



21世纪数学精编教材
数学基础课系列

近世代数

Abstract Algebra

杜奕秋 程晓亮 主编



北京大学出版社
PEKING UNIVERSITY PRESS



21 世纪数学精编教材
数学基础课系列

近 世 代 数

主 编 杜奕秋 程晓亮
副主编 王 丽 张 平
王 琦 张安玲



北京大学出版社
PEKING UNIVERSITY PRESS

图书在版编目(CIP)数据

近世代数/杜奕秋,程晓亮主编. —北京:北京大学出版社,2013.8

(21世纪数学精编教材·数学基础课系列)

ISBN 978-7-301-23017-6

I. ①近… II. ①杜… ②程… 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(2013)第 183220 号

书 名: 近世代数

著作责任者: 杜奕秋 程晓亮 主编

责任编辑: 曾婉婷

标准书号: ISBN 978-7-301-23017-6/O · 0947

出版发行: 北京大学出版社

地 址: 北京市海淀区成府路 205 号 100871

网 址: <http://www.pup.cn> 新浪官方微博: @北京大学出版社

电子信箱: zyjy@pup.cn

电 话: 邮购部 62752015 发行部 62750672 编辑部 62767347 出版部 62754962

印 刷 者: 北京大学印刷厂

经 销 者: 新华书店

787mm×980mm 16 开本 10 印张 220 千字

2013 年 8 月第 1 版 2013 年 8 月第 1 次印刷

印 数: 0001—3000 册

定 价: 25.00 元

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究

举报电话: (010)62752024 电子信箱: fd@pup.pku.edu.cn

内 容 简 介

本书从代数学的发展简史出发,深入浅出地阐述近世代数的基本理论、基本问题和基本方法. 全书共分为五章,内容包括: 代数学发展简史、同态与同构、群、环和域等. 本书每节主题鲜明,内容翔实丰富,既有理论阐述,又有实际应用举例. 本书的另一特色在于以读者熟悉的高等代数知识作为背景知识,类比地引入近世代数中相应的概念,使读者能够更好地理解和掌握相关的内容. 另外,不惜笔墨介绍代数学的发展简史,说明近世代数的产生、发展过程,这样既能激发学生学习的积极性和主动性,又方便教师根据历史线索,结合教学实际,有侧重地安排教学内容. 本书每节配有适量的习题,书末附有习题答案与提示,以便于教师教学和学生自学.

本书既可作为高等院校数学与应用数学专业近世代数课程的教材,也可作为非数学专业该课程的教学参考书,还可作为相关科研人员的参考书.

为了方便教师多媒体教学,作者提供与教材配套的相关内容的电子资源(包括电子教案、ppt 课件、习题解答、试题库等),需要者请电子邮件联系 chengxiao-liang92@163.com.

前 言

近世代数即抽象代数,近世代数课程是数学与应用数学专业的必修课程.近世代数是现代数学的重要基础,主要研究群、环、域等代数结构.它的概念与思想渗透到所有数学分支,而其理论与方法在统计学、信息论、计算机科学、近代物理、化学以及其他许多科学与工程领域中都有广泛而深入的应用.本书从代数学的发展简史出发,深入浅出地阐述近世代数的基本理论、基本问题和基本方法.

全书共分为五章,内容包括:代数学发展概述、集合与整除、群、环及域等.第一章介绍了初等代数与近世代数的发展简史,让学生从整体把握本门课程的脉络,在学习中能居高临下地审视课程内容,增强其学习的积极性和主动性.第二章介绍了集合与关系、映射、代数运算与运算律、同态、同构与自同构等内容.近世代数的主要内容就是研究所谓的代数系统,即带有运算的集合,因此集合也是近世代数中一个最基本的概念.虽然在高等代数中集合、映射、关系等一些基本概念已经有详细介绍,但是在这里,我们为了内容的完整和学生自学的需要也稍做简要阐述.第三章由群的概念与基本性质出发,从纯粹抽象的角度讨论了两个群没有差别的本质,即群同态或同构,其中具体讨论了子群结构的基本性质以及循环群的存在问题、数量问题和结构问题(在同构的意义下);讨论了比循环群略微复杂一点的有限交换群是循环群的充分必要条件;讨论了子群的陪集和非空有限集合上的变换群;从多角度讨论了原群及其子结构的性质,即商群,再利用商群介绍了群的同态基本定理与同构定理.第四章介绍了一种重要的代数系统——环.环可以看成我们熟悉的整数集和数域上多项式函数集等代数系统的推广.第五章介绍了域理论.域理论是研究特定种类偏序集合(通常叫做域)的数学分支.因此域理论可以看做序理论的分支.域是定义了两个代数运算的代数系统,是可以进行四则运算的数集的抽象.它是同时具有顺序关系和代数运算的集合,在数学上起着非常重要的作用.

