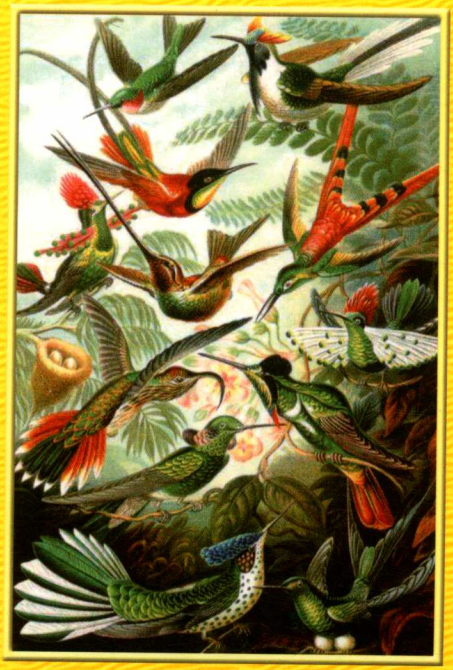
《数学中的小问题大定理》丛书（第六辑）

从根式解到伽罗华理论



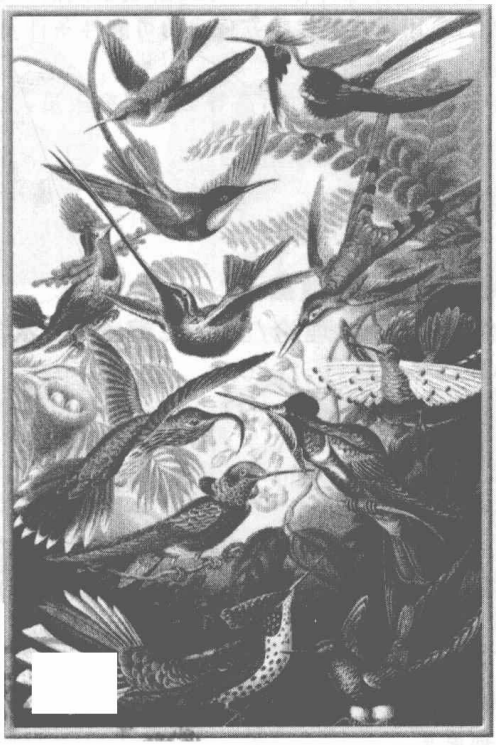
王鸿飞 编

◎方程式解成根式的问题
◎数域及其代数扩张
◎可解群·交错群与对称群的结构
◎论四次以上方程式不能解成根式
◎克罗内克定理
◎用根式解代数方程式的可解性条件

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

《数学中的小问题大定理》丛书（第六辑）

从根式解到伽罗华理论



王鸿飞 编

◎ 方程式解数的问题
◎ 数域及其扩张
◎ 可解群·交错群与对称群的结构
◎ 论四次以上方程式不能解成根式
◎ 克罗内克定理
◎ 用根式解代数方程式的可解性条件

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容提要

本书分为六章，详细介绍了方程式解成根式的问题，数域的扩张，置换，群，用根式解代数方程式的可解性条件及克罗内克定理等内容.

本书适合大学教师及学生，高等数学研究人员，方程及群论学习爱好者参考阅读.

图书在版编目(CIP)数据

从根式解到伽罗华理论/王鸿飞编. —哈尔滨：哈尔滨工业大学出版社，2020.1

ISBN 978-7-5603-6356-1

Ⅰ.①从… Ⅱ.①王… Ⅲ.①伽罗瓦理论 Ⅳ.①O153.4

中国版本图书馆 CIP 数据核字(2019)第 275074 号

策划编辑	刘培杰 张永芹
责任编辑	张永芹 刘春雷
封面设计	孙茵艾
出版发行	哈尔滨工业大学出版社
社　　址	哈尔滨市南岗区复华四道街 10 号　邮编 150006
传　　真	0451-86414749
网　　址	http://hitpress.hit.edu.cn
印　　刷	哈尔滨市工大节能印刷厂
开　　本	787mm×960mm　1/16　印张 10　字数 101 千字
版　　次	2020 年 1 月第 1 版　2020 年 1 月第 1 次印刷
书　　号	ISBN 978-7-5603-6356-1
定　　价	48.00 元

