伽罗华理论

丁伟岳 北大院士*

PKU 2007

伽罗华理论是代数学的一个重要组成部分, 它的产生源于一个古老的问题, 即代数方程的求解问题.

1 求解代数方程

n 次代数方程就是多项式方程

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

其中的系数属于给定的一个"数域", 且 $a_n \neq 0$. 由于在古代这些系数总是整数, 我们假定的数域是有理数域, 记为 $\boldsymbol{Q}$.

据说早在公元前1500年, 居住在两河流域的巴比伦人就知道如何利用配方法来解2次方程. 他们把问题和解法刻在湿的粘土上, 然后晒干, 形成"土版文书". 如我们在中学学到的, 方程

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

的解是

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

人们自然希望对于3次和更高次的代数方程能找到类似的求解公式. 然而, 经过了大约3000年, 这个问题仍毫无进展.

大约在1500年前后, 意大利数学家 Ferro 发现了3次方程

$$x^3 + px + q = 0, \tag{1}$$

*Revised by Van Abel: van141.abel@gmail.com

(p, q 都是自然数, 负数在当时还不被接受, 大约在100年后才被普遍接受.) 但是按照当时通常的做法, Ferro 对他的解法秘而不宣, 作为向对手挑战的法宝. 后来, 一位被叫做 Tartaglia (口吃者)的意大利数学家发现了更多类型的3次方程的解法, 战胜了 Fior 的挑战. 在另一位数学家 Cardan 的恳求下, Tartaglia 透露了他的解法, 但没有提供证明, 并提出条件是必须保密. 然而 Cartan 没有信守承诺, 在他写的一本书里公布了 Tartaglia 的解法, 同时给出了他自己的证明. 他的证明如下:

假设(1)的解 $x = u + v$, 那么代入方程得到

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

由于 u, v 可变动(相对于给定的方程), 不妨假设 $3uv + p = 0$. 这样方程进一步转化为如下方程组

$$u^3 + v^3 = -q, \quad u^3 v^3 = -(p/3)^3.$$

明显地, 这已经转化为一个二次方程. 直接求解得出

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{q^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{q^3}{27}}.$$

注意到, 尽管 u, v 可以交换顺序, 但是将其代入 $x = u + v$ 将得到同一个根. 为了得到另外的两个根, 必须允许开3次方可取复数值.

在 Cartan 的书中也发表了一些4次方程的解法, 基本上类似于上述解法, 即寻求好的“变量替换”, 用新的未知数代替原来的未知数, 使得心的未知数满足的方程是可以解出的.

2 Lagrange 的研究

1770–1771年, 拉格朗日发表了长篇论文“关于方程的代数解法的思考”, 对代数方程的求解问题进行了深入研究. 他的想法是: 对于3次和4次方程的已知解法做深入分析, 以求对高次方程的求解问题有所启发—期以找出一般的求解方法. 这是典型的从特殊到一般的归纳思维, 但其实现并不是轻而易举的, 需要有过人的观察和分析能力.

拉格朗日考察了3次方程解法. 对于一般的3次方程

$$x^3 + ax^2 + bx + c = 0,$$

总可以通过配3次方消掉 x^2 项. 所以只需要考虑如下的方程, 不失一般性设为

$$x^3 + px + q = 0.$$

这个方程可以通过如下方法解出: 首先, 令

$$x = y - \frac{p^3}{3y}, \tag{2}$$

得到关于 y 的方程

$$y^6 + qy^3 - \frac{p^3}{27} = 0. \tag{3}$$

再令

$$r = y^3,$$

导出

$$r^2 + qr - \frac{p^3}{27} = 0.$$

这是2次方程, 所以可以解出它的两个根 r_1 和 r_2. 这样只要解出

$$y^3 = r_1, \quad y^3 = r_2, \tag{4}$$

再把 y 的值代入(2), 便得到原方程的根.

