Fri, Nov 17 2017

Last time, we saw:

<u>Thm</u> Fix $K \subset L$ finite extension. Let $G = \mathrm{Gal}(L/K)$.
TFAE:
(1) $L^G = K$
(2) L is separable and satisfies $(*)$ (over K)
(3) L is splitting field of some separable $g \in K[x]$
(4) $|G| = [L:K]$.

<u>Rmk</u> In the course of proving $(2) \Leftrightarrow (4)$, we saw that $|G|$ always divides $[L:K]$. Let's record that here:

<u>Prop'n</u> If $[L:K] < \infty$, $|\mathrm{Gal}(L/K)|$ always divides $[L:K]$.

<u>Def'n</u> Let $[L:K] < \infty$. Then L is called a <u>Galois</u> extension of K if any (hence all) of $(1) \sim (4)$ holds.

The proof of the equivalence of (4) relied on two theorems, the first of which we've yet to prove:

<u>Thm</u> (Artin's Theorem) Fix $[L:K] < \infty$. Then $\exists\, \alpha \in L$ s.t. $L = K[\alpha]$ iff $\mathrm{Subfields}_K(L)$ is finite.

Artin's theorem, combined w/

Prop If $[L:K]<\infty$ and $K\subset L$ is Galois, then the inclusion

$$\mathrm{Subfields}_K(L) \supset \mathbb{F}\mathrm{ix} =: \{K\subset K_1 \subset L \text{ st } K_1 = L^H \text{ for some } H\subset \mathrm{Gal}(L/K)\}.$$

is a bijection.

led to a proof of

Thm (Primitive element theorem). Let $K\subset L$ be a finite extension and separable. Then $\exists\, \alpha\in L$ st $L=K[\alpha]$.

The proof used a common trick: pass to a splitting field $L\subset \mathbb{L}$, so all minimal polynomials with roots in L split in $\mathbb{L}$. Since L is separable, so are these minimal polynomials; and knowing $K\subset\mathbb{L}$ is Galois allowed us to compute the size of $\mathrm{Subfields}_K(L)=\mathbb{F}\mathrm{ix}$.

We're still pursuing:

Goal If $K\subset L$ is a finite Galois extension, then the inclusion

$$\mathbb{G}\mathrm{al} \subset \mathrm{Subgps}(\mathrm{Gal}(L/K))$$
$$\rotatebox{90}{$=:$}$$
$$\{H\subset G \mid H=\mathrm{Gal}(L/K_1) \text{ for some } K\subset K_1\subset L\}$$

is a bijection.

<u>Lemma</u> Fix $K \subset L$ arbitrary extension, and let $G = Gal(L/K)$. Fix any finite $H \subset G$. Then

(1) $|H| = [L : L^H]$

(2) $H = Gal(L/L^H)$

(3) L is Galois over L^H.

<u>Pf</u> Because H is finite, note:

(☆) For any $\alpha \in L$, deg(min polyn of α) $\leq |H|$.

Why? Let $H\alpha \subset L$ be the orbit of α as usual, and define

$$g = \prod_{\beta \in H\alpha} (x - \alpha) \in L[x].$$

Then $\forall\, \sigma \in H\alpha$, again $\sigma(g) = g$. So $g \in L^H[x]$. Moreover let $f \in L^H[x]$ be min polyn of α. Then $f | g$ in $L^H[x]$, so

$$\deg(f) \leq \deg(g) = |H\alpha| \underset{(*)}{\leq} \#\text{Roots}_L(f) \leq \#\text{Roots}_{\overline{L^H}}(f)$$

$$\leq \deg(f),$$

where (*) follows because any $\sigma \in H$ takes α to another root of f, as H fixes L^H pointwise by definition. We conclude $L^H \subset L$ is the splitting field of $g = f$, which we see is a separable polynomial because $\#\text{Roots}_{\overline{L^H}}(f) = \deg(f)$. This proves (3).

But let's focus back on (⊗). Since $\deg(g) = |H\alpha| \leq |H|$, (⊗) follows.

Choose α to be an element which maximizes $|H\alpha|$.
Then we have $L = L^H[\alpha]$.

