

献给热爱研读数学的朋友们

Évariste Galois

从一元一次方程到伽罗瓦理论

冯承天◎著



伽罗瓦在十九岁时创建了这一理论，彻底而又完美地解决了近三百年来多项式方程的根式求解问题

只要勤于思考，你一定能掌握近世代数的一些内容、方法和理论；只要乐于思考，你一定能理解伽罗瓦理论的精髓及其各种重大应用



著名
上海市

华东师范大学出版社

全国百佳图书出版单位



Évariste Galois

从一元一次方程到 伽罗瓦理论

冯承天◎著



华东师范大学出版社

图书在版编目 (CIP) 数据

从一元一次方程到伽罗瓦理论 / 冯承天著. — 上海:
华东师范大学出版社, 2012. 7
ISBN 978 - 7 - 5617 - 9699 - 3

I. ①从… II. ①冯… III. ①数学—普及读物 IV.
①01 - 49

中国版本图书馆 CIP 数据核字(2012)第 148574 号

从一元一次方程到伽罗瓦理论

著 者 冯承天
策划组稿 王 焰
项目编辑 王国红
审读编辑 王小双
封面设计 卢晓红

出版发行 华东师范大学出版社
社 址 上海市中山北路 3663 号 邮编 200062
网 址 www.ecnupress.com.cn
电 话 021 - 60821666 行政传真 021 - 62572105
客服电话 021 - 62865537 门市(邮购)电话 021 - 62869887
地 址 上海市中山北路 3663 号华东师范大学校内先锋路口
网 店 <http://hdsdcbs.tmall.com>

印 刷 者 上海华大印务有限公司
开 本 700 × 1000 16 开
印 张 9.5
字 数 144 千字
版 次 2012 年 8 月第一版
印 次 2012 年 8 月第一次
书 号 ISBN 978 - 7 - 5617 - 9699 - 3 / O · 232
定 价 20.00 元

出 版 人 朱杰人

(如发现本版图书有印订质量问题,请寄回本社客服中心调换或电话 021 - 62865537 联系)



前 言

1832年5月30日清晨,随着一声枪响划破巴黎的长空,年龄还不到二十一岁的伽罗瓦倒了下去,第二天他就因急性腹膜炎离开了人间.然而,他却给人们留下了一份极为宝贵的珍品——伽罗瓦理论.

伽罗瓦在十九岁时创建了这一理论,彻底而又完美地解决了近三百年来多项式方程的根式求解问题.但他的天才思想大大超越了时代,以致当时的一些数学大师都“完全不能理解”.不过人们还是逐渐理解和掌握了他的思想和理论,而且从他所创立并完善的群、域等概念中发展出一门新的数学分支——近世代数学,并且使得这些有关的概念、思想和理论成为数学、物理、化学、晶体学,甚至密码学等学科中不可或缺的重要武器.

伽罗瓦理论深刻又优美,不过它确实过于深奥,所以为了与广大数学爱好者分享这一理论,本书起点较低:只要求读者掌握复数的概念与运算.为了尽量说得透彻而详尽,本书多从具体例子讲起,且做到前后呼应,在阐述整个理论来龙去脉的同时,使读者能见树又见林.随着理论的逐步展开与深入,我们还会不断地和大家一起去解决一系列重大的古典难题,比如:尺规作图问题,三次实系数不可约方程的“不可简化情况”以及伽罗瓦的根式可解判别定理等.

本书后有参考文献,这是笔者在研读伽罗瓦理论和撰写本书时读过的部分好书.本书中没有细述的那些部分,读者都可以在所引的书目中找到详细的阐述.

