UMSS

大学数学科学丛书 — 4

抽象代数

张勤海 著

科学出版社
www.sciencep.com

内 容 简 介

本书系统地介绍了抽象代数的基本概念、基本方法和基本理论. 全书分为5章，前两章介绍具有一定深度和广度的群、环、域的一般知识；第3章介绍Galois理论，它是群论与域论结合所得到的深刻数学结果的具体体现；第4章介绍模与代数的有关知识；第5章介绍有限群的特征标理论及其初步应用. 本书内容丰富、举例众多，特别注意通过分析例子概括出抽象概念. 本书包含大量的习题，书末附有习题提示，便于学生自学.

本书可作为高等院校数学系高年级本科生、研究生的教学用书，也可供有关数学工作者阅读.

图书在版编目(CIP)数据

抽象代数/张勤海著. —北京：科学出版社，2004
ISBN 7-03-013559-8

I. 抽… II. 张… III. 抽象代数 IV. O135

中国版本图书馆CIP数据核字(2004)第063664号

责任编辑：鄢德平 贾瑞娜/责任校对：赵桂芬
责任印制：钱玉芬/封面设计：王 浩

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2004年8月第 一 版 开本：B5(720×1000)
2004年8月第一次印刷 印张：16 1/4
印数:1-2 500 字数：300 000
定价:30.00元
(如有印装质量问题,我社负责调换〈环伟〉)

作 者 简 介

张勤海 男，1955 年 12 月 25 日生。山西翼城人。1998 年 8 月毕业于美国纽约州立大学宾厄姆顿分校，获该校数学博士学位。现为山西师范大学数学与计算机科学学院教授，基础数学、应用数学专业硕士生导师。陕西师范大学兼职博士生导师。美国《数学评论》评论员。

长期以来，从事高校数学系本科生和研究生的教学工作。主要研究方向：群论。长期致力于研究具有某种性质的子群以及具有某种形式的阶的子群对群构造的影响问题。特别是在肯定方向上首次部分回答了由著名群论学家 B. Huppert 等人于上个世纪 60 年代提出的非可解群中一个长期以来悬而未决的公开问题以及上个世纪 90 年代群论学家 V. S. Monakhov 提出的有限非交换单群中的一个公开问题。所得主要结果发表在《Comm. Alg.》、《Arch. Math.》、《Algebra Colloquium》、《数学学报》等国内外知名学术刊物上。先后发表论文 30 余篇。5 篇论文先后获山西省优秀学术论文一、二等奖。先后主持承担国家级、省部级科研项目 7 项，已完成 5 项。主持完成的项目“子群对群构造的影响”获 2001 年度山西省科技进步二等奖。同年被山西省政府授予“优秀留学回国人员”荣誉称号。

《大学数学科学丛书》序

按照恩格斯的说法，数学是研究现实世界中数量关系和空间形式的科学. 从恩格斯那时到现在，尽管数学的内涵已经大大拓展了，人们对现实世界中的数量关系和空间形式的认识和理解已今非昔比，数学科学已构成包括纯粹数学及应用数学内含的众多分支学科和许多新兴交叉学科的庞大的科学体系，但恩格斯的这一说法仍然是对数学的一个中肯而又相对来说易于为公众了解和接受的概括，科学地反映了数学这一学科的内涵. 正由于忽略了物质的具体型态和属性、纯粹从数量关系和空间形式的角度来研究现实世界，数学表现出高度抽象性和应用广泛性的特点，具有特殊的公共基础地位，其重要性得到普遍的认同.

整个数学的发展史是和人类物质文明和精神文明的发展史交融在一起的. 作为一种先进的文化，数学不仅在人类文明的进程中一直起着积极的推动作用，而且是人类文明的一个重要的支柱. 数学教育对于启迪心智、增进素质、提高全人类文明程度的必要性和重要性已得到空前普遍的重视. 数学教育本质是一种素质教育；学习数学，不仅要学到许多重要的数学概念、方法和结论，更要着重领会到数学的精神实质和思想方法. 在大学学习高等数学的阶段，更应该自觉地去意识并努力体现这一点.