(Otherwise, fix $\beta \in L \setminus L^H[\alpha]$, and we have $L^H \subset L^H[\alpha] \subset L^H[\alpha, \beta] \subset L$ but L is Galois over L^H, so $L^H[\alpha, \beta]$ is separable over L^H. By prim. elt. thm, $L^H[\alpha, \beta] = L^H[\alpha']$, violating that α had maximal degree over L.)

We conclude

$$\deg(\text{min polyn of } \alpha) = |H\alpha| \leq |H| \underset{(a)}{\leq} |\mathrm{Gal}(L/L^H)| \underset{(b)}{\leq} [L : L^H] = \deg(\text{min polyn of } \alpha).$$

Here, (a) is because $H \subseteq \mathrm{Gal}(L/L^H)$ by defn of L^H, and
(b) is because $|\mathrm{Gal}(L/K)|$ always divides $[L:K]$.

This proves each claim in the lemma. //

Note if $[L:K]$ is finite, $\mathrm{Gal}(L/K)$ is finite because $\mathrm{Gal}(L/K)$ embeds into a symmetric group (of finitely many roots of finitely many minimal polynomials). So the lemma, which is really an easy corollary of the primitive element theorem, gives the following (improving on our goal):

<u>Thm</u> For any finite extension $K \subset L$, $\mathrm{Subgps}(\mathrm{Gal}(L/K)) = \mathrm{Gal}$.

Collecting facts:

(1) For arbitrary $K \subset L$, setting $G := \mathrm{Gal}(L/K)$, we have

$$\begin{array}{ccccc} L^{\bullet} : & \mathrm{Subgps}(G) & \rightleftarrows & \mathrm{Subfields}_K(L) & : \mathrm{Gal}(L/\cdot) \\ & \cup & & \cup & \\ L^{\bullet} : & \mathbb{G}\mathrm{al} & \rightleftarrows & \mathbb{F}\mathrm{ix} & : \mathrm{Gal}(L/\cdot) \end{array}$$

and $L^{\bullet}$, $\mathrm{Gal}(L/\cdot)$ are mutually inverse bijections between $\mathbb{G}\mathrm{al}$ and $\mathbb{F}\mathrm{ix}$.

(2) For $[L:K] < \infty$, the inclusion $\mathbb{G}\mathrm{al} \subset \mathrm{Subgps}(G)$ is a bijection — ie, $\mathbb{G}\mathrm{al} = \mathrm{Subgps}(G)$.

(3) If $K \subset L$ is Galois, then $\mathbb{F}\mathrm{ix} \subset \mathrm{Subfields}_K(L)$ is a bijection — ie, $\mathbb{F}\mathrm{ix} = \mathrm{Subfields}_K(L)$.

So we conclude

<u>Thm</u> (Fundamental Theorem of Galois Theory)
If $K \subset L$ is a finite Galois extension, then

$$\begin{array}{ccc} \mathrm{Subgps}(\mathrm{Gal}(L/K)) & \rightleftarrows & \mathrm{Subfields}_K(L) \\ H & \longmapsto & L^H \\ \mathrm{Gal}(L/K_1) & \longleftarrow\!\shortmid & K \subset K_1 \subset L \end{array}$$

are inverse bijections. These reverse inclusions, so
$H \subset H' \implies L^H \supset L^{H'} \implies H \subset H'$. $\leadsto$

Moreover,

<u>Thm</u> (CONT'D)

(a) $[L : L^H] = |H|$ and $[L^H : K] = [G : H]$.

(order $\leftrightarrow$ deg. of top extension and index $\leftrightarrow$ deg of bottom extension)

(OTIB, order top, index bottom

$$\begin{array}{rcl} \text{top}\left\{ \begin{array}{c} L \\ \cup \end{array} \right. & & \longleftrightarrow |H| \text{ order} \\ & L^H & \\ \text{bottom}\left\{ \begin{array}{c} \cup \\ K \end{array} \right. & & \longleftrightarrow [G:H] \text{ index} \end{array}$$

)

(b) If $H = \mathrm{Gal}(L/K_1)$ for $K \subset K_1 \subset L$, and $\sigma \in \mathrm{Gal}(L/K)$,
then $\mathrm{Gal}(L/\sigma K_1) = \sigma H \sigma^{-1} \subset G$.

