近世代数

主　编　徐常青　徐光辉

P2={{a
P1={a,b,c,
P1={a,b,c,d}
P2={{a,b},{c,d}}

P1={a,b,c,d}
P2={{a,b},{c,d}}

JINSHI DAISHU

合肥工业大学出版社

近世代数

JINSHI DAISHU

近世代数

主　　编　徐常青　徐光辉
编写组成员　徐常青　徐光辉　王章雄

合肥工业大学出版社

图书在版编目(CIP)数据

近世代数/徐常青,徐光辉主编.—合肥:合肥工业大学出版社,2007.2
ISBN 978-7-81093-537-1

Ⅰ.近… Ⅱ.徐… Ⅲ.抽象代数—高等学校—教材 Ⅳ.0153

中国版本图书馆 CIP 数据核字(2007)第 013064 号

近 世 代 数

主编 徐常青 徐光辉　　责任编辑 朱移山

出 版	合肥工业大学出版社	版 次	2007 年 2 月第 1 版
地 址	合肥市屯溪路 193 号	印 次	2007 年 2 月第 1 次印刷
邮 编	230009	开 本	710×1000 1/16
电 话	总编室:0551-2903038	印 张	16
	发行部:0551-2903198	字 数	291 千字
网 址	www.hfutpress.com.cn	发 行	全国新华书店
E-mail	press@hfutpress.com.cn	印 刷	合肥现代印务有限公司

ISBN 978-7-81093-537-1　　定价:25.00 元

前　言

近世代数的教学几个世纪以来并没有因为时代的变迁而有所改观。在高校里，一提起“抽象”，人们似乎就想到“抽象代数”，因而也就想到那些几个世纪以来一直没有改变的“群、环、域”，想到令人头痛、摸不着头脑甚至一辈子也用不上的子群、商群。事实上，如果你随机问问那些在校的大学生或者研究生，大概不会有人说：“我喜欢近世代数这门课。”尽管隐藏在它的“抽象性”背后的广泛实用性和具体性已经人人皆知，但能适应这种抽象的纯数学（包含近世代数、实变函数、微分几何等）的学生并不多。有的院校在考虑到学生个人喜好、毕业去向和今后的创业发展时，甚至认为这种抽象的东西因不能被本科生所普遍接受而应当被诸如计算机网络、人工智能等非数学课所取代。确实，这种抽象的传统数学基础课程无论如何也不可能吸引众多学生的眼球。相反，大部分学生（除了一部分因为考研需要）因为对近世代数的应用没有足够的了解，缺乏足够的兴趣和信心而选择放弃抽象代数的学习。因此，抽象代数的教学改革就显得更加迫在眉睫：我们首先必须认识到抽象代数是很多后续课程（包括泛函分析、统计学以及计算机科学等工程学科的课程）的必备工具：没有抽象代数作为基础，各种自然科学的理论以及应用性研究（其中包括国防尖端科技、航天航空、人工智能、模式识别、计算机网络等）是不可能进行的，我们必须让我们的学生能领会到（至少是初步地）这些应用。同时我们也必须清醒地意识到，近世代数与高中数学以及微积分等课程的区别（我们在后面将会介绍这些区别）。

如何改革这门课程的教学方法，将这种传统数学基础课程继续下去，并能适应新世纪人才发展和培养的需要，是摆在我们面前的迫切任务。我们在这一方面做出了大胆的尝试，并运用多媒体教学方法、部分内容的可视化（与相关数学计算软件如 MatLab 等结合起来）等渠道来使得这些抽象概念变得具体一些。但这一改革的难点是：抽象代数中的定义、定理特别是结论的证明很难用多媒体来展示，而且多媒体课件（例如 PowerPoint 幻灯片）制作使得抽象代数的证明更

加笨拙。这使得很多人反对将多媒体教学引入数学特别是近世代数课程的教学中。为此,我们转而尝试在教材内容上的改革,使得学生在掌握近世代数的内容时能了解近世代数的每一个概念诞生的主要背景,从而更进一步了解他们之间的内部联系。事实上,我们很多人并没有意识到,近世代数这一学科恰好印证了传统哲学的发展观:从具体(问题),到抽象(概念),再回到具体(问题)。其内容具有以下特点:

