Lecture 32

(32.0) Let E/F be an algebraic extension. Recall that we have proved the equivalence of the following properties:

(a) E/F is Galois, i.e. $E^G = F$ where $G = \mathrm{Gal}(E/F)$.

(b) E/F is normal and separable. i.e. $\forall \alpha \in E$, the min'l polynomial $f_\alpha(x) \in F[x]$ factors into a product of <u>distinct</u>. <u>linear</u> factors in $E[x]$.

(c) E = splitting field of a set of <u>separable</u> polynomials $\mathcal{P} \subset F[x]$.

Along the way, we needed to prove different equivalent formulations of normality:

(1) E/F is normal

(2) E/F is a splitting extn. of a set $\mathcal{P} \subset F[x]$.

(3) $\forall$ K, $F \subset E \subset K$, and $\forall\, \sigma \in \mathrm{Gal}(K/F)$,

$$\sigma(E) = E$$

(i.e. $\sigma|_E \in \mathrm{Gal}(E/F)$)

(4) $\forall\, \sigma \in \mathrm{Gal}(\bar{F}/F)$, $\sigma(E) = E$.

Remark. (3) means that we have a restriction homomorphism

$$\mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(E/F)$$

Thus its kernel $= \mathrm{Gal}(K/E)$ is normal in $\mathrm{Gal}(K/F)$.

Note: restriction hom need not be surjective. We will prove below that it is surjective if K/F is normal.

Example (from HW 10.) $F = \mathbb{Q}$ $E = \mathbb{Q}(\sqrt{2})$
$= $ splitting extn. of $X^2 - 2 \in \mathbb{Q}[X]$

$K = \mathbb{Q}(2^{\frac{1}{4}}) = $ splitting extn. of $X^2 - \sqrt{2} \in E[X]$.

$\simeq \mathbb{Q}[X]/(X^4 - 2)$ $\quad Gal(K/F) = \mathbb{Z}/2\mathbb{Z} = \{1, \sigma\}$

$\downarrow$ ← restriction = trivial

$Gal(E/F) = \mathbb{Z}/2\mathbb{Z}$

$\sigma(2^{\frac{1}{4}}) = -2^{\frac{1}{4}}$

$\Rightarrow \sigma(2^{\frac{1}{2}}) = 2^{\frac{1}{2}} \Rightarrow \sigma|_E = Id_E$

(32.1) Fundamental Theorem of (finite) Galois theory.

Let K/F be a finite Galois extension.

Theorem (1) We have a bijection

Sub-F-extensions of K $\longleftrightarrow$ Subgroups of $Gal(K/F)$

$F \subset E \subset K \longmapsto Gal(K/E) < Gal(K/F)$

$F \subset K^H \subset K \longleftarrow H < Gal(K/F)$

$\forall$ • $F \subset E \subset K$, K/E is a Galois extension.

(2) In the bijection above, E/F is normal iff

$Gal(K/E) < Gal(K/F)$ is normal.

In this case, we have a short exact seq.

$1 \to Gal(K/E) \hookrightarrow Gal(K/F) \to Gal(E/F) \to 1$

i.e. $Gal(E/F) \simeq Gal(K/F)/Gal(K/E)$

Proof. (1) If K/F is Galois and $F \subset E \subset K$ is an intermediate field, then K = splitting extn. of a set of separable poly. $\mathcal{P} \subset F[X]$

Viewing $\mathcal{P}$ as a subset of $E[X]$, we conclude that K/E is again Galois.

Consider the map. Subgroups of $\mathrm{Gal}(K/F) \longrightarrow$ Sub-F-extns. of K

$$H \longmapsto K^H$$

Injectivity. If $H_1 \neq H_2$ but $K^{H_1} = K^{H_2} = K^H$ (H = subgp. gen. by H_1 & H_2)

Then by Artin's theorem

$$|H| = (K : K^H) = (K : K^{H_\ell}) = |H_\ell| \quad (\ell = 1 \text{ or } 2).$$

which contradicts $H_1 \neq H_2$.

Surjectivity. It suffices to show that $\forall\ F \subset E \subset K$; $H = \mathrm{Gal}(K/E)$ maps to E, i.e. $E = K^H$. By definition, this means K/E is a Galois extension which, we already know, is true.

(2) By Remark on page 1, if $E/_{\text{sub}}F$ is Galois (being a subextension of a separable extension K/F, it is always separable. So, for E/F, being normal is equivalent to being Galois)

Then $\mathrm{Gal}(K/E)$ is normal in $\mathrm{Gal}(K/F)$.

Conversely, if E/F is not normal, $\exists\ \sigma \in \mathrm{Gal}(\bar{F}/F)$ s.t. $\sigma(E) \neq E$ (see equivalent descriptions of

normality on page 1). As K/F is normal, $\sigma(K) = K$.

That is, $\sigma \in \mathrm{Gal}(K/F)$ and $\sigma(E) = E' \neq E$. Hence

$$\forall \tau \in \mathrm{Gal}(K/E), \quad \sigma\tau\sigma^{-1}\Big|_{\sigma(E)=E'} = \mathrm{Id}_{E'}$$

$$\Rightarrow \quad \sigma\,\mathrm{Gal}(K/E)\,\sigma^{-1} = \mathrm{Gal}(K/E')$$

As $E \neq E'$, $\mathrm{Gal}(K/E) \neq \mathrm{Gal}(K/E')$ by part(1). Hence $\mathrm{Gal}(K/E)$ is not normal (subgroup of $\mathrm{Gal}(K/F)$).

