Galois group of polynomials, Insovability of the Quintics

Useful tool: Linear independence of characters

Definition. Let H be an abelian group and let L be a field.

A character (特征) χ of H with values in L is group homomorphism

$$\chi : H \longrightarrow \underset{\nwarrow \text{ mult. gp of } L = L \setminus \{0\}}{L^{\times}}$$

Theorem (Artin's linear independence of characters)

If $\chi_1, \cdots, \chi_n$ are distinct characters of a group H with values in L,

then they are linearly independent as functions on H,

i.e. $\nexists\ a_1, \cdots, a_n$ not all zero, s.t. $a_1\chi_1(h) + \cdots + a_n\chi_n(h) = 0\ \forall h \in H$.

(Main application: $H = L^{\times}$, $\chi_i \leftrightarrow$ embeddings $\sigma_i : L \to L$.)

Proof: Suppose that they are linearly dependent.

Then among all linear relations, there's one with minimal number of $a_i \neq 0$

WLOG $a_1\chi_1 + \cdots + a_r\chi_r = 0$ (as functions on H)

Then $\forall h \in H$, $a_1\chi_1(h) + \cdots + a_r\chi_r(h) = 0$

Since $\chi_1 \neq \chi_r$, $\exists h_0 \in H$ s.t. $\chi_1(h_0) \neq \chi_r(h_0)$

$\rightsquigarrow \quad a_1\chi_1(h_0 h) + \cdots + a_r\chi_r(h_0 h) = 0$

$\Rightarrow a_1\chi_1(h_0)\chi_1(h) + \cdots + a_r\chi_r(h_0)\chi_r(h) = 0$

$$\to \underbrace{a_2(\chi_1(h_0) - \chi_2(h_0))}_{= b_2} \cdot \chi_2(h) + \cdots + \underbrace{a_r(\chi_1(h_0) - \chi_r(h_0))}_{= b_r}\chi_r(h) = 0$$

This gives a linear relation with small number of χ_i's

- Cyclic extensions.

Definition The extension K/F is called cyclic if K/F is Galois and $\mathrm{Gal}(K/F)$ is cyclic

Proposition Assume ① $\operatorname{char} F \nmid n$

② F contains all n^{th} roots of unity.

Then $K = F(\sqrt[n]{a})$ is a cyclic extension of degree dividing n.

Proof: $x^n - a = (x - \sqrt[n]{a})(x - \zeta_n \sqrt[n]{a}) \cdots (x - \zeta_n^{n-1} \sqrt[n]{a})$ ← separable polynomial

So K is the splitting field of $x^n - a$ over F

$$\begin{array}{c} K = F(\sqrt[n]{a}) \\ | \\ F \end{array} \qquad \forall \sigma \in \operatorname{Gal}(K/F),\ \sigma(\sqrt[n]{a}) = \zeta_n^{\lambda(\sigma)} \cdot \sqrt[n]{a} \text{ for some } \lambda(\sigma) \in \{0, 1, \cdots, n-1\}$$

$\rightsquigarrow$ get an injective map $\operatorname{Gal}(K/F) \longrightarrow \mu_n \simeq \mathbb{Z}_n$

$$\sigma \longmapsto \zeta_n^{\lambda(\sigma)} \leftrightarrow \lambda(\sigma)$$

b/c σ is determined by where $\sqrt[n]{a}$ is sent.

This is a homomorphism: $\forall \tau, \sigma \in \operatorname{Gal}(K/F)$

$$\tau\sigma : \sqrt[n]{a} \xmapsto{\sigma} \zeta_n^{\lambda(\sigma)} \sqrt[n]{a} \xmapsto{\tau} \zeta_n^{\lambda(\sigma)} \cdot \zeta_n^{\lambda(\tau)} \sqrt[n]{a} \qquad \text{So } \lambda(\tau\sigma) = \lambda(\tau) + \lambda(\sigma)$$

$\operatorname{Gal}(K/F) \hookrightarrow \mathbb{Z}_n$ injective $\Rightarrow \operatorname{Gal}(K/F)$ is a cyclic subgroup of order $| n$.

Theorem (Kummer theory) If F is a field s.t. $\operatorname{char} F \nmid n$ and F contains all n^{th} roots of unity.

Then any cyclic field extension K/F of degree n is of the form $K = F(\sqrt[n]{a})$ for some $a \in F^\times$

Proof: $\begin{array}{c} K \\ | \\ F \end{array}$ Let $\operatorname{Gal}(K/F) \simeq \mathbb{Z}_n = \langle \sigma \rangle$

For $\alpha \in K$, define $b := \alpha + \zeta_n \sigma(\alpha) + \cdots + \zeta_n^{n-1} \sigma^{n-1}(\alpha)$ ← Lagrange resolvent 拉格朗日预解式.

