对一般五次方程没有根式解问题的重新认识

梅 晓 春

理论物理与纯粹数学部 福州原创物理研究所

内容摘要 本文证明，阿贝尔和伽罗华关于五次方程没有根式解的证明是无效的。由于阿贝尔和伽罗华的工作，数学界普遍认为一般的五次以及五次以上代数方程没有根式解。然而近年来汤健儿等人证明，某些特殊形式的五次方程存在根式解，阿贝尔和伽罗华的理论无法解释这种结果。另一方面，历史上高斯等人用多种方法证明了代数基本定理。该定理认为任何 n 次代数方程都有 n 个解，就不能排除存在根式解，因此代数基本定理与阿贝尔和伽罗华的理论是有矛盾的。由于以上原因，有必要对阿贝尔和伽罗华的证明进行重新审查。本文仔细分析了阿贝尔的原始论文，发现存在严重的错误。为了证明他的代数方程一般解对三次方程有效，阿贝尔把三次方程的解当做前提，来计算他提出的方程解的参数，因此他的证明是一个逻辑循环论证。阿贝尔还把代数方程的变量和系数（常数）混为一谈，把一个有 14 项的展开式写成 7 项，遗漏了 7 项，因此阿贝尔的证明不成立。伽罗华的理论与其说是证明，不如说是假说。伽罗华根据 S_5 置换群没有真正规子群，断言五次方程没有根式解，但这两个问题实际上没有必然的逻辑关联。为了证明自同构扩域群对三、四次方程的有效性，伽罗华理论实际上用方程的根的某些代数关系，来代替方程的根本身。这违背自同构算符的原始定义，不但概念混肴，而且引入任意性。本文还证明，对于一般的三次和四次代数方程，实际的求解过程不满足伽罗华可解群的塔式结构。其预解式关系也不存在伽罗华可解群的对称性，用可解群理论来判断高次方程是否有根式解是无效的。本文的结论是，n 次代数方程的根与系数之间只存 S_n 置换对称性，不存在伽罗华的可解群对称性，伽罗华实际上并没有证明高次方程无根式解。数学家需要摆脱阿贝尔和伽罗华理论的约束，继续寻找高次代数方程的一般根式解。

关键词 五次方程，根式解，阿贝尔，伽罗华，高斯定理，拉格朗日预解式，扩域，自同构算符

一 前言

所谓的五次方程求根式解问题，通俗地说就是找到一个通用的公式，将任意五次方程的解用方程的系数的根号形式统一地表示出来。在公元 7 世纪，人们就已经知道如何解二次方程。经过历代数学家的努力，三次和四次方程的一般解在四百多年前也找到了。但求五次和五次以上代数方程（以下简称高次方程）的一般解却至今是个大难题。尽管对于某些特殊形式的五次方程，也找到一些特殊解。

历史上欧拉、达朗贝尔，拉格朗日和高斯等人都做过努力，试图求五次方程解，却都没有成功。1824 年阿贝尔发表文章，证明五次方程没有一般的解【1】。继阿贝尔之后，伽罗华利用群论证明了相同的结果【2】。伽罗华给出一般代数方程的可解性判别准则，其证明被认为是更一般、更严格的。至此，这个著名的问题被认为得到完美的解决，此后大多数数学家都不再考虑这个问题。

原文发表于 Advance in Pure Mathematics, 2020, No.10, 508-539, doi: 10.4236/apm.2020.109032 Sep.14

阿贝尔的论文实际上是证明一般的五次方程没有解，而不是证明没有根式解。伽罗华引入了根式扩域概念，把求解五次方程问题转化为五次方程是否有根式解的问题。阿贝尔和伽罗华的说法有细微的差别，但伽罗华的说法往往会导致误解。五次方程没有根式解是一种技术性的说法，更准确的说法应当是，我们找不到一个通式，来描述一般五次方程的解。

另一方面，按照高斯代数学基本定理，任何一元 n 次方程有 n 个解，因此一定可以将方程写成：

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0$$

$$=(x-x_1)(x-x_2)(x-x_3)\cdots(x-x_n)=0 \qquad (1)$$

其中 $a_1,a_2,\cdots a_n\in Q$ 是有理数，$x_1,x_2,\cdots x_n$ 是方程的根。如果我们加上一条限制，假设方程（1）是所谓的 Q 上不可约的，即方程没有有理数解，按照代数基本定理它仍然有解，就一定存在无理数和复数解。

然而，按照阿贝尔和伽罗华的理论，如果 $f(x)$ 是 Q 上不可约的五次方程，它就没有根式解。也就是说我们不能用系数 $a_1,a_2,\cdots a_n$ 的根号形式把方程解 $x_1,x_2,\cdots x_n$ 来表示，即 x_i 一般不能写成 $\sqrt{a_k+\sqrt{a_i}}$ 和 $\sqrt[5]{a_i+\sqrt{a_j}+\sqrt[3]{a_k}}$ 之类的形式。考虑到复数 $z=a+ib=|z|e^{i\theta}$ 的绝对值 $|z|=\sqrt{a^2+b^2}$ 也是用根号来表示的，没有根式解实际上也排除了存在复数解的可能性（如果 $|z|$ 是一个无理数）。

因此高次方程没有根式解的结论是很奇怪的。众所周知，已知的数域分为有理数，无理数，复数和超越数。所谓的没有根式解，实际上意味着方程的根不可能是无理数。由于我们已经约定 $f(x)$ 在 Q 上不可约，即方程的解不可能是有理数，考虑到超越数不可能是代数方程的根，如果不可能用根号形式表示，就只剩下不含根号的复数这种可能性了。

此外，数学上已证明，代数方程的复数根具有共轭性，任何一个奇数次的实系数多项式方程至少有一个实数根【3】。五次方程有四个复数根和一个实数根，或者有两个复数根和三个实数根。如果这些实根即不是有理数，也不是无理数，更不可能是超越数，又会是什么数呢？

显而易见，高次方程没有根式解的结论与代数学基本定理是互相矛盾的，二者中必有一个是错误的。高斯本人曾提出三，四种方法来证明代数定理，高斯之后有更多的人研究这个问题，至今为止已经有一百多种证明【4】。这说明代数基本定理是可靠的，因此高次方程没有根式解的论断是值得怀疑的，需要做进一步的深究。

本世纪以来，求解五次方程的研究获得一些重要的进展。上海财经大学应用数学系教授汤健儿2012年1月在《高等数学研究》上发表文章，证明有五类特殊的五次方程存在根式解【5】。盛兴平、范军和孔志宏也做了类似的工作【6】【7】。郑良飞（石泉）则用特殊方法，解出大量的数字系数五次方程【8】。用阿贝尔理论和伽罗华理论，无法解释这些结果。考虑到五次方程的求解是代数学中最基本的大问题之一，笔者认为有必要对阿贝尔和伽罗华的证明进行重新审查。

本文的研究发现，阿贝尔关于五次方程没有根式解的证明是不成立的。阿贝尔的计算中存在逻辑混乱和基本概念错误，导致他的文章难以理解。他提出的代数方程的解的基本形式与三次和四次方程的解的形式不符合，没有理由认为五次方程的解会具有阿贝尔提出的形式。

尽管伽罗华的群论是数学上的一个伟大的发现，但他的可解群理论仍然没有解决高次方程的可解性问题。伽罗华的理论与其说是证明，不如说是假设。伽罗华根据五次方程的 S_5 置换群没有真正规子群，来证明五次方程没有根式解。然而没有真正规子群不等于方程没有根式解，二者之间没有必然的逻辑关联。伽罗华的根式扩域理论与实际的解方程过程也是不匹配的。

本文的更详细内容要点如下：

1. 介绍汤健儿的计算方法和两个特殊五次方程的根式解。比如对（1）式中 $a_5=1$，$a_4=a_2=0$，$a_3^2=5a_1$ 的情况，汤健儿给出的五次方程的解与三次方程的解有类似的结构。汤健儿计算的这五类方程满足的 S_5 置换群，没有真正规子群，不存在伽罗华可解群，但它们仍然有根式解。

2. 分析阿贝尔关于五次方程没有根式解的证明，指出其中存在的严重的错误。为了证明他提出的一般代数方程的解的形式对三次方程有效，阿贝尔把三次方程的解当成前提来计算他的方程的参数。因此阿贝尔的证明是一个逻辑循环论证，没有意义。

3. 阿贝尔在计算中把方程的变量和常数系数混为一谈，一个有 14 项的展开式被写成 7 项，遗漏了 7 项。本文证明三次方程和四次方程的解都不满足阿贝给出的形式，没有理由认为高次方程的解也能满足阿贝尔提出的形式。

4. 伽罗华的可解群理论牵强附会，其结论与前提是相互矛盾的。伽罗华理论承认方程的根和系数的对称性可以用置换群 S_n 来描述。只是由于 S_5 群是单群，没有真正规子群，就认为不可能有根式解。然而这样的论证是理由不充分的。既然认为根和系数的对称性可以用置换群 S_5 来描述，实际上已经承认方程的解是存在的，只不过这个解没有真正规子群的对称性罢了。

5. 伽罗华理论用根式扩域自同构映射的方法来构建伽罗华群。自同构映射群算符的作用是将代数方程的根变成相同方程的其他根，或保持根自身不变。然而为了证明这种方法对三、四次方程有效，在实际计算过程中，伽罗华理论却是用方程的根之间的某种代数关系来代替方程的根本身。这不但是偷换概念，而且引入任意性，导致唯一性被破坏。

6. 伽罗华的根式扩域理论与实际的解方程过程不匹配，实际的解方程过程并不遵守伽罗华群的塔式结构。解高次方程的过程不是通过对多重根式一层一层地进行添加来进行的，而是可以按照 S_n 置换群的降阶过程来进行的。对 n 次方程，先找的一个解，原方程降为 $n-1$ 次方程，根与系数的对称性降低到 $S_{n\text{-}1}$。因此实际的解方程过程与伽罗华可解群的塔式结构无关，伽罗华根式扩域理论只是一个形式上的东西，没有实际意义。

7. 一般的三次和四次方程的预解式只能部分地满足可解群的对称性，不能满足全部的对称性。比如对于三次方程，预解式关系只对 S_3 群的正规子群 A_3 的 (123) 置换保持不变，不能对 (132) 置换保持不变。

总之，代数基本定理证明高阶方程一般解的存在，汤健儿等人已经明确地找到一些特殊的五次方程的根式解。伽罗华理论并没有对这类特殊方程给出限制，证明它们是伽罗华可解群的例外。n 次代数方程的根与系数之间只存 S_n 置换对称性，不存在伽罗华的可解群对称性。

