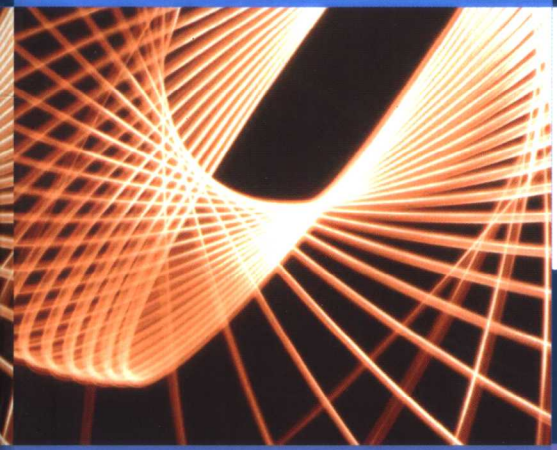
抽象代数基础

高等学校教材



抽象代数基础

唐忠明

唐忠明

高等教育出版社
HIGHER EDUCATION PRESS

高等教育出版社

高等学校教材

抽象代数基础

唐忠明

高等教育出版社

内容提要

本书是作者根据给苏州大学国家理科基地(数学)班多年讲授抽象代数课程的讲义整理编写而成的。

本书的内容除了传统的群、环和域外还包含了模。在域论中,讨论了尺规作图问题;在模论中,讨论了在线性代数和有限交换群中有重要应用的主理想整环上的有限生成挠模。这些内容的加入将使学生了解抽象代数的应用性。

本书可作为高等院校数学类专业的教材或教学参考书。

图书在版编目(CIP)数据

抽象代数基础/唐忠明.—北京:高等教育出版社,
2006.4
ISBN 7-04-018690-X

Ⅰ.抽… Ⅱ.唐… Ⅲ.抽象代数-高等学校-
教学参考资料 Ⅳ.0153

中国版本图书馆 CIP 数据核字(2006)第 014435 号

策划编辑 李 蕊 **责任编辑** 崔梅萍 **封面设计** 王凌波 **责任绘图** 宗小梅
版式设计 范晓红 **责任校对** 金 辉 **责任印制** 陈伟光

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100011	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	涿州市星河印刷有限公司	**畅想教育**	http://www.widedu.com
开 本	787×960 1/16	**版 次**	2006 年 3 月第 1 版
印 张	7	**印 次**	2006 年 3 月第 1 次印刷
字 数	120 000	**定 价**	9.50 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

物料号 18690-00

前　言

抽象代数(或近世代数)是数学专业的重要课程。抽象代数的知识不仅是纯粹数学和应用数学工作者所必备的,而且在物理、化学和通信等领域都有广泛的应用。所以,学好抽象代数对数学专业的学生来说相当重要。

本书是根据作者给苏州大学国家理科基地(数学)班多年讲授抽象代数课程的讲义整理编写而成的。在编写本书时,首先碰到的问题是:什么是抽象代数的最基本又是最重要的内容?我们认为,除了传统的群论、环论和域论外还应包括模论,因为,只有用模论才能在更高的层次上讨论线性代数,而这正是学习抽象代数的一个目的。再进一步的问题是:如何处理每一部分的内容?为了使学生能清楚地掌握理论的主线,我们不主张,为了把一个概念说得更清楚而又把有关的更一般的概念加进来。例如,我们不过多地讨论左、右单位元,左、右可逆元和群的等价定义,因为,相对于后面的重要理论,这些概念之间的关系并不重要。我们注重主要知识的传授,表述力求简明扼要,避免形式的、繁琐的推广,使学生抓住主要的东西。同时,我们给学生留下思考的空间,有些细节和简单的结论留给了学生或作为习题,有些习题的结论在后面的正文中还会用到,所以做好每道习题也很重要。在本书中,我们列入了尺规作图问题和主理想整环上的有限生成挠模及在线性代数中的应用的内容。通过这些内容的学习,会使学生理解:抽象代数中的抽象概括是实际的需要,抽象的理论有广泛的应用。

本书分为四章,分别由群论、环论、域论和模论组成。每章的最后一节或两节,即第一章的第7节、第二章的第6、7节、第三章的第5、6节和第四章的第5、6节,是这一章的重点内容,也是进一步学习的起点。作为教材,本书的内容可以在一学期(每周4课时)授完。

中国科学院万哲先院士和复旦大学许永华教授仔细审阅了本书并提出了许多宝贵的修改意见,作者在此表示衷心的感谢。

限于作者的水平,本书一定会有许多不足之处,敬请读者提出宝贵意见。

唐忠明

2005年10月于苏州大学

郑重声明

目　录

第一章 群 论

§1 代数运算

本书讨论的群、环、域和模等都是具有满足一定条件的代数运算的代数结构，所以，我们首先讨论代数运算.

