Friday, April 19, 2019 11:28

$\sqrt{-3} \in F$: only needed to express roots of cubics/quartics in radicals.

$f(x) = x^4 + px^2 + qx + r$.

Roots are $\alpha_1, \ldots, \alpha_4$.

$K = F(\alpha_1, \ldots, \alpha_4)$

$G = Gal(K/F) = Gal(f)$.

D - discriminant of f.

R - cubic resolvent of f.

$$\begin{array}{c} 1 \\ \| \\ G \cap V_4 \\ \| \\ G \cap A_4 \\ \| \\ G \end{array} \quad \longleftrightarrow \quad \begin{array}{c} K \\ \| \\ L \\ \| \\ F(\sqrt{D}) \\ \| \\ F \end{array} \qquad L = Fix(G \cap V_4) = F(\theta_1, \theta_2, \theta_3).$$

Case 1 : R is irreducible.

Then $Gal(L/F) \cong S_3$ or $\mathbb{Z}_3$

(i) $\sqrt{D} \notin F$. Then $Gal(L/F) \cong S_3$

So $|G| \geq 6$. Also $4 \mid |G|$, so

either $G \cong A_4$ or S_4.

Since $\sqrt{D} \notin F$, $G \not\leq A_4$ so $G \cong S_4$.

(ii) $\sqrt{D} \in F$. Then $Gal(L/F) \cong \mathbb{Z}_3$.

But $4 \mid |G|$, so $|G| \geq 12$.

And $G \leq A_4$ so $G \cong A_4$.

Case 2: R splits completely: $\theta_1, \theta_2, \theta_3 \in F$.

Then $L = F$ so $G \cong Gal(K/L) \cong V_4$

Case 3: $R = (x - \theta_1) R_2$, (θ_1 or θ_2 or θ_3) $\theta_1 \in F$. R_2 is irreducible over F.

Then $Gal(L/F) \cong \mathbb{Z}_2$. $Gal(K/L) \leq V_4$.

So $|Gal(K/F)| = 8$ or 4.

($H_i \cong D_8$ or $C_i \cong \mathbb{Z}_4$).

$H_1 = \langle (12), (1324) \rangle$ } G is $\cong$ to one of these.

$C_1 = \langle (1\ 2\ 3\ 4) \rangle$

If f is irr-ble over $F(\sqrt{D})$, $G \cong H_1 \cong D_8$

Otherwise $G \cong C_1 \cong \mathbb{Z}_4$.

f - irr-ble $\Rightarrow |K:L| \geq 4$ so $|K:F| \geq 8$, so $G = H_1$.

↳ $|K:L| \geq 4$ so $|K:F| \geq 8$ so $G = H_1$

f reducible $\Rightarrow$ $f = f_1 f_2$ (quadratic), $f_1, f_2 \in F(\sqrt{D})(x)$

if $G = H_1$, then $G \cap V_4$ acts transitively on $\{\alpha_1, \ldots, \alpha_4\}$

So they are conjugate over $L = F(\sqrt{D})$,

So f is irr-ble over $F(\sqrt{D})$.

Examples. $x^3 - x - 1$ - irr-ble. $D = -23$,

(over $\mathbb{Q}$) So $Gal \cong S_3$

$x^3 - 3x - 1$ - irr-le. $D = 81 = 9^2$, $G \cong \mathbb{Z}_3$.

$x^4 - x - 1$ - irr-le over $\mathbb{Z}_2$ so over $\mathbb{Z}$ so over $\mathbb{Q}$ by Gauss Lemma.

$D = -283$, $R = x^3 + 4x + 1$ irr-le. So $G \cong S_4$.

↑ using $\theta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$

$x^4 + 8x + 12$ - irr-le. $D = 576^2$. $R = x^3 - 48x + 64$ - irr-le

$G \cong A_4$

$x^4 + 36x + 63$ $D = 4320^2$

Theorem: f - monic $\in \mathbb{Z}[x]$.

Let $p \nmid \deg f = n$.

↑ prime.

Then $Gal(f/\mathbb{Z}_p) \leq Gal(f/\mathbb{Q})$.

↑ cyclic group ↑ as groups of permutations of roots.

Let $f = f_1 \cdots f_k$

irr-le

. .

Let A_i be the set of roots of f_i, $|A_i| = \deg f_i$.

Then $\mathrm{Gal}(f/\mathbb{Q}_p)$

$\langle \sigma \rangle$ is transitive on each of A_i.

Then σ has cycle type $n_1, n_2, \ldots, n_k$

where $n_i = \deg f_i$.

So $G = \mathrm{Gal}(f/\mathbb{Q})$ contains an element of this cycle type.

Final: Friday, April 26, 12-2, Baker

or Tuesday, April 30, 10-12, Enarson

Examples from Keith Conrad