中国科学技术大学数学丛书

代数学 I

代 数 学 基 础

欧阳毅
申伊塽 编

高等教育出版社

中国科学技术大学数学丛书

代数学 I

代数学基础

欧阳毅
申伊塊 编

高等教育出版社·北京

内容简介

本书是中国科学技术大学代数系列教材三部曲的第一部，是“代数学基础”课程参考教材。本书对群、环、域的定义和基本性质，循环群和对称群（置换群），整数理论，域和整数上的多项式理论等进行介绍，目的是为后续的线性代数、近世代数和数论（包括数论的应用）等众多课程提供基础。本书在保留中国科学技术大学初等数论课程传统内容的基础上，增加了复数、韦达定理等高中忽视的内容，强调了等价关系这个大学数学教学难点，增加了群、环、域的基础知识特别是循环群的知识，对线性代数教学急需的置换的概念进行讨论。这样编写的目的，首先是让学生较早接触到群、环、域等抽象概念，尽早锻炼学生的抽象思维能力，为后续的近世代数课程降低难度。其次本书统一使用代数的思想介绍整数和多项式的理论，希望同学们能够了解初等数论不是数学竞赛中高不可攀的一道道难题，而是在统一逻辑框架下的优美理论，它不仅在今后数学各方面学习中有很多用处，而且是数学在实际生活中应用的重要理论基石。

本书可以作为“初等数论”和“近世代数”（或“抽象代数”）课程的参考书籍。本书适用于高等院校数学和信息安全专业学生，以及其他对代数思想和方法感兴趣的学生和学者。

图书在版编目（CIP）数据

代数学．Ⅰ，代数学基础 / 欧阳毅，申伊塊编．--
北京：高等教育出版社，2016.8
（中国科学技术大学数学丛书）
ISBN 978-7-04-045949-4

Ⅰ.①代… Ⅱ.①欧… ②申… Ⅲ.①代数－高等学校－教材 Ⅳ.①O15

中国版本图书馆 CIP 数据核字（2016）第 170604 号

策划编辑	杨 波	责任编辑	杨 波	封面设计 王 鹏	版式设计 马 云
插图绘制	黄建英	责任校对	陈旭颖	责任印制 耿 轩	

出版发行	高等教育出版社	网 址	http://www.hep.edu.cn
社 址	北京市西城区德外大街4号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.hepmall.com.cn
印 刷	廊坊市科通印业有限公司		http://www.hepmall.com
开 本	787mm×960mm 1/16		http://www.hepmall.cn
印 张	9.25		
字 数	160 千字	版 次	2016年 8 月第 1 版
购书热线	010-58581118	印 次	2016年 8 月第 1 次印刷
咨询电话	400-810-0598	定 价	15.20 元

物 料 号 45949-00

“中国科学技术大学数学丛书”

编审委员会

“中国科学技术大学数学丛书”

总　序

建设世界一流大学的一个首要目标是培养世界一流的学生，一直以来中国科学技术大学（以下简称科大）都把实现这一目标作为我们的崇高使命。教材建设是教书育人的重要方面。为培养适合于现代科技发展的优秀人才，就需要有既尊重教学规律又面向科学前沿的一流教材。本套丛书是我们为中国科学技术大学数学科学学院学生，特别是华罗庚科技英才班学生准备的教材。

本套丛书凝聚科大数学系（学院）数代科大人的心血。华罗庚、关肇直、吴文俊诸先生在科大创校之初教导58级、59级、60级学生（即著名的华龙、关龙和吴龙）之时，就十分重视教材建设。华罗庚先生编著的《高等数学引论》是高水平数学教材的不朽名著，值得当今每位高等数学教育工作者学习和借鉴。在大师引领之下，科大数学系前辈出版了许多带有鲜明科大特色并受到国内外同行高度认可的教材，比如陈希孺先生的《数理统计学教程》，龚昇先生的《简明微积分》，常庚哲、史济怀先生的《数学分析》，冯克勤等教授的《近世代数引论》，李尚志教授的《线性代数》等。这些教材至今广为使用，为科大带来了崇高声誉。我们这套丛书，就是在科大前辈教材基础上编写而成的。

