

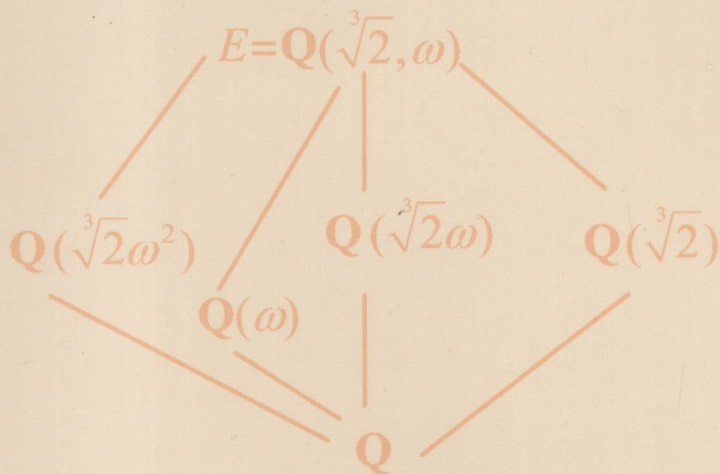
“十一五”国家重点图书
中国科学院指定考研参考书

中国科学技术大学 **精品** 教材


近世代数引论

第3版

冯克勤 李尚志 章 璞 编著



中国科学技术大学出版社



中国科学技术大学 **精品** 教材

近世代数引论

JINSHI DAISHU YINLUN

第3版

冯克勤 李尚志 章 璞 编著



中国科学技术大学出版社

内 容 简 介

近世代数是代数学一个基础学科,讲述代数基本结构的特性.本书除系统介绍群、环和域的基础知识(包括域的有限伽罗瓦扩张理论)之外,还力图强调近世代数中的思想和方法.书中有大量习题.除主线内容之外,还增加一些附录用来开拓和深化所学内容.

本书在中国科学技术大学讲授多年的讲义基础上修改写成.可作为高等学校数学系基础课教材,也可供数学工作者和通信、计算机科学等领域的工程技术人员参考.

图书在版编目(CIP)数据

近世代数引论/冯克勤,李尚志,章璞编著. —3版. —合肥:中国科学技术大学出版社,2009.12

(中国科学技术大学精品教材)

“十一五”国家重点图书

中国科学院指定考研参考书

ISBN 978-7-312-02292-0

I. 近… II. ①冯… ②李… ③章… III. 抽象代数 IV. O153

中国版本图书馆 CIP 数据核字(2008)第 161523 号

中国科学技术大学出版社出版发行

地址 安徽省合肥市金寨路 96 号,230026

网址 <http://press.ustc.edu.cn>

安徽辉隆农资集团瑞隆印务有限公司印刷

全国新华书店经销

开本:710×960/16 印张:12.25 插页:2 字数:240 千

1988 年 9 月第 1 版 2009 年 12 月第 3 版 2009 年 12 月第 6 次印刷

印数:17001—20000 册

定价:20.00 元

总 序

2008年是中国科学技术大学建校五十周年.为了反映五十年来办学理念 and 特色,集中展示教材建设的成果,学校决定组织编写出版代表中国科学技术大学教学水平的精品教材系列.在各方的共同努力下,共组织选题281种,经过多轮、严格的评审,最后确定50种入选精品教材系列.

1958年学校成立之时,教员大部分都来自中国科学院的各个研究所.作为各个研究所的科研人员,他们到学校后保持了教学的同时又作研究的传统.同时,根据“全院办校,所系结合”的原则,科学院各个研究所在科研第一线工作的杰出科学家也参与学校的教学,为本科生授课,将最新的科研成果融入到教学中.五十年来,外界环境和内在条件都发生了很大变化,但学校以教学为主、教学与科研相结合的方针没有变.正因为坚持了科学与技术相结合、理论与实践相结合、教学与科研相结合的方针,并形成了优良的传统,才培养出了一批又一批高质量的人才.

