研 究 生 数 学 丛 书 5
Mathematics Series for Graduate Students

抽象代数基础

Basic Algebra

李克正 著
Li Kezheng

清华大学出版社
Springer

研 究 生 数 学 丛 书 5
Mathematics Series for Graduate Students

0153
37
2007

抽象代数基础

Basic Algebra

李克正 著
Li Kezheng

清华大学出版社
北京

Springer

内 容 简 介

本书的主要内容为群论、环论基础、域上的线性代数、域论和伽罗瓦理论。对于抽象的概念，本书力求通过阐述其与分析、几何、物理和其他应用学科的联系以及通过大量具体直观的例子，使读者对抽象代数能有较深入的理解。书中有充足的习题，并对其中较难的习题给出了参考解答。阅读本书所需要的预备知识仅为大学微积分和线性代数。

本书是抽象代数的基础教材，适于作为数学专业研究生基础课教学或自学的教科书，也可供其他相关专业的学生、研究者以及大学本科教学用作参考书。

版权所有，侵权必究。侵权举报电话：010-62782989　13501256678　13801310933

图书在版编目（CIP）数据

抽象代数基础 = Basic Algebra/李克正著. —北京：清华大学出版社，2007.4
(研究生数学丛书)
ISBN 978-7-302-14407-6

Ⅰ. 抽… Ⅱ. 李… Ⅲ. 抽象代数–研究生–教材–英文 Ⅳ. O153

中国版本图书馆 CIP 数据核字(2006)第 162451 号

责任编辑：陈朝辉
责任校对：焦丽丽
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市兴旺装订有限公司
经　　销：全国新华书店
开　　本：170×230　**印　张**：13　**字　数**：259 千字
版　　次：2007 年 4 月第 1 版　　**印　　次**：2007 年 4 月第1 次印刷
印　　数：1～3000
定　　价：29.80 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：023863-01

编审委员会

主　编：李大潜

副主编：冯克勤

编　委：（姓氏按拼音字母排序）

程崇庆　陈木法　陈叔平　陈志杰

李克正　李　忠　邵嘉裕　王维克

文志英　肖　杰　袁亚湘　周　青

张伟平

1. 连续介质力学中的数学模型
(Mathematical Modeling in Continuum Mechanics)

2. 应用密码学
(Applied Cryptography)

3. Introduction to Malliavin Calculus
(Malliavin 随机变分引论)

4. 纠错码的代数理论
(Algebraic Theory of Error-Correcting Codes)

5. 抽象代数基础
(Basic Algebra)

6. Algebraic Geometry
(代数几何)

7. 反问题
(Inverse Problem)

8. 泛函分析——理论和应用
(Analyse Fonctionnelle —— Théorie et applications)

9. 素数论
(Les nombres premiers)

此为试读,需要完整PDF请访问: www.ertongbook.com

总　序

数学是一门在非常广泛的意义下研究自然和社会现象中的数量关系和空间形式的科学。长期以来，在人们认识世界和改造世界的过程中，数学作为一种精确的语言和一个有力的工具一直发挥着重要的作用。在现代，数学科学已构成包括纯粹数学及应用数学内涵的众多分支学科和许多新兴交叉学科的庞大的科学体系。作为各门科学的重要基础，作为“四化”建设的重要武器，作为人类文明的重要支柱，数学科学在很多重要的领域中已起着关键性甚至决定性的作用，数学技术已成为高技术的突出标志和重要组成部分。数学的影响和作用已深入到各行各业，可以说无处不在。马克思当年的预言：“一门科学只有当它成功地运用了数学之后，才算达到了真正完善的地步”，正在不断得到证实。在这样的背景下，数学科学的重要性已得到空前广泛的认同。在研究生（不限于数学专业的研究生）的培养中，重视数学基础的训练，强调数学思想的熏陶，也已成为一种必然的趋势。但是，国内研究生数学教材及参考读物的实际情况，无论从品种、数量及质量各方面来看，都远远不能适应这个形势，甚至也远远落后于本科生的数学教材。这已成为制约提高研究生培养质量的一个重要瓶颈。清华大学出版社和施普林格出版社(Springer-Verlag)合作，倡议出版这一套《研究生数学丛书》(Mathematics Series for Graduate Students)，可望改善这方面的状况，为我国的研究生打好数学基础、提高数学素质起到积极的作用。

