现代数学基础

37 伽罗瓦理论

——天才的激情

章璞 著

高等教育出版社
HIGHER EDUCATION PRESS

37 伽罗瓦理论

——天才的激情

章璞 著

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

内容简介

这是一本专门讲述伽罗瓦理论的教材。内容包括伽罗瓦理论基本定理和多项式方程的根式可解性、伽罗瓦群的计算及其反问题，本书强调通过伽罗瓦对应，可将代数数域中的问题转化成群论的问题加以解决。作为这种思想的应用，证明了代数基本定理，解决了 e 和 π 的超越性及尺规作图的四大古代难题。为方便读者查阅，附录中详细梳理了所要用到的群、环、域方面的结论。每节配有充足的习题并包含提示。

本书可作为高等学校数学类各专业的教材，也可供其他相关专业参考。

图书在版编目（CIP）数据

伽罗瓦理论：天才的激情 / 章璞著．-- 北京：高等教育出版社，2013.5

ISBN 978-7-04-037252-6

Ⅰ.①伽… Ⅱ.①章… Ⅲ.①伽罗瓦理论 Ⅳ.①O153.4

中国版本图书馆 CIP 数据核字（2013）第 073073 号

策划编辑 赵天夫　　责任编辑 赵天夫　　封面设计 赵 阳　　责任印制 张泽业

出版发行	高等教育出版社	咨询电话	400-810-0598
社　　址	北京市西城区德外大街4号	网　　址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印　　刷	中国农业出版社印刷厂	网上订购	http://www.landraco.com
开　　本	787 mm×1092 mm　1/16		http://www.landraco.com.cn
印　　张	9	版　　次	2013 年 5 月第 1 版
字　　数	110 千字	印　　次	2013 年 5 月第 1 次印刷
购书热线	010-58581118	定　　价	35.00 元

物 料 号　37252-00

谨以此书寄托我对妻子风华永远的怀念

序　言

近世代数是研究各种代数结构的一门大学课程. 作为数学发展的一个重要的里程碑, 它起源于 19 世纪 30 年代法国数学家伽罗瓦 (É. Galois) 研究高次代数方程根式可解性问题而给出的置换群概念. 后来在研究数论和几何当中又发展了环和域的理论. 这些代数结构和相关的抽象代数方法不仅极大地推动了数学的发展, 成为数学各领域从事研究的重要代数语言和工具, 而且在物理、力学、化学等方面得到重要的应用. 20 世纪 60 年代以来, 随着数字通信技术的飞速进步, 近世代数 (特别是有限交换群、多项式环和有限域) 已成为信息科学与技术不可缺少的数学工具.

1930—1931 年, 德国数学家范德瓦尔登 (B. L. Van der Waerden) 写出经典名著《近世代数》(*Modern Algebra*). 1958 年再版时书名改成 *Algebra*, 说明它已不那么 "摩登". 1980 年贾柯勃逊 (Nathan Jacobson) 的书中讲述了比传统近世代数更为丰富的内容, 而书名叫做《基础代数》(*Basic Algebra*). 这表明, 半个世纪前还认为很现代和很抽象的代数, 现已成为基本知识. 2009 年, 法国数学家 Luc Illusie 在和我们讨论中法联合培养计划时就说过, 近世代数的群、环、域以及模论、同调代数、交换代数、群的线性表示, 在法国数学界都被认为是 "线性代数". 反观目前我国高校的数学教育, 近世代数在不少学校的数学系只是选修课, 学时很少, 甚至讲不到域论的知识. 在课程安排和教学方法上也需改进, 不少学生未能学到近世代数的真谛. 特别是在数学发展中体现数学魅力的一些重要内容 (例如域的伽罗瓦理论) 不能讲授, 这是很遗憾的.

