Galois Theory

Wei Wenqing

2021.8.31

$$ax^2 + bx + c = 0 \longrightarrow x_1, x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$
$$x^3 + px + q = 0 \longrightarrow$$

$$x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$x_2 = \omega\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$x_3 = \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Definition

Let F be a field and $f(x) \in F[x]$. We say $f(x)$ is solvable by radicals if there exists a sequence of field extension:

$$F \to F(u_1) \to F(u_1, u_2) \cdots F(u_1, u_2, ..., u_n)$$

(1) for each $i = 1, 2, ..., n$, there exists a $n_i \in \mathbb{N}_+$ such that $u_i^{n_i} \in F(u_1, ..., u_(i - 1))$
(2) the splitting field of $f(x)$ over F is contained in $F(u_1, u_2, ..., u_n)$

If the splitting field of $f(x)$ over F is contained in $F(u_1, u_2, ..., u_n)$, then every root of $f(x)$ has a form

$$\frac{h(u_1, u_2, ..., u_n)}{g(u_1, u_2, ..., u_n)}$$

$h(x_1, ..., x_n)$, $g(x_1, ..., x_n)$ are polynomials.
we can know it is a combination of elements in F with $+, -, \times$, $\div$, and $\sqrt[r]{*}$.

Let K be a field extension of F, consider all the field isomorphisms of K which map every elements in F to itself (called $F - isomorphism$).
For exmaple, $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ provides that

$$a + b\sqrt{2} \mapsto a - b\sqrt{2}$$

is a $F - isomorphism$.
Denote $Gal(K/F)$ as the set of all the $F - isomorphisms$. It is easy to prove that $Gal(K/F)$ is a group.
For any subgroup H of $Gal(K/F)$, denote K^H as the set of all the elements in K which map to itself for every morphism in H. It is easy to prove that K^H is a field.

Definition

K is called a Galois extension of F if

$$F = K^{Gal(K/F)}$$

Theorem

Galois Theory If K is a finite dimensional Galois extension of F, then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the $Gal(K/F)$, given by

$$E \mapsto Gal(K/E)$$

(1) the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups.
(2) E is an intermediate field of K, F, then E is Galois over F if and only if $Gal(K/E)$ is a normal subgroup of $Gal(K/F)$

$$Gal(K/E) \triangleleft Gal(K/F)$$

$$F \to F_1 \to F_2 \to \cdots \to F_n$$

we can extend this squence of field extensions to

$$F = F_0 \to F_1' \to F_2' \to \cdots \to F_n'$$

such that for any $0 \le i < j \le n$, F_j' is a Galois extension of F_i'. Thus,

$$Gal(F_n'/F_0') \rhd Gal(F_n'/F_1') \rhd \cdots \rhd Gal(F_n'/F_{n-1}') \rhd \{id\}$$

And after studying, we find that

$$Gal(F_n'/F_i')/Gal(F_n'/F_{i+1}') \cong Gal(F_{i+1}'/F_i')$$

and $Gal(F_{i+1}'/F_i')$ is a commutative group.

Therefore, we get information about groups.

$$G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{id\}$$

and for any $i \in 0, 1, ...n-1$

$$G_i/G_{i+1}$$

is commutative group. we say such kind of G_0 is solvable. If group G is solvable, then any subgroup of G is also solvable. Therefore, assume the splitting field of $f(x)$ over F is E, then $Gal(E/F)$ is solvable.
Now we turn to study the structure of Galois group for Galois extension.

Theorem

$CharF = 0$, Let K be an finite dimensional algebraic extension of F, K is Galois extension of F if and only if K is a splitting field of a polynomial in $F[x]$.

Therefore, assume K is a splitting of $l(x) \in F[x]$ over F, assume $l(x)$ has different roots $u_1, u_2, ...u_k$, then $K = F(u_1, u_2, ..., u_k)$. So any $\alpha \in K$ has form

$$\frac{h(u_1, u_2, ..., u_k)}{g(u_1, u_2, ..., u_k)}$$

$h(x_1, ..., x_k)$, $g(x_1, ..., x_k) \in F(x_1, ..., x_k)$
For $\sigma \in Gal(K/F)$, what's the relation between α and $\sigma(\alpha)$?

assume $l(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then

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

act σ on two sides of the equation, we get

$$\sigma(a_n)\sigma(u_i)^n + \sigma(a_{n-1})\sigma(u_i)^{n-1} + \cdots + \sigma(a_1)\sigma(u_i) + \sigma(a_0) = 0$$

$$a_n\sigma(u_i)^n + a_{n-1}\sigma(u_i)^{n-1} + \cdots + a_1\sigma(u_i) + a_0 = 0$$

so for any $i \in 1, 2, ..., k$, $\sigma(u_i)$ is also a root of $f(x)$.
Therefore, $\sigma(u_1), ..., \sigma(u_k)$ is a permutation of $u_1, ..., u_k$, and

$$\sigma(\alpha) = \sigma(\frac{h(u_1, u_2, ..., u_k)}{g(u_1, u_2, ..., u_k)}) = \frac{h(\sigma(u_1), \sigma(u_2), ..., \sigma(u_k))}{g(\sigma(u_1), \sigma(u_2), ..., \sigma(u_k))}$$

$\sigma \in Gal(K/F)$ is uniquely determined by the values of $\sigma(u_1), \sigma(u_2), ..., \sigma(u_k)$. Therefore, σ uniquely link to a permutation given by

$$\begin{pmatrix} 1 & 2 & \cdots & k \\ i_1 & i_2 & \cdots & i_k \end{pmatrix}$$

$$\begin{pmatrix} u_1 & u_2 & \cdots & u_k \\ \sigma(u_1) = u_{i_1} & \sigma(u_2) = u_{i_2} & \cdots & \sigma(u_k) = u_{i_k} \end{pmatrix}$$

$Gal(K/F)$ is isomorphic to a subgroup of the symmetric group S_n.

At last, we transform the polynomial equation problem to a group problem. The splitting field of $f(x)$ over F is E, then $Gal(E/F)$ is solvable. It means a subgroup of symmetric group, G_0, is solvable

$$G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{id\}$$

and for any $i \in \{0, 1, ...n-1\}$

$$G_i/G_{i+1}$$

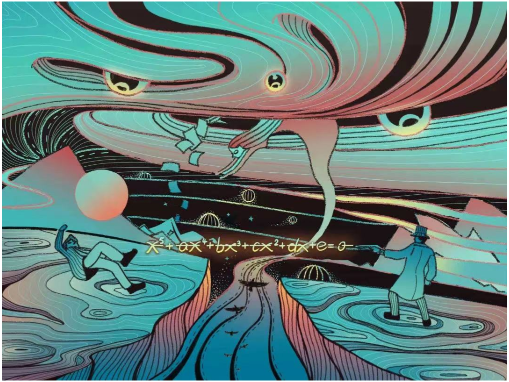
is commutative group.

Theorem

For $n \geq 5$, the alternating group A_n is simple group, which means A_n has no proper normal subgroup.

Therefore, for $n \geq 5$, A_n and S_n are not solvable(A_n is not commutative group). And there exists a lot of polynomial with degree ≥ 5 whose Galois group of splitting field is isomorphism to S_n.

polynomial has radical solution $\longrightarrow$ field extension problem $\xrightarrow{\textit{Galois Theory}}$ group problem $\xrightarrow{\textit{roots} \quad \textit{correspondence}}$ symmetric group problem



The problem of whether polynomials have radical solutions is much harder than the Galois theory itself. But the Galois theory is much more valuable than the problem itself.