合的子集合为$\{\cdots,-7,-4,-1,2,5,8,\cdots\}$.

进一步,如果我们把上面的这三个集合分别记为$\bar{0},\bar{1}$和$\bar{2}$,并将$\bar{0},\bar{1}$和$\bar{2}$看成是元素,那么可以构造一个新的有限集合$\{\bar{0},\bar{1},\bar{2}\}$,我们将其记为$\mathbf{Z}_3$.

对于任意的一个正整数$n\in\mathbf{Z}^+$($\mathbf{Z}^+$表示正整数集合),我们有如下的定义.

定义 1.1　设$a,b\in\mathbf{Z}$,若a,b被n除后余数相等,则称a与b模n同余,记其为$a\equiv b(\mathrm{mod}\ n)$,并称集合$\bar{a}=\{b\in\mathbf{Z}\mid b\equiv a(\mathrm{mod}\ n)\}$为模$n$与$a$同余的剩余类(也简称为模$n$的剩余类),其中的$a$则称为剩余类$\bar{a}$的代表元素.

显然,$\mathbf{Z}_3$是所有模3的剩余类构成的集合. 所有模n的剩余类构成的集合记为$\mathbf{Z}_n$,即$\mathbf{Z}_n=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{n-1}\}$.

命题 1.1　在$\mathbf{Z}_n$中下列结论成立:

(1) $a\in\bar{a}$;

(2) 若$b\in\bar{a}$,则$\bar{b}=\bar{a}$;

(3) $\bar{b}=\bar{a}$的充分必要条件是存在整数t,使得$a-b=nt$.

证　(1) 因为$a\equiv a(\mathrm{mod}\ n)$,所以$a\in\bar{a}$.

(2) 对任意$c\in\bar{b}$,由定义1.1知$c\equiv b(\mathrm{mod}\ n)$. 又由$b\in\bar{a}$有$b\equiv a(\mathrm{mod}\ n)$,因此$c\equiv a(\mathrm{mod}\ n)$,即$c\in\bar{a}$,所以$\bar{b}\subseteq\bar{a}$. 类似地,可以证明$\bar{b}\supseteq\bar{a}$,因此$\bar{b}=\bar{a}$.

(3) 若$\bar{b}=\bar{a}$,则由(1)知$b\in\bar{a}$,因此$b\equiv a(\mathrm{mod}\ n)$,再由整数的带余除法($x=yq+r$)可知存在整数$t$,使得$a-b=nt$. 反之,若$a-b=nt$,则$b\equiv a(\mathrm{mod}\ n)$. 所以,由(2)有$\bar{b}=\bar{a}$. □

由命题1.1(2)知$\bar{a}$中任何元素都是$\bar{a}$的代表元素,因此,剩余类的代表元素不唯一.

集合之间存在我们熟知的一些运算关系:

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

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

差集　$A-B=\{x\mid x\in A,x\notin B\}$等.

更一般地,基于某个指标集I(可以是无限集),我们可以定义

$$\bigcap_{i\in I}A_i=\{x\mid\forall i\in I,x\in A_i\},\quad\bigcup_{i\in I}A_i=\{x\mid\exists i\in I,x\in A_i\}$$

例如,$\{1,2,3\}\cap\{2,3,4,5\}=\{2,3\}$,$\{1,2,3\}\cup\{2,3,4,5\}=\{1,2,3,4,5\}$,$\{1,2,3\}-\{2,3,4,5\}=\{1\}$.

命题 1.2　设A,B,C均为集合,则

$$(A\cap B)\cup C=(A\cup C)\cap(B\cup C).$$

证　首先,证明$(A\cap B)\cup C\subseteq(A\cup C)\cap(B\cup C)$. 对任意$x\in(A\cap B)\cup C$,有

$x\in A\cap B$ 或 $x\in C$. 若 $x\in A\cap B$,则 $x\in A$ 且 $x\in B$,从而有 $x\in A\cup C$ 且 $x\in B\cup C$,即 $x\in(A\cup C)\cap(B\cup C)$. 若 $x\in C$,则 $x\in A\cup C$ 且 $x\in B\cup C$,从而 $x\in(A\cup C)\cap(B\cup C)$. 于是对任意 $x\in(A\cap B)\cup C$,总有 $x\in(A\cup C)\cap(B\cup C)$,即 $(A\cap B)\cup C\subseteq(A\cup C)\cap(B\cup C)$.

