

高
等
学
校
教
材

近世代数

(第三版)

杨子胥 编著



高等教育出版社
HIGHER EDUCATION PRESS

高等学校教材

近世代数

Jinshi Daishu

(第三版)

杨子胥



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

内容简介

本书是作者在长期教学实践的基础上,参考国内外大量相关教材、专著、文献并吸纳个人一些科研成果编写而成的。本次修订是在《近世代数》(第二版,杨子胥编著)的基础上,作了较大的修改:删除了部分内容,降低了深度和难度;改写和调整了一些定理及其证明;删去了一些例题和习题;改正了部分错误;增强了本书的可读性、适用性。内容包括基本概念、群、正规子群和群的同态与同构、环与域、唯一分解整环、域的扩张等。

本书第一版由万哲先、王梓坤两位院士推荐出版,并由刘绍学教授撰写序言。

本书可作为综合性大学、高等师范院校数学类专业近世代数课程的教材。

图书在版编目(CIP)数据

近世代数/杨子胥编著. —3版. —北京:高等教育出版社,2011.1

ISBN 978-7-04-030072-7

I. ①近… II. ①杨… 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(2010)第 215765 号

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	咨询电话	400-810-0598
邮政编码	100120	网 址	http://www.hep.edu.cn http://www.hep.com.cn
经 销	蓝色畅想图书发行有限公司	网上订购	http://www.landaco.com http://www.landaco.com.cn
印 刷	北京七色印务有限公司	畅想教育	http://www.widedu.com
开 本	850×1168 1/32	版 次	2000年5月第1版 2011年1月第3版
印 张	8.25	印 次	2011年1月第1次印刷
字 数	210 000	定 价	16.00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。

版权所有 侵权必究

物料号 30072-00

第一版序言

近世代数(或抽象代数)是大学数学系的重要基础课之一,主要介绍群、环、域(以及模)的基本概念和基本理论。在这里人们将受到良好的代数训练,并为进一步学习数学打下一个扎实的代数基础。

我们知道,数、多项式和矩阵的出现是为了刻画一些物理量和几何量,诸如长度、面积、速度、物理定律、空间中点的位置、平面的运动和几何变换等。它们的表现能力是很强的,使用数、多项式和矩阵足以刻画我们遇到的许多物理量和几何量。然而当人们企图刻画对称性——无论是物理现象中,还是数学世界中(尤其是在几何图形中)的对称性时,都无法用单个的数、多项式或矩阵去刻画。为了刻画对称这一概念,人们发现了群。现在我们知道,群是研究对称性的有力工具。物理、几何、数学中对称这一概念的特殊重要性,使群成为近代数学极其深刻、极其重要的概念之一。

类似地,环、域、模也是刻画物理量和几何量的数学工具。

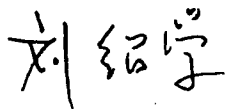
因而研究群、环、域、模的方式可分为两大类。一类是紧密结合其背景去研究,如晶体群、群与量子力学等;另一类是对群、环、域、模作理论上的研究。当然两者有着相互的联系。这样,自然地在介绍群、环、域、模的书中有两种不同的倾向。

本书则是介绍群、环、域的基本概念和基本理论。本书作者写的另一本书《正交表的构造》则是以群、环、域为基本工具,讲述正交表的构造原理和方法。

杨子胥教授从事高校代数教学与科研工作数十年,经验丰富,成果不断。他编写的这本《近世代数》,是他在长期教学实践的基础上,经过反复修改提炼整理而成的。本书取材广泛,内容丰富且

紧扣大纲,前后呼应,非常紧凑。其中一个概念的引入,一种思想的建立或一个定理的证明,都字斟句酌一丝不苟,既保持严格的科学性和系统性,又自然明快易于接受。

近世代数是比较抽象的一门学科,但本书所举正反例子较多,涉及面广,尽量把抽象的概念和问题具体化。而且还特别注意同高等代数的联系,每节所配备的习题的数量和难易程度适当,尤其是文句叙述和表达自然流畅,读来引人入胜,确实不失为一本好的近世代数教材。

The image shows a handwritten signature in black ink. The characters are '刘绍学' (Liu Zhenxue), written in a cursive, calligraphic style. The first character '刘' is on the left, and '绍学' are on the right, with a vertical line separating them.