在本书的编写过程中,全国十余所兄弟院校的同行提出了许多宝贵的建议,本书的出版也得到了北京大学出版社的大力支持,我们在此表示诚挚的谢意.

本书既可作为高等院校数学与应用数学专业近世代数课程的教材,也可作为非数学专业该课程的教学参考书,还可作为相关科研人员的参考书.

本书内容虽然经过各编者多次讨论、审阅、修改,但限于编者的水平,不妥之处仍然会存在,诚恳希望广大同行和读者给予批评指正.

编 者
2013年3月

目 录

第一章 代数学发展简史	1	§ 3.3 群的同构	36
§ 1.1 代数学概述	1	一、群的同态和同构的基本概念	37
§ 1.2 代数学的发展	2	二、群的同态和同构的基本性质	39
一、代数学的发展基础——算术	2	习题 3.3	42
二、代数学成为独立分支		§ 3.4 循环群	43
——初等代数	3	习题 3.4	46
三、代数学的深化阶段——高等代数	3	§ 3.5 子群与子群的陪集	46
四、代数学的抽象化阶段		一、子群	46
——近世代数	5	二、群的直和分解	49
第二章 同态与同构	7	三、子群的陪集	51
§ 2.1 集合与关系	7	习题 3.5	55
习题 2.1	11	§ 3.6 Lagrange 定理	55
§ 2.2 映射	11	习题 3.6	58
习题 2.2	14	§ 3.7 置换群	58
§ 2.3 代数运算与运算律	14	一、置换群的基本概念及性质	58
习题 2.3	19	二、置换的轮换表示	61
§ 2.4 同态	20	习题 3.7	67
习题 2.4	22	§ 3.8 商群	67
§ 2.5 同构与自同构	22	一、正规子群	67
习题 2.5	24	二、商群	72
第三章 群	25	三、群同态基本定理	74
§ 3.1 群的基本概念及性质	25	习题 3.8	78
习题 3.1	31	第四章 环	79
§ 3.2 变换群	31	§ 4.1 环的基本概念及性质	79
一、变换群	32	一、环的概念及运算法则	79
二、图形的对称性群	34	二、常见的环	84
三、多元对称函数的对称性群	35	三、子环	86
习题 3.2	36	四、理想	88

目录

五、商环	90	二、子域	113
习题 4.1	91	三、商域	113
§ 4.2 交换环	92	习题 5.1	119
习题 4.2	97	§ 5.2 有序域	119
§ 4.3 多项式环	97	习题 5.2	123
习题 4.3	98	§ 5.3 扩域	124
§ 4.4 整环的因式分解	98	一、扩域的概念	124
习题 4.4	106	二、单纯扩域	124
§ 4.5 环的同态与同构	106	三、分裂域	130
习题 4.5	109	习题 5.3	131
第五章 域	110	参考文献	132
§ 5.1 域的基本概念及性质	110	名词索引	133
一、域的概念及基本性质	110	习题答案与提示	138



第一章

代数学发展简史

正如德国数学家希尔伯特(D. Hilbert)所言:“数学科学是一个不可分割的整体,它的生命正是在于各个部分之间的联系。”数学根据自身发展过程中不同时期表现出的不同特点,分为初等数学和高等数学;根据数学问题研究的内容特点分为代数学、几何学、概率与统计学等;作为教育任务的数学内容,则从知识结构和逻辑关系进行编排整理,分为不同门类,以便于让学生理解和掌握具体的数学概念与数学问题.从数学史发展的角度重新认识所教授的数学内容,从数学文化新视角开展教学活动,用崭新的数学发展历史来解释数学形成过程,以达到数学教学与数学真实的和谐统一,这对学生未来的发展是大有益处的.本章主要介绍代数学发展史.

§ 1.1 代数学概述

公元 8 世纪,阿拉伯第一位伟大的数学家阿尔·花拉子米(al-Khowārizmī)的著名数学著作《还原和对消计算》(或翻译成《论复位及调整》),是代数学成为数学独立分支的重要标志.此书名由阿拉伯文译为拉丁文“*Ludus algebrae et almucgrabalaeque*”,简称为“*algebra*”.1859 年,我国清代数学家李善兰首次把“*algebra*”译成“代数学”.