设 $A_1, A_2, \cdots, A_n$ 是非空集合，令 $A_1, A_2, \cdots, A_n$ 的**卡氏积**为

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i, i = 1, 2, \cdots, n\}.$$

定义 1.1 设 A 是一个非空集合，$A \times A$ 到 A 的映射 f 称为是集合 A 上的一个(二元)**代数运算**.

设 f 是集合 A 上的一个代数运算，则由映射的定义，对 A 中任意两个元素 a, b，在运算 f 下，都有 A 中唯一确定的元素 c 使得 $c = f(a, b)$，一般地，记为 $afb = c$. 通常记代数运算为“$\cdot$”，称为**乘法**，称 c 为 a 与 b 的**乘积**，记为 $a \cdot b = c$.

我们见过很多代数运算的例子.

例如，设 $\mathbb{P}$ 是数域，V 是 $\mathbb{P}$ 上的一个向量空间，则加法“+”是 V 上的一个代数运算，加法“+”和乘法“$\cdot$”都是 $\mathbb{P}$ 上的代数运算.

又例如，设 $\mathbb{P}^{n \times n}$ 是 $\mathbb{P}$ 上的 n 阶方阵构成的集合，则矩阵的加法和乘法也都是 $\mathbb{P}^{n \times n}$ 上的代数运算.

类似地，我们可以定义一元代数运算，三元代数运算以及一般的 n 元代数运算. 例如，若令 $\mathbb{P}^*$ 是 $\mathbb{P}$ 中非零元素构成的集合，则取逆：

$$\begin{aligned} \mathbb{P}^* &\to \mathbb{P}^* \\ a &\mapsto a^{-1} \end{aligned}$$

是 $\mathbb{P}^*$ 上的一个一元运算. 本书讨论的代数结构上的代数运算都是二元代数运算，所以，我们不对一般的 n 元运算加以讨论，以后所称的代数运算都是二元代数运算.

有限集上的代数运算可以用简单具体的方法表示出来. 设 $A = \{a_1, a_2, \cdots, a_n\}$ 是有限集，则 A 上的代数运算可以用一个乘法表来表示

$\cdot$	a_1	a_2	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nn}

其中 $a_{ij}=a_i\cdot a_j$，$i,j=1,2,\cdots,n$. 例如，令 $A=\{e,a,b,c\}$，定义 A 上的乘法“$\cdot$”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

我们要讨论的代数运算都是满足一定性质的，下面的结合律是最基本的性质.

定义 1.2 设“$\cdot$”是非空集合 A 上的一个代数运算.

(1) 如果，对 $\forall a,b,c\in A$ 都有

$$(a\cdot b)\cdot c=a\cdot(b\cdot c),$$

则称“$\cdot$”适合**结合律**.

(2) 如果，对 $\forall a,b\in A$ 都有

$$a\cdot b=b\cdot a,$$

则称“$\cdot$”适合**交换律**.

(3) 如果，对 $\forall a,b,c\in A$，由 $a\cdot b=a\cdot c$ 必有 $b=c$，则称“$\cdot$”适合**左消去律**；如果，对 $\forall a,b,c\in A$，由 $b\cdot a=c\cdot a$ 必有 $b=c$，则称“$\cdot$”适合**右消去律**；如果“$\cdot$”既适合左消去律又适合右消去律，则称“$\cdot$”适合**消去律**.

例如，设 V 是向量空间，则 V 上的加法适合结合律、交换律和消去律.

根据矩阵的性质，我们知道，矩阵的乘法适合结合律. 由于对任意两个 n 阶方阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$，$\boldsymbol{AB}$ 与 $\boldsymbol{BA}$ 不一定相等且当 $\boldsymbol{A}\neq\boldsymbol{O},\boldsymbol{B}\neq\boldsymbol{O}$ 时，$\boldsymbol{AB}=\boldsymbol{O}$ 是可能成立的，所以 $\mathbb{P}^{n\times n}$ 上的矩阵乘法既不适合交换律也不适合消去律.

有限集上的代数运算根据乘法表可以很容易地看出其是否适合交换律和消去律. 设 $A=\{a_1,a_2,\cdots,a_n\}$，“$\cdot$”是 A 上的代数运算，乘法表为

$\cdot$	a_1	a_2	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nn}

令矩阵 $\boldsymbol{X}=(a_{ij})_{n\times n}$，则易见，“$\cdot$”适合交换律当且仅当 $\boldsymbol{X}$ 为对称矩阵；“$\cdot$”适合

左(右)消去律当且仅当 $\boldsymbol{X}$ 的每一行(列)都是 $a_1, a_2, \cdots, a_n$ 的一个排列.

例如,从前面定义的 $A=\{e,a,b,c\}$ 的乘法表立即得到这个乘法是适合交换律和消去律的.

