Recall: If $f(x) \in K[x]$ with distinct roots $\alpha_1, \dots, \alpha_n$ in some splitting field over K. Then the discriminant of f

$$\Delta_f = \prod_{i<j} (\alpha_j - \alpha_i) \qquad D_f = \Delta_f^2$$

If F is the splitting field and $\sigma \in Aut(F/K)$

$$\sigma(\Delta) = (-1)^{sgn(\sigma)} \Delta$$ where sgn is as a permutation of $\alpha_1, \dots, \alpha_n$.

Proof: Let $\tau = (i_0, j_0) \in S_n$, consider the action on

$$\Delta = \prod_{i<j} (\alpha_j - \alpha_i).$$

Terms $\alpha_j - \alpha_i$ with $\{j, i\} \cap \{j_0, i_0\} = \emptyset$

Suppose $|\{i, j\} \cap \{i_0, j_0\}| = 1$. WLOG, $i_0 < j_0$. If $i < i_0 < j_0$

τ swaps $(\alpha_{j_0} - \alpha_{i_0})$ and $(\alpha_{i_0} - i)$. If $j > j_0 > i_0$,

$(\alpha_j - \alpha_{j_0})$ swapped with $(\alpha_j - \alpha_{i_0})$. If $i_0 < i < j_0$

$$\tau(\alpha_{j_0} - \alpha_i) = \alpha_{i_0} - \alpha_i = -(\alpha_i - \alpha_{i_0})$$

$$\tau(\alpha_i - \alpha_{i_0}) = \alpha_i - \alpha_{j_0} = -(\alpha_{j_0} - \alpha_i)$$

So $(\alpha_{j_0} - \alpha_i)(\alpha_i - \alpha_{i_0})$ fixed by τ. The only term left is

$\alpha_{j_0} - \alpha_{i_0} \xrightarrow{\tau} -(\alpha_{j_0} - \alpha_{i_0}) \implies \tau(\Delta) = -\Delta \implies \sigma(\Delta) = (-1)^{\#swaps} \Delta$

So $\sigma(\Delta) = \Delta$ if and only if $\sigma \in A_n \cap Aut(F/K)$

$\implies K(\Delta)$ is the fixed field of $A_n \cap Gal(F/K)$.

Example: Let $char(K) \neq 2$ or 3, $f(x) \in K[x]$ an irreducible cubic, and F is a splitting field, then $Gal(F/K) \simeq S_3$ or $Gal(F/K) \simeq A_3$. But $Gal(F/K) \simeq A_3$ if and only if $\sigma(\Delta) = \Delta$ for all $\sigma \in Gal(F/K)$ if and only if $\Delta \in K$ if and only if D_f is a square in K.

For $f(x) = x^3 + Ax + B$. Then $D = -4A^3 - 27B^2$

Since $\operatorname{char}(K) \neq 3$, if $f(x) = x^3 + ax^2 + bx + c$,

$$f(x - \tfrac{a}{3}) = x^3 + Ax + B$$

Now, if $x^3 + Ax + B = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, then

$\alpha_1 + \alpha_2 + \alpha_3 = 0$, so $A = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$ and

$-B = \alpha_1\alpha_2\alpha_3$, $D = (\alpha_3 - \alpha_1)^2(\alpha_3 - \alpha_2)^2(\alpha_2 - \alpha_1)^2$

Example: If $f(x) = x^3 - B$ (irreducible) for $B \in \mathbb{Q}$, then $D = -27B^2 \notin \mathbb{Q}$,

so Galois group is S_3, because the splitting field is $\mathbb{Q}(\sqrt[3]{B}, \omega)$

with $\omega^3 = 1$, $\omega \neq 1$. Then $\mathbb{Q}(\Delta) = \mathbb{Q}(\sqrt{-27B^2}) = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$

Example: $x^3 + 3x + 1$ $D = 81 = 9^2 \in \mathbb{Q}$, so Galois group is

A_3

Degree Four Polynomials

Proposition: Let K be a field of characteristic not 2 or 3,

Let $f(x)$ be an irreducible quartic polynomial, F splitting

field, $\operatorname{Gal}(F/K) \hookrightarrow S_4$. Let $V \leq S_4$ generated by

$(12)(34)$, $(13)(24)$

$$V = \{ \mathrm{id}, (12)(34), (13)(24), (14)(23) \} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

If $f(x) = (x-u_1)(x-u_2)(x-u_3)(x-u_4)$, the following are

fixed by V

$$\alpha = u_1u_2 + u_3u_4, \quad \beta = u_1u_3 + u_2u_4, \quad \gamma = u_1u_4 + u_2u_3$$

In fact, $(x-\alpha)(x-\beta)(x-\gamma)$ is fixed by S_4. This is called the resolvent cubic. If

$$f(x) = x^4 + bx^3 + cx^2 + dx + e$$

then $f(x) = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$

$\alpha, \beta, \gamma \in F$, so $K(\alpha, \beta, \gamma) \subseteq F$ fixed by $V \cap Gal(F/K)$

$K(\alpha, \beta, \gamma)$ is the fixed field of $V \cap Gal(F/K)$.