作为面向大学本科生和研究生以及有关教师的教材，教学参考书或课外读物的系列，本丛书将努力贯彻加强基础、面向前沿、突出思想、关注应用和方便阅读的原则，力求为各专业的大学本科生或研究生(包括硕士生及博士生)走近数学科学、理解数学科学以及应用数学科学提供必要的指引和有力的帮助，并欢迎其中相当一些能被广大学校选用为教材，相信并希望在各方面的支持及帮助下，本丛书将会愈出愈好.

李大潜

2003 年 12 月 27 日

前　言

代数学对数学本身以及其他学科的重要性已被公认. 代数学的概念和方法已渗透到现代科学的其他分支. 特别是所有的数学家都要用到代数学的有关知识. 因而大多数高等院校的数学系都不同程度地开设抽象代数 (或近世代数) 课程, 而且在数学专业硕士研究生第一学期也继续开设抽象代数作为其专业基础课. 近几年, 随着研究生招生规模的不断扩大, 研究生教材短缺的现象日趋突出. 本书就是为数学专业硕士生阶段设计的一学期 (72 学时) 抽象代数课程教材. 特别是针对地方高等师范院校数学专业硕士生设计的.

学习本书之前我们假定学生具有抽象代数课程的基本知识. 但由于硕士生来自全国不同高校, 而各校所学的内容也不尽相同, 为了使大家有个共同的基础, 本书内容是自包含的. 为了方便学生学习, 也为了知识的连贯性, 本科阶段抽象代数课程中已经学过的群、环、域的基本概念和基本内容在本书中也做了介绍. 这样本书也适应高等院校本科高年级学生作为必修课或选修课教材. 这就是本书的编写初衷.

鉴于本书的编写初衷和读者对象, 本书安排 5 章内容. 前两章是群、环、域基本知识的复习, 但内容比现行的本科抽象代数教材更具深度和广度, 而且配备了较多的习题, 目的在于兼顾不同读者的需要. 本书的第 3 章介绍了 Galois 理论, 目的在于使学生在欣赏优美的 Galois 理论的同时, 一方面了解群论和域论的结合在解决世界数学难题中是如何发挥作用的, 另一方面强化概念之间的联系. 第 4 章介绍模与代数的有关知识, 一方面它们本身就是非常重要的研究对象, 另一方面它们是第 5 章要介绍的有限群表示理论所必需的. 对于大多数学生来说, 结合代数与有限群的表示理论是全新的内容, 我们在第 5 章对这些内容进行了初步的介绍, 作为应用, 给出了群论中两个著名定理的证明. 总之, 通过 Galois 理论和群的表示理论的学习, 目的在于使学生体验到抽象代数中不同概念的相互联系将会有多大的作用.

抽象代数不论对本科生还是研究生都是一门较难学的课程, 原因之一是概念抽象, 推理性强, 缺少例子. 本书中, 我们在每章每节前都对所要讲的内容进行引入, 使学生对所要学的内容有一个清楚的轮廓. 我们也介绍了许多例子, 并通过分析基本例子介绍抽象概念. 这样既利于学生发现问题, 激发原始性创新的源泉, 又培养了学生对抽象数学概念的理解能力.

本书的取材比较灵活, 第 1 、 2 、 3 章是一个完整的教学内容, 第 1 、 2 、 4 、 5 章也是一个完整的教学内容. 教师可根据教学时间和学生情况, 灵活掌握.

由于假定读者已具有群、环、域的基本知识, 因而本书中, 有些定理的证明写

得比较简短，给读者留有思考的余地. 这样读起来可能会感到吃力，但对训练推理能力以及将来阅读文献，学做研究都会有一定的帮助. 另外本书中的习题是不可不做的，它们是本书重要的组成部分. 而且只有通过多做习题才能更好地理解数学，学好数学.