根据数学这门科学的特点，同时考虑到研究生学习数学的基本要求和特有方式，这套以面向研究生（包括高年级本科生、硕士及博士研究生）的数学教材或参考读物，将力求体现以下的一些原则：

- 主题具有理论或（和）应用方面的重要性；
- 在重点介绍基础性内容的前提下，兼顾学科前沿的重要发展趋势和研究成果；
- 在讲授数学内容的同时，充分体现数学的思想方法和精神实质；
- 少而精，在较小的篇幅中展现基本的内容；

- 有相当好的可读性，适宜读者自学；
- 附有习题、思考题及参考资料目录，书末有索引，方便读者深入学习与思考。

为了有利于体现这些原则，本丛书将采取相当灵活的体例及风格：内容可以是纯粹数学、应用数学或数学与其他学科的交叉；可以是较系统地介绍某一个分支的教材，或是介绍某一前沿分支状况的综述，也可以是课外参考书；可以是原著，也可以是译著；可以是国内作者，也可以是国外作者；可以用中文编写，也可以用英文编写，等等。

要实现本丛书的目标和宗旨，任重而道远，但千里之行，始于足下。在学界同仁和广大读者的支持和帮助下，让我们共同努力。

李大潜

2003 年 9 月于上海

前　言

抽象代数是数学和其他一些相关专业的一门研究生基础课程。这方面的教材和参考书甚为丰富，一般在教学中是同时参考几本书，或以一本为主。但近年来，由于研究生对教材的需求，作者觉得写一本新的教材是有意义的，目的是根据我国大学本科毕业生目前的情况，提供一本内容仅包括抽象代数初步理论的研究生教科书，以方便学生的学习和参考，并力求在一学期的教学时间中，可在代数方面为进一步学习打下较坚实的基础。这一想法得到多位专家的支持。

抽象代数可以说是开创于 19 世纪末到 20 世纪初的德国学派，100 余年来有了很大的发展，有些好的代数学教科书（如[15]）包含了这方面的丰富内容，但这样的书势必内容庞大。很多专家（例如曾肯成先生）认为，一本旨在用于一学期教程的教科书，内容应包括群论、环与模的初等理论、域论和伽罗华理论，作者完全赞同这样的看法。大体上看，这样的安排是从群论开始，经过一些必由之路，最终回到群论的历史来源和最主要应用之一 —— 伽罗瓦理论。完成了这样一个（黑格尔所谓的）“逻辑的圆周”，读者将能理解代数中的一些哲学思想，体验到其中的奥妙，从而获得深刻的印象。这些内容基本上属于早期的抽象代数的范围，而本书在有限的篇幅下，适当地反映了一些代数学的近代发展。

抽象代数的一个基本特点是“抽象”。对于相当一部分读者，如何适应抽象的语言并理解其中的深刻思想，是开始学习时的一个难点。抽象的概念需要具体地理解，例如对于群的概念，尽管定义很简单，但只有在接触了多种多样的群，看到群与数、代数方程、线性代数、几何、微分等很多方面的联系以及多方面的应用，特别是理解了表示以后，才能深刻地理解群的意义及其重要性。在这方面，作者近年来看到两种不良倾向：一种是“从抽象到抽象”，就是从一些抽象的定义出发，一味作抽象的逻辑推导，不管这些定义和推导出的命题有什么背景或应用。另一种是把一些本质上是新的概念完全纳入自己原有的知识体系，例如把群列表表达，甚至把用乘法表计算当做研究群的唯一方法。这两种倾向都会阻碍从具体到抽象的认识过程。

作者曾在芝加哥大学、南开大学等学校讲授本科代数课程，此后又曾在中国科学院研究生院多次讲授抽象代数课程。本书是在多年积累的讲义的基础上，进行改写和补充而成书。在写作过程中，一个较大的改动是将线性代数专门辟为一章。值