概念顺序并不是按照其历史发展的时间顺序来的;

每一概念涉及的定理可以有多种表达形式;

每一部分内容相互关联、彼此影响(概念的彼此依赖性),又自成一体,很多概念后来甚至独立发展而成为一个代数发展分支(概念的彼此独立性);

与其他数学学科与应用学科的交叉,形成诸如量子群理论、代数几何、代数数论、代数拓扑学、组合群论、计算机代数(Computation Algebra)等重要分支。

我们有时对这种高度抽象的逻辑体系无所适从,对于那些初学者,情况更是如此。是的,数学,尤其是代数学,不像文学、历史或经济学能让读者立竿见影地感受到其中的乐趣,恰恰相反,它会让你在不经意中错过一点似乎是微不足道的东西,但就是这种不经意的思绪迁移(这也是一种数学概念)会让你对以后的内容感到琢磨不透,云里雾里。怎样才能理解每一个结论的含义和证明的思路?那些冗长的奇思妙想只会让人感叹它的美妙,而很难让人领略其中道理。这里,我们提倡先用一种非正规的自然论证方法(和语言)来使问题和解答通俗、简单化,从而可以帮助读者理解领会其中的精髓。"原来如此!"我们需要学生的这一句感叹,如果那是发自内心的!我们不但要求学生能知其然,还要求他们能知其所以然。

本书原计划分为 9 章,但考虑到本书主要读者对象为本科生(大三),我们删除了最后的 3 章。现在版本共分 6 章。我们建议用两学期共 160 学时左右的授课时间来讲授本门课程,具体课时以及章节次序请视具体情况而定。本书前 4 章为近世代数预备知识、群论基础、环和域论基础以及模理论部分的教学要占一学期(72～80 学时)的教学课时;这部分是大学代数课程的必修部分。我们要求相关专业的每一个本科生都能熟悉掌握其中的每一个概念、记号和结论,并能了解它们之间的关联,能独立解答各个章节后面的习题。

第 4 章中,我们将利用 Smith 标准型来介绍主理想整环上有限生成模的基

本结构定理，这样做是因为学生比较习惯于矩阵行、列初等变换。第5章将讨论群在集合上的作用。这方面结论的直接应用给出组合数学上的一些相关结论、Sylow定理以及简单群方面的一些结论；我们通过对正规群列的分析得出Jordan—Hölder定理以及可解群和幂零群。本章最后还将考察单群的有关性质；有关交错群和半直积的概念放在了本章的练习中。在第6章，我们主要介绍方程的Galois理论。首先我们将介绍多项式方程根的求解问题，导出Galois理论产生的背景。在第一节（预备知识部分），我们定义了一个域的本原子域，介绍了域的扩张，特别是有限维扩域理论；在第二节，我们详细介绍了著名的古希腊三大几何难题的求解——直尺/圆规作图问题，并证明了：只利用直尺和圆规，这三个几何问题（即：三分角、倍立方和圆化方问题）都是无解的；在第三节，我们考虑任意域上多项式的分裂域；在第四节，我们考察多项式的重根以及多项式的不可约性；第五节介绍了Galois群的一些基本结论。这些结论被用来作为判别方程可解性的Galois判别法的基础；作为本章也是本书的最后一节，第六节介绍了Galois群的定义、计算方程Galois群的方法，以及Abel扩张、循环扩张等。

作为本书的续编，我们计划在不久编辑一本《近世代数续论》，内容将主要介绍近世代数在其他领域（包括代数数论、代数几何、非交换代数和同调代数[含类(categories)和算子(functors)理论]）的应用、仿射空间理论，并由此引出Hilbert基本定理、基定理(Basistheorem)以及Nullstellensatz理论，给出Nullstellensatz理论的几种等价形式和它在几何中的应用（有关局部化理论和本原分解的代数技巧也由此产生），张量积，几个应用广泛的代数概念如偏序、偏序集、格、布尔代数、范畴和函子。如果你是从事计算机科学，或者是物理学、化学分子学、生物学等学科研究的话，那么你一定不会对这些概念感到陌生。这些概念因其在物理、计算机科学和电子等领域（尤其是交叉领域）应用广泛而越来越被人们所重视。事实上，上述的这些基本概念在不同的阶段已经产生了相应的不同分支。它们（如计算机代数学等）对数学本身以及其他自然科学（甚至社会科学）领域的发展都起到了非常重要的作用。如果可能的话，我们还将简单介绍同调代数。

