03/05/2021

<u>Examples</u> Galois group of the splitting field of cubic and quartic equation

(1) $f(T) = T^3 + b_1 T^2 + b_2 T + b_3 \in k[T]$, separable irreducible

$= (T-\alpha_1)(T-\alpha_2)(T-\alpha_3)$, $E = k(\alpha_1, \alpha_2, \alpha_3)$ = a splitting field of $f(T)$

$\rightsquigarrow \mathrm{Gal}(E/k) \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } [E:k]=3 \\ S_3 & \text{if } [E:k]=6 \end{cases}$

$[E:k]$ = either 3 or 6

$\because$ $E/k(\alpha_1)$ is the splitting field of a quadratic poly with coeff in $k(\alpha_1)$ namely, $f(T)/(T-\alpha_1)$

$\because$ $\mathrm{Gal}(E/k) \hookrightarrow \mathrm{Perm}(\{\alpha_1,\alpha_2,\alpha_3\}) \cong S_3$

Q. <u>How to distinguish these two cases?</u>

$\mathrm{Gal}(E/k) \leq S_3$

operates transitively on $\{1,2,3\}$ $\rightsquigarrow$ S_3 either A_3 or S_3

Can distinguish these two cases by $G/(G\cap A_3)$

$G/(G\cap A_3) = \begin{cases} \{1\} \\ \mathbb{Z}/2\mathbb{Z} \end{cases}$ What is $E^{G\cap A_3}$ — the subgroup of $\mathrm{Gal}(E/k)=G$ which are even permutation.

$\mathbb{Z}/2\mathbb{Z}$ iff $\Delta \notin (k^\times)^2$

$\| $ Galois theory

$\mathrm{Gal}(E^{G\cap A_3}/k)$

Let $\Delta = (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)$

$\forall s \in \mathrm{Perm}(\{\alpha_1,\alpha_2,\alpha_3\})$,

$${}^s\Delta = (s(\alpha_1)-s(\alpha_2))(s(\alpha_2)-s(\alpha_3))(s(\alpha_1)-s(\alpha_3))$$
$$= (-1)^{\mathrm{sgn}(s)}\Delta$$

$$D \overset{\text{def}}{=} \Delta^2 = \prod_{1 \le i < j \le 3} (\alpha_i - \alpha_j)^2 \in k$$

discriminant of $f(T)$

$$E^{G \cap A_3} = k \iff D \text{ has a square root } (\pm\Delta) \text{ in } k$$

Classical formula for Δ: when $\alpha + \beta + \gamma = 0$.
i.e. $b_1 = 0$

$$\boxed{\Delta = -4b_2^3 - 27b_3^2}$$

$$g(T) = T^4 + b_1 T^3 + b_2 T^2 + b_3 T + b_4 \in k[T]$$
$$= \prod_{i=1}^{4} (T - \beta_i)$$

irreducible, separable.

$E = k(\beta_1, \beta_2, \beta_3, \beta_4)$

extension field, Galois.

k

Solvable!

$G = \mathrm{Gal}(E/k) \longleftrightarrow S_4 = \mathrm{Perm}(\{\beta_1, \dots, \beta_4\})$

operates transitively on $\{1, 2, 3, 4\}$

S_4 has a unique normal subgroup $V \cong (\mathbb{Z}/2\mathbb{Z})^2$

$V = \{1, (12)(34), (13)(24), (14)(23)\}$ a Klein 4.

$S_4 / V \cong S_3$

Q. Which subgroups $G \le S_4$ of S_4 operate transitively on $\{1, 2, 3, 4\}$?
(Classify them up to conjugation)

Constraint on $\#G$: $\#G \equiv 0 \pmod 4$

$\rightsquigarrow \#G = 4, 8, 12, 24$

Does G contain V? i.e. what can $V \cap G$ be?

