国家理科基地教材

近世代数讲义

杨劲根　编著

科学出版社
www.sciencep.com

国家理科基地教材

近世代数讲义

杨劲根　编著

科学出版社

北京

内 容 简 介

本书根据作者在复旦大学多年教学的讲义修改而成，内容包括群的基本知识、环和域的基本知识、多项式和有理函数、向量空间、群论中一些进一步的知识、域的扩张、有限域、Galois 理论初步. 本书配有相当数量的习题，难度变化大，适应多层次教学的需要. 书后附有习题解答和提示，供读者参考.

本书可作为综合性大学数学系和计算机系本科生作为教材使用，也可作为相关专业及数学爱好者参考使用.

图书在版编目(CIP)数据

近世代数讲义/杨劲根编著. —北京：科学出版社，2009
国家理科基地教材
ISBN 978-7-03-023546-6

Ⅰ. 近… Ⅱ. 杨… Ⅲ. 抽象代数-高等学校-教材 Ⅳ. O153

中国版本图书馆 CIP 数据核字(2008) 第 189231 号

责任编辑：姚莉丽　房　阳 / 责任校对：陈玉凤
责任印制：张克忠 / 封面设计：陈　敬

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

明辉印装有限公司 印刷
科学出版社发行　　各地新华书店经销
*
2009 年 2 月第　一　版　开本：B5(720×1000)
2009 年 2 月第一次印刷　印张：11
印数：1—4 000　　字数：204 000

定价：22.00 元

(如有印装质量问题，我社负责调换〈明辉〉)

前　言

提起代数, 一般人想起的是中学里学的一大部分数学, 如因式分解、解方程、指数函数、对数函数等. 这些数学是学习微积分的预备知识. 这门课程所讲述的代数有所不同, 它着重于探讨群、环、域、向量空间等一些常用的代数结构以及它们之间的映射. 为了有别于古典代数, 它被称为“近世代数”或“抽象代数”. 它的思想起源于何时没有统一的说法, 但是数学界一般认为近世代数作为一门学科是在 20 世纪由 E. Noether 和 E. Artin 等数学家建立起来的.

在大学一年级的线性代数课程中, 我们已经接触了向量空间这个代数结构, 在这个结构上加入内积运算又产生欧氏空间、酉空间等结构. 再看整数集合 $\mathbb{Z}$ 和实系数单变量多项式全体所构成的集合 $R[x]$. 它们都具有加法和乘法运算. 它们有一系列重要的性质是非常相似的, 从代数结构的观点来看, 它们有内在的联系. 粗略地说, 一个代数结构是带有一种或多种满足某些条件的运算的集合. 这是数学研究的基本对象之一. 另一个重要的基础数学结构是拓扑结构, 它不在本课程讨论范围之内, 在拓扑结构的基础上又产生微分结构、解析结构等, 代数结构和拓扑结构合起来又产生拓扑群、李群等结构. 近百年的数学发展证实了近世代数有着不可缺少的作用.

正因如此, 近世代数已成为数学系的一门重要基础课程, 一般安排在大学二、三年级. 理想的学时安排是一个学年, 但是由于种种原因我国大学课程的学时越来越紧张, 以至于大部分大学数学系只能安排一个学期的近世代数课. 尽管如此, 这门课必须包括群、环、域、同态等基本内容, 作者还认为 Galois 理论是代数学的一个里程碑, 如果修了这门课的学生不知道 Galois 理论是一件憾事. 通过十来年的教学实践, 作者对某些内容作了一定的精简, 使得重点更加突出, 在一个学期时间内使学生学到 Galois 理论的主要定理和五次以上的方程无求根公式这个经典定理的证明.

本书根据作者在复旦大学多年教学的讲义修改而成. 在所有代数结构中, 群是最基本的, 内容也非常多. 为了突出重点, 把有些技术性比较强的内容, 如 Sylow 定理、有限生成的 Abel 群的结构定理、可解群等安排在较后的章节讲述. 在前两章着重介绍群、环、域和同态的基本知识, 这符合先易后难的原则. 环论方面, 以剩余数环 $\mathbb{Z}/n\mathbb{Z}$ 和多项式环 (包括多变量多项式环) 为重点, 通过它们来熟悉主理想环和唯一因子分解环的概念. 非交换环在本讲义中讲得较少, 仅限于矩阵环和四元数体等一些基本常识. 在介绍了群、环、域和同态的基本知识后, 加入任意域上的向

量空间这一章. 由于学生一般都有较好的线性代数基础, 所以这一部分内容比较简略, 主要目的是使学生掌握有限域上的向量空间的一些特点, 同时为一般的域扩张理论作准备, 使学生比较容易接受扩域是基域上的向量空间这个观点. 这些章节构成上半学期的内容.