其次,证明 $(A\cap B)\cup C\supseteq(A\cup C)\cap(B\cup C)$. 对任意 $x\in(A\cup C)\cap(B\cup C)$,则有 $x\in A\cup C$ 且 $x\in B\cup C$. 如果 $x\notin C$,则有 $x\in A$ 且 $x\in B$,即 $x\in A\cap B$,所以 $x\in(A\cap B)\cup C$. 如果 $x\in C$,则显然有 $x\in(A\cap B)\cup C$. 于是,对任意 $x\in(A\cup C)\cap(B\cup C)$,总有 $x\in(A\cap B)\cup C$,即 $(A\cap B)\cup C\supseteq(A\cup C)\cap(B\cup C)$.

至此,有 $(A\cap B)\cup C=(A\cup C)\cap(B\cup C)$. □

事实上,关于集合的“∩,∪”运算,还有许多很好的性质.

例如,我们很容易验证

$$A\cap B=B\cap A,A\cup B=B\cup A,$$

$(A\cap B)\cap C=A\cap(B\cap C),(A\cup B)\cup C=A\cup(B\cup C)$ 等等.

定义 1.2　设 A 和 B 是两个集合,则称集合

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

为集合 A 和 B 的笛卡儿(Descartes)积,并规定

$$(a,b)=(x,y)\Leftrightarrow a=x,b=y.$$

一般地,我们可以定义 n(可以是无穷大)个集合的笛卡儿积为

$$\prod_{i=1}^{n}A_i=A_1\times\cdots\times A_i\times\cdots\times A_n=\{(a_1,\cdots,a_i,\cdots,a_n)\mid a_i\in A_i,1\leqslant i\leqslant n\},$$

并且规定

$$(a_1,\cdots,a_n)=(b_1,\cdots,b_n)\Leftrightarrow a_i=b_i,i=1,\cdots,n.$$

容易知道,有限个有限集合的笛卡儿积还是有限集合. 显然,$A\times\varnothing=\varnothing\times A=\varnothing$. 但是,在一般情况下 $A\times B\neq B\times A$. 例如,当 $A=\{1,2\},B=\{3,4\}$ 时,

$$A\times B=\{(1,3),(1,4),(2,3),(2,4)\}\neq\{(3,1),(3,2),(4,1),(4,2)\}=B\times A.$$

例 1.1　求集合 $\mathbf{Z}_2=\{\bar{0},\bar{1}\}$ 和 $\mathbf{Z}_5=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$ 的笛卡儿积.

解　$\mathbf{Z}_2\times\mathbf{Z}_5=\{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{0},\bar{3}),(\bar{0},\bar{4}),(\bar{1},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{2}),(\bar{1},\bar{3}),(\bar{1},\bar{4})\}$.

注意,$\mathbf{Z}_2$ 中的 $\bar{0},\bar{1}$ 与 $\mathbf{Z}_5$ 中的 $\bar{0},\bar{1}$ 的含义是有区别的.

下面,我们简单回顾一下与映射相关的概念及性质.

定义 1.3　设 A 和 B 是两个非空集合,φ 是它们元素之间的对应法则. 若对任意的 $a\in A$,在法则 φ 的作用下都有唯一的 $b\in B$ 与之对应,则称 φ 是集合 A 到 B 的映射,并记 $b=\varphi(a)$,而且称 b 是 a(在 φ 下)的像,a 是 b(在 φ 下)的原像.

若 φ 是集合 A 到 B 的映射且 $b=\varphi(a)$，则我们时常用

$$\begin{aligned}\varphi:A &\to B\\ a &\to b\end{aligned}$$

或 $A\xrightarrow{\varphi}B, a\xrightarrow{\varphi}b$ 表示之.

另外，对于 A 到 B 的映射 φ，若 A 中不同的元素在 φ 下的像不同，则称 φ 是单射，也就是说，对于 $a_1, a_2\in A$，当 $\varphi(a_1)=\varphi(a_2)$ 时，必有 $a_1=a_2$. 若 B 中的每个元素在 φ 下都有原像，则称 φ 是满射. 若 φ 既是单射又是满射，则称 φ 是双射（或称 φ 是一一映射）.

集合 A 到 A 自身的映射称为 A 上的变换. 对于变换，同样有单变换、满变换和双变换的概念.

