近世代数

丘维声 著

北京大学出版社
PEKING UNIVERSITY PRESS

近世代数

丘维声 著

北京大学出版社
PEKING UNIVERSITY PRESS

图书在版编目(CIP)数据

近世代数/丘维声著. —北京：北京大学出版社，2015.3
ISBN 978-7-301-25580-3

Ⅰ.①近… Ⅱ.①丘… 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（2015）第 042153 号

书　　名	近世代数
著作责任者	丘维声　著
责任编辑	潘丽娜
标准书号	ISBN 978-7-301-25580-3
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　　新浪微博：@北京大学出版社
电子信箱	zpup@pup.cn
电　　话	邮购部 62752015　发行部 62750672　编辑部 62752021
印 刷 者	北京大学印刷厂
经 销 者	新华书店
	880 毫米 × 1230 毫米　A5　9.625 印张　266 千字
	2015 年 3 月第 1 版　2015 年 3 月第 1 次印刷
定　　价	29.00 元

内容简介

本书是大学数学系近世代数(或抽象代数)课程的教材,是作者积三十多年讲授近世代数及相关课程的经验和心得体会写成的.本书以研究各种代数系统及其态射为主线,内容包括:绪论;第一章群;第二章环的理想,域的构造;第三章整环的整除性;第四章域扩张,伽罗瓦理论;第五章模.本书按照数学的思维方式编写,从客观现象抽象出概念并猜测可能有的规律,解剖麻雀,讲清楚想法,建立严密的讲授体系.学习本书不仅可以学到近世代数的基础知识和基本方法,而且可以受到数学思维方式的熏陶和训练.本书的书末附有习题解答,这是学习近世代数的组成部分.

本书可作为综合性大学、理工科大学和高等师范院校的数学系、应用数学系的近世代数(或抽象代数)课程的教材,也可用作数学教师和科研工作者的参考书.

作者简介

丘维声　1966年毕业于北京大学数学力学系.现为北京大学数学科学学院教授,博士生导师,全国高等学校首届国家级教学名师,美国数学会 *Mathematical Reviews* 评论员,中国数学会组合数学与图论专业委员会首届常务理事,《数学通报》副主编,曾任"数学与力学教学指导委员会"(第一、二届)成员.

出版著作41部,发表教学研究论文22篇,译著(合译)6部.作者编写的具有代表性的优秀教材有:《高等代数(上册、下册)——大学高等代数课程创新教材》(清华大学出版社,2010),《高等代数(第二版)(上、下)》(高等教育出版社,2002,2003),《高等代数》(科学出版社,2013),《群表示论》(高等教育出版社,2011),《简明线性代数》(北京大学出版社,2002),《解析几何(第二版)》(北京大学出版社,1996),《抽象代数基础》(高等教育出版社,2003),《有限群和紧群的表示论》(北京大学出版社,1997),《解析几何》(高等教育出版社,2014)等.

作者的研究方向:代数组合论、群表示论、密码学,发表科学研究论文46篇.承担国家自然科学基金重点项目2项,主持国家自然科学基金面上项目3项.

丘维声教授获全国高等学校首届国家级教学名师奖,三次被评为北京大学最受学生爱戴的十佳教师,获宝钢教育奖优秀教师特等奖,北京市高等教育教学成果一等奖,被评为全国电大优秀主讲教师、北京市科学技术先进工作者,获北京大学杨芙清—王阳元院士教学科研特等奖,三次获北京大学教学优秀奖、北京大学科研成果奖等.

前　言

伽罗瓦(E. Galois)在1829—1831年间完成的几篇论文中彻底解决了一元 n 次方程根式可解的问题，给出了方程可用根式求解的充分必要条件. 伽罗瓦解决这个问题提出的理论引发了代数学的革命性的变化. 古典代数学以研究方程的根为中心. 伽罗瓦理论创立以后，代数学转变为以研究各种代数系统(群、环、域、模等)的结构及其态射(保持运算的映射)为中心，由此创立了近世代数学(或称为抽象代数学). 近世代数学研究结构和态射的观点已经深入到现代数学的各个分支中.

近世代数是大学数学系的必修课程，学生们普遍认为这门课比较难学. 作者根据1980年以来讲授近世代数(或抽象代数)课三十多年的经验，力求使这门课不那么难学. 继作者于2003年写的《抽象代数基础》之后，写了本书. 作者采取了以下措施使近世代数成为比较容易学的一门课程.

抓住主线. 近世代数课的主线是研究代数系统(群、环、域、模等)的结构及其态射. 群论的主线是群同态；环论的主线是环的理想；域论的主线是域扩张，其目标是伽罗瓦理论.