得说明的一点是，在国外的数学专业代数教材中，很多是先讲抽象代数再讲线性代数，这样在逻辑上比较“顺”，可以把线性代数建立在一般域上；但这种讲法有一个缺点，就是与从具体到抽象的认识过程不一致。本书则是假定读者已学过高等代数教程，在线性代数这一章说明如何将线性代数的方法和结果推广到一般的体或域上，此外加入张量、线性群、结式等在高等代数教程中不一定包含的内容，并初步介绍了线性表示。

除引言外，正文共有 5 章，内容是这样安排的：第 1 章为群论，包括群的概念、同态与同构、表示的概念、交错群的单性、有限生成阿贝尔群的结构、同构定理与分解定理、西罗子群等，并对群论的历史发展和应用作了一个简单的回顾；第 2 章为环论初步，包括环的概念、同态与理想、模、多项式环等；第 3 章为线性代数，包括线性空间、多重线性代数、线性变换群、矩阵的标准形、结式等，并对线性表示作了初步介绍；第 4 章为域论，包括素体、域扩张、代数扩张的构造、单位根、伽罗瓦域、本原元素定理、无限域扩张等；第 5 章为伽罗瓦理论，包括伽罗瓦群、正规扩张、伽罗瓦扩张、伽罗瓦理论的基本定理、伽罗瓦理论的经典应用、范数与迹等。此外有三个附录：附录 A 是为了读者的方便，将集合论中有关选择公理的一些内容列出；附录 B 简单介绍了一般体或域上的射影几何，这些背景知识对于理解线性群是必要的；正文每节后附有若干习题，其中带有星号的习题在附录 C 中给出参考解答（之所以称为“参考解答”是希望读者先尽可能尝试自己解答，而且读者也可能给出与书中不同的解答方法）。

本书中的数学用语均参照全国自然科学名词审定委员会 1993 年公布的《数学名词》。对《数学名词》中未收入的词语一般采用一些暂定译名。

作者希望借此机会感谢与本丛书有关的专家们对本书出版的支持，感谢众多同事和学生对本书提出的宝贵意见和建议。

李克正

目　录

抽象代数基础

此为试读,需要完整PDF请访问: www.ertongbook.com

0 引 言

代数学是一个有悠久历史的数学分支。在 19 世纪后期, 德国学派在代数学中系统地建立了一套抽象的语言和方法, 从根本上影响了此后代数学的发展。在 20 世纪中, 这些抽象的语言和方法逐渐被代数领域甚至更广的领域普遍接受。在今天, 至少在数学领域, "代数" 和 "抽象代数" 这两个术语实际上已是同一个意义。

按照 Dieudonné 的观点, 代数学是由代数数论和代数几何两个方面激发的。这是一种通过观察人类文明史而提出的哲学观点, 并非仅指现代代数学 (如同另一些学者指出的, 现代代数学还受到一些其他方面的激发, 例如代数拓扑就起了极其重要的影响)。我们简单地回顾一下代数学的发展史, 就不难理解这些哲学观点。

代数方程 (即多项式方程) 是代数学的一个古老的研究课题, 有广泛的应用背景。而丢番都 (Diophantus) 方程 (即代数方程的整数解问题) 则是代数数论的古老的研究课题。代数方程的研究使代数学逐渐成为一个独立的数学分支。自从 17 世纪 30 年代费马 (Fermat) 和笛卡儿 (Descartes) 建立直角坐标系, 产生了解析几何, 将代数与几何联系了起来, 代数几何就从此发源。从 17 世纪到 19 世纪是代数学蓬勃发展的时期, 研究的对象有代数运算、多项式、线性代数等, 主要还是围绕着代数方程及其应用。

1830 年前后, 伽罗瓦和阿贝尔在代数方程的解的研究中发现了一类新的数学对象 —— 群。伽罗瓦巧妙地把代数方程的可解性问题化为群论的问题, 证明了 5 次以上的方程没有一般的解法 (5 次方程的情形是阿贝尔解决的)。这一工作显示出群论的强大威力。此后人们逐渐认识到群是一种普遍的的存在, 而且又是一种强有力的工具。因此群逐渐成为数学中最重要的基本概念之一, 对此后的数学以至其他科学产生了深远的影响。19 世纪中期, 黎曼所开创的黎曼曲面的研究, 是数学的又一基本课题, 它与分析、代数、几何和数论都有密切的联系。

