Lecture 36

(36.0) Summary of some important results regarding finite Galois extension E/F.

(1) Fundamental Thm. (Thm. 32.1 page 2)

$$\begin{array}{ccc} \text{Sub-}F\text{-extns.} & \longleftrightarrow & \text{Subgps of } G = \mathrm{gal}(E/F) \\ F \subset E' \subset E & \longmapsto & \mathrm{gal}(E/E') \end{array}$$

$$\begin{array}{ccc} \cup & & \\ \text{Those for which } E'/F & \longleftrightarrow & \text{Normal Subgroups.} \\ \text{is Galois} & & \end{array}$$

(2) $\exists\ \alpha \in E$ s.t. $E \simeq F(\alpha)$: Primitive element

(equivalently, $\mathrm{Stab}_G(\alpha) = \{e\}$)

(3) $\exists\ \theta \in E$ s.t. $\{g(\theta)\}_{g \in G}$ is a basis of E as F-v.s.

(equivalently, $E \simeq FG$ as G-representations)

$$\theta \longleftrightarrow \delta_e : \begin{array}{ccc} G & \longrightarrow & F \\ \sigma & \longmapsto & \begin{cases} 0 & \text{if } \sigma \neq e \\ 1 & \text{if } \sigma = e \end{cases} \end{array}$$

(36.1) Roots of unity. Let F be a field of Characteristic either 0 or prime p.

Fix $n \in \mathbb{Z}_{\geq 2}$ s.t. $(p,n) = 1$ if $\mathrm{Char}(F) = p$

no constraint if $\mathrm{Char}(F) = 0$.

$E :=$ Splitting extn. of $X^n - 1 \in F[X]$.

Note : $\frac{d}{dX}(X^n - 1) = nX^{n-1} \neq 0$ by our hypothesis on n & p.

so $X^n - 1$ is separable (see Prop 33.1 page 1).

Hence E/F is finite Galois extn. (Thm 29.8 page 8).

Let $S \subset E^\times$ be the set containing n roots of $X^n - 1$.

As S is a group (in the special case: roots of $X^n - 1$ form a group),

finite, abelian

and any such subgroup of $E^\times$ is cyclic, $\exists\ \zeta \in S$ s.t.

$$S = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$$

[Hence, $E \simeq F(\zeta)$. We will assume below that $\zeta \notin F$]

Definition. - Any such $\xi \in S$ (i.e. a generator of S) is called a primitive n^{th} root of unity. (of E over F).

(36.2) Theorem. With the notations and hypotheses of (36.1) above. $\mathrm{Gal}(E/F) \hookrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ invertible elements of $\mathbb{Z}/n\mathbb{Z}$.

subgroup

And hence $(E:F) = |\mathrm{Gal}(E/F)|$ divides $\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^\times|$.

Proof. $\sigma \in \mathrm{Gal}(E/F)$ is completely determined by $\sigma(\zeta) = \zeta^{n_\sigma} \in S$. This n_σ must lie in $(\mathbb{Z}/n\mathbb{Z})^\times$ for ζ^{n_σ} to generate E over F as field.

Moreover, $\sigma(\tau(\zeta)) = \tau(\sigma(\zeta)) = \zeta^{n_\sigma n_\tau}$

$= (\sigma\tau)(\zeta) = \zeta^{n_{\sigma\tau}}$

$\Rightarrow n_\sigma \cdot n_\tau \equiv n_{\sigma\tau} \pmod{n}$.

Thus we get $\mathrm{Gal}(E/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ $(\sigma \longmapsto n_\sigma)$

If n is prime, this group is in fact cyclic. □

(36.3) Fun application. Let $m \geq 3$.

Cor. $\cos\left(\frac{2\pi}{m}\right) \in \mathbb{Q} \iff m = 3, 4, 6.$
(or 1, 2 but those are obvious)

Pf. E = Splitting extn. of $X^m - 1$ over $\mathbb{Q}$

$= \mathbb{Q}(e^{2\pi\sqrt{-1}/m})$ } degree $= \left|(\mathbb{Z}/m\mathbb{Z})^\times\right|$

Ex. $\mathrm{Gal}(\mathbb{Q}(e^{2\pi\sqrt{-1}/m})/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$

$= \varphi(m)$

$\left(= \#\{1 \leq k \leq m-1 \mid (k,m)=1\}\right)$

Let $\sigma \in Gal(E/F)$ be the complex conjugation.