Proposition: With $f(x)$, K as above, let $m = [K(\alpha, \beta, \gamma) : K]$ where $(x-\alpha)(x-\beta)(x-\gamma)$ is the resolvent cubic. Then

m	$Gal(F/K)$
6	S_4
3	A_4
2	D_4 or $\mathbb{Z}_4$
1	V

$D_4 \iff f(x)$ irreducible over $K(\alpha, \beta, \gamma)$.

$$[K(\alpha, \beta, \gamma) : K] = [Gal(F/K) : Gal(F/K) \cap V]$$

Example: $x^4 - 2$ in $\mathbb{Q}[x]$. The splitting field is then $\mathbb{Q}(2^{\frac{1}{4}}, i2^{\frac{1}{4}}, -2^{\frac{1}{4}}, -i2^{\frac{1}{4}}) = \mathbb{Q}(2^{\frac{1}{4}}, i)$

$$\sigma(i) = \pm i \qquad \sigma(2^{\frac{1}{4}}) = i^k 2^{\frac{1}{4}}$$

$\Rightarrow Gal(F/K) \simeq D_4$.

Resolvent cubic: $x^3 + 8x = x(x^2 + 8)$

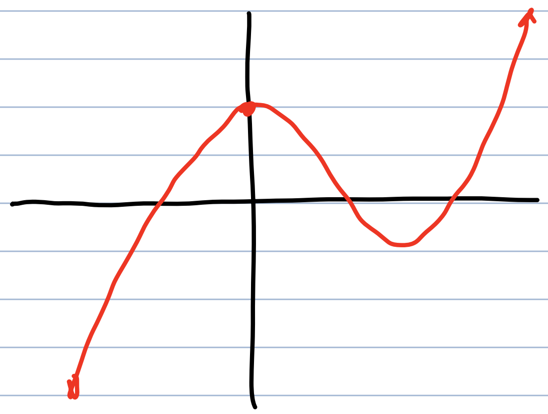
$K(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{-2})$ so $m = 2$. Note $x^4 - 2$ not reducible over $\mathbb{Q}(\sqrt{-2})$

Example: $x^4 + 2x + 2$ over $\mathbb{Q}[x]$. The resolvent cubic is $x^3 - 8x^2 - 4$ irreducible, so $m = 3$ or 6. $D = 1616 = 2^4 \cdot 101$

$\notin \mathbb{Q}^2$, so $m = 6$, Galois group of $x^4 + 2x + 2$ is S_4.

Theorem: Let p be a prime, $f(x) \in K[x]$ be irreducible of degree p, suppose $f(x)$ has exactly two nonreal roots. Then f has Galois group S_p.

Example: $x^5 - 4x + 2$ has Galois group S_5. Indeed, it is irreducible, has exactly 3 roots. (use calculus).



Proof: View the Galois group as a subgroup of S_p. Since $f(x)$ is irreducible, $f(\alpha) = 0$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, so $p \mid [F : \mathbb{Q}] = |Gal(F/\mathbb{Q})| \Rightarrow Gal(F/\mathbb{Q})$ contains an element of order p, so $Gal(F/\mathbb{Q})$ has a p-cycle.

On the other hand, $z \to \bar{z}$ gives an element of $Gal(F/\mathbb{Q})$. This element is a transposition in S_p. WLOG, the transp. is $(1\,2)$. Some power of the p-cycle is $(1\,2 \dots)$. WLOG the p-cycle $(1\,2 \dots p)$

$$\Rightarrow (2\,3) = (1\,2 \dots p)(1\,2)(1\,2 \dots p)^{-1}$$

$$(k, k+1) = (1\,2 \dots p)(k-1\;k)(1\,2 \dots p)^{-1}$$

$$(1\,3) = (1\,2)(2\,3)(1\,2)$$

$\vdots$

$$(1\ k) = (1\ k{-}1)(k{-}1\ k)(1\ k{-}1)$$

$$\Rightarrow (m\ k) = (1\ m)(1\ k)(1\ m)$$

so all transpositions are in $\langle (1\ 2), (1\ 2 \ldots, p) \rangle$, so this subgroup is S_p

Symmetric Polynomials

The generic quintic has Galois group S_5. There are specific polynomials (quintic) over $\mathbb{Q}$ with Galois group of S_5