新世纪以来，特别是2009年华罗庚科技英才班创建以来，由于学生基础、兴趣和爱好有所变化，前沿数学发展日新月异，为更好实践数学优秀人才的培养，数学科学学院对数学核心课程教学内容和方式进行调整。为配合这一调整，我们组织教学和科研第一线老师编写了这套教材。

教材建设是为教学服务的。一部好的教材将给学生打开一扇大门，引领学生翱翔科学知识的海洋，而坏的教材，则往往粗制滥造，错误极多，非但没有教书育人的作用，而常常有误人子弟的后果。基于此，我们在教材建设上是战战兢兢，如履薄冰，不敢有丝毫马虎。我们的教学内容，经学院全体教授反复讨论达两年时间。编写讲义之时，大量参考了之前的科大教材，甚至直接征询前辈老师的意见。讲义编写好之后，也几经试用，反复修改增删，接受老师同学的批评建议，历经数年方成书出版。即使如此，教材一定还有不足之处，祈望读者诸君不

吝指出，以便我们提高。

古人有云：“百年之计，莫如树人”。我们希望这套丛书能为培养中国数学拔尖人才略尽绵薄之力，希望中国数学之树“亭亭如盖”。

马志明

2015 年 9 月

序

近世代数（或叫抽象代数）研究群、环、域和模等各种代数结构。它不仅是一个基本的数学分支，而且也是物理学、化学和力学等其他科学的重要数学工具。20 世纪 50 年代以来由于数字通信和数字计算技术的飞速发展，近世代数在信息科学和计算机科学也发挥愈来愈大的作用。更广一点来说，近世代数中所体现的数学思维方式（共性和个性，比较和分类，局部和整体 ……）对于人们从事任何社会活动都是有益的。

中国科学技术大学 1958 年建校以来，数学系一向重视近世代数的教学。20 世纪 60 年代，老一辈数学家华罗庚、万哲先、王元和曾肯成培养了不少从事代数教学、研究和应用领域的人才。我本人有幸聆听过王元的“数论导引”，万哲先和曾肯成的“抽象代数”（用 van der Waerden 的《代数学》一书），华罗庚和万哲先的“典型群”以及吴文俊先生的“代数几何”课。我们不仅学到了知识，更重要的是受到他们对学问的理解方式和研究经验的感染。他们风格各异的讲授方式对于年轻学生成长的影响是至关重要的，是由所谓量化条件和单一标准约束出来的“名师”无可比拟的。半个世纪以来，科大教师一直努力继承这个传统。20 世纪 80 年代至 90 年代，我和李尚志、查建国、余红兵、章璞等志同道合者在近世代数教学、教材建设和培养人才方面做过一些努力。现在为了适应我国高等教育和数学发展的新形势，科大数学系欧阳毅、叶郁等人对于近世代数的教学做进一步的改革，编写这套新的教材，这是令人高兴的。

教学经验讲以下三点体会：

（1）把初等数论作为近世代数教学的有机组成部分。中国科学技术大学从 20 世纪 70 年代起，一直把初等数论作为本科生一年级的必修课，其目的不仅是传授整数性质和方程整数解方面的基本知识，更不是训练做数论难题，而是把初等数论视为近世代数的一个源头。18 世纪和 19 世纪，伟大数学家欧拉和高斯对于费马关于整数和素数的一系列猜想产生浓厚的兴趣。他们花了不少精力研究整数的性质，得到一系列关于整除性和同余性的重要结果，所创造的一系列深刻的数学思想成为近世代数的源头，而初等数论本身也提供了近世代数中抽象代

数结构的第一批具体例子。整数模 m 的同余类全体 $\mathbb{Z}/m\mathbb{Z}$ 给出有限交换群和交换环的简单例子，中国剩余定理是交换环直和分解的原始模型。模素数 p 的原根 g 就是循环群 $\mathbb{F}_p^\times$ 的生成元，而 $\mathbb{F}_p$ 给出第一批有限域。费马小定理和更一般的欧拉定理在近世代数中推广成有限群的拉格朗日（Lagrange）定理。而高斯的二次互反律在后来的二百年中不断增添新的视野而得到最现代的形式。高斯在研究整数的二平方和问题时，考虑整数的推广（高斯整数），而为了证明任何数域中的代数整数形成环，戴德金（Dedekind）采用了一种新的代数概念，这就是“模”。库默尔（Kummer）在研究费马猜想时发明了“理想数”（ideal number）。后人发现这个概念本质上不是一个数，而是环中的一类十分重要的集合，即环中的理想（ideal）。这些数学家在研究初等数论所产生的深刻数学思想和结果，很值得后人学习和欣赏。