设 φ 是集合 A 到 B 的映射，若 A_0 是 A 的子集合，则记 $\varphi(A_0)=\{\varphi(a)\mid a\in A_0\}$. 若 B_0 是 B 的子集合，则记 $\varphi^{-1}(B_0)=\{a\in A\mid \varphi(a)\in B_0\}$. 特别地，当 $B_0=\{b\}$ 为单点集时，记 $\varphi^{-1}(b)=\{a\in A\mid \varphi(a)=b\}$. 显然，若 $\varphi(A)=B$，则 φ 是满射.

例 1.2　设 A 是一个非空集合，定义

$$\begin{aligned}\varphi:A &\to A\\ a &\to a,\end{aligned}$$

即对于 $\forall a\in A$，有 $\varphi(a)=a$. 显然，φ 是映射. 一般地，我们称映射 φ 是 A 上的恒等映射. 显然，恒等映射是双变换. 集合 A 上的恒等映射记为 id_A 或者 1_A. 在不至于引起混淆的情况下，也可以将其简记为 id 或者 1.

例 1.3　定义

$$\begin{aligned}\varphi:\mathbf{Z} &\to \mathbf{Z}_3\\ n &\to \overline{n},\end{aligned}$$

即对任意的 $n\in\mathbf{Z}$，$\varphi(n)=\overline{n}$，易知 φ 是 $\mathbf{Z}$ 到 $\mathbf{Z}_3$ 的满射，但不是单射.

例 1.4　设 φ 是集合 A 到 B 的映射，A_0 是 A 的非空子集. 若 $\upsilon:A_0\to B$ 是 A_0 到 B 的映射，且对任意的 $a\in A_0$，有 $\upsilon(a)=\varphi(a)$，则称 υ 是 φ 在 A_0 上的限制，并记其为 $\upsilon=\varphi\mid_{A_0}$.

例 1.5　试证明

$$\begin{aligned}\varphi:\mathbf{Z}_n\times\mathbf{Z}_n &\to \mathbf{Z}_n\\ (\overline{a},\overline{b}) &\to \overline{ab}\end{aligned}$$

是一个映射.

证　对任意 $(\overline{a},\overline{b})=(\overline{c},\overline{d})$，有 $\overline{a}=\overline{c}$，$\overline{b}=\overline{d}$，于是由命题 1.1(3) 可知，存在整数 s,t 使得 $a-c=nt$，$b-d=ns$，所以 $ab-cd=(a-c)b+c(b-d)=n(tb-cs)$. 进而由命题 1.1(3) 得 $\overline{ab}=\overline{cd}$，即相等元素的像相等，$\varphi$ 是一个

映射.

例 1.6　试证明

$$\begin{aligned}\phi:\mathbf{Z}_n \times \mathbf{Z}_n &\to \mathbf{Z}_n\\ (\bar{a},\bar{b}) &\to \overline{a+b}\end{aligned}$$

是一个映射.

证　对任意$(\bar{a},\bar{b})=(\bar{c},\bar{d})$,有$\bar{a}=\bar{c},\bar{b}=\bar{d}$,于是由命题 1.1(3)可知,存在整数$s,t$使得$a-c=nt,b-d=ns$,所以$(a+b)-(c+d)=(a-c)+(b-d)=n(t+s)$.进而由命题 1.1(3)有$\overline{a+b}=\overline{c+d}$,即相等元素的像相等,$\phi$是一个映射.

例 1.7　试说明

$$\begin{aligned}\tau:\mathbf{Z}_2 \times \mathbf{Z}_3 &\to \mathbf{Z}_3\\ (\bar{a},\bar{b}) &\to \overline{ab}\end{aligned}$$

不是一个映射.

解　按照τ的定义有$(\bar{0},\bar{1})\to\bar{0},(\bar{0},\bar{1})=(\bar{2},\bar{1})\to\bar{2}$,即$(\bar{0},\bar{1})$的像不唯一,因此$\tau$不是一个映射.

定义 1.4　设ψ是集合A到B的映射,ϕ是集合B到C的映射,则存在映射$\phi\psi:A\to C$,满足对任意的$a\in A$,有$\phi\psi(a)=\phi(\psi(a))$.称映射$\phi\psi$是$\phi$与$\psi$的合成(如图 1.1).

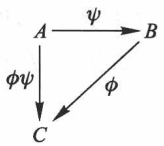


图 1.1

易知,映射的合成满足结合律,即对于映射$\psi:A\to B,\phi:B\to C$和$\sigma:C\to D$有$\sigma(\phi\psi)=(\sigma\phi)\psi$.且对任意映射$\psi:A\to B$,有$\psi\,\mathrm{id}_A=\psi$和$\mathrm{id}_B\psi=\psi$.