尽管乘法"$\cdot$"只是对两个元素定义的,但当"$\cdot$"适合结合律时,我们可以对任意有限多个元素进行乘法,这是因为,任意 n 个元素 $a_1, a_2, \cdots, a_n$ 的乘积(在不改变元素的顺序的前提下)与所加括号无关(习题 2),记为 $a_1 \cdot a_2 \cdot \cdots \cdot a_n$. 例如,$n=4$ 时

$$\begin{aligned}((a_1 \cdot a_2) \cdot a_3) \cdot a_4 &= (a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = a_1 \cdot ((a_2 \cdot a_3) \cdot a_4) \\ &= (a_1 \cdot (a_2 \cdot a_3)) \cdot a_4 = a_1 \cdot (a_2 \cdot (a_3 \cdot a_4)).\end{aligned}$$

对 $\forall\, n \geqslant 1$,令

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

称之为 a 的 n 次**幂**. 易见 $a^m \cdot a^n = a^{m+n}$, $(a^n)^m = a^{nm}$. 进一步地,若"$\cdot$"又适合交换律,则

$$(a \cdot b)^n = a^n \cdot b^n.$$

习题

1. 设 $A=\{e,a,b,c\}$, A 上的乘法"$\cdot$"的乘法表如定义 1.2 前,证明:"$\cdot$"适合结合律.

2. 设"$\cdot$"是集合 A 上一个适合结合律的代数运算,对于 A 中的元素,归纳定义 $\prod\limits_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \cdots \cdot a_n$ 为: $\prod\limits_{i=1}^{1} a_i = a_1$; $\prod\limits_{i=1}^{r+1} a_i = \left(\prod\limits_{i=1}^{r} a_i\right) \cdot a_{r+1}$,证明:

$$\left(\prod_{i=1}^{n} a_i\right) \cdot \left(\prod_{j=1}^{m} a_{n+j}\right) = \prod_{k=1}^{n+m} a_k.$$

进而证明:在不改变元素的顺序的前提下,A 中的元素的乘积与所加括号无关.

3. 设$\mathbb{Q}$ 是有理数集,对 $\forall\, a, b \in \mathbb{Q}$,令 $a \cdot b = a + b^2$,证明:"$\cdot$"是$\mathbb{Q}$ 上的一个代数运算,它既不适合结合律也不适合交换律.

§2 群的概念

群是我们要讨论的第一个代数结构,后面讨论的环、域和模等代数结构都是以群为基础的.

定义 2.1 设 G 是一个非空集合,"$\cdot$"是 G 上的一个代数运算,如果"$\cdot$"满足下列条件

(1) "·"适合结合律;

(2) 存在 $e\in G$,使得对 $\forall a\in G$ 都有 $a\cdot e=e\cdot a=a$;

(3) 对 $\forall a\in G$,存在 $b\in G$ 使得

$$a\cdot b=b\cdot a=e,$$

则称 G 关于代数运算"·"构成一个**群**,也称$(G,\cdot)$构成一个**群**.

设$(G,\cdot)$是一个群,如果 G 是有限集(无限集),则称$(G,\cdot)$是**有限群(无限群)**;称 G 中所含元素的个数为群$(G,\cdot)$的**阶**,记为$|G|$;如果"·"适合交换律,则称$(G,\cdot)$是**交换群**或 Abel **群**.

事实上,以前我们见到过许多群.例如:设 V 是一个向量空间,则 V 关于加法"+"构成一个交换群.

令$\mathbb{Z}$是所有整数构成的集合,则$\mathbb{Z}$关于加法也构成一个交换群.

对于$\mathbb{P}^{n\times n}$,由于加法"+"适合结合律和交换律,存在 n 阶零矩阵 $\boldsymbol{O}$ 使得对 $\forall \boldsymbol{A}\in\mathbb{P}^{n\times n}$都有 $\boldsymbol{O}+\boldsymbol{A}=\boldsymbol{A}+\boldsymbol{O}=\boldsymbol{A}$,且有 $-\boldsymbol{A}\in\mathbb{P}^{n\times n}$使得 $\boldsymbol{A}+(-\boldsymbol{A})=(-\boldsymbol{A})+\boldsymbol{A}=\boldsymbol{O}$,所以$\mathbb{P}^{n\times n}$关于矩阵加法构成一个交换群.

然而,尽管$\mathbb{P}^{n\times n}$上的乘法适合结合律且有单位矩阵 $\boldsymbol{E}$ 使得对 $\forall \boldsymbol{A}\in\mathbb{P}^{n\times n}$都有 $\boldsymbol{A}\cdot\boldsymbol{E}=\boldsymbol{E}\cdot\boldsymbol{A}=\boldsymbol{A}$,但定义 2.1 中的条件(3)不成立,所以$\mathbb{P}^{n\times n}$关于矩阵乘法不构成群.

