Lecture 6: Galois Correspondence

Aim Lecture: Galois correspondence lets you read off a host of info about a finite Galois ext^{n}.

Galois Correspondence

Let K/F = finite field ext^{n}, $G = Gal(K/F)$

Def^{n}: An intermediate field of K/F is a subfield L of K containing F so $F \subseteq L \subseteq K$.

e.g. If $H \leq G$ then
$K^H \geq F$ since $\sigma \in H$ fixes F
so K^H is an intermediate field.

Fact: Conversely, for an intermediate field L, $H := Gal(K/L) \leq G$.
Why? H = subgroup of field autom^{ns} fixing L so they fix F too.

Galois correspondences consist of 2 maps:

$$L \longmapsto L' = Gal(K/L)$$

$$\{\text{inter. fields of } K/F\} \rightleftarrows \{\text{subgroups of } G\}$$

$$H' := K^H \longleftarrow H$$

Prop^{n}: ⓐ $L_1 \subseteq L_2 \Rightarrow L_1' \supseteq L_2'$

ⓑ $H_1 \subseteq H_2 \Rightarrow H_1' \supseteq H_2'$

i.e. Galois correspondences reverse inclusions.

Proof: easy, e.g. ⓐ $\sigma \in L_2'$ fixes L_2 & $\therefore$ L_1 too so $\sigma \in L_1'$.

Fundamental Thm of Galois Theory

Fundamental Thm: If K/F is a finite Galois ext^{n} then the Galois correspondences are inverse bijections.

Half Proof: Today only prove

Lemma: For intermediate field L Galois ext^{n} K/F, K/L is Galois & $L = L'' \overset{\text{def}}{=} K^{H}$ where $H = L' = \mathrm{Gal}(K/L)$

Proof: e.g. $\Rightarrow$ $L'' \supseteq L$ so suff. show $[K:L''] \geq [K:L]$ for then $[L'':L] = 1$.

If K = splitting field of sep. $f(x)/F$ then it's also splitting field of $f(x)$ $/L$ & L'' i.e. K/L, K/L'' are Galois.

Note $H' \subset \mathrm{Gal}(K/L'')$ so Lect. 5 Cor. $\Rightarrow$

$[K:L''] = |\mathrm{Gal}(K/L'')| \geq |H| = |\mathrm{Gal}(K/L)| = [K:L]$ □

Cor: K/F Galois with Galois group $G \Rightarrow F = K^G$.

Example

$\omega = e^{2\pi i/3}$

$K = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ splitting field of $x^3 - 2$ / $\mathbb{Q}$.