下半学期的内容相对高深一点, 先讲 Sylow 定理、有限生成的 Abel 群的结构定理、可解群, 再讲域扩张和 Galois 理论的基础知识. 根据作者的教学实践, 所有 8 章内容在一个学期内可以讲完, 有些内容根据情况还可以压缩. 为了使用者的方便, 有些可以跳过的内容用 * 号标出, 6.4 节"代数闭域"的证明用了 Zorn 引理, 也可以作为选学内容, 此节用 ‡ 号标出.

附录是为有兴趣的学生安排的, 二次剩余定理的一个证明展示有限域的技巧, 有限体是域的证明巧妙应用了群的作用, 以上两个证明分别根据 J.P. Serre 和 A. Weil 的证明改编. 由于课时关系, 在正文中只讲五次方程的求解公式不存在问题, 用 Galois 理论推导三次方程和四次方程的求根公式就放在附录里了.

本书的习题数量适中, 难度变化比较大, 以适应各种程度的学生. 部分习题取自国外研究生试题. 书后附有习题的解答或提示, 供读者参考. 大部分证明题都有各种不同的证明方法, 作者不可能列出所有的证法, 希望学生不要过分依赖习题解答, 要尽量发掘自己的创造力, 这样才能体验数学推理的魅力.

总之, 本书是作者试图用既严密又朴素的方式讲授近世代数中最重要的一些知识和基本方法, 主要对象是综合性大学数学系二年级学生.

李克正教授对本书的初稿提出了很多宝贵的修改意见, 在此深表感谢. 修过本课程的复旦大学数学系历届本科生对本书提供了很多建设性的意见, 在此一并感谢. 在选材和写作上本书一定有很多不足和疏漏, 望读者批评指正. 科学出版社的姚莉丽女士对本书出版提供大力帮助, 特此感谢.

杨劲根

2008 年 9 月

预备知识和记号

由于本书的主要对象是大学数学系本科生, 假定读者已经学过线性代数和微积分 (至少单变量微积分), 知道集合和映射的基本知识. 由于术语上不可避免会有不统一处, 在此对一些基本的数学概念和符号作一些约定.

从一个集合 S 到另一个集合 T 的映射 f 叫做单射 (injection), 若 $x \neq y \in S$ 推出 $f(x) \neq f(y)$; 叫做满射 (surjection), 若对任意 $z \in T$, 存在 $x \in S$ 使 $f(x) = z$. 既是单射又是满射的映射叫双射 (bijection), 有的书也叫一一对应 (one-one correspondence). 设 U 是 S 的一个子集, 记 $f|_U$ 为映射 f 在 U 上的限制.

记号 $f : S \to T, x \mapsto z$ 表示一个把元素 x 映成 z 的映射. 例如, $x \mapsto \mathrm{e}^x$ 表示通常的指数函数.

设 f 是从集合 S 到集合 T 的映射, g 是从集合 T 到集合 U 的映射. 记 $g \circ f : S \to U, x \mapsto g(f(x))$, 称为 f 和 g 的复合映射. 在不会引起混淆时也可记成 gf.

集合 S 的一个子集常常用 $\{x \in S | P\}$ 来定义, 这里 P 是 x 在这个子集中所需要满足的条件. 例如, $\{x \in \mathbb{R} | 0 \leqslant x \leqslant 1\}$ 表示闭区间 $[0, 1]$. 集合的并和交按通常的记号 $\cup$ 和 $\cap$, 集合 A 和 B 的差 $\{x \in A | x \notin B\}$, 记作 $A - B$ 或 $A \backslash B$, 更多地使用后一种. 元素个数不多的集合常常用 $\{\cdots\}$ 表示, 这里 $\cdots$ 为具体的元素列表. 例如, 由一个元素 a 构成的集合记为 $\{a\}$, 由 0, 1 两个元素组成的集合记为 $\{0, 1\}$, 空集记为 $\varnothing$.

学过等价关系和等价类对本书的理解会有很大的益处, 但在第一次使用这些概念时会详细解释.

假定读者熟知数域的概念, 它是复数域的对四则运算封闭的子集. 最常见的数域是复数域、实数域和有理数域.