一系列的教学实践使笔者深信：只要勤于思考，你一定能掌握近世代数的一些内容、方法和理论；只要乐于思考，你一定能理解伽罗瓦理论的精髓及其各种重大应用。愿广大数学爱好者在阅读本书的同时能得到美的享受。

最后，我要感谢首都师范大学栾德怀教授，感谢他长期的关心、教导与鞭策，也要感谢上海师范大学周才军教授，他仔细地阅读了全书，并提出了一些宝贵的意见和建议。上海考试院的牟亚萍女士认真打出了一次又一次的修改稿件，为本书的出版作出了巨大努力。还有华东师范大学出版社的诸同仁，他们为本书的出版给予了极大的促进和帮助。

希望本书能为广大的数学爱好者提供一本学习数域上的伽罗瓦理论的可读性较强的读物，也极希望得到他们的批评和指正。

冯承天

2011年5月于上海师范大学



目 录

第一部分 解三次和四次多项式方程的故事

第一章 一次和二次方程的求解	3
§ 1.1 一次方程的求解与数集的扩张	3
§ 1.2 二次方程的求解与根式可解	3
第二章 求解三次方程的故事	5
§ 2.1 波洛那的费尔洛	5
§ 2.2 菲俄与塔尔塔里亚	6
§ 2.3 卡丹与费拉里	7
第三章 三次方程和四次方程的根式求解	9
§ 3.1 三次方程的根式求解	9
§ 3.2 赫德方法的数学背景	10
§ 3.3 四次方程的根式求解	11

第二部分 向五次方程进军

第四章 有关方程的一些理论	15
§ 4.1 韦达与根和系数的关系	15
§ 4.2 牛顿与牛顿定理	16
§ 4.3 欧拉与复数	18
§ 4.4 1 的根	18

第五章 范德蒙与他的“根的对称式表达”方法	20
§ 5.1 范德蒙与范德蒙方法	20
§ 5.2 用范德蒙方法解三次方程	21
第六章 拉格朗日与他的预解式方法	23
§ 6.1 拉格朗日与他的预解式	23
§ 6.2 用拉格朗日方法解三次方程	24
§ 6.3 用拉格朗日方法解四次方程	24
§ 6.4 $n = 5$ 时的情况	25
第七章 高斯与代数基本定理	27
§ 7.1 高斯与代数基本定理	27
§ 7.2 分圆方程与它的根式求解	27
§ 7.3 开方运算的多值性与卡丹公式	28
第八章 鲁菲尼、阿贝尔与伽罗瓦	30
§ 8.1 被人遗忘的鲁菲尼	30
§ 8.2 死于贫穷的阿贝尔	30
§ 8.3 死于愚蠢的伽罗瓦	31

第三部分 一些数学基础

第九章 集合与映射	35
§ 9.1 集合论中的一些基本概念	35
§ 9.2 集合间的映射	35
§ 9.3 集合 A 中的变换	36
§ 9.4 关系、等价关系与分类	37
§ 9.5 整数集合 \mathbf{Z} 与同余关系	38
§ 9.6 算术基本定理与欧拉函数 $\varphi(n)$	38
第十章 群论基础	40
§ 10.1 群的定义	40
§ 10.2 群与对称性	41
§ 10.3 对称群 S_n	41
§ 10.4 子群与陪集	42

§ 10.5	正规子群与商群	43
§ 10.6	循环群与 n 次本原根	44
§ 10.7	单群	45
§ 10.8	群的同态映射与同构映射	46
第十一章	数与代数系	48
§ 11.1	自然数集 \mathbf{N} 作为可换半群及其可数性	48
§ 11.2	整数集合 \mathbf{Z} 与整环	48
§ 11.3	域与有理数域 \mathbf{Q}	49
§ 11.4	实数域 \mathbf{R} 的不可数性	50
§ 11.5	复数域 \mathbf{C} 与子域	50
第十二章	域上的向量空间	52
§ 12.1	向量空间的定义	52
§ 12.2	向量空间的一些基础理论	52
§ 12.3	数域作为向量空间	53
第十三章	域上的多项式	54
§ 13.1	一些基本事项	54
§ 13.2	多项式的可约性与艾森斯坦定理	54
§ 13.3	关于三次方程根的一些定理	55

第四部分 扩域理论

第十四章	有限扩域	59
§ 14.1	扩域作为向量空间	59
§ 14.2	维数公式	59
第十五章	代数数与超越数	61
§ 15.1	代数元与代数数	61
§ 15.2	代数数集 \mathbf{A} 是可数的	62
§ 15.3	超越数的存在	62
§ 15.4	代数扩域	63
第十六章	单代数扩域	64
§ 16.1	最小多项式	64

