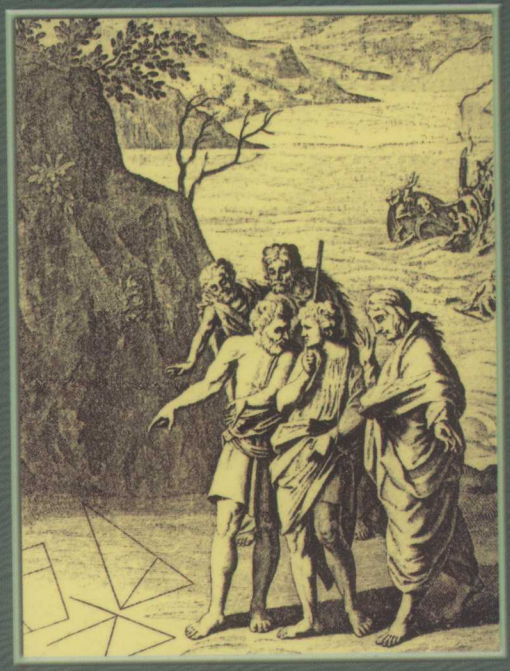
《数学中的小问题大定理》丛书（第五辑）

伽罗华与群论



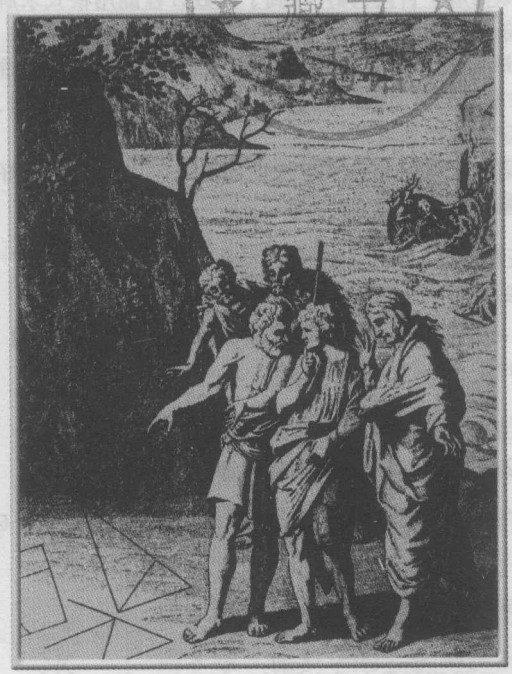
[英]勒贝尔（Lieber, L.R.）著　樊墉 译

◎群是什么
◎群的重要性质
◎一个方程式的群
◎伽罗华的鉴定
◎用直尺与圆规的作图

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（第五辑）

伽罗华与群论



[英]勒贝尔(Lieber, L.R.) 著
樊墉 译

◎群是什么
◎群的重要性质
◎一个方程式的群
◎伽罗华的鉴定
◎用直尺与圆规的作图

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

内容简介

本书从一个方程能用根式求解所必须满足的本质条件开始研究，建立了方程的根的“容许”置换. 这些置换通过添加方程的根的域构成了自同构群. 得到了代数方程能用根式求解的充分必要条件是自同构群可解. 讲述了伽罗华理论的始末. 全书共分八章，分别为：伽罗华、群的重要、群是什么、群的重要性、一个方程式的群、伽罗华的鉴定、用直尺与圆规的作图、伽罗华的鉴定为什么是对的.

本书适合于数学专业的本科生和研究生以及数学爱好者阅读和收藏.

图书在版编目(CIP)数据

伽罗华与群论/(英)勒贝尔(Lieber, L. R.)著；樊㙍译. —哈尔滨：哈尔滨工业大学出版社，2014. 1

ISBN 978-7-5603-4487-4

Ⅰ. ①伽… Ⅱ. ①勒…②樊… Ⅲ. ①群论 Ⅳ①O152

中国版本图书馆 CIP 数据核字(2013)第 292516 号

策划编辑　刘培杰　张永芹
责任编辑　张永芹　刘家琳
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　哈尔滨工业大学印刷厂
开　　本　787mm×960mm　1/16　印张 4.75　字数 56 千字
版　　次　2014 年 1 月第 1 版　2014 年 1 月第 1 次印刷
书　　号　ISBN 978-7-5603-4487-4
定　　价　28.00 元

目录

引　言

大家都知道：科学知识是与时俱进的，科学是一种活的，蓬勃滋长的东西. 然而一般人总把数学看作又老又朽，似乎再也不能滋长发扬的了. 的确，在学校里所教的数学——算术、代数、几何——在几世纪前大家早都知道；就是专门学院的教程差不多也有三百多年的历史. 笛卡儿(Descartes) 创造的解析学和牛顿(Newton) 发明的微积分，那都是17世纪的事情. 可是，事实是这样的：数学的范围甚至比科学的范围还要来得广些，就从那个时候起，它已在脚踏实地地向前迈进了.

