

Galois groups of splitting fields

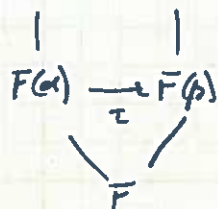
Thm Let  $L$  be the splitting field of  $f \in F[x]$ . Then

$|\text{Gal}(L/F)| \leq [L:F]$  with equality iff  $f$  is separable over  $F$ .

Pf by induction on  $[L:F]$ . If  $[L:F]=1$ , then  $L=F$  and  $\text{Gal}(F/F)=1$  and has order 1. If  $[L:F]>1$ , then  $f$  has at least one irred factor  $p$  of deg  $> 1$ . Let  $\alpha$  be a fixed root of  $p$  and  $\sigma \in \text{Gal}(L/F)$ .

Set  $\tau = \sigma|_F(\alpha)$  and  $\beta = \tau(\alpha)$ . We get  $L \xrightarrow{\sigma} L$

~~Claim~~ Conversely, for  $\beta$  any root of  $p$ ,  
we ~~claim~~ <sup>know</sup>  $\exists \tau: F(\alpha) \rightarrow F(\beta)$  extending  
idf.



~~Assuming the claim~~ <sup>Thus</sup> we get an associated action of  $\tau$  to all of  $L$ .

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

$\prod \text{# distinct factors on } L \text{ of irred factors of } f \text{ over } F$   
 $\leq \prod \text{deg}(p_i)$  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  $|\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4$ .

Note Splitting field & separable are necessary hypotheses  
for equality:  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ,  $k(t, \sqrt[t]{t})/k(t)$  for 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  $\text{deg}(f)=n$ ,  $f = a_0(x-\alpha_1)\cdots(x-\alpha_n)$   
for  $a_0 \neq 0 \in F$ ,  $\alpha_i$  distinct elts of  $L$ .

Since  $\sigma \in \text{Gal}(L/F)$  permutes the roots  $\alpha_i$ , we get a hom

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

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

Prop The hom  $\text{Gal}(L/F) \rightarrow \Sigma_n$  is injective.

Pf  $\sigma$  is determined by its action on  $\alpha_1, \dots, \alpha_n$  so  $\sigma = \text{id}_L$  iff  $\sigma(\alpha_i) = \alpha_i \forall i$  iff  $\sigma \mapsto 1$ .  $\square$

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  $\text{Gal}(L/F) \leq \Sigma_n$  by the prop, so this is implied by Lagrange's theorem.  $\square$

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

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

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

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

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

$$\begin{aligned} \text{Get } \text{Gal}(L/\mathbb{Q}) &\cong \{e, (12), (34), (12)(34)\} \\ &= \langle (12), (34) \rangle \leq \Sigma_4. \end{aligned}$$

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

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

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

Recall A gp action  $G \times S \rightarrow S$  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  $\text{Gal}(L/F)$  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  $\text{Gal}(L/F)$  on roots of  $f$ . Transitivity on all roots then corresponds to there being only 1 irred factor, i.e.  $f$  irred.  $\square$