因此，数学家有必要摆脱阿贝尔和伽罗华理论的约束，继续寻找高次代数方程的一般根式解。

二 某些特殊的五次方程的根式解

盛兴平最早给出一元四次方程的矩阵解法【6】。受到盛兴平的启发，范军和孔志宏用这种方法求解三类特殊的实系数一元六次方程【7】。该方法将六次方程降阶为三次方程，从而可以直接求解，但这种方法不能用来求解五次方程。

按照这种方法，汤健儿提出用五个变量代替原方程的单个变量，给出五类特殊的五次方程的根式解，具有一般的意义。将一元五次方程写成以下形式：

$$x^5+px^3+qx^2+rx+s=0 \qquad (2)$$

将五次分圆方程$\zeta^5-1=0$的单位根写为：

$$\zeta=e^{i2\pi/5}=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5} \tag{3}$$

引入变数y,z,u,v，利用五阶循环行列式，汤健儿证明存在以下恒等式【5】：

$$x^5+px^3+qx^2+rx+s=\prod_{j=0}^{4}\left(x+\zeta^j y+\zeta^{2j}z+\zeta^{3j}u+\zeta^{4j}v\right) \tag{4}$$

（2）式的系数p,q,r,s与y,z,u,v的关系则为：

$$p=-5(yv+zu) \tag{5}$$

$$q=5(yz^2+zv^2+uy^2+vu^2) \tag{6}$$

$$r=5(yv^2+z^2u^2-y^3z-z^3v-u^3y-v^3u-yzuv) \tag{7}$$

$$s=y^5+z^5+u^5+v^5-5y^3uv-5z^3yu-5u^3zv$$

$$-5v^3yz+5u^2v^2y+5u^2v^2z+5z^2v^2u+5y^2z^2v \tag{8}$$

按照（2）式，（4）式意味着：

$$x+\zeta^j y+\zeta^{2j}z+\zeta^{3j}u+\zeta^{4j}v=0 \tag{9}$$

一元五次方程的 5 个解就是：

$$x_j=-\zeta^j y-\zeta^{2j}z-\zeta^{3j}u-\zeta^{4j}v \qquad j=0,\ 1,\ 2,\ 3,\ 4 \tag{10}$$

如果能从（5）~（8）式中用p,q,r,s来表示y,z,u,v，从（10）式就得到五次方程的五个解。汤健儿在论文中给出五个具体的例子，本文以下引用其中的两个。

（I） 在（2）式中令$q=0$，得到只有奇数次的五次方程：

$$x^5+px^3+rx+s=0 \tag{11}$$

按（6）式，对于$q=0$，可令$y=0$，$v=0$。代入（5），（7）和（8）式，得到：

$$p=-5zu \tag{12}$$

$$r=5z^2u^2 \tag{13}$$

$$s=u^5+z^5 \tag{14}$$

从（12）和（13）式可得$p^2=5r$，从（12）式得到$z=-p/(5u)$，代入（14）式，得到：

$$u^{10}-su^5-\left(\frac{p}{5}\right)^5=0 \tag{15}$$

上式的解是：

$$u^5=\frac{s}{2}\pm\sqrt{\left(\frac{s}{2}\right)^2+\left(\frac{p}{5}\right)^5} \tag{16}$$

取：
$$u=\left[\frac{s}{2}+\sqrt{\left(\frac{s}{2}\right)^2+\left(\frac{p}{5}\right)^5}\right]^{\frac{1}{5}} \tag{17}$$

按照（12）式计算，可得：

$$z=\left[\frac{s}{2}-\sqrt{\left(\frac{s}{2}\right)^2+\left(\frac{p}{5}\right)^5}\right]^{-\frac{1}{5}} \tag{18}$$

因此，在满足（15）式的情况下，（11）式的解（$j=0$）为$x_0=-z-u$，或：

$$x_0=-\left[\frac{s}{2}+\sqrt{\left(\frac{s}{2}\right)^2+\left(\frac{p}{5}\right)^5}\right]^{\frac{1}{5}}-\left[\frac{s}{2}-\sqrt{\left(\frac{s}{2}\right)^2+\left(\frac{p}{5}\right)^5}\right]^{\frac{1}{5}} \tag{19}$$

考虑（14）式，可以直接验证（19）式是（11）式的解，另外四个解则由（10）式确定。

另一方面，对于三次方程：

$$x^3+px+s=0 \tag{20}$$

其解为：

$$x_0=\left[-\frac{s}{2}+\sqrt{\left(\frac{s}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right]^{\frac{1}{3}}+\left[-\frac{s}{2}-\sqrt{\left(\frac{s}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right]^{\frac{1}{3}} \tag{21}$$

因此（19）式是很有趣的，它表明如果五次方程（11）式的系数p和r满足关系$p^2=5r$，其解与三次方程（20）式的解具有相似的结构。

（II）在（2）式中令$p=0$，即：

$$x^5+qx^2+rx+s=0 \tag{22}$$

在（5）式中取$u=v=0$，代入（6）~（8）式，得到：

$$q=5yz^2 \qquad \text{或} \qquad yz^2=\frac{1}{5}q \tag{23}$$

$$r=-5y^3z \qquad \text{或} \qquad y^3z=-\frac{1}{5}r \tag{24}$$

$$s=y^5+z^5 \tag{25}$$

以上三式满足以下关系：

$$\frac{(y^3z)^2}{yz^2}+\frac{(yz^2)^3}{y^3z}=y^5+z^5 \tag{26}$$

利用（23）~（25）式，也可以将（26）式写为：

$$q^4+25qrs-5r^3=0 \tag{27}$$

从（23）和（24）式解出：

$$y=\left(\frac{r^2}{5q}\right)^{1/5} \qquad z=-\left(\frac{q^3}{25r}\right)^{1/5} \tag{28}$$

因此按照（10）式，（22）式的一个解（$j=0$）是：

$$x_0=y+z=\left(\frac{r^2}{5q}\right)^{1/5}-\left(\frac{q^3}{25r}\right)^{1/5} \tag{29}$$

另外四个解也由（10）式确定。可以用一个具体的数值来验证，对于方程：

$$x^5+10x^2+5x-\frac{15}{2}=0 \tag{30}$$

我们有 $p=0$，$q=10$，$r=5$，$s=-15/2$，它们满足（26）式。按照（28）式可得 $y=2^{1/5}$，$z=-8^{1/5}$。按照（29）式得 $x_0=2^{1/5}-8^{1/5}\approx 0.6451$，可以直接验证它满足（30）式。

注意到（19）和（29）式都是用根式来表示方程的解。虽然它们是特殊情况下的解，但阿贝尔和伽罗华的理论无法说明在这种条件下为什么它们可以有解，因此所谓的五次方程没有根式解的结论不成立。

三 阿贝尔的证明简介

3.1 阿贝尔 1824 年的证明

本章内容引用阿贝尔 1824 年的论文第一部分和 1826 年发表的论文，存在的问题在第四章讨论。在 1824 年的论文中，阿贝尔将一般的五次方程写为【1】：

$$y^5-ay^4+by^3-cy^2+dy-e=0 \tag{31}$$

阿贝尔假设（31）式的解可以写成由 a,b,c,d,e 的根式组成的量的函数，具有以下形式：

$$y=p+p_1R^{1/m}+p_2R^{2/m}+\cdots p_{m-1}R^{(m-1)/m} \tag{32}$$

其中 m 是素数，$R,p,p_1,p_2,\cdots$ 是与 y 有相同形式的函数。按照这种方法继续下去，直至得到 a,b,c,d,e 的有理函数。

阿贝尔同时认为，可以用 R/p_1^m 代替 R，令 $p_1=1$，将（32）式简化成：

$$y=p+R^{1/m}+p_2R^{2/m}+\cdots p_{m-1}R^{(m-1)/m} \tag{33}$$

将（33）式代入（31）式，得到：

$$q+q_1R^{1/m}+q_2R^{2/m}+\cdots q_{m-1}R^{(m-1)/m}=0 \tag{34}$$

其中 $q,q_1,q_2\cdots q_{m-1}$ 是 a,b,c,d,e 和 $p,q_2\cdots R$ 的有理函数。然后，阿贝尔采用反证法，证明为了使方程（34）式能够成立，必须有:

$$q=q_1=q_2\cdots=q_{m-1}=0 \tag{35}$$

证明如下：令 $z=R^{1/m}$，考虑（34）式，就得到两个方程：

$$z^m-R=0 \tag{36}$$

$$q+q_1z+q_2z^2+\cdots+q_{m-1}z^{m-1}=0 \tag{37}$$

如果$q,q_1,q_2\cdots q_{m-1}$不等于零，（36）和（37）式必有一个或多个公共根。若这些根的个数为k，就能够找到一个k次方程，其根就是所提及的k个根。令这个方程是：

$$r+r_1z+r_2z^2+\cdots+r_kz^k=0 \tag{38}$$

它的所有根与方程（36）式的根相同，其系数$r,r_1,r_2\cdots r_k$为$R,q,q_1,q_2\cdots q_{m-1}$的有理函数。这个方程的根具有形式$\alpha_\mu z$，$\alpha_\mu$是方程$\alpha_\mu^m-1=0$的一个根。将（38）式的$z$用$\alpha_\mu z$替换，得到$k$个方程：

$$r+r_1z+r_2z^2+\cdots+r_kz^k=0$$

$$r+\alpha r_1z+\alpha^2r_2z^2+\cdots+\alpha^kr_kz^k=0$$

.....

$$r+\alpha_{k-1}r_1z+\alpha_{k-2}^2r_2z^2+\cdots+\alpha_{k-1}^kr_kz^k=0 \tag{39}$$

从这k个方程，总可以得到表示成量$r,r_1,r_2\cdots r_k$的有理函数z的值。由于这些量本身是a,b,c,d,e,R，$p,p_1,p_2\cdots$的有理函数，可以推出z也是这些量的有理函数。然而按照定义$z=R^{1/m}$，z一般不可能是一个有理数，因此导致矛盾。要使（37）式成立，只能得到（35）式的结果。至于（35）式的结果与方程解的基本形式（33）式有什么关系，阿贝尔1824年的文章中没有任何说明。