最后我要感谢北京大学徐明曜教授，他阅读了本书全部书稿，并提出了宝贵的修改意见以及在排版工作中给予了大力协助. 研究生王丽芳、周进鑫、王玲丽、安立坚、宋蔷薇、祁燕详细阅读了本书并做了习题. 周进鑫还做了大量的排版工作. 我也要感谢国家自然科学基金委员会对本书的资助.

张勤海

2004 年 4 月于山西师范大学

本书所用的符号

$\mathbb{Z}$	整数集 (全体整数组成的集合)
$\mathbb{N}$	自然数集
$\mathbb{Q}$	有理数集
$\mathbb{R}$	实数集
$\mathbb{C}$	复数集
$\mathbb{Z}^+$	正整数集
$\mathbb{Q}^+$	正有理数集
$\mathbb{R}^+$	正实数集
$\in$, $a \in A$	“属于”符号, a 属于 A
$\notin$, $a \notin A$	“不属于”符号, a 不属于 A
$\subseteq$, $A \subseteq B$	“包含于”符号, A 包含于 B 中
$\varnothing$	空集
$\cap$, $A \cap B$, $\cap_{a \in I} A_a$	集合的交
$\cup$, $A \cup B$, $\cup_{a \in A} A_a$	集合的并
$\forall$, $\forall\, a \in A$	“对于所有”符号, 对于所有 a 属于 A
$a \equiv b \pmod{H}$	a, b 属于 H 的同一陪集
$[x, y]$	x 和 y 的换位子
$\exp(G)$	群 G 的方次数
$\lvert G \rvert$	群 G 的阶
$H \leqslant G$	H 为 G 的子群
$H < G$	H 为 G 的真子群
$\langle X \rangle$	由集合 X 生成的群
$\langle x \rangle$	由 x 生成的循环群
xH	H 的左陪集
Hx	H 的右陪集
$\lvert G : H \rvert$	H 在 G 中的指数
Σ_X	集合 X 的所有变换组成的集合
S_n	次数为 n 的对称群
A_n	次数为 n 的交代群
$\mathcal{M}_n(F)$	分量在 F 中的所有 $n \times n$ 矩阵组成的集合
$GL(n, F)$	一般线性群
$GL(V)$	V 上所有可逆线性变换组成的集合
$SL(n, F)$	特殊线性群
$PGL(n, F)$	一般射影线性群

$PSL(n,F)$	特殊射影线性群
$GL(n,q)$	阶为 q 的有限域上的一般线性群
$SL(n,q)$	阶为 q 的有限域上的特殊线性群
$PGL(n,q)$	阶为 q 的有限域上的一般射影线性群
$PSL(n,q)$	阶为 q 的有限域上的特殊射影线性群
$\mathrm{Aut}(G)$	群 G 的自同构组成的群
$\mathrm{End}(G)$	群 G 的自同态组成的群
$\mathrm{Inn}(G)$	群 G 的内自同构组成的群
$\mathrm{Out}(G)$	群 G 的外自同构群
$N \trianglelefteq G$	N 是 G 的正规子群
$Z(G)$	G 的中心
G'	群 G 的导群
G/N	群 G 关于其正规子群 N 作成的商群
$\mathrm{Ker}\varphi$	同态映射的核
$\mathrm{Im}\varphi$	同态映射的像
$\mathbf{Z}_n$	n 阶循环群
$\gcd(a,b)$	a 和 b 的最大公因子
$\mathrm{lcm}(a,b)$	a 和 b 的最小公倍数
N char G	N 为 G 的特征子群
$A \times B$, $\prod_{\alpha \in I} A_\alpha$	卡氏积
$N \rtimes H$	N 关于 H 的半直积
$G \sim H$	G 与 H 同态
$G \cong H$	G 与 H 同构
Gx	G 的含点 x 的轨道
G_x	点 x 在 G 中的稳定子群
$C_G(x)$	x 在 G 中的中心化子
$N_G(H)$	H 在 G 中的正规化子
$\mathrm{Syl}_p(G)$	G 的所有 Sylow p 子群组成的集合
δ_{ij}	Kronecker 记号
$(S,\leqslant)$	S 关于偏序关系 $\leqslant$ 所成的偏序集
RG	群环
$\mathrm{char}R$	环 R 的特征
$\deg f(x)$	多项式 $f(x)$ 的次数
$R[\alpha]$	R 上的 α 的多项式环
(a)	a 生成的主理想
$R(I)$	I 的根
$R(I)/I$	R/I 的拟根
$b \mid a$	b 整除 a