As $\exp\left(\frac{2\pi\sqrt{-1}}{m}\right) = \cos\left(\frac{2\pi}{m}\right) + \sqrt{-1}\ \sin\left(\frac{2\pi}{m}\right)$, we get

$\cos\left(\frac{2\pi}{m}\right) \in \mathbb{Q} \iff E^{\langle\sigma\rangle} = \mathbb{Q}$, i.e.

$Gal(E/\mathbb{Q}) = \langle\sigma\rangle$ has size 2.

$\iff \varphi(m) = 2 \iff m = 3, 4, 6.$

□

(36.4) Noether's equations.- Again assume E/F is finite Galois extension. Let $G = Gal(E/F)$.

Theorem. Given any function $G \xrightarrow{\eta} E^x$ s.t.

$$\eta(\sigma_1\sigma_2) = \sigma_1(\eta(\sigma_2)) \cdot \eta(\sigma_1) \quad \text{- Noether's eq}^{\underline{n}}\text{s.}$$

There exists $\alpha \in E^x$ s.t. $\eta(\sigma) = \frac{\alpha}{\sigma(\alpha)}$.

Proof.- By Dedekind's independence theorem (Thm (28.3) page 4.- - warning about notational confusion - G in Thm (28.3) and K^x are both E^x; $S = Gal(E/F)$)

elements of $G = Gal(E/F)$ are linearly independent/E.

Thus $\exists$ $a \in E$ such that

$$\sum_{\sigma \in G} \eta(\sigma) \cdot \sigma(a) \neq 0 \quad .$$ Let α be this non-zero elt.

Then $$\sigma_1(\alpha) = \sum_{\sigma_2 \in G} \boxed{\sigma_1\left(\eta(\sigma_2)\right)} \cdot \sigma_1\sigma_2(a)$$

$$\boxed{\sigma_1\left(\eta(\sigma_2)\right)} \longrightarrow \frac{\eta(\sigma_1\sigma_2)}{\eta(\sigma_1)}$$

$$= \frac{1}{\eta(\sigma_1)} \cdot \sum_{\tau \in G} \eta(\tau)\,\tau(a) = \frac{\alpha}{\eta(\sigma_1)}$$

Hence, $\eta(\sigma_1) = \dfrac{\alpha}{\sigma_1(\alpha)}$ as claimed. $\square$

Remark. The converse of this theorem is automatic since

if $\eta : G \longrightarrow E^\times$ is defined by $\eta(\sigma) = \dfrac{\alpha}{\sigma(\alpha)}$, $\left(\begin{smallmatrix}\alpha \in E^\times \\ \text{fixed}\end{smallmatrix}\right)$

then $$\eta(\sigma_1\sigma_2) = \frac{\alpha}{\sigma_1\sigma_2(\alpha)} = \frac{\sigma_2(\alpha)}{\sigma_1(\sigma_2(\alpha))} \cdot \frac{\alpha}{\sigma_1(\alpha)}$$

$$= \sigma_1\left(\frac{\alpha}{\sigma_2(\alpha)}\right) \cdot \frac{\alpha}{\sigma_1(\alpha)} = \sigma_1\left(\eta(\sigma_2)\right) \cdot \eta(\sigma_1)$$

(36.5) Corollary. - Again let E/F be a Galois extn. (finite) and let $\chi : G \to F^\times$ be a set map. Then χ is a group homomorphism (i.e., a character) if, and only if $\exists\, \alpha \in E^\times$ s.t. $\chi(\sigma) = \dfrac{\alpha}{\sigma(\alpha)}$ $(\in F^\times)$.

Furthermore if $m = \text{l.c.m.}\{\text{order}(\sigma) \mid \sigma \in G\}$ then $\alpha^m \in F^\times$

Proof. As $F^\times \subset E^\times$, we can view χ as an $E^\times$-valued function on G. Noether's eq$^{\underline{n}}$s in this case become

$$\chi(\sigma_1\sigma_2) = \sigma_1\big(\chi(\sigma_2)\big)\,\chi(\sigma_1) = \chi(\sigma_2)\,\chi(\sigma_1)$$
$$= \chi(\sigma_1)\,\chi(\sigma_2)$$

(since G acts trivially on F - where χ takes values.)