By linear independent of characters, $1, \sigma, \cdots, \sigma^{n-1} : K \to K$ are linearly independent.

$\Rightarrow \exists\, \alpha$ s.t. $b \neq 0$

__Note__: $\sigma(b) = \sigma(\alpha) + \zeta_n \sigma^2(\alpha) + \cdots + \zeta_n^{n-1} \sigma^n(\alpha) = \zeta_n^{-1} \cdot b$

$\Rightarrow \sigma(b^n) = (\zeta_n^{-1} b)^n = b^n =: a$ ← This is why we choose b in such a form.

Then $\sqrt[n]{a} = b \in K$

__Note__: $\forall \sigma^i$, $\sigma^i(\sqrt[n]{a}) = \zeta_n^{-i} \cdot \sqrt[n]{a}$. So $\sqrt[n]{a}$ is not contained in any intermediate fields

$\Rightarrow K = F(\sqrt[n]{a})$

(In principle, we may solve for α by radicals.)

From now on, we assume $\operatorname{char} F = 0$

<u>Definition</u> An element α algebraic$/F$ can be <u>expressed by radicals</u> or <u>solved in terms of radicals</u> if $\alpha \in K$ for some finite extension K/F admitting a succession of simple extensions (根式求解)

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K \qquad (*) \quad , \text{ where } K_{i+1} = K_i\left(\sqrt[n_i]{a_i}\right) \leftarrow \text{called radical extensions}$$

E.g. $\alpha = \sqrt[5]{\sqrt{5+\sqrt{7}} + \sqrt[4]{\sqrt{13}+\sqrt{17}}}$

<u>Proposition</u> If an element $\alpha \in K$ can be expressed by radicals, then α is contained in a Galois extension L of F satisfying $(*)$.

Proof:

$$\begin{tikzcd}[column sep=small]
K_s \arrow[d, dash] & & \sigma(K_s) \arrow[d, dash] \\
\vdots \arrow[d, dash] & & \vdots \arrow[d, dash] \\
K_1 \arrow[dr, dash] & & \sigma(K_1) \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

Let L be the Galois closure of K/F.

$\forall\, \sigma \in \operatorname{Hom}_F(K, L)$, $K_s\,\sigma(K_s)$ is an extension of F filtered by radical extensions

continue this way proves the proposition.

<u>Theorem</u> An (irreducible) polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group.

$\quad\uparrow$ meaning the Galois group of the splitting field.

Proof: "$\Rightarrow$" As in the proposition, $f(x)$ splits over L/F

$$\text{s.t. } F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L \qquad K_i = K_{i-1}\left(\sqrt[n_i]{a_i}\right)$$

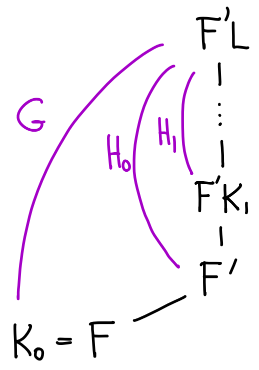
$$\begin{tikzcd}[column sep=small, row sep=small]
K_r = L \arrow[r, dash] \arrow[d, dash] & F'L \arrow[d, dash] \\
\vdots \arrow[d, dash] & \vdots \arrow[d, dash] \\
K_1 \arrow[r, dash] \arrow[d, dash] & F'K_1 \arrow[d, dash] \\
K_0 = F \arrow[r, dash] & F'
\end{tikzcd}$$

Define $F' = F(\zeta_{n_1}, \cdots, \zeta_{n_r})$ Galois extension of F

$F'L$ is Galois over F

Moreover, each $F'K_i = F'K_{i-1}\left(\sqrt[n_i]{a_i}\right)$ is Galois over $F'K_{i-1}$

On the group side, $G = \operatorname{Gal}(F'L/F)$.



Write $H_i = \mathrm{Gal}(F'L/F'K_i)$

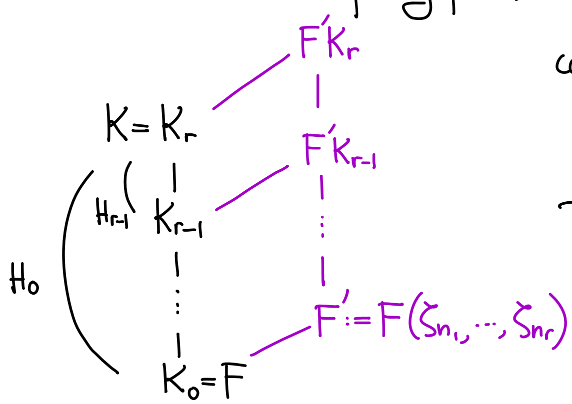
As F'/F is Galois $\Rightarrow H_0 \trianglelefteq G$ and G/H_0 is abelian

$F'K_1/F'$ is Galois $\Rightarrow H_1 \trianglelefteq H_0$ and H_0/H_1 is abelian

. . . . . .

