Lecture 35

(35.0) Recall: last time we proved that for a finite field extension E/F s.t. there are only finitely many sub-F-extns of E, there exists $\alpha \in E$ s.t. $E \cong F(\alpha)$.

For example: if E/F is a finite Galois extn. $G = gal(E/F)$ is finite and hence has finitely many subgroups. By the Fundamental Theorem, E/F has finitely many subextns.

We saw that in this case $E \cong F(\alpha) \iff Stab_G(\alpha) = \{e\}$ (HW 11)

(i.e. $|G \cdot \alpha| = |G| = (E:F)$).

(35.1) Primitive element theorem. E/F : finite extn.

$E \cong F(\alpha)$ for some $\alpha \in E \iff$ There are finitely many sub-F-extns. of E

Proof. ($\Leftarrow$) was already proved.

($\Rightarrow$) Let $f(X) \in F[X]$ be the min'l poly. of α. (E/F finite $\Rightarrow$ algebraic)

~~Consider the factorization of $f(x)$ into monic~~

Given $F \subset K \subset E$, let $g(X) \in K[X]$ = min'l poly of α over K.

Claim: K = sub-F-extn. of E generated by coefficients of $g(X) \in K[X]$

Pf. - Denote the r.h.s. by K'. Then $K' \subset K$ because $g(X) \in K[X]$.

As $E \simeq F(\alpha) = K(\alpha) = K'(\alpha)$

$g(X) \in K'[X] \subset K[X]$ is the min'l poly of α (in K or K').

We get $(E:K) = (E:K') =$ degree of g. Thus $K = K'$ □

Now $g(X)$ divides $f(X)$ in $E[X]$. Thus sub-F-extns. of E are generated by coefficients of monic factors of $f(X)$ in $E[X]$. As there are only finitely many such monic factors, the assertion of the theorem follows. □

(35.2) Example of a finite extn w/ infinitely many subextns.

Let $p \in \mathbb{Z}_{\geq 2}$ be a prime, $F = \mathbb{F}_p(\lambda_1, \lambda_2)$.

$E = \mathbb{F}_p(\mu_1, \mu_2)$ where $\mu_\ell^p = \lambda_\ell$ $(\ell = 1, 2)$.

Claim: E/F is not of the form $F(\gamma)$ for any $\gamma \in E$.

Proof. For any $\gamma \in E$, $\gamma = \sum_{0 \leq i,j \leq p-1} a_{ij} \mu_1^i \mu_2^j$ $(a_{ij} \in F)$

$$\Rightarrow \gamma^p = \sum a_{ij}^p \lambda_1^i \lambda_2^j \in F.$$

So, every $\gamma \in E$ satisfies an eqⁿ of the form

$X^p - f$ (for some $f \in F$). Hence $(F(\gamma) : F) \leq p$.

But $(E : F) = p^2$ (Check this!).

So $E \neq F(\gamma)$ for any $\gamma \in E$. $\square$

(35.3) Normal basis theorem. Let E/F be a Galois extn (finite).

Let $G = \mathrm{Gal}(E/F)$. Then there exists $\theta \in E$ s.t.

$\{g(\theta)\}_{g \in G}$ is a basis of E as an F-vector space.

(35.4) Remark. If $\theta \in E$ is such that $\{g(\theta)\}_{g \in G}$ is a basis of E as an F-v.s. then $E \simeq F(\theta)$ (see (35.0) above).

because $|G.\theta| = \dim_{F\text{-v.s}} E = |G|$. But the converse need not hold. (Primitive elt $\not\Rightarrow$ Normal basis).

Example

$E = \mathbb{Q}(2^{\frac{1}{3}}, \omega) = F(2^{\frac{1}{3}})$ $\qquad \mathrm{Gal}(E/F) = \langle t \rangle$

$|$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\mathrm{ord}(t) = 3$

$F = \mathbb{Q}(\omega)$ $\qquad\qquad\qquad\qquad\qquad\qquad$ $t : 2^{\frac{1}{3}} \longmapsto 2^{\frac{1}{3}}\omega$

$|$

$k = \mathbb{Q}$

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

Orbit of $2^{\frac{1}{3}} = \{2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2\}$

all distinct but their sum is zero, so not l.i.

(35.5) Proof of Normal basis theorem (F is infinite case).

We begin by remarking that for $\theta \in E$, (s.t. $|G\cdot\theta| = |G|$)

$G\cdot\theta$ is a basis of E (as F-v.s.) $\iff$ $|G| \times |G|$ - matrix w/ entries from E $\left(g_i(\theta)\right)_{g,h\in G}$ is invertible.

[Proof ($\Leftarrow$) Assume there is a dependence relation

$$\sum_{g\in G} a_g \cdot g(\theta) = 0 \quad \text{for some } (a_g)_{g\in G} \quad a_g \in F.$$

Then (rename $g \mapsto g_2$, apply g_1)

$$\sum_{g_2\in G} a_{g_2} \cdot g_1 g_2(\theta) = 0 \quad \forall\, g_1 \in G.$$

$\Rightarrow$ $(a_g)_{h\in G} \in F^N \subset E^N$ ($N = |G|$) is in the kernel of the matrix $\left(g_i(\theta)\right)_{g,h\in G}$.

