Lecture 37

Kummer extensions - abelian case

(37.0) The term "Kummer extension" is usually applied to the splitting extension of a polynomial of the form

$X^n - a \in F[X]$ or more generally

$(X^n - a_1) \cdots (X^n - a_r) \in F[X]$ (where F is a field).

Let E/F be the splitting extension. Abelian vs non-abelian cases of Kummer extensions are separated by - whether F contains a primitive n^{th} root of unity or not. For example

$$\begin{array}{c} E = \mathbb{Q}(2^{\frac{1}{3}}, \omega) \\ | \\ F = \mathbb{Q}(\omega) \end{array}$$

$\mathrm{Gal}(E/F) \simeq \mathbb{Z}/3\mathbb{Z}$ (abelian)

(see Ex. 35.4 page 3)

$\langle t \mid t^3 = e \rangle$

where $s(2^{\frac{1}{3}}) = 2^{\frac{1}{3}}$

$t(2^{\frac{1}{3}}) = 2^{\frac{1}{3}}\omega$

$[t(\omega) = \omega]$

$$\begin{array}{c} E = \mathbb{Q}(2^{\frac{1}{3}}, \omega) \\ | \\ k = \mathbb{Q} \end{array}$$

$\mathrm{Gal}(E/k) \simeq S_3$ (non-abelian)

$\langle s, t \mid s^2 = t^3 = e,\ sts = t^{-1} \rangle$

$s: \omega \leftrightarrow \omega^2$ (hence $2^{\frac{1}{3}}\omega \leftrightarrow 2^{\frac{1}{3}}\omega^2$)

(hence $t(2^{\frac{1}{3}}\omega) = 2^{\frac{1}{3}}\omega^2 \xrightarrow{t} 2^{\frac{1}{3}}$)

(37.1) We will focus solely at the abelian case.

Notation. For a field K and $m \in \mathbb{Z}_{\geq 2}$, we denote by

$$\mu_m(K) = \{a \in K^\times \mid a^m = 1\} \subset K^\times$$ finite (cyclic - by (34.2) page 3) subgroup

We say K contains a primitive m^{th} root of unity if $|\mu_m(K)| = m$, i.e., $\exists\ \zeta \in K$ s.t. $\mu_m(K) = \{1, \zeta, \zeta^2, \cdots, \zeta^{m-1}\}$ ($m = \text{order}(\zeta)$)

Note. If K contains a primitive m^{th} root of unity, then

$$X^m - 1 = (X-1)(X-\zeta)\cdots(X-\zeta^{m-1})$$ has m distinct roots

$\Rightarrow$ $X^m - 1 \in K[X]$ is separable. So, either $\text{Char}(K) = 0$ or p (prime) where $(p, m) = 1$. (See differential criterion for separability - Prop. 33.1, page 1).

e.g. $$\mu_m(\mathbb{C}) = \{e^{2\pi\sqrt{-1}\frac{k}{m}} : 0 \leq k \leq m-1\}$$

$$\mathbb{F}_p^\times = \mu_{p-1}(\mathbb{F}_p)$$ ($= \mathbb{F}_p \setminus \{0\}$) (as an abelian gp. $\mathbb{F}_p^\times$ has $p-1$ elements so $a^{p-1} = 1\ \forall a \in \mathbb{F}_p^\times$)

(37.2) Now let $\begin{matrix} E \\ | \\ F \end{matrix}$ be the splitting extension of

$$(X^n - a_1) \dots (X^n - a_r) \in F[X]. \quad (\text{so } a_1, \dots, a_r \in F).$$

Assumption. – F contains a primitive n^{th} root of unity.

Let us fix one such $\zeta \in F^\times$ (i.e. $\mu_n(F) = \langle \zeta \rangle$

$= \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$)

For $(1 \le i \le r)$, let $\alpha_i \in E$ be s.t. $\alpha_i^n = a_i$. Then

$$X^n - a_i = \prod_{j=0}^{n-1} (X - \zeta^j \alpha_i)$$ ← n <u>distinct</u> roots (hence separable)

Remark. – To avoid redundancies, we may assume, without losing any further generality that

$$a_1, \dots, a_r \in F^\times \quad \text{and} \quad \frac{a_j}{a_i} \notin \mu_n(F) \quad \text{for } i \neq j.$$

Thus E/F is the splitting extn. of a separable polynomial

hence a Galois extension (§ 29.6 & 29.7 pages 6-8).

We first prove the following theorem for $G = gal(E/F)$.

Theorem. • E/F = splitting extn. of $(X^n - a_1)\dots(X^n - a_r) \in F[X]$

• F contains a primitive n^{th} root of unity

Then E/F is a (finite, of course) Galois extension.