然后，阿贝尔设$y_1,y_2,y_3,\cdots y_m$代表m次方程的根，α是方程$x^{m-1}+x^{m-2}+\cdots+x+1=0$的根，同时令：

$$y_1=p+R^{1/m}+p_2R^{2/m}\cdots+p_{m-1}z^{(m-1)/m}$$

$$y_2=p+\alpha R^{1/m}+\alpha^2p_2R^{2/m}\cdots+\alpha^{m-1}p_{m-1}z^{(m-1)/m}$$

.....

$$y_m=p+\alpha^{m-1}R^{1/m}+\alpha^{m-2}p_2R^{2/m}\cdots+\alpha p_{m-1}z^{(m-1)/m} \tag{40}$$

在（40）式的基础上，阿贝尔考虑不同的解之间的交换对称性。利用柯西发表在综合工科学校杂志上的一篇文章的结果【9】，阿贝尔声称m不能等于或大于5，由此证明五阶和更高阶代数方程没有根式解。

3.2 阿贝尔1826年的补充证明

在阿贝尔1824年的论文中，没有对公式（33）~（35）式的有效性进行具体计算。在1826年的论文中，阿贝尔对三次方程进行了计算，利用（35）式的关系，得出（33）式有效的结果【10】。证明如下：

对于三次方程，令$c=0$，（31）式变成：

$$y^3+dy-e=0 \tag{41}$$

令$m=3$，（33）式是：

$$y=p+R^{1/3}+p_2R^{2/3} \tag{42}$$

阿贝尔认为，对于三次方程（41）式，应当在（42）式中取 $p=0$，证明如下。方程（41）式的三个根是：

$$y_1=\left[\frac{e}{2}+\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}}+\left[\frac{e}{2}-\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}} \tag{43}$$

$$y_2=\omega\left[\frac{e}{2}+\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}}+\omega^2\left[\frac{e}{2}-\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}} \tag{44}$$

$$y_3=\omega^2\left[\frac{e}{2}+\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}}+\omega\left[\frac{e}{2}-\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}} \tag{45}$$

其中 ω 是三次分圆方程 $y^3-1=0$ 的根，存在关系 $1+\omega+\omega^2=0$。将（43）~（45）式相加，按照韦达公式，得到：

$$(y_1+y_2+y_3)=(1+\omega+\omega^2)\left[\frac{e}{2}+\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}}$$

$$+(1+\omega+\omega^2)\left[\frac{e}{2}-\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3}\right]^{\frac{1}{3}}=0 \tag{46}$$

因此阿贝尔认为对于（42）式，也有：

$$y_1+y_2+y_3=3p+(1+\omega+\omega^2)R^{1/3}+(1+\omega+\omega^2)p_2R^{2/3}=3p=0 \tag{47}$$

由此证明 $p=0$，就可以将（42）式写为:

$$y=R^{1/3}+p_2R^{2/3} \tag{48}$$

将（48）式代入（41）式，并写成（34）式的形式，阿贝尔得到：

$$(R+p_2^3R^2-e)+(3p_2R+d)R^{1/3}+(3p_2^2R+dp_2)R^{2/3}=0 \tag{49}$$

将上式改写成：

$$q+q_1R^{1/3}+q_2R^{2/3}=0 \tag{50}$$

按照（35）式，就应当有：

$$q=R+p_2^3R^2-e=0 \tag{51}$$

$$q_1=3p_2R+d=0 \tag{52}$$

$$q_2=3p_2^2R+dp_2=0 \tag{53}$$

从（52）式得到 $p_2=-d/(3R)$，代入（53）式，右边恰好等于零。将 $p_2=-d/(3R)$ 代入（51）式，得：

$$R^2-eR-(d/3)^3=0 \tag{54}$$

这是一个关于 R 的二次方程，它的两个解是：

$$R_+=\frac{e}{2}+\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3} \qquad R_-=\frac{e}{2}-\sqrt{\left(\frac{e}{2}\right)^2+\left(\frac{d}{3}\right)^3} \tag{55}$$

从 $p_2=-d/(3R)$ 可得：

$$p_2R_+^{2/3}=-\frac{d}{3R_+}R_+^{2/3}=-\frac{d}{3}R_+^{-1/3} \tag{56}$$

方程（54）式的两个根与系数的韦达公式为：

$$R_++R_-=e \qquad R_+R_-=-(d/3)^3 \tag{57}$$

利用（56）和（57）式，就可以将（48）式写成：

$$y=R_+^{1/3}+p_2R_+^{2/3}=R_+^{1/3}-\frac{d}{3}R_+^{-1/3}=R_+^{1/3}+R_-^{-1/3} \tag{58}$$

（58）式与（43）式一样，令 $R_+\to R_1$，$R_-\to R_2$，恰好就是三次方程的解。因此阿贝尔认为，他提出的代数方程一般解的形式对三次方程是正确的。

四 阿贝尔的证明存在的问题

阿贝尔的证明存在概念含糊，逻辑混乱的问题，使他的证明难以理解。以下证明，对于二次方程外，（35）式一般不成立。对三次和四次方程，（33）式不成立的，（35）式更不可能成立，因而（40）式不成立。

Ⅰ) 对于二次方程：

$$y^2-dy+e=0 \tag{59}$$

令 $m=2$，按照（33）式，可以有两种结果：

$$y=p+R^{1/2} \tag{60}$$

和：

$$y=p+R^{1/2}+p_2R+p_1R^{1/2}$$

$$=p+(1+p_1)R^{1/2}+p_2R \tag{61}$$

如果直接解（59）式，结果是：

$$y=\frac{d}{2}\pm\frac{\sqrt{d^2-4e}}{2}=p\pm R^{1/2} \tag{62}$$

其中：

$$p=d/2 \qquad R=(d^2-4e)/4 \tag{63}$$

可知（60）式成立，（61）式不成立，我们只需讨论（60）式。

将（60）式代入（59）式，得到：

$$q + q_1 R^{1/2} + q_2 R = 0 \qquad (64)$$

其中：

$$q = p^2 - dp + e \qquad q_1 = 2p - d \qquad q_2 = 1 \qquad (65)$$

将（63）式的 $p = d/2$ 代入（65）式，得：

$$q = -d^2/4 + e \qquad q_1 = 0 \qquad q_2 = 1 \qquad (66)$$

阿贝尔认为必须有 $q = q_1 = q_2 = 0$，这显然是不成立的，我们有 $q_2 \neq 0$。由于方程系数 d 和 e 是独立的，我们可以有 $d \neq 2\sqrt{e}$，因此一般而言 $q \neq 0$。对于二次方程，阿贝尔推导的（35）式不成立。

II) 对于三次方程，阿贝尔的（35）式是显然是不可能的。将（49）式展开，一共有 7 项，结果是：

$$-e + dR^{1/3} + dp_2 R^{2/3} + R + 3p_2 R^{4/3} + 3p_2^2 R^{5/3} + p_2^3 R^2 = 0 \qquad (67)$$

将（42）式代入（41）式，进行同类项合并后，实际的结果是：

$$q' + q_1' R^{1/3} + q_2' R^{2/3} + q_3' R + q_4' R^{4/3} + q_5' R^{5/3} + q_6' R^2 = 0 \qquad (68)$$

其中：

$$q' = p^3 + dp - e \qquad q_1' = 3p^2 + d \qquad q_2' = 3p + 3p^2 p_2 + dp_2$$

$$q_3' = 1 + 6pp_2 \qquad q_4' = 3p_2 + 3pp_2^2 \qquad q_5' = 3p_2^2 \qquad q_6' = p_2^3 \qquad (69)$$

因此（68）式实际上有 14 项，阿贝尔的（49）和（67）式漏掉了包含 p 的另外 7 项。将（68）式写成（42）式的形式，结果是：

$$(q' + q_3' R + q_6' R^2) + (q_1' + q_4' R) R^{1/3} + (q_2' + q_5' R) R^{2/3} = 0 \qquad (70)$$

按照（35）式，就得到三个方程：

$$q = q' + q_3' R + q_6' R^2 = p^3 + dp - e + (3p^2 + d) R + p_2^3 R^2 = 0 \qquad (71)$$

$$q_1 = q_1' + q_4' R = 3p^2 + d + 3p_2 (1 + pp_2) R = 0 \qquad (72)$$

$$q_2 = q_2' + q_5' R = 3p + 3p^2 p_2 + dp_2 + 3p_2^2 R = 0 \qquad (73)$$

(71)，（72）和（73）式是关于未知变量 R，p 和 p_2 的三元三次方程组，其形式比（41）式复杂得多。假设我们能够解这个方程组，得到的结果是 $R = R(d,e)$，$p = p(d,e)$，$p_2 = p_2(d,e)$。由于系数 d 和 e 是任意的，一般而言有 $p(d,e) \neq 0$。因而一般有 $p_2 \neq -d/(3R)$，也就不可能有（54）和（55）式，三次方程的解一般不可能具有（42）式的形式。在一般情况下，我们有 $q \neq 0$，$q_1 \neq 0$，$q_2 \neq 0$。对于三次方程，阿贝尔的证明（35）式不成立。

可以看出，阿贝尔对(47)式的证明是一个循环论证，他把需要证明的结果当作前提。（47）式意味着存在以下关系：

$$y_1 = p + R^{1/3} + p_2 R^{2/3} \qquad (74)$$

$$y_2 = p + \omega R^{1/3} + \omega^2 p_2 R^{2/3} \tag{75}$$

$$y_3 = p + \omega^2 R^{1/3} + \omega p_2 R^{2/3} \tag{76}$$

将以上三式相加，就得到（47）式。然而，阿贝尔需要先证明，（75），（75）和（76）也是三次方程的解，但他并没有做出证明。他的做法实际上是令（43）和（48）式相等，得：

$$p + R^{1/3} + p_2 R^{2/3} = R_1^{1/3} + R_2^{1/3} \tag{77}$$

然后在上式中直接令 $R^{1/3} = R_1^{1/3}$ 和 $p_2 R^{2/3} = R_2^{1/3}$，就得到 $p = 0$ 的结果。显然，这样的证明是没有意义的。

除此之外，阿贝尔还将方程的自变量与系数混为一谈。在三次方程（41）式中，y 是一个未知的自变量，通过解方程可以将它表示成系数 d, e 的函数。用（42）式来表示 y 后，自变量就变成 $R^{1/3}$。因此（42）式中的 p, p_2 应当是 d, e 的函数，不可能包含 R。这是解代数方程需要遵守的基本规则，否则会引起混乱，导致严重的错误。