§ 16.2	单代数扩域	64
§ 16.3	单代数扩域的性质	65
§ 16.4	添加 2 个代数元的情况	66
§ 16.5	有限个代数元的添加与单扩域	67
§ 16.6	代数数集 A 是域	67
§ 16.7	m 型纯扩域与根式塔	68

第五部分 尺规作图问题

第十七章	尺规作图概述	71
§ 17.1	尺规作图的出发点、操作公理与作图法则	71
§ 17.2	最大可作数域 K	72
§ 17.3	Q 的可作扩域	72
第十八章	尺规不可作问题	74
§ 18.1	存在不可作数	74
§ 18.2	立方倍积、三等分任意角与化圆为方	75
第十九章	正 n 边形的尺规作图	76
§ 19.1	把正 n 边形的可作性归结为一些简单的情况	76
§ 19.2	有关 p_j^v 边形的两个域列	77
§ 19.3	分圆多项式	78
§ 19.4	数 p_j^v 应满足的必要条件	79
§ 19.5	对具有 $p = 2^m + 1$ 形式的奇素数的讨论	79
§ 19.6	费马数	79
§ 19.7	作出正 n 边形的“充要条件”	80

第六部分 两类重要的群与一类重要的扩域

第二十章	对称群 S_n	83
§ 20.1	循环与对换	83
§ 20.2	置换的奇偶性	84

§ 20.3	S_n 中元素的对称类与其对换乘积表示	85
§ 20.4	交代群 A_n 的性质	85
§ 20.5	A_5 是单群	86
§ 20.6	可迁群	87
第二十一章	可解群	89
§ 21.1	可解群的定义	89
§ 21.2	可解群的性质	89
§ 21.3	$n \geq 5$ 时, S_n 是不可解群	90
第二十二章	正规扩域	92
§ 22.1	多项式的基域与根域	92
§ 22.2	正规扩域	93
§ 22.3	正规扩域的性质	93

第七部分 伽罗瓦理论

第二十三章	从域得到群	97
§ 23.1	域 E 的自同构群	97
§ 23.2	E 作为 F 扩域时的一类特殊自同构群	98
§ 23.3	正规扩域时的伽罗瓦群	98
§ 23.4	伽罗瓦群的一些重要性质	99
§ 23.5	域 F 上方程的伽罗瓦群	99
§ 23.6	域 F 上的一般的 n 次多项式方程	101
第二十四章	伽罗瓦理论的基本定理	102
§ 24.1	伽罗瓦对应	102
§ 24.2	伽罗瓦理论的基本定理	103

第八部分 伽罗瓦理论的应用

第二十五章	多项式方程的根式可解问题	109
§ 25.1	一些特殊的伽罗瓦群	109
§ 25.2	根式可解的数学含义	110

§ 25.3	根式扩域与根式可解的精确数学定义	110
§ 25.4	循环扩域与拉格朗日预解式	111
§ 25.5	多项式方程根式可解的必要条件	113
§ 25.6	$2x^5 - 10x + 5 = 0$ 不可根式求解	115
§ 25.7	多项式方程根式可解的充分条件	116
§ 25.8	用伽罗瓦理论解三次方程	118
第二十六章	三次实系数不可约方程有 3 个实根时的“不可简化情况”	120
§ 26.1	从判别式看根的情况	120
§ 26.2	不可简化情况	120
§ 26.3	根域的表达	120
§ 26.4	$x^p - a = 0, a \in \mathbf{R}$ 型方程	121
§ 26.5	实根要通过复数得到	122
第二十七章	正 n 边形尺规作图的充分条件	124
§ 27.1	正 n 边形尺规作图必要条件的回顾与充分条件的提出	124
§ 27.2	p 群的一个定理	124
§ 27.3	正 n 边形尺规作图的充分条件	125
§ 27.4	作正 17 边形的高斯方法	125
§ 27.5	从伽罗瓦理论看正 17 边形的尺规作图	127
第二十八章	对称多项式的牛顿定理	129
§ 28.1	一个引理	129
§ 28.2	牛顿定理	129