章璞教授的这本书用来弥补上述不足, 生动地介绍了域论的基本知识, 相当详细地讲述了域的伽罗瓦理论和它的各种精彩的应用. 并且在本书的附录中, 作者对于本来在近世代数课程中已讲述的群、环、域基本内容作了概要的回顾, 以方便读者. 章璞教授于 2012 年夏在扬州大学承办的全国研究生数学暑期学校为国内 150 名数学研究生讲授了本书的内容, 取得了很好的效果. 我相信, 对于广大的数学教师、学生以及对于数学和数学史有兴趣的数学爱好者, 本书都会是一个很好的教材和读物.

冯克勤

2013 年 1 月

于清华大学数学科学系

前　言

这个舞台很小
却要焕发光辉

近年来伽罗瓦理论的教学面临新的情况. 随着学期的缩短, 它在近世代数课程中可用的时间更少; 若不高效地处理其核心内容, 同学往往未得要领课已结束. 而若作为后续课程, 则需梳理所要用到的群、环、域的结论; 同时, 由于伽罗瓦理论没有及时跟进, 近世代数课程可能流于概念, 未见精彩深刻的应用.

作者在中国科学技术大学和上海交通大学讲授此课 20 余次, 了解其中的困难. 我们琢磨如何在尽可能少的课时内讲清伽罗瓦理论的核心内容; 同时也思考作为后续课程它的教学内容. 这本小书就是在此双重考虑下实践的产物.

如果作为近世代数课程中的一章, 则可只讲本书中不带星号的小节, 它们是最基本的内容, 只需 8 个课时便可完成. 这得益于在技术处理上充分运用了同构延拓定理: 它和阿廷引理并用即可证明伽罗瓦理论基本定理. 带星号的小节则用于后续课程.

在思想和方法上, 我们强调通过伽罗瓦对应, 将代数数域中的问题转化成有限群的问题加以解决. 作为例证, 包含了伽罗瓦理论基本定理在代数 (多项式方程的根式可解性和代数基本定理)、数论 (e 和 π 的超越性) 和几何 (正 n-边形的尺规作图) 中的应用. 在内容上, 突出了伽罗瓦群的计算及其反问题, 特别是模 p 法的使用. 附录 I 和 II 详细梳理了所要用到的群、环、域方面的结论, 以便读者查阅. 每节配有

充足的习题, 并对较难想到的步骤作了提示.

张英伯教授仔细审阅了全书, 给予热情支持和鼓励并提出宝贵意见. 这本小书也在国家自然科学基金委数学天元基金 "基础数学" 研究生暑期学校试用并得以完稿, 感谢冯克勤教授和周青教授的邀请、支持和指正. 我从刘绍学教授和冯克勤教授的著述和谈话中受益匪浅. 冯克勤教授应出版社之约为本书作序. 陈惠香、黄华林、李立斌、叶郁、张跃辉诸位教授在完稿过程中给予帮助并提出宝贵意见. 宋科研和熊保林博士提供了 CTEX 作图方面的帮助并指出笔误; 章雨星同学帮忙收集相关历史资料; 德乐思 (Andreas Dress)、卡吉耶 (Pierre Cartier)、哈珀 (Dieter Happel)、凯勒 (Bernhard Keller)、林格尔 (Claus Michael Ringel) 诸位教授与我讨论了相关的历史人物. 感谢高等教育出版社赵天夫编辑的工作. 欢迎读者提出宝贵意见.

谨以此书寄托我对妻子风华永远的怀念: 这促使我仔细地完成本书!