代数学从广义而言,是研究符号形式的运算的科学.其发展经历了三个阶段:文辞阶段、缩写阶段、符号阶段.文辞阶段的代数特点就是完全不用符号.缩写阶段的代数,首先是在埃及发展起来的,其特点是用某些常用的字逐渐缩写来表示运算,缩写已经成为一种符号.公元 3 世纪,希腊数学家丢番图(Diophantus)在著作《算术》中用的全部符号都是缩写.丢番图将符号引入到数学中,研究的对象就变为一个完全抽象物,成为某一指定运算的运算符号.公元 7 世纪,印度数学家和天文学家婆罗摩笈多(Brahmagupta)创造了一套用颜色表示未知数的符号,即用相应颜色名称的字头作为未知数的符号.我国古代也曾用不同字表示常数(已知

数)或未知数,在南宋数学家李冶的著作中,用“元”表示未知数,“太”表示已知数.代数学史的转折点是16世纪法国人弗朗西斯科·维叶德(Franciscus Vieta)用A和其他大写字母表示未知量,使代数学进入了符号化时代.直到十六七世纪,法国数学家韦达(F. Vieta)才在前人经验的基础上,有意识、系统地用字母表示数.在他的作品《分析入门》中,把代数学看做一门完全符号化的科学,引入了抽象的符号,用元音字母表示未知数,用辅音字母表示已知数.他被西方人称为“代数之父”.1637年,法国数学家笛卡儿(Descartes)用小写字母 $a, b, c, \dots$ 表示已知数,用 $x, y, z, \dots$ 表示未知数,初步建立了代数学符号系统,发展成为今天的习惯用法.初等代数是算术的推广,即用字母表示数,进行数、字母与表达式之间的运算.字母将代数学从字句的制约下解放出来,使得方程的研究获得了新的生命.方程的解法使人们获得了打开未知世界的金钥匙.由此,方程的研究成为代数学研究的中心问题之一.

在方程发展与完善的历史长河中,随着字母表示数参与的运算体系的形成,直到十六七世纪,代数方程体系在韦达奠定的基础上,由笛卡儿基本完成.伴随数域的扩张,方程理论跨入了现代化.代数的发展由古代的算术、代数、几何的相互交融的初等代数时期,逐渐发展到了高等代数和抽象代数的广阔领域.

§ 1.2 代数学的发展

一、代数学的发展基础——算术

算术是数学中最古老的一个分支,它的一些结论是在长达数千年的时间里,缓慢而逐渐地建立起来的.算术有两种含义:一种是从中国传下来的,相当于一般所说的“数学”,如《九章算术》中的“算术”;另一种是从欧洲数学翻译过来的,源自希腊语,有“计算技术”之意.现在一般所说的“算术”,往往指自然数的四则运算.如果是在高等数学中,则有“数论”的含义.作为现代小学课程内容的算术,主要讲的是自然数、正分数以及它们的四则运算,并通过由计数和度量而引出的一些最简单的应用题加以巩固.

《九章算术》是世界上最早系统叙述了分数运算的著作,其中“盈不足”的算法更是一项令人惊奇的创造;“方程”章还在世界数学史上首次阐述了负数及其加减运算法则.在代数方面,《九章算术》在世界数学史上最早提出负数概念及正、负数加减运算法则.现在中学讲授的线性方程组的解法和《九章算术》介绍的方法大体相同.《九章算术》是我国几代人共同劳动的结晶,它的出现标志着我国古代数学体系的形成.唐、宋两代都由国家明令规定它为教科书.1084年,由当时的北宋朝廷对《九章算术》进行刊刻,这是世界上最早的印刷本数学书.后世的数学家,大多数都是从《九章算术》开始学习和研究数学知识的.所以,《九章算术》是我国为世界数学发展做出的杰出贡献.

19 世纪中叶,德国数学家格拉斯曼(Grassmann)第一次成功地挑选出一个基本公理体系,来定义加法与乘法运算,而算术的其他命题,可以作为逻辑的结果从这一体系中被推导出来.后来,意大利数学家皮亚诺(G. Peano)进一步完善了格拉斯曼的体系,形成了皮亚诺公理.

算术的基本概念和逻辑推论法则,以人类的实践活动为基础,深刻地反映了世界的客观规律性.尽管它是高度抽象的,但由于它概括的原始材料是如此广泛,因此我们几乎离不开它.同时,它又构成了数学其他分支的最坚实的基础.

二、代数学成为独立分支——初等代数

作为中学数学课程主要内容的初等代数,其中心内容是方程理论.代数方程理论在初等代数中是由一元一次方程向两个方面扩展的:其一是增加未知数的个数,考查由几个未知数的若干个方程所构成的二元或三元方程组(主要是一次方程组);其二是增高未知数的次数,考查一元二次方程或准二次方程(即双二次方程,其一般形式为 $ax^4 + bx^2 + c = 0 (a, b \neq 0)$).初等代数的主要内容在 16 世纪便已基本上发展完备.