$b \nmid a$	b 不整除 a
$U(I)$	I 的单位组成的集
E^G	群 G 的固定域
$[E:F]$	E 在 F 上的次数
E/F(或 $F \lhd E$)	E 是 F 的 Galois 扩域
$\mathrm{G}(E/F)$	Galois 扩张 E/F 的 Galois 群
$H_1 \vee H_2$	H_1 和 H_2 生成的子群
$E_1 \vee E_2$	E 的所有包含 E_1 与 E_2 的子域的交
$\mathrm{Ann}_R(M)$	R 模 M 的零化理想
Rx(或 $R(x)$)	循环模
$\mathrm{Hom}_R(M,N)$	由 R 模 M 到 R 模 N 的所有模同态构成的集合
$\mathrm{End}_R(M)$	R 模 M 的自同态环
$M_1 \oplus M_2 \oplus \cdots \oplus M_n$	模 $M_1, M_2, \cdots, M_n$ 的直和
$r(M)$	自由 R 模 M 的秩
$M \otimes_R N$	M 和 N 在模 R 上的张量积
$\mathrm{End}_A(M)$	模 M 的自同态代数
$\mathrm{Irr}(G)$	G 的不可约特征标集
ϕ^G	ϕ 在 G 上的诱导类函数

目　录

第 1 章　群　论

群是抽象代数中最早的而且最基本的一个代数系统，它也是现代数学中一个极其重要的概念. 群论不仅在数学的各个分支有广泛的应用，而且在许多现代科学，如结晶学、理论物理、量子力学以及密码学、系统科学、数理经济等领域也有许多应用.

在群论的众多分支中，有限群论无论从理论本身还是从实际应用来说都占据着更为突出的地位. 特别是著名的有限单群分类问题解决之后，有限群的理论和方法在其他数学分支及其他学科的应用越来越引起人们的重视. 本章介绍群论的基本概念与基本方法，侧重于有限群以及学习 Galois 理论必需的群论知识.

1.1　群 和 子 群

本节中，我们复习一下群论中的一些基本概念和术语并给出一些群的例子. 首先我们介绍比群的概念更广泛的一个概念.

称非空集合 G 为一个 *半群*, 若在 G 上存在一个叫做乘法的二元运算，满足：

(i) 结合律：　$(xy)z = x(yz)$, 对任意的 $x, y, z \in G$.

例如，全体自然数组成的集关于数的乘法是一个半群. 数域 F 上全体 n 阶方阵组成的集关于矩阵的乘法是一个半群.

半群是代数学中一个重要的研究对象. 但鉴于本书的目标，这里我们对此不做进一步讨论.

一个半群 G 称为 *群*, 若它还满足：

(ii) 存在唯一元素 $1 \in G$, 使对任意的 $x \in G$, 满足 $x1 = 1x = x$. 1 称为 G 的 *单位元素*.

(iii) 对每个 $x \in G$, 存在唯一的元素 $x^{-1} \in G$, 满足 $xx^{-1} = x^{-1}x = 1$. x^{-1} 称为 x 的 *逆*.