特别地,若ϕ是集合A上的变换,则我们用ϕ^t表示t个ϕ的合成,并规定$\phi^0=\mathrm{id}_A$.

例 1.8　令$2\mathbf{Z}$表示偶数集合,定义映射$\psi:\mathbf{Z}\to 2\mathbf{Z}$,使得$\psi(a)=2a$,和映射$\phi:2\mathbf{Z}\to\mathbf{Z}$,使得$\phi(a)=\frac{1}{2}a$,求$\psi\phi$和$\phi\psi$.

解　易知,合成映射$\phi\psi=\mathrm{id}_{\mathbf{Z}}$,合成映射$\psi\phi=\mathrm{id}_{2\mathbf{Z}}$.

定义 1.5　设ψ是集合A到B的映射,若存在集合B到A的映射ϕ,使得$\phi\psi=\mathrm{id}_A$并且$\psi\phi=\mathrm{id}_B$,则称ψ是可逆映射,ϕ是ψ的逆映射.

命题 1.3　设ψ是集合A到B的映射,若ψ是可逆映射,则ψ的逆映射是唯一的.

证　设ϕ和ϑ是ψ的两个逆映射,则

$$\vartheta=\mathrm{id}_A\vartheta=(\phi\psi)\vartheta=\phi(\psi\vartheta)=\phi\,\mathrm{id}_B=\phi.$$　□

既然逆映射是唯一的,如果ψ是可逆映射,那么以后我们将ψ的逆映射记

为 ψ^{-1}. 特别地,若 ψ 是集合 A 到 A 的可逆映射(变换),n 是正整数,则记 $\psi^{-n}=(\psi^{-1})^n$.

关于逆映射我们有如下性质.

命题 1.4　若 ψ 是集合 A 到 B 的可逆映射,ϕ 是集合 B 到 C 的可逆映射,则可逆映射的合成 $\phi\psi$ 还是可逆映射,并且 $(\phi\psi)^{-1}=\psi^{-1}\phi^{-1}$.

证　请读者自证. □

命题 1.5　设 A,B 是非空集合,$\psi:A\to B$ 是映射,则

(1) ψ 是单射的充分必要条件是存在映射 $\phi:B\to A$,使得 $\phi\psi=\mathrm{id}_A$;

(2) ψ 是满射的充分必要条件是存在映射 $\phi:B\to A$,使得 $\psi\phi=\mathrm{id}_B$.

证　在此我们只考证如果存在映射 $\phi:B\to A$,使得 $\phi\psi=\mathrm{id}_A$,则 ψ 是单射的情形.

事实上,如果 ψ 不是单射,那么存在 $a_1\neq a_2\in A$,使得 $\psi(a_1)=\psi(a_2)$. 从而

$$\mathrm{id}_A(a_1)=\phi\psi(a_1)=\phi\psi(a_2)=\mathrm{id}_A(a_2),$$

即 $a_1=a_2$,矛盾. □

以后为了讨论映射问题的方便,我们可使用图形表示映射的合成关系:多边形的顶点表示集合,有箭头的线段表示映射. 特别地,如果由始点集合 A 到终点集合 B 所经历的各条线路所组成的映射合成都相等,则称这样的图形是交换图. 例如,若 $f_nf_{n-1}\cdots f_2f_1=g_mg_{m-1}\cdots g_2g_1$,则称图 1.2 是交换图.

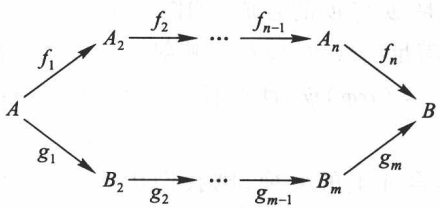


图 1.2

再例如,若 $A\xrightarrow{f}B,B\xrightarrow{g}C,A\xrightarrow{\sigma}C$ 是映射,并且它们满足 $gf=\sigma$,则图 1.3 是交换图.

类似地,若 $A\xrightarrow{f}B,C\xrightarrow{g}D,A\xrightarrow{\sigma}C,B\xrightarrow{\tau}D$ 是映射,并且它们满足 $\tau f=g\sigma$,则图 1.4 是交换图.

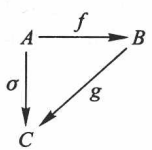


图 1.3

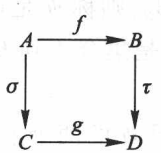


图 1.4

习题 1.1

1. 试写出集合 $\mathbf{Z}_4$ 中的所有元素.