学校非常重视基础课和专业基础课教学的传统,也是她特别成功的原因之一.当今社会,科技发展突飞猛进、科技成果日新月异,没有扎实的基础知识,很难在科学技术研究中作出重大贡献.建校之初,华罗庚、吴有训、严济慈等老一辈科学家、教育家就身体力行,亲自为本科生讲授基础课.他们以渊博的学识、精湛的讲课艺术、高尚的师德,带出一批又一批杰出的年轻教员,培养了一届又一届优秀学生.这次入选校庆精品教材的绝大部分是本科生基础课或专业基础课的教材,其作者大多直接或间接受到过这些老一辈科学家、教育家的教诲和影响,因此在教材中也贯穿着这些先辈的教育教学理念与科学探索精神.

改革开放之初,学校最先选派青年骨干教师赴西方国家交流、学习,他们在带回先进科学技术的同时,也把西方先进的教育理念、教学方法、教学内容等带回到中国科学技术大学,并以极大的热情进行教学实践,使“科学与技术相结合、理论与实践相结合、教学与科研相结合”的方针得到进一步

修订版前言

这本讲义《近世代数引论》在中国科学技术大学使用了二十余年,也在清华大学、上海交通大学、北京航空航天大学、同济大学等校使用多年. 师生的反映尚好. 主要问题是习题较难. 所以我们在书末对于较难的习题增加了提示; 补充了一些新的习题; 同时对较难的习题标了星号; 其中有些可作为课堂上的例题, 有些可作为同学课后研讨之用, 而不作为基本的要求. 在内容上去掉了“幂零群与可解群”和“ $n(\geq 5)$ 次一般方程的根式不可解性”两节, 把它们改成两个附录. 我们也将正文中可略讲或只做简介的内容改用楷体字印刷. 其他一些内容, 例如伽罗瓦理论, 也可以只介绍基本定理的内容和它的应用, 而不讲证明.

作者

2002年2月第2版修订

2008年6月第3版修订

第 1 版前言

近世代数是讲述群、环、域(以及模)等代数对象基本性质的一门大学课程.它是今后学习和研究代数学的基础,也是研究其他数学、物理学和计算机科学等不可缺少的工具.

本书是我们于 1982 年在中国科学技术大学授课讲义基础上,经过五年教学实践改写而成.原讲义共五章,为了在一学期(周四学时)内讲完,这次删去了模论和线性代数两章.

近世代数从它产生的年代起就明显有别于古典代数学.它的主要研究对象不是代数结构中的元素特性,而是各种代数结构本身和不同代数结构之间的相互联系(同态).掌握近世代数中所体现的丰富的数学思想和方法,比背诵一些代数学定义和名词字典要重要得多.我们在教学中几乎用半个学期讲述第 1 章群论,这是因为在群论中体现了近世代数的基本研究思想和方法,而这些思想和方法在学生过去学习中是不熟悉的.群论中的定理基本上可分为定量和定性两类:前者的典型例子是拉格朗日定理,后者的典型例子是同态基本定理.我们着重讲授定性内容,特别是同态基本定理和群在集合上的作用,这是群论的关键所在.

第 2 章讲述环论和域论初步,正文中的内容是标准的.但是在几个附录中,我们介绍了在数学发展中有历史意义的几个课题(高斯二平方和问题、代数基本定理、尺规作图、三等分角等),最后一章向学生展示关于域的有限伽罗瓦扩张的优美理论.

最后,我们向过去几年里对此书的前身提供意见的许多学者、教师和学生表示深深的谢意,我们也欢迎大家今后对此书给予更多的批评和指正.

作者

1987 年 3 月于合肥

目 次

总序	(i)
修订版前言	(iii)
第 1 版前言	(v)
第 1 章 群	(1)
1.1 集合论预备知识	(1)
1.2 什么是群	(6)
1.3 子群和陪集分解	(11)
1.4 循环群	(18)
1.5 正规子群、商群和同态定理	(21)
1.6 置换群	(25)
1.7 群在集合上的作用	(30)
1.8 西罗定理	(35)
1.9 自由群和群的表现	(40)
1.10 有限生成阿贝尔群的结构	(45)
1.11 小阶群的结构	(49)
附录 1.1 可解群	(53)
第 2 章 环和域	(56)
2.1 基本概念	(56)
2.2 环的同构定理	(64)
2.3 同态的应用	(69)
2.4 交换环中的因子分解	(78)

第 1 章 群

1.1 集合论预备知识

群是集合上赋予某种二元运算的一种代数结构. 所以在讲述什么是群之前, 先要介绍集合论中我们所需要的一些预备知识.