代数方程式公式求解的发展者

花拉子米(约 783–850)

冯塔纳(1499–1557)

卡尔丹诺(1501–1576)

韦达(1540–1603)

拉格朗日(1735–1813)

鲁菲尼(1765–1822)

高斯(1777–1855)

阿贝尔(1802–1829)

伽罗华(1811–1832)

这些学者曾为代数方程式公式求解的发展奉献出无比的智慧和学识,谨于此致敬最高礼赞!

编者的话

大约12年前，编者作为大学预科班学生的时候，就对五次及以上代数方程式的代数解（实际上就是根式求解）问题产生兴趣了，虽然那时就已经了解到“四次以上代数方程式不能有代数解”（鲁菲尼—阿贝尔定理），然而对它的了解也仅此结论而已．因为就连“代数解”的确切含义，当时都是很模糊的，更不用说它的详细内容了．这其中的一个原因就是很难找到这方面的比较详细的叙述；一些带有历史性的叙述材料，仅仅提供如上的结果；而抽象代数中，似乎对此又“不屑一顾”，它的中心是代数结构，而不是方程式的根式解．

后来在大学选择了化学专业，自然也一直无暇顾及这些数学问题. 2010 年年底，开始了早年的那个想法：搜集代数学（主要是古典代数学）各部门的相关材料，以汇编成一本教程. 也正是从那时起，又重新开始学习代数学. 在这个过程中慢慢理解了彻底解决代数方程式代数解问题的伽罗华理论，这其中颇费周折. 一方面是由于伽罗华理论的抽象性；另一方面如前所述，缺少适合初学者的中文文献也是一个原因.

虽然国内已经出版了很多专门叙述伽罗华理论的著作（大多是很优秀的教程），但就笔者所能找到的那些，仍嫌叙述的过于偏向“代数结构”. 例如把很重要的伽罗华群定义为正规域（分裂域）关于基域的那些自同构构成的群. 这在初学者看来是很难“接受”的，因为这个变换群有些抽象并且初看起来似乎与我们的主要问题——求解代数方程——毫无关系. 因为这些，编者计划编辑整理一个小册子，试图以最简洁的方式来完整地叙述方程式的伽罗华理论，在这样的方式下读者可以有较少的准备知识来阅读它.

为了做到上面所讲的那些，我们在编辑整理时注意了一些细节. 首先，尽量避免出现那些与我们的主题关系不大的抽象代数的概念（例如商群、陪集等），因为那些概念无形中会增加阅读的困难. 其次，我们按照伽罗华的原始思想定义了方程式的伽罗华群，然后再证明它与前面讲过的那个变换群就同构而言重合. 这样做的最大好处就是便于初学者对伽罗华群的理解. 第三，尽量简化伽罗华大定理（代数方程式可根式解的充分必要条件）的证明.

在整个成书过程中，得到了哈尔滨工业大学出版社刘培杰等老师的大力支持与帮助，我认为向他们表示感谢是自己应尽的义务.

人们公认，伽罗华理论是数学中最抽象、最繁杂的篇章之一.在伽罗华理论诞生200年后的今天，即便是数学专业的学生，也要具备相当的代数学专门知识才能理解伽罗华理论！整理完这本小册子，对此深有体会，我们很难想象当初伽罗华是如何发展他的理论的，例如在他的那个年代，诸如群、域等概念才刚刚模糊地产生，可是伽罗华必须利用这些概念背后深层次的性质与联系！

编写这本小册子，虽然已经“竭尽全力”，但由于编者学识有限，错漏之处在所难免，恳请读者批评指正.