但是,若令 G 是$\mathbb{P}$上所有 n 阶可逆矩阵所构成的集合,则关于矩阵的乘法 G 构成一个群.这是因为,由可逆矩阵的乘积仍是可逆矩阵知矩阵的乘法是 G 上的一个代数运算,又矩阵乘法适合结合律,存在单位矩阵 $\boldsymbol{E}\in G$ 使得对 $\forall \boldsymbol{A}\in G$ 都有 $\boldsymbol{A}\cdot\boldsymbol{E}=\boldsymbol{E}\cdot\boldsymbol{A}=\boldsymbol{A}$,且对 $\forall \boldsymbol{A}\in G$ 存在 $\boldsymbol{A}^{-1}\in G$ 使得 $\boldsymbol{A}\cdot\boldsymbol{A}^{-1}=\boldsymbol{A}^{-1}\cdot\boldsymbol{A}=\boldsymbol{E}$.通常称 G 为$\mathbb{P}$上的 n 级**一般线性群**,记为 $GL_n(\mathbb{P})$.

设 $G=\{e,a,b,c\}$,G 上的代数运算"·"的乘法表如定义 1.2 前,则"·"适合结合律(§1 习题 1)和交换律,从乘法表中易见 e 对 $\forall u\in G$ 都有 $u\cdot e=e\cdot u=u$,且对 $\forall u\in G$,存在 $v(=u)\in G$ 使得 $u\cdot v=v\cdot u=e$,所以$(G,\cdot)$构成一个群,称之为 Klein **四元群**.

尽管在群的定义中,没有要求元素 e 及任意元素 a 所对应的 b 唯一,事实上它们都是唯一的.

命题 2.2 设$(G,\cdot)$是一个群,则存在唯一的元素 $e\in G$,使得对 $\forall a\in G$ 都有

$$a\cdot e=e\cdot a=a.$$

证明 由群的定义,存在 $e\in G$,使得对 $\forall a\in G$ 都有

$$e\cdot a=a\cdot e=a.$$

下证这样的 e 是唯一的.如果 $e'\in G$ 也具有性质:对 $\forall a\in G$ 都有

$$e'\cdot a=a\cdot e'=a.$$

则 $e'=e\cdot e'=e$. 所以,存在唯一的元素 $e\in G$,使得对 $\forall a\in G$ 都有 $a\cdot e=e\cdot a=a$. □

这样唯一确定的元素 e 称为是群$(G,\cdot)$的**单位元**.

命题 2.3 设$(G,\cdot)$是一个群,则对 $\forall a\in G$,存在唯一的元素 $b\in G$ 使得

$$a\cdot b=b\cdot a=e.$$

证明 对 $\forall a\in G$,由群的定义,存在 $b\in G$ 使得

$$a\cdot b=b\cdot a=e.$$

下证这样的 b 是唯一的. 如果 $b'\in G$ 也满足 $a\cdot b'=b'\cdot a=e$,则

$$b'=b'\cdot e=b'\cdot a\cdot b=e\cdot b=b.$$

所以,存在唯一的 $b\in G$ 使得 $a\cdot b=b\cdot a=e$. □

对 $\forall a\in G$,唯一存在的满足 $a\cdot b=b\cdot a=e$ 的元素 b,称之为 a 的**逆元**,记为 a^{-1}.

因而,群的定义可以表述为:

设"$\cdot$"是非空集合 G 上的一个代数运算,如果"$\cdot$"适合结合律,G 中存在单位元且每个元素都有逆元,则称$(G,\cdot)$构成一个**群**.

在§1中,对一般的适合结合律的代数运算,我们只能定义一个元素的正整数次幂,但在群中,我们可以定义一个元素的任意整数次幂. 设$(G,\cdot)$是群,则对 $\forall n\in\mathbb{Z},a\in G$,$a$ 的 n 次**幂**定义为

$$a^n=\begin{cases}\underbrace{a\cdot a\cdot\cdots\cdot a}_{n\text{个}}, & n>0,\\ e, & n=0,\\ (a^{-1})^{-n}, & n<0.\end{cases}$$

对于群$(\mathbb{Z},+)$中的任意元素 a,a 的 n 次"幂"就是:

$$na=\begin{cases}\underbrace{a+a+\cdots+a}_{n\text{个}}, & n>0,\\ 0, & n=0,\\ (-n)(-a), & n<0.\end{cases}$$

今后,群$(G,\cdot)$简记为 G,元素 a,b 的乘积 $a\cdot b$ 简写为 ab,G 的单位元记为 e.

下面我们来讨论两类群:变换群和置换群,它们是特殊的群,但由§6中的Cayley定理知道,它们又是最一般的群,因而具有重要的地位.

