Galois 理论(续)

一个三次方程 $x^3+bx+c=0$ 的解为

$$A+B,\ -\frac{(A+B)}{2}+\frac{(A-B)}{2}\sqrt{-3},\ -\frac{(A+B)}{2}-\frac{(A-B)}{2}\sqrt{-3}$$

其中 $A=\sqrt[3]{\frac{-c}{2}+\sqrt{\frac{b^3}{27}+\frac{c^2}{4}}}$，$B=\sqrt[3]{\frac{-c}{2}-\sqrt{\frac{b^3}{27}+\frac{c^2}{4}}}$，

解公式只涉及加、减、乘、除和开根号等运算，用域论语言，即：

定义 $\mathbb{F}$ 域，$f(x)\in\mathbb{F}[x]$，$f(x)$ 根式可解(在 $\mathbb{F}$ 上)(solvable by radicals over $\mathbb{F}$) 若 $f(x)$ 在 $\mathbb{F}$ 的某扩域 $\mathbb{F}(a_1,\cdots,a_n)$ 中分裂，其中 $a_1,\cdots,a_n$ 满足：存在正整数 $k_1,\cdots,k_n$，$a_1^{k_1}\in\mathbb{F}$，$a_2^{k_2}\in\mathbb{F}(a_1)$，$a_3^{k_3}\in\mathbb{F}(a_1,a_2)$，$\cdots$，$a_n^{k_n}\in\mathbb{F}(a_1,\cdots,a_{n-1})$.

定义展示 $f(x)=0$ 的零点可表达为 $a_1,\cdots,a_n$ 的多项式，而 $a_1,\cdots,a_n$ 可表达成 $\mathbb{F}$ 中元素的加、减、乘、除和开根号.

例 $\mathbb{F}=\mathbb{Q}$，$f(x)=x^8-3$ 零点：$\sqrt[8]{3}\,w^k$ $k=0,1,\cdots,7$

$w=\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$ $\quad a_1=\sqrt[8]{3}$，$a_2=\sqrt{-1}\sqrt[8]{3}$，$a_3=\sqrt[8]{3}\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{-1}\sqrt{2}}{2}\right)$

$a_4=\sqrt[8]{3}\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{-1}\sqrt{2}}{2}\right)$

定理 设 $\mathrm{char}\,\mathbb{F}=0$，$a\in\mathbb{F}$，$n>0\in\mathbb{N}$，$\mathbb{E}$ 是 x^n-a 在 $\mathbb{F}$ 上分裂域，则 $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ 可解.

证明框架：x^n-a的零点（在$\mathbb{E}$中）：$b=\sqrt[n]{a}, \omega b, \cdots, \omega^{n-1}b$

$\forall \tau \in Gal(\mathbb{E}/\mathbb{F})$ $\tau(b)=\omega^i b$ $\exists i$. $\tau(\omega)=\omega^j$ $\exists j$

$\mathbb{F}(\omega)$是$\mathbb{F}$的正规扩张 $\Rightarrow Gal(\mathbb{E}/\mathbb{F}(\omega)) \lhd Gal(\mathbb{E}/\mathbb{F})$

检查 $Gal(\mathbb{F}(\omega)/\mathbb{F}) \simeq Gal(\mathbb{E}/\mathbb{F}) / Gal(\mathbb{E}/\mathbb{F}(\omega))$ 是Abelian的.

$Gal(\mathbb{E}/\mathbb{F}(\omega))$是Abelian的.

定理（Galois）$char\,\mathbb{F}=0$，$f(x)\in\mathbb{F}[x]$，$f(x)$在$\mathbb{F}(a_1,\cdots,a_t)$中分裂，其中$a_1^{n_1}\in\mathbb{F}$，$a_i^{n_i}\in\mathbb{F}(a_1,\cdots,a_{i-1})$，令$\mathbb{E}\subseteq\mathbb{F}(a_1,\cdots,a_t)$是$f(x)$在$\mathbb{F}$上分裂域，则$Gal(\mathbb{E}/\mathbb{F})$可解.

