Galois groups of splitting fields

Thm Let L be the splitting field of $f \in F[x]$. Then $|\mathrm{Gal}(L/F)| \leq [L:F]$ with equality iff f is separable over F.

Pf by induction on $[L:F]$. If $[L:F]=1$, then $L=F$ and $\mathrm{Gal}(F/F)=1$ and has order 1. If $[L:F]>1$, then f has at least one irred factor p of deg >1. Let α be a fixed root of p and $\sigma \in \mathrm{Gal}(L/F)$. Set $\tau = \sigma|_{F(\alpha)}$ and $\beta = \tau(\alpha)$, which is a root of p. We get

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ | & & | \\ F(\alpha) & \xrightarrow{\tau} & F(\beta) \\ & \searrow \quad \swarrow & \\ & F & \end{array}$$

Conversely, for β any root of p, we know $\exists\ \tau : F(\alpha) \to F(\beta)$ extending id_F.

Thus, assuming the claim, we get an associated ext'n of τ to all of L.

Thus $|\mathrm{Gal}(L/F)| =$ $\prod$ # distinct factors over L of irred factors of f over F

$\leq \prod \deg(p_i)$ with equality iff f separable. $\square$

e.g. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field of the sep poly $(x^2-2)(x^2-3)$, so $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = 4$.

Note Splitting field & separable are necessary hypotheses for equality: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $k(t, \sqrt[p]{t})/k(t)$ for $\mathrm{char}\, k = p$.

Defn L/F with L the splitting field of a separable polynomial is called a Galois extension of F.

Permutations of the roots

Assume L/F Galois for $f \in F[x]$. If $\deg(f)=n$, $f = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ for $a_0 \neq 0 \in F$, α_i distinct elts of L.

Since $\sigma \in Gal(L/F)$ permutes the roots α_i, we get a hom

$$Gal(L/F) \longrightarrow \Sigma_n$$
$$\sigma \longmapsto \tau : \{1,\dots,n\} \to \{1,\dots,n\}$$
where $\sigma(\alpha_i) = \alpha_{\tau(i)}$.

(Every gp action $G \times S \to S$ gives a hom $G \to \Sigma_{|S|}$ in this way.)

Prop The hom $Gal(L/F) \to \Sigma_n$ is injective.

Pf σ is determined by its action on $\alpha_1,\dots,\alpha_n$ so $\sigma = id_L$ iff $\sigma(\alpha_i) = \alpha_i$ $\forall i$ iff $\sigma \mapsto 1$. □

Cor If L is the splitting field of a sep poly $f \in F[x]$, then $[L:F] \mid n!$ for $n = \deg(f)$.

Pf May regard $Gal(L/F) \leq \Sigma_n$ by the prop, so this is implied by Lagrange's theorem. □

Note Already proved $[L:F] \leq n!$ (w/o separability hypothesis), so this refines that result.

e.g. $L = \mathbb{Q}(\sqrt{2},\sqrt{3})$, $f = (x^2-2)(x^2-3)$

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

Take $\sigma : \alpha_1 \leftrightarrow \alpha_2$, $\alpha_3 \circlearrowright$ $\alpha_4 \circlearrowright$

$\tau : \alpha_1 \circlearrowright$ $\alpha_2 \circlearrowright$ $\alpha_3 \leftrightarrow \alpha_4$

Get $Gal(L/\mathbb{Q}) \cong \{e, (1\,2), (3\,4), (1\,2)(3\,4)\}$
$= \langle (1\,2), (3\,4) \rangle \leq \Sigma_4$.

e.g. $L = \mathbb{Q}(\omega, \sqrt[3]{2})$ with $\omega = e^{2\pi i/3}$, splitting field of x^3-2 / $\mathbb{Q}$.

Have $Gal(L/\mathbb{Q}) \hookrightarrow \Sigma_3$ and $|Gal((L/\mathbb{Q})| = [L:\mathbb{Q}] = 6$.

But $|\Sigma_3| = 6$, so $Gal(L/\mathbb{Q}) \cong \Sigma_3$.

Recall A gp action $G \times S \to S$ is transitive if $\forall s,t \in S$ $\exists g \in G$ s.t. $gs = t$.

Prop Let L be the splitting field of sep $f \in F[x]$. Then $\mathrm{Gal}(L/F)$ acts transitively on the roots of f iff f is irred / F.

Pf We've already seen that f acts transitively on roots of irred factors of f. By separability, these sets are disjoint, and thus form the orbits of the action of $\mathrm{Gal}(L/F)$ on roots of f. Transitivity on all roots then corresponds to there being only 1 irred factor, i.e. f irred. $\square$