到此为止, 拉格朗日只是总结归纳了前人对于3次方程的解法, 给出了一个统一的处理方法; 还没用看出这种方法含有什么一般性的东西. 这时他注意到: 只要 $r_1 \neq r_2$, (4)给出了方程(3)的6个不同的根, 但是把这6个不同的数代入(2)以后只得出3个不同的值, 因为3次方程只能有3个根. (3)的六个根分别是

$$y = \sqrt[3]{r_1}, \quad \sqrt[3]{r_1}\omega, \quad \sqrt[3]{r_1}\omega^2, \quad \sqrt[3]{r_2}, \quad \sqrt[3]{r_2}\omega, \quad \sqrt[3]{r_2}\omega^2.$$

其中

$$\omega = e^{i\frac{2\pi}{3}} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3},$$

是3次单位根. 代入(2)得到原方程的3个根

$$x = \sqrt[3]{r_1} + \sqrt[3]{r_2}, \quad \sqrt[3]{r_1}\omega + \sqrt[3]{r_2}\omega^2, \quad \sqrt[3]{r_1}\omega^2 + \sqrt[3]{r_2}\omega.$$

拉格朗日的过人之处在于他进一步发现: (3)的根可以用原方程的根表示为

$$y = \frac{1}{3}(x_1 + x_2\omega + x_3\omega^2). \tag{5}$$

其中 x_1, x_2, x_3 表示原方程的3个不同的根. 由于对于3个数的不同排列方式一共有6种, (5)式给出了方程(3)的所有6个根.

改变一组有序的数的顺序叫做“置换”. 比如, 把 $(1,2,3)$ 换为 $(3,2,1)$, 如果用数学记号来描述, 这个置换就是

$$\sigma(1)=3, \quad \sigma(2)=2, \quad \sigma(3)=1.$$

一般而言, 给定一个集合 $S=\{a_1, a_2, \cdots, a_n\}$, 在此集合上的一个置换就是一个一一对应 $\sigma: S \to S$. 所有的置换构成的集合是一个群 (Group), 叫做 S 的“对称群”, 记为 S_n.

在拉格朗日的时代还没有群的概念, 但他发现了: 跟到置换在求解代数方程中的作用. 用现代的语言讲,

$$y^3=\frac{1}{27}(x_1+x_2\omega+x^3\omega^2)^3$$

在 S_3 的作用下只取两个不同的值, 因此 $r=y^3$ 应当满足一个2次方程.

对于一般的 n 次方程

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

拉格朗日证明(假设方程没有重根): 如果 $\phi(x_1, x_2, \ldots, x_n)$ 是方程的根的一个有理函数, 它在根的所有置换下取 r 个值, 那么这 r 个值是一个 r 次代数方程的根. 而该方程的系数由 $a_1, a_2, \ldots, a_n$ 确定.

拉格朗日实际上开辟了一条研究求解代数方程的新路, 但是他没有找到求解一般5次或更高次方程的方法. 他猜测不存在求解一般高次方程的代数方法. 这个猜测不久便被证明了.

3 Ruffini-Abel 定理

所谓 Ruffini-Abel 定理就是, 5次或5次以上的代数方程一般不能“根式求解” (not solvable by radicals). 根式求解的意思是, 用四则运算和开方运算求出方程的解.

Paolo Ruffini (1765–1822), 意大利数学家兼医生, 在拉格朗日工作的影响下试图证明5次代数方程一般不能根式求解. 他的工作发表于1799年, 宣布他证明了这个命题. 在他的著作中, 他第一次研究了 S_5 的群伦性质, 当时还没有群和群论的概念, 对于具体的群 S_5 他发明了这些概念, 如子群和子群的指数. 但是, 在他对5次代数方程一般不能根式求解的证明中含有一个漏洞, 因为他没有证明地利用了一个关键命题, 这个命题现在被称为 *Abel 定理*.

Niels Henrik Abel (1802–1829) 是著名的挪威数学家. 他在1825年的论文中证明了5次代数方程一般不能根式求解. 所谓 Abel 定理如下:

定理(Abel 定理)**.** 如果一个代数方程有根式解, 则根可以表示成一种形式, 在其中被开方的项是方程的根和单位根的有理函数.

4 Galois 理论简介

以下我们将围绕多项式的根式可解问题介绍伽罗华理论, 而不是一般的伽罗华理论. 即使这样, 也不能完全还原伽罗华当时的思路和做法, 伽罗华当时并没有抽象的"域"和"群"的概念. 这些概念是从他的工作中被后人抽象出来的, 而他的思想则被总结和推广为一般的伽罗华理论.

4.1 数域

我们可以吧数域想象成一个由实数或复数构成的集合, $\boldsymbol{F} \subset \boldsymbol{C}$, 满足

(i) $0, 1 \in \boldsymbol{F}$;

(ii) F 关于加、减、乘、除这些运算是"封闭的". 即, 如果 $a, b(\neq 0) \in \boldsymbol{F}$, 则 $a+b$, $a-b$, $a \cdot b$, $a/b \in \boldsymbol{F}$.