编　者

2019年8月16日

于浙江新安

目录

方程式解成根式的问题·二项方程式

第1章

§1 方程式解成根式的问题

设有一个 n 次代数方程式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n=0\ (a_0\neq 0) \tag{1.1.1}$$

它的系数是给定的复数，那么这个方程式恰好有 n 个复根（每根按其重数计算个数）. 这就是著名的代数基本定理[①]. 现在发现一个问题——如何在方程式(1.1.1)

①远在 1692 年，荷兰数学家吉拉尔（Albert Girard，1595－1632）就曾预想任何一个 n 次代数方程式都有 n 个根（实根或虚根）. 在 1746 年，法国学者达朗贝尔（Jean le Rond d'Alembert，1717－1783）首先企图证明这个代数基本定理，但是他的证明法不够严格. 直到 1799 年，德国高斯（Carolus Fridericu Gauss，1777－1855）才完全地证明了这个定理.

的系数上实施各种运算来求这些根.

一个复数 a 的 n 次方根的开方运算和解所谓的二项方程式

$$x^n-a=0 \quad (a\neq 0) \qquad (1.1.2)$$

是同一个问题. 在代数学中,$\sqrt[n]{a}$ 这个符号通常理解为二项方程式(1.1.2)的一个根,而这符号常常叫作根式.

于是可施于复数的基本代数运算是四种算术运算,以及开方运算. 所以很自然地提出这样一个问题,即所谓方程式解成根式的问题:把方程式(1.1.1)的根用有限次加、减、乘、除、开方运算以其系数表示出来.

在初等代数学的教程中,我们已经知道二次方程式的根式解法. 历史上,早在公元前 1700 年左右,古巴比伦人就知道了求解二次方程式的方法. 一般的三次、四次方程式的代数解法在 16 世纪也已经被发现. 以后几乎有三个世纪之久,人们在做下面的失败的事情,就是想对任何一个五次方程式(也就是带有符号系数的五次方程式),找出它的解,而经它的系数用根式表出.

我们很难想象,为了解一般的五次方程式,不知耗去多少枉然的精力. 我们说这个问题是向人类智慧的一个挑战并不过分. 在 18 世纪 70 年代初,法国学者拉格朗日(Joseph－Louis Lagrange,1736－1813)首先指出一个已知方程式的根可由另外一个辅助方程式的根的对称函数表示,这个辅助方程式拉格朗日把它叫作预解式. 拉格朗日的结果,并不使人感到满意. 就三次方程式或四次方程式而言,拉格朗日的结果是完全适合的,因为在这种情形下,预解式的次数常较已知方程式的次数少一. 但是,就五次方程式而言,就完全不同

了，因为五次方程式的预解式已经是一个六次方程式了. 所以，就五次方程式而论，拉格朗日的方法完全失去了作用.

继拉格朗日之后，摆在当时数学家面前的问题是：代数的运算是否能够解一个次数高于四次的方程式. 1798 年，意大利学者鲁菲尼(Paolo Ruffini，1765－1822)曾经试图证明次数高于四次的一般方程式不能用代数运算解，但是他的理由并不充分.

次数高于四次的一般方程式用代数运算解的不可能性的严格证明，首先由挪威数学家阿贝尔(Niels Henrik Abel，1802－1829)所给出. 在短暂的生命过程中，这是他对于数学各部门成功的深入研究之一.

实际上，鲁菲尼和阿贝尔并没有对这个问题作出完全的解答. 他们只是证明了对于所有次数已知的 $n(n\geqslant 5)$ 次方程式都适合的根式解不存在. 但这绝不是说任意一个具体数字的方程式不能用代数的运算求解(例如实际上 $2x^5-3=0$ 就有根式解，但是 $2x^5-10x+5=0$ 没有根式解).

第一个回答这个问题的是法国天才数学家伽罗华(Évariste Galois，1811－1832). 伽罗华证明了不能用代数运算求解的具体方程式的存在，同时他还说明了方程式的代数解的可能性是根据怎样的理由. 伽罗华把方程式求解问题转化成置换群的问题，他在繁杂的计算中发现了方程式代数求解的本质.