公元前 19 世纪至前 17 世纪,古巴比伦人解决了一次和二次方程问题.欧几里得(Euclid)的《几何原本》(公元前 4 世纪)中有用几何形式解二次方程的方法.我国的《九章算术》(公元 1 世纪)中有三次方程和一次联立方程组的解法,并运用了负数.3 世纪,丢番图用有理数求一次、二次不定方程的解.13 世纪,我国出现的天元术(见李冶的《测圆海镜》)是有关一元高次方程的数值解法.16 世纪,意大利数学家塔尔塔利亚(N. Tartaglia)、费拉里(L. Ferrari)先后成功地得到了三次和四次方程的求根公式.16 世纪,法国数学家韦达开始有意识地系统使用数学符号,他不仅用字母表示未知数及其方幂,而且还用字母表示方程的系数和常数项.韦达认为,代数与算术是不同的,算术仅研究关于具体数的计算方法,而代数则研究关于事物的类或形式的运算方法.字母表示数的思想方法是代数学发展史上的一个重大转折,从此,代数从算术中很快分离出来,成为一门独立的学科.

三、代数学的深化阶段——高等代数

随着生产力的进一步发展,许多数量关系问题,都被归结为代数方程的求解问题.人们开始把注意力集中到关于方程和方程组求解的一般理论研究上.对二次以上方程求解问题的研究发展成为多项式理论;对一次方程组(即线性方程组)求解问题的研究发展成为线性代数理论.

16 世纪初,人们开始研究 5 次以至更高次代数方程的根式解法.在随后的三个世纪中,许多数学家为此付出了大量的精力,最后由挪威数学家阿贝尔(Abel)完成了定理“次数大于 4 的一般代数方程不可能有根式解”的证明.1830 年,法国数学家伽罗瓦(E. Galois)解决了

方程有根式解的充分必要条件这个意义更为广泛的问题,创立了伽罗瓦理论.代数方程的另一个极其重要的成果是代数学基本定理,即:一元 n 次复系数多项式方程在复数域内有且只有 n 个根(重根按重数计算).在瑞士数学家欧拉(Euler)、法国数学家达朗贝尔(d'Alembert)研究的基础上,由德国数学家高斯(Gauss)于1799年圆满地完成了它的证明.

17世纪,日本数学家关孝和(Seki Kowa)提出了行列式的概念,他在1683年写了一部叫做《解伏题之法》的著作,意思是“解行列式问题的方法”,书里对行列式的概念和它的展开已经有了清楚的叙述.而在欧洲,第一个提出行列式概念的是德国的数学家、微积分学奠基人之一——莱布尼茨(Leibnitz).17世纪下半叶,从研究线性方程组的解法出发,在莱布尼茨、英国数学家凯莱(Cayley)等人的努力下,建立了以行列式、矩阵、线性变换等为主要内容的线性代数.这标志着高等代数理论体系的建立.

1750年,瑞士数学家克莱姆(Cramer)在他的《线性代数分析导言》中发表了求解线性系统方程的重要基本公式(即人们熟悉的克莱姆法则).

1764年,法国数学家贝祖(Bezout)把确定行列式每一项的符号的方法系统化.对给定含 n 个未知量的 n 个齐次线性方程,贝祖证明了系数行列式等于零是这方程组有非零解的条件.法国数学家范德蒙(Vandermonde)是第一个对行列式理论进行系统阐述(即把行列式理论与线性方程组的求解相分离)的人,并且给出了一条法则,用二阶子式和它们的余子式来展开行列式.针对行列式本身进行研究这一点而言,他是这门理论的奠基人.1772年,法国数学家拉普拉斯(Laplace)在《对积分和世界体系的探讨》中证明了范德蒙的一些规则,并推广了行列式展开的方法:在 n 阶行列式中,任意取定 r 行(列)($1 \leq r \leq n$),由这 r 行(列)组成的所有 r 阶子式与它们的代数余子式的乘积之和等于其行列式.这个方法现在仍然以他的名字命名,称为拉普拉斯定理.1841年,德国数学家雅可比(Jacobi)总结并提出了行列式的最系统的理论.另一个研究行列式的是法国最伟大的数学家柯西(Cauchy),他大大发展了行列式的理论.在行列式的记号方面,他把元素排成方阵并首次采用了双重足标的新记法;与此同时,他发现两行列式相乘的公式,还改进并证明了拉普拉斯的展开定理.