章璞

2012 年 3 月 20 日

于上海交通大学

现代数学基础　图书清单

注：书号前缀为 978-7-04-0xxxxx-x

	书号	书名	著译者
1	21717-9	代数和编码 (第三版)	万哲先 编著
2	22174-9	应用偏微分方程讲义	姜礼尚、孔德兴、陈志浩
3	23597-5	实分析 (第二版)	程民德、邓东皋、龙瑞麟 编著
4	22617-1	高等概率论及其应用	胡迪鹤 著
5	24307-9	线性代数与矩阵论 (第二版)	许以超 编著
6	24465-6	矩阵论	詹兴致
7	24461-8	可靠性统计	茆诗松、汤银才、王玲玲 编著
8	24750-3	泛函分析第二教程 (第二版)	夏道行 等编著
9	25317-7	无限维空间上的测度和积分 —— 抽象调和分析 (第二版)	夏道行 著
10	25772-4	奇异摄动问题中的渐近理论	倪明康、林武忠
11	27261-1	整体微分几何初步 (第三版)	沈一兵 编著
12	26360-2	数论 I —— Fermat 的梦想和类域论	[日] 加藤和也、黒川信重、斎藤毅 著
13	26361-9	数论 II —— 岩泽理论和自守形式	[日] 黒川信重、栗原将人、斎藤毅 著
14	26547-7	微分方程与数学物理问题	[瑞典] 纳伊尔·伊布拉基莫夫 著
15	27486-8	有限群表示论 (第二版)	曹锡华、时俭益
16	27431-8	实变函数论与泛函分析 (上册, 第二版修订本)	夏道行 等编著
17	27248-2	实变函数论与泛函分析 (下册, 第二版修订本)	夏道行 等编著
18	28707-3	现代极限理论及其在随机结构中的应用	苏淳、冯群强、刘杰 著
19	30448-0	偏微分方程	孔德兴
20	31069-6	几何与拓扑的概念导引	古志鸣 编著
21	31611-7	控制论中的矩阵计算	徐树方 著
22	31698-8	多项式代数	王东明 等编著
23	31966-8	矩阵计算六讲	徐树方、钱江 著
24	31958-3	变分学讲义	张恭庆 编著
25	32281-1	现代极小曲面讲义	[巴西] F. Xavier、潮小李 编著

续表

	书号	书名	著译者
26	32711-3	群表示论	丘维声 编著
27	34675-6	可靠性数学引论 (修订版)	曹晋华、程侃 著
28	34311-3	复变函数专题选讲	余家荣、路见可 主编
29	35738-7	次正常算子解析理论	夏道行
30	34834-7	数论——从同余的观点出发	蔡天新
31	36268-8	多复变函数论	萧荫堂、陈志华、钟家庆
32	36168-1	工程数学的新方法	蒋耀林
33	34525-4	现代芬斯勒几何初步	沈一兵、沈忠民
34	36472-9	数论基础	潘承洞 著
35	36950-2	Toeplitz 系统预处理方法	金小庆 著
36	37037-9	索伯列夫空间	王明新
37	37252-6	伽罗瓦理论——天才的激情	章璞 著

网上购书：academic.hep.com.cn, www.china-pub.com, www.joyo.com, www.dangdang.com

其他订购办法：

各使用单位可向高等教育出版社读者服务部汇款订购。书款通过邮局汇款或银行转账均可。**购书免邮费**，发票随后寄出。

单位地址：北京西城区德外大街 4 号

电　　话：010-58581118/7/6/5/4

传　　真：010-58581113

通过邮局汇款：

地　　址：北京西城区德外大街 4 号

户　　名：高等教育出版社销售部综合业务部

通过银行转账：

户　　名：高等教育出版社有限公司

开 户 行：交通银行北京马甸支行

银行账号：110060437018010037603

目 录

§0. 伽罗瓦理论概述*

那些洞察分明的人　安详地激情澎湃
那些成就伟业的人　感动得热泪盈眶

0.1 伽罗瓦理论的核心是建立了域扩张 E/F 的中间域集合与伽罗瓦群 $\mathrm{Gal}(E/F)$ 的子群集合之间的一一对应, 这种对应是反序的, 并且保持共轭性, 这里 E/F 是有限伽罗瓦扩张, 即 E/F 是有限可分正规扩张.

利用这种对应, 可以在域和群之间进行转化和互补性研究, 解决了多项式方程的根式可解性问题以及其他一系列难题, 宣告了古典代数学的终结. 伽罗瓦理论开创了一个范例: 通过引入不同的概念并建立它们之间的联系, 将困难的问题逐步转化, 从而达到解决难题的目的. 更加重要的意义在于: 这一理论中所创立和使用的群和域, 意味着以代数结构为研究对象的近世代数学的开始; 而群论及其所描述的对称性, 其应用和影响已超出数学领域, 成为科学技术乃至人文科学中的基本工具和观念之一.