附 录

附录 1	关于两个正整数最大公因数的一个关系式	133
附录 2	多项式方程的重根问题	134
附录 3	计算三次方程的判别式 D	136
参考文献		137

第一部分

解三次和四次多项式方程的故事

从一元一次方程到伽罗瓦理论

三次、四次方程的根式求解是代数史上的两个里程碑。在这一部分中，我们讲述解三次和四次方程的故事，并具体给出简化的三次和四次方程的求解方法。

第一章

一次和二次方程的求解

§ 1.1 一次方程的求解与数集的扩张

人类最早认识的数集是自然数集 $\mathbf{N} = \{0, 1, 2, \dots\}$. 于是当人们求解未知数时, 多项式方程就出现了. 根据考古资料, 我们知道古巴比伦和古埃及都有解一次方程的记录. 成书于公元前 206 年到公元前 221 年期间的中国《九章算术》就已经有了三元一次方程组的题目. 话虽这样说, 但从事后的眼光来看, 对于 $x+n=0, n \in \mathbf{N}^* = \{1, 2, 3, \dots\}$ 型的方程而言, 它的解 $(-n)$ 就是一个负数.

于是为了使我们的解仍然属于我们的数集, 就有必要把自然数集 \mathbf{N} 扩张为整数集 $\mathbf{Z} = \{0, \pm 1, \pm 2, \dots\}$.

对于一次方程

$$px + q = 0, p, q \in \mathbf{Z}, p \neq 0 \quad (1.1)$$

有解 $x = -\frac{q}{p}$. 同样, 为了使解 $-\frac{q}{p}$ 也在一定的数集之中, 就得进一步把数集 \mathbf{Z}

扩张为有理数集 $\mathbf{Q} = \left\{ \frac{q}{p} \mid q, p \in \mathbf{Z}, p \neq 0 \right\}$. 于是在 \mathbf{Q} 中, 任何一次方程都可解了. 这样, 下一个要研究的方程便是一元二次方程了.

§ 1.2 二次方程的求解与根式可解

由于古巴比伦、古希腊, 尤其是 7 世纪古印度数学家的努力, 人们已经会解许多类型的二次方程了. 不过对一般的二次方程

$$ax^2 + bx + c = 0, a \neq 0 \quad (1.2)$$

解的完整叙述一直到 12 世纪才在欧洲出现, 它的解是

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad (1.3)$$

这个公式我们太熟悉了. 不过在此还想着重说明以下各点:

(i) 这是一个公式, 它针对系数 a, b, c 为具体数字的一个方程而言, 例如 $3x^2 - 13x - 10 = 0$, 只要以 $a = 3, b = -13, c = -10$ 代入(1.3), 便能得出 $x_1 = 5, x_2 = -\frac{2}{3}$ 这两个解.

(ii) 以方程 $x^2 - 2 = 0$ 为例, 它的根为 $x = \pm\sqrt{2}$. 由于 $\sqrt{2}$ 是无理数, 这就使我们进一步要把 \mathbf{Q} 扩张为实数集 \mathbf{R} . 同样地, 对于 $x^2 + 1 = 0$, 它的根为 $\pm i$, 这就要求我们把 \mathbf{R} 扩张到复数集 $\mathbf{C} = \{a + bi \mid a, b \in \mathbf{R}\}$. 由此, 我们看到伴随着方程的解, 数的集合在不断地扩大.

(iii) 给定了方程(1.2), 也即给定了系数 a, b, c , 它的根 $x_{1,2}$ 显然可以由 a, b, c 通过有限次加、减、乘、除以及开方运算得到. 在此意义下, 我们说(1.2)是根式可解的.

于是, 下一步就是求解一般三次方程了. 它是否也是根式可解呢?

第二章

求解三次方程的故事

§ 2.1 波洛那的费尔洛

一般三次方程指的是

$$ax^3 + bx^2 + cx + d = 0, a \neq 0 \quad (2.1)$$

对于其中的一些特殊方程,古巴比伦人已经会解了. 12 世纪波斯诗人欧玛尔·海亚梅(Omar Khayyam, 1048—1122) 又用几何方法解出了另一些三次方程. 14 世纪意大利数学家达迪(Maestro Dardi) 为 198 种不同的三次方程给出了解答,但对解一般的三次方程仍没有突破. 意大利数学家帕西阿利(L. Paciali, 1445—1577) 用意大利文撰写了一本有 600 多页的百科全书般的巨著,论述了算术、代数、几何、比例等课题. 这对那些不谙拉丁文的学者来说就容易读懂了,所以这本书对代数的传播起了积极的作用. 他在书中写道:“迄今,三次和四次方程仍无一般求解公式.”于是求解一般的三次方程对许多人来说就是一次智力大挑战. 此时,意大利波洛那的费尔洛(S. d. Ferro, 1465—1526) 登场了.