数学中一些比较新颖的概念是什么？是不是它们太抽象了——虽然好

些概念还是由很年轻的数学天才所创的 —— 使得这一代的青年人连听都够不上听一听呢?是不是他们距离平常的一般思维方法太远了,以致不能使一般普通的人们从中得到任何用处和快乐?难道连一般数学教员对于这些概念也不能有一个认识的机会吗?不是的!其实是这样的:那些近代数学上的发展不但能使数学家产生兴趣,而且正像微积分一样,对于科学家也能有相当伟大的帮助. 哲学家公认:近代数学与基本的宇宙观是有直接关系的. 心理学家在近代数学中也会看到一种能从偏见中把心胸解放出来的以及能在陈腐的、偏见的荒墟上建立起簇新有力的伟大工具 —— 像是在非欧几里得几何学的创造中所可以看到的. 的确,谁都要珍重现代数学的特殊的旺盛和卓绝的本色.

这本小册子,作者有心想把它当作现代数学中一支的入门,使得那些对于这门数学愿作更进一步研究的人们在阅读时较为容易些、有趣些.

伽罗华

第1章

这本小册子里所讲的是群论(Theory of Groups),群论是近代数学的一种. 伽罗华(Évariste Galois) 对于这门数学的理论和应用发扬很多. 伽罗华殁于一百年以前[①],死的时候还不满二十一岁. 在他那短促而悲惨的生命中,对群论有颇多贡献;而这门数学在今日已成为数学中的重要部分了. 自古以来的二十五位大数学家中,他就是其中的一位[②].

他的一生,除了在数学上有惊人的成功,其余尽是失意的事. 他渴望着

① 译者按:伽罗华卒于1832年,此书原本系在1932年出版,所以原书作者说:"伽罗华殁于一百年以前".

② G. A. Miller in Science, Jan. 22, 1932.

进巴黎的 L'Ecole Polytechnique，但是入学考试时竟失败了；过了一年，他再去应试，然而仍旧是失败. 他拿自己研究的结果给柯西（Cauchy）和傅里叶（Fourier）二人看，这两人是当时很出色的数学家，但是他们对他都没有注意，而且两人都把他的稿本抛弃了. 他的师长们谈起他的时候，常说："他什么也不懂"，"他没有智慧，不然就是他把他的智慧隐藏得太好了，使我简直没法子去发现他". 他被学校开除了. 又因为是革命党徒，他曾经被拘入狱. 他曾与人决斗，就是在这决斗中他被杀了①.

敬祝他的灵魂安乐！

① 在决斗的前夜，他自己预知必死，仓猝中将自己在数学上的心得草率写出，交给他的一个朋友（参看 Annales de L'Ecole Normale Superieure，1896 中 M. P. Dupuy 所作的伽罗华傅，或参阅 David Eugene Smith 所著的 Source Book in Mathematics 一书）.

群的重要

第2章

在讲群论之前，先把群论之所以重要的几个原因之一说一下.

我们都知道数学中一桩要紧的事情是解方程式. 代数方程式[①]可以依它的次数来分类，一次方程式[②]

$$ax + b = 0$$

只要是学过初等代数的小孩子都会解[③]，它的解答是

$$x = -\frac{b}{a}$$

---

① 代数方程式是形如

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

的形式的方程式，此中 n 是正整数.

② $a = 0$ 而 $b \neq 0$ 的情形除外.

③ 一次方程式的解法是在纪元前 1700 年发明的，这年代是根据 Ahmes Papyrus 书中的记载. 此抄本是一部最早的数学文献，现已得美国数学会的赞助而出版.

二次方程式

$$ax^2 + bx + c = 0$$

的解法在初等代数中也有，它的解答是

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

在纪元前数世纪，巴比伦人(Babylonians)已能解这种形状的方程式了①.

三次方程式

$$ax^3 + bx^2 + cx + d = 0$$

和四次方程式

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

的解法已比解一次、二次的方程式难得多了. 直到16世纪才有了解法. 这法子在每本方程式论的书中都可以找到.

当方程式的次数增大时，解法的困难增加得很快. 向来数学家虽都不会解一般高于四次的方程式，可是都相信一定是可能的②. 直到19世纪，利用群论的道理，才证明了这是不可能的事.

此处读者应该要懂得透彻的是刚才所说的“不可能”三个字.