设 x, y 为群 G 的两个元素，若 $xy = yx$, 我们称 x 和 y *可交换*. 更一般地，称元素 $[x, y] = x^{-1}y^{-1}xy$ 为 x 和 y 的 *换位子*. 因而 x 和 y 可交换当且仅当 $[x, y] = 1$. 称群 G 为 *交换群*, 若群 G 的任意两个元素可交换. 此时，元素的乘积与它们的次序无关；否则，我们称 G 为 *非交换群*. 在交换群中，两个元素 x, y 的乘积 xy 通常记为 $x + y$, 而 x 的逆记为 $-x$, 单位元素记为 0. 交换群也称为 *加群*. 我们称 G 的

元素 x 是 **有限阶的**, 如果存在正整数 n 使得 $x^n = 1$. 如果 x 是有限阶的, 我们定义群 G 的元素 x 的 **阶** 为满足 $x^n = 1$ 的最小正整数 n. x 的阶记为 $|x|$. 若群 G 的所有元素是有限阶的, 且它的所有元素的阶存在最小公倍数 m, 则称 m 为群 G 的 **方次数**, 记为 $\exp(G)$. 群 G 称为 **有限群**, 若 G 中元素的个数是有限的. 否则为 **无限群**. 我们定义群 G 的 **阶** 为 G 中元素的个数, 记为 $|G|$.

我们用 $\mathbb{N}$ 表示自然数集, $\mathbb{Z}$ 表示整数集, $\mathbb{Q}$ 表示有理数集, $\mathbb{R}$ 表示实数集, $\mathbb{C}$ 表示复数集. 则易得 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 对数的加法构成群. 若用 F^* 表示任一域 F 的非零元素构成的集, 则 F^* 对乘法是群. 特别地, $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ 是群. 进一步地, 正有理数集 $\mathbb{Q}^+$, 正实数集 $\mathbb{R}^+$ 对数的乘法是群.

群 G 的子集 H 称为群 G 的 **子群**, 如果 H 在 G 的乘法下也构成群. 等价地, $H \subseteq G$ 是子群, 当且仅当满足下列条件:

(i) G 的单位元素 $1 \in H$;

(ii) 若 $x, y \in H$, 则 $xy \in H$;

(iii) 若 $x \in H$, 则 $x^{-1} \in H$.

显然 G 是它自身的子群, 集合 $\{1\}$ 也是群 G 的子群, 称它们为 G 的 **平凡子群**. 若 H 是群 G 的子群, 则我们记为 $H \leqslant G$; 若 H 真包含在 G 中, 则我们称 H 为 G 的 **真子群**, 记为 $H < G$. 群 G 的真子群 H 称为 **极大子群**, 若 G 中没有真子群包含 H. 如指数为素数的子群必然是 G 的极大子群. 以后我们会看到极大子群在有限群研究中起着很重要的作用.

设 X 和 Y 是群 G 的子集, 定义 X 和 Y 在 G 中的 **乘积** 为 $XY = \{xy | x \in X, y \in Y\} \subseteq G$.

我们知道, 若 H 和 K 是群 G 的子群, 则 $H \cap K$ 也为群 G 的子群. 一个很自然的问题是: 群 G 的两个子群的乘积是否也为群 G 的子群? 这一问题一般来讲不成立, 但我们有:

命题 1.1.1 若 H 和 K 是群 G 的两个子群, 则 $HK \leqslant G$ 当且仅当 $HK = KH$. ■

设 X 是群 G 的子集, 定义 $\langle X \rangle$ 为群 G 的包含 X 的所有子群的交. 易证 $\langle X \rangle$ 也是 G 的子群, 称 $\langle X \rangle$ 为 G 的 **由 X 生成的子群**. 若 $X \leqslant G$, 则 $\langle X \rangle = X$. 若 $X = \{x\}$, 则 $\langle x \rangle$ 称为 G 的 **循环子群**. 特别地, $G = \langle x \rangle$ 称为 **循环群**. 一般地, 若 X 是 G 的子集, 则 $\langle X \rangle$ 由单位元 1 和所有形如 $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ 的元素组成, 其中 $r \in \mathbb{N}, x_i \in X$ 且 $\varepsilon_i = \pm 1, \forall\, i$. 如果 G 为由 x 生成的 n 阶循环群, 则 $G = \langle x \rangle = \{1, x, \cdots, x^{n-1}\}$.