（2）充分讲授域的扩张理论，特别是域扩张的伽罗瓦理论。目前高校的近世代数课程，由于学时所限无法讲授伽罗瓦理论，实在令人惋惜。这不仅是由于这个理论非常漂亮，也因为它为数学发展上一个精彩的例子，表明数学家们为追求数学自身的完善而对人类文明所做的贡献。为了证明 n 次（$n \geqslant 5$）的一般代数方程是根式不可解的，阿贝尔和伽罗瓦考虑此方程所有根之间的置换，由此产生了群的概念，并且揭示出这类方程根式不可解的深层次原因：方程所有 n 个根允许一个最大可能的置换群 S_n，而当 $n \geqslant 5$ 时这个群的结果过于复杂（用现在的语言，S_n 是不可解群）。后来人们逐渐认识到，群是研究各种事物对称性的有力工具。从而群论（特别是群表示理论）在物理、化学、力学等各个领域中均起到重要作用。群的产生和非欧几何等许多思想一样源于数学内部问题的探究，我们不能低估人们追求真理和美对人类文明所起的作用。

（3）增加了传统近世代数课以外的许多内容。相对于分析课程，代数和几何教学在中国高校中非常薄弱，这是一个长期存在的问题，它直接影响我国数学研究的水平。当前的代数组合学研究需要交换代数和群表示理论工具，多复变和微分几何研究要求上同调理论，控制理论需要模论。本世纪初，我和清华大学数学科学系的同人文志英、欧阳毅、姚家燕和印林生等，与法国数学家合作，从一年级初等数论讲起至法国数学家为高年级讲现代代数几何。培养了几届具有现代代数素质的学生。记得我们与 Illusie（Grothendieck 的关门弟子）讨论法国数学家来华前我们需要对清华学生的前期准备时，他说只需要线性代数即可。进一步交换才知，他把群的线性表示，模论（环上的线性代数），以及交换代数中的许多内容均看做是线性代数。我们和法国对于代数学作用和地位在认识上有很大差距。所以，这套教材增加了群表示理论和模论的初步内容，把这些内容看做是大学生应当掌握的知识，是非常必要的。

教学事业其实并不如有些人搞得那么复杂，不需要花样翻新的标语和口号。只需要设计好教学内容，并且有好的老师，坚持至少五年，就会培养出好的学生，因为中国不缺乏勤奋能吃苦的学生。说到根本，只需要老师和学生都有一点精神。老师具有培养学生的热情，而学生要有对数学的热爱和提高数学素质非功利主义的动力。我预祝并且相信，在科大数学系师生共同努力之下，这套教材一定能培养出新一代年青代数学人才。

冯克勤

2015 年 12 月 11 日

于

香港科技大学

前言

代数方法和分析方法是数学研究中两种最基本的方法，也是大学数学专业学生数学教育的重点。中国科学技术大学创校伊始就受到华罗庚、王元、万哲先、曾肯成等前辈数论和代数大家的谆谆教导，代数和数论方面人才辈出。20世纪80年代以来，在冯克勤教授和李尚志教授等领导下，中国科学技术大学的代数教学水平一直维持在较高水平，培养的代数和数论人才受到国内外同行高度称许。科大之所以能够在代数教学方面取得较好成果，一方面原因是学生们受到严格的“线性代数”基础训练；另一方面科大一直坚持为数学系学生开设“初等数论”和“近世代数”基础课程，并在高年级和研究生阶段开设“群表示论”“交换代数”等课程，并配备有《整数与多项式》(冯克勤、余红兵编著)，《近世代数引论》(冯克勤、李尚志、查建国、章璞编著)，《群与代数表示论》(冯克勤、章璞、李尚志编著)等著名教材。