证明框架：关于t归纳. $t=1$ $\mathbb{F}\subseteq\mathbb{E}\subseteq\mathbb{F}(a_1)$，令$\mathbb{L}$是$x^{n_1}-a$在$\mathbb{F}$上分裂域 $\mathbb{F}\subseteq\mathbb{E}\subseteq\mathbb{L}$（$\mathbb{L}$是$\mathbb{E}$的正规扩张）（令$a=a_1^{n_1}$）

$Gal(\mathbb{E}/\mathbb{F}) \simeq Gal(\mathbb{L}/\mathbb{F}) / Gal(\mathbb{L}/\mathbb{E})$. 由前一定理，

$Gal(\mathbb{L}/\mathbb{F})$可解 $\Rightarrow Gal(\mathbb{E}/\mathbb{F})$可解.

设$t>1$，$\mathbb{L}$是$x^{n_1}-a$（令$a=a_1^{n_1}$）在$\mathbb{E}$上分裂域. $\Rightarrow \mathbb{L}$是$f(x)(x^{n_1}-a)$在$\mathbb{F}$上分裂域，令K是$x^{n_1}-a$在$\mathbb{F}$上分裂域 $\Rightarrow \mathbb{L}$是$f(x)$在K上分裂域

由假设$Gal(\mathbb{L}/K)$可解 $\Rightarrow Gal(\mathbb{L}/\mathbb{F})$可解 $\Rightarrow Gal(\mathbb{E}/\mathbb{F})$可解.

注：定理的逆命题也对.

定理 设 $f(x)\in\mathbb{Q}[x]$ 是 p 次不可约多项式，p 是素数，且 $f(x)$ 的全部根中除了两个，其余均属于 $\mathbb{R}$，令 $\mathbb{E}$ 是 $f(x)$ 在 $\mathbb{Q}$ 上 Galois 群，则 $Gal(\mathbb{E}/\mathbb{F})\simeq S_p$. $\mathbb{F}=\mathbb{Q}$

证明框架：令 $\mathbb{E}=\mathbb{Q}(r_1,\cdots,r_p)\subseteq\mathbb{C}$，则 $Gal(\mathbb{E}/\mathbb{F})\hookrightarrow S_p$

$p\mid[\mathbb{E}:\mathbb{Q}]=|Gal(\mathbb{E}/\mathbb{F})|\Rightarrow Gal(\mathbb{E}/\mathbb{F})$ 包含一个 p-循环.

$f(x)$ 有两个非实根，必共轭 $\Rightarrow Gal(\mathbb{E}/\mathbb{F})$ 包含一个对换. 使用：

S_n 是由 $(12),(12\cdots n)$ 生成的

例 $f(x)=3x^5-15x+5$，由 Eisenstein 判别法，它不可约.

$f(-2)=-61$，$f(-1)=17$，$f(0)=5$. $f(1)=-7$，$f(2)=71$

$\Rightarrow f(x)$ 在 $[-2,2]$ 有 3 个实根，因为 $f'(x)=15x^4-15$.

这 3 个实根是单根. 若有第 4 个实根（由罗尔定理）$\Rightarrow f'(x)=0$ 有三个实根，矛盾！因此另两根 $a+bi$，$a-bi$.

令 $\alpha_1,\alpha_2,\cdots,\alpha_5$ 是 $f(x)$ 在 $\mathbb{E}$ 中 5 个零点. $\mathbb{E}=\mathbb{Q}(\alpha_1,\cdots,\alpha_5)$

$Gal(\mathbb{E}/\mathbb{Q})\leqslant S_5$ $[\mathbb{Q}(\alpha_1):\mathbb{Q}]=5\Rightarrow(12345)\in Gal(\mathbb{E}/\mathbb{Q})$

$\mathbb{C}\to\mathbb{C}$ 共轭诱导了一个 $\sigma\in Gal(\mathbb{E}/\mathbb{Q})$ $\sigma(a+bi)=a-bi$.