对一些常用集合约定使用下面记号:

自然数集合 $\mathbb{N}$

整数集合 $\mathbb{Z}$

有理数集合 $\mathbb{Q}$

实数集合 $\mathbb{R}$

复数集合 $\mathbb{C}$

目　录

第 1 章　群的基本知识

数学中所遇到的集合常常带有运算, 有时同一个集合上有多种运算, 带有运算的集合通常叫做一个代数结构. 在本书中要学习的代数结构是群、环和向量空间, 其中群的结构最为单纯, 它是只带一种基本运算的代数结构. 本章讲述群的定义、例子、群的一些基本性质以及群之间的同态, 关于群的一些进一步的知识将在以后有关章节里叙述.

1.1　定义和例子

设 S 是一个集合, 用记号 $S\times S$ 表示 S 与 S 的 (直) 积, 也叫笛卡儿积, 它中的元素可用 (a,b) 表示, 其中 a,b 可以是 S 的任意元素. 要注意的是如果 $a\neq b$, 则 (a,b) 和 (b,a) 是 $S\times S$ 中两个不同的元素. 把从 $S\times S$ 到 S 的一个映射 f 叫做 S 上的一个二元运算. 也就是说, 对于 S 中的任何一对元素 a,b, 都有 S 中唯一确定的一个元素 $f(a,b)$ 与之对应.

例如, 取 S 为实数全体所构成的集合, 将映射

$$f: S\times S\to S$$

定义为

$$f(a,b)=a+b,$$

则 f 就是一个二元运算. 也可以用各种别的式子来定义其他形式的 f, 如 $f(a,b)=a^2+b^3$ 或 $f(a,b)=ab$ 等.

在具体的应用中, 用 $f(a,b)$ 来记二元运算是笨拙的, 二元运算一般有更方便的记号, 如 $a+b,[A,B],\boldsymbol{u}\times\boldsymbol{v}$ 等. 在不引起混淆的情况下最简单的记号是 ab. 对于已经熟悉的一些运算则使用已经熟悉的记号, 如数的加法记为 $+$, 三维空间中矢量的叉乘记为 $\times$.

再举几个二元运算的例子.

(1) 设 S 是三维欧氏空间, 则向量和 $\boldsymbol{u}+\boldsymbol{v}$, 矢量积 (即叉乘) $\boldsymbol{u}\times\boldsymbol{v}$ 都是二元运算, 内积不是二元运算, 因为这个运算的结果不再是向量, 而是一个数;

(2) 设 S 是 n 阶方阵全体所构成的集合, 则 $\boldsymbol{A}+\boldsymbol{B},\boldsymbol{AB},\boldsymbol{AB}-\boldsymbol{BA}$ 是 3 种不同的二元运算 (最后一种运算是李代数中的一种基本运算);

(3) 设 S 是处处有定义的单变量实值函数全体构成的集合, 则函数的复合 $f\circ g$ 是 S 上的一个二元运算.

一元运算也很常见, 如数 a 的相反数 $-a$, 平方 a^2, 复数 a 的共轭 $\bar{a}$, 方阵 $\boldsymbol{A}$ 的转置 $\boldsymbol{A}^{\mathrm{T}}$ 等.

说 S 上的一种二元运算满足**结合律**, 如果

$$f(a, f(b, c)) = f(f(a, b), c)$$

对任意 $a, b, c \in S$ 成立. 根据约定的简单记号, 这个条件写为

$$a(bc) = (ab)c,$$

恰好是所熟悉的形式.

在一开始所举的例子中, 大部分二元运算都满足结合律. 矢量积 $\boldsymbol{u} \times \boldsymbol{v}$ 和方阵的运算 $\boldsymbol{AB} - \boldsymbol{BA}$ 不满足结合律. 容易验证实数集合上的运算 $f(a, b) = a^2 + b^3$ 不满足结合律.

称集合 S 上二元运算满足**交换律**, 如果

$$ab = ba$$

对任意 $a, b \in S$ 成立.

例如, 数的乘法满足交换律, 方阵的乘法不满足交换律.

S 中有一个元素 e 称为 S 中的一个**恒等元** (identity element), 如果

$$ea = ae = a$$

对任何 $a \in S$ 成立.

以下是一些例子:

(1) 0 是实数集合加法运算的恒等元;

(2) 1 是实数集合乘法运算的恒等元;

(3) 单位矩阵 $\boldsymbol{I}_n$ 是 n 阶方阵集合乘法运算的恒等元.

命题 1.1.1　带二元运算的集合 S 中最多只有一个恒等元.