进入新世纪以来，新一代科大学生入学时的数学基础和20世纪八十、九十年代学生有较大区别。这里面一部分原因是高中新课标和高考指挥棒的影响，大部分学生在高中时代受到题海战术的锤炼，但独立探索和抽象思维能力受到压制。他们更早接触到微积分的思想，对于高考中出现的各种题型十分熟练，但在平面几何、因式分解和三角函数等方面的基本训练远不如以前，在数学证明和逻辑严格性方面的训练也不如以前。另一方面，这一代学生或多或少参加过数学竞赛，而其中最体现抽象思维能力的初等数论问题常常是他们最头疼的问题之一。当同学们在大一开始接触“初等数论”课程时，上述两方面的原因就让同学们对于课程学习产生畏难情绪。到大二开始学习“近世代数”课程时，扑面而来的抽象代数思想，特别是群论思想和方法更让不少学生感到无所适从。因此科大的代数教学在前些年受到比较严重的挑战。另一方面，我们的教材没有及时体现新时期学生的最新情况，需要得到及时更新。从教学本身来看，通过多年教学和科研实践，我们发现各代数课程之间的衔接以及对应教材之间衔接不是特别流畅(各数学核心课程的衔接亦是如此)，在统一的框架下对代数课程教学和教材建设进行规划成为必要。

2011 年，在编者的组织下，数学科学学院全体教授对于代数系列课程的教学大纲和教学内容进行了热烈讨论，《代数系列课程纲要》数易其稿，最终得到通过。我们对代数方面涉及的 6 门课程进行全面改革和优化。原来的“初等数论”课程由“代数学基础”课程替代，与“近世代数”“代数学”一起构成代数教学三门核心课程。它们由浅入深，目标是为数学学院学生奠定扎实的代数基础。基于课程改革的需要，我们当即着手对应的教材建设，计划在原来教材的基础上编写代数学三部系列教材：《代数学 I　代数学基础》，《代数学 II　近世代数》和《代数学 III　代数学进阶》。

本书即是代数学系列教材三部曲的第一部。我们在冯克勤教授和余红兵教授编著的教材《整数与多项式》基础上，参照 Artin, Lang, Hungerford, Dummit-Foote 等著名英文教材，对群、环、域的定义和基本性质，循环群和对称群，整数理论，多项式理论等进行介绍，目的是为后续的线性代数，近世代数和数论（包括数论的应用）等众多课程提供基础。我们在保留原来初等数论课程整数理论和多项式理论的基础上，增加了复数、韦达定理等高中忽视的内容，强调了等价关系这个大学数学教学难点，增加了群、环、域的基础知识特别是循环群的知识，对线性代数教学急需的置换的概念进行讨论。这样编写的目的，首先是让学生较早接触到群、环、域等抽象概念，尽早锻炼学生的抽象思维能力，为后续的近世代数课程降低难度。其次我们统一使用代数的思想介绍整数和多项式的理论，希望同学们能够了解初等数论不是数学竞赛中高不可攀的一道道难题，而是在统一逻辑框架下的优美理论，它不仅在今后数学各方面学习中有很多用处，而且是数学在实际生活中应用的重要理论基石。这也是我们将《初等数论》改名为《代数学基础》的原因。

本书分为九章。第一章为预备知识，总结了集合和映射等概念，特别对等价关系进行详细阐述，介绍了复数的基本性质，以及求和与求积符号等内容。此章内容实为数学各学科之基础，在此一并给出，应属必要。第二章引入了群、环、域的概念，包括同态、同构、正规子群和理想等概念，给出例子和简单性质。第三章和第四章是整数整除和同余理论的学习，包括算术基本定理和欧几里得算法，剩余类环的构造以及欧拉定理、费马小定理和中国剩余定理等著名定理。第五章则是域上多项式环的介绍，这里大部分结果是整数环理论的平行结果，另外则是多项式零点研究，并给出了根与系数关系的韦达定理。第六章是群论基础，介绍了元素的阶，循环群的基本性质，陪集和群论拉格朗日定理。第七章是对置换和对称群的介绍，包括置换奇偶性和交错群。第八章则是对 p 元有限域乘法群的学习，包括原根和二次剩余的概念，以及二次互反律的证明。最后一章我们回到对多项式的学习，介绍了整系数多项式和对称多项式的性质。

本书可以作为“代数学基础”或者“初等数论”课程参考教材，适用于尚未学习“近世代数”（“抽象代数”）课程的大学数学类专业学生。对于未开设“初等数论”或者“代数学基础”课程的学校学生，本书也可以作为“近世代数”课程的参考书籍。另外，本书也适用于信息安全专业学生，或者其他对代数思想、方法感兴趣的学生和学者。

本书初稿自 2012 年开始，在中国科学技术大学数学科学学院大一新生（代数学基础）课程试用，迄今已有三个年级 500 余名学生使用。编者向这些年来对代数课程体系调整和本书初稿提供意见的各位学者、教师和学生表示深深感谢，并欢迎大家继续提供宝贵意见。

编者

2015 年 8 月 1 日

目 录

第一章 预备知识

1.1 集合与映射

1.1.1 集合的定义

首先引入集合的定义.