1998年7月1日于北京师范大学

第三版前言

考虑到近世代数教学学时不多的现实,同时也是为了更好地适应教与学,本书这次修订的重点是“瘦身”,即对第二版中的诸如传递群、群的直积、共轭关系与正规化子、 p -环、零化子、环的同态与同构、分式域、环的直和、可离扩域等内容,都进行了删减。有些内容,例如群的直积,整节删去,只保留其中必要的内容在适当的章节中加以介绍。

这次修订还删去了一些例题和习题,特别是习题,共删去一百余题。另外还改写和调整了一些定理及其证明,这使所讨论的问题和证明更加流畅和明晰。

为了适应新的需要,这次修订新增两节——群在集合上的作用和有限域的一种应用。但都打了星号,可选讲或不讲。

本课程若每周上课4学时,一学期共约70学时,讲完全书未打星号的34节,基本上是可以的;若每周上课3学时,一学期共约50学时,讲完前四章未打星号的25节也是可以的。当然,若时间仍紧,还可以压缩一些例题和定理的证明;若时间宽裕,也可以选讲一些打星号的内容,如素理想和极大理想等。

新的第三版,可望用起来会更加自然流畅和得心应手。

顺便指出,作者针对第二版内容所编写的配套书《近世代数学习辅导与习题选解》对新的第三版仍然适用。该书对教师备课会很有帮助,并可节省时间。

这次修订,山东大学许玉铭教授提出不少宝贵意见,我表示衷心感谢!

虽力求修订完善,但书中肯定仍有不足甚至错误,恳请读者多予指正。

杨子胥

2010年6月

第二版前言

本书这次修订主要的变动有如下四个方面：

一、更正了一些错误，改动了个别定理的证明方法，特别是去掉了一些不很必要的内容。

二、增加了传递群、单群、可解群和幂集环等概念和相应的一些定理和例子。此外还增加了少数交换图、一些研究对象的历史背景介绍以及“本书所用符号”和“参考文献”等。

三、对习题作了较大调整，去掉了少数题目，每节题量减少，难度降低。但在每章最后一节的习题中却增加题目较多，题量稍大一些。其主要目的是，可通过这些习题对本章内容起一个复习巩固的作用；当然，其中也有少数题目难度稍大一些，可供学生参考或习作。

四、个别章节顺序作了调整，有的章节和个别定理打上星号，这些内容可略讲或不讲。

由于各校情况不同，因此在使用本书时应灵活掌握，不可千篇一律。例如上面已谈到，对于打星号的章节可略讲或不讲。比如 Sylow 定理，它是群论特别是有限群论中经典结论之一，尤其是它的证明几乎涉及了前三章中群理论的所有概念。不仅如此，由 Sylow 定理还可以很容易地推演出大量有关一些群的重要结论和结构定理。因此，若课时不够，即使不讲定理证明但介绍一下 Sylow 定理本身的内容和意义也是很有价值的。

据知，有些高校只讲前四章，其实这也是可以的，因为这四章可以说涵盖了近世代数最基本的内容。当然，如果条件允许，也可以简略介绍一下主理想整环和欧氏环以及第六章的前三节。

对于习题，一般而言，每节选 3 至 5 个题做作业即可。而对余

下的题目,特别是每章最后一节中的习题,可让学有余力和考研的同学课下自行练习。

我将编写《近世代数学习辅导与习题选解》(高等教育出版社出版),几乎包含了本书所有习题的解答,因此可作为高校师生学习参考之用。但这里应提醒读者的是,对任何题解都不可产生太大的依赖性。这如同身体不适服药一样,适当用药有益健康,过量服用则有损机体。正确的方法应该是,对于一个题目要尽量自己先动脑去想,实在做不出时再参阅题解。这样用辅导书可能效果会更好一些。

在本书这次修订中,山东大学张顺华教授、陕西师大雷天德教授、潍坊学院王新民教授、解放军信息工程大学马传贵教授以及曲阜师大、济南大学和山东师大等校有关老师,都提出了不少宝贵意见,我表示衷心的感谢!

这次修订虽主观力求完善,但仍难免还有不妥之处,希望读者多多指正。

杨子胥

2003年6月

第一版前言

本书是作者在长期教学实践的基础上,参考国内外大量相关教材、专著、文献并吸纳个人一些科研成果编写而成的。

全书共六章,可大致分为三个部分:

第一部分,包括引言和第一章基本概念,它是全书的基础,在以后各章都要用到,应予以充分重视。

第二部分,包括第二、三两章,介绍含一个代数运算的群的理论。其中第二章介绍群的最基本的知识;第三章则进一步介绍正规子群和群的同态与同构,以及和它们相关联的群论中最基本、最重要的定理,如群的同态和同构定理,共轭、正规化子和中心化子, Sylow 定理和有限交换群基本定理等等。