从客观现象抽象出概念并猜测可能有的规律. 本书从星期这一人们熟悉的生活现象，抽象出集合的划分与等价关系，以及模 m 剩余类环 $\mathbb{Z}_m$ 的概念. 从 $\mathbb{Z}_m$ 的可逆元组成的集合 $\mathbb{Z}_m^*$ 只有乘法一种运算，抽象出群的概念；从整数环 $\mathbb{Z}$ 和域 F 上的一元多项式环 $F(x)$ 都有带余除法抽象出欧几里得整环的概念. 从Abel加法群、域 F 上的线性空间、有单位元 $1(\neq 0)$ 的环等抽象出环上的模的概念. 从几何空间的投影猜测可能有群同态基本定理. 从4阶群，8阶Abel群，9阶群的类型，猜测Abel p-群的结构.

讲清楚想法. 从交错群 A_4 有 1,2,3,4,12 阶子群,但是没有 6 阶子群,激发我们去探索对于有限群 G,若素数 p 是 G 的阶的因数,则 G 是否有 p 的方幂阶子群? 设 $|G|=n=p^lm$,其中 p 为素数,$(m,p)=1$,$l>0$. 对于 $1\leqslant k\leqslant l$,G 是否有 p^k 阶子群? 想法:G 的 p^k 阶子群是 G 的一个 p^k 元子集,但是 G 的任意一个 p^k 元子集不一定是子群. 因此,我们要考虑 G 的所有 p^k 元子集组成的集合 Ω. 如果群 G 在 Ω 上有一个作用,那么 Ω 的一个元素 A 的稳定子群 G_A 就是 G 的一个子群. 为了使得 $|G_A|=p^k$,需要选择适当的元素 A. 由于 $|\Omega|=C_n^{p^k}$,因此首先要探索 $C_n^{p^k}$ 的性质,然后我们就能找到 Ω 的合适的元素 A_j,使得 $|G_{A_j}|=p^k$,从而证明了 Sylow 第一定理. 对于 Abel p-群的结构,我们详细讲了证明的想法.

解剖麻雀. 麻雀虽小,五脏俱全,我们在讲伽罗瓦理论时,为了弄清楚伽罗瓦的思想,解剖四次一般方程 $x^4+px^2+q=0$. 它有 4 个复根:

$$x_1=\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}},\quad x_2=-\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}},$$

$$x_3=\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}},\quad x_4=-\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}.$$

通过研究使得方程的根之间其系数属于域 F 的全部代数关系不变的置换组成的集合,给出了方程关于域 F 的群的概念. 进而发现了方程系数域的根式升链与方程的群的递降子群列的联系. 从而引出了伽罗瓦基本定理.

建立严密的讲授体系. 数学的论证是采用公理化的方法,只能从定义、公理和已经证明了的命题出发进行逻辑推理. 因此在讲授近世代数课程时,要全局在胸,在讲前面的知识时要为后面的知识做铺垫. 这样读者学起来就感到自然,渐入佳境,引人入胜. 本书在全局的构思上,以及每一章内容的安排上,都力求构建一个科学的讲授体系. 例如,在第四章域扩张,伽罗瓦理论中,读者学这一章时会感受到这一点.

学习一门课程,一方面要扎实地掌握这门课程的基础知识,这样才能为基础科学研究或数学的应用提供扎实的基础. 但是这还不够,还应

当有科学的思维方式，才能有创新. 数学的思维方式就是一种科学的思维方式，它是一个全过程：观察客观现象，提出要研究的问题，抓住主要特征，抽象出概念，或者建立模型；运用解剖麻雀、直觉、归纳、类比、联想、逻辑推理等进行探索，猜测可能有的规律；采用公理化的方法，只使用定义、公理和已经证明了的命题进行逻辑推理来严密论证，揭示出事物的内在规律，从而使纷繁复杂的现象变得井然有序. “观察—抽象—探索—猜测—论证”是数学思维方式全过程的五个重要环节. 本书就是按照数学的思维方式来写的，这是本书的一个鲜明的特色. 这样写教材就可以使得读者不仅比较容易地学到数学知识，而且可以受到数学思维方式的熏陶和训练，这对于读者今后从事基础科学研究或者从事数学的应用都有帮助，做出创造性的成果.

学习数学一定要做适当多的习题. 通过做习题去掌握基础知识和基本方法，培养分析问题和解决问题的能力，为今后的基础科学研究或数学的应用打下基础. 我们建议读者首先要自己思考，运用学过的理论和方法经过深入分析去做习题. 一道题是否做对了，论证过程是否严密，这对于初学者是不容易判断的. 因此本书在书末写了习题解答，建议读者在自己独立思考做了习题以后，再看本书的习题解答，这样做的收获会更大.