设 $H \leqslant G, x \in G$, 集合 $xH = \{xh | h \in H\}$ 称为 H 在 G 中的 **左陪集**. 类似地, Hx 称为 H 在 G 中的 **右陪集**. 由于对左陪集成立的结论对右陪集也成立, 所

以我们在本书中仅对左陪集进行讨论. 本书中的"陪集"均指的是"左陪集". 利用 $xH = yH$ 当且仅当 $y^{-1}x \in H$, 易证 H 在 G 中的两个陪集或者相等或者互不相交, 所以群 G 的元素 x 仅含于 H 的一个陪集中, 即 xH. 对任意 $x \in G$, 在 H 与 xH 之间有一个一一对应, 即 $h \mapsto xh$, $\forall\, h \in H$. H 在 G 中的**指数**是指 H 在 G 中的陪集的个数, 记为 $|G:H|$. 因而, H 在 G 中的所有陪集把 G 分割成基数为 $|H|$ 的 $|G:H|$ 个集合的并. 把 H 在 G 中的所有陪集组成的集合称为 H 的**陪集空间**, 记为 G/H.

下面的定理给出有限群 G 的子群的本质特征, 其证明由上可得.

Lagrange定理 设 G 为有限群, $H \leqslant G$, 则 $|H|\,||\,|G|$. ■

下面的结果推广了 Lagrange 定理. 其证明留给读者.

命题 1.1.2 若 $K \leqslant H \leqslant G$, 则 $|G:K| = |G:H||H:K|$. ■

下面我们再介绍群论中经常用到的一些概念和术语. 设 x, g 为群 G 的元素, G 中的元素 gxg^{-1} 称为 x 关于 g 的**共轭元素**, 记作 x^g. 群 G 的两个元素 x, y 称为**共轭的**, 若存在 $g \in G$, 使得 $y = gxg^{-1}$. 显然, 交换群的每个元素只能与它自身共轭. 换句话说, 交换群的任意两个不同的元素都不共轭.

设 X 为一非空集合, X 的一个**变换**是指从 X 到 X 的一个一一映射. 特别地, 若 X 为有限集合时, 它的一个变换也叫做**置换**. X 的所有变换所组成的集合在映射合成之下形成一个群, 记为 $\sum_X$. $\sum_X$ 的子群称为 X 上的**变换群**. 本书中, 映射合成是指从右到左作用. 若 $X = \{1, \cdots, n\}$, $n \in \mathbb{N}$, 则这个群称为**次数为 n 的对称群**, 记为 S_n. 易见 $|S_n| = n!$. S_n 的子群称为**置换群**. S_n 的一个元素 ρ 称为一个**长度为 r 的轮换**(或 r 轮换), 若存在不同的整数 $1 \leqslant a_1, \cdots, a_r \leqslant n$, 满足 $\rho(a_i) = a_{i+1}$ 对所有 $1 \leqslant i < r, \rho(a_r) = a_1$ 且 $\rho(b) = b$, 其中 $1 \leqslant b \leqslant n$ 且 $b \neq a_i$. 若 ρ 如上定义, 我们记为 $\rho = (a_1 \cdots a_r)$. 两个轮换称为**互不相交的**, 若这两个轮换中没有公共元素.

S_n 的每个元素都可写为互不相交的轮换的乘积, 这种表达式称为这个置换的**互不相交的轮换分解式**. 给定一个置换, 它的任意两个互不相交的轮换分解式必含有相同的轮换但顺序可能不同. 因而, 我们可以把和为 n 的一些正整数组成的集合 (这个集合称为 n 的一个**划分**) 与 S_n 的每个元素对应起来. n 的这个划分由置换 ρ 的轮换分解式中出现的轮换长度组成, 称为 ρ **的轮换结构**. 例如, 在 S_6 中, $\rho = (124)(35)$ 的轮换结构是划分 $(3,2,1)$. 利用这些术语, 我们有下面的结论.