III) 对于四次方程：

$$y^4 + by^3 + cy^2 + dy + e = 0 \tag{78}$$

按照（33）式，取 $m = 4$，阿贝尔的解可以写为：

$$y = p + p_1 R^{1/4} + p_2 R^{2/4} + p_3 R^{3/4} \tag{79}$$

另一方面，令：

$$\Delta_1 = c^2 - 3bd + 12e \qquad \Delta_2 = 2c^3 - 9bcd + 27d^2 + 27b^2 e - 72ce \tag{80}$$

$$\Delta = \frac{2^{1/3}\Delta_1}{3[\Delta_2 + \sqrt{-4\Delta_1^3 + \Delta_2^2}]^{1/3}} + \frac{[\Delta_2 + \sqrt{-4\Delta_1^3 + \Delta_2^2}]^{1/3}}{3 \times 2^{1/3}} \tag{81}$$

（78）式的四个解可以写为【11】：

$$y_1 = -\frac{b}{4} - \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} + \Delta} - \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} - \Delta - \frac{-b^3 + 4bc - 8d}{4\sqrt{b^2/4 - 2c/3 + \Delta}}}$$

$$y_2 = -\frac{b}{4} - \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} + \Delta} + \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} - \Delta - \frac{-b^3 + 4bc - 8d}{4\sqrt{b^2/4 - 2c/3 + \Delta}}}$$

$$y_3 = -\frac{b}{4} + \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} + \Delta} - \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} - \Delta - \frac{-b^3 + 4bc - 8d}{4\sqrt{b^2/4 - 2c/3 + \Delta}}}$$

$$y_4 = -\frac{b}{4} + \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} + \Delta} + \frac{1}{2}\sqrt{\frac{b^2}{4} - \frac{2c}{3} - \Delta - \frac{-b^3 + 4bc - 8d}{4\sqrt{b^2/4 - 2c/3 + \Delta}}} \tag{82}$$

令 $p = -b/4$，$p_1 = p_2 = 1/2$ 以及

$$R_1 = \sqrt{\frac{b^2}{4} - \frac{2c}{3} + \Delta} \tag{83}$$

$$R_2=\sqrt{\frac{b^2}{4}-\frac{2c}{3}-\Delta-\frac{-b^3+4bc-8d}{4\sqrt{b^2/4-2c/3+\Delta}}} \tag{84}$$

由于 R_1 和 R_2 包含对 b,c,d,e 四则运算的开方 Δ，它们都不是 b,c,d,e 的有理函数。更重要的是，R_1 和 R_2 不具有对称性。（82）式可以简写为:

$$y_1=p-p_1R_1^{1/2}-p_2R_2^{1/2} \qquad y_1=p-p_1R_1^{1/2}+p_2R_2^{1/2}$$

$$y_3=p+p_1R_1^{1/2}-p_2R_2^{1/2} \qquad y_1=p+p_1R_1^{1/2}+p_2R_2^{1/2} \tag{85}$$

另一方面，取 $m=4$，（40）式则变成：

$$y_1=p+p_1R^{1/4}+p_2R^{2/4}+p_3R^{3/4}$$

$$y_2=p+p_1\alpha R^{1/4}+p_2\alpha^2R^{2/4}+p_3\alpha^3R^{3/4}$$

$$y_3=p+p_1\alpha^2R^{1/4}+p_2\alpha^3R^{2/4}+p_3\alpha R^{3/4}$$

$$y_4=p+p_1\alpha^3R^{1/4}+p_2\alpha R^{2/4}+p_3\alpha^2R^{3/4} \tag{86}$$

（86）式与（85）式是不一样的。因此对于四次方程，阿贝尔假设的解（33）和（40）式也不成立。事实上，阿贝尔的证明要求（32）式中 m 是素数，因此我们至少可以认为，阿贝尔的证明不具有普遍性，因为它对最高项 $m>2$ 偶数次方程都不适合。

V) 由于（33）式对三次和四次方程都不成立，对于一般的五次和五次以上方程，我们没有理由认为其解可以用（33）和（40）式表示。可以想象的是，五次方程的解的形式会比四次方程复杂的多。二次方程，三次方程和四次方程的解的基本形式都不一样。因此五次方程的根式解的基本形式是难以预测的，除非我们通过解方程真正地得到它。

VI) 阿贝尔导出的（36）和（37）式也是有问题的。（36）式实际上是定义，或者说是一个恒等式，其中的 z 和 R 都是未知的量。作为一个有意义的方程，必须同时包含已知量和未知量。通过方程，我们用已知量来表示未知量，但（36）式不是这样的方程。

阿贝尔认为（36）和（37）式有共同的根，这里存在概念的混肴。事实上，（37）式只不过是（34）式利用了（36）式的变数替换。通过求解（37）式，我们可以确定 z，等于确定了 R。因此（37）可以独立求解，根本不需要（36）式。将它们进行联合求解没有意义，（38）和（39）式不存在。

因此一般而言，（33），（34）和（35）式都不成立，阿贝尔 1824 年文章的第一部分是错误的。阿贝尔文章第二部分的证明建立在（33）和（40）式的基础上，其推导就没有意义，本文不再讨论。

五 伽罗华理论简介

5.1 一般代数方程的系数与根的对称性

对于一般的 n 次代数方程，可以将它写为首系数为 1 的形式，即令：

$$f(x)=x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0=0 \tag{87}$$

其中系数 $a_i\in Q$ 一般为有理数。按照高斯代数基本定理，存在 n 个根 $x_1,x_2\cdots x_n$，就可以将（87）

式改写为：

$$(x-x_n)(x-x_{n-1})(x-x_{n-2})\cdots(x-x_1)=0 \qquad (88)$$

将（88）式的连乘展开并与（87）式进行比较，得到方程根与系数的关系，即韦达公式【12】：

$$x_1+x_2+x_3\cdots+x_n=-a_{n\text{-}1}$$

$$x_1x_2+x_1x_3+\cdots+x_1x_n+x_2x_3+x_2x_4\cdots=a_{n-1}$$

.....

$$x_1x_2x_3\cdots x_n=(-1)^n a_0 \qquad (89)$$

以上诸式的右边是常数，将左边的$x_1,x_2\cdots x_n$进行任意代换，比如令$x_1\Leftrightarrow x_2$，或$x_i\Leftrightarrow x_k$，结果是不变。用置换群的语言，n次代数方程的根与系数间存在S_n置换对称性。

5.2 伽罗华可解群G_n

伽罗华理论通过引入根式扩域概念，将S_n置换对称性变成伽罗华根式扩域群的塔式结构对称性，在此基础上讨论高次方程的根式解问题。伽罗华定理认为，一个代数方程可根式解的充要条件是，该方程对应的伽罗华群是可解群。可解群的定义如下【12】。设S_n是一个有限的置换群，且存在的一个正规子群系列：

$$S_n\sim G_n\geq G_1\geq G_2\cdots\geq G_r=I \qquad (90)$$

其中I是群的单位元，G_{i+1}是G_i的正规子群。如果系列中每个商群G_i/G_{i+1}都是可交换群，则称该系列为可解群系列，G_n就称为可解群。按照伽罗华理论，（90）式的正规子群塔式结构等价于将（87）式分解成（88）式的各个单项相乘形式。

由于五次方程对应的S_5置换群是单群，它没有真正规子群，不存在（90）式的塔式分解，不是可解群，伽罗华就认为五次方程没有根式解。由于$n>5$时S_n群都有S_5的子群，因此伽罗华认为五次以上方程也不存在根式解。

5.3 伽罗华根式扩域理论

为了能将可解群理论应用于代数方程的求解，需要引入根式扩域理论【12】【13】。需要指出的是，伽罗华最初的文章中并没有真正用到根式扩域的概念，但存在这种思想。严格的根式扩域理论，以及本文引用的扩域理论的大多实际应用，都是后人对其理论进行完善的结果。作为数域的概念，扩域还需要满足某些规则，本文就不赘述。

用伽罗华理论讨论的，一般是$Q(a_i)$上不可约多项式。方程的求根过程被认为是根域的扩张过程，或者说是在$Q(a_i)$中逐步添加方程的根的过程。假设通过解方程得到一个非有理数解，例如$x_1\sim\sqrt{b}$。将它加入$Q(a_i)$，变成$Q(a_i,\sqrt{b})$，就把$Q(a_i,\sqrt{b})$称为$Q(a_i)$的扩域。继续解方程，得到多重根，比如$x_2\sim\sqrt{g+\sqrt{b}}$，根域被再次扩大为$Q(a_i,\sqrt{b},\sqrt{g+\sqrt{b}})$，如此等等。最后得到方程的所有根$x_1,x_2,\cdots x_n$，根域就用$E=E(x_1,x_2,\cdots x_n)$来表示。

按照伽罗华理论，如果一个方程能够进行根式扩域，就认为有根式解。如果不能进行根式扩域，就认为没有根式解。五次方程被认为无法进行根式扩域，就没有根式解。

5.4 根式扩域自同构映射群 $GalE/Q$

引入根式扩域概念后，为了与置换群建立关系，还需要引入根式扩域自同构映射概念。在此基础上建立自同构群 $GalE/Q$。然后通过伽罗华对应定理，将 $GalE/Q$ 群与可解群 G_n 对应，或者说用 G_n 代替 $GalE/Q$。通过考察 G_n 是否具有塔式结构，来证明高次方程是否有根式解。因此根式扩域自同构映射是伽罗华理论的核心概念，是理解伽罗华理论的关键，我们有必要搞清楚这里的逻辑关系。

自同构映射用符号 σ 表示，它不改变代数方程中的系数，但将方程的根变为相同方程的其他根，或者保持原来的根不变【12】。设 x_i 是（87）式的一个根，即 $f(x_i)=0$。令 E 是方程的根域，定义：

$$\sigma(x_i)=x_j \mid \ x_i,x_j\in E \tag{91}$$

则有：

$$\sigma f(x_i)=\sum_{k=1}^{n}a_k\sigma(x_i^k)=\sum_{k=1}^{n}a_k(\sigma x_i)^k=\sum_{k=1}^{n}a_kx_j^k=0 \tag{92}$$

按照这种方式，如果方程的根已知，就可以得到算符 σ 的具体形式。同时证明自同构映射成群，称为根式扩域的伽罗华自同构群，用 $GalE/Q$ 表示。

通过复杂的论证过程，可以证明自同构群 $GalE/Q$ 与置换群 S_n 等价【12】。更繁复的论证证明，$GalE/Q$ 与 S_n 的某些子群 G_n 等价（比如 S_3 的正规子群 A_3）【13】。我们无法在此复述这种证明，但对于一些简单的情况，可以用实例来说明。