伽罗华的个性是非常独特的，我们在这里把他的生平略为介绍一下. 投考高等技术学校的入学考试他曾经两次失败，1829 年，伽罗华进入了师范学校，但是由于语言和对指导人的抵触，不久即被斥退(在 1830

年七月革命之后).之后伽罗华参加了当时法国的暴风雨式的政治活动,而且成了一个活跃人物.他不但是一个热情的共和党人,而且也是法皇路易·菲利普(Louis－Philippe de France,1773—1850)的死敌.经过不止一次地被逮捕,结果在决斗中结束了他完美的生命(二十岁的年龄).伽罗华的高深结果并未得到和他同时代的权威学者的赞许,他提交给法国科学院的两篇文章,不但没有得到答复,甚至被认为是一种混乱.1846 年,在伽罗华死后 14 年,他的这一伟大成果才得以发表.1870 年,法国数学家若尔当(Jordan,1838－1922)根据伽罗华的思想撰写了《论置换与代数方程》一书,人们才真正领略伽罗华的伟大思想.

§2 二项方程式[①]

现在回到二项方程式

$$x^n-a=0 \quad (a\neq 0) \tag{1.2.1}$$

的求解问题.我们证明这方程式可以变换成形式如下的二项方程式

$$y^n-1=0$$

任取二项方程式(1.2.1)的一个根,例如 x_0,令新的未知量为 y,并设 $x=x_0y$.代入方程式(1.2.1)后可得

① 自然本节所讨论的解并非代数解,而是超越(三角)解.以后我们将会了解到任何二项方程式均能解成根式.但是由这三角形式的解预先得出二项方程式的根的一些性质是有必要的,因为这些性质本身对于了解方程式是否能解为根式是有用的.

$$x_0^n y^n - a = 0$$

因为 $x_0^n = a$，所以

$$y^n - 1 = 0 \tag{1.2.2}$$

这样，就证明了下述的结果：

定理 1.2.1　a 的所有 n 次方根可由 1 的所有 n 次方根乘以 a 的某一个 n 次方根而得到.

为求 1 的 n 次方根，我们可以利用复数的三角表示. 这就是说，任意复数可以表为

$$r(\cos\theta + \mathrm{i}\sin\theta)$$

其中 r 是它的模，θ 是它的幅角. 并且我们有

$$\begin{aligned} & r(\cos\varphi + \mathrm{i}\sin\varphi) \cdot s(\cos\psi + \mathrm{i}\sin\psi) \\ =\ & rs[(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + \\ & \mathrm{i}(\cos\varphi\sin\psi + \sin\varphi\cos\psi)] \\ =\ & rs[\cos(\varphi+\psi) + \mathrm{i}\sin(\varphi+\psi)] \end{aligned}$$

据此，用数学归纳法易证

$$[r(\cos\theta + \mathrm{i}\sin\theta)]^n = r^n(\cos n\theta + \mathrm{i}\sin n\theta) \tag{1.2.3}$$

此数的模是 r^n，幅角是 $n\theta$.

因为复数 1 的模是 1，幅角是 $2k\pi$，$k = 0, \pm 1, \pm 2, \cdots$，所以，由(1.2.3)知

$$r(\cos\theta + \mathrm{i}\sin\theta)$$

是 n 次单位根，当且仅当

$$r^n = 1, n\theta = 2k\pi$$

或

$$r = 1, \theta = \frac{2k\pi}{n}$$

因此，一个复数是 n 次单位根，当且仅当它具有下列形式

$$\cos\frac{2\pi k}{n} + \mathrm{i}\sin\frac{2\pi k}{n} \quad (k = 0, 1, \cdots, n-1) \tag{1.2.4}$$

但

$$\cos\frac{2\pi k}{n}+\mathrm{i}\sin\frac{2\pi k}{n}=\left(\cos\frac{2\pi}{n}+\mathrm{i}\sin\frac{2\pi}{n}\right)^k$$

故若命

$$\varepsilon_1=\cos\frac{2\pi}{n}+\mathrm{i}\sin\frac{2\pi}{n} \tag{1.2.5}$$

则一个复数是 n 次单位根，当且仅当它是 ε_1 的整数次方. 由此可见，所有 n 次单位根在乘法下作成一个循环群，式(1.2.5)所规定的 ε_1 是它的一个生成元素①.