本书可作为大学数学系或应用数学系的近世代数（或抽象代数）课程的教材. 各章所需要的课时大致为：绪论 6 学时，第一章 22 学时，第二章 8 学时，第三章 5 学时，第四章 14 学时，第五章 3 学时，合计 58 学时. 如果近世代数课的周学时为 4，那么可以在一学期讲完本书（除去加 * 号的内容外）. 如果周学时为 3，那么可以不讲第三章的 § 3.3，第四章的 § 4.4，§ 4.5，以及第五章.

作者感谢西安交通大学及其数学与统计学院. 西安交通大学经教育部批准办了数学拔尖班和物理拔尖班，这属于教育部的“基础学科拔尖人才培养试验计划”. 西安交大聘请作者给数学拔尖班讲授高等代数和高等几何、近世代数等课程. 这本书就是作者运用三十多年讲授近世代数课的经验，在给西安交大数学拔尖班 2010 级和 2011 级学生讲授近世代数课的讲稿的基础上，结合作者写的《抽象代数基础》写成的.

作者感谢北京大学出版社的潘丽娜责任编辑，她为本书的出版付出了辛勤的劳动.

作者欢迎广大读者对本书提出宝贵意见.

丘维声
北京大学数学科学学院
2014 年 3 月

目　录

绪　论

§0.1　近世代数学的创立

大约在公元前1700年，巴比伦人实际上就知道了一元二次方程的求根公式，但是他们的方程是用语言叙述并且用语言解出的. 16世纪，韦达(Vieta)不仅用字母表示未知量和未知量的乘幂，而且用字母表示系数，从而研究一般的二次方程 $ax^2+bx+c=0(a\neq 0)$. 这使代数成为研究一般类型的方程的学问.

三次、四次方程直到公元1500年左右才由费罗(S. L. Ferro)、塔塔格利亚(N. Fontana)、卡尔丹诺(G. Cardano)和费拉里(L. Ferrari)等人先后给出解的公式.

从16世纪中叶一直到19世纪初，数学家们致力于五次及更高次方程的代数解法，即对于方程

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0,$$

其中 $n\geqslant 5$，它的解能否通过对方程的系数做加、减、乘(包括乘方)、除和开方(求正整数次方根)运算的公式得到，但是所有寻求这种解法的努力都失败了. 历史上第一个明确宣布“不可能用根式解四次以上方程”的数学家是拉格朗日(J. L. Lagrange). 他在1770年发表的《关于代数方程解的思考》一文中，对二次、三次、四次一般方程的可解性做了透彻的分析，给出了解二次、三次、四次一般方程的统一的、有效的方法，但是对于五次及更高次一般方程则遇到了不可克服的困难.

受到拉格朗日的影响，鲁菲尼(P. Ruffini)在1813年的论文中，大胆地着手证明，五次及更高次一般方程是不能用根式解的. 鲁菲尼用了一条辅助定理，但是没有证明它. 阿贝尔(Abel)读了拉格朗日关于方程论的论文，证明了上述辅助定理(现在叫做阿贝尔定理)，然后用这个定理证明了高于四次的一般方程不可能用根式求解，论文在1826年发表. 由于阿贝尔不知道鲁菲尼的工作，因此阿贝尔的证明是迂回而又不

必要的复杂.

在阿贝尔的工作之后,数学家所面临的一个问题是:什么样的特殊的高于四次的方程可用根式求解?伽罗瓦(E. Galois)在1829—1831年间完成的几篇论文中彻底解决了这个问题,给出了方程可用根式求解的充分必要条件,并且由此推导出了阿贝尔-鲁菲尼定理.伽罗瓦在研究方程可用根式求解的充分必要条件这个问题时,创立了崭新的理论,被人们称之为伽罗瓦理论.伽罗瓦理论不仅彻底解决了方程根式可解的问题,而且由此引发了代数学的革命性变化.古典代数学以研究方程的根为中心,伽罗瓦理论创立以后,代数学转变为以研究各种代数系统的结构及其态射(保持运算的映射)为中心,由此创立了近世代数学(或称为抽象代数学).

§0.2　近世代数的重要性

近世代数学研究代数系统的结构和态射的观点已经深入到现代数学的各个分支中.

近世代数学的知识已经用于许多数学分支以及现代物理学、现代化学等学科.例如,群可以用来度量客观事物的对称性,群还可以用来分类几何学.1872年,德国数学家克莱因(F. Klein)在被聘为爱尔朗根大学的数学教授的就职演讲中创造性地提出了运用变换群的观点来区分各种几何:每种几何都由变换群所刻画,并且每种几何所做的是研究在这个变换群下的不变量;一个几何的子几何是在原来变换群的子群下的一族不变量.他的这个观点后来以爱尔朗根纲领(Erlanger Programm)著称.