$\#G = 24 \longleftrightarrow G = S_4$

$\#G = 12 \longleftrightarrow G = A_4 \supseteq V$

$\#G = 8 \longleftrightarrow G$ is a Sylow 2-subgroup of S_4 (there are 3 of them, conjugate to each other)

$\Rightarrow G \supseteq V$

$\#G = 4$

2 cases: either V

or G is a cyclic subgroup of order 4, generated by a 4-cycle

whether $G \supseteq V$, i.e. want to "know" $G \cap V$

$$E^{G\cap V} \supseteq k\Big(\underbrace{\beta_1\beta_2 + \beta_3\beta_4}_{=\gamma_1},\ \underbrace{\beta_1\beta_3 + \beta_2\beta_4}_{=\gamma_2},\ \underbrace{\beta_1\beta_4 + \beta_2\beta_3}_{=\gamma_3}\Big)$$

E

$|$ $G \cap V$

$k(\gamma_1, \gamma_2, \gamma_3)$

$|$

k

$\mathrm{Gal}(E/k(\gamma_1,\gamma_2,\gamma_3)) = G \cap V$

Question: Is $E^{G\cap V} \overset{?}{=} k(\gamma_1, \gamma_2, \gamma_3)$

$\supseteq$ know

Exer: Show $=$ holds!

Exer: $k(\gamma_1, \gamma_2, \gamma_3)$ is the splitting field of a cubic polynomial in $k[T]$ (coeff. given by classical formula)

$|$

k

$$\begin{array}{c} k(\gamma_1,\gamma_2,\gamma_3) \\ \Big| \\ k \end{array} \qquad \begin{tikzcd} \mathrm{Gal}(k(\gamma_1,\gamma_2,\gamma_3)/k) \cong G/(G\cap V) \arrow[r, hook] \arrow[d, hook] & S_3 \arrow[d, equal] \\ S_3/V \arrow[r, "\sim"] & S_3 \end{tikzcd}$$

In other words:

You can tell the 5 cases apart by looking at the Galois group of

$$\left.\begin{array}{c} k(\gamma_1,\gamma_2,\gamma_3) \\ \Big| \\ k \end{array}\right]$$

splitting field of the "resolvant poly" of $g(T)$

computed by elementary symmetric polynomials of $\gamma_1, \gamma_2, \gamma_3$

$\gamma_1, \gamma_2, \gamma_3$

Let $s_1(u_1, u_2, u_3)$, $s_2(u_1, u_2, u_3)$, $s_3(u_1, u_2, u_3)$ be the 3 elem. symm poly. in u_1, u_2, u_3

Resolvant poly:

$$R(T) = T^3 - s_1(\gamma_1,\gamma_2,\gamma_3)T^2 + s_2(\gamma_1,\gamma_2,\gamma_3)T - s_3(\gamma_1,\gamma_2,\gamma_3)$$

$s_i(\gamma_1, \gamma_2, \gamma_3) \in k \quad \forall i = 1, 2, 3$

because it is fixed by S_4.

Lemma: k: an infinite field

Given $k[X_1, \dots, X_n] \ni f(X_1, \dots, X_n) \neq 0$

Then: $\exists\, a_1, \dots, a_n \in k$ s.t. $f(a_1, \dots, a_n) \neq 0$.

(Proof by induction. $n=1$ trivial)

Induction step:

Write $f(X_1, \dots, X_n) = a_d(X_1, \dots, X_{n-1}) X_n^d + \dots + a_1(X_1, \dots, X_{n-1}) X_n + a_0(X_1, \dots, X_{n-1})$)

Cor: Given any finitely many non-zero polynomials $f_1, \dots, f_m \in k[X_1, \dots, X_n]$

$\exists\, a_1, \dots, a_n \in k$ st $f_i(a_1, \dots, a_n) \neq 0 \quad \forall i = 1, \dots, m$

(Consider $f = f_1 \cdots f_m$)

Application Artin's alg. indep. of characters.

Suppose E is a finite separable ext^n field of k

k: infinite field

$\sigma_1, \dots, \sigma_m : E \longrightarrow \Omega$

distinct k-linear ring homog from E to a alg. closed ext^n field Ω of k.

Let $F(T_1, \dots, T_m) \in \Omega[T_1, \dots, T_m]$

be a polynomial

s.t. $0 = F(\sigma_1(a), \dots, \sigma_m(a)) \quad \forall a \in E$.

Then $F(T_1, \dots, T_m) = 0$.