Thus χ is a character $\iff$ Noether's eq$^{\underline{n}}$s

$\iff$ $\exists\, \alpha \in E^\times$ s.t. $\chi(\sigma) = \dfrac{\alpha}{\sigma(\alpha)}$

(see Thm (36.4) and Remark after)

It remains to check that if $\alpha \in E^\times$ is s.t. $\chi_\alpha(\sigma) := \dfrac{\alpha}{\sigma(\alpha)} \in F^\times$ (and hence is a character - remark on page 5), then $\alpha^m \in F^\times$. To prove this, it is enough to check

that $\sigma(\alpha^m) = \alpha^m \quad \forall\, \sigma \in G$. This is true because

$$\frac{\alpha^m}{\sigma(\alpha^m)} = \left[\frac{\alpha}{\sigma(\alpha)}\right]^m = \chi(\sigma)^m = \chi(\sigma^m) = \chi(e) = 1.$$

$(\sigma^m = e \ \forall\, \sigma \in G)$

Note $\chi_\alpha = \chi_\beta \iff \frac{\alpha}{\beta} = \frac{\sigma(\alpha)}{\sigma(\beta)} \ \forall \sigma \in G \iff \frac{\alpha}{\beta} \in F$ □

(36.6) Relation with group cohomology (see Lecture 21 for definitions). – The statement of Theorem (36.4) can be rewritten as: $H^1(G; E^x) = \{1\}$.

Recall that E^x is an abelian group with G-action via group automorphisms

$$(G \longrightarrow \underset{\text{ab gps.}}{\text{Aut}}\,(E^x))$$

Thus $H^1(G; E^x) =$ Kernel of d^1 / Image of d^0 of the following

$$\begin{array}{ccccc} C^0(G;E^x) & \xrightarrow{d^0} & C^1(G;E^x) & \xrightarrow{d^1} & C^2(G;E^x) \\ \| & & \| & & \| \\ E^x & & \{G \to E^x\} & & \{G \times G \to E^x\} \\ \cup & & & & \\ \alpha & \longmapsto & (d^0\alpha)(\sigma) = \frac{\alpha}{\sigma(\alpha)} & & \\ & & \text{(set maps)} & & \\ & & \cup & & \\ & & \eta & \longmapsto & (d^1\eta)(\sigma_1,\sigma_2) = \frac{\sigma_1(\eta(\sigma_2))\,\eta(\sigma_1)}{\eta(\sigma_1\sigma_2)} \end{array}$$

(36.7) Theorem (additive form of Thm 36.4)

$$H^1(G;E) = \{0\}$$

Proof. We need to show that: given any set map

$$\eta : G \to E \quad \text{s.t.} \quad \eta(\sigma_1\sigma_2) = \sigma_1\left(\eta(\sigma_2^{-1}) + \eta(\sigma_1)\right), \quad \forall\, \sigma_1, \sigma_2 \in G$$

there exists $\alpha \in E$ s.t. $\eta(\sigma) = \alpha - \sigma(\alpha)$.

So choose $\theta \in E$ s.t. $y = \sum_{\sigma \in G} \sigma(\theta) \neq 0$

As $\sigma(y) = y \;\; \forall\, \sigma \in G$, we know that $y \in F^{\times}$.

Now set $\alpha = \frac{1}{y} \sum_{\tau \in G} \eta(\tau) \cdot \tau(\theta)$. Then

$$\sigma(\alpha) = \frac{1}{y} \sum_{\tau \in G} \boxed{\sigma(\eta(\tau))}\,(\sigma\tau)(\theta)$$

$$\boxed{\sigma(\eta(\tau))} \longrightarrow \eta(\sigma\tau) - \eta(\sigma)$$

$$[\sigma(y) = y]$$

$$= \frac{1}{y} \sum_{\tau' \in G} \eta(\tau')\,\tau'(\theta) - \eta(\sigma)\,\frac{\sum_{\tau' \in G} \tau'(\theta)}{y} \qquad (\text{the } y \text{ in the denominator})$$

$$= \alpha - \eta(\sigma)$$

□