2. 试写出集合 $\mathbf{Z}_3 \times \mathbf{Z}_5$ 和 $\mathbf{Z}_5 \times \mathbf{Z}_3$ 中的所有元素,并判断这两个集合是否相等.

3. 设 $a,b,c,d \in \mathbf{Z}, n \in \mathbf{Z}^+$,若 $ac \equiv bd (\mathrm{mod}\ n)$, $c \equiv d (\mathrm{mod}\ n)$,且 c 与 n 互素,证明 $a \equiv b (\mathrm{mod}\ n)$.

4. 设 A,B,C 都是集合,试证明 $C-(A \cup B)=(C-A) \cap (C-B)$.

5. 对于 $\mathbf{Z}_3$ 的元素 $\bar{0},\bar{1},\bar{2}$,我们有 $\bar{0} \cap \bar{1} = \varnothing, \bar{0} \cap \bar{2} = \varnothing, \bar{1} \cap \bar{2} = \varnothing$,并且 $\bar{0} \cup \bar{1} \cup \bar{2} = \mathbf{Z}$. 试分析对于 $\mathbf{Z}_5$ 的元素是否也具有这样的性质.

6. 设 $A=\{1,2,3\}$,试构造一个 $A \times A$ 到 A 的满射,并说明是否存在 $A \times A$ 到 A 的单射.

7. 请分别讨论例 1.5 和例 1.6 中的映射是否是满射,是否是单射?

8. 设 φ 是集合 A 到 B 的映射,证明 φ 是双射的充分必要条件是 φ 是可逆映射.

9. 设 $M_n(\mathbf{R})$ 是实数域 $\mathbf{R}$ 上所有 n 阶方阵构成的集合,$V_n(\mathbf{R})$ 是实数域 $\mathbf{R}$ 上的 n 维线性空间,试给出 $M_n(\mathbf{R})$ 到 $V_n(\mathbf{R})$ 的一个满射.

10. 试证明

$$\phi:(\mathbf{Z}_2 \times \mathbf{Z}_3) \times (\mathbf{Z}_2 \times \mathbf{Z}_3) \to \mathbf{Z}_2 \times \mathbf{Z}_3$$

$$((\bar{a}_1,\bar{b}_1),(\bar{a}_2,\bar{b}_2)) \to \left(\overline{a_1 a_2}, \overline{b_1 + b_2}\right)$$

是映射.

第 2 节　置换集合 S_n

令 A 是含有 n 个元素的集合,$S_n=\{\sigma \mid \sigma$ 是 A 上的双射$\}$. 一般地,我们称 S_n 中的元素为 n 元置换. 不妨令集合 $A=\{1,2,\cdots,n\}$,则任意置换 $\sigma \in S_n$ 均可以表示成如下形式:

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

又由于 σ 是 A 上的双射,所以 $\sigma(1),\sigma(2),\cdots,\sigma(n)$ 是 $1,2,\cdots,n$ 的一个全排列. 反之,对 $1,2,\cdots,n$ 的任意一个全排列 $i_1,i_2,\cdots,i_n$ 都能给出一个置换

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},$$

并且对不同的全排列给出不同的置换,所以 S_n 含有 $n!$ 个元素. 特别地,当 $n=1$ 时,S_n 只含有一个元素,即恒等变换 1. 在以下的讨论中,我们总假定 $n>1$.

例 2.1　设 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$,试计算 $\sigma\varphi$ 和

$\varphi\tau\sigma$.

解 我们先来求 $\sigma\varphi$. 因为 $\sigma\varphi(1)=\sigma(2)=3,\sigma\varphi(2)=\sigma(1)=2,\sigma\varphi(3)=\sigma(3)=1$,因此,$\sigma\varphi=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$.

实际上,这个过程可以用下式表示:

$$\sigma\varphi=\begin{pmatrix}1&2&3&\\\downarrow&\downarrow&\downarrow&\varphi\\2&1&3&\\\downarrow&\downarrow&\downarrow&\sigma\\3&2&1&\end{pmatrix}$$

类似地,我们可以求 $\varphi\tau\sigma$,如下式:

$$\varphi\tau\sigma=\begin{pmatrix}1&2&3&\\\downarrow&\downarrow&\downarrow&\sigma\\2&3&1&\\\downarrow&\downarrow&\downarrow&\tau\\2&1&3&\\\downarrow&\downarrow&\downarrow&\varphi\\1&2&3&\end{pmatrix}$$

因此,$\varphi\tau\sigma=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=\mathrm{id}$.