一些特定的对象放在一起就叫做一个集合. 例如全体正整数构成一个集合, 表示成 \mathbf{N} . 全体整数构成整数集合, 表示成 \mathbf{Z} . 类似地有复数集合 \mathbf{C} , 实数集合 \mathbf{R} , 有理数集合 \mathbf{Q} 等等. 集合 A 中每个对象 a 叫做 A 中的元素, 表示成 $a \in A$, 说成 a 属于 A . 否则, 如果某个对象 b 不属于 A , 则表示成 $b \notin A$.

设 A 和 B 是两个集合, 如果 A 中每个元素均是 B 中元素, 即

$$a \in A \Rightarrow a \in B.$$

则 A 叫做 B 的一个子集, 表示成 $A \subseteq B$ 或者 $B \supseteq A$. 如果 $A \subseteq B$ 并且 $B \subseteq A$, 即

$$a \in A \Leftrightarrow a \in B,$$

这也相当于说集合 A 与 B 包含同样的元素, 这时叫做集合 A 与 B 相等, 表示成 $A = B$. 如果 A 是 B 的子集并且不等于 B , 则 A 叫 B 的真子集, 表示成 $A \subsetneq B$ 或者 $B \supsetneq A$. 不包含任何元素的集合叫做空集, 表示成 \emptyset . 空集显然是每个集合的子集.

可以有多种方式来表达一个确定的集合. 例如若集合 A 只有有限多(不同)元素 $a_1, \dots, a_n (n \in \mathbf{N})$, 则这个集合可表成

$$A = \{a_1, \dots, a_n\}.$$

只有有限多个元素的集合叫有限集, 否则叫无限集. 具有 n 个元素的集合叫 n 元集, 元素个数表示成 $|A| = n$. 在一般情形下, 集合 S 中具有某种性质 P 的全体元素构成的集合通常表成

$$\{x \in S \mid x \text{ 有性质 } P\}.$$

例如: 偶数集合 $\{0, \pm 2, \pm 4, \dots\}$ 可以表成

$$\{n \in \mathbf{Z} \mid n \equiv 0 \pmod{2}\}.$$

设 $f: A \rightarrow B$ 和 $g: B \rightarrow C$ 都是集合之间的映射. 则可经过连续作用, 得到一个从 A 到 C 的映射

$$g \circ f: A \rightarrow C, \quad (g \circ f)(a) = g(f(a)).$$

映射 $g \circ f$ 叫做 f 与 g 的合成映射.

设 f 和 g 均是从集合 A 到集合 B 的映射, 我们称 f 和 g 相等 (表示成 $f = g$), 是指对于每个 $a \in A$, 均有 $f(a) = g(a)$.

引理 1 (合成运算满足结合律) 设 $f: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$ 均是集合的映射, 则

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

证明 对于 $a \in A$, 令 $f(a) = b$, $g(b) = c$, $h(c) = d$. 则

$$(g \circ f)(a) = c, \quad (h \circ g)(b) = d.$$

于是

$$(h \circ (g \circ f))(a) = h(c) = d, \quad ((h \circ g) \circ f)(a) = (h \circ g)(b) = d.$$

从而对每个 $a \in A$, $(h \circ (g \circ f))(a) = ((h \circ g) \circ f)(a)$; 这就表明 $h \circ (g \circ f) = (h \circ g) \circ f$. 证毕.