在这一时期, 代数数论也有很大的发展, 如 Kummer 在研究费马大定理时产生了“理想数” (现在称为理想) 的概念。在 19 世纪后期, 索弗斯 · 李将群论的思想用于研究微分方程, 产生了李群的概念, 而李代数则是代数学的一个新研究课题。

19 世纪后期到 20 世纪初期, 德国学派 (代表人物有阿廷、诺特、希尔伯特等) 将代数学中的基本概念推广, 形成抽象概念如群、环、同态等, 这样也有了很多新的研究课题, 如特征 p 的几何或数论。抽象的语言至少有下面几个好处: 一是有了一套统一高效的语言, 有利于抓住问题的关键; 二是隐含着不同课题之间的类比, 从而对新的研究思路有激励作用; 三是用抽象的眼光观察一些具体的研究对象, 可以理解其在更宽广的领域中的意义。此后, 代数学中的抽象语言逐渐被普遍接受, 以致今天很多作者不再用 “抽象代数” 这个术语而直接称之为 “代数学”。

然而, 抽象的语言也是有缺点的。一个重要的缺点是往往将具体的背景掩埋在抽象的、形式的或 “一般情形” 的定义中, 即使不了解这些背景, 仍可以从这些定义出发推导出很多命题; 但如果完全不顾背景地研究下去, 很难保证会得到有价值的结果, 在极端的情形甚至会成为 “纯粹形式逻辑”。因此, 许多专家都非常强调在代数的学习和研究中随时注意问题的背景。

20 世纪 20 年代以后, 拓扑学逐渐对代数学有了重要影响。起初人们发现, 拓扑学中的同调用群论的语言表述很合适, 这刺激了阿贝尔群的研究, 后来基础群的研究又刺激了自由群的研究。更重要的是同调代数的产生, 它将拓扑学中同调的方法推广到其他领域 (包括几何、代数、数论等), 而且在逻辑上将抽象代数从集合的层次提高到 “范畴” 的层次。

除了代数数论、代数几何和代数拓扑以外, 在 20 世纪对代数学有重要影响的学科还有物理学、组合学、信息科学和其他一些应用学科。代数学本身也有一些经典的研究课题, 如有限单群的分类。

代数学的基本研究对象是有限运算 (即仅涉及有限多个对象的运算), 特别是二元运算 (即两个对象的运算, 例如加、减、乘、除都是二元运算)。与此对照, 在分析中研究的极限则不是有限运算。现代代数学研究的课题很多, 具体地说, 有:

i) 群与半群, 二者都是带有一种二元运算的集合, 但它们的背景很不相同: 群的基本背景是变换, 可以理解为物理意义下的运动; 而半群的基本背景是自同态 (集合到自身的映射)。

ii) 环, 是带有两种二元运算 (一般称为 “加法” 和 “乘法”) 的集合。两种二元运算由 “乘法分配律” 联系在一起。交换环的背景主要是数和函数; 结合环的基本背景是矩阵、微分算子等; 而非结合环 (如李代数、八元数、克利福德代数等) 则各有不同的背景。与环密切联系的一个研究对象是模。

iii) 域论和伽罗瓦理论, 这是最重要的经典课题, 也是现代数学的一类最重要的工具。

iv) 线性代数是一个经典的分支, 但从抽象代数的观点可以拓宽其研究范围, 即研究一般域上的线性代数, 其背景有分析、数论、几何、组合学、计算数学、代数学的若干其他分支以及物理学、化学、计算机科学、信息科学等应用领域。

v) 双线性及多重线性代数 (张量积等), 这是一个不可缺少的基本工具。

vi) 同调代数, 它将拓扑学的方法应用到其他学科以寻求各种 "不变量", 而不变量在各学科中都是分类学的基础。在各学科中建立了很多种同调, 一个很深入的研究方向是 K-理论, 它在拓扑、代数、数论、微分几何等学科都有重要的应用。另一方面, 在建立一般的同调方法中, 形成了 "范畴" 的语言, 而以往在抽象代数中用的是集合论的语言, 可以说范畴比集合更抽象。

vii) 在群、环、模等代数对象的研究中, 表示是一个根本的方法, 在很多课题中也是主要的研究对象; 而对表示的长期深入的研究, 使表示论逐渐成为一个分支, 而且是数学最强有力的工具之一。

viii) 线性代数群虽属于群论的范围, 但已形成一个独立的分支。

(上面并未列出所有的方向。)