这本小书的目的就是要以简短的篇幅讲清伽罗瓦理论的核心, 以及它是如何用来解决多项式方程根式可解性和其他几个难题的.

0.2 伽罗瓦理论起源于对多项式方程求根公式的探究. 公元前数百年人类就已知 2 次方程的求根公式. 设 $f(x)=x^2+a_1x+a_2$. 则 $f(x)=0$ 的两个根由公式 $\frac{-a_1\pm\sqrt{a_1^2-4a_2}}{2}$ 给出. 到了文艺复兴时代, 3 次和 4 次方程的求根公式也已在意大利数学家中间流传. 从 16 世纪人们开始关心 5 次和 5 次以上方程是否也有类似的求根公式, 即对于给

定的整数 $n \geq 5$, 是否存在这样一个公式, 使得任意 n 次多项式的根, 都能够通过其系数的有限次加减乘除运算和有限次开方运算 (开 2 次方、3 次方等等) 得到. 此后两百余年, 这个问题困惑了许多数学家, 包括像欧拉 (Leonhard Euler, 1707—1783) 这样伟大的人物. 大数学家拉格朗日 (Joseph Louis Lagrange, 1736—1813) 说: "它好像在向人类智慧挑战!"

拉格朗日是第一个预见高次方程的上述求根公式不存在的人, 但他无法证明. 阿贝尔 (Niels Henrik Abel, 1802—1829) 1824 年完全解决了这一难题: 他证明了当 $n \geq 5$ 时, n 次一般方程是根式不可解的, 也就是说, 它的根不会落在其系数域的有限次根式扩张之中. 因为一般方程的系数均是不定元, 这意味着不存在 n 次方程的上述求根公式. 在此之前, 1799 年鲁菲尼 (Paolo Ruffini, 1765—1822) 也发表了这个结论, 但他的证明有严重的错误. 今天人们将此称为阿贝尔–鲁菲尼定理.

阿贝尔–鲁菲尼定理虽然解决了这个古典数学难题, 但从推动科学发展的意义上说, 似乎并不具备建设性. 今天来看, 不存在求根公式并不要紧, 如果必要例如可以通过数值计算的方法近似求解. 另一方面, 尽管高次方程的求根公式不存在, 但仍然存在许多高次方程, 它们是根式可解的, 即它们的根是落在系数域的有限次根式扩张之中. 如何描述方程根式可解与根式不可解的差别? 它产生的机理是什么? 这在大数学家阿贝尔的工作中并未得到体现。1829 年 4 月 6 日阿贝尔就因患当时的不治之症肺结核而辞世.

0.3 埃瓦里斯特 · 伽罗瓦 (Évariste Galois, 1811—1832) 更进一步. 他首次注意到一个多项式方程是否根式可解, 是由这个方程根集上的一些特殊置换作成的集合是否具有某种性质决定的. 为此, 他最早使用了 "群" 这个词 (法文 "groupe"). 所谓 "这个方程根集上的一些特殊置换作成的集合", 用今天的语言说就是这个方程的伽罗瓦群. 它是这个方程根集上的一个置换群, 但未必是根集的对称群: 这是因为一部分根可能被另外一些根 "生成", 那些被生成的根在置换下变向何处,

当然是由生成它们的那些根的变化情况确定. 也就是说, 伽罗瓦本人使用的方程 $f(x)$ 的伽罗瓦群, 是指 $f(x)$ 的根集上的保持根之间所有代数关系的置换所构成的群.

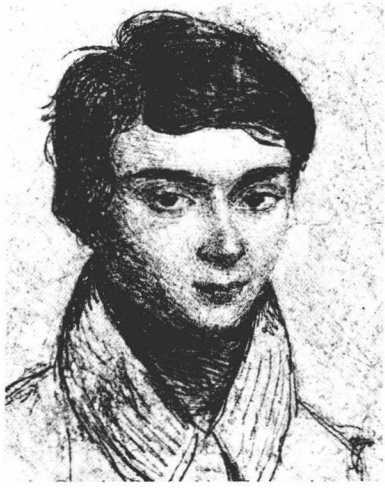
除了群的概念, 伽罗瓦还引进正规子群和可解群的概念. 群 G 为可解群是指 G 有一个链 $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$, 其中每一个 G_i 均是 G_{i-1} 的正规子群, 使得商群 G_{i-1}/G_i 是交换群, $1 \leq i \leq r$.