设 $f: A \rightarrow B$ 是集合的映射. 对于 A 的每个子集 A' , 令

$$f(A') = \{f(x) \mid x \in A'\},$$

这是 B 的子集, 叫做 A' 在 f 之下的像. 另一方面, 对于 B 的子集 B' , 令 $f^{-1}(B') = \{x \in A \mid f(x) \in B'\}$, 这是 A 的子集, 叫做 B' 的原像. 如果 $f(A) = B$, 即 B 中每个元素均是 A 中某个元素 (在 f 之下) 的像, 则 f 叫做满射. 另一方面, 如果 A 中不同元素被 f 映成 B 中不同元素, 即: $a, a' \in A, a \neq a' \Rightarrow f(a) \neq f(a')$, 则 f 叫做单射. 最后, 若 $f: A \rightarrow B$ 同时是单射和满射, 则 f 叫做一一映射或一一对应. 例如: 将集合 A 中每个元素均映成其自身的映射

$$1_A: A \rightarrow A, \quad 1_A(a) = a.$$

就是 A 到 A 的一一对应. 映射 1_A 叫做集合 A 的恒等映射. 通常采用下面引理来判断一个映射是否为一一对应.

引理 2 映射 $f: A \rightarrow B$ 是一一对应的充分必要条件是存在映射 $g: B \rightarrow A$, 使得 $f \circ g = 1_B$, $g \circ f = 1_A$.

证明 如果 f 是一一对应, 由定义知这意味着对每个 $b \in B$, 均存在唯一的 $a \in A$ 使得 $f^{-1}(b) = a$ (存在性由于 f 是满射, 唯一性由于 f 是单射) 于是可定义映射

$$g: B \rightarrow A, \quad g(b) = f^{-1}(b).$$

直接验证 $g \circ f = 1_A$ 和 $f \circ g = 1_B$ 成立.

$$a \sim b \Leftrightarrow a \text{ 和 } b \text{ 在同一 } A_i \text{ 之中.}$$

请读者证明这是等价关系. 以 E 表示 A 的全部等价关系, 以 P 表示 A 的全部分拆, 则上面由等价关系到分拆的映射 $f: E \rightarrow P$ 和从分拆到等价关系的映射 $g: P \rightarrow E$ 满足 $f \circ g = 1_P$, $g \circ f = 1_E$, 从而 f 是一一对应(引理 2). 换句话说, 集合 A 上的等价关系和 A 的分拆是一一对应的.

例如, 设 F 是由某些集合构成的集族. 在 F 上定义如下的关系: 对于 $A, B \in F$,

$$A \sim B \Leftrightarrow \text{存在从 } A \text{ 到 } B \text{ 的一一对应.}$$

这是 F 上的等价关系(自反性: $1_A: A \rightarrow A$ 是一一对应, 从而 $A \sim A$. 对称性: 若 $f: A \rightarrow B$ 是一一对应, 则 $f^{-1}: B \rightarrow A$ 是一一对应, 从而 $A \sim B \Rightarrow B \sim A$. 传递性基于习题 3.) 对于这种等价关系, 彼此等价的集合叫做是等势的. 比如说, 两个有限集合等势(即存在一一对应)的充要条件是它们有同样多元素, 即 $|A| = |B|$. 与正整数集合 \mathbf{N} 等势的集合叫做可数无限集合, 其他无限集合叫做不可数集合. 熟知实数集合 \mathbf{R} 是不可数集合. 而正偶整数的全体 E 是可数(无穷)集合, 因为存在着 $1-1$ 对应 $\mathbf{N} \rightarrow E, n \mapsto 2n$. 这个例子也表明, 无限集合 A 的一个真子集可以与 A 等势!

设 A 是集合. 从 $A \times A$ 到 A 的映射

$$f: A \times A \rightarrow A$$

叫做集合 A 上的一个(二元)运算. 例如: 通常复数加法就是运算

$$f: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}, \quad f(\alpha, \beta) = \alpha + \beta.$$

我们经常把集合 A 上的运算表示成 \cdot , 即对于 $a, b \in A$, $f(a, b)$ 写成 $a \cdot b$ ($\in A$) 或者更简单地写成 ab .