证明　设 e, e' 是两个恒等元. 由于 e 是恒等元, 故 $ee' = e'$. 又因为 e' 是恒等元, 故 $ee' = e$. 合起来得 $e = ee' = e'$. □

定义 1.1.1　设非空集合 S 具有一个满足结合律的二元运算, 则 S 在该运算下构成一个**半群** (semigroup), 含恒等元的半群称为**幺半群** (monoid).

例 1.1.1　自然数集合在加法运算下构成一个半群, 但不是幺半群.

定义 1.1.2　设 a 是幺半群 S 中的一个元素, e 是 S 的恒等元. 如果存在 $b \in S$, 使

$$ab = ba = e,$$

则称 a 为 S 中的一个**可逆元** (invertible element), 并称 b 为 a 的**逆** (inverse). 可逆元 a 的逆元通常记作 a^{-1}.

很明显, "逆" 这个关系是相互的. 若 b 是 a 的逆, 则 a 是 b 的逆.

命题 1.1.2 可逆元的逆元是唯一的.

证明 设 b, b' 是 a 的逆元, 则 $b = be = b(ab') = (ba)b' = eb' = b'$. □

定义 1.1.3 带有一个二元运算的非空集合 G 称为一个**群** (group), 如果下面 3 个条件成立:

(1) 结合律成立;

(2) 恒等元存在;

(3) 每个元素是可逆元.

条件 (1) 和条件 (2) 表明群一定是一个幺半群. 虽然半群概念比群更一般, 但它不是抽象代数的主要研究对象, 群才是本章学习的主要对象.

在一个群中有一个一元运算 $a \mapsto a^{-1}$, 这个运算叫做求逆运算, 它由群的二元运算所确定, 所以认为它不是群的基本运算.

关于记号和术语的一些说明

前面已经说过, 群中的二元运算 (简称群运算) 在不同场合下用不同的记号, 缺省的记法是 ab. 二元运算也可称为乘法, 这时 a 的逆记作 a^{-1}, 恒等元 e 可以记作 1, 有时为了强调它是群 G 中的恒等元也可记作 1_G, 它也可以叫做 G 中的单位元或幺元. 对于自然数 n, 元素 a 的 n 次幂 a^n 定义为 n 个 a 的乘积, 而 a^{-n} 表示 n 个 a^{-1} 的乘积.

对于群 G, 如果 $ab = ba$ 对任意 $a, b \in G$ 成立, 则 G 称为一个可交换群或 **Abel 群**(Abelian group). 经常采用后一种叫法.

对于 Abel 群, 群运算常常叫做加法, 记为 $a + b$. 这时恒等元称为零元, 记作 0, 元素 a 的逆元记作 $-a$. 对任意自然数 n, 元素 a 的 n 倍 na 定义为 n 个 a 相加. 这样的群也可称为加法群.

由有限多个元素构成的群 G 叫做**有限群**(finite group), 其中元素的个数记作 $|G|$, 叫做 G 的阶 (order). $|G| = \infty$ 表示 G 是无限群.

设 g 是群 G 中的一个元素, 如果不存在自然数 n 使 $g^n = 1$, 则称 g 为一个无限阶元素, 否则使 $g^n = 1$ 成立的最小的自然数 n 称为元素 g 的**阶**, 记为 $o(g)$. 按照这个规定, 恒等元的阶是 1. 规定无限阶元素的阶是 ∞.

例 1.1.2 (1) 任何一个数域在加法运算下构成 Abel 群. 这里说明一下, 虽然一个数域有加法和乘法运算, 当它被当成一个群处理的时候, 乘法运算被忽略, 因为群的定义只牵涉一种二元运算;

(2) 整数全体构成的集合 $\mathbb{Z}$ 在加法下构成 Abel 群, 叫做整数加法群;

(3) 数域 K 上全体 n 阶可逆阵在乘法运算下构成群, 称为**一般线性群**(general linear group), 记作 $GL_n(K)$. 当 $n > 1$ 时它不是 Abel 群;

(4) 数域 K 在乘法运算下是个幺半群, 但它不是群, 因为元素 0 的逆元不存在.

记 $K^* = K\backslash\{0\}$, 则 K^* 在乘法运算下是一个 Abel 群, 它和 $GL_1(K)$ 是一样的. 从这个例子看出, Abel 群中的运算并不是非要叫成加法的;

(5) 任意一个向量空间在加法运算下构成一个 Abel 群;

(6) 三维欧氏空间在叉乘运算下连半群也不是, 因为结合律不成立;

(7) 最小的群只含一个元素;

(8) 空集不是群.

命题 1.1.3(消去律)　设群 G 中的元素 a, b, c 满足 $ab = ac$ 或 $ba = ca$, 则 $b = c$.