定义 2.4 设 A 是一个非空集合,称 A 到 A 的映射为 A 的**变换**,称 A 到 A 上的一一对应(即 1-1 的且到上的对应)为 A 的**一一变换**.

令 X 是 A 的所有变换构成的集合,则映射的合成"$\cdot$"定义了 X 上的一个代数运算:$\forall f,g\in X$,

$$(f\cdot g)(a)=f(g(a)),a\in A,$$

称之为**变换的乘积**,易见这乘积适合结合律.

命题 2.5 设 A 是一个非空集合,则 A 的所有一一变换构成的集合关于变换的乘积构成一个群.

证明 令 G 为 A 的所有一一变换构成的集合.由于 A 的两个一一变换的乘积仍是 A 的一个一一变换,所以变换的乘积是 G 上的一个代数运算.又由于变换的乘积适合结合律,A 上的恒等变换 I_A 是 A 的一一变换且对 $\forall f\in G$ 都有

$$f\cdot I_A=I_A\cdot f=f,$$

而且,若 $f\in G$ 是 A 的一个一一变换,则 f 的逆变换 f^{-1} 存在且也是 A 的一一变换,故 $f^{-1}\in G$,且适合等式

$$f\cdot f^{-1}=f^{-1}\cdot f=I_A,$$

因而,由群的定义,G 关于变换的乘积构成一个群. □

定义 2.6 A 的某些(不一定全部)一一变换构成的集合关于变换的乘积(当然,变换的乘积必须是这个集合上的一个代数运算)构成的群统称为**变换群**.

若 $A=\{a_1,a_2,\cdots,a_n\}$ 是有限集,则 A 的一一变换称为是 A 的**置换**;A 的所有置换构成的集合关于置换的乘积构成的群称为是 n 次**对称群**,记为 S_n;A 的某些(不一定全部)置换构成的集合关于置换的乘积构成的群统称为**置换群**.

下面讨论置换的表示方法,从而简化置换群的元素的表示形式.

设 $f\in S_n$,则 f 可表示成

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}.$$

由于 f 是 A 的一个一一变换,所以 $f(a_1),f(a_2),\cdots,f(a_n)$ 是 $a_1,a_2,\cdots,a_n$ 的一个排列;反过来,$a_1,a_2,\cdots,a_n$ 的任意一个排列唯一确定 A 的一个一一变换:若 $a_{i_1},a_{i_2},\cdots,a_{i_n}$ 是 $a_1,a_2,\cdots,a_n$ 的一个排列,则映射

$$\begin{aligned} g:A&\to A\\ a_j&\mapsto a_{i_j},j=1,2,\cdots,n, \end{aligned}$$

定义了 A 的一个一一变换.

注意到,对于 A 的置换,起关键作用的是 A 的元素的足标,所以,我们不妨假设 $A=\{1,2,\cdots,n\}$.于是

$$S_n=\left\{\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}\middle| i_1i_2\cdots i_n\text{是}n\text{级排列}\right\}.$$

由于 n 级排列一共有 $n!$ 个,所以 S_n 中含有 $n!$ 个元素,即 $|S_n|=n!$.例如,

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\right.$$

$$\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}.$$

设

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

则对 f 的列作一个置换所得到的仍是 f，即，若 $j_1j_2\cdots j_n$ 是一个 n 级排列，则

$$f=\begin{pmatrix}j_1&j_2&\cdots&j_n\\i_{j_1}&i_{j_2}&\cdots&i_{j_n}\end{pmatrix}.$$

于是，对 $\forall f,g\in S_n$，设

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

$$g=\begin{pmatrix}1&2&\cdots&n\\j_1&j_2&\cdots&j_n\end{pmatrix},$$

则

$$f\cdot g=\begin{pmatrix}j_1&j_2&\cdots&j_n\\i_{j_1}&i_{j_2}&\cdots&i_{j_n}\end{pmatrix}\cdot\begin{pmatrix}1&2&\cdots&n\\j_1&j_2&\cdots&j_n\end{pmatrix}$$

$$=\begin{pmatrix}1&2&\cdots&n\\i_{j_1}&i_{j_2}&\cdots&i_{j_n}\end{pmatrix},$$

注意，这里不是矩阵的乘积.

而对于 f^{-1}，由于

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

所以，只需对其列作置换使第一行成为 $1,2,\cdots,n$ 即可得出 f^{-1} 的表达式.