我们认为，一本好的教材应该是在作者借鉴大量的其他教材和资料（包括前人的研究成果）的基础上，结合该学科当前发展动向（为日后培养高素质的科研人员作准备），渗透个人教学的思想和见解才能完成的（这只是必要条件）。数学

各学科乃至自然科学的教与学，都有一定的共性，但更重要的是，数学每一门学科还有它自己独特的一面。教材既要反映这种共性，又要反映这种个性。最后，我们还应站在读者的角度看问题和思考问题。这就好比写一本小说，我们知道萧伯纳写小说的故事：他在完成每一部作品之前，总要先把自己的作品读给其他人听，直到对方满意为止。当然，数学教材不是通俗读物，你很难做到让每一个人满意，但你必须首先了解你的读者群。我们试图将这种思想贯穿于这本教材。但它毕竟是近世代数，我们无法改变它抽象的本质，只能借有限的篇幅在有限的空间里做出有限的尝试。错误、不妥在所难免，敬请各位能提出宝贵意见。

这里，我们要感谢浙江林学院教务处对于本教材出版的大力支持，他们为本教材的出版发行提供了经费赞助。我们还要特别感谢合肥工业大学出版社对于本书出版的大力支持。

编　者

2006 年 12 月 1 日

于杭州临安

目　录

第一章　预备知识

§1.1　背景介绍

1.1.1　代数学:一部长篇史记

在西方数学史上,最早让方程式等号一边为 0 的数学家当是韦达(F. Vieta, 1540～1603),他同时也是符号代数(symbolic algebra)的发明人. 他不仅利用符号(字母)代表未知数,而且也开创了用符号来代表已知数;他还严格区分算术与代数:前者处理数目,而后者处理事物的形式 (species or forms of things). 因此,他强调研究方程式的一般形式,而非个别的特定方程式. 正是他的符号法则创立了方程式理论这一门新学科. 事实上,在韦达之后,代数不再只是几个特定方程的求解,它已经被认为是一种"真正合法的"数学语言了.

尽管如此,在韦达出版其经典作品《解析方法入门》(*Introduction to Analytic Art*, 1595)100 年内,符号代数始终被认为是一种"新"的代数(modern Algebra). 18 世纪初,求根方法被引入中国. 但在整个 17 世纪的西方,代数学仍然是新旧并存的局面(这里的旧代数是指算术). 即使在 1650 年之后,新代数逐渐被多数人接受,旧代数仍有它的市场. 至于为什么有人无法全面接受新代数,或许是因为大多数人还无法赋予符号运算以实际意义吧!

人们在教授近世代数的时候,很少提及当初一些概念(如群、环、域、模和代数)的产生. 普遍的观点是,这些东西与我们讲授的内容似乎关系不大. 殊不知,无论是本科生还是研究生,他们都想知道何人何时在何地为什么、怎样创立了这些理论体系(如群、环论)等. 本书试图让读者感受到时间隧道的功能,让读者顺着时间坐标轴的负方向站在每一位数学巨匠所处的那一时刻,来观赏代数学的绚丽火花在每一历史时刻的绽放. 有了时间这根线索,我们就能赋予抽象代数以故事情节,让抽象的概念融入到具体的历史环境中. 这里,我们有故事的主人翁——每一位数学概念的缔造者,数学家. 将抽象的数学概念与具体的人物结合在一起,不但使我们能进一步理解其中每一个概念与伟大结论的诞生,更能使我

们了解时代的变迁对于近世代数发展的影响，以及其中的基本概念与结论的进化、演变和相互之间的关联.