$K/\mathbb{Q}$ Galois &

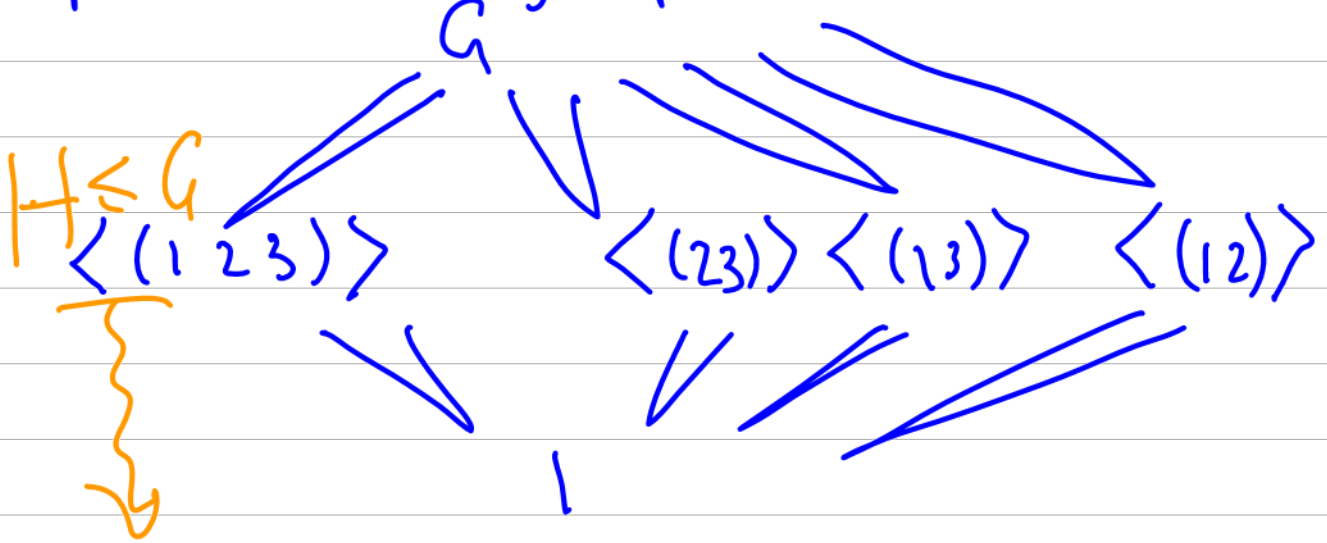
$G := Gal(K/\mathbb{Q}) = S_3$

on identifying autom. with permutations of roots above.

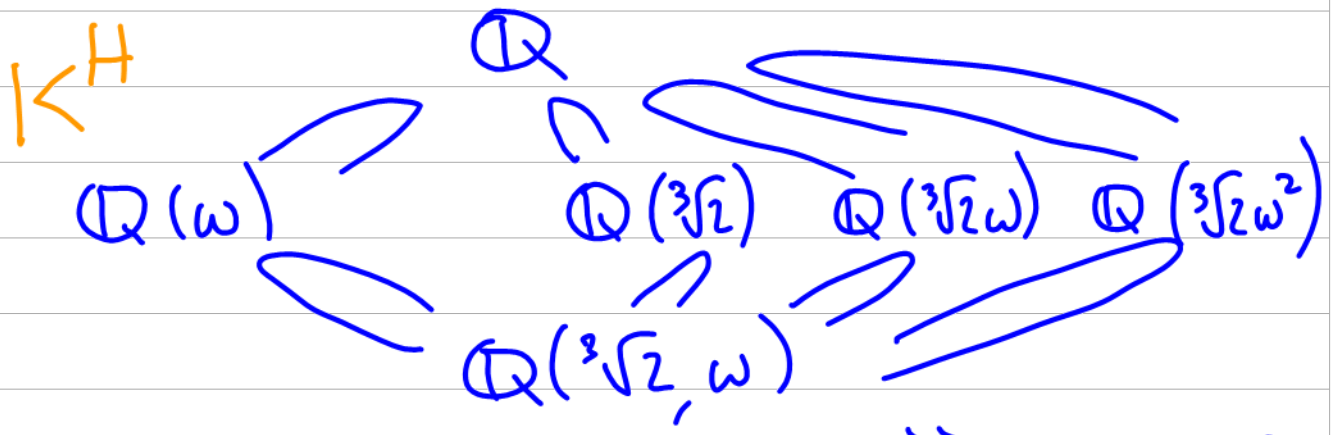
N.B. It's unclear what the intermediate fields of $K/\mathbb{Q}$ are but the subgroups of G are easily computable.

If $H < G$ is a proper subgroup, Lagrange $\Rightarrow |H| \mid 6$ so $|H| = 2$ or 3;

$\therefore$ H is a cyclic group gen. by a 2-cycle or a 3-cycle. Hence the poset of subgroups is



The corresponding poset of intermediate fields is



Why? Let's check $K^{\langle(23)\rangle} = \mathbb{Q}(\sqrt[3]{2})$

Note (23) swaps $\sqrt[3]{2}\omega \leftrightarrow \sqrt[3]{2}\omega^2$ & fixes $\sqrt[3]{2}$ so $\mathbb{Q}(\sqrt[3]{2}) \subseteq K^{\langle(23)\rangle} \subsetneq K$

But $[K : \mathbb{Q}(\sqrt[3]{2})] = 2$ is prime so multiplicativity of degrees of field ext^{n}s $\Rightarrow$ $K^{\langle(23)\rangle} = \mathbb{Q}(\sqrt[3]{2})$

Computation of other fixed fields similar.

W.B. Without the Galois corresp., it's not even clear the no. intermediate fields $< \infty$.

Application: $\mathbb{Q}(\omega + \sqrt[3]{2}) = K$ since $\mathbb{Q}(\omega + \sqrt[3]{2})$ is not contained any other intermediate field.