比如对最简单的二次方程:

$$f(x)=x^2+ax+b=0 \tag{93}$$

它的两个根是：

$$x_1=\frac{1}{2}(-a+\sqrt{a^2-4b}) \qquad x_2=\frac{1}{2}(-a-\sqrt{a^2-4b}) \tag{94}$$

根式扩域过程为 $Q(a,b)\to Q(a,b,\sqrt{a^2-4b})$。设 I 是恒等变换，群元(12)代表置换 $x_1\leftrightarrow x_2$，则有 $\sigma\sim S_2=\{I,(12)\}$。显然，$GalE/Q$ 与 S_2 等价。

再比如对于四次方程：

$$f(x)=(x^2-a)(x^2-b)=0 \tag{95}$$

有四个根 $x_1=\sqrt{a}$，$x_2=-\sqrt{a}$，$x_3=\sqrt{b}$，$x_4=-\sqrt{b}$。设 I 是恒等变换，群元(12)代表 $x_1\leftrightarrow x_2$，群元(34)代表 $x_3\leftrightarrow x_4$，则有 $\sigma\sim\{I,(12),(34),(12)(34)\}$，它就是 S_4 群的克莱因子群 V_4【12】。

一般而言，$GalE/Q$ 的具体形式是很难计算的，因为需要事先知道方程的解的具体形式。由于高阶方程的求解是非常困难的，我们实际上无法求出自同构群 $GalE/Q$ 的具体形式。

因此就提出所谓的伽罗华对应关系【13】，直接用伽罗华可解群 G_n 来代替根式扩域自同构 $GalE/Q$ 群。并用 G_n 是否能进行塔式结构分解，来说明方程是否能进行根式扩域。由于五次方程的 S_n 群没有真正的正规子群，G_5 不是可解群，没有塔式结构，就认为五次方程的根式扩域过程不可能，因此没有根式解。

六 伽罗华的理论存在的问题

6.1 伽罗华理论存在的一般性问题

以下证明，伽罗华实际上只是假设五次方程没有根式解，并没有真正证明五次方程无根式解。伽罗华理论通过自同构算符对方程的根的作用，来建立自同构群。但为了证明对三次和四次方程有效，却不得不用方程的根之间的某种关系代替根本身。这种做法违背了自同构的定义，是不合法的，导致证明的无效。根式塔扩域理论也与实际的解方程过程不符，只是一种形式的东西，没有实用性。用可解群理论描述三次四次方程的预解式关系是不成功的，伽罗华关于高次方程没有根式解的证明是不成立的。

伽罗华的可解群理论本身就是一个逻辑悖论。既然证明伽罗华扩域群 $GalE/Q$ 与置换群 S_n 的真正规子群等价，就等于承认方程的根与系数之间存在 S_n 群的对称性，就等于承认方程的根的存在。如果只是由于 S_5 群没有真正规子群，就认为不可能有根式解，这样的论证是没有根据的。没有正规子群只意味着方程的根之间没有正规子群的对称性，并不意味着方程的根式解不存在，除非证明 5 次方程的韦达公式和 S_5 群都不存在。

事实上，伽罗华只证明了交错群 A_n（$n \geq 5$）是单群，以及 S_5 是单群。但没有证明 S_n（$n > 5$）也是单群。比如 S_5 是 S_9 的真正规子群，含有非素数阶循环群作为子群的置换群 S_{n} 一定不是单群。我们怎么可以说次数 $n > 5$ 的方程都没有根式解呢？

6.2 不能解释汤健儿得到的五次方程解

显然，伽罗华可解群理论不能解释汤健儿得到的五次方程根式解。以（11）式为例，该方程用（10）和（19）式表示的五个解仍然满足韦达公式（89），根与系数之间仍然存在 S_5 群的对称性。虽然方程的两个系数存在关系 $p^2 = 5r$，但这不改变 S_5 群的对称性。由于 S_5 群没有真正规子群，不存在（90）式的可解群塔式结构，按照伽罗华理论，（11）式就应当没有根式解，然而汤健儿明确给出（11）式的根式解。

6.3 数字系数高次方程的解

伽罗华理论讨论的是 Q 上不可约方程，然而现实中存在大量的数字系数高次方程，除了某些特殊的情况外，一般难于判断它们是否是 Q 上不可约的。按照伽罗华理论，一般都将它们判定为不可根式解，这与实际完全不符。例如，郑良飞书中给出以下五次方程：

$$3x^5 + 7x^4 - 18x^3 - 49x^2 + 17x + 14 = 0 \qquad (96)$$

并根据方程根与系数之间的关系，求出一个解，将五次方程降低为四次方程。然后再求解四次方程，得到的五个解是【7】：

$$x_1 = \frac{2}{3} \qquad x_{2,3} = 1 \pm \sqrt{2} \qquad x_{4,5} = \frac{-5 \pm i\sqrt{3}}{2} \qquad (97)$$

因此（96）式有三个实数解，两个复数解。三个实数解中，两个无理数，一个有理数。由于存在一个有理数解，方程（96）是 Q 上可约的。然而如果方程没有解出，我们就无法判断它是 Q 上可约的还是不可约的。在一般的情况下，判断方程是否可约的过程实际上就是解方程的过程，因此假定某个高次方程 Q 上可约实际上是没有意义。

已知数学上有一个艾森斯坦判据，可以用来判断方程是否 Q 上可约【12】。然而这个判据只是

一个充分条件，不是必要条件，其应用范围很有限。比如对方程（96）式，我们有 $a_0=14$，$a_1=17$，$a_2=-49$，$a_3=-18$，$a_4=7$，$a_5=3$。按照艾森斯坦判据，如果能够找到一个素数 p，它能够整除 a_0,a_1,a_2,a_3,a_4，但不能整除 a_5，同时 p^2 不能整除 a_0，则（96）式就是 Q 上可约的。显然对（96）式我们找不到这样素数，就无法判断它是 Q 上是否可约。然而，实际解方程的结果证明，（96）式有一个有理数解 $x_1=2/3$。

因此目前我们并没有一个通用的有效方法，来判断一般的代数方程是否 Q 上可约。按照流行的看法，五次方程没有根式解。如果要解（96）式，首先就碰到伽罗华理论的拦路虎。一般都会就断定它没有根式解，实际上认为它不可解。

关于数字系数高次方程的求解，中国学者郑良飞（石泉）做了大量的工作，写出一本专著《一元五次方程的破解》。书中提出一些相当有效的方法，对各种不同的情况，解出大量的数字系数五次方程。按照郑良飞的看法，任何数字系数的高次方程，不管是否 Q 上可约，原则上都是可解的。

6.4 高次分圆多项式方程的根式解

我们将方程 $x^n-1=0$ 称为分圆多项式方程，它可以按以下方式进行分解：

$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots+1)=0 \qquad (98)$$

因此它是一个 Q 上可约多项式，$x=1$ 是有理数解。该方程的根被称为本源根，可以统一写为：

$$x_k=\omega^k=e^{i2\pi k/n}=\cos 2\pi k/n+i\sin 2\pi k/n \qquad k=0,\ 1,\ 2,\cdots n-1 \qquad (99)$$

取 $n=6$，（98）式可写成两个方程，即 $x-1=0$ 和一个五次方程：

$$x^5+x^4+x^3+x^2+x+1=0 \qquad (100)$$

（100）式的解是：

$$x_k=\omega^k=\cos(2\pi k/6)+i\sin(2\pi k/6) \qquad k=1,\ 2,\ 3,\ 4,\ 5 \qquad (101)$$

因此 x_k 一般不是有理数，比如 $x_1=1/2+i\sqrt{3}/2$。这说明（100）式的根式解是存在的，它是可以扩域的。然而，（100）式的韦达公式满足的是 S_5 置换群，它是一个可换的循环群。按照伽罗华理论，它不是可解群，没有根式解，因此伽罗华理论对（100）式的五次方程无效。

6.5 一般三次方程的根式扩域理论是无效的

以下分析指出，伽罗华的根式扩域理论只是一个形式化的东西，实际的解方程过程并不遵守该理论的根式塔添加程序。根据作者所见，虽然有大量的文献讨论二次方程和某些可约的三、四次方程的根式塔构造，却很少有文献讨论一般的不可约的三和四次方程的根式塔构造问题。

以下是作者从文献【12】中引用的，构造一般三次方程伽罗华根式塔的过程。从中可以看出这个证明牵强附会，逻辑混乱，存在严重的问题。将一般的三次方程写为：

$$f(x)=x^3+px+q=0 \qquad (102)$$

系数 $p,q\in Q$ 是有理数，它的三个解是：

$$x_1=\sqrt[3]{-q/2+\sqrt{(q/2)^2+(p/3)^3}}+\sqrt[3]{-q/2-\sqrt{(q/2)^2+(p/3)^3}} \qquad (103)$$

$$x_2=\omega\sqrt[3]{-q/2+\sqrt{(q/2)^2+(p/3)^3}}+\omega^2\sqrt[3]{-q/2-\sqrt{(q/2)^2+(p/3)^3}} \tag{104}$$

$$x_3=\omega^2\sqrt[3]{-q/2+\sqrt{(q/2)^2+(p/3)^3}}+\omega\sqrt[3]{-q/2-\sqrt{(q/2)^2+(p/3)^3}} \tag{105}$$

其中：

$$\omega=e^{i2\pi/3}=\cos 2\pi/3+i\sin 2\pi/3=-1/2+\mathrm{i}\sqrt{3}/2$$

$$\omega^2=e^{i4\pi/3}=(-1/2+\mathrm{i}\sqrt{3}/2)^2=-1/2-i\sqrt{3}/2 \tag{106}$$

（102）式的韦达公式对应的置换群是 S_3，它有六个群元，即：

$$S_3=\{I,(12),(13),(23),(123),(132)\} \tag{107}$$

S_3 唯一的真子群是 A_3，它是正规子群，有三个群元：

$$A_3=\{I,(123),\ (132)\} \tag{108}$$

其中 (123) 和 (132) 是偶置换。按照伽罗华理论，可解群的塔式结构为：

$$S_3\sim G_3\geq A_3\geq I \tag{109}$$

那么我们该怎么描述伽罗华的根式扩域过程呢？从（109）式可知，按照可解群理论，$G_3\to I$ 只有两个步骤。然而按照根式扩域理论，却需要三次根式添加。如（103）式所示，第一次扩域是考虑第一层根号，令：

$$Q(p,q)\to Q_1\left(p,q,\sqrt{(q/2)^2+(p/3)^3}\right) \tag{110}$$

第二次扩域引入第二重根号，有：

$$Q_1\to Q_2\left(p,q,\sqrt[3]{-q/2\pm\sqrt{(q/2)^2+(p/3)^3}}\right) \tag{111}$$

第三次扩域如（104）和（105）式所示，要同时引入虚数和根号 $\omega\sim\mathrm{i}\sqrt{3}$，即：

$$Q_2\to Q_3\left(p,q,i\sqrt{3},\sqrt[3]{-q/2\pm\sqrt{(q/2)^2+(p/3)^3}}\right) \tag{112}$$