定义 2.7 (1) 设 $f\in S_n$，如果存在 $k(\geqslant 1)$ 个不同的元素 $i_1,i_2,\cdots,i_k\in\{1,2,\cdots,n\}$，使得 $f(i_1)=i_2,f(i_2)=i_3,\cdots,f(i_{k-1})=i_k,f(i_k)=i_1$，且对 $\forall j\in\{1,2,\cdots,n\}\setminus\{i_1,i_2,\cdots,i_k\}$ 都有 $f(j)=j$，则称 f 是一个 k 阶**循环置换**，记为 $f=(i_1i_2\cdots i_k)$.

(2) 设 $f=(i_1i_2\cdots i_k),g=(j_1j_2\cdots j_l)\in S_n$ 是两个循环置换，如果 $\{i_1,i_2,\cdots,i_k\}\cap\{j_1,j_2,\cdots,j_l\}=\varnothing$，则称 f 与 g **互不相交**.

(3) 形如 (i_1i_2) 的循环置换称为是一个**对换**.

注意到，$(1)=(2)=\cdots=(n)$ 就是单位置换(恒等置换)；易见，

$$(i_1i_2\cdots i_k)=(i_2\cdots i_ki_1);$$

又若 $(i_1i_2\cdots i_k)$ 与 $(j_1j_2\cdots j_l)$ 互不相交，则它们的乘积可交换：

$$(i_1 i_2 \cdots i_k)(j_1 j_2 \cdots j_l) = (j_1 j_2 \cdots j_l)(i_1 i_2 \cdots i_k).$$

这里,要验证两个置换相等即要验证作为映射,它们在每个 $\alpha \in \{1,2,\cdots,n\}$ 处的值都相等.

命题 2.8 $S_n(n \geqslant 2)$ 中的每个置换都可以表示成一些两两互不相交的循环置换的乘积.

证明 设 $f \in S_n$. 若 f 是单位置换,则 $f=(1)$. 下设 f 不是单位置换,则存在 i 使 $f(i) \neq i$.

任取 i_1 使 $f(i_1) \neq i_1$,令 $i_2 = f(i_1)$,则 $i_2 \neq i_1$. 由于 $\{1,2,\cdots,n\}$ 是有限集且 f 是一一变换,所以存在 $k \geqslant 2$ 使得 $f(i_1)=i_2, f(i_2)=i_3, \cdots, f(i_{k-1})=i_k$, $f(i_k)=i_1$,其中 $i_1, i_2, \cdots, i_k$ 互不相同. 如果对 $\forall j \in \{1,2,\cdots,n\} \setminus \{i_1, i_2, \cdots, i_k\}$ 都有 $f(j)=j$,则 $f=(i_1 i_2 \cdots i_k)$. 下面假设,存在某个 $j \in \{1,2,\cdots,n\} \setminus \{i_1, i_2, \cdots, i_k\}$ 使得 $f(j) \neq j$.

注意到,由于 f 是一一的,所以,对 $\forall j \in \{1,2,\cdots,n\} \setminus \{i_1, i_2, \cdots, i_k\}$ 都有 $f(j) \in \{1,2,\cdots,n\} \setminus \{i_1, i_2, \cdots, i_k\}$. 任取 $j_1 \in \{1,2,\cdots,n\} \setminus \{i_1, i_2, \cdots, i_k\}$ 使得 $f(j_1) \neq j_1$,则类似地,存在 $l \geqslant 2$ 使得 $f(j_1)=j_2, f(j_2)=j_3, \cdots, f(j_{l-1})=j_l, f(j_l)=j_1$,其中 $j_1, j_2, \cdots, j_l$ 互不相同. 由于 $\{i_1, i_2, \cdots, i_k\}$ 和 $\{j_1, j_2, \cdots, j_l\}$ 都是 $\{1,2,\cdots,n\}$ 的子集且互不相交,而 $\{1,2,\cdots,n\}$ 是有限集,所以上面的过程只能进行有限步,即存在 $\{1,2,\cdots,n\}$ 的两两互不相交的子集

$$\{i_1, i_2, \cdots, i_k\}, \{j_1, j_2, \cdots, j_l\}, \cdots, \{s_1, s_2, \cdots, s_t\}$$

使得 $f(i_1)=i_2, f(i_2)=i_3, \cdots, f(i_{k-1})=i_k, f(i_k)=i_1$; $f(j_1)=j_2, f(j_2)=j_3, \cdots, f(j_{l-1})=j_l, f(j_l)=j_1$; $\cdots$; $f(s_1)=s_2, f(s_2)=s_3, \cdots, f(s_{t-1})=s_t, f(s_t)=s_1$ 且对

$$\forall u \in \{1,2,\cdots,n\} \setminus (\{i_1, i_2, \cdots, i_k\} \cup \{j_1, j_2, \cdots, j_l\} \cup \cdots \cup \{s_1, s_2, \cdots, s_t\})$$

都有 $f(u)=u$. 则我们有

$$f = (i_1 i_2 \cdots i_k)(j_1 j_2 \cdots j_l) \cdots (s_1 s_2 \cdots s_t). \qquad \square$$

命题 2.8 的证明过程实际上给出了,对任意给定的 $f \in S_n$,如何把 f 表示成一些两两互不相交的循环置换的乘积的具体方法.

