Galois Theory

Binhe Huang

2023.02.12

前言

在上个学期的《代数学基础》课上, 胡老师带我们一起研读了 *Galois Theory* 这本书; 在寒假期间, 我又仔细阅读了 Galois 的原文. 这本书不仅清楚地阐述了 Galois 理论, 还严谨地对原文给出了补充, 让我们从 Galois 的角度来理解 Galois 理论的主要内容与证明推导.

谈到 Galois 理论, 人们往往想到的是它可以得出结论: 一般高次方程（次数大于等于 5）没有根式解. 为了方便, 我就以证明这个结论为出发点, 一步一步地引入 Galois 理论中的定义与定理.(尽管 Galois 远远不止只关心一般高次方程)

目录

1 概述 **1**

1.1 初步转化 1

1.2 预览 3

2 Galois 的引理 **5**

2.1 对称多项式定理 5

2.2 Galois 预解式 5

1 概述

1.1 初步转化

问题 1. *一般 5 次方程是否有根式解?*

事实上, 二次方程的求根公式早在公元前一千多年就被美索不达米亚人知晓. 但是对于三次甚至更高次数的方程的求根公式, 人类在很长一段时间内都没有任何进展. 直至 16 世纪, 意大利学者卡尔丹发现了三次方程的求根公式, 进而四次方程的求根公式也得到解决. 但对于五次方程, 人们迟迟未能给出解答. 因此人们开始思考求根公式的存在性. 在想办法解决问题 1.1 之前，我们必须弄清楚其中一些名词的定义。首先，一般方程的定义是很自然的。

定义 1.1. *给定域 k, 方程 $x^n + A_1x^{n-1} + \cdots + A_n = 0$ 称为域 k* **一般 n 次方程**, *其中 A_1, A_2,$\cdots$, A_n 是 k 上的超越元.*

有根式解是什么意思呢? 不严谨地说, 对于一个方程, 如果存在一个求根的公式, 这个公式的运算仅包含下列五种:

(1) 对已知量的多重根号运算
(2) 对已知量或已知量的多重根号的加, 减, 乘, 除 (除数非 0) 法运算

则称该方程可以根式解. 这里的已知量必须含有域 k 中的所有元素与方程的系数. 但实际上他应该还包含某些次数的单位根 (以后我们求出这些次数). 由于已知量的加减乘除仍是已知量, 故若记 K 为全体已知量, 则 K 是一个域.

尽管这么定义是符合常理的, 但是一方面它不太严谨, 另一方面, 它不好去研究. 所以我们仍需要把这个定义转化成更" 数学" 的语言.

我们容易观察到, 条件 (2) 等价于: 方程的根存在于一个包含已知量与已知量的多重根号的域中. 域 k 不满足已知量的多重根号运算, 所以我们还需要找到一个方法描述如何将多重根号融入到域 k 中. 因此, 我们需要引入下面这个记号.

如果 r 是一个已知量的多重根号, 我们记

$$k(r) = \left\{ \frac{a_0 + a_1r + \cdots + a_nr^n}{b_0 + b_1r + \cdots + b_mr^m} : n, m \in \mathbb{N}, a_i \in k, b_j \in k, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m \right\}.$$

称 $k(r)$ 为添加 r 生成的**单扩张**. 因此我们给出下面更好的定义.

定义 1.2. *给定方程 $f(x) = 0$, 记 $x_1, x_2, \cdots, x_n$ 为 $f(x)$ 的 n 个根. 我们称 $f(x)$ 有根式解, 当且仅当, 存在一系列的域扩张*

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\mu,$$

使得 $x_1, \cdots, x_n \in K_\mu$. 其中 $K_{i+1} = K_i(r_i)$, r_i 是 K_i 中元素的 p_i 次方根.