伽罗瓦大定理指出: 一个多项式方程是根式可解的当且仅当这个方程的伽罗瓦群是可解群. n 次一般方程的伽罗瓦群是对称群 S_n; 而当 $n \geq 5$ 时, S_n 不是可解群. 因此根据伽罗瓦大定理立即得到阿贝尔-鲁菲尼定理: 当 $n \geq 5$ 时, n 次一般方程是根式不可解的. 另一方面, 当 $n \leq 4$ 时, n 次方程的伽罗瓦群都是可解群, 因而它们均是根式可解的. 当然, 所有 n 次方程均根式可解, 并不意味着存在 n 次方程的求根公式; 但是, 此前我们已知当 $n \leq 4$ 时 n 次方程的求根公式的确是存在的.

正如登月英雄阿姆斯特朗 (Neil Alden Armstrong, 1930—2012) 所言: "这是个人的一小步, 却是人类的一大步." (That's one small step for a man, one giant leap for mankind.)

0.4 伽罗瓦不足 21 年的传奇人生拥有众多的传记. 这位集莫扎特的天赋、贝多芬的激情、拜伦的浪漫于一身的天才数学家, 其生平资料的缺乏为许多传记作家提供了部分主观想象的空间. 每隔几十年, 他的生平中的某些细节又成为一些新的研究者的兴趣, 而这只能是永恒之谜. 我们采用至少有 3 篇相对独立的文献的共同说法.

伽罗瓦 1811 年 10 月 25 日生于巴黎南郊小镇. 他的父亲是中学校长并担任了 14 年的镇长, 母亲能熟读拉丁文并精通古典文学. 伽罗瓦幼年没有受过特别的数学训练, 12 岁之前, 他与姐姐和弟弟一起度过愉快的童年. 母亲是他们的启蒙老师, 教授古典文化和宗教方面的知识. 1823 年 10 月伽罗瓦离家到巴黎有名的路易-勒-格兰中学学习, 其杰出毕业生包括作家雨果 (Victor Hugo, 1802—1885). 14 岁那年他



伽罗瓦 (Évariste Galois, 1811.10.25—1832.5.31)

开始对数学产生严肃的兴趣. 史料记载, 伽罗瓦 "像读小说一样" 很快读完勒让德 (Adrien Marie Legendre, 1752—1833) 的《几何原理》并得其要领, 而这本书是两年的教程. 他向大师们学习, 阅读了拉格朗日的论文集《论数值方程解法》和专著《解析函数论》. 1828 年伽罗瓦报考当时法国最著名的高校巴黎综合理工大学 (École Polytechnique), 据说失败的原因是面试时解释不充分. 次年他再次报考巴黎综合理工大学又告失败, 据说因父亲不久前去世而变得没有耐心, 口试中他认为考官的问题无趣并与之发生争执. 1830 年初伽罗瓦只得进入声望较低的师范学院学习, 它就是今天法国最著名的高校巴黎高等师范大学 (École Normale Supérieure) 的前身.

1828 年, 17 岁的伽罗瓦提交关于高次方程代数解的论文, 法国科学院交柯西 (Augustin Louis Cauchy, 1789—1857) 审理. 柯西是当时法国科学院的首席数学家, 其丰富的创造力少有人能比, 作品数量仅次于欧拉 [或许还有凯莱 (Arthur Cayley, 1821—1895)]. 据说柯西未审论文便将稿件丢失. 1830 年, 伽罗瓦再次呈交论文, 但负责审理的法国科学院秘书傅里叶 (Joseph Fourier, 1768—1830) 不久去世. 傅里叶的成就