1848年,英格兰的西尔维斯特(J. J. Sylvester)首先提出了“矩阵”这个词,它来源于拉丁语,代表一排数.矩阵代数在1855年得到了凯莱的进一步发展.凯莱研究了线性变换的组成并提出了矩阵乘法的定义,使得复合变换 ST 的系数矩阵变为矩阵 S 和矩阵 T 的乘积.他还进一步研究了那些包括矩阵的逆在内的代数问题.1858年,凯莱在他的矩阵论文集中提出著名的Cayley-Hamilton理论:在矩阵 A 的特征方程中,以 A 代替变量,则得到一个零矩阵.利用单一的字母 A, B 等来表示矩阵对矩阵代数发展是至关重要的.在发展的早期,公式 $\det(AB) = \det(A)\det(B)$ 为矩阵代数和行列式之间提供了一种联系.柯西首先给出了特征方程的术语,并证明了阶数超过3的矩阵有特征值及任意阶实对称矩阵都有实特征值;给出了相似矩阵的概念,并证明了相似矩阵有相同的特征值;研究了代换理论.

数学家试图研究向量代数,但在任意维数中并没有两个向量乘积的自然定义.第一个涉及不可交换向量积(即 $\mathbf{V} \times \mathbf{W}$ 不等于 $\mathbf{W} \times \mathbf{V}$)的向量代数是德国数学家格拉斯曼(Grassmann)在他的《线性扩张论》(1844年)一书中提出的.他的观点还被引入一个列矩阵和一个行矩阵的乘积中,结果就是现在称之为秩为1的矩阵,或简单矩阵.19世纪末,美国数学物理学家吉布斯(Willard Gibbs)发表了关于《向量分析基础》的著名论述,其后物理学家P. A. M. Dirac提出了行向量和列向量的乘积为标量.我们习惯的列矩阵和向量都是由物理学家在20世纪给出的.

矩阵的发展是与线性变换密切相连的,到19世纪它还仅占线性变换理论形成中有限的空间.第二次世界大战后,随着现代数字计算机的发展,矩阵又有了新的含义,特别是在矩阵的数值分析等方面.由于计算机的飞速发展和广泛应用,许多实际问题可以通过离散化的数值计算得到定量的解决.于是作为处理离散问题的线性代数,成为从事科学研究和工程设计的科技人员必备的数学基础.

四、代数学的抽象化阶段——近世代数

近世代数又称抽象代数,它产生于19世纪.近世代数是研究各种抽象的公理化代数系统的数学学科.由于代数可处理实数与复数以外的物集,例如向量、矩阵、变换等的集合,这些物集分别是依它们各自的演算定律而定的,而数学家将每个物集中的个别演算经由抽象手法把共有的内容升华出来,并因此而达到更高层次,这就诞生了近世代数.近世代数包含群论、环论、伽罗瓦理论、格论、线性代数等许多分支,并与数学其他分支相结合产生了代数几何、代数数论、代数拓扑、拓扑群等新的数学学科.近世代数已经成了当代大部分数学的通用语言.

被誉为天才数学家的伽罗瓦是近世代数的创始人之一.他深入研究了一个方程能用根式求解所必须满足的本质条件,他提出的“伽罗瓦域”、“伽罗瓦群”和“伽罗瓦理论”都是近世代数所研究的最重要的课题.伽罗瓦群理论被公认为19世纪最杰出的数学成就之一,它给方程可解性问题提供了全面而透彻的解答,解决了困扰数学家们长达数百年之久的问题.伽罗瓦群论还给出了判断几何图形能否用直尺和圆规作图的一般方法,圆满解决了三等分任意角和倍立方体的问题都是不可解的.最重要的是,群论开辟了全新的研究领域,以结构研究代替计算,把从偏重计算研究的思维方式转变为用结构观念研究的思维方式,并把数学运算归类,使群论迅速发展成为一门崭新的数学分支,对近世代数的形成和发展产生了巨大影响.同时这种理论对于物理学、化学的发展,甚至对于20世纪结构主义哲学的产生和发展都产生了巨大的影响.

1843年,爱尔兰数学家哈密顿(W. R. Hamilton)发明了一种乘法交换律不成立的代数——四元数代数.第二年,格拉斯曼推演出更具有一般性的几类代数.他们的研究打开了

近世代数的大门. 实际上, 减弱或删除普通代数的某些假定, 或将某些假定代之以别的假定 (与其余假定是兼容的), 就能研究出许多种代数体系.

1870 年, 德国数家克罗内克 (Kronecker) 给出了有限阿贝尔群的抽象定义; 德国数学家戴德金 (R. Dedekind) 开始使用“体”的说法, 并研究了代数体; 1893 年, 德国数学家韦伯 (Weber) 定义了抽象的体; 1910 年, 德国数学家施坦尼茨 (Steinitz) 展开了体的一般抽象理论; 戴德金和克罗内克创立了环论; 1910 年, 施坦尼茨总结了包括群、代数、域等在内的代数体系的研究, 开创了近世代数学.