定义 2.1 设 $\sigma\in S_n$,若在集合 $\{1,2,\cdots,n\}$ 中存在 t 个不同的数 $i_1,i_2,\cdots,i_t$,使得 $\sigma(i_1)=i_2,\sigma(i_2)=i_3,\cdots,\sigma(i_{t-1})=i_t,\sigma(i_t)=i_1$,并且对于 $\{i_1,i_2,\cdots,i_t\}$ 之外的 $n-t$ 个元素(如果存在的话),在 σ 的作用下都保持不变,即 $\sigma(i)=i$,则称 σ 是长度为 t 的轮换,记其为 $\sigma=(i_1i_2\cdots i_t)$.

特别地,长度为 2 的轮换称为对换. S_n 中的恒等变换称为长度是 1 的轮换,记为(1). 对于两个轮换 $(i_1i_2\cdots i_t)$ 和 $(j_1j_2\cdots j_s)$,如果对于任意的 $k\in\{1,2,\cdots,t\}$,$l\in\{1,2,\cdots,s\}$ 都有 $i_k\neq j_l$,即 $\{i_1,i_2,\cdots,i_t\}\cap\{j_1,j_2,\cdots,j_s\}=\varnothing$,则称这两个轮换是不相交的.

显然,若 $\sigma=(i_1i_2\cdots i_t)$ 和 $\tau=(j_1j_2\cdots j_s)$ 是 S_n 中两个不相交的轮换,则它们的合成是可交换的,即 $(i_1i_2\cdots i_t)(j_1j_2\cdots j_s)=(j_1j_2\cdots j_s)(i_1i_2\cdots i_t)$.

例 2.2 判断置换 $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\1&3&7&4&6&2&5\end{pmatrix}$ 是否是轮换.

解 在集合 $\{1,2,3,4,5,6,7\}$ 中有 5 个数 2,3,7,5,6 满足 $\sigma(2)=3,\sigma(3)=7,\sigma(7)=5,\sigma(5)=6$ 和 $\sigma(6)=2$,而且对于余下的两个数 1 和 4 有 $\sigma(1)=1,\sigma(4)=4$. 因此,根据定义 2.1,σ 是长度为 5 的轮换,且 $\sigma=(23756)$.

注意,在一般情况下,置换不一定是轮换. 例如,置换 $\sigma=\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix}$ 就不是轮换.

定理 2.1　每一个置换可以表示成不相交的轮换的合成.

证　不妨设 $\sigma\in S_n$ 且 $\sigma\neq(1)$.

首先,取 $i_1\in\{1,2,\cdots,n\}$,并要求其满足 $\sigma(i_1)\neq i_1$. 由于 $i_1,\sigma(i_1),\sigma^2(i_1),\cdots\in\{1,2,\cdots,n\}$,故必存在 $t_1<t_2$,使得 $\sigma^{t_1}(i_1)=\sigma^{t_2}(i_1)$,即有 $\sigma^{t_2-t_1}(i_1)=i_1$. 若令 t 是满足 $\sigma^t(i_1)=i_1$ 的最小正整数,那么从 i_1 的选取方法,我们可知 $t>1$,并且 σ 在 $\{i_1,\sigma(i_1),\sigma^2(i_1),\cdots,\sigma^{t-1}(i_1)\}$ 上的限制构成一个轮换.