($\Rightarrow$) We showed this in the proof of Artin's theorem that (Thm. 29.1 page 1)
if $\{\omega_1, \dots, \omega_N\}$ is a basis of E as an F-v.s. and $G = \{\sigma_1, \dots, \sigma_N\}$, then $[\sigma_i(\omega_j)]_{1\le i,j\le N}$ is invertible]

So, let $\alpha \in E$ be such that $E \simeq F(\alpha)$. Let $f(X) \in F[X]$ be the min'l poly. of α and let $\{\alpha_1, \ldots, \alpha_N\}$ be (distinct necessarily) roots of $f(X)$. (Recall that E/F is finite Galois extn.). Here $N = |G| = (E:F)$, and

$G.\alpha = \{\alpha_1, \ldots, \alpha_N\}$. We can list elements of G, $\{g_1, \ldots, g_N\}$ so that $g_i \alpha = \alpha_i \quad \forall\ 1 \le i \le N$.

Now $f(X) = \prod_{j=1}^{N} X - \alpha_j$ in $E[X]$

Set $f_j(X) = \dfrac{f(X)}{(X-\alpha_j) f'(\alpha_j)} \in E[X]$ of deg $N-1$.

$(\forall\ 1 \le j \le N)$

$$\left(= \prod_{\substack{1 \le k \le N \\ k \ne j}} \frac{X - \alpha_k}{\alpha_j - \alpha_k} \right)$$

Note: (1) $f_j(\alpha_i) = \begin{cases} 0 & i \ne j \\ 1 & i = j \end{cases}$

Hence $\sum_{j=1}^{N} f_j(X) - 1$ is a degree $\le N-1$ polynomial w/ N distinct roots $\{\alpha_1, \ldots, \alpha_N\}$

$$\Rightarrow \sum_{j=1}^{N} f_j(X) = 1$$

Note: This statement is just proving the partial fraction formula

$$\prod_{i=1}^{N} \frac{1}{X-\alpha_i} = \sum_{i=1}^{N} \frac{1}{X-\alpha_i} \cdot \left(\prod_{k \neq i} \frac{1}{\alpha_i - \alpha_k} \right)$$

Note (2) For $i \neq j$, every one of $\{\alpha_1, \ldots, \alpha_N\}$ is a root of $f_i(X) f_j(X)$

$$\Rightarrow f_i(X) f_j(X) \equiv 0 \pmod{f(X)} \text{ for } i \neq j.$$

Combining we get

$$f_i(X) f_j(X) = \begin{cases} 0 \mod f(X) & \text{if } i \neq j \\ f_i(X) \mod f(X) & \text{if } i = j \end{cases}$$

and $$\sum_{i=1}^{N} f_i(X) = 1$$

Again, if $d(X) = \dfrac{f(X)}{(X-\alpha) f'(\alpha)} \in E[X]$, then

$$g_i(d(X)) = f_i(X) \quad \forall \ 1 \leq i \leq N$$

Combining all this, we get that the rows/columns of $\mathcal{D}(X) = \left[g_i g_j(d(X)) \right]_{1 \le i,j \le N}$ are orthonormal

i.e. $\mathcal{D}(X)\,\mathcal{D}(X)^T = Id_{N \times N} \mod f(X)$ ← entry-wise

$\Rightarrow \det(\mathcal{D}(X))^2 = 1 \mod f(X)$

So $\det(\mathcal{D}(X)) \not\equiv 0$. As E is infinite, we can find $\beta \in E$ s.t. $\det(\mathcal{D}(X \mapsto \beta)) \neq 0$. Then $\theta = d(\beta)$ is the required element. □

(35.6) When E (or F) is finite, the argument is different and will be given in Homework 12.

(35.7) Corollary of Thm 35.3. – There exists an iso. of G-representations $E \simeq FG$

[Assumption: E/F is finite Galois extn.]

Here • FG = F-vector space of set maps $G \to F$

• $G \xrightarrow{\rho} \underset{F\text{-V.S.}}{\mathrm{Aut}}(FG)$

$\forall\ \eta : G \to F \in FG$

$\forall\ \sigma, \tau \in G$

$$[\rho(\sigma)(\eta)](\tau) := \eta(\sigma^{-1}\tau)$$

$E \xrightarrow{\sim} FG$ depends on the choice of $\theta \in E$ s.t.

$\{g(\theta)\}_{g \in G}$ is a basis of E over F

map the basis

$g(\theta) \longmapsto \delta_g$ (function $h \longmapsto \begin{cases} 1 & \text{if } h = g \\ 0 & \text{o/w} \end{cases}$)

Then $\sigma(g(\theta)) = (\sigma g)(\theta) \longmapsto \delta_{\sigma g}$

and $(\sigma \cdot \delta_g)(\tau) = \delta_g(\sigma^{-1}\tau)$

$= 1 \iff \sigma^{-1}\tau = g$

i.e. $\sigma g = \tau$

i.e. $\sigma \cdot \delta_g = \delta_{\sigma g}$. So $E \xrightarrow{\sim} FG$ is an iso. of

G-representations. □