我们可以要求其中的 p_i 均是素数. 因为, 若不是, 我们可以将 p_i 素数因子分解为 $q_1q_2 \cdots q_t$. 以 $t = 2$ 为例, 令 $K_i' = K_i(\sqrt[q_1]{r_i})$, 则

$$K_i \subset K_i' \subset K_{i+1}$$

是满足上述条件的域扩张.($t > 2$ 可以类似处理)

更进一步, 我们还可以要求域 K_μ 尽量小, 恰好包含所有根就可以了. 为了描述" 恰好", 我们引入分裂域的概念:

定义 1.3. *给定域 K 上的多项式 $f(x)$, 若存在域 $L \supset K$, 满足:*

(i) *$f(x)$ 在域 L 上可以分解成一次因式的乘积;*
(ii) *任意 L 的子域都不满足 (i),*

*则域 L 是 $f(x)$ 的*__分裂域__.

事实上, 我们可以证明分裂域是存在且唯一的 (证明在第三节). 因此我们可以得到定义 1.2 的等价定义

定义 1.4. 给定方程 $f(x)=0$, 令 $f(x)$ 的分裂域为 L. 我们称 $f(x)$ 有根式解, 当且仅当, 存在一系列的域扩张

$$K=K_0\subset K_1\subset K_2\subset\cdots\subset K_\mu=L,$$

, 其中 $K_{i+1}=K_i(r_i)$, r_i 是 K_i 中元素的 p_i 次方根.

综上所述, 问题 1.1 可以转化为

问题 2. 对于方程 $x^5+A_1x^4+\cdots+A_5=0$, 是否存在一系列满足上述条件的域扩张?

尽管 *Galois Theory* 书中没有详细讲转化的过程, 但我认为这一步转化是很重要的. 它把一个解方程的问题, 转化成了域论中的问题, 使得问题简化.

1.2 预览

为了给 Galois 理论一个概括性的瞻望, 我想在这一节大致地给出 Galois 原文中的思路. 这不可避免的引入了一些没定义的概念, 如 Galois 群. 这无伤大雅, 我认为这样可以时刻知道目标是什么, 避免在读后文的时候迷失方向. 下面引入两个关键性的定理 (原文中的 Proposition II, IV 和 V), 证明后文中会给出:

定理 1.1. 设 G 是方程 $f(x)$ 在域 K 上的 *Galois* 群. 给定素数 p, 要求域 K 包含 p 次本原单位根. 若域 K' 是域 K 通过添加 k 生成的单域扩张, 其中 k 是 K 中某元素的 p 次方根, 当且仅当方程 $f(x)$ 在 K' 上的 *Galois* 群 G' 满足要么 $G'=G$ 不变, 要么 $G\rhd G'$ 且 $[G,G']=p$.

定理 1.2 (Galois)**.** 给定无重根的方程 $f(x)=0$, $f(x)$ 有根式解当且仅当这个方程对应的 *Galois* 群可解, 即有一系列正规子群

$$G\rhd G_1\rhd\cdots\rhd G_\nu$$

使得 $[G_i,G_{i+1}]$ 为素数且 G_ν 是平凡群.

上面两个定理是 Galois 理论中的最核心定理. 它将问题 1.2 转化为群论的问题.

问题 3. 一般 *5* 次方程的 *Galois* 群是否可解?

为了更好地理解上述两条定理, 我从正面给出例子:

例 1.1. 众所周知, 给定域 k, 一般二次方程 $f(x)=ax^2+bx+c=0$ 有根式解:

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

我们令域 $K=k(a,b,c)$. 显然 $f(x)$ 的分裂域为 $L=K(\sqrt{b^2-4ac})$. 因此, 存在域扩张

$$K=K_0\subset K(\sqrt{b^2-4ac})=L$$

, 其中 $\sqrt{b^2-4ac}$ 是 K 中元素 b^2-4ac 的二次方根, 故 $f(x)$ 有根式解.

同时, $f(x)=0$ 的 *Galois* 群 S_2 确实存在满足定理 *2.2* 的一系列正规子群:

$$S_2\rhd\{0\},$$

并且 $[S_2, \{0\}] = 2$.