有一位杰出女数学家被公认为近世代数奠基人之一, 被誉为“代数女皇”, 她就是德国数学家诺特 (E. Noether). 诺特的工作在代数拓扑学、代数数论、代数几何的发展中有重要影响. 1907—1919 年, 她主要研究代数不变式及微分不变式. 她给出了三元四次型不变式的完全组, 还解决了有理函数域的有限有理基的存在问题, 对有限群的不变式具有有限基给出了一个构造性证明. 她不用消去法而用直接微分法生成微分不变式, 讨论连续群 (李群) 下不变式问题, 给出了诺特定理, 把对称性、不变性和物理的守恒律联系在一起. 1916 年后, 她开始由古典代数学向近世代数学过渡. 1920 年, 她已引入“左模”、“右模”的概念. 1921 年, 她完成的《整环的理想理论》是交换代数发展的里程碑, 其中建立了交换诺特环理论, 证明了准素分解定理. 1926 年, 她发表了《代数数域及代数函数域的理想理论的抽象构造》, 给戴德金环一个公理刻画, 指出素理想因子唯一分解定理的充分必要条件. 诺特的这套理论也就是现代数学中的“环”和“理想”的系统理论. 一般认为近世代数形成的时间就是 1926 年, 从此代数学研究对象由研究代数方程根的计算与分布, 进入到研究数字、文字和更一般元素的代数运算规律和各种代数结构, 完成了古典代数到近世代数的本质的转变. 诺特的思想通过她的学生、荷兰数学家范·德·瓦尔登 (Van der Waerden) 的名著《近世代数学》得到广泛的传播, 她的主要论文收在《诺特全集》(1982) 中.

1930 年, 美国数学家伯克霍夫 (G. Birkhoff) 建立格论, 它源于 1847 年的布尔代数. 第二次世界大战后, 出现了各种代数系统的理论和布尔巴基学派. 1955 年, 法国数学家亨利·嘉当 (Henri Cartan)、法国数学家格洛辛狄克 (A. Grothendieck) 和美国数学家艾伦伯格 (S. Eilenberg) 建立了同调代数理论.

到现在为止, 数学家们已经研究过二百多种代数结构, 其中最主要的若当代数和李代数是服从结合律的例子. 这些工作的绝大部分属于 20 世纪, 它们使一般化和抽象化的思想在现代数学中得到了充分的反映.

第二章

同态与同构

本章所要介绍的内容是在以后各章中都要用到的基本概念,是学习本书后面各个代数系统的必备知识. 它们分别是: 集合与关系、映射、代数运算与运算律、同态、同构与自同构、可除性、欧几里得算法、算术基本定理及同余式.

§ 2.1 集合与关系

近世代数的主要内容就是研究所谓的代数系统,即带有运算的集合. 因此,集合是近世代数中一个最基本的概念. 关于集合的一些基本运算和性质,也是我们研究代数系统必不可少的理论工具.

定义 1 若干个(有限个或无限个)固定事物的全体,叫做一个**集合**(简称**集**).

通常用大写英文字母 $A, B, C, \dots$ 来表示集合. 特别地, $\mathbf{C}$ 表示复数集, $\mathbf{R}$ 表示实数集, $\mathbf{Q}$ 表示有理数集, $\mathbf{Z}$ 表示整数集, $\mathbf{N}$ 表示自然数集; $\mathbf{C}^*$ 表示非零复数集, $\mathbf{R}^+$ 表示正实数集, $\mathbf{R}^-$ 表示负实数集.

定义 2 组成一个集合的各个事物称为这个集合的**元素**(简称**元**).

通常用小写英文字母 $a, b, c, \dots$ 来表示元素. 当 a 是集合 A 的元素时,称 a 属于 A ,记做 $a \in A$; 当 a 不是集合 A 的元素时,称 a 不属于 A ,记做 $a \notin A$ 或 $a \in A$.

定义 3 由所讨论的全部元素组成的集合称为**全集**,记为 U .

定义 4 不含任何元素的集合称为**空集**,记为 $\emptyset$.

定义 5 包含有限个元素的集合称为**有限集**; 否则,称为**无限集**. 有限集 A 所包含的元素个数是一个非负整数,记为 $|A|$.

特别地,有 $|\emptyset| = 0$.

表示一个集合的方法通常有两种:

(1) 列举法,即列出它的所有的元素,并且用一对花括号括起来.

例如, $A = \{1, 2, 3\}$, $B = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right\}$.

(2) 描述法,即用它的元素所具有的特性来刻画.

例如, $A = \{x | x^2 - 2x - 3 = 0\}$.

定义 6 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, 记做

$$A \subseteq B \text{ 或 } B \supseteq A.$$

定义 7 如果 A 是 B 的一个子集, 而且 B 中至少有一个元素不属于 A , 则称 A 是 B 的一个真子集, 记做 $A \subset B$ 或 $B \supset A$.