证明　设 $ab = ac$. 在此等式两边同时从左边乘 a^{-1} 得 $a^{-1}(ab) = a^{-1}(ac)$, 利用结合律得 $(a^{-1}a)b = (a^{-1}a)c$, 根据逆元的定义得 $eb = ec$, 最后根据恒等元 e 的定义得 $b = c$.

从 $ba = ca$ 用同样的方法可推出 $b = c$. □

系 1.1.1　设 a, b 是群 G 中的两个元素.

(1) 若 $ab = a$ 或 $ba = a$, 则 $b = 1$;

(2) 若 $ab = 1$ 或 $ba = 1$, 则 $b = a^{-1}$.

证明　(1) 将消去律用于 $ab = a1$ 即可.

(2) 将消去律用于 $ab = aa^{-1}$ 即可. □

命题 1.1.4　设 a, b 是群 G 中的两个元素, 则 $(ab)^{-1} = b^{-1}a^{-1}$.

证明　等式 $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1$ 及系 1.1.1(2) 表明 $b^{-1}a^{-1} = (ab)^{-1}$. □

回忆在线性代数中学过可逆方阵的逆满足 $(\boldsymbol{AB})^{-1} = \boldsymbol{B}^{-1}\boldsymbol{A}^{-1}$, 道理是一样的.

已经知道, 任何一个数域在加法运算下成为一个群, 在这个意义下加法运算可以认为是数域中第一个基本的运算, 事实上这也是小学算术所学的第一种运算. 减法运算却不是基本运算, 由于 $a - b = a + (-b)$, 所以 $a - b$ 这个运算可以看成群中的求逆运算 $b \mapsto -b$ 和加法运算的合成.

习　题　1.1

1. 在集合 $G = \{a \in \mathbb{R} | a > 0, a \neq 1\}$ 上定义二元运算 $a * b = a^{\ln(b)}$, 问 G 在这个二元运算下是不是一个群? 这里 $\ln(x)$ 是自然对数函数.

2. 设 A 是由所有在 $[0,1]$ 区间上满足 $f(0) = 0, f(1) = 1$ 的严格单调递增连续函数全体所构成的集合, 对任意 $f, g \in A$ 规定 fg 为 f 和 g 的复合, 即 $(fg)(x) = f(g(x))$ 对任何 $x \in [0,1]$ 成立. 求证 A 在这个二元运算下构成群.

3. 设 G 是一个满足下面两个条件的半群:

(1) 存在一个 $e \in G$, 使 $ea = a$ 对任何 $a \in G$ 成立;

(2) 对任何 $a \in G$, 存在 $b \in G$ 使 $ba = e$ 成立.

求证 G 是一个群.

4. 证明任何一个有限群中每个元素的阶是有限数.

5. 设 G 是一个有限群, $a,b\in G$. 证明 ab 和 ba 有相同的阶.

6. 设群 G 中每个元素 a 满足 $a^{-1}=a$. 证明 G 是 Abel 群.

1.2 子　群

定义 1.2.1　设 H 是群 G 的一个满足下面两个条件的非空子集:

(1) (乘法封闭) 对任意 $a,b\in H$ 都有 $ab\in H$;

(2) (求逆封闭) 对任意 $a\in H$ 都有 $a^{-1}\in H$.

则 H 叫做 G 的一个子群.

根据乘法封闭性, H 中的乘法运算是有意义的, 乘法结合律自然成立. 由于 H 非空, 存在 $a\in H$, 于是 $a^{-1}\in H, 1=a^{-1}a\in H$, 因此 H 含有恒等元. 所以 H 在乘法下构成一个群, 这就是"子群"这个名词的意义. 子群概念和线性代数中子空间的概念非常相似.

容易看出, Abel 群的子群仍然是 Abel 群.

例 1.2.1　(1) 每个群 G 天生有两个子群 $\{1_G\}$ 和 G, 称为平凡子群. 只要 G 的元素个数大于 1, 这两个平凡子群是不同的.

(2) 设 n 是一个自然数. 令 $n\mathbb{Z}$ 为所有被 n 整除的整数所构成的集合, 它是整数加法群 $\mathbb{Z}$ 的子群.

(3) 令 $SL_n(K)$ 为数域 K 上行列式等于 1 的 n 阶方阵全体所构成的集合, 它是 $GL_n(K)$ 的子群, 叫做**特殊线性群** (special linear group).

