Lecture 17: Computing Galois groups of polynomials

Aim Lecture: Give some tips for computing $\mathrm{Gal}(f(x)/F)$ & consequences.

A quintic insolvable by radicals

Lemma: Fix prime p. Let $\tau, \sigma \in S_p$ be a 2-cycle & p cycle resp. Then $\langle \tau, \sigma \rangle = S_p$.

Proof: Re-labelling indices, we may assume

$\tau = (1\ 2)$, $\sigma = (n_1\ n_2 \dots n_p)$.

Pick i so $\sigma^i(1) = 2$. Then replacing σ with σ^i (which also has order p) & re-labelling if nec., we may further assume $\sigma = (1\ 2 \dots p)$.

Note $\langle \sigma, \tau \rangle \ni \sigma^j \tau \sigma^{-j} = (\sigma^j(1)\ \ \sigma^j(2))$

$= (j+1\ \ j+2)$.

But S_p is gen. by such transpositions $\therefore$ any permutation can be obtained by successively swapping neighbouring elts. $\square$

Prop^n 1: Let $f(x) \in \mathbb{Q}[x]$ be an irred. poly of prime degree p. Suppose $f(x)$ has exactly 2 non-real roots. Then $G := \mathrm{Gal}(f(x)/\mathbb{Q}) \simeq S_p$. In particular if $p \geq 5$, then $f(x)$ is not solvable by radicals.

Proof: Let K = splitting field of $f(x)/\mathbb{Q}$ &

identify G with a subgroup of S_p by fixing some order of the roots.

Note that the conjug^{n} map $\tau \in G$ is the 2-cycle swapping the 2 non-real roots.

If $\alpha \in K$ is a root of $f(x)$ then $K/\mathbb{Q}$ Galois $\Rightarrow$

$$p = [\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [K : \mathbb{Q}] = |G|.$$

$\therefore$ If $P \leq G$ is a Sylow p-subgroup then $p \mid |P|$. Also, Lagrange's thm $\Rightarrow$ $|G| \mid |S_p| = p!$ so we must have $|P| = p$.

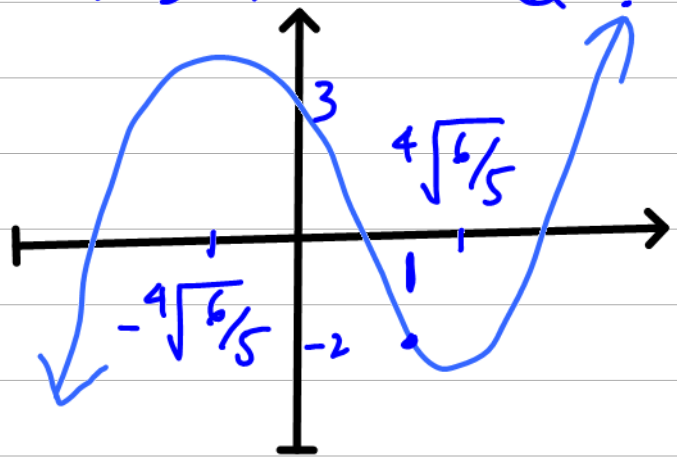
Let σ be a gen. of the cyclic group P of order p. Since $\sigma \in S_p$, it must be a p-cycle. Also $G \geq \langle \sigma, \tau \rangle$ so $G = S_p$ by the lemma.

□

Eg. 1. We show $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is not solvable by radicals $/\mathbb{Q}$.

Eisenstein $\Rightarrow$ $f(x)$ is irred. $/\mathbb{Q}$.

$f'(x) = 5x^4 - 6$



Graph $\Rightarrow$ exactly 2 non-real roots.
Prop^{n} 1 $\Rightarrow$ not solvable by radicals.

Rem 1: This e.g. also shows in a strong sense that the general quintic is not solvable by radicals.

The discriminant

Rem 2: Symmetry encoded in $G := Gal(f(x)/F)$ actually helps us solve separable $f(x)/F$.
To illustrate, consider

Q How do you start a radical tower for K/F where K = splitting field for $f(x)/F$?

Galois corresp. suggests seek $N \trianglelefteq G$ with G/N cyclic. Viewing $G \leq S_n$, where $n \geq n_0$. roots of $f(x)$ we have

Obvious candidate: $N = G \cap A_n$.

Isom thm $\Rightarrow \varphi: G/N \hookrightarrow S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$
& φ is an isom. iff $G \not\leq A_n$.

Recall equiv. def^{n} of odd/even perm^{n}

Fact or Def^{n}: Let $\sigma \in S_n$ &

$$\Delta(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]$$

Then $(\sigma\Delta)(x_1, \ldots, x_n) = \Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \begin{cases} \Delta & \sigma \text{ even} \\ -\Delta & \sigma \text{ odd.} \end{cases}$

Prop^n 2: Suppose $\operatorname{char} F \neq 2$ & $\alpha_1, \ldots, \alpha_n \in K$ are distinct roots of $f(x)$.

(a) $K^N = F(\delta)$ where $\delta = \prod_{i<j} (\alpha_i - \alpha_j)$

(b) $D := \delta^2 \in F$.

(c) $G \leq A_n$ iff D is already a square in F.

Proof: (a) Fact-Def^n $\Rightarrow$ for any $\sigma \in G$,

$$\sigma(\delta) = \begin{cases} \delta & \text{if } \sigma \text{ even} \\ -\delta & \text{if } \sigma \text{ odd} \end{cases}$$

so $\operatorname{char} F \neq 2$ ensures $\operatorname{Gal}(K/F(\delta)) = G \cap A_n = N$.

(b) $\sigma(D) = \sigma(\delta)^2 = (\pm\delta)^2 = \delta^2 = D$ so $D \in K^G = F$,

(c) $G \leq A_n \iff N = G \overset{\text{Galois corresp.}}{\iff} F(\delta) = F$ □

Def^n: The elt D above is called the discriminant of $f(x)$. It can be computed in terms of the co-eff. of $f(x)$ so Prop^n 2 (c) is helpful in determining $\operatorname{Gal}(f(x)/F)$.

Eg. 2. $f(x) = x^2 + bx + c \Rightarrow$

$$D = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c$$

Eg. 3 $f(x) = x^3 + px + q \overset{\text{ex.}}{\Rightarrow} D = -27q^2 - 4p^3$

$\operatorname{Gal}(x^3 + 2x + 2/\mathbb{Q}) = S_3 \because D < 0$ (irred. by Eis.)