(Moving subfields $\longleftrightarrow$ conjugating subgroups)

(c) If $H = \mathrm{Gal}(L/K_1)$, $H \trianglelefteq G \iff K \subset K_1$ Galois.

(normal subgroups $\longleftrightarrow$ Galois bottoms)

(note $K \subset K_1 \subset L$, $K_1 \subset L$ is always Galois if $K \subset L$ is, since $\mathrm{subfields}_K(L) = \mathrm{Fix}$.)

(d) If $H \trianglelefteq G$, $\mathrm{Gal}(K_1/K) \cong G/H$. (Galois subfields $\longleftrightarrow$ quotient groups)

Pf of (a): We have $[L:L^H]=|H|$ from lemma. Then

$$|\mathrm{Gal}(L/K)| \overset{(4)}{=} [L:K] = [L:L^H][L^H:K] \overset{\text{lemma}}{=} |\mathrm{Gal}(L/L^H)|[L^H:K]$$

$$= |H|\,[L^H:K]$$

So $[L^H:K] = |G|/|H| = [G:H]$.

Pf of (b): Clearly $\sigma H\sigma^{-1} \subset \mathrm{Gal}(L/\sigma L^H)$ because

$$\alpha \in L^H \Rightarrow \sigma\alpha \in \sigma L^H \Rightarrow \sigma h\sigma^{-1}(\sigma\alpha) = \sigma h\alpha = \sigma\alpha \quad \forall h \in H.$$

But $|\sigma H\sigma^{-1}| = |H|$ and any L^H basis $\beta_1, \dots, \beta_n$ for L becomes a σL^H basis $\sigma\beta_1, \dots, \sigma\beta_n$ for L, so $[L:L^H] = [L:\sigma L^H] = |\mathrm{Gal}(L/\sigma L^H)|$.

So this inclusion is a bijection, and we have $\sigma H\sigma^{-1} = \mathrm{Gal}(L/\sigma L^H)$.
And any $K \subset K_1 \subset L$ is of the form $K \subset L^H \subset L$ for some $H \subset \mathrm{Gal}(L/K)$.

Pf of (c): (b) says the Galois correspondence is G-equivariant, where G acts on $\mathrm{Subgp}(G)$ by conjugation, and on $K_1 \in \mathrm{Subfields}_K(L)$ by $K \mapsto \sigma K$.
So fixed points are sent to fixed points — $H \triangleleft G \Rightarrow \sigma L^H = L^H \ \forall \sigma \in G$. We'll show L^H satisfies (*) and is separable over K. It's separable because L is. If $\exists\, \alpha \in L^H$ and $\alpha' \in L$ a root of the min polyn of α (over K), $\exists\ \sigma \in G$ s.t. $\sigma(\alpha) = \alpha'$. (Construct splitting field $\mathbb{L}$, so $K[\alpha] \subset \mathbb{L} \subset L$, use extension lemma for splitting field L (over $\mathbb{L}$).) Hence any root $\alpha' \in L^H$, so L^H satisfies (*).
This shows L^H is Galois over L.

Conversely, if $K \subset L^H$ is Galois, L^H is splitting field for some $g \in K[x]$. This is equivalent to saying that for any $L^H \subset \mathbb{L}$, any $\sigma : \mathbb{L} \to \mathbb{L}$ has $\sigma(L^H) = L^H$. Hence, taking $\mathbb{L} = L$, L^H is a fixed point of $\mathrm{Gal}(L/K)$-action, hence we see that $\mathrm{Gal}(L/L^H) = H$ is normal by (b).

Pf of (d): Note that since $\sigma L^H = L^H$ $\forall \sigma \in G$, we have a restriction map

$$\begin{aligned} \mathrm{Gal}(L/K) &\longrightarrow \mathrm{Gal}(L^H/K) \\ \sigma &\longmapsto \sigma|_{L^H} \end{aligned}$$

with kernel $\mathrm{Gal}(L/L^H)$. Thus it suffices to show this map is a surjection, but this follows from the extension lemma for splitting fields, noting L is a spl field over L^H.