(4) 由

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad \begin{bmatrix}-1&0\\0&-1\end{bmatrix}$$

构成的集合 H 是 $SL_2(K)$ 的子群, $|H|=2$.

(5) 实数集合 $\mathbb{R}$ 在加法下构成群, 而 $\mathbb{R}^*=\mathbb{R}-\{0\}$ 在乘法下也构成群, 后者虽然是前者的子集, 但不是子群, 因为加法和乘法是不同的二元运算.

命题 1.2.1 (子群的一个判别法)　设 H 是群 G 的一个非空子集. 若 $ab^{-1}\in H$ 对任意 $a,b\in H$ 成立, 则 H 是 G 的一个子群.

证明　任取 $c\in H$, 则 $1=cc^{-1}\in H$. 对任意 $a\in H$, 有 $a^{-1}=1a^{-1}\in H$, 因此 H 对求逆封闭.

对任意 $a,b\in H$ 都有 $ab=a(b^{-1})^{-1}\in H$, 所以 H 对乘法封闭. □

命题 1.2.2　设 $\{H_i\}_{i\in I}$ 是群 G 的一组子群 (可以有无限多个), 则 $H=\bigcap\limits_{i\in I}H_i$ 是 G 的一个子群.

证明　因为 $1 \in \bigcap\limits_{i\in I} H_i$, 所以 H 非空. 设 $a, b \in H$, 则 $ab^{-1} \in H_i$ 对每个 $i \in I$ 成立, 故 $ab^{-1} \in H$. □

定义 1.2.2　设 g 是群 G 的一个元素, 则集合 $C(g)=\{a\in G|ag=ga\}$ 称为 g 在 G 中的**中心化子** (centralizer). 设 $S \subseteq G$, 则集合 $C(S) = \{a \in G|ag = ga$ 对所有$g \in S\}$ 称为 S 在 G 中的中心化子, $C(G)$ 称为 G 的**中心** (center).

容易看出, $C(g), C(S) = \bigcap\limits_{g\in S} C(g)$ 均为 G 的子群. $C(G)$ 是 Abel 群, G 是 Abel 群当且仅当 $G = C(G)$.

设 S 为群 G 的一个非空子集. 令 $\langle S\rangle$ 为所有包含 S 的子群的交, 那么 $\langle S\rangle$ 为包含 S 的最小子群, 称为 S 生成的群. 如果 S 是一个有限集 $\{a_1, \cdots, a_n\}$, 则可将 $\langle S\rangle$ 记成 $\langle a_1, \cdots, a_n\rangle$.

若 $G = \langle S\rangle$, 则说 G 由 S 生成.

例 1.2.2　(1) $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$.

(2) $GL_n(K)$ 由所有 n 阶初等矩阵生成.

设群 G 由一个有限子集生成, 则 G 叫做一个有限生成的群. 更特殊些, 如果 G 可以由一个元素 g 生成, 则 G 叫做一个**循环群** (cyclic group). 例如, $\mathbb{Z}$ 是循环群, 而 $GL_n(K)$ 不是循环群. 任何一个循环群是 Abel 群.

设 $a \in G$, 则 $\langle a\rangle$ 是 G 的一个子群, 它本身是一个循环群, 所以叫做 G 的一个循环子群, 满足 $o(a) = |\langle a\rangle|$. 事实上, 若 $o(a) = \infty$, 则

$$\langle a\rangle = \{\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots\}.$$

若 $o(a) = n < \infty$, 则

$$\langle a\rangle = \{1, a, a^2, \cdots, a^{n-1}\}.$$

例 1.2.3　在群 $GL_n(K)$ 中矩阵

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

生成一个无限循环子群, 矩阵

$$\begin{bmatrix} -\dfrac{1}{2} & -\dfrac{\sqrt{3}}{2} \\ \dfrac{\sqrt{3}}{2} & -\dfrac{1}{2} \end{bmatrix}$$

生成一个三阶循环子群.

命题 1.2.3　设 S 是群 G 的一个非空子集, 则

$$\langle S\rangle = \{a_1^{e_1}a_2^{e_2}\cdots a_n^{e_n}|a_1, \cdots, a_n \in S, e_1, \cdots, e_n = \pm 1, n \text{ 是任意自然数}\}.$$

证明 首先要注意的是表达式中的 $a_1, a_2, \cdots, a_n$ 不一定两两互异.

记等式右边的集合为 T, 则 T 是包含 S 的一个子群, 因此 $\langle S\rangle \subseteq T$.