常用的数域有: 实数域 $\boldsymbol{R}$、复数域 $\boldsymbol{C}$、有理数域 $\boldsymbol{Q}$. 假定 $\boldsymbol{F}$ 是一个数域 ($\boldsymbol{F} \neq \boldsymbol{C}$), 我们可以在 $\boldsymbol{F}$ 中添加一些不在其中的数 $u_1, u_2, \ldots, u_n$, 而使它"扩张"成一个"扩域", 记为 $\boldsymbol{F}[u_1, u_2, \ldots, u_n]$. $a \in \boldsymbol{F}[u_1, u_2, \ldots, u_n]$ 当且仅当 $a = R(u_1, u_2, \ldots, u_n)$. 这里 R 表示任意一个 n 元有理函数.

我们在考察一个代数方程

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

的时候, 首先要假定它的系数 $a_1, a_2, \ldots, a_n$ 是在一个给定的数域 $\boldsymbol{K}$ 中. (通常 $\boldsymbol{K} = \boldsymbol{Q}$, 一般有 $\boldsymbol{K} = \boldsymbol{Q}[a_1, a_2, \ldots, a_n]$.) 一般来说, 方程的根不在系数域中. 比如, 设系数是有理数, 当 $n = 2$ 时, $a_1 = b$, $a_2 = c$,

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2},$$

一般不是有理数, 但是根属于 $\boldsymbol{Q}[\sqrt{b^2-4c}]$. 此外, 被开方的项 b^2-4c 还是根的函数:

$$b=-(x_1+x_2),\quad b^2-4c=(x_1+x_2)^2-4x_1x_2.$$

4.2 数域的自同构

设 $\boldsymbol{F}$ 是一个数域. F 的一个自同构是一个1–1对应 $\sigma\colon \boldsymbol{F}\to\boldsymbol{F}$, 它"保持"域的运算, 即对任意的 $a,b\in\boldsymbol{F}$,

$$\sigma(a\pm b)=\sigma(a)\pm\sigma(b),\quad \sigma(ab)=\sigma(a)\sigma(b),\quad \sigma(a/b)=\sigma(a)/\sigma(b).$$

容易验证, 若 σ_1 和 σ_2 是自同构, 则它们的复合 $\sigma_1\circ\sigma_2$ 也是. 由此不难看出, $\boldsymbol{F}$ 的所有自同构构成一个群, 其乘法运算就是复合, 单位元素就是恒同同构.

4.3 多项式的 Galois 群

考虑一个有理系数的多项式 $f(x)$, 它的根是 $x_1,x_2,\ldots,x_n$. 令

$$\boldsymbol{F}=\boldsymbol{Q}[x_1,x_2,\ldots,x_n],$$

则 $\boldsymbol{F}$ 是包含 f 的所有根的最小数域, 称为 f 的"分裂域" (splitting field). f 的伽罗华群是 $\boldsymbol{F}$ 的自同构群的一个子群, 这个子群是由所有保持有理数域 $\boldsymbol{Q}$ 不变的所有自同构组成. 通常记伽罗华群为 $G=\boldsymbol{Gal}(\boldsymbol{F}/\boldsymbol{Q})$.

看一个简单的例子, $f=x^2-2$. 显然, 分裂域 $\boldsymbol{F}=\boldsymbol{Q}[\sqrt{2}]$. 另一方面, 由自同构的定义我们知道自同构必须把根变到根, 因为如果 $f(a)=0$, 则 $f(\sigma(a))=\sigma(f(a))=\sigma(0)=0$. 即 $\sigma(a)$ 也是根. 所以, 若 $\sigma\in\boldsymbol{Gal}(\boldsymbol{F}/\boldsymbol{Q})$, 则必有

$$\sigma(\sqrt{2})=\pm\sqrt{2}.$$

另一方面, 上式也唯一确定了 σ 本身, 因为 $\boldsymbol{F}$ 的任何一个元素都具有形式 $\phi(\sqrt{2})$, 其中 ϕ 是一个系数为有理数的有理函数. 因此, 我们可以把 $\boldsymbol{Gal}(\boldsymbol{F}/\boldsymbol{Q})$ 等同于2个元素的置换群 S_2. 它只有两个成员

$$(1,2),\quad (2,1).$$

这个例子有一般性, 即多项式的伽罗华群是它的 n 个根的对称群 S_n 的一个子群.