第三部分,包括第四、五、六三章,介绍含有两个代数运算的环与域的理论。其中第四章介绍环的基本知识;第五章介绍环论中一个特殊问题——唯一分解整环内的因子分解理论,并由此介绍了两种特殊的环类,即主理想整环和欧氏环;第六章介绍域,一种加强条件的环,并且主要介绍代数扩域,特别是有限次扩域和有限域。

本书取材广泛,有的高校若教学时间不够,有些内容,例如多项式环、环的直和、非交换环、唯一分解整环的多项式扩张、可离扩域或其他内容,可粗讲或不讲,或只详述结论而略去证明。本书每节都配备了习题,其题量和难度比较适中,个别稍难题目都有提示,各校可根据不同情况择题而做。

本书承蒙我国数学家、中科院院士万哲先研究员和我国数学家、中科院院士王梓坤教授推荐出版,并承蒙我国数学家、北京师范大学博士生导师刘绍学教授撰写序言,作者由衷地对他们表示最诚挚的感谢!

作者才疏学浅，书中错误和疏漏之处恐在所难免，恳请读者批评指正。

作者

1999年5月

目 录

引言	1
第一章 基本概念	3
§ 1 集合	3
§ 2 映射与变换	5
§ 3 代数运算	11
§ 4 运算律	15
§ 5 同态与同构	20
§ 6 等价关系与集合的分类	24
第二章 群	29
§ 1 群的定义和初步性质	30
§ 2 群中元素的阶	37
§ 3 子群	43
§ 4 循环群	48
§ 5 变换群	53
§ 6 置换群	58
§ 7 陪集、指数和 Lagrange 定理	65
*§ 8 群在集合上的作用	72
第三章 正规子群和群的同态与同构	78
§ 1 群同态与同构的简单性质	78
§ 2 正规子群和商群	83
§ 3 群同态基本定理	92
§ 4 群的同构定理	97
§ 5 群的自同构群	102
*§ 6 Sylow 定理	107

*§ 7	有限交换群	120
第四章	环与域	130
§ 1	环的定义	130
§ 2	环的零因子和特征	138
§ 3	除环和域	142
§ 4	模 n 剩余类环	148
§ 5	环与域上的多项式环	155
§ 6	理想	159
§ 7	商环与环同态基本定理	166
*§ 8	素理想和极大理想	171
*§ 9	非交换环	177
第五章	唯一分解整环	186
§ 1	相伴元和不可约元	186
§ 2	唯一分解整环定义和性质	191
§ 3	主理想整环	195
§ 4	欧氏环	199
*§ 5	唯一分解整环的多项式扩张	201
第六章	域的扩张	207
§ 1	素域和域的添加	207
§ 2	单扩域	212
§ 3	代数扩域和有限次扩域	217
§ 4	多项式的分裂域	223
§ 5	有限域	227
*§ 6	有限域的一种应用	232
	本书所用符号	243
	名词索引	245
	参考文献	249

引 言

代数学是数学的一个古老分支,有着悠久的历史.但是,近一百年来,随着数学的发展和应用的需要,代数学的研究对象和研究方法发生了巨大的变化,一系列新的代数领域被建立起来,大大地扩充了代数学的研究范围,形成了所谓的近世代数学.

大家知道,数是我们研究数学的最基本的对象,数的最基本的运算是加、减、乘、除.但是,数并不是我们研究数学的唯一对象,而且我们所遇到的许多运算也不全是数的普通加、减、乘、除.例如,向量、力以及多项式、函数、矩阵和线性变换等等,它们虽然都不是数,但却也可以类似于数那样来进行运算.特别是,尽管这些研究对象千差万别,各有自己的特性,但是从运算的角度看却有着很多共同的性质.于是,从一般的集合出发,研究各种运算的种种性质,就具有非常重要的意义,因为它的结论和方法不仅可以渗透到数学的各个分支,而且在其他学科,例如在物理、化学、正交试验设计和编码等理论中都有重要应用.

一个集合,如果有一种或数种代数运算,我们就笼统地称它是一个代数系统.简言之,近世代数就是研究各种代数系统的一门学科.在近世代数中,尽管有时,特别是在举例时,也讲具体的集合和具体的运算,但其最根本的任务是研究各种抽象的代数系统.也就是说,一般来讲,不仅所说的集合是抽象的,而且所说的运算也是抽象的.因此,也常把近世代数叫做抽象代数.