$\Rightarrow G$ is solvable $\Rightarrow \mathrm{Gal}(L/F)$ is solvable

"$\Leftarrow$" Let K be a splitting field, and we have a tower $K_r/K_{r-1}/\cdots$



corresponding to $\{1\} = H_r \leqslant \cdots \leqslant H_0 = G$

s.t. $H_{i+1} \trianglelefteq H_i$ and H_i/H_{i+1} = cyclic of order n_i.

Put $F' := F(\zeta_{n_1}, \cdots, \zeta_{n_r})$

Then $F'K_{i+1} = F'K_i(\sqrt[n_i]{a_i})$ by Kummer theory

$\Rightarrow$ solvable by radicals

Corollary. If an equation has Galois group $\simeq S_n$ or A_n with $n \geqslant 5$ (e.g. general irreducible polynomial of deg n), then it is not solvable by radicals.

Explicit Galois group of a polynomial

Definition. Let F be a field and $f(x) \in F[x]$ a separable polynomial

$K :=$ splitting field of $f(x)$ over F. Define the Galois group for $f(x)$ to be $\mathrm{Gal}(K/F)$.

Example. Galois group for $x^7 - 5$ over $\mathbb{Q}$ (irred. by Eisenstein criterion)

The splitting field is $\mathbb{Q}(\sqrt[7]{5}, \zeta_7)$. The associated Galois group is $\mathbb{Z}_7 \rtimes (\mathbb{Z}/7\mathbb{Z})^\times$

Question. How to determine the Galois group of a polynomial $f(x)$?

- May assume that $f(x)$ has no repeated zeros ; $\deg f(x) = n$.

$K \qquad f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$

$$\begin{array}{c} | \\ F \end{array} \qquad \mathrm{Gal}(K/F) \text{ acts on } \{\alpha_1, \dots, \alpha_n\} \rightsquigarrow G = \mathrm{Gal}(K/F) \hookrightarrow S_n$$

<u>Example</u> F field $\rightsquigarrow$ function field $F(x_1, \dots, x_n)$ "universal case"

Define the <u>elementary symmetric functions</u> to be

$$s_1 = x_1 + \dots + x_n, \quad s_2 = \sum_{i<j} x_i x_j, \quad \dots, \quad s_n = x_1 x_2 \cdots x_n$$

$$\rightsquigarrow \begin{array}{c} F(x_1, \dots, x_n) =: M \\ | \\ F(s_1, \dots, s_n) =: L \end{array}$$

<u>Note</u>: $f(x) = (x - x_1) \cdots (x - x_n)$

$$= x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n \in L[x]$$

$\rightsquigarrow$ M is the splitting field of $f(x)$ over L (& $f(x)$ is separable)

<u>Proposition</u>. The fixed field of M under S_n is L.

Proof: M is Galois $/L$ $\rightsquigarrow$ $\mathrm{Gal}(M/L) \hookrightarrow S_n$

On the other hand, S_n acts on M, fixing L

$\rightsquigarrow S_n \subseteq \mathrm{Gal}(M/L)$.

$\Rightarrow \mathrm{Gal}(M/L) = S_n$

<u>Slogan</u>: Model the process of solving equations by the universal function field case.

① <u>Universal version</u>
$$\begin{array}{c} F(x_1, \dots, x_n) \\ | \\ F(s_1, \dots, s_n) \end{array}$$

Consider the "discriminant" $\tilde{D} = \prod_{1 \le i < j \le n} (x_i - x_j)^2 \rightsquigarrow \sqrt{\tilde{D}} = \prod_{1 \le i < j \le n} (x_i - x_j)$

$\sigma \in S_n$ acts on $F(x_1, \dots, x_n)$, $\sigma(\sqrt{\tilde{D}}) = \mathrm{sgn}(\sigma) \sqrt{\tilde{D}}$

where $\mathrm{sgn}: S_n \longrightarrow \{\pm 1\}$, $\ker(\mathrm{sgn}) = A_n$

$$\rightsquigarrow \begin{array}{ccc} M = F(x_1, \dots, x_n) & & \\ & \diagdown^{A_n} & \\ S_n \Big| & & L(\sqrt{\tilde{D}}) \\ & \diagup_{\{\pm 1\}} & \\ L = F(s_1, \dots, s_n) & & \end{array}$$

② <u>Number field version</u> K/F splitting field of irreducible polynomial $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$

Put $D = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in F$ b/c any $\sigma \in \mathrm{Gal}(K/F)$ keeps the expression invariant.

<u>Claim</u>. $\mathrm{Gal}(K/F) \subseteq A_n$ if and only if D is a square in F.