例如, 对于任何集合 A , 都有 $A \subseteq A$; 又如, $\{1, 2\} \subset \{1, 2, 3\}$.

空集被认为是任意集合的一个子集.

集合的包含关系(子集)具有下列性质:

(1) 自反性: 对于任意的集合 A , 有 $A \subseteq A$;

(2) 传递性: 若 $A \subseteq B, B \subseteq C$, 则 $A \subseteq C$.

定义 8 设 A, B 是两个集合. 若 $A \subseteq B$, 且 $B \subseteq A$, 则称 A 与 B 相等, 记做 $A = B$.

两个相等的集合包含相同的元素.

定义 9 设 A 是一个给定的集合, 由 A 的全体子集所组成的集合称为 A 的幂集, 记做 2^A .

例如, 设 $A = \{1, 2, 3\}$, 则 $2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

下面再讨论一下集合的相关运算.

定义 10 由集合 A 和集合 B 的所有共同元素组成的集合叫做 A 与 B 的交集(简称交), 用符号 $A \cap B$ 来表示, 即 $A \cap B = \{x | x \in A \text{ 且 } x \in B\}$.

定义 11 由属于集合 A 或集合 B 的所有元素组成的集合叫做 A 与 B 的并集(简称并), 用符号 $A \cup B$ 来表示, 即 $A \cup B = \{x | x \in A \text{ 或 } x \in B\}$.

定义 12 在全集 U 中取出集合 A 的全部元素, 余下的所有元素组成的集合称为 A 的余集, 记做 A' , 即

$$A' = \{x | x \in U, x \notin A\}.$$

特别地, 有 $U' = \emptyset, \emptyset' = U$.

定义 13 设 A, B 是全集 U 的两个子集, 由属于 A 而不属于 B 的所有元素组成的集合称为 B 在 A 中的差集, 记做 $A \setminus B$, 即

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

例如, 设 $U = \{x | 2 \leq x \leq 10, x \in \mathbf{Z}\}$, $A = \{2, 4, 6, 8\}$, $B = \{2, 3, 5, 7\}$, 则 $A \cup B = \{2, 3, 4, 5, 6, 7, 8\}$, $A \cap B = \{2\}$, $A' = \{3, 5, 7, 9, 10\}$, $B' = \{4, 6, 8, 9, 10\}$.

集合的上述三种运算具有下列性质:

定理 1 设 A, B, C 是集合 U 的三个子集, 则有

(1) 交换律: $A \cup B = B \cup A$, $A \cap B = B \cap A$;

- (2) 结合律: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$;
 (3) 分配律: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
 (4) 模律: 如果 $A \subseteq C$, 那么 $A \cup (B \cap C) = (A \cup B) \cap C$;
 (5) 幂等律: $A \cup A = A$, $A \cap A = A$;
 (6) 吸收律: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$;
 (7) 两极律: $A \cup U = U$, $A \cap U = A$, $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$;
 (8) 补余律: $A \cup A' = U$, $A \cap A' = \emptyset$;
 (9) 对合律: $(A')' = A$;
 (10) 对偶律: $(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B'$.

定义 14 设 A, B 是两个集合, 作一个新的集合: $\{(a, b) \mid a \in A, b \in B\}$, 称这个集合是 A 与 B 的笛卡儿积(简称卡氏积), 记做 $A \times B$.

注意: (a, b) 是一个有序元素对, 从而

$$B \times A = \{(b, a) \mid b \in B, a \in A\}.$$

一般来说, $A \times B$ 并不等于 $B \times A$. 例如, 设 $A = \{1, 2, 3\}$, $B = \{4, 5\}$, 则

$$A \times B = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\},$$

$$B \times A = \{(4, 1), (4, 2), (4, 3), (5, 1), (5, 2), (5, 3)\}.$$

然而, 当 A, B 都是有限集时, $A \times B$ 与 $B \times A$ 包含元素的个数是相同的, 都等于 $|A| \cdot |B|$.

卡氏积的概念可以推广: n 个集合 $A_1, A_2, \dots, A_n$ 的卡氏积定义为

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, i = 1, 2, \dots, n\}.$$

通常将 $A_1 \times A_2 \times \cdots \times A_n$ 简记为 $\prod_{i=1}^n A_i$.

定义 15 设 A, B 是两个集合, 则 $A \times B$ 的子集 R 称为 A, B 间的一个二元关系. 对 $\forall a \in A, b \in B$, 当 $(a, b) \in R$ 时, 称 a 与 b 具有关系 R , 记做 aRb ; 当 $(a, b) \notin R$ 时, 称 a 与 b 不具有关系 R , 记做 $aR'b$.

定义 16 设 R 是 $A \times B$ 的子集, 则 R 在 $A \times B$ 中的余集 $R' = (A \times B) \setminus R$ 也是 $A \times B$ 的子集, 所以 R' 也是 A, B 间的一个二元关系, 称为 R 的余关系.