运算 \cdot 叫做满足结合律, 是指

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad (\text{对任意 } a, b, c \in A).$$

运算 \cdot 叫做满足交换律, 是指

$$a \cdot b = b \cdot a \quad (\text{对任意 } a, b \in A).$$

一个集合赋予满足某些特定性质的(一个或多个)二元运算, 便得到各种代数结构. 本书讲述群、环和域三种代数结构.

习 题

1. 设 $B, A_i (i \in I)$ 均是集合. 试证:

他们将半群 S 中这个唯一的幺元素(如果存在的话)通常记作 1_S 或者 1 , 具有幺元素的半群叫含幺半群.

定义 3 设 S 是含幺半群. 元素 $y \in S$ 叫做元素 $x \in S$ 的逆元素, 是指 $xy = yx = 1$.

如果 x 有逆元素, 则它一定唯一. 因为若 y' 也是 x 的逆元素, 则 $xy' = y'x = 1$. 于是

$$y = y \cdot 1 = y(xy') = (yx)y' = 1 \cdot y' = y'.$$

所以, 若 x 具有逆元素, 我们把这个唯一的逆元素记作 x^{-1} , 则 $xx^{-1} = x^{-1}x = 1$.

定义 4 半群 G 如果有幺元素, 并且每个元素均可逆, 则 G 叫做群. 此外, 若运算又满足交换律, 则 G 叫做交换群或叫阿贝尔(Abel)群.

下面给出半群和群的一些例子.

例 1 设 M 为非负整数全体, $(M, +)$ 是含幺交换半群, 幺元素是数 0 , 但它不是群, 因为, 只有 0 对于加法在 M 中才可逆.

$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ 对于加法均是阿贝尔群, 分别叫做整数加法群, 有理数加法群等等.

(\mathbf{N}, \cdot) 是含幺交换(乘法)半群, 幺元素为 1 . 它不是群. 令 \mathbf{Q}^* 为非零有理数全体, 则 (\mathbf{Q}^*, \cdot) 是交换群, 幺元素为 1 , 非零有理数 α 的乘法逆为 α^{-1} . 这叫非零有理数乘法群, 同样有 (\mathbf{R}^*, \cdot) 和 (\mathbf{C}^*, \cdot) , 这些都是阿贝尔群.

例 2 以 $M_{m,n}(\mathbf{C})$ 表示全体 m 行 n 列复矩阵组成的集合, 它对矩阵加法形成阿贝尔群. 幺元素是全零矩阵, 而矩阵 $A = (\alpha_{ij})$ 的加法逆是 $-A = (-\alpha_{ij})$. 以 $M_n(\mathbf{C})$ 表示 n 阶复方阵全体, 它对乘法形成含幺半群, 幺元素是单位方阵 I_n . 由线性代数可知, n 阶复方阵 A 有乘法逆的充要条件是 $\det A \neq 0$. 从而 $M_n(\mathbf{C})$ 不是群, 并且当 $n \geq 2$ 时, 易知半群 $M_n(\mathbf{C})$ 不是交换的. 类似有加法交换群 $M_{m,n}(\mathbf{R})$, 含幺半群 $M_n(\mathbf{Q})$ 等等.

例 3 设 A 是非空集合, 以 $\Sigma(A)$ 表示从 A 到 A 全体映射组成的集合. 则 $\Sigma(A)$ 对于映射合成运算形成含幺半群. 幺元素为 A 上恒等映射 1_A . 由 1.1 的引理 2 可知, $\Sigma(A)$ 中映射 f 可逆的充要条件是 f 为一一对应. 所以当 $|A| > 1$ 时, $\Sigma(A)$ 不是群, 并且半群 $\Sigma(A)$ 不是交换的.

例 4 欧氏平面 \mathbf{R}^2 中保持欧氏距离不变的运动叫做欧氏运动. 由于欧氏运动必为 \mathbf{R}^2 到自身之上的一一对应, 并且它的逆仍是欧氏运动, 而两个欧氏运动的合成仍是欧氏运动, 从而全体欧氏运动形成群, 叫做平面上的欧氏运动群, 这也是非阿贝尔群.

例 5 设 n 为正整数, 我们在 \mathbf{Z} 上定义如下关系: 对于整数 a 和 b ,