命题 1.1.3 S_n 中的两个元素共轭当且仅当它们有相同的轮换结构. ■

S_n 的 2 轮换称为**对换**. 我们知道, S_n 的每一个元素可以写为多种不同形式的对换的乘积 (不一定互不相同), 但是给定置换的两个表达式中, 对换个数的奇偶

性是相同的. 因而, 我们定义一个置换是 *偶 (奇) 置换*, 如果它可写成偶 (奇) 数个对换的乘积. 显然, S_n 的所有偶置换组成的集合是 S_n 的指数为 2 的子群, 称为*次数为 n 的交代群*, 记为 A_n. 它是有限群中一个非常重要的研究对象.

作为本节的结束, 我们再介绍在有限群中起着重要作用的几个群的例子.

例 1.1.1 设 F 是域, $n \in \mathbb{N}$. 用 $\mathcal{M}_n(F)$ 表示分量在 F 中的所有 $n \times n$ 矩阵组成的集合. $\mathcal{M}_n(F)$ 中所有可逆矩阵在矩阵乘法之下形成一个群, 称这个群为*一般线性群*, 记为 $GL(n, F)$. 另一方面, 给定 F 上的 n 维向量空间 V, 则 V 上所有可逆线性变换组成的集合在映射合成之下形成一个群, 记为 $GL(V)$. 由线性代数我们知道, $GL(V) \cong GL(n, F)$. 因此我们可以重点来研究群 $GL(n, F)$.

特殊线性群 是 $GL(n, F)$ 中行列式为 1 的矩阵组成的子群, 记为 $SL(n, F)$. 换句话说, $SL(n, F)$ 是同态 $\det: GL(n, F) \longrightarrow F^*, \forall\ A \in GL(n, F), A \mapsto \det(A)$ 的核, 其中 $\det(A)$ 为矩阵 A 的行列式, 因而 $SL(n, F) \trianglelefteq GL(n, F)$.

群 $GL(n, F)/Z$(这里, Z 表示群 $GL(n, F)$ 的中心, 其定义可见 1.2 节.) 称为*一般射影线性群*. 群 $SL(n, F)/(Z \cap SL(n, F))$ 称为*特殊射影线性群*. 分别用 $PGL(n, F)$ 和 $PSL(n, F)$ 来表示 (由第一同构定理 (见 1.3 节) 可知 $PSL(n, F) \cong Z \cdot SL(n, F)/Z \leqslant GL(n, F)/Z = PGL(n, F)$.). 由于 $Z \cong F^*$, 故若 F 是有限域时, 我们有 $|PGL(n, q)| = |SL(n, q)|$, 其中 q 为素数方幂.

命题 1.1.4 设 E 为方次数为 p 的有限交换群, 其中 p 是素数, 则 $\mathrm{Aut(E)} \cong GL(n, p)$, 其中 $n \in \mathbb{N}$, $|E| = p^n$.

证明 设 $F = \mathbb{Z}/p\mathbb{Z}$ 是 p 元域, 我们希望给 E 一个向量空间结构. 在 E 中定义加法为: $\forall\ x, y \in E$, $x + y = xy$. 对 $\alpha \in F$, 定义数量乘法为: $\alpha x = x^a$, 其中 $a \in \mathbb{Z}$, 满足 $\alpha = a + p\mathbb{Z}$. 易证, E 作成一个 F 向量空间. 由于群 E 的自同态同时也是 F 向量空间 E 的线性变换, 反之亦然. 因此有 $\mathrm{Aut}(E) \cong GL(n, p)$, 其中 $n = \dim_F(E)$. ■

显然由命题 1.1.4 知 $\mathrm{Aut}(\mathbf{Z_p}) \cong GL(1, p) \cong (\mathbb{Z}/p\mathbb{Z})^*$.