$\Rightarrow\sigma=(12)\in Gal(\mathbb{E}/\mathbb{Q})$.

因为 S_5 不可解群 $\Rightarrow f(x)$ 不能根式求解（在 $\mathbb{Q}$ 上）.

（一些证明细节见下页）

Theorem 32.2 Condition for Gal (E/F) to be Solvable

Let F be a field of characteristic 0 and let $a \in F$. If E is the splitting field of $x^n - a$ over F, then the Galois group $\mathrm{Gal}(E/F)$ is solvable.

PROOF We first handle the case where F contains a primitive nth root of unity ω. Let b be a zero of $x^n - a$ in E. Then the zeros of $x^n - a$ are $b, \omega b, \omega^2 b, \ldots, \omega^{n-1}b$, and therefore $E = F(b)$. In this case, we claim that $\mathrm{Gal}(E/F)$ is Abelian and hence solvable. To see this, observe that any automorphism in $\mathrm{Gal}(E/F)$ is completely determined by its action on b. Also, since b is a zero of $x^n - a$, we know that any element of $\mathrm{Gal}(E/F)$ sends b to another zero of $x^n - a$. That is, any element of $\mathrm{Gal}(E/F)$ takes b to $\omega^i b$ for some i. Let ϕ and σ be two elements of $\mathrm{Gal}(E/F)$. Then, since $\omega \in F$, ϕ and σ fix ω and $\phi(b) = \omega^j b$ and $\sigma(b) = \omega^k b$ for some j and k. Thus,

$$(\sigma\phi)(b) = \sigma(\phi(b)) = \sigma(\omega^j b) = \sigma(\omega^j)\sigma(b) = \omega^j\omega^k b = \omega^{j+k}b,$$

whereas

$$(\phi\sigma)(b) = \phi(\sigma(b)) = \phi(\omega^k b) = \phi(\omega^k)\phi(b) = \omega^k\omega^j b = \omega^{k+j}b,$$

so that $\sigma\phi$ and $\phi\sigma$ agree on b and fix the elements of F. This shows that $\sigma\phi = \phi\sigma$, and therefore $\mathrm{Gal}(E/F)$ is Abelian.

Now suppose that F does not contain a primitive nth root of unity. Let ω be a primitive nth root of unity and let b be a zero of $x^n - a$ in E. The case where $a = 0$ is trivial, so we may assume that $b \neq 0$. Since ωb is also a zero of $x^n - a$, we know that both b and ωb belong to E, and therefore $\omega = \omega b/b$ is in E as well. Thus, $F(\omega)$ is contained in E, and $F(\omega)$ is the splitting field of $x^n - 1$ over F. Analogously to the case above, for any automorphisms ϕ and σ in $\mathrm{Gal}(F(\omega)/F)$ we have $\phi(\omega) = \omega^j$ for some j and $\sigma(\omega) = \omega^k$ for some k. Then,

$$\begin{aligned}(\sigma\phi)(\omega) &= \sigma(\phi(\omega)) = \sigma(\omega^j) = (\sigma(\omega))^j = (\omega^k)^j \\ &= (\omega^j)^k = (\phi(\omega))^k = \phi(\omega^k) = \phi(\sigma(\omega)) = (\phi\sigma)(\omega).\end{aligned}$$

Since elements of $\mathrm{Gal}(F(\omega)/F)$ are completely determined by their action on ω, this shows that $\mathrm{Gal}(F(\omega)/F)$ is Abelian.

Because E is the splitting field of $x^n - a$ over $F(\omega)$ and $F(\omega)$ contains a primitive nth root of unity, we know from the case we have already done that $\mathrm{Gal}(E/F(\omega))$ is Abelian and, by Part 2 of Theorem 32.1, the series

$$\{e\} \subseteq \mathrm{Gal}(E/F(\omega)) \subseteq \mathrm{Gal}(E/F)$$

is a normal series. Finally, since both $\text{Gal}(E/F(\omega))$ and

$$\text{Gal}(E/F)/\text{Gal}(E/F(\omega)) \approx \text{Gal}(F(\omega)/F)$$

are Abelian, $\text{Gal}(E/F)$ is solvable. ∎

To reach our main result about polynomials that are solvable by radicals, we need two important facts about solvable groups.