一个问题的能否解决是要看我们对于解答所加的限制条件而定的. 譬如

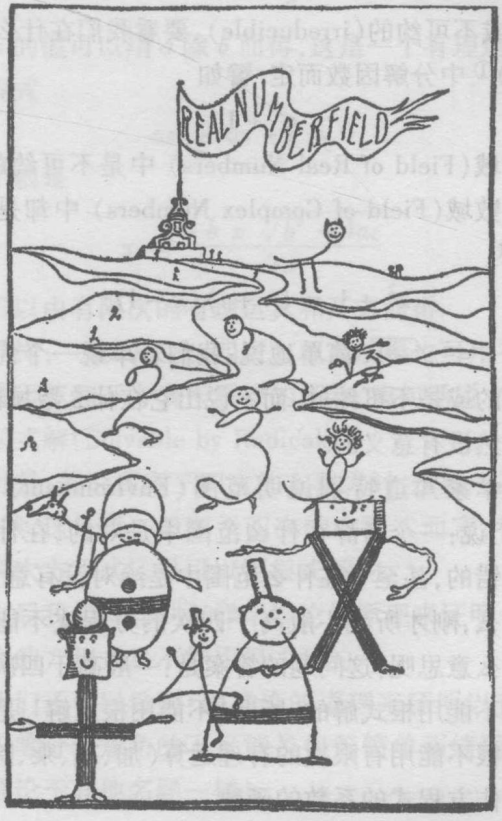
$$x + 5 = 3$$

是能解的，假使我们允许 x 可以是负数的话. 设若我们

---

① 参阅 School and Society, June 18, 1932, p. 833, G. A. Miller 著的 The Oldest Extant Mathematics 一文.

② 如18世纪的大数学家欧拉(Euler)也相信这是可能的.



限定 x 不能是负数，那么这方程式就不能解了.

同样，假使 x 表示银圆数，方程式

$$2x + 3 = 10$$

是可解的. 如果 x 表示人数，这方程式就不能解了，因为 $x = 3\frac{1}{2}$ 没有意义.

要三等分任意一角，若只准用直尺与圆规，这是不可能的. 但是若允许用别的仪器，就可能了.

一个代数式为可约的(reducible,就是说可以分解因数)或不可约的(irreducible),要看我们在什么数域(Field)[①]中分解因数而定. 譬如

$$x^2 + 1$$

在实数域(Field of Real Numbers)中是不可约的. 可是在复数域(Field of Complex Numbers)中却是可约的,因为

$$x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$$

此处的 $\mathrm{i} = \sqrt{-1}$. 简单地说:我们若单说一个代数式是可约的或是不可约的,而不说出它在什么数域内,这话是全然没有意义的.

数学家知道特别说明范围(Environment)的重要. 我们说:一个命辞在什么范围中是对的,在什么范围中是错的,甚至于在什么范围中是绝对没有意义的.

那么,刚才所说一般高于四次的方程式不能解究竟是什么意思呢?这问题的答案是:一般高于四次的方程式是不能用根式解的. 所谓'不能用根式解'是说方程式的根不能用有限次的有理运算(加、减、乘、除)和开方表作方程式的系数的函数.

为要说明这一点,拿一次方程式

$$ax + b = 0$$

来看,这方程式的根是

---

① 一个数域是一个数的集合,其中任两数的和、差、积和商(但零不许作除数)仍在这集合中. 故所有复数做成一个数域;所有实数也做成一个数域;所有有理数也做成一个数域. 但是一切整数的集合不做成一个数域. 因为两个整数的商不一定还是整数. 许多有趣的数域的例子,可以在 L. W. Reid 的 The Theory of Algebraic Numbers 中看到.

$$x = -\frac{b}{a}$$

所以 x 的值可以用 a 除 b 而得，这是一个有理运算！二次方程式

$$ax^2 + bx + c = 0$$

的两个根是

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

这也可以由有限次的有理运算和开方而得.

同样，一般的三次、四次方程式的根也可用有限次的有理运算和开方表作系数的函数. 换句话说：它们可以用根式解(Solvable by Radicals).

可是，若论到高于四次的方程式时，这就不再成立了. 当然，这是指一般高于四次的方程式而言，有些特殊的高次方程式还是可以用根式解的.

以后我们将看到怎样用群论的原理来证明一般高于四次的方程式是不能用根式解的①.

我们还可以看到：用群论的道理来证明以直尺与圆规三等分任意角的不可能是何等简单而绮丽，正如应用群论于其他名题一样！

---

① 若不限定单用有理运算和开方来解高于四次的方程式，关于这点，可参读 L. E. Dickson 的 Modern Algebraic Theories 以及该书中所指的参考书(这当然不是指近似解法如圆解法或霍纳氏法(Horner's method) 等而言的，这类近似解法只在应用数学上有用).