其次,如果 $\{i_1,\sigma(i_1),\sigma^2(i_1),\cdots,\sigma^{t-1}(i_1)\}$ 之外的元素在 σ 作用下都保持不动,那么 $\sigma=(i_1\sigma(i_1)\sigma^2(i_1)\cdots\sigma^{t-1}(i_1))$,即 σ 是(单个)轮换的合成. 否则,我们可以在 $\{i_1,\sigma(i_1),\sigma^2(i_1),\cdots,\sigma^{t-1}(i_1)\}$ 之外选取一个在 σ 作用下变动的元素 i_2. 然后,对 i_2 重复上述过程,则存在 $s>1$,使得 σ 在 $\{i_2,\sigma(i_2),\sigma^2(i_2),\cdots,\sigma^{s-1}(i_2)\}$ 上的限制构成一个轮换. 如果 $\{i_1,\sigma(i_1),\sigma^2(i_1),\cdots,\sigma^{t-1}(i_1)\}\cup\{i_2,\sigma(i_2),\sigma^2(i_2),\cdots,\sigma^{s-1}(i_2)\}$ 之外的元素在 σ 作用下都保持不动,那么 $\sigma=(i_1\sigma(i_1)\sigma^2(i_1)\cdots\sigma^{t-1}(i_1))(i_2\sigma(i_2)\sigma^2(i_2)\cdots\sigma^{s-1}(i_2))$ 且 $(i_1\sigma(i_1)\sigma^2(i_1)\cdots\sigma^{t-1}(i_1))$ 与 $(i_2\sigma(i_2)\sigma^2(i_2)\cdots\sigma^{s-1}(i_2))$ 互不相交(注意,对任意 $k,l\in\mathbf{Z},\sigma^k(i_2)\neq\sigma^l(i_1)$,否则导致 $i_2=\sigma^{l-k}(i_1)$,这与 i_2 的选取矛盾),即 σ 可以表示成不相交的两个轮换的合成. 否则,再重复上面的讨论过程,由于 $n<\infty$,所以,我们一定可以在有限步之内完成上述讨论,即得到分解式的存在性. □

例 2.3　试将 S_7 中的置换 $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\1&7&2&6&5&4&3\end{pmatrix}$ 表示成不相交的轮换的合成.

解　因为 $\sigma(2)\neq2$ 且 $\sigma(2)=7,\sigma(7)=3,\sigma(3)=2$,因此,$\sigma$ 在集合 $\{2,7,3\}$ 上的限制是轮换(273). 又因为 $4\notin\{2,7,3\}$ 且 $\sigma(4)=6,\sigma(6)=4$,因此,σ 在集合 $\{4,6\}$ 上的限制是轮换(46). 又因为 $1,5\notin\{2,7,3\}\cup\{4,6\}$,且 $\sigma(1)=1$,$\sigma(5)=5$,所以,根据定理 2.1 知 σ 是不相交的两个轮换(273)和(46)的合成,即 $\sigma=(273)(46)$.

例 2.4　试将 S_5 中的置换 $\sigma=\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix}$ 表示成不相交的轮换的合成.

解　因为 $\sigma(1)\neq1$ 且 $\sigma(1)=2,\sigma(2)=5,\sigma(5)=1$,因此,$\sigma$ 在集合 $\{1,2,5\}$ 上的限制是轮换(125). 又因为 $3\notin\{1,2,5\}$ 且 $\sigma(3)=4,\sigma(4)=3$,因此,σ 在集合 $\{3,4\}$ 上的限制是轮换(34). 另外 $\{1,2,5\}\cup\{3,4\}=\{1,2,3,4,5\}$,所以,根

据定理2.1,我们知道 σ 是不相交的两个轮换(125)和(34)的合成,即 $\sigma=(125)(34)$.

例2.5 易见,在 S_3 中,$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12)$,$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(13)$和$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(23)$是长度为2的轮换.$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(123)$和$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132)$是长度为3的轮换.此外,容易验证,$(123)=(13)(12)$,$(132)=(12)(13)$,$(1)=(12)(12)$,即对于 S_3 中的元素来说,每个置换都是轮换且可以用对换表示,即 $S_3=\{(1),(12),(13),(23),(12)(13),(13)(12)\}$.

更一般地,关于轮换与对换的关系,我们有:

例2.6 设 $\sigma=(i_1i_2\cdots i_t)$ 是 S_n 中的一个轮换,则容易验证

$$\sigma=(i_1i_t)(i_1i_{t-1})\cdots(i_1i_3)(i_1i_2)=(i_1i_2)(i_2i_3)\cdots(i_{t-2}i_{t-1})(i_{t-1}i_t),$$

即 S_n 中每个轮换都可以表示成对换合成的形式.

由此,再结合定理2.1,我们可知每个置换可以表示成对换合成的形式,但表达式不唯一.

例2.7 试将置换 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&1&4&5&3&2\end{pmatrix}$ 表示成对换合成的形式.

解 我们先将置换表示成轮换合成的形式,然后再将轮换表示成对换合成的形式.因为

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&1&4&5&3&2\end{pmatrix}=(162)(345),(162)=(16)(62),(345)=(34)(45),$$

所以,$\sigma=(16)(62)(34)(45)$.

定理2.2 若将置换表示成对换合成的形式,则其表达式中出现的对换个数的奇偶性保持不变.