因此根式扩域的塔式结构实际上是 $Q\leq Q_1\leq Q_2\leq Q_3=E$，显然与伽罗华理论的（109）式不一致。

为了使扩域过程满足伽罗华理论，文献【12】给出以下繁复且漏洞百出的证明：

1. 一开始就把 $\omega\sim i\sqrt{3}$ 加到方程的基域 F 中，令：

$$F=F(r,p,q,i\sqrt{3}) \tag{113}$$

方程的根域则是：

$$E=E(x_1,x_2,x_3)=F''(r,p,q,i\sqrt{3},x_1,x_2,x_3) \tag{114}$$

2. 于是就有伽罗华群 $G(E/F)=S_3$，根式塔结构为 $G=S_3\geq A_3\geq I$，它是一个可解群。相应的塔式扩域结构为 $F(r,p,q,i\sqrt{3})\leq B\leq E(x_1,x_2,x_3)$。其中 $B=\mathrm{I}nvA_3$（Inv 意指不变的）

$A_3 = G(E/B)$ 是三阶循环群。设 B 是 F' 的正规扩域， E 则看成是 B 的一个阶数为 $|A_3| = 3$ 的三次循环扩域。

3. 引入三次方程判别式:

$$\Delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \tag{115}$$

Δ 在 $A_3 = \{I,(123),\ (132)\}$ 的偶置换下不变，因此 $\Delta \in B$ 。但是 Δ 在 S_3 的奇置换下不能保持不变，因此 $\Delta \notin F$ 。令 $D = \Delta^2$ ，由于 D 在奇置换下仍然不变，因此 $D \notin F'$ 。可以证明：

$$D = \Delta^2 = -27q^2 - 4p^2 = a \tag{116}$$

4. 由于 $\Delta \notin F$ ， $\Delta \in B$ ，因此就构成 F 的扩域 $F'(\Delta)$ ，意味着 $F \le F'(\Delta) \le B$ 。然而，由于 $D = \Delta^2 = a \in F$ ， Δ 是方程 $x^2 - a = 0$ 的根，故所以 $[F'(\Delta) : F] = 2$ 。又由于 $G(B/F) = G(E/F)/G(B/F) = G(E/F)/G(E/B) \approx S_3/A_3$ ，可得 $[B:F] = |G(B/F)| = |S_3|/|A_3| = 2$ ，因此就证明 $B = F'(\Delta)$ 。

5. 如果所有的三个根 x_1, x_2, x_3 都属于 B ，则有 $B = E$ ，这是矛盾的。因此可设 $x_1 \notin B$ ，就可构造 $B' = B(x_1) \ge B$ 。由于 $|A_3| = 3$ ，在 $A_3 \ge I$ 中间就不能插进其它子群，意味着 $B(x_1) = E$ 。于是就有根域的塔式结构 $F \le B \le E$ ，可以更明确地写为：

$$F(r,p,q,i\sqrt{3}) \to B(r,p,q,i\sqrt{3},x_2,x_3) \to E(r,p,q,i\sqrt{3},x_1,x_2,x_3) \tag{117}$$

于是就完成了一般三次方程的根式塔构造，证伽罗华理的有效性。

显然，这样的扩域过程有严重的问题。首先，将 $\omega \sim i\sqrt{3}$ 加到基域 F 中根本不合理。伽罗华扩域理论的前提是，基域是有理数域，不含根号和虚数。之所以要把基域用（113）式表示，是因为三次方程的解包含了多重根和虚数，但 S_3 群的对称性只能容纳一个中间域，无法按伽罗华理论的模式进行扩域。于是就只好把 $i\sqrt{3}$ 加入到基域，使理论能自圆其说。

其次，这种做法没有说明如何通过自同构映射得到 A_3 群。按照以上方式，中间域 B 中包含 x_2, x_3 ，不包括 x_1 。自同构映射意味着自同构群中只含 x_2, x_3 之间的置换 (23) ，不包含 x_1 与 x_2, x_3 的交换，也就不包含群元 (123) 和 (132) 。然而 A_3 恰恰包含 (123) 和 (132) ，不包含 (23) 。事实上，由于 A_3 群同时包含指标 $1,\ 2,\ 3$ ，第一次扩域就无法将三个解的任何一个排除在外，所谓的根式多层塔式扩域是不可能的。

除此之外，为什么要引入（116）式的关系，则是无法解释的。 $x^2 - a = 0$ 与扩域过程没有关系，用它的根来建造中间域是不合法的。实际的解方程过程是，先找到一个解 x_1 ，然后再按照（103）和（105）式得到其他两个解，过程与以上描述不一样。由此可见，伽罗华的扩域理论对一般的三次方程是无效。

6.6 实际扩域过程置换群对称性的改变

按照三次方程的解（103）~（105）式，设解方程得到的第一个解是 x_1 。因此第一次扩域是从有理数域扩充到无理数域，有：

$$Q(p,q) \to Q_1\left(p,q,\sqrt[3]{-q/2 \pm \sqrt{(q/2)^2 + (p/3)^3}}\right) \tag{118}$$

然后再得到第二和第三个解 x_2 和 x_3 ，第二次扩域就从实数域扩充到虚数域：

$$Q_1 \to Q_2\left(p,q,i\sqrt{3},\sqrt[3]{-q/2\pm\sqrt{(q/2)^2+(p/3)^3}}\right) \tag{119}$$

通过两次扩域，（119）式右边包含了方程的全部根，扩域过程的塔式结构是 $Q \le Q_1 \le Q_2 = E$。这说明三次方程的实际求解过程不是通过一次一次的多重根号的添加来完成的，而是一次性地得双重根的根式，然后再进入虚数域并添加 $i\sqrt{3}$。

更一般地看，假设我们解三次方程得到一个根 x_1 后，就可以将（102）式改写成：

$$（x-x_1)(x^2+ax+b)=0 \tag{120}$$

将上式展开，得：

$$x^3+(a-x_1)x^2+(b-ax_1)x-bx_1=0 \tag{121}$$

与（102）式比较，就有 $a-x_1=0$，$b-ax_1=p$，$bx_1=-q$。得到 $a=x_1$，$b=-q/x_1=p+x_1^2$。为了求方程的另外两个解，按照（120）式有：

$$x^2+ax+b=0 \tag{122}$$

（122）式是二次方程，其韦达公式满足 S_2 的对称性，即 $S_2=\{I,(12)\}$，而不是 A_3 群。因此在实际的解方程过程中，A_3 子群不起作用。方程的系数与根的对称性变化应当是 $S_3 \to S_2 \to I$，而不是 $S_3 \ge A_3 \ge I$，伽罗华的可解群理论与实际过程不匹配。

6.7 用根之间的关系代替根本身来构造自同构映射是不合法的

许多教科书在证明伽罗华理论的有效性时，都犯了一个普遍而致命的错误。在构造自同构扩域群时，不是按照（92）式的定义，将自同构算符作用于方程的根，而是作用于方程不同的根之间的某种关系。因此这种证明是无效性的，遗憾的是这个问题被一直被忽视。

以下以四次方程为例，来说明这个问题。同时也用这个例子证明，伽罗华理论对四次方程的无效性【14】。将四次方程写为：

$$f(x)=x^4+px^2+q=0 \tag{123}$$

其中 $p,q \in Q$。令 $x^2=\mathrm{y}$，上式就变成二次方程 $y^2+py+q=0$。它的两个解是：

$$y_1=\frac{-p+\sqrt{p^2-4q}}{2} \qquad y_1=\frac{-p-\sqrt{p^2-4q}}{2} \tag{124}$$

因此（123）式的四个解是：

$$x_1=\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}} \qquad x_2=-\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}}$$

$$x_3=\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}} \qquad x_4=-\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}} \tag{125}$$

为了证明这个过程满足伽罗华理论，考虑两个解的关系 $x_1+x_2=0$ 和 $x_3+x_4=0$。这两个关系式对以下 8 个置换保持不变性，被称为最早的伽罗华群【14】：

$$B=\left\{ I,(12),(34),(12)(34),(13)(24),(14)(23),(1423),(1324) \right\} \tag{126}$$

另外，从（125）式得：

$$x_1^2-x_3^2=\sqrt{p^2-4q} \tag{127}$$

$$x_2^2-x_4^2=\sqrt{p^2-4q} \tag{128}$$

由于 $x_1^2=x_2^2$， $x_3^2=x_4^2$，可以验证（126）的前四个置换 $I,(12),(34),(12)(34)$ 使（127）式不变。将（127）式右边的关系添加到方程（113）的初始域 $Q(p,q)$ 中，得到扩域：

$$Q(p,q)\to Q'(p,q,\sqrt{p^2-4q}) \tag{129}$$

然而（126）式的后四个置换 $(13)(24),(14)(23),(1423),(1324)$ 却不能使（127）式保持不变。为了证明扩域理论的有效性，文献【14】构造新的关系:

$$x_3-x_4=2\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}} \tag{130}$$

它对置换 I 和 (12) 不变，可以认为这个两个置换是 B 的一个子群。将（130）的右边添加到域 Q' 中，构成新的扩域：

$$Q'(p,q,\sqrt{p^2-4q})\to Q''(p,q,\sqrt{p^2-4q},\sqrt{(-p-\sqrt{p^2-4q})/2}) \tag{131}$$

然后再令：

$$x_1-x_2=2\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}} \tag{132}$$

它对置换 $I,(34)$ 保持不变。（131）式的根域被进一步被扩张，得到方程（123）的根域，有：

$$Q''(p,q,\sqrt{p^2-4q},\sqrt{(-p+\sqrt{p^2-4q})/2})$$

$$\to Q'''(p,q,\sqrt{p^2-4q},\sqrt{(-p-\sqrt{p^2-4q})/2},\sqrt{(-p+\sqrt{p^2-4q})/2})=E \tag{133}$$