近世代数学的知识还被直接用于信息时代的现实生活中.例如,为了满足现代社会信息安全的需要,密码学显得越来越重要,而密码学就用到近世代数学的许多知识.现代通信中为了检错和纠错而产生的编码理论也用到近世代数学的许多知识.

近世代数学的创立生动地体现了数学思维方式的威力.数学的思维方式是一个全过程:观察客观现象,提出要研究的问题,抓住主要特征,抽象出概念,或者建立模型;运用解剖麻雀、直觉、归纳、类比、联想、

逻辑推理等进行探索，猜测可能有的规律；深入分析，只使用公理、定义和已经证明了的定理进行逻辑推理来严密论证，揭示出事物的内在规律，从而使纷繁复杂的现象变得井然有序. 学习近世代数可以受到数学思维方式的很好的训练，从而在今后不论从事何种工作都可以受益.

§0.3 近世代数的基本方法和应用举例

§0.3.1 集合的划分与等价关系，商集

下表是 2013 年 7 月份的月历：

日	一	二	三	四	五	六
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

从时间长河中的所有日子组成的集合 Ω 到整数集 $\mathbb{Z}$ 建立一个对应法则：

$$
\begin{array}{ccc}
\Omega & \longrightarrow & \mathbb{Z} \\
\vdots & & \vdots \\
\text{2013 年 6 月 29 日} & \longmapsto & -1 \\
\text{6 月 30 日} & \longmapsto & 0 \\
\text{7 月 1 日} & \longmapsto & 1 \\
\text{7 月 2 日} & \longmapsto & 2 \\
\vdots & & \vdots
\end{array}
$$

这在 Ω 与 $\mathbb{Z}$ 之间建立了一个一一对应. 于是星期日、星期一、……、星期六分别是 $\mathbb{Z}$ 的下述子集：

$$\begin{aligned}
&\text{星期日}\quad H_0 := \{7k \mid k \in \mathbb{Z}\},\\
&\text{星期一}\quad H_1 := \{7k+1 \mid k \in \mathbb{Z}\},\\
&\text{星期二}\quad H_2 := \{7k+2 \mid k \in \mathbb{Z}\},\\
&\quad\vdots\qquad\qquad\vdots\\
&\text{星期六}\quad H_6 := \{7k+6 \mid k \in \mathbb{Z}\}.
\end{aligned}$$

从而有

$$\mathbb{Z} = H_0 \cup H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5 \cup H_6,\quad H_i \cap H_j = \varnothing,\ \text{当 } i \neq j.$$

从星期这个例子和其他许多例子抽象出下述概念：

定义 1　如果集合 S 是它的一些非空子集的并集，其中每两个不相等的子集的交为空集（此时称它们**不相交**），那么把这些子集组成的集合称为 S 的一个**划分**.

在星期的例子中，$\{H_0, H_1, H_2, H_3, H_4, H_5, H_6\}$ 是整数集 $\mathbb{Z}$ 的一个划分.

有没有给出任一集合 S 的划分的统一方法？

从星期的例子看到：两个整数 a 与 b 属于同一个子集当且仅当它们被 7 除后余数相同，此时称 a 与 b **模** 7 **同余**，记做

$$a \equiv b \pmod 7,$$

读做“a 同余于 b 模 7”或“a 模 7 同余于 b”.

任给两个整数 a 与 b，要么 a 与 b 模 7 同余，要么 a 与 b 模 7 不同余，二者必居其一且只居其一. 很自然地可以把模 7 同余称为整数集 $\mathbb{Z}$ 上的一个二元关系. 数学上如何给出集合 S 上的二元关系的定义呢？从 $\mathbb{Z}$ 上的模 7 同余关系看到，要考虑所有有序整数对组成的集合：

$$\{(a,b) \mid a,b \in \mathbb{Z}\},$$

把这个集合称为 $\mathbb{Z}$ 与自身的笛卡儿积，记做 $\mathbb{Z} \times \mathbb{Z}$. 一般地，设 S 和 M 是两个集合，令

$$S \times M := \{(s,m) \mid s \in S, m \in M\},$$

称这个集合为 S 与 M 的**笛卡儿积**.

由于整数 a 与 b 模 7 同余当且仅当 a 与 b 被 7 除后余数或者都是 0，或者都是 1，……，或者都是 6，因此

$$a \equiv b \pmod 7 \Leftrightarrow (a,b) \in \bigcup_{i=0}^{6} H_i \times H_i,$$