定义 17 设 R 是 $A \times B$ 的子集, 则 $\{(b, a) \mid (a, b) \in R\}$ 是 $B \times A$ 的子集, 从而是 B, A 间的一个二元关系, 称为 R 的逆关系, 记做 R^{-1} .

例如, 设 $A = B = \mathbf{R}$, 则

$$R_1 = \{(a, b) \mid (a, b) \in \mathbf{R} \times \mathbf{R}, a = b\}, \quad R_2 = \{(a, b) \mid (a, b) \in \mathbf{R} \times \mathbf{R}, a \leq b\},$$

$$R_3 = \{(a, b) \mid (a, b) \in \mathbf{R} \times \mathbf{R}, a = 2b\}, \quad R_4 = \{(a, b) \mid (a, b) \in \mathbf{R} \times \mathbf{R}, a^2 + b^2 = 1\}$$

都是实数集 $\mathbf{R}$ 间的二元关系, 而且 $aR_1b \Leftrightarrow a = b$, 所以 R_1 就是实数间的“相等”关系; $aR_2b \Leftrightarrow a \leq b$, 所以 R_2 就是实数间的“小于或等于”关系. 另外, R_1 的逆关系 R_1^{-1} 就是 R_1 ; R_1 的余关

系 R'_1 就是实数间的“不等”关系; R_2 的逆关系 R_2^{-1} 就是实数间的“大于或等于”关系; R_2 的余关系 R'_2 就是实数间的“大于”关系.

定义 18 $A \times A$ 的子集 R 称为集合 A 上的一个二元关系.

有一种常见的特殊的二元关系, 叫做等价关系.

定义 19 设 $\sim$ 是集合 A 上的一个二元关系. 若 $\sim$ 满足以下条件:

- (1) 自反性: 对 $\forall a \in A$, 有 $a \sim a$;
- (2) 对称性: 对 $\forall a, b \in A$, 有 $a \sim b \Rightarrow b \sim a$;
- (3) 传递性: 对 $\forall a, b, c \in A$, 有 $a \sim b, b \sim c \Rightarrow a \sim c$,

则称 $\sim$ 是 A 上的一个等价关系. 这时, 若 $a \sim b$, 则称 a 与 b 等价.

定义 20 若把集合 A 的全体元素分成若干互不相交的子集, 即任意两互异子集都无公共元素, 则每个这样的子集叫做 A 的一个类, 类的全体叫做 A 的一个分类.

集合的分类与集合的等价关系之间有密切的联系. 集合 A 的一个分类可以决定 A 上的一个等价关系; 反之, 集合 A 上的一个等价关系也可以决定 A 的一个分类. 下面的两个定理刻画了这种关系.

定理 2 集合 A 的一个分类决定 A 的一个等价关系.

证明 利用给定的分类来作一个二元关系, 即规定

$$a \sim b \iff a \text{ 与 } b \text{ 在同一类.}$$

这样规定的 $\sim$ 显然是 A 上的一个二元关系. 下面证明它是一个等价关系:

- (1) a 与 a 在同一类, 所以 $a \sim a$.
- (2) 若 a 与 b 在同一类, 那么 b 与 a 也在同一类. 所以 $a \sim b \Rightarrow b \sim a$.
- (3) 若 a, b 在同一类, b, c 在同一类, 那么 a, c 也在同一类. 所以

$$a \sim b, b \sim c \Rightarrow a \sim c.$$

定理 3 集合 A 的一个等价关系决定 A 的一个分类.

证明 利用给定的等价关系来作 A 的一些子集: 把所有同 A 的一个固定的元素 a 等价的元素都放在一起, 作成一个子集, 这个子集用符号 $[a]$ 来表示. 所有这样得到的子集就组成 A 的一个分类. 下面我们分三步来证明这一点:

- (1) 证明 $a \sim b \Rightarrow [a] = [b]$.

假定 $a \sim b$, 那么由等价关系的条件(3)及 $[a], [b]$ 的定义有

$$c \in [a] \Rightarrow c \sim a \Rightarrow c \sim b \Rightarrow c \in [b], \quad \text{即 } [a] \subseteq [b].$$

但由等价关系的条件(2), $b \sim a$, 因此同样可推得 $[a] \supseteq [b]$. 故 $[a] = [b]$.

- (2) 证明 A 的每一个元素 a 只能属于一个类.

假定 $a \in [b], a \in [c]$, 那么由 $[b], [c]$ 的定义有 $a \sim b, a \sim c$. 这样, 由等价关系的条件(2), (3)有 $b \sim c$. 由前面的(1)可得 $[b] = [c]$.