由此认为伽罗华理论对四次方程成立。

同样，以上论证存在许多问题。

1. 首先，方程（123）式只是一个特殊的四次方程，其本质仍然是二次方程。对于一般的四次方程（78）式，其解（83）式非常复杂，用伽罗华的塔式添加扩域理论是根本无法描述的。

2. 四次方程的根与系数满足的韦达公式具有 S_4 的对称性，它有 24 个群元，即：

$$S_4=\left\{ I,(12),(13),(14),(23),(24),(34),(12)(34),(13)(24),(14)(23),(123),(132),(124),\right.$$

$$\left.(142),(134),(143),(324),(243),(1234),(1243),(1324),(1342),(1423),(1432) \right\} \tag{134}$$

按照正规子群的定义，伽罗华可解群的塔式结构为：

$$S_4\sim G_4\geq A_4\geq V\geq I \tag{135}$$

其中 A_4 是 S_4 的最大的正规子群，它有 12 个群元：

$$A_4 = \{\ I,(12)(34),(13)(24),(14)(23),(123),(132),$$

$$(124),(142),(134),(143),(324),(243)\ \} \qquad (136)$$

V 则是克莱因群，有四个群元：

$$V = \{\ I,(12)(34),(13)(24),(14)(23)\ \} \qquad (137)$$

显然（126）式的 B 不属于（134）式中的任何一个子群，它甚至不是正规子群，因此用（126）式的置换对称性来证明伽罗华理论是无效的。

3.对（126）置换不变的 $x_1+x_2=0$ 和 $x_3+x_4=0$ 与方程（123）的求解一点关系也没有。按照伽罗华的根式扩域理论，自同构映射算符将方程的根变成方程的根。然而 x_1+x_2 和 x_3+x_4 都不是原方程的根，比如将 x_1+x_2 代入（123）式，得 $(x_1+x_2)^4+p(x_1+x_2)^2+q=q\neq 0$。因此用 $x_1+x_2=0$，$x_3+x_4=0$ 来构造（121）式的伽罗华群没有意义的。同样，x_1-x_2 和 x_3-x_4 也不是方程（123）式的根，用自同构算符对它们作用没有意义，用添加（130）和（132）式的右边来扩域，即不符合自同构映射理论，也与实际的解方程过程没有关系。

4. 用方程的根的代数关系的置换对称性来代替根的置换对称性，被普遍地用来证明伽罗华理论的有效性。这种做法是概念混淆的结果，然而如果不这样做，就不能证明伽罗华理论的有效性。这种做法同时破坏了理论的唯一性。一个方程的不同解可以任意构造不同的关系，比如用 x_1,x_2,x_3,x_4 还可以构造 x_1x_2，$x_1^2x_2$ 和 $x_1^2x_3+x_4$ 等等。我们没有理由只用其中的某些关系，不用其他关系。

5. 事实上，用这种方法仍然无法构成伽罗华群的塔式结构。（127）和（128）式的根式扩域满足的置换群是：

$$B_1 = \{I,(12),(34),(12)(34)\} \qquad (138)$$

（131）和（133）的根式扩域满足的置换对称性是

$$B_2 = \{I,(12)\} \qquad B_3 = \{I,(34)\} \qquad (139)$$

它们与（126）式的关系不是正规子群链的关系，显然不满足（135）式的伽罗华群的塔式结构。因此这种扩域理论即不能正确描述方程的求解过程，也不能证明伽罗华根式扩域理论的有效性。

由于三、四次方程的扩域理论与实际的解方程过程不匹配，我们就没有理由认为，伽罗华可解群理论对五次方程也有效。对于高次方程，解方程过程可能的置换群对称性链应当是：

$$S_n \to S_{n-1} \to \cdots \to \mathrm{S}_2 \to I \qquad (140)$$

也就是说对于代数方程，一般而言系数与根之间只存在 S_n 置换对称性，与 S_n 的正规子群链对应的伽罗华群 G_n 及其塔式结构在解方程的实际过程中不存在。

6.8 三次方程预解式

1770 年拉格朗日发表论文“关于方程的代数解法的思考”，将置换群的概念引入解代数方程，提出用预解式来解代数方程【12】。二次方程比较简单，它的对称置换群 S_2 只有两个群元，没有必要讨论。对于三次方程（102）式的预解式，按照文献【15】，构造以下两个函数：

$$\alpha = x_1 + \omega x_2 + \omega^2 x_3 \tag{141}$$

$$\beta = (x_1 + \omega x_3 + \omega^2 x_2) \tag{142}$$

其中x_1, x_2, x_3是方程的三个根，用（103）~（105）式表示。已经证明以α^3和β^3为根的二次方程，是三次方程的拉格朗日预解式。我们有：

$$\alpha^3 + \beta^3 = (x_1 + \omega x_2 + \omega^2 x_3)^3 + (x_1 + \omega x_3 + \omega^2 x_2)^3$$

$$= 2(x_1^3 + x_2^3 + x_2^3) + 3(\omega + \omega^2)(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 + x_1^2 x_3)^3 + 12 x_1 x_2 x_3 \tag{143}$$

考虑到$1 + \omega + \omega^2 = 0$，则$\omega + \omega^2 = -1$，从（143）式可得：

$$\alpha^3 + \beta^3 = 2[(x_1 + x_2 + x_3)^3 - 3(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 + x_1^2 x_3) - 6 x_1 x_2 x_3]$$

$$-3(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 + x_1^2 x_3) + 12 x_1 x_2 x_3$$

$$= 2(x_1 + x_2 + x_2)^3 - 9(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 + x_1^2 x_3)$$

$$= 2(x_1 + x_2 + x_3)^3 - 9[(x_1 x_2 + x_1 x_3 + x_2 x_3)(x_1 + x_2 + x_3) - 3 x_1 x_2 x_3] \tag{144}$$

$$\alpha\beta = (x_1 + \omega x_2 + \omega^2 x_3)(x_1 + \omega x_3 + \omega^2 x_2)$$

$$= (x_1^2 + x_2^2 + x_2^2) + (\omega + \omega^2)(x_1 x_2 + x_2 x_3 + x_3 x_1)$$

$$= (x_1 + x_2 + x_3)^2 - 2(x_1 x_2 + x_2 x_3 + x_3 x_1) - (x_1 x_2 + x_2 x_3 + x_3 x_1) \tag{145}$$

三次方程（102）的根与系数的韦达公式是：

$$x_1 + x_2 + x_3 = 0 \qquad x_1 x_2 + x_1 x_3 + x_2 x_3 = p \qquad x_1 x_2 x_3 = -q \tag{146}$$

从（145）和（146）式得：

$$\alpha^3 + \beta^3 = -27q \tag{147}$$

$$\alpha\beta = -3p \qquad \alpha^3 \beta^3 = -27 p^3 \tag{148}$$

因此α^3和β^3可以看成是以下以y为变量的二次方程的根：

$$y^2 + 27qy + -27 p^3 = 0 \tag{149}$$

解（149）式，得：

$$\alpha^3 = \frac{-27q + \sqrt{27^2 q^2 + 4 \times 27 p^3}}{2} \tag{150}$$

$$\beta^3 = \frac{-27q - \sqrt{27^2 q^2 + 4 \times 27 p^3}}{2} \tag{151}$$

就有：

$$\alpha = 3\left[\frac{-q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right]^{\frac{1}{3}} \tag{152}$$

$$\beta = 3\left[\frac{-q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right]^{\frac{1}{3}} \tag{153}$$

再按照定义：

$$x_1 + x_2 + x_3 = 0 \tag{144}$$

$$x_1 + \omega x_2 + \omega^2 x_3 = \alpha \tag{155}$$

$$x_1 + \omega x_3 + \omega^2 x_2 = \beta \tag{156}$$

从以上三式就可以得到三次方程的解（103）~（105）式。

6.9 用伽罗华理论解释三次方程预解式的有效性问题。

如何用伽罗华可解群理论证明三次方程预解式的有效性？本文作者查阅了许多文献，发现对这个问题的表述都是含含糊糊的。

问题主要涉及伽罗华群对预解式作用的有效性。已知三次方程（102）式对应的置换群是 S_3，用（108）式表示。它唯一的真子群是 A_3，用（109）式表示，其中的群元 (123) 和 (123) 是偶置换。因此有些文献就认为，只要证明三次方程预解式的解 α^3 和 β^3 具有 A_3 置换不变性，就等于证明伽罗华理论对三次方程的预解式有效。然而情况并非如此。

容易证明，α^3 对群元 (123) 的置换是不变的，有：

$$(123)\alpha^3 = (123)(x_1 + \omega x_2 + \omega^2 x_3)^3 = (x_2 + \omega x_3 + \omega^2 x_1)^3$$

$$= \omega^3(x_1 + \omega x_2 + \omega^2 x_3)^3 = [\omega(x_2 + \omega x_3 + \omega^2 x_1)]^3$$

$$= (\omega x_2 + \omega^2 x_3 + x_1)]^3 = \alpha^3 \tag{157}$$

然而，如果用群元 (132) 对 α^3 作用，结果却是：

$$(132)\alpha^3 = (x_3 + \omega x_1 + \omega^2 x_2)^3$$

$$= \omega^3(x_3 + \omega x_1 + \omega^2 x_2)^3 = [\omega(x_3 + \omega x_1 + \omega^2 x_2)]^3$$

$$= (\omega x_3 + \omega^2 x_1 + x_2)]^3 \neq \alpha^3 \tag{158}$$

而且容易看出，$(132)\alpha^3 \neq \beta^3$。事实上，将置换 (23) 作用于 α^3，结果是：

$$(23)\alpha^3 = (x_1 + \omega x_3 + \omega^2 x_2)^3 = \beta^3 \tag{159}$$

然而问题是，置换 (23) 不属于 A_3，因此（159）式恰恰证明伽罗华可解群的无效性。

此外，由于α^3和β^3都不是三次方程的根，而是二次方程（149）式的根。三次方程的根是x_1,x_2,x_3，用α^3和β^3来代替x_1,x_2,x_3是偷换概念。虽然用它们来构造三次方程的根式是有效的，但并不能证明伽罗华理论的有效性。按照伽罗华根理论，应当用自同构算符对x_1,x_2,x_3的作用来建立伽罗华自同构群$GalE/Q$，而不是用二次方程的根来构造三次方程的伽罗华群。