代数学有非常广泛的应用领域, 其中有的学科通常划入代数学的范围, 如代数组合论, 编码和密码学, 数学物理中的代数对象 (如卡茨 - 穆迪代数、量子群等), 数学机械化等。

代数学与拓扑学、微分几何、数论、代数几何、李群、泛函分析、计算数学、应用数学等许多数学学科, 物理学、化学、计算机科学、系统科学、信息科学等其他学科以及很多应用领域有密切联系。

在今天, 由于代数学的内容非常广泛, 在一本教科书中已无法作全面的介绍, 在一个基础教程中更是只能选择几个课题。在本书中仅涉及群论、交换环与模的初等理论、域论和伽罗瓦理论。这些内容基本上都是 "经典的", 很多是 20 世纪初甚至更早的, 在今天已相当成熟, 而这些内容对于抽象代数的初步学习都是基本的和必需的。在内容的处理上, 本书在有些地方采用了一些较近代的观点, 并介绍了一些应用。

1 群　论

1 群

在几何中经常会遇到对称的图形. 所谓对称性, 就是图形经过某种运动后能和自身重合. 我们来看几个例子.

例 1.1　平面上的一个正 n 边形 (如图 1.1 中的正六边形) 绕中心旋转角 $\frac{2\pi}{n}$ 的整数倍可与自身重合, 且有 n 条对称轴 (如图 1.1 中的虚线所示). 正多边形对这些对称轴反射后也与自身重合 (反射也可以看作在空间中的翻转). 不难看出, 如果先作一次旋转再作一次反射, 其结果相当于对另一个对称轴作一次反射; 而若对两条对称轴依次作反射, 其结果相当于一个旋转, 而旋转的角度与两个反射的先后次序有关.

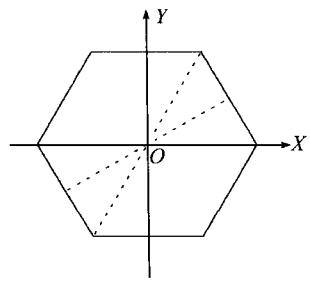

图　1.1

例 1.2　一个正方体 (见图 1.2) 有多个旋转对称轴, 两个相对面中心的连线是一条四次对称轴 $\left(\text{即绕此轴旋转 } \frac{2\pi}{4} \text{ 可与自身重合}\right)$, 而两个相对顶点的连线是一条三次对称轴 $\left(\text{即绕此轴旋转 } \frac{2\pi}{3} \text{ 可与自身重合}\right.$, 如图 1.2 中的短长虚

线所示)。此外正方体的中心是一个对称中心,还有一些反射对称面等。不难验证,如果先后绕一条三次对称轴和一条四次对称轴作旋转,其结果相当于另一个旋转,其旋转轴和旋转的角度都与所作的两个旋转的先后次序有关。由这个例子可见对称性可能是很复杂的。

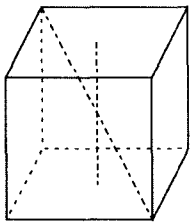

图 1.2

例 1.3 图 1.3 是由边长为 1 的正三角形的顶点铺成的点阵,称为一个"格"。这个格沿 X 轴方向平移 1 单位可与自身重合,绕原点 O 旋转 $\frac{\pi}{3}$ 也可与自身重合。与例 1.1 和例 1.2 不同的一点是,有无限多种运动能使格移到与自身重合的位置。

