~~Graduate~~ Algebra II Lecture 5: ★ Notes Now Up (posted)

Thm: K/F is Galois $\Leftrightarrow$ K is a splitting field of a separable F-polynomial
(K a finite extension)

Pf: We showed before the direction $\Leftarrow$.

To show the converse, assume K/F Galois, with Galois group G.

[redacted]

Let $\alpha \in K$, say it's a root of an irred. poly. $p(x)$. Then if $G = \{\sigma_1, \dots, \sigma_n\}$; $\sigma_i = id_K$, apply all the elts of G to α, namely $\alpha_1, \sigma_2(\alpha), \dots, \sigma_n(\alpha)$, and let $\alpha_1, \dots, \alpha_r$ be the distinct elts. on this list. As G is a group, multiplying all σ_i by some elt. $\tau \in G$ simply permutes them, and so applying τ to each α_i gives the α_i again in some order.

Thus, the polynomial $f(x) = \prod_{i=1}^{r} (x - \alpha_i)$ has coeffs. fixed by G (as G just permutes factors) $\Rightarrow$ the coefficients lie in the fixed field of G, which from last time is F.

That is, $f(x) \in F[x]$. Now $p(x)$ is irred with root α, so $p(x) = \min\text{poly}_F(\alpha)$, and so $p(x) \mid f(x)$.

As automorphisms fixing F send roots of min polys / F to roots of min polys / F (previously shown in theorem), $f(x) \mid p(x)$.

Thus, $f(x) = p(x)$. By choice, the roots α_i are

$p(x)$ is separable with all roots lying in K.
Moreover, we've shown $p(x)$ has its roots in K,
so $p(x)$ splits over K, so we've shown that
K/F is normal, hence a splitting field. (see book for a short alternate pf. here) $\square$

Recall: Last time:

Thm 1: $G \leq Aut(k)$, $F = Fix(G)$

$\rightsquigarrow [k:F] = |G|$.

Cor 2: $|Aut(k/F)| \leq [k:F]$ any finite ext^n.

We have $=$ $\iff F = Fix(Aut(k/F))$

Cor 3: With notation above, $Aut(k/F) = G$

$\Rightarrow k/Fix(G)$ is Galois, $Gal(k/Fix(G)) = G$.

Cor 4: $G_1 \neq G_2 \Rightarrow Fix(G_1) \neq Fix(G_2)$.

Thm (Fundamental Thm of Galois Theory).

If K/F is a finite Galois extension, with $G := Gal(K/F)$, there is a bijection:

$$\left\{\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} | \\ | \\ H \\ | \\ G \end{array}\right\}$$

intermediate fields $\qquad$ subgroups of G.

This is given by

$$E \longmapsto \{\text{elts of } G \text{ fixing } E\}$$

Fixed field of H $\longleftarrow H$

$=: K_H$.

Further, we have the properties:

1). If $E_1 \leftrightarrow H_1$, $E_2 \leftrightarrow H_2$, then $E_1 \subseteq E_2 \Leftrightarrow H_2 \leq H_1$.

2). In the tower
$$\begin{array}{c} K \\ | \; |H| \\ E \\ | \; [G:H] \\ F \end{array} \quad [K:E] = |H|, \quad [E:F] = [G:H]$$

3). K/E is automatically Galois, $Gal(K/E) = H$.

4). E/F is Galois $\Leftrightarrow H \trianglelefteq G$.

In this case, $Gal(E/F) \cong G/H$.

More generally, the set of cosets G/H is always in bijection w/ the isomorphisms of E (into a fixed algebraic closure of F containing K) fixing F.

5). If $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$ ← subgp. generated by H_1, H_2
and the compositum $E_1E_2 \leftrightarrow H_1 \cap H_2$.

(intersection of all fields in K containing E_1 and E_2)

Thus, the lattice of subfields of K containing F is the upside-down diagram of the lattice of subgps of G. $\square$

Pf: Cor 4 $\Rightarrow$ Corr. from subgps to subfields is injective.

K/F Galois $\Rightarrow$ $K = \mathrm{Spl}_F(f)$, some sep poly. $f(x) \in F[x]$.

Now $f(x) \in E[x]$ for any $F \subseteq E$ too.

$K = \mathrm{Spl}_E(f(x))$ too $\Rightarrow$ K/E is Galois.

Cor 2 $\Rightarrow$ E is the fixed field of $\mathrm{Aut}(K/E)$.

Thus, every subfield of K cont. F really is a fixed field, and hence our map from subgps. to subfields is a bijection.

Cor 2 $\Rightarrow$ The aut. of K fixing E are exactly $\mathrm{Aut}(K/E)$, and so the two dir$^{\underline{n}}$ of our correspondence are inverses.

$[E \to \mathrm{Aut}(K/E) \to \text{Fixed field of } \mathrm{Aut}(K/E) = E]$.

We already proved inclusion reversal $\Rightarrow$ (1).

For 2): Th$^{\underline{m}}$ 1 $\Rightarrow$ for $E = K_H$, $[K:E] = |H|$, $[K:F] = |G|$.

$\Rightarrow [E:F] = [K:F]/[K:E] = |G|/|H| = [G:H]$.

3): This was shown in Cor. 3.

4): Let $E = K_H$, some $H \leq G$. Given $\sigma \in G$, $\sigma|_E$ is an embedding $E \hookrightarrow \sigma(E) \subseteq K$.

Conversely, if $\tau: E \xrightarrow{\sim} \tau(E) \subseteq \bar{F}$ is an embedding (into a fixed alg. closure cont. K), we claim: $\tau(E) \subseteq K$.