Theorem 32.5 (Galois) Solvable by Radicals Implies Solvable Group

Let F be a field of characteristic 0 and let $f(x) \in F[x]$. Suppose that $f(x)$ splits in $F(a_1, a_2, \ldots, a_t)$, where $a_1^{n_1} \in F$ and $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, t$. Let E be the splitting field for $f(x)$ over F in $F(a_1, a_2, \ldots, a_t)$. Then the Galois group $\text{Gal}(E/F)$ is solvable.

PROOF We use induction on t. For the case $t = 1$, we have $F \subseteq E \subseteq F(a_1)$. Let $a = a_1^{n_1}$ and let L be a splitting field of $x^{n_1} - a$ over F. Then $F \subseteq E \subseteq L$, and both E and L are splitting fields of polynomials over F. By part 2 of Theorem 32.1, $\text{Gal}(E/F) \approx \text{Gal}(L/F)/\text{Gal}(L/E)$. It follows from Theorem 32.2 that $\text{Gal}(L/F)$ is solvable, and from Theorem 32.3 we know that $\text{Gal}(L/F)/\text{Gal}(L/E)$ is solvable. Thus, $\text{Gal}(E/F)$ is solvable.

Now suppose $t > 1$. Let $a = a_1^{n_1} \in F$, let L be a splitting field of $x^{n_1} - a$ over E, and let $K \subseteq L$ be the splitting field of $x^{n_1} - a$ over F. Then L is a splitting field of $(x^{n_1} - a)f(x)$ over F, and L is a splitting field of $f(x)$ over K. Since $F(a_1) \subseteq K$, we know that $f(x)$ splits in $K(a_2, \ldots, a_t)$, so the induction hypothesis implies that $\text{Gal}(L/K)$ is solvable. Also, Theorem 32.2 asserts that $\text{Gal}(K/F)$ is solvable, which, from Theorem 32.1, tells us that $\text{Gal}(L/F)/\text{Gal}(L/K)$ is solvable. Hence, Theorem 32.4 implies that $\text{Gal}(L/F)$ is solvable. So, by part 2 of Theorem 32.1 and Theorem 32.3, we know that the factor group $\text{Gal}(L/F)/\text{Gal}(L/E) \approx \text{Gal}(E/F)$ is solvable. ∎

Theorem 3.2. *Let $f(T) \in \mathbf{Q}[T]$ be an irreducible polynomial of prime degree p with all but two roots in $\mathbf{R}$. The Galois group of $f(T)$ over $\mathbf{Q}$ is isomorphic to S_p.*

Proof. Let $L = \mathbf{Q}(r_1, \ldots, r_p)$ be the splitting field of $f(T)$ over $\mathbf{Q}$. The permutations of the r_i's by $\mathrm{Gal}(L/\mathbf{Q})$ provide an embedding $\mathrm{Gal}(L/\mathbf{Q}) \hookrightarrow S_p$ and $\#\,\mathrm{Gal}(L/\mathbf{Q})$ is divisible by p by Theorem 2.9, so $\mathrm{Gal}(L/\mathbf{Q})$ contains an element of order p by Cauchy's theorem. In S_p, the only permutations of order p are p-cycles (Lemma 3.1). So the image of $\mathrm{Gal}(L/\mathbf{Q})$ in S_p contains a p-cycle.

We may take L to be a subfield of $\mathbf{C}$, since $\mathbf{C}$ is algebraically closed. Complex conjugation restricted to L is a member of $\mathrm{Gal}(L/\mathbf{Q})$. Since $f(T)$ has only two non-real roots by hypothesis, complex conjugation transposes two of the roots of $f(T)$ and fixes the others. Therefore $\mathrm{Gal}(L/\mathbf{Q})$ contains a transposition of the roots of $f(T)$. (This is the reason for the hypothesis about all but two roots being real.)