费尔洛的爸爸是一个纸张制造商. 费尔洛的青年时代以及是什么促使他研究数学都已无案可查了. 不过,他很可能在波洛那大学完成了大学学业. 这所现在还存在的大学,创立于 1088 年,而且自 15 世纪起已是欧洲最好的大学之一. 1496 年,费尔洛开始在该大学执教,而 1501 年帕西阿利也来到波洛那大学讲课. 费尔洛很可能在帕西阿利的激励下,开始尝试去解一般的三次方程. 约在 1515 年费尔洛成功地解出了 $ax^3 + bx + c = 0$ 型的三次方程. 于是解一般三次方程也就大功告成了.

因为一般三次方程(2.1)是与 $z^3 + \frac{b}{a}z^2 + \frac{c}{a}z + \frac{d}{a} = 0$ 同解的,于是我们只要求解

$$y^3 + ay^2 + by + c = 0 \quad (2.2)$$

型的方程就可以了. 这种最高次项的系数为 1 的方程, 称为首 1 (多项式) 方程.

对(2.2)进行变量代换: $y = x - \frac{a}{3}$, 即得到

$$x^3 + ax + b = 0 \quad (2.3)$$

型的方程. 这类方程的特点是比较最高次项低一次的项(在这里是二次项)消失了. 这就是所谓的简化的(一般首 1 的)三次方程.

综上所述, 解(2.1)型的方程归结为解(2.2)型的方程, 而解(2.2)型的方程又归结为解(2.3)型的方程. 因此费尔洛解出了 $x^3 + ax + b = 0$ 型方程, 那么解一般三次方程(2.1)的问题也就彻底地解决了.

从 12 世纪人们完整地讨论了一般二次方程的解到 16 世纪初费尔洛解出了一般三次方程, 人们大约花费了三四百年之久. 这是一个新的里程碑.

费尔洛并没有发表这一重大结果, 只是把他的解法告诉了他的女婿和学生纳弗(A. d. Nave)以及他的学生菲俄(A. M. Fior), 而其他的数学家仍在摸索之中.

§ 2.2 菲俄与塔尔塔里亚

16 世纪的波洛那学术气氛相当浓, 数学家及其他学者有时会举行各种公开的辩论和对抗赛. 尽管费俄才能相当平庸, 但在他的老师费尔洛死后, 也没有急于发表这一成果. 他想等待时机, 充分利用这份知识财富, 一举成名, 以谋取教职的延聘. 秘密武器当然是举足轻重的.

1535 年, 机会终于来临了. 菲俄听说数学家塔尔塔里亚(N. Tartaglia, 1499—1557)已成功解出了三次方程, 不过菲俄认为他是在吹牛. 于是菲俄与塔尔塔里亚进行了一次公开的解题大赛.

塔尔塔里亚出生于约 1499 年, 原名方丹诺(Fontana). 只是因为他在 12 岁时, 一名法国军人用马刀刺入了他的口腔, 使他患上了“口吃”, 因此塔尔塔里亚(“结巴”)才成了他的浑名. 塔尔塔里亚自小生活艰难, 自学成材. 1543 年, 他搬到威尼斯, 在那里做数学老师.

这场大赛是这样进行的: 双方各出 30 道题, 由对方用 40 到 50 天来解答. 1535 年 2 月 22 日对抗赛如期进行. 菲俄的 30 道题都属 $ax^3 + bx + c = 0$ 这一类型, 而塔尔塔里亚却题题不同. 大赛的结果可想而知: 菲俄大败而归. 塔尔塔里亚用两小时解答了所有的题目, 而菲俄却交了白卷.