例 1.2. 给定域 k, 一般三次方程 $f(x) = ax^3 + bx^2 + cx + d = 0$ 有求根公式:

$$x = \omega \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} + \omega^2 \sqrt[3]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}},$$

其中 $p = \frac{3ac-b^2}{3a^2}$, $q = \frac{27a^2d-9abc+2b^3}{27a^3}$, ω 是三次单位根. 我们令域 $K = k(a, b, c, d, w)$. 因为

$$\omega \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} \cdot \omega^2 \sqrt[3]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} = \omega_0 \frac{p}{3},$$

其中 ω_0 为某一特定三次单位根, 所以 $f(x)$ 的分裂域为

$$L = K\left(\sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}\right).$$

令域 $K_1 = K\left(\sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}\right)$, 故存在域扩张

$$K = K_0 \subset K_1 \subset K_1\left(\sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}\right) = L$$

其中 $\sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$ 是 K 中元素 $(\frac{q}{2})^2 + (\frac{p}{3})^3$ 的二次方根, $\sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}$ 为 K_1 中元素 $-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$ 的三次方根. 因此, 一般三次方程有根式解.

同时 $f(x) = 0$ 的 *Galois* 群 S_2 确实存在满足定理 *2.2* 的一系列正规子群:

$$S_3 \rhd A_3 \rhd \{0\}.$$

并且 $[S_3, A_3] = 2$, $[A_3, \{0\}] = 3$.

给出上述两个定理之后, Galois 有给出了下面定理:

定理 1.3. 给定素数次不可约方程 $f(x) = 0$, 对根进行排序 $x_1, x_2, \cdots, x_p$, 令 G 是其对应的 *Galois* 群, 则 $f(x)$ 有根式解的充要条件是对于任意 $S \in G$ 均满足: 存在常数 a, b 使得对任意 k 均有

$$S(x_k) = x_{ak+b},$$

其中 $x_{i+rp} = x_i$, $r \in \mathbb{N}$

因此我们可以发现可解的 p 阶不可约方程的 Galois 群至多有 $p(p-1)$ 个置换. 而我们后续可以证明下面这个定理, 这也意味着, 一般五次方程的 Galois 群有 $5! = 120$ 个元素.

命题 1.4. 给定域 K 与一般 n 次方程 $x^n + A_1x^{n-1} + \cdots + A_n = 0$, 在域 $K(A_1, A_2, \cdots, A_n)$ 的 *Galois* 群是置换群 S_n.

故一般五次方程没有根式解.

后文是对上述解法的补充和证明.

2 Galois 的引理

2.1 对称多项式定理

Galois 文中多次引用了 Gauss 的文章,Gauss 对 Galois 的研究的影响很深. 这一节的定理是 Gauss 证明的很有名的定理, 证明所需要的知识不高深, 但结论却十分精妙.

定理 2.1 (对称多项式定理)**.** *关于 $r_1, r_2, \cdots, r_n$ 的对称多项式一定能被基本多项式表示. 其中 $r_1, r_2, \cdots, r_n$ 的基本多项式是*

$$\sigma_i = \sum_{0<j_1<\cdots<j_i\leqslant n} r_{j_1} r_{j_2} \cdots r_{j_i},$$

其中 $0 < i < n + 1$.

证明. □

有了这个定理, 我们可以立刻得到

推论 2.2. *给定方程 $x^n + a_1 x_{n-1} + \cdots + a_n = 0$, 则关于根的对称多项式可以被 $a_1, a_2, \cdots, a_n$ 表示.*

2.2 Galois 预解式

Galois 的工作面向的是普遍的代数方程, 所以我们不再像上一节一样只讨论一般 n 次方程. 这一节中, 若未说明, 均默认多项式为域 K 上的.

引理 2.3 (Galois 引理 I)**.** *若不可约多项式 $f(x)$ 与多项式 $g(x)$ 有一个相同的根, 则 $f \mid g$.*

证明. 易证. □

引理 2.4 (Galois 引理 II)**.** *给定方程 $f(x) = 0$, 令其根为 $x_1, x_2, \cdots, x_n$, 若 $f(x)$ 无重根, 则存在关于 $x_1, x_2, \cdots, x_n$ 的多项式 t 满足任意置换两个根均改变 t 的值.*

证明. □

满足上述引理的 t 被称为 ***Galois* 预解式**