4.4 根式的扩张域

对于高次多项式, 分裂域及其伽罗华群是不容易确定的. 伽罗华的想法是, 通过逐次构造扩张域, 每次只添加一个数, 对分裂域进行分解. 在这个过程中也对伽罗华群进行分解. 而如果多项式是可以用根式解出的, 这个分解就可以揭示伽罗华群必须满足的某些性质. 所以他的着眼点是找出根式可解的必要条件.

设 $\boldsymbol{F}$ 是多项式 f 的分裂域, 称 $\boldsymbol{F}$ 是"根式扩张域", 如果存在一串 $\boldsymbol{F}$ 的子域

$$\boldsymbol{Q} = \boldsymbol{F}_0 \subset \boldsymbol{F}_1 \subset \boldsymbol{F}_2 \subset \cdots \subset \boldsymbol{F}_m = \boldsymbol{F}, \tag{6}$$

满足: 对 $i = 0, 1, 2, \ldots, m-1$ 存在 $\alpha_i \in \boldsymbol{F}$ 和自然数 n_i 使

(i) $\boldsymbol{F}_{i+1} = \boldsymbol{F}_i[\alpha_i]$;

(ii) $\alpha_i^{n_i} \in \boldsymbol{F}_i$.

由根式可解的定义不难看出, 若 $\boldsymbol{F}$ 是根式扩张域, 则 f 是根式可解的. 进一步可证, 逆命题也成立.

定理. *多项式 f 是根式可解的当且仅当它的分裂域是根式扩张域.*

4.5 可解群

在分裂域 $\boldsymbol{F}$ 是根式扩张域的时候, 对应于(6)有伽罗华群 $\boldsymbol{Gal}(\boldsymbol{F}/\boldsymbol{Q})$ 的一串子群:

$$\boldsymbol{Gal}(\boldsymbol{F}/\boldsymbol{Q}) = G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{I\}.$$

称 G 是"可解群"如果对每个 $i = 1, 2, \ldots, m$, G_i 是 G_{i-1} 的"正规子群"; 而且"商群" G_{i-1}/G_i 是"循环群".

对于 G 的一个子群 H 和 $g \in G$, 我们有"左陪集" $gH = \{gh | h \in H\}$ 和"右陪集" $Hg = \{hg | h \in H\}$. H 是正规子群当且仅当

$$gH = Hg, \quad \forall g \in G.$$

由于这个性质, 我们可以定义两个陪集之间的乘法

$$g_1 H \cdot g_2 H = (g_1 g_2) H.$$

所有的陪集在这个乘法下构成一个群, 叫做 G 对于 H 的“商群”, 记作 G/H.

一个 p 阶循环群是一个有 p 个元素的群, 它有一个生成元 a, 其它元素都是 a 的幂次, 而 $a^p = e$.

伽罗华证明了以下定理

定理. *一个多项式 f 根式可解当且仅当它的伽罗华群是可解群.*

对于任意给定的方程, 没有计算它的伽罗华群的一般方法. 但是, 用构造的办法, 我们可以构造出 n 次方程, 使得它的伽罗华群是对称群 S_n. 另一方面, 可以证明当 $n \geq 5$ 时, S_n 不是可解的. 因此, 在次数大于等于5的情形, 存在不能用根式求解的代数方程. 因此, Ruffin–Abel 定理可以看着是伽罗华理论的一个推论.

伽罗华理论在现代数论中有重要的应用. 在 Wiles 证明 Taniyama–Shimura 猜想, 从而完成费尔马大定理的证明工作中, 伽罗华理论起来非常重要的作用.

5 小结

伽罗华可以说是数学史上的一个奇迹. 他15岁才开始学习数学, 18岁就做出了重大发现, 向法国科学院递交了关于代数方程求解的论文. (即使按最终修改稿完成的日期算, 他也只有20岁.) 他对于代数方程根式求解问题的深入研究引导他发现了现代群论的最基本而重要的概念, 并且应用群论于代数方程根式求解问题, 得到了完整的解答. 应当说, 他的思想对于代数学是革命性的, 对现代数学的许多方面有深刻的影响.

群论在现代数学中具有非常重要的地位, 它是描述各种数学对象对称性的主要工具. 而对称性在数学和其它科学中是无处不在的, 在代数、几何、分析的许多问题中存在, 也在理论物理的各种模型中存在, 甚至在生命科学中经常出现.