在1930年的一次公开演讲中，萧伯纳在评价爱因斯坦时说："伟人有一般人中的伟人，但也有伟人中的伟人. 拿破仑和其他伟人就是这样的人(伟人中的伟人)，他们是国家的缔造者. 但还有一种人是超越他们之上的，他們不是国家的缔造者，是宇宙的缔造者."萧伯纳在这里说的宇宙是指自然及其规律，宇宙的缔造者当然就是那些创立发现了这些隐藏其中的奥秘和规律体系的人，自然这些伟人应该包括像 Euler、Gauss、Euclid、Abel、Galios 这些数学巨匠. 离开了这些伟人，代数学乃至各个自然科学就无法诞生，代数学中的每一个概念也就无法具体、形象化. 在代数学这部浩瀚的史书里，我们不但可以领略到那些改变历史和创造宇宙自然的伟人的风采，还能体会到他们那种为了数学科学献身的精神.

我们不是数学史研究者，不可能去翻阅众多的数学发展史资料. 但我们始终相信，了解数学发展史，才能了解代数学(何止是代数学?)中的每一个抽象概念的含义和它的来龙去脉，从而才能了解代数学家们创立各种代数体系的思想根源，才能进一步体会每一个定理结论的真实意图和发展方向. 了解数学家所处的环境和习惯，有助于我们在相关领域做进一步的研究，更能激发学生的学习热情，让他们知道，献身于数学正和献身于其他任何一项事业或专业一样，也能获得无穷的乐趣. 让学生了解历史，了解历史人物的诞生和他们那种天才的思维，对于后人无疑是一种启发.

1.1.2 思维的转变：公理系统的诞生

代数学科的诞生同时也意味着数学公理系统(或规则)的诞生. 我们一般并不能告诉我们的学生公理系统是如何诞生的. 但是，对于那些在此之前只接触过线性代数和微积分的学生来说，他们很难理解为什么要用更加抽象的概念和方法(近世代数中的"代数"结构)来处理诸如线性代数中的线性空间这样一个非常具体的东西. 我们甚至想当然认为有些东西的存在(如欧式几何)是显然的. Euclid 在给出欧式几何的公理之前，首先定义了几何的基本元素(如点、线等). 近世代数体系则不然，它首先并不关心所研究的对象(如一个群、环、域中的每一个元素代表什么，几何中的点、线代表什么)，而只关心建立在此系统上涉及的一些(运算)规则(如乘法的结合律、交换律；几何中两点决定一条直线等). 这和中学数学以及大学微积分迥然不同：在那里，首先你得理解具体涉及的数集(数域)以及其上定义的加法、减法和乘法运算，然后你才能进行运算(如求导、求极限、求积分等)；你得首先熟悉大量具体的函数实例以及微、积分概念，然后才能掌握进

行微积分运算的一些规律.那里涉及的运算、规则非常自然,没有人会想到为什么要如此定义.但近世代数则不然:通常一本近世代数教材以群论(预备知识除外)为开篇,并以下面的方式来介绍群:"一个满足以下三条规则的代数结构(集合连同它上面定义的运算)称为一个群"……我们强调的是这三条公理:关于运算的结合律、单位元存在性、逆元存在性.对于集合中的元素是什么,上面定义的运算是如何定义的,我们毫不关心.这种处理问题的方式(即只关心规则,而不关心所研究的对象是什么)是我们学习抽象代数必须具备的认知上的飞跃,也是学习抽象代数的心理基础.当然,为了让学生对群有一个直观的感觉,我们通常会举出一些熟悉的例子,如整数群等.但这往往也会造成一些误导:因为这些我们比较熟知的群并不具备一般群的特点(可能具备群的某些特点).例如,整数群为可交换群,也为无限循环群.因此,我们必须给出更多的不为人们所熟知的群的例子,用以概括群的特性.但并非所有的抽象代数中的概念都有对应的熟知的例子供人们参考.这是抽象代数教学的一大难点.在这一点上,公理方法给了我们极大的帮助.你不需要了解张量积到底是什么,而只需要找到它的运算规则,来刻画它的具体行为.公理体系的主要优势就在于:你不需要了解你所研究的具体事物(这使得理论的适用性更加广泛),而只需要了解这些事物所遵循的规律.这也是我们传统哲学的研究方法:关心自然规律的演变发展.