证 设 $\sigma\in S_n$,n 阶单位矩阵 $\boldsymbol{E}=(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n)$,其中 $\boldsymbol{e}_i(i=1,2,\cdots,n)$ 是 n 维单位列向量.我们规定 $\sigma(\boldsymbol{E})=(\boldsymbol{e}_{\sigma(1)},\boldsymbol{e}_{\sigma(2)},\cdots,\boldsymbol{e}_{\sigma(n)})$.于是若 $\sigma=\sigma_m\cdots\sigma_2\sigma_1$,其中每个 σ_i 都是对换,那么

$$\det(\sigma(\boldsymbol{E}))=(-1)^m\det\boldsymbol{E}=(-1)^m.$$

因此,若 $\sigma=\sigma_m\cdots\sigma_2\sigma_1=\sigma_k'\cdots\sigma_2'\sigma_1'$,其中 $\sigma_1,\cdots,\sigma_m,\sigma_1',\cdots,\sigma_k'$ 都是对换,那么有 $\det(\sigma(\boldsymbol{E}))=(-1)^m=(-1)^k$,所以 m 与 k 的奇偶性相同. □

定义2.2 如果一个置换可写成偶数个对换合成的形式,那么称其为偶置换,否则称其为奇置换.

显然,两个偶置换的合成是偶置换,两个奇置换的合成是偶置换,偶置换(奇置换)与奇置换(偶置换)的合成是奇置换.

实际上,如果令 $\sigma=\sigma_m\cdots\sigma_2\sigma_1\in S_n$,其中每个 σ_i 都是对换,那么可以将置换

σ 的符号函数定义为 $\varepsilon(\sigma)=(-1)^m$，即

$$\varepsilon: S_n \to \{1, -1\}$$
$$\sigma \to \varepsilon(\sigma).$$

当然，这样定义的 ε 确实是映射. 而且偶置换的符号函数为 1，奇置换的符号函数为 -1.

例 2.8　设 $\sigma=(i_1 i_2 \cdots i_t)$ 是 S_n 中的一个轮换，则由例 2.6 可知 $\varepsilon(\sigma)=(-1)^{t-1}$. 这就是说，长度为偶数的轮换是奇置换，长度为奇数的轮换是偶置换.

定理 2.3　若令 $A_n(n>1)$ 表示 S_n 中所有偶置换构成的集合，则

$$|A_n|=\frac{|S_n|}{2}=\frac{n!}{2},$$

其中 $|A_n|$，$|S_n|$ 分别表示集合 A_n，S_n 中所含元素的个数.

证　因为 A_n 是 S_n 中偶置换构成的集合，所以 S_n-A_n 是 S_n 中奇置换构成的集合，若这两个集合所含元素个数相等，则结论得证. 令

$$\varphi: A_n \to (S_n - A_n)$$
$$\sigma \to (12)\sigma,$$

则容易验证 φ 是双射，从而 $|A_n|=|S_n-A_n|$. □

命题 2.1　在 $S_n(n\geqslant 3)$ 中，任意两个对换的合成可以表示成长度为 3 的轮换的合成. 任意偶置换可以写成长度为 3 的轮换的合成.

证　设 (ij) 和 (kl) 是 $S_n(n\geqslant 3)$ 中两个对换. 若 (ij) 和 (kl) 不相交，则 $(ij)(kl)=(ij)(jk)(jk)(kl)=(ijk)(jkl)$. 若这两个对换相交，但不相同，则不妨令它们的合成为 $(ij)(jk)$，则 $(ij)(jk)=(ijk)$. 若这两个对换相同，则不妨令它们的合成为 $(ij)(ij)$. 因为 $n\geqslant 3$，所以存在 $t\neq i,j$，使得 $(ij)(ij)=(ij)(it)(it)(ij)=(itj)(ijt)$. 即任意两个对换的合成可以表示成长度为 3 的轮换的合成. 因此任意偶置换可以写成长度为 3 的轮换的合成. □

例 2.9　在 $S_n(n\geqslant 3)$ 中，试将置换 (1)，$(12)(34)$，$(12)(23)$ 表示成长度为 3 的轮换的合成.

解　$(1)=(12)(12)=(132)(123)$，$(12)(34)=(123)(234)$，$(12)(23)=(123)$.

习题 1.2

1. 在 S_5 中，令 $\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&4&1&5\end{pmatrix}$，$\tau=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}$，试计算 $\sigma^2\tau$.

2. 设置换 $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&8&1&3&2&7&5&6\end{pmatrix}$，