命题 2.9 $S_n(n \geqslant 2)$ 中的每个循环置换都可以表示成一些对换的乘积.

证明 设 $f=(i_1 i_2 \cdots i_k)$ 是一个循环置换.

若 $k=1$,则 $f=(i_1)$. 由于 $n \geqslant 2$,故存在 $j \in \{1,2,\cdots,n\}$ 使 $j \neq i_1$,则 $f=(i_1)=(i_1 j)(i_1 j)$. 下设 $k \geqslant 2$,则

$$f = (i_1 i_2 \cdots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_2). \qquad \square$$

由命题 2.8 和命题 2.9 即得

推论 2.10 $S_n(n\geqslant 2)$中的每个置换都可以表示成一些对换的乘积.

例如,(1) $\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}=(24)$, $\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=(124)=(14)(12)$,

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

(2) $S_3=\{(1),(12),(13),(23),(123),(132)\}$.

习题

1. 证明:$G=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|a,b,c,d\in\mathbb{Z}\right\}$关于矩阵的加法构成一个群.

2. 令 $G=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}$,证明:$G$ 关于矩阵的乘法构成一个群.

3. 在整数集$\mathbb{Z}$中,令 $a\circ b=a+b-2$,证明$\mathbb{Z}$关于这样的乘法"$\circ$"构成一个群.

4. 写出 S_3 的乘法表.

5. 设$(G,\cdot)$是一个群,证明:"$\cdot$"适合消去律.

6. 在 S_5 中,令

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

计算 fg,gf 和 f^{-1}.

7. 设 $a=(i_1i_2\cdots i_k)$是循环置换,求 a^{-1}.

8. 设 f 是任意一个置换,证明:$f\cdot(i_1i_2\cdots i_k)\cdot f^{-1}=(f(i_1)f(i_2)\cdots f(i_k))$.

9. 设 S 是一个非空集合,"$\cdot$"是 S 上的一个代数运算,如果"$\cdot$"适合结合律,则称$(S,\cdot)$构成一个**半群**.证明:整数集$\mathbb{Z}$关于乘法构成一个半群,但不构成一个群.

10. 设 A 是一个非空集合,S 是由 A 的所有子集构成的集合,则集合的并"$\cup$"是 S 上的一个代数运算,证明:$(S,\cup)$构成一个半群.

11. 令 $S=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|a,b,c,d\in\mathbb{Z}\right\}$,证明:$S$ 关于矩阵的乘法构成一个半群.

12. 设$(S,\cdot)$是一个半群,$e\in S$ 称为是S 的一个**左(右)单位元**,如果对 $\forall a\in S$ 都有 $e\cdot a=a(a\cdot e=a)$;设 e 是S 的一个左(右)单位元,对于 $a\in S$,如果存

在 $b\in S$ 使 $b\cdot a=e(a\cdot b=e)$，则称 a 是**左(右)可逆的**，b 是 a 的一个**左(右)逆元**.假设 S 有右单位元 e，且 S 中每个元素都有关于 e 的右逆元，证明：$(S,\cdot)$ 构成一个群.

13. 设 G 是一个群，证明：对 $\forall a,b\in G$，有 $(ab)^{-1}=b^{-1}a^{-1}$，$(a^{-1})^{-1}=a$.

14. 设 G 是一个群，$a_1,a_2,\cdots,a_n\in G$，证明：$(a_1a_2\cdots a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$.

15. 设 G 是一个群，$a\in G$，证明：对 $\forall m,n\in\mathbb{Z}$ 都有 $a^m\cdot a^n=a^{m+n}$，$(a^m)^n=a^{mn}$.

16. 设 G 是一个群，证明：G 是交换群的充要条件是，对 $\forall a,b\in G$，都有 $(ab)^2=a^2b^2$.

17. 设 G 是一个群，假设对 $\forall a\in G$ 都有 $a^2=e$，证明：G 是交换群.

18. 设 G 是非空集合，“$\cdot$”是 G 上的代数运算且适合结合律.

(1) 证明：G 是一个群当且仅当对 $\forall a,b\in G$，方程 $a\cdot x=b$，$y\cdot a=b$ 在 G 中都有解.

(2) 假设 G 是有限集，证明：$(G,\cdot)$ 是一个群当且仅当“$\cdot$”适合消去律.

19. 证明命题 2.8 中的表示法在不计循环置换的顺序的意义下是唯一的.

§3 子　群

为了研究代数结构的性质，我们首先要研究其子结构，本节讨论群的子结构——子群.