It remains to show that when E/F is normal, the restriction map $\mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(E/F)$ is surjective. That is,

every iso. of fields $\sigma: E \xrightarrow{\simeq} E$ (i.e. $\sigma(a) = a \ \forall a \in F$) lifts to $\tilde{\sigma}: K \xrightarrow{\simeq} K$ ($\tilde{\sigma}(a) = \sigma(a) \ \forall a \in E$).

This was a consequence of normality of K and was assigned in HW10. □

(32.2) For infinite extensions, the statement (of Thm 32.1 (1)) is false. e.g. let

$F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{p} : p \in \mathbb{Z}_{\geq 1} \text{ prime}) =$ splitting field of $\{X^2 - p : p \text{ prime}\} \subset \mathbb{Q}[X]$

Then $G = \mathrm{Gal}(K/F) = \prod_{p:\text{prime}} \mathbb{Z}/2\mathbb{Z}$

$+V$

$H = \bigoplus \mathbb{Z}/2\mathbb{Z}$. Then $F = K^G = K^H$ but $H \neq G$.

(32.3) A result about finiteness. In HW10, we saw that E/F finite $\Rightarrow$ $\mathrm{Gal}(E/F)$ is finite. For the converse:

Assume E/F is an algebraic extension s.t. $\mathrm{Gal}(E/F)$ is finite. We further assume that E/F is Galois.

Remark. We can always replace E by its "normal closure" as follows. View E as a subfield of $\overline{F}/F$ and take

$$E^{\text{normal}} = F\left(\mathrm{Gal}(\overline{F}/F)\text{-orbits of elements of } E\right)$$
$$= \text{smallest subfield of } \overline{F} \text{ containing } \sigma(E),\ \forall \sigma \in \mathrm{Gal}(\overline{F}/F).$$

If E/F is finite, so is E^{normal}/F as it will be generated by a finite set of algebraic elements.

($\mathrm{Gal}(\overline{F}/F)$-orbit of an (algebraic) element is finite.)

- E^{normal} = splitting field of $\{f_\alpha(x) \in F[x] \text{ min'l poly of } \alpha \in E\}_{\alpha \in E}$
- $\forall$ field map $\sigma: E \to \overline{F}$, $\sigma(E) \subset E^{\text{normal}}$.

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & \overline{F} \\ & \searrow \quad \swarrow & \\ & F & \end{array}$$

By Thm (32.1) E/F Galois extn. & $G = \mathrm{Gal}(E/F)$ finite

$\Rightarrow$ there are only finitely many sub-F-extns. of E.

(32.4) Prop. Let E/F be an algebraic extn. Let

I = (index) set of all finite E_i/F sub-F-extns. of E.

i.e. $F \subset E_i \subset E$ s.t. $(E_i : F) < \infty$. $(i \in I)$.

We have a partial order $i \leq j$ on I : $i \leq j$ if $E_i \subset E_j$

Then $E \simeq \varinjlim_{i \in I} E_i$

[Homework exercise. - Prove that E/F algebraic s.t. there are only finitely many sub-F-extns. of E, then E/F is finite.

- Hint : proof of Proposition (32.4)]

Pf. - We have to show first that I is a directed set. i.e.

$\forall\, i,j \in I,\ \exists\, k \in I$ s.t. $i \leq k$ & $j \leq k$. So let E_i, E_j be two finite-sub-F-extns. of E. Set $E' = E_i \cdot (E_j)$ $(= E_j \cdot (E_i))$ the smallest sub field of E containing E_i & E_j. As before, let

$\{\alpha_1, \ldots, \alpha_n\}$: basis of E_i as F-vector space

$\{\beta_1, \ldots, \beta_m\}$: basis of E_j as F-vector space.

Exercise (easy). $\{\alpha_i \beta_j\}_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ spans E'.

Hence $E' = E_k$ for some $k \in I$. Thus $i \leq k$ & $j \leq k$.

Now we have $E_k \hookrightarrow E \quad \forall k \in I$. We need to prove that for every set of field morphisms (over F)

$$\varphi_k : E_k \longrightarrow L \quad \text{(for some field } L \text{ over } F)$$

s.t. $k \leq l$ in $I \Rightarrow \varphi_k = \varphi_l|_{E_k}$,

we can find $\varphi : E \to L$ s.t. $\varphi_k = \varphi|_{E_k}$ $\forall k \in I$.

We note that $\forall \alpha \in E$, $F(\alpha)/F$ is finite hence in I.

Thus $\varphi|_{E_k} = \varphi_k$ determines φ uniquely. This (unique) φ, if exists, needs to be a field map:

$\varphi(0) = 0$ and $\varphi(1) = 1$ is true because it is so $\forall E_k$ $(k \in I)$

Let $a, b \in E$. Then $\exists\, k, l \in I$ s.t. $a \in E_k$ and $b \in E_l$.

Take $q \in I$, $q \geq k$ & $q \geq l$. Then $a, b \in E_q$ which is a field.

So, $a+b, ab \in E_q \subset E$. As φ_q is a field morphism

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{and} \quad \varphi(ab) = \varphi(a)\varphi(b).$$

□

(32.5) Exchange of terminology:

E/F is abelian if $\mathrm{Gal}(E/F)$ is abelian.

Similarly solvable, simple etc. We will see later the relation between E/F being "solvable by radicals" and $\mathrm{Gal}(E/F)$ being solvable.