Lecture 24: Galois Groups of Polynomials

Consider $f(x) \in F[x]$ and suppose E/F is a splitting field for separable, irreducible $f(x)$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$. Then suppose $Gal(E/F) = Aut(E/F)$ the F-fixing automorphisms of E. Since E/F is Galois, $[E:F] = \#$ of automorphisms in $Aut(E/F)$. Let $[E:F] = p$ then

$$Gal(E/F) = \{1, \sigma_2, \sigma_3, \ldots, \sigma_p\}$$

Proposition: If $z \in E$ then $\prod_{i=1}^{p} \sigma_i(z) = \sigma_1(z)\sigma_2(z)\cdots\sigma_p(z)$ is an element of F thus for $z \neq 0$ we have $z^{-1} = \dfrac{\prod_{i=2}^{p} \sigma_i(z)}{\prod_{i=1}^{p} \sigma_i(z)}$

Proof: Let $\tau \in Aut(E/F)$ and consider for $z \in E$,

$$\tau\left(\prod_{i=1}^{p} \sigma_i(z)\right) = \prod_{i=1}^{p} (\tau\sigma_i)(z) = \prod_{j=1}^{p} \sigma_{i_j}(z)$$

$\{\sigma\tau_i\}_{i=1}^{p} = \{\sigma_j\}_{j=1}^{p}$

Thus $\prod_{i=1}^{p} \sigma_i(z)$ is fixed by $\tau \in Aut(E/F)$ $\therefore \prod_{i=1}^{p} \sigma_i(z) \in F$.

The rest of the prop. is clear by algebra of solving for $1/z = z^{-1}$. //

E1 $f(x) = x^2 + 1 \in \mathbb{R}[x]$ splits over $\mathbb{C}$ and $Aut(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$ where $\sigma(z) = \bar{z}$, $z^{-1} = \dfrac{\bar{z}}{z\bar{z}}$.

Given $f(x) \in F[x]$ separable the Galois group $G = Gal(E/F)$ permutes the roots of $f(x)$. If $\deg(f(x)) = n$ then $\sigma \in G$ sends roots $\alpha_1, \alpha_2, \ldots, \alpha_n \longrightarrow \alpha_1, \alpha_2, \ldots, \alpha_n$ so we can view G as subgroup of S_n. This means $|Gal(E/F)| \leq n! = |S_n| = [E:F]$.

We can split a given n^{th} degree polynomial with at most an $n!$-degree extension, of course sometimes we can do with less.

E2 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = E$ for $f(x) = (x^2-2)(x^2-3)$

we face roots $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$

$$\sigma: \begin{cases} \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3} \end{cases} = \begin{cases} \alpha_1 \longmapsto \alpha_2 \\ \alpha_3 \longmapsto \alpha_3 \end{cases} \qquad \sigma = (12)$$

$$\tau: \begin{cases} \sqrt{2} \longmapsto \sqrt{2} \\ \sqrt{3} \longmapsto -\sqrt{3} \end{cases} = \begin{cases} \alpha_1 \longmapsto \alpha_1 \\ \alpha_3 \longmapsto \alpha_4 \end{cases} \qquad \tau = (34)$$

$$\sigma\tau: \begin{cases} \alpha_1 \longmapsto \alpha_2 \\ \alpha_3 \longmapsto \alpha_4 \end{cases} \qquad \sigma\tau = (12)(34)$$

Hence $Gal(E/F) \cong \{1, (12), (34), (12)(34)\} \leq S_4$

$$\frac{1}{1+3\sqrt{2}+4\sqrt{3}} = \frac{(1-3\sqrt{2}+4\sqrt{3})(1+3\sqrt{2}-4\sqrt{3})(1-3\sqrt{2}-4\sqrt{3})}{(1+3\sqrt{2}+4\sqrt{3})(1-3\sqrt{2}+4\sqrt{3})(1+3\sqrt{2}-4\sqrt{3})(1-3\sqrt{2}-4\sqrt{3})}$$

$$= \frac{-65-93\sqrt{2}+116\sqrt{3}+24\sqrt{6}}{769}.$$

E3 $E = \mathbb{Q}(\sqrt[3]{2}, \rho)$ splits $f(x) = x^3 - 2$

where roots $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \rho\sqrt[3]{2}$, $\alpha_3 = \rho^2\sqrt[3]{2}$

$$\sigma: \begin{cases} \alpha_1 \longmapsto \alpha_2 \\ \alpha_2 \longmapsto \alpha_3 \\ \alpha_3 \longmapsto \alpha_1 \end{cases} \qquad \tau: \begin{cases} \alpha_1 \longmapsto \alpha_1 \\ \alpha_2 \longmapsto \alpha_3 \\ \alpha_3 \longmapsto \alpha_2 \end{cases}$$

$\sigma = (123)$ $\qquad$ $\tau = (23)$

Then $Gal(E/F) \cong \{1, (123), (132), (23), (13), (12)\} = S_3$

$\qquad\qquad\qquad\qquad\quad \sigma \quad \sigma^2 \quad \tau \quad \tau\sigma \quad \tau\sigma^2$

It turns out **E3** is typical, a generic polynomial of degree n has Galois group isomorphic to S_n. To understand this we must return to some math we looked at in the early story arc of this course,

Def^n/ Let $X_1, X_2, \ldots, X_n$ be <u>indeterminants</u>. The <u>elementary symmetric functions</u> $S_1, S_2, \ldots, S_n$ are defined by

$$S_1 = X_1 + X_2 + \cdots + X_n$$

$$S_2 = X_1X_2 + X_1X_3 + \cdots + X_2X_3 + X_2X_4 + \cdots + X_{n-1}X_n$$

$$\vdots$$

$$S_n = X_1X_2\cdots X_n$$

That is, the i^{th} <u>symmetric function</u> of $X_1, \ldots, X_n$ is S_i and it is formed by sum of all products of the X_j's taken i at a time (without repeats)

Indeterminants $x_1, x_2, \ldots, x_n$ are commuting, but generally outside that assumption they're featureless. This makes a poly. with $x_1, \ldots, x_n$ as roots the general n^{th} order poly.

Def'n/ The **general polynomial of degree n** is the polynomial $(x-x_1)(x-x_2)\cdots(x-x_n)$ whose roots are $x_1, x_2, \ldots, x_n$ (indeterminants)

CLAIM: The coefficients of the general poly. of degree n with roots $x_1, \ldots, x_n$ are the elementary symmetric functions in $x_1, \ldots, x_n$ up to a sign. In particular,

$$(x-x_1)(x-x_2)\cdots(x-x_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$$

Proof: by induction, but I'll just illustrate for small n,

$$(x-x_1)(x-x_2) = x^2 - (x_1+x_2)x + x_1x_2$$
$$= \underline{x^2 - s_1 x + s_2}. \quad (n=2)$$

$$(x-x_1)(x-x_2)(x-x_3) = \left(x^2 - (x_1+x_2)x + x_1x_2\right)(x-x_3)$$

$$= x^3 - (x_1+x_2)x^2 + x_1x_2x - x_3x^2 - (x_1+x_2)x_3x - x_1x_2x_3$$
$$= x^3 - (x_1+x_2+x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3$$
$$= \underline{x^3 - s_1x^2 + s_2x - s_3} \quad (n=3)$$