1.1.3　焦点是什么

那么这种新的数学思维模式又是怎样产生的呢?事实上,这一切变化都是逐渐、悄悄发生的,且是如此的自然.事情开始于19世纪早期,当时的数学家们开始关注于一种新的事物,它与代数有关,但并非方程求解中的代数,尽管在当时代数方程的求解确实是数学家们的主要兴趣之一.这里的代数是指一种代数结构,类似于我们现在的近世代数教科书上所说的代数概念.它类似于我们熟知的有理数域、实数域、复数域,以及后来诞生的四元素域、各种代数数环、矩阵环(由Sylvester和Cayley创造)和逻辑代数(由Boole发明)等.此外,为了研究代数方程的解集,Legendre, Abel, 和Galois等人从结构上开始了对置换群的研究.所有这些概念以及体系的诞生都是那样的自然,且都是为了解决或研究几何、分析、数论和方程理论中的某些实际问题而诞生的.新的数学思维的诞生是因为人们不再考虑每一个不同代数结构上的运算,而是把这些不同的代数结构视为一个整体,然后考虑它们这些不同结构的共性.这一点从Legendre, Abel和Galois等人在置换群上的研究工作上可以看出.他们考虑的是置换群的子群集,而不是每一个单个的置换.

最后我们指出近世代数发展的三个主流方向. 这是由 Bourbaki 指出的:

1. 代数数论,由 Gauss, Dedekind, Kronecker, 和 Hilbert 等人创立.

2. 置换群理论(以及后来的几何变换群),由 Galois 和 Abel 创立.

3. 线性代数和代数系统(又称为超复系统).

我们必须指出,尽管有限群已经被人们彻底刻画,但群论毕竟是一切代数理论的基础. 因此我们说:在群论部分,无论你花费多少时间也不为过.

§1.2 初等数论

我们通常把集合 $\{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$ 称为整数集,并记为 Z.

1.2.1 定义

一个整数 a 称为整数 b 的倍数,如果存在整数 q,使得 $a = bq$. 此时,我们称 b 为 a 的一个因子,记为 $b \mid a$. 有时也称 a 可以被 b 整除(或 b 可以整除 a). 整数 a 的所有倍数构成的集合记为 aZ,即 $aZ = \{m \in Z : m = aq, \exists q \in Z\}$.

1.2.2 公理

[良序公理] 每一个非空自然数集都含有一个最小元.

1.2.3 定理

[除法法则] 对任意给定的整数 a 和 b,其中 $b \neq 0$,有唯一的整数 q(商)和 r(余数),使得 $a = bq + r$,其中 $0 \leqslant r < b$.

1.2.4 定理

设 I 为一个非空整数集合,I 在加法与减法运算下封闭. 则 I 或者只含有零元,或者 I 含有一个最小正整数 r,且 r 的所有倍数都在内.

1.2.5 定义

一个正整数 d 称为非零整数 a 和 b 的最大公因子,如果它满足

(i) d 为 a 和 b 的因子;且

(ii) a 和 b 的任意一个(公)因子均为 d 的因子.

我们记 $gcd(a,b)$ 或 (a,b) 为 a 和 b 的最大公因子.

1.2.6　定理

任意非零整数 a 和 b 都有最大公因子 d，且 d 为 a 和 b 的线性组合数中最小的正整数. 进一步，一个整数 p 为 a 和 b 的一个线性组合当且仅当它为 d 的倍数.

两个整数的最大公因子可以通过欧几里得算法(Euclidean algorithm) 求得. 首先注意到，如 $a \neq 0, b \mid a$，那么 $gcd(a,b) = |b|$. 进一步，若 $a = bq + r$，则 $(a,b) = (b,r)$. 因此，若给定正整数 $a > b > 0$，则连续使用除法法则，可得

$$a = bq_1 + r_1, \quad 0 < r_1 < b$$

$$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$\cdots.$$

由于余数变得越来越小，经过有限步(譬如 $n+1$ 步) 后，必有 $r_{n+1} = 0$. 因此有 $gcd(a,b) = gcd(b,r_1) = \cdots = r_n$.