在式(1.2.4)中取 $k=0,1,2,\cdots,n-1$，我们得到 n 个 n 次单位根

$$1,\varepsilon_1,\varepsilon_1^2,\cdots,\varepsilon_1^{n-1} \tag{1.2.6}$$

这 n 个单位根的幅角都是$\frac{2\pi}{n}$的整倍数；用平面上的点代表复数，把代表这 n 个单位根的点用线段联结起来便成为单位圆的一个内接正 n 边形. 可见，式(1.2.6)中 n 个 n 次单位根都不同. 又 ε_1 是 n 次单位根，当然 $\varepsilon_1^n=1$，所以 ε_1 的周期恰等于 n. 这就证明了下面的定理.

定理 1.2.2 复数域中恰有 n 个 n 次单位根，它们在乘法下作成一个 n 元循环群，式(1.2.5)所规定的 ε_1 是一个生成元素.

周期等于 n 的 n 次单位根称为本原 n 次单位根，除 ε_1 以外，还有另外的本原 n 次单位根存在，这就有下述定理成立.

定理 1.2.3 方程式(1.2.2)的根

$$\varepsilon_k=\cos\frac{2k\pi}{n}+\mathrm{i}\sin\frac{2k\pi}{n}$$

是本原根的充分必要条件为 k 与 n 互素.

---

①关于群及其相关概念见第 3 章.

证明　先求满足

$$\varepsilon_k^m=1 \tag{1.2.7}$$

的最小自然数 m. 因为 $\varepsilon_k=\varepsilon_1^k$，所以等式(1.2.7)可以写成

$$\varepsilon_1^{km}=1=\varepsilon_1{}^n$$

于是，km 应该被 n 整除

$$km=nq \tag{1.2.8}$$

令 d 代表 k 和 n 的最大公约数. 设

$$k=k_1d,n=n_1d$$

式中的 k_1 和 n_1 代表互素整数. 把 k 和 n 的值代入式(1.2.8)后再除以 d 得

$$k_1m=n_1q$$

即 k_1m 可被 n_1 整除. k_1 既然和 n_1 互素，那么 m 必被 n_1 整除. 在所有的自然数中能够被 n_1 整除的，显然以 n_1 自身为最小，因此 $m=n_1=\dfrac{n}{d}$. 假若取 ε_k 的 n_1 次幂，则有

$$\varepsilon_k^{n_1}=\varepsilon_1^{kn_1}=\varepsilon_1{}^{\frac{kn}{d}}=(\varepsilon_1^n)^{\frac{k}{d}}=(\varepsilon_1^n)^{k_1}=1^{k_1}=1$$

假若 k 和 n 互素，则 $d=1$，于是 $m=n$. 因此在 k 和 n 互素的假设下，ε_k 的周期等于 n，也就是说 ε_k 是本原根.

反之若 k 和 n 不互素，则有 $m=\dfrac{n}{d}$，$d>1$，在这种情形下，ε_k 的周期应是 $\dfrac{n}{d}<n$，也就是说 ε_k 不是本原根. 这就证明了定理 1.2.3.

由定理 1.2.3 立刻得出推论如下：

推论　n 次单位本原根的个数等于和 n 互素且小于 n 的自然数的个数.

n 次单位本原根的个数常用 $\varphi(n)$[①] 表示. 自然 $\varphi(1)=1$,因为 1 的一次本原根只有一个,这个本原根就是 1 自身.

例 试求 1 的六次本原根,就是说求

$$\varepsilon^6-1=0$$

的本原根. 在 1,2,3,4,5 诸数中,只有 1 和 5 才与 6 互素,因此 $\varphi(6)=2$. 下面两个本原根就是 1 的六次本原根

$$\varepsilon_1=\cos\frac{2\pi}{6}+\mathrm{i}\sin\frac{2\pi}{6}=\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$$

$$\varepsilon_5=\cos\frac{10\pi}{6}+\mathrm{i}\sin\frac{10\pi}{6}=\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}$$

①在数论上 $\varphi(n)$ 被叫作欧拉函数.