反之, 设 H 是包含 S 的一个子群, 根据子群中的乘法封闭和求逆封闭的性质, 每个形为 $a_1^{e_1}a_2^{e_2}\cdots a_n^{e_n}(a_i \in S, e_j = \pm 1)$ 的元素都在 H 中. 于是 $T \subseteq H$, 所以 $\langle S\rangle = T$. □

下面讨论整数加法群 $\mathbb{Z}$ 有哪些子群. 首先, $0, \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \cdots$ 都是 $\mathbb{Z}$ 的子群. 下面证明它没有其他子群.

设 H 是 $\mathbb{Z}$ 的一个非平凡子群, 它含有非零整数. 由于 H 对求逆 (即取相反数) 封闭, 故 H 含有正整数. 设 n 是 H 中最小的正整数, 则 $n\mathbb{Z} \subseteq H$. 对任何 $m \in H$, 根据欧氏除法, 存在整数 q, r 使 $m = qn + r$, 其中 $0 \leqslant r \leqslant n-1$. 由于 $r = m - qn \in H$, 根据 n 的最小性推得 $r = 0$, 所以 $m \in n\mathbb{Z}$, 从而 $H \subseteq n\mathbb{Z}$.

由此可见, 除了平凡子群 0 外, $\mathbb{Z}$ 的子群是无限循环群.

习 题 1.2

1. 设 G 是由所有对角线上元素为 1 的 3×3 实上三角矩阵所组成的集合, 求证 G 在矩阵乘法下形成一个群并确定 G 的中心.

2. 设 G 是一个群, X, Y 是 G 的子集. 求证

(1) 若 $X \subseteq Y$, 则 $C(X) \supseteq C(Y)$;

(2) $X \subseteq C(C(X))$;

(3) $C(X) = C(C(C(X)))$.

3. 设 H 是群 G 的一个子群, 它包含在 G 的每一个非平凡子群中, 求证 H 包含在 G 的中心中.

4. 一个群 G 中的一个元素 $a \in G$ 叫做完全平方, 若存在 $b \in G$ 使 $a = b^2$. 现设 G 是一个循环群. 假定 $a, b \in G$ 都不是完全平方, 求证 ab 是完全平方. 举例说明对于非循环群此结论不一定成立.

5. 设 H 是有限群 G 的一个非空子集. 若 $ab \in H$ 对任意 $a, b \in H$ 成立, 则 H 是 G 的一个子群.

6. 设 $\boldsymbol{A}$ 是一个 $n\times n$ 实可逆矩阵, G 是由所有满足条件 $\boldsymbol{P}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{P} = \boldsymbol{A}$ 的矩阵 $\boldsymbol{P}$ 构成的集合. 验证 G 是 $GL_n(\mathbb{R})$ 的子群, 这里 $\boldsymbol{P}^{\mathrm{T}}$ 是 $\boldsymbol{P}$ 的转置.

1.3 置 换 群

中学里学过排列和组合, 如 $2, 1, 4, 5, 3$ 就是 $1, 2, 3, 4, 5$ 的一个排列, 知道 $1, 2, 3, 4, 5$ 总共有 $5! = 120$ 个不同的排列.

现在换个角度来看排列. $2,1,4,5,3$ 这个排列可以看成集合 $\{1,2,3,4,5\}$ 到它自身的一个双射 σ, 它把 1 映成 2, 2 映成 1, 3 映成 4, 4 映成 5, 5 映成 3. 用列表的方法可以把这个映射表示成

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{bmatrix}.$$

一般地, 有下面的定义:

定义 1.3.1　设 n 是一个自然数, 从集合 $\{1,2,3,\cdots,n\}$ 到它自身的一个双射称为 n 个文字的一个**置换** (permutation).

从上面的例子看出, 用列表法可把一个一般的置换 σ 表示为

$$\begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{bmatrix}.$$

这里的 $1,2,3,\cdots,n$ 并没有数量上的意义, 只是 n 个方便的符号而已, 这就是为什么把它们叫做“文字”而不是“数字”.

把 n 个文字的置换全体所构成的集合记作 S_n. 可以知道 S_n 是一个有限集合, 含 $n!$ 个元素, 这里 $n!$ 表示 n 的阶乘.

至此只是把排列这个概念用“双射”来重新叙述一遍, 但是利用它现在可以在 S_n 中引进二元运算. 设 $\sigma,\tau\in S_n$, 规定 $\sigma\tau$ 为这两个映射的复合, 复合的次序是先 τ 后 σ, 即 $\sigma\tau$ 是这样的映射, 它把 i 映成 $\sigma[\tau(i)]$. 很明显, $\sigma\tau$ 仍然是 $\{1,2,3,\cdots,n\}$ 到其自身的一个双射, 所以这确实是个二元运算.