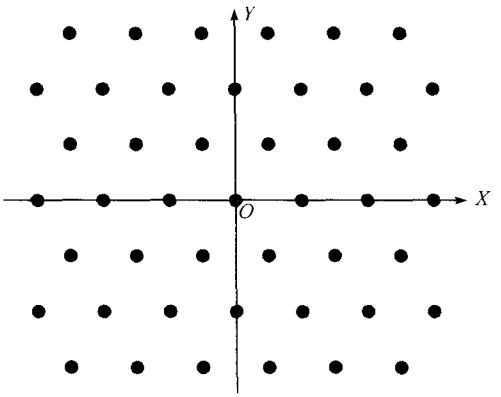

图 1.3

对称性在数论、拓扑、分析、代数等很多其他数学领域也可以遇到,而且在物理、化学等学科以及很多应用领域也经常遇到。实际上,对称性在自然界中普遍存在,而且是研究自然界的一个极为重要的着眼点。

研究对称性的根本工具是群论。我们先给出群的一般定义,然后再详细解释。

定义 1.1 一个群是一个集合 G 带有一个"二元运算",即一个映射 $G\times G\to$

G (称为*乘法*, $(a,b)\in G\times G$ 在此映射下的像记作 $a\cdot b$ 或 ab, 称为 a 与 b 的*积*), 满足条件:

i) $(ab)c=a(bc)$ 对任意 $a,b,c\in G$ 成立 (这称为 "乘法结合律");

ii) 存在 (唯一的) $e=e_G\in G$ 使得 $ae=ea=a$ 对任意 $a\in G$ 成立 (e 称作*单位元*);

iii) 对任意 $a\in G$, 存在 (唯一的) $b\in G$ 使得 $ab=ba=e$ (b 称作 a 的*逆元*, 记 $b=a^{-1}$)。

群 G 称为*交换群*或*阿贝尔群*, 如果除上述三个条外还有

iv) $ab=ba$ 对任意 $a,b\in G$ 成立。

(对任两个元 $a,b\in G$, 若 $ab=ba$, 则称 a 与 b *交换*, 条件 iv) 就是说 G 的任意两个元交换。)

上面的定义来源于多方面的背景, 是从多种相距甚远的不同情形中抽象出来的, 因此需要通过多方面的具体情形来理解。我们先举几个例子, 并解释例 1.1~ 例 1.3 中的图形与群的关系。在以下几节将看到更多的例子。

例 1.4 所有非零有理数的集合 $\mathbb{Q}^*$ 是一个以乘法为二元运算的群。类似地, 所有非零实数的集合 $\mathbb{R}^*$ 和所有非零复数的集合$\mathbb{C}^*$ 也是以乘法为二元运算的群。此外, 所有正有理数的集合 $\mathbb{Q}_{>0}$ 也是一个以乘法为二元运算的群。

注意在例 1.4 中, $\mathbb{Q}^*$ 是 $\mathbb{R}^*$ 的子集, 而且二者的群运算是一致的, 我们说 $\mathbb{Q}^*$ 是 $\mathbb{R}^*$ 的 "子群"。一般地, 如果 G 是一个群, H 是 G 的子集, 且按 G 的乘法运算组成一个群, 则称 H 为 G 的*子群*。

引理 1.1 设 G 为群, H 为 G 的子集, 则 H 为 G 的子群当且仅当下列条件成立:

i) 若 $a,b\in H$ 则 $ab\in H$;

ii) $e\in H$;

iii) 对任意 $a\in H$ 有 $a^{-1}\in H$。

证明很简单, 留给读者作为习题 (习题 1.8)。

在例 1.4 中, $\mathbb{Q}^*$, $\mathbb{R}^*$ 和 $\mathbb{Q}_{>0}$ 都是 $\mathbb{C}^*$ 的子群。对任意群 G, 一元子集 $\{e\}$ 和 G 本身都是 G 的子群。我们将只有一个元的群称为*零群*, 故称 $\{e\}$ 为 G 的*零子群*。

例 1.5 所有整数的集合 $\mathbb{Z}$ 是一个以加法为二元运算的群, 对此我们将定义中的 "乘法" 改称为 "加法", 而称 $\mathbb{Z}$ 为 "加法群"。类似地, 所有有理数的集合

此为试读,需要完整PDF请访问: www.ertongbook.com