Proof: Note that $\delta := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \in K$ is a square root of D

For $\sigma \in \mathrm{Gal}(K/F)$, $\sigma(\delta) = \mathrm{sgn}(\sigma) \cdot \delta$

So $\mathrm{Gal}(K/F) \subseteq A_n \iff \forall \sigma \in \mathrm{Gal}(K/F),\ \sigma(\delta) = \delta \iff \delta \in F$ $\square$

In fact, we prove that

$$\begin{tikzcd} K = F(\alpha_1, \dots, \alpha_n) \arrow[d, dash, "G"'] \arrow[dr, dash, "G \cap A_n"] & \\ F \arrow[r, dash] & F(\sqrt{D}) \end{tikzcd}$$

$F(\sqrt{D}) = F \iff G \subseteq A_n$

③ Determine the Galois group of an irreducible cubic $f(x) = x^3 + ax^2 + bx + c$

$\rightsquigarrow f(x) = x^3 + px + q$ with zeros α, β, γ

$$\begin{tikzcd} F = \mathbb{Q}(\alpha, \beta, \gamma) \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q} \arrow[r, dash] & \mathbb{Q}(\sqrt{D}) \arrow[r, dashed, dash] & \mathbb{Q}(\sqrt{D}, \omega) \text{ for } \omega = e^{2\pi i/3} \end{tikzcd}$$

$D = (\alpha - \beta)^2 (\beta - \gamma)^2 (\gamma - \alpha)^2 = -4p^3 - 27q^2$

So if D is a square, $\mathrm{Gal}(F/\mathbb{Q}) = A_3 = \mathbb{Z}_3$

if D is not a square, $\mathrm{Gal}(F/\mathbb{Q}) = S_3$.

To solve for α, consider $\theta_1 := \alpha + \omega\beta + \omega^2\gamma$ $\leftarrow$ Lagrange resolvent from Kummer theory

$\theta_2 := \alpha + \omega^2\beta + \omega\gamma$

Then $\theta_1^3 = \cdots = \frac{-27}{2} q + \frac{3}{2}\sqrt{-3D}$

$\theta_2^3 = \cdots = \frac{-27}{2} q - \frac{3}{2}\sqrt{-3D}$ From this, we solve for α, β, γ.

④ Solving quartics $x^4 + ax^2 + bx + c$ (and determine the Galois group)

<u>Universal case</u> <u>Number field case</u>

$$
\begin{array}{c}
1 \\
| \\
K_4 = \text{Klein 4-group} = \{1, (12)(34), (13)(24), (14)(23)\} \\
3 \, | \\
A_4 \\
2 \, | \\
S_4
\end{array}
\qquad
\begin{array}{c}
M = F(x_1, x_2, x_3, x_4) \\
| \\
M^{K_4} = L(\sqrt{\tilde{D}}, \tilde{\theta}_1, \tilde{\theta}_2, \tilde{\theta}_3) \\
| \\
L(\sqrt{\tilde{D}}) \\
| \\
L = F(s_1, s_2, s_3, s_4)
\end{array}
\qquad
\begin{array}{l}
\tilde{\theta}_1 = (x_1+x_2)(x_3+x_4) \\
\tilde{\theta}_2 = (x_1+x_3)(x_2+x_4) \\
\tilde{\theta}_3 = (x_1+x_4)(x_2+x_3)
\end{array}
$$

$$
\begin{array}{c}
K \\
G \cap K_4 \;\; | \\
F(\sqrt{D})(\theta_1, \theta_2, \theta_3) \\
| \;\; G \cap A_4 \\
F(\sqrt{D}) \\
| \\
F
\end{array}
\qquad G
$$

$$\theta_1 := (\alpha_1+\alpha_2)(\alpha_3+\alpha_4), \; \theta_2 := (\alpha_1+\alpha_3)(\alpha_2+\alpha_4), \; \theta_3 := (\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$$

By working upwards of the right tower to get $G \cap A_4$, $G \cap K_4$, ...
usually enough to determine G

<u>Steps of solving the quartics</u>:

① First solve for $\sqrt{D}$

② then solve $\eta_1 = \underbrace{\theta_1 + \omega\theta_2 + \omega^2\theta_3}_{\text{cubic root of something}}$, $\eta_2 = \theta_1 + \omega^2\theta_2 + \omega\theta_3$, $\eta_3 = \theta_1 + \theta_2 + \theta_3 = 2a$

$\Rightarrow \theta_1, \theta_2, \theta_3$ ✓

③ Now, we know K^{K_4}. Say want to solve for $K^{\{1, (12)(34)\}}$

generators are $\alpha_1 + \alpha_2$, $\alpha_3 + \alpha_4$

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0 \\ (\alpha_1+\alpha_2)(\alpha_3+\alpha_4) = \theta_1 \; ✓ \end{cases} \Rightarrow \text{both } \alpha_1+\alpha_2, \, \alpha_3+\alpha_4 \text{ are known.}$$

....