命题 1.3.1　S_n 在如上定义的二元运算下构成一个 $n!$ 阶的有限群.

证明　根据复合映射的规则 $\sigma(\tau\pi)=(\sigma\tau)\pi$ 对任何 $\sigma,\tau,\pi\in S_n$ 成立, 所以结合律成立.

记 id 为 $\{1,2,3,\cdots,n\}$ 到其自身的恒等映射, 即 $\mathrm{id}(i)=i$ 对所有 $i=1,2,3,\cdots,n$, 则 $\mathrm{id}\sigma=\sigma\mathrm{id}=\sigma$ 对任何 $\sigma\in S_n$ 成立, 所以 id 是 S_n 的恒等元. 对任何 $\sigma\in S_n$, 由于它是一个双射, 它的逆映射存在, 它恰好是群论意义下 σ 的逆元. □

用列表法来作具体的群运算是很直接的, 如

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{bmatrix}=\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{bmatrix}^{-1}=\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{bmatrix}.$$

定义 1.3.2　S_n 的任何一个子群叫做一个**置换群** (permutation group), S_n 本身叫做 n 个文字的**对称群** (symmetric group).

本节介绍置换群的原因有两个, ① 这是一大类非常重要的有限群, ② 很多非 Abel 群的例子可以在置换群中找到, 这对于初学者尤为重要.

先来看几个低阶的置换群. 当 $n=1,2$ 时是十分简单的, 不去说它们了. 第 1 个非平凡的置换群是 S_3, 它的 6 个元素可罗列为

$$\sigma_0=\begin{bmatrix}1&2&3\\1&2&3\end{bmatrix},\quad \sigma_1=\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix},$$

$$\sigma_2=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix},\quad \sigma_3=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix},$$

$$\sigma_4=\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix},\quad \sigma_5=\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}.$$

容易算得 $\sigma_1\sigma_2=\sigma_4$, 而 $\sigma_2\sigma_1=\sigma_3$. 因此 S_3 不是 Abel 群!

不难验证 S_3 的非平凡子群有以下 4 个: $\{\sigma_0,\sigma_1\}$, $\{\sigma_0,\sigma_3\}$, $\{\sigma_0,\sigma_4\}$, $\{\sigma_0,\sigma_2,\sigma_5\}$.

S_3 的所有子群可以用图 1.1 来表示. 图 1.1 中的连接线表示该两个子群的包含关系, 下方子群是上方子群的子群. 这样的表示法可以使子群的包含关系一目了然.

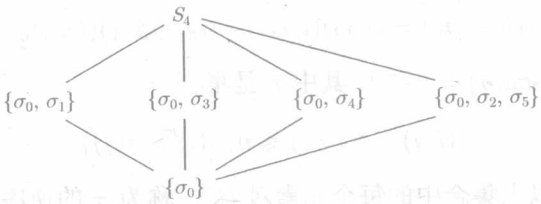

图 1.1

认真的读者可以尝试写出 S_4 的全部元素以及它的若干子群 (不一定要写出全部子群) 以及它们的关系图.

我们已经注意到, 置换的列表表示法不经济, 它的第一行实在显得多余. 更有甚者, 下面一个置换

$$\begin{bmatrix}1&2&3&4&5&6&7&8&9\\2&1&3&4&5&6&7&8&9\end{bmatrix}$$

用语言表达很简明: "把 1,2 两个文字交换一下, 其他文字保持不动", 但列表却很累赘. 这启发我们引进下面的概念:

定义 1.3.3 设 $i_1,i_2,\cdots,i_d$ 是在 $[1,n]$ 中的 d 个两两不同的文字. 作 $\sigma\in S_n$ 满足

$$\sigma(i_1)=i_2,\quad \sigma(i_2)=i_3,\quad \cdots,\quad \sigma(i_d)=i_1,$$

并且 $\sigma(i)=i$ 对 $[1,n]$ 中的所有其他文字 i 成立, 则 σ 叫做一个 d **轮换** (cycle) 或叫做长度是 d 的轮换, 记成 $(i_1i_2\cdots i_d)$. 这个记法不是唯一的, 如 $(i_2i_3\cdots i_di_1)$ 表示相同的轮换. 两个轮换称为不相交, 如果第一个轮换中的任何一个文字在第二个轮换中均不出现. 例如, 轮换 (142) 和 (36) 不相交, 轮换 (261) 和 (324) 相交.