1.2.7　定义

非零整数 a 和 b 称为互素的，若有 $(a,b) = 1$.

1.2.8　性质

设 a,b 为非零整数. 则 $(a,b) = 1$ 当且仅当存在整数 m 和 n，使得

$$ma + nb = 1.$$

1.2.9　性质

设 a,b,c 均为整数.

(a) 若 $b \mid ac$，则 $b \mid (a,b)c$.

(b) 若 $b \mid ac$ 且 $(a,b) = 1$，则 $b \mid c$.

(c) 若 $b \mid a$，$c \mid a$，且 $(b,c) = 1$，则 $bc \mid a$.

(d) $(a,bc) = 1$ 当且仅当 $(a,b) = 1, (a,c) = 1$.

1.2.10　定义

一个整数 $p > 1$ 称为素数，如果它的因子只有 1 和自身. 整数 $a > 1$ 被称为合数，如果它不是一个素数.

1.2.11 引理

[Euclid] 整数 $p>1$ 为一个素数当且仅当它满足以下性质：

$$\forall a,b,p \mid ab \Rightarrow p \mid a, \text{或 } p \mid b.$$

1.2.12 定理

[算术基本定理] 任何一个整数 $a>1$ 均可以唯一的分解成素数积的形式，即

$$a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

其中 $p_1, p_2, \cdots, p_r$ 和指数 $m_1, m_2, \cdots, m_r$ 均为正整数.

1.2.13 定理

[Euclid] 存在有无穷多个素数.

1.2.14 定义

一个正整数 m 称为整数 a 和 b 的最小公倍数，如果
(i) m 为 a 和 b 的倍数，且
(ii) a 和 b 的任意一个倍数均为 m 的倍数.
我们记 $lcm[a,b]$ 为 a 和 b 的最小公倍数.

1.2.15 性质

设 a,b 为两个正整数，且有以下素数分解

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}.$$

其中 a_i 和 b_i 均为非负整数. 对任意 i，我们记

$$d_i = \min\{a_i, b_i\}, m_i = \max\{a_i, b_i\}.$$

则有以下分解

(a) $\gcd(a,b) = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$；

(b) $\text{lcm}[a,b] = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$.

1.2.16　定义

设 n 为一个正整数. 整数 a 和 b 称为模 n 同余，如果它们被 n 除后的余数相同，并记

$$a \equiv b(\bmod n).$$

1.2.17　性质

设 a,b 和 $n>0$ 均为整数. 则

$$a \equiv b \pmod{n} \text{ 当且仅当 } \quad n \mid (a-b).$$

1.2.18　性质

设 n 为一个正整数. 则对任意整数 a,b,c,d，有：

(a) 若 $a \equiv c \pmod{n}$，$b \equiv d \pmod{n}$，则

$a+b \equiv c+d \pmod{n}$，　$ab \equiv cd \pmod{n}$.

(b) 若 $a+c \equiv a+d \pmod{n}$，则 $c \equiv d \pmod{n}$.

若 $ac \equiv ad \pmod{n}$，且 $(a,n)=1$，则 $c \equiv d \pmod{n}$.

1.2.19　性质

设 a 和 $n>1$ 为两个整数. 则存在整数 b 使得 $ab \equiv 1 \pmod{n}$ 当且仅当 $(a,n)=1$.

1.2.20　定理

同余方程

$$ax \equiv b \pmod{n} \tag{1.1}$$

有解当且仅当 b 能被 d 整除，其中 $d=(a,n)$. 反之，若 $d \mid b$，则(1.1)有 d 个不同的解(mod n)，且这些解模 n/d 同余.

1.2.21　定理

[中国剩余定理] 设 n 和 m 为两个互素的正整数，即 $(n,m)=1$. 则同余方程组

$$x \equiv a \pmod{n}, x \equiv b \pmod{m}$$