将一些不同的对象放在一起, 即为**集合** (set), 其中的对象称为集合的**元素** (element). 在本书中, 我们将使用大写字母 $A, B, C, \cdots$ 来表示集合, 用小写字母 $a, b, c, \cdots$ 来表示集合中的元素. 记 A 为一个集合. 如果 a 是 A 中的元素, 则称 a 属于 A, 记为 $a \in A$, 否则记为 $a \notin A$. 我们也可以将集合 A 表示为 $A = \{a \mid a \in A\}$, 其中 $a \in A$ 可以用 A 中元素满足的共同性质代替, 比如说偶数集合=$\{a$ 为整数 $\mid a$被 2 整除$\}$. 注意到集合中元素总是不重复的.

如果集合 A 中的每一个元素均是集合 B 中元素, 则称 A 是 B 的**子集** (subset), 换言之, 即若 $a \in A$, 则 $a \in B$. 此时我们记为 $A \subseteq B$ 或 $B \supseteq A$. 可以用图 1.1 来表示 $A \subseteq B$.

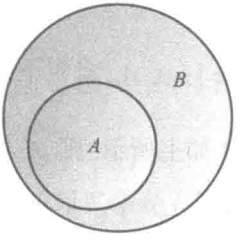

图 1.1 集合的包含关系

如果集合 $A \subseteq B$ 且 $B \subseteq A$, 即 $a \in A$ 当且仅当 $a \in B$, 称 A 与 B **相等**, 并记为 $A = B$. 如果 $A \subseteq B$ 且 $A \neq B$, 我们称 A 为 B 的**真子集** (proper subset), 记为 $A \subset B$ 或者 $A \subsetneq B$.

不含任何元素的集合称为**空集** (empty set), 记为 $\varnothing$. 由定义可知, 空集 $\varnothing$ 是任何集合的子集, 且是任何非空集合的真子集.

如果集合 A 的元素个数有限, 称 A 为**有限集** (finite set), 其元素个数称为**集合的阶** (cardinality 或 order), 记为 $|A|$. 元素个数无限的集合称为**无限集** (infinite set), 它的阶定义为 ∞.

1.1.2 集合的基本运算

一般来说, 集合有如下的四种基本运算.

(I) **集合的交** 设 A, B 为两个集合, 则 A **与** B **的交集** (intersection) 为

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

可以用图 1.2 表示集合的交. 在上式中, 记号 := 表示的是将其右边的集合记作 $A \cap B$.

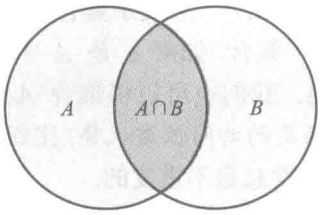

图 1.2 集合的交

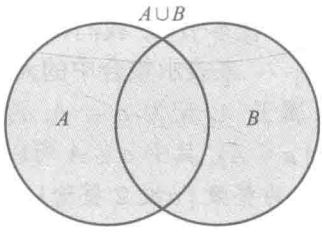

图 1.3 集合的并

更一般地, 设 I 为集合, I 中每个元素 i 对应集合 A_i, 则集合 $A_i (i \in I)$ 的交为

$$\bigcap_{i \in I} A_i := \{x \mid x \in A_i, \text{对每个} i \in I \text{成立}\}.$$

(II) **集合的并** 设集合 A, B 如上所示, 则 A **与** B **的并集** (union) 为

$$A \cup B := \{x \mid x \in A \text{ 或} x \in B\}.$$

可以用图 1.3 表示集合的并. 更一般地, 集合 $A_i (i \in I)$ 的并为

$$\bigcup_{i \in I} A_i := \{x \mid x \in A_i, \text{ 对某个} i \in I \text{ 成立}\}.$$