命题 1.1.5 设 $n \in \mathbb{N}, q$ 为素数幂, 则:

$$\text{(i)} \quad |GL(n, q)| = \prod_{k=1}^{n} (q^n - q^{k-1}) = q^{\frac{n(n-1)}{2}} (q^n - 1) \cdots (q - 1);$$

$$\text{(ii)} \quad |SL(n, q)| = \prod_{k=1}^{n-1} (q^{n+1} - q^k) = q^{\frac{n(n-1)}{2}} (q^n - 1) \cdots (q^2 - 1).$$

证明 (i) 要决定 $|GL(n, q)|$, 只需计算域 F 上行线性无关的 $n \times n$ 矩阵的个数即可.

为了构造这样一个矩阵，第一行我们可以在 F^n 中任选一个非零向量，因而有 q^n-1 种选法. 对 $1<k\leqslant n$, 第 k 行可在 F^n 中任选一个与前 $k-1$ 行线性无关的向量，即可选除了 q^{k-1} 个向量以外的向量，因而第 k 行有 q^n-q^{k-1} 种选法. (i) 得证.

(ii) 显然同态映射 $\det: GL(n,F)\longrightarrow F^*$ 是满射，由同态基本定理，对任意域 F, 有 $F^*\cong GL(n,F)/SL(n,F)$. 特别地，若 $|F|=q$, 则 $|GL(n,q):SL(n,q)|=q-1$. (ii) 得证. ■

例 1.1.2 n 维欧氏空间 V 上全体正交变换构成群 O_n. 由线性代数知道，一个正交变换也可以看为一个 n 级正交矩阵. 因而

$$O_n=\{P\in GL(n,\mathbb{R})|PP^t=P^tP=I\},$$

其中 P^t 是 P 的转置，I 是单位矩阵. 在 O_n 中，所有行列式为 1 的矩阵构成子群 O_n^+. 特别地，O_3^+ 就是三维空间中所有旋转构成的群.

例 1.1.3 考虑平面上正 n 边形 ($n\geqslant 3$) 的全体对称作成的集合 D_{2n}. 它包含 n 个旋转和 n 个反射 (沿 n 条不同的对称轴). 从几何上容易看出，D_{2n} 对于变换的合成构成一个群，叫做 *二面体群*. 它含 $2n$ 个元素.

若以 a 表示绕这个正 n 边形的中心沿反时针方向旋转 $\dfrac{2\pi}{n}$ 的变换，则 D_{2n} 中所有旋转都可表为 a^i 的形式，$i=0,1,\cdots,n-1$. 再以 b 表示沿某一预先指定的对称轴 l 所作的反射变换，则有关系式

$$a^n=1,\ b^2=1,\ b^{-1}ab=a^{-1}.$$

最后一式表示先作反射 b, 接着旋转 $\dfrac{2\pi}{n}$, 然后再作反射 b, 其总的效果就相当于向反方向旋转 $\dfrac{2\pi}{n}$. 无论从几何上还是从群论中都可看出，

$$D_{2n}=\langle a,b\rangle=\{b^ja^i|j=0,1;\ i=0,1,\cdots,n-1\},$$

且 D_{2n} 中乘法依照规律：$b^ja^i\cdot b^sa^t=b^{j+s}a^{(-1)^si+t}$.

例 1.1.4 四元数集 $\{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$ 在乘法下构成一个 8 阶群，叫做 *四元数群*, 记做 Q_8. Q_8 中元素的乘法满足

$$i^2=j^2=k^2=-1,\ ij=k=-ji,\ jk=i=-kj,\ ki=j=-ik.$$

容易验证 Q_8 同构于 $\mathbf{C}$ 上二阶矩阵

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}0&-1\\1&0\end{pmatrix},\ \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\ \pm\begin{pmatrix}0&i\\i&0\end{pmatrix}$$