群是什么

第3章

数学中的系统(System)可以说是一部数学的机器(A Mathematical Machine),他的主要成分是:

(1)元素(Element);

(2)一种运算(Operation).

例如:

(a)(1)元素是一切整数(正或负或0);

(2)运算是加法.

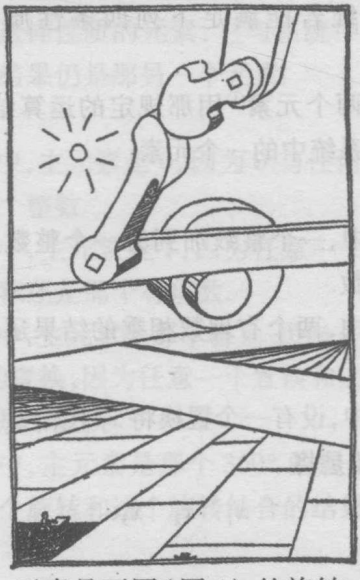
(b)(1)元素是一切有理数[①](0除外);

(2)运算是乘法.

① 一个有理数是一个可以写作两个整数的商的数.譬如$\frac{3}{5}$是一个有理数.但是$\sqrt{2}$不是有理数,因为$\sqrt{2}$不能表作两个整数的商的形式;这事实的证明,可参考 Rietz and Crathorne: College Algebra, p. 23.

(c)(1) 元素是某几个文字(如 x_1, x_2, x_3) 的置换(Substitution);

(2) 运算是将一个置换跟着另一个置换(这个且待以后再解释).



(d)(1) 元素是下圆(图 1) 的旋转,转的度数是 60° 或是 60° 的倍数;

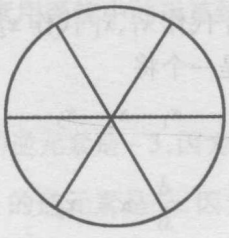


图 1

(2) 运算是如(c) 中一般,将一个旋转跟着另一

个旋转.

从这么一个简单的出发点着手,看上去似乎弄不出什么东西来,然而这样讨论下去所得的结果会令人诧异的!

这种系统若能满足下列四条性质,就称为群(Group):

1. 假使两个元素[①]用那规定的运算结合时,所得的结果还是系统中的一个元素.

例如:

在(a)中,一个整数加到另一个整数上去的结果还是一个整数.

在(b)中,两个有理数相乘的结果还是一个有理数.

在(c)中,设有一个置换将 x_1 代作 x_2,x_2 代作 x_3,x_3 代作 x_1,即是将

$$x_1 \quad x_2 \quad x_3$$

换作

$$x_2 \quad x_3 \quad x_1$$

若在这置换之后跟着另一个置换,假设这另一个置换是将 x_2 代作 x_3,x_3 代作 x_1,x_1 代作 x_2 的,那么,这两个置换结合的结果是一个将

$$x_1 \quad x_2 \quad x_3$$

换作

$$x_3 \quad x_1 \quad x_2$$

的置换.

---

① 这两个元素不必相异,也可以是同一个元素.

在(d)中,设在一个60°的旋转(逆时针方向)之后跟着一个120°的旋转(逆时针方向),其结果是一个180°的旋转(逆时针方向).

2. 系统中必须含有主元素(Identity Element). 所谓主元素是这样性质的元素:它与系统中任意另一个元素结合的结果仍是那另一个元素.

例如:

在(a)中,主元素是0,因为0与任何整数相加的结果还是那个整数.

在(b)中,主元素是1,因为任意一个有理数用1乘了之后的积还是那个有理数.

在(c)中,主元素是那个将x_1代作x_1,x_2代作x_2,x_3代作x_3的置换,因为任意一个置换和这个置换结合的结果还是那个置换.

在(d)中,主元素是那个360°的旋转,因为系统中的任意一个旋转和这个旋转结合的结果还是那个旋转.

3. 每个元素必须有一个逆元素(Inverse Element). 所谓一个元素的逆元素是这样规定的:一个元素和它的逆元素用系统中的运算结合的结果是主元素.

例如:

在(a)中,3的逆元素是-3,因为3加-3的和是0.

在(b)中,$\frac{a}{b}$的逆元素是$\frac{b}{a}$,因为$\frac{a}{b}$和$\frac{b}{a}$相乘的积是1.

在(c)中,将x_1代作x_2,x_2代作x_3,x_3代作x_1的置换的逆元素是那个将x_2代作x_1,x_3代作x_2,x_1代作x_3