由于代数系统中运算个数以及对运算所要求的附加条件的不同,从而产生了各种各样的不同的代数系统,这就形成了近世代数中各个不同的分支.其中最基本、最重要的分支是群、环和域,它们所研究的内容极为丰富和广泛.实践已经证明,这些理论不仅对数

学本身产生重要影响并有重要应用,而且对其他学科也有重要影响和应用. 这样一来,古老的代数学在新的基础上又以全新的面貌和更加旺盛的生命力飞速地向前发展着.

本课程的任务是,介绍近世代数中最基本的代数系统——群、环、域的最基本的概念和性质.

第一章 基本概念

本章所介绍的内容,是在以后各章中都要用到的基本概念.它们是:集合、映射与变换、代数运算、运算律、同态与同构、等价关系与集合的分类等.

§ 1 集 合

我们在讨论问题时,在一定范围内所说的对象,例如,数、向量、多项式、矩阵、点、直线,甚或书架上的书、桌子上的茶杯、钢笔、铅笔等等,都笼统地称为元素或元.

若干个(有限个或无限个)固定元素的全体,叫做一个集合,或简称为集.

集合常用大写拉丁字母 $A, B, C, \dots, G, R, F, \dots$ 来表示;集合中的元素常用小写拉丁字母 $a, b, c, \dots, x, y, \dots$ 来表示.

如果 x 是集合 A 中的一个元素,就说 x 属于集合 A 或集合 A 包含 x ,记为 $x \in A$ 或 $A \ni x$;如果 x 不是集合 A 中的元素,就说 x 不属于集合 A 或集合 A 不包含 x ,记为 $x \notin A$ 或 $A \not\ni x$.

不包含任何元素的集合称为空集合,记为 \emptyset .

不过今后凡谈到集合时,一般均指非空集合.

今后还常用 Z 表示整数集, Z^* 表示非零整数集;用 Q 表示有理数集, Q^* 表示非零有理数集.

要指明一个集合是由哪些元素构成的,可以用列举法,例如

$$A = \{1, 3, 5\}, \quad B = \{\text{东}, \text{西}\},$$

$$C = \left\{ 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots \right\};$$

有时也可以用描述法,例如

$$E = \{\text{全体正有理数}\}, \quad F = \{x | x \text{ 是实数且 } x^2 < 1\}.$$

定义 1 如果集合 A 的每个元素都属于集合 B , 则称 A 是 B 的一个子集, 记为 $A \subseteq B$.

如果 A 是 B 的一个子集, 又 B 中有元素不在 A 中, 则称 A 是 B 的一个真子集, 记为 $A \subset B$.

空集合被认为是任意集合的一个子集.

当集合 A 不是集合 B 的子集或真子集时, 分别记为 $A \not\subseteq B$ 或 $A \not\subset B$.

显然, $A \subseteq B$ 意味着 $A \subset B$ 或 $A = B$ (即 A 与 B 是由完全相同的元素作成的集合). 一个虽然简单但却非常重要的事实是:

$$A = B \iff A \subseteq B \text{ 且 } B \subseteq A.$$

因此, 要证两个集合 A 与 B 相等, 常需证明 $A \subseteq B$ 且 $B \subseteq A$, 即 A 与 B 互相包含. 这个事实虽然简单, 但它却是贯穿整个近世代数的一个一般方法.

如果把集合 A 的每一个子集当成一个元素, 则 A 的所有子集 (包括空集合) 也作成集合, 称为 A 的幂集, 记为 $P(A)$.

如果集合 A 包含无限多个元素, 则记为 $|A| = \infty$; 如果 A 包含 n 个元素, 则记为 $|A| = n$. 于是易知, 当 $|A| = n$ 时,

$$|P(A)| = 2^n.$$

定义 2 由集合 A 和集合 B 的所有公共元素作成的集合, 记为 $A \cap B$, 叫做 A 与 B 的交集, 简称 A 与 B 的交. 即

$$A \cap B = \{x | x \in A \text{ 且 } x \in B\}.$$

例如, 集合 $A = \{0, 1, 2, 3\}$ 与集合 $B = \{0, 2, 4\}$ 的交为

$$A \cap B = \{0, 2\}.$$

但是, 集合 A 与集合 $C = \{4, 5, 6\}$ 的交为空集合, 即

$$A \cap C = \emptyset.$$

定义 3 由属于集合 A 或集合 B 的所有元素作成的集合, 记为 $A \cup B$, 叫做 A 与 B 的并集, 简称 A 与 B 的并. 即