We now show the only subgroup of S_p containing a p-cycle and a transposition is S_p, so $\mathrm{Gal}(L/\mathbf{Q}) \cong S_p$. By suitable labeling of the numbers from 1 to p, we may let 1 be a number moved by the transposition, so our subgroup contains a transposition $\tau = (1a)$. Let σ be a p-cycle in the subgroup. As a p-cycle, σ acts on $\{1, 2, \ldots, p\}$ by a single orbit, so some σ^i with $1 \leq i \leq p-1$ sends 1 to a: $\sigma^i = (1a\ldots)$. This is also a p-cycle, because σ^i has order p in S_p and all elements of order p in S_p are p-cycles, so writing σ^i as σ and suitably reordering the numbers $2, \ldots, p$ (which replaces our subgroup by a conjugate subgroup), we may suppose our subgroup of S_p contains the particular transposition (12) and the particular p-cycle $(12\ldots p)$. For $n \geq 2$, it is a theorem in group theory that the particular transposition (12) and n-cycle $(12\ldots n)$ generate S_n, so our subgroup is S_p. $\square$

Consider $g(x) = 3x^5 - 15x + 5$. By Eisenstein's Criterion (Theorem 17.4), $g(x)$ is irreducible over Q. Since $g(x)$ is continuous and $g(-2) = -61$ and $g(-1) = 17$, we know that $g(x)$ has a real zero between -2 and -1. A similar analysis shows that $g(x)$ also has real zeros between 0 and 1 and between 1 and 2.

Each of these real zeros has multiplicity 1, as can be verified by long division or by appealing to Theorem 20.6. Furthermore, $g(x)$ has no more than three real zeros, because Rolle's Theorem from calculus guarantees that between each pair of real zeros of $g(x)$ there must be a zero of $g'(x) = 15x^4 - 15$. So, for $g(x)$ to have four real zeros, $g'(x)$ would have to have three real zeros, and it does not. Thus, the other two zeros of $g(x)$ are nonreal complex numbers, say, $a + bi$ and $a - bi$. (See Exercise 65 in Chapter 15.)

Now, let's denote the five zeros of $g(x)$ by a_1, a_2, a_3, a_4, a_5. Since any automorphism of $K = Q(a_1, a_2, a_3, a_4, a_5)$ is completely determined by its action on the a's and must permute the a's, we know that $\mathrm{Gal}(K/Q)$ is isomorphic to a subgroup of S_5, the symmetric group on five symbols. Since a_1 is a zero of an irreducible polynomial of degree 5 over Q, we know that $[Q(a_1):Q] = 5$, and therefore 5 divides $[K:Q]$. Thus, the Fundamental Theorem of Galois Theory tells us that 5 also divides $|\mathrm{Gal}(K/Q)|$. So, by Cauchy's Theorem (corollary to Theorem 24.3), we may conclude that $\mathrm{Gal}(K/Q)$ has an element of order 5. Since the only elements in S_5 of order 5 are the 5-cycles, we know that $\mathrm{Gal}(K/Q)$ contains a 5-cycle. The mapping from $\mathbf{C}$ to $\mathbf{C}$, sending $a + bi$ to $a - bi$, is also an element of $\mathrm{Gal}(K/Q)$. Since this mapping fixes the three real zeros and interchanges the two complex zeros of $g(x)$, we know that $\mathrm{Gal}(K/Q)$ contains a 2-cycle. But, the only subgroup of S_5 that contains both a 5-cycle and a 2-cycle is S_5. (See Exercise 25 in Chapter 25.) So, $\mathrm{Gal}(K/Q)$ is isomorphic to S_5. Finally, since S_5 is not solvable (see Exercise 27), we have succeeded in exhibiting a fifth-degree polynomial that is not solvable by radicals.