Why: $\forall$ $\text{minpoly}_F(\alpha) = m_\alpha(x)$ for any $\alpha \in E$.

Then $\tau(\alpha)$ is a root of $m_\alpha(x)$. By Thm last time, K/F Galois implies this is also a root in K.

(every irred. poly @ a root in K splits). Thus, $\tau(E) \subseteq K$.

Now, $K = \text{spl}_E(f) \rightsquigarrow$ also the splitting field of $\tau f(x)$ (same as $f(x)$ as $f(x)$ has coeffs. in F) over $\tau(E)$.

By our lifting theorem, we can extend τ to σ:

$$\begin{array}{ccc} K & \xrightarrow{\sim}_{\sigma} & K \\ \uparrow & & \uparrow \\ E & \xrightarrow[\tau]{\sim} & \tau(E) \end{array}$$

Now τ fixes F $\Leftrightarrow$ σ fixes F $\Rightarrow$

Thus, every embedding τ of E fixing F is the restriction to E of an elt. of $\text{Aut}(K/F)$.

That is, every embedding of E is $\sigma|_E$, some $\sigma \in G$.

Also, given $\sigma, \sigma' \in G$, $\sigma|_E = \sigma'|_E \Leftrightarrow \sigma^{-1}\sigma'|_E = \text{id}_E$.

But (3) $\Rightarrow$ the aut of K fixing E are the elts of H

$\Rightarrow \sigma^{-1}\sigma' \in H \Rightarrow \sigma' \in \sigma H$.

Thus, the distinct embeddings of E are in bijection with cosets of H in G $\rightsquigarrow$ contains $\text{Aut}(K/F)$!

$$\Rightarrow |\text{Emb}(E/F)| = [G:H] = [E:F].$$

Now E/F is Galois $\Leftrightarrow |\text{Aut}(E/F)| = [E:F]$ $\square$

$\Rightarrow$ E/F Galois iff all embeddings of E are automorphisms of $E \iff \sigma(E) = E \ \forall \sigma \in G$.

Given $\sigma \in G$, we claim the subgp. of G fixing $\sigma(E)$ is $\sigma H \sigma^{-1}$, i.e., $\sigma(E) = K^{\sigma H \sigma^{-1}}$.

Why: If $\sigma\alpha \in \sigma(E)$, then

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

(as h fixed $\alpha \in E$) and so $\sigma H \sigma^{-1}$ fixes $\sigma(E)$.

The group fixing $\sigma(E)$ has size $[K : \sigma(E)]$.

As the fields are isomorphic, $[\sigma(E) \cong E]$,

$$[K : \sigma(E)] = [K : E] = |H|.$$

$\Rightarrow$ $\sigma H \sigma^{-1}$ = the gp. fixing $\sigma(E)$ as we have containment and equal sizes.

Now the corr. is a bijection, so E/F Galois

$\iff \sigma(E) = E \quad \forall \sigma \in G \iff$ their fixing subgps are equal

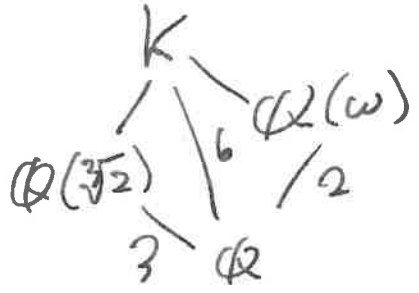
$\iff \sigma H \sigma^{-1} = H \ \forall \sigma \in G \iff H \trianglelefteq G$.

We showed identified embeddings of E over F with cosets of H in G, and when $H \trianglelefteq G$, the embeddings are automorphisms. Thus, the group of cosets in this case is identified to the group of automorphisms of E/F under fn composition $\Rightarrow G/H \cong \mathrm{Gal}(E/F)$.

5): Note that any elt. of $H_1 \cap H_2$ fixes both E_1 and E_2, hence every elt. of the compositum: [why: K_1, K_2 finite extns of F living in K.
bases: K_1/F: $\alpha_1, \dots, \alpha_n$
K_2/F: $\beta_1, \dots, \beta_m$
$\rightsquigarrow FK_1K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$
$\rightsquigarrow \{\alpha_i \beta_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ span $K_1 K_2$]

Conversely, σ fixes $E_1 E_2 \Rightarrow \sigma$ fixes E_1 and E_2
The other claim in (5) $\Rightarrow \sigma \in H_1 \cap H_2$. is similar.

Ex: $K = \mathrm{Spl}(x^3 - 2)/\mathbb{Q}$. $\omega^3 = 1$ primitive



$K = \mathbb{Q}(\omega, \sqrt[3]{2})$.
aut. determined by permutations of the 3 roots of $x^3 - 2$
Call them $1 = \sqrt[3]{2}$, $2 = \omega\sqrt[3]{2}$, $3 = \omega^2\sqrt[3]{2}$
$\rightsquigarrow$ at most 6 choices.
But $|\mathrm{Gal}(K/\mathbb{Q})| = 6 \Rightarrow$ all permutations come from an automorphism $\Rightarrow \mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.
Explicitly: $\sigma: \sqrt[3]{2} \to \omega^i \sqrt[3]{2}$, $i = 0,1,2$, $(i \in \mathbb{Z}_3)$
$\omega \mapsto \omega^j$, $j = 1,2$. $(j \in \mathbb{Z}_3^\times)$
$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non-Galois: corresponds to $\{\mathrm{id}, \sigma: \substack{\sqrt[3]{2} \to \sqrt[3]{2} \\ \omega \mapsto \omega^2}\} = \{\mathrm{id}, (23)\}$
$\le S_3$ of index 3, non-normal.