定义 3.1　设 G 是一个群，H 是 G 的一个非空子集.如果 H 关于 G 上的代数运算也构成一个群，则称 H 是 G 的**子群**.

显然，$\{e\}$ 和 G 是 G 的子群，称为是 G 的**平凡子群**，G 的不同于自身的子群称为是 G 的**真子群**.

从定义中可见，群 G 的子群 H 的代数运算是由 G 的代数运算限制在 H 上所得到的.而使这样的限制成为 H 的代数运算当且仅当，对 H 中的任意两个元素 a,b，若把 a,b 看作是 G 中的元素，在 G 中做乘积所得到的乘积元素必须仍在 H 中，也就是说，H 关于 G 的乘法是封闭的.

设 G 是一个群，H 和 K 都是 G 的子群，如果 $K\subseteq H$，则由定义易见，K 也是群 H 的子群.

命题 3.2　设 H 是群 G 的子群，则

(1) H 的单位元就是 G 的单位元；

(2) 对 $\forall a\in H$，a 在 H 中的逆元就是 a 在 G 中的逆元.

证明　(1) 设 e 是 G 的单位元，e' 是 H 的单位元，则由 e 是 G 的单位元得

$ee'=e'$，又由 e' 是 H 的单位元得 $e'e'=e'$. 于是有

$$ee'=e'e',$$

右边同乘 e' 在 G 中的逆元(或由消去律)，即得 $e=e'$.

(2) 设 a 在 G 中的逆元为 a^{-1}，a 在 H 中的逆元为 a'，则由(1)，e 既是 G 的单位元也是 H 的单位元. 所以 $aa^{-1}=e$ 且 $aa'=e$，于是

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

左边同乘 a^{-1}(或由消去律)，即得 $a^{-1}=a'$. □

于是，对群 G 的子群 H，其单位元也是 e，对 $\forall a\in H$，把 a 看作是 H 中的元素还是看作是 G 中的元素，其逆元都是相同的.

下面的定理给出了检验群 G 的非空子集构成子群的充要条件.

定理 3.3 设 $(G,\cdot)$ 是一个群，H 是 G 的一个非空子集，则 H 是 G 的子群的充分必要条件是

(1) 对 $\forall a,b\in H$，都有 $a\cdot b\in H$；

(2) 对 $\forall a\in H$，都有 $a^{-1}\in H$.

证明 "⇒"假设 H 是 G 的子群，则 G 上的代数运算"$\cdot$"也是 H 上的代数运算. 于是(1)成立，又由命题 3.2，对 $\forall a\in H$，有 $a^{-1}\in H$.

"⇐"由(1)知，G 上的代数运算"$\cdot$"也是 H 上的代数运算，而"$\cdot$"在 G 上适合结合律，从而"$\cdot$"在 H 上也适合结合律. 任取 $a\in H$，由(2)知 $a^{-1}\in H$，于是，由(1)得 $e=a\cdot a^{-1}\in H$，故 H 中有单位元 e. 又由(2)得 $a^{-1}\in H$ 且在 H 中有 $a\cdot a^{-1}=a^{-1}\cdot a=e$，因而 H 中的每个元素在 H 中都有逆元，所以 H 关于 G 上的代数运算"$\cdot$"也构成一个群，从而 H 是 G 的子群. □

定理中的条件(1)可简单地表述为"H 关于乘法封闭"，而条件(2)可表述为"H 关于取逆封闭".

由定理易得：H 是 G 的子群的充分必要条件是对 $\forall a,b\in H$ 都有 $ab^{-1}\in H$(习题 2).

例如，设 $G=GL_n(\mathbb{P})$ 是数域 $\mathbb{P}$ 上的 n 级一般线性群，令 H_1 是 G 的由全体 n 阶可逆上三角形矩阵组成的子集，由于两个上三角形矩阵的乘积仍是上三角形的且可逆上三角形矩阵的逆矩阵也是上三角形的，所以由定理 3.3 得 H_1 是 G 的子群；再令 H_2 是由 G 的所有行列式为 1 的矩阵构成的子集，则 H_2 也是 G 的子群，称之为 $\mathbb{P}$ 上的 n 级**特殊线性群**，记为 $SL_n(\mathbb{P})$.

容易验证，$A_3=\{(1),(123),(132)\}$ 是 S_3 的子群，注意到，若令 $e=(1)$，$a=(123)$，$b=(132)$，则有 $ab=e$，故 $a^{-1}=b$，$b^{-1}=a$，且 $a^2=b$，$b^2=a$.

设 S 是一个集合，则 S 的一族子集(可能有无限多个)可以表示为 S_i，$i\in I$，其中 I 是一个集合，I 称为是指标集. S 的子集族 S_i，$i\in I$ 的交集记为 $\bigcap\limits_{i\in I}S_i$，