6.10 四次方程的预解式

在现有的文献中，用伽罗华理论构造四阶方程预解式的方法是同样混乱的。它有多种版本，比如欧拉和费拉里（Ferrari）提出的方法，但没有一种能够严格按伽罗华理论得到预想结果。本文以欧拉提出的方法为例来说明，其它版本存在相同的问题，就不赘述。将四次方程写为【15】：

$$x^4+px^2+qx+c=0 \tag{160}$$

设x_1,x_2,x_3,x_4是（160）式的四个根式解，用它们构造以下三个函数：

$$\alpha^2=\frac{1}{16}(x_1+x_3-x_2-x_4)^2 \tag{161}$$

$$\beta^2=\frac{1}{16}(x_2+x_3-x_1-x_4)^2 \tag{162}$$

$$\gamma^2=\frac{1}{16}(x_3+x_4-x_1-x_2)^2 \tag{163}$$

按照（161）~（163）式，利用方程（160）式的韦达公式，可得：

$$\alpha^2+\beta^2+\gamma^2=\frac{3}{16}[(x_1+x_2+x_3+x_4)]^2$$

$$-\frac{1}{2}(x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4)=-\frac{1}{2}p$$

$$\alpha^2\beta^2+\alpha^2\gamma^2+\beta\gamma^2=\frac{1}{16}(x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4)^2$$

$$-\frac{1}{4}x_1x_2x_3x_4=\frac{1}{16}p^2-\frac{1}{4}c \tag{164}$$

$$\alpha\beta\gamma=\frac{1}{8}(x_1x_2x_3+x_1x_2x_4+x_2x_3x_4)=-\frac{1}{8}q \tag{165}$$

因此α^2，β^2和γ^2是以下y为变量的三次方程的根，也称为四次方程的预解式：

$$y^3+\frac{1}{2}py^2+\left(\frac{1}{16}p^2-\frac{1}{4}c\right)y-\frac{1}{64}q^2=0 \tag{166}$$

解这个三次方程，得到三个根。将它们开平方，就得到α，β和γ。它们各有两个值，考虑到（165）式的限制关系，先选定α和β，然后确定γ，于是得到α，β和γ的四组解。任选一组，利用（161）~（163）式和韦达公式，即有：

$$x_1+x_2+x_3+x_4=0 \tag{167}$$

$$\frac{1}{4}(x_1+x_3-x_2-x_4)=\alpha \tag{168}$$

$$\frac{1}{4}(x_1+x_3-x_2-x_4)=\beta \tag{169}$$

$$\frac{1}{4}(x_3+x_4-x_1-x_2)=\gamma \qquad (170)$$

利用（167）~（170）式，就可以得到四次方程的一组解($\alpha\beta\gamma=-1/(8q)$):

$$x_1=\alpha-\beta-\gamma \qquad x_2=-\alpha+\beta-\gamma$$

$$x_3=\alpha+\beta+\gamma \qquad x_4=-\alpha-\beta+\gamma \qquad (171)$$

6. 11 用伽罗华理论解释四次方程预解式存在的问题。

假设按照伽罗华的扩域理论，得到方程（160）的第一个根式解后，第一次根式扩域使方程的对称性从（134）式的 S_4 变成（136）式的 A_4，（161）~（163）式应当满足 A_4 的置换不变性。然而情况并非如此。容易验证，在 A_4 置换下 α^2 能够保持不变，但 β^2 和 γ^2 却不能保持不变。例如用 A_4 的群元 (124) 作用，结果是：

$$(124)\beta^2=\frac{1}{16}(x_4+x_1-x_2-x_1)^2\neq\beta^2 \qquad (172)$$

$$(124)\gamma^2=\frac{1}{16}(x_3+x_1-x_2-x_4)^2\neq\gamma^2 \qquad (173)$$

如果用 S_4 的群元 (12) 和 (1342) 作用于 α^2，得到以下结果：

$$(12)\alpha^2=\frac{1}{16}(x_2+x_3-x_1-x_4)^2=\beta^2 \qquad (174)$$

$$(1342)\alpha^2=\frac{1}{16}(x_3+x_4-x_1-x_2)^2=\gamma^2 \qquad (175)$$

然而我们知道，置换 (12) 和 (1342) 不属于 A_4，因此也不属于 V 。

同样的道理 α^2， β^2 和 γ^2 都不是四次方程的根，而是三次方程（102）式的根。四次方程的根是 x_1,x_2,x_3,x_4，用 α^2， β^2 和 γ^2 来代替 x_1,x_2,x_3,x_4 是偷换概念。虽然用它们来构造四次方程的预解式是有效的，但并不证明伽罗华理论的有效性。对于四次方程的预解式关系，伽罗华自同构根式扩域群理论也是无效的。

六 结论

阿贝尔和伽罗华被认为是数学史上的悲剧人物，命运多舛，生命短暂。他们生前未能看到自己的理论被世人认可，身后却声名盖世。他们关于五次方程没有根式解的证明被认为是一座丰碑，至今无法超越。为了解决五次方程的求解问题，在前人的工作的基础上，伽罗华提出比较完整的群论体系，将传统代数推进到近世代数，为现代数学的发展做出重要的贡献。

自从阿贝尔和伽罗华的文章发表之后，五次以及五次以上方程没有根式解的看法成为定论。主流数学家们似乎不再关心这个问题，尽管阿贝尔和伽罗华的理论与高斯代数基本定理是矛盾的。然而科学的发展往往难以意料，近年以来不断有人解出某些特殊的五次和六次方程，而且大多都是用根式表示的，阿贝尔和伽罗华的理论无法解释为什么这些方程是可解的。

为了了解事情的真相，作者对阿贝尔和伽罗华的理论做了深入的研究，结果发现情况与想象的完全不一样。阿贝尔对五次方程没有根式解的证明是完全错误的，他提出的代数方程的普遍解的形式与实际不符。三次方程和四次方程的解都不具有阿贝尔的解的形式，因而没有理由认为阿贝尔对

五次方程没有根式解的证明是正确的。事实上，阿贝尔的证明是一个循环论证，存在许多逻辑混乱，概念误用和初级计算错误，他的证明是不成立。

虽然伽罗华的群论是一个重要的发现，但伽罗华用群论来证明一般五次方程不可根式解却是不成功的。伽罗华的理论与其说是一个严格的证明，不如说是一个猜想。而且这个猜想证据不足，证明过程牵强附会，实际上是在拼凑结果。

按照高斯等人提出的代数基本定理，任何 n 次方程都有 n 个解，其中必然会包含根式解。因此伽罗华的理论与代数基本定理的矛盾的。代数基本定理的证明是严格的，而且可以从许多方面进行证明。我们有理由认为代数基本定理是正确的，就只能认为伽罗华理论是错的。

事实上，伽罗华的可解群理论与五次方程是否可解没有关系。五次方程的根与系数对应的关系用 S_5 置换群来表示，这个事实本身就说明了五次方程的根的存在。五次方程没有可解群，只不过说明方程的根与系数的关系不满足可解群的对称关系，并不能说方程没有根式解。

为了构造伽罗华根式扩域群，并在扩域群与可解群之间建立联系，需要引入自同构映射概念。按照伽罗华理论的定义，自同构算符对方程的根作用不改变根自身，或者将它变成相同的方程的其他根。然而为了证明伽罗华群对三次和四次方程的有效性，在实际计算过程中，却将自同构算符作用于方程的根之间的某些关系。这直接违背了自同构算符的原始定义，导致证明无效。而且由于根之间的关系可以任意设定，使这种结果缺乏唯一性和普遍性。

高次方程的实际求解过程也不满足伽罗华可解群的塔式结构，或者说伽罗华的根式扩域理论与解方程的过程不一致。为了达到一致性，就不得不编造出某些中间过程。但这种中间过程实际上不存在，导致伽罗华扩域理论无效。由于同样的原因，用伽罗华理论求解一般的三次和四次方程的预解式也是无效的。

关于五次方程的一般解问题，在阿贝和伽罗华之后仍然有一些进展。1858 年法国数学家埃米而特和德国数学家罗克内克等分别独立地证明，一般五次方程可以用一类称为椭圆模函数解出。1870 年，法国数学家约当证明，利用这类函数可以解出任意次的多项式方程【10】。然而这类解都用无穷级数来表示，是很不直观的。由于无穷级数的求和是困难的，很难从中得出有实际意义的结果，不可能用它们来代替方程的根式解。

因此本文的结论是，阿贝尔和伽罗华并没有证明五次方程和高于五次的方程没有根式解。数学家们应当继续努力，去寻找五次方程和高于五次方程的一般解。

参考文献

1. 李文林, 数学珍宝: 历史文献精选［M］, 北京, 科学出版社, 1998, p.471-476.
2. 李文林, 数学珍宝: 历史文献精选［M］, 北京, 科学出版社, 1998, p. 4771-478.
   GALOIS E. Discussion on the process of pure analysis[J], Journal de Mathématiques Pures et Appliqués, 1846, 11(2)，p. 381-444.
3. 冯承天，从求解多项式方程到阿贝尔不可能定理，细说五次方程求根式，华东师范大学出版社，2014，p. 117.
4. 冯承天，从代数基本定理到超越数，一段经典数学的奇幻之旅，华东师范大学出版社，2017，p. 17.
5. 汤健儿，几类能用根式求解的五次方程，高等数学研究，2012年1月，第15卷第1期，p.58-61。
6. 盛兴平，实系数一元四次方程的矩阵解法,数学通报，2002 年，12期，p. 37。
7. 范军，孔志宏．三类特殊的实系数一元六次方程的矩阵解法，高等数学研究，2009，12(4)：p.66-69．

8. 郑良飞，石泉，一元五次方程破解，国防工业出版社，2009，p.127。
9. Cauchy, Memoire Ie, Nombre des valeurs qu’une fonection peut acquerie, Journal de l’ecole polytechnic que, Vol, 17.
10. Pesic P. Abel’s Proof, An Essay on the Sources and Meaning of Mathematical Un-solvability, The MIT Press, 2003, p. 174, 198.
11. 彭长文，孟颖等，关于一元五次方程求实根的方法研究，考试周刊，数学与教学研究，2018，第七期，p. 62.
12. 冯承天，从一元一次方程到伽罗华理论，华东师范大学出版社，2018，p. 15, 55，98, 103.
13. 徐诚浩，Aritin定理—古典数学难题与伽罗华理论，哈尔滨工业大学出版社，2018，p.100,110。
14. 郑美玉，代数学简史(四)，荆门技术学院学报，2000年，15卷，第6期, p. 89.
15. 谢彦麟，代数方程的根式解及伽罗华理论，哈尔滨工业大学出版社，2011，p.35-43.