Moreover $Gal(E/F)$ is abelian and $\sigma^n = e \;\forall\, \sigma \in Gal(E/F)$.

[In other words, exponent of G := $lcm\{order(\sigma) \mid \sigma \in G\}$ divides n]

Proof We have already shown that E/F is a Galois extension. We retain the notation as on the last page. Let $\sigma \in G = Gal(E/F)$.

As $E = F(\alpha_1, \dots, \alpha_r)$ where $\alpha_i^n = a_i$

σ is completely determined by its action on $\alpha_1, \dots, \alpha_r$.

Moreover, since $\sigma(\alpha_i)^n = a_i$, and $\{\alpha_i, \zeta\alpha_i, \dots, \zeta^{n-1}\alpha_i\}$ are all the roots of $X^n - a_i$, we get $(\forall\ 1 \le i \le r)$

$$\sigma(\alpha_i) = \xi_{i,\sigma} \cdot \alpha_i \qquad \text{where } \xi_{i,\sigma} \in \mu_n(F)$$

$$\Rightarrow \forall\, \sigma, \tau \in G, \quad \sigma(\tau(\alpha_i)) = \xi_{i,\sigma}\,\xi_{i,\tau} \cdot \alpha_i$$

$$= \xi_{i,\tau}\,\xi_{i,\sigma}\,\alpha_i = \tau(\sigma(\alpha_i))$$

$\Rightarrow \sigma\tau = \tau\sigma$ on each α_i $(1 \leq i \leq r)$, hence are equal. Thus, we proved that G is abelian.

Moreover, $\forall\, \sigma \in G$, $i \in \{1, \dots, r\}$, we get

$$\sigma^k(\alpha_i) = \xi_{i,\sigma}^k \, \alpha_i .$$

As $\xi_{i,\sigma} \in \mu_n(F)$, $\xi_{i,\sigma}^n = 1 \Rightarrow \sigma^n = Id$ on $\alpha_1, \dots, \alpha_r$ as required. □

(37.3) Converse of Theorem (37.2). - Statement. -

Assume. - • E/F is a finite Galois extension

• $G = Gal(E/F)$ is abelian. Let $m = \underset{\sigma \in G}{l.cm}\{ord(\sigma)\}$

• F contains a primitive m^{th} root of unity.

Theorem. - E/F is then a splitting extension of a polynomial of the form $(X^m - a_1) \dots (X^m - a_r) \in F[X]$.

The proof of this theorem is in several steps, and uses

Cor (36.5): $\left\{ \begin{array}{c} \text{Characters} \\ \chi : G \to F^\times \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \alpha \in E^\times : \frac{\alpha}{\sigma(\alpha)} \in F^\times \\ \forall\, \sigma \in G \end{array} \right\} \Big/ F^\times$

↑

for such α's, $\alpha^m \in F^\times$ (m = exponent of G)

Outline of the steps of the proof. –

I. As G is abelian and $\mu_m(F) \simeq \mathbb{Z}/m\mathbb{Z}$, we have
(of exponent m)

an iso. $G \xrightarrow{\sim} \underset{\text{gps}}{\mathrm{Hom}}\,(G, \mu_m(F))$ $\left(= \underset{\text{gps}}{\mathrm{Hom}}\,(G, F^\times)\right)$
↑ characters

II. (Corollary 36.5 page 6)

$$\mathrm{Hom}_{\text{gps}}\,(G, \mu_m(F)) \longleftrightarrow \left\{\alpha \in E^\times \mid \alpha^m \in F^\times\right\} \Big/ F^\times$$

(hence ↑ this set is finite and non-empty)

III. Let $A = \{\alpha \in E^\times \mid \alpha^m \in F^\times\}$ by the bijection above

$$A = \alpha_1 F^\times \sqcup \dots \sqcup \alpha_N F^\times \quad (N = |G| = (E:F))$$

Let $a_i \in F^\times$ be the m^{th} power of α_i $(1 \le i \le N)$

Then E contains the splitting extn. of $X^m - a_i$ $(1 \le i \le N)$

The last step is to show that that E = this splitting extn.

(37.4) Proof of Thm (37.3) - I.

$(*)$: $G \xrightarrow{\sim} \operatorname{Hom}_{gps}(G, \mu_m(F))$ [depending on a choice of $\zeta \in \mu_m(F)$ primitive]

$\sigma_j \longmapsto \chi^{\sigma_j}$ defined ($1 \le j \le t$) by: $\chi^{\sigma_j}: \sigma_\ell \longmapsto 1$ if $\ell \neq j$, $\sigma_j \longmapsto \zeta^{m/m_j}$

where we have to use the structure theorem of finite abelian groups to write

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \qquad (m = m_t)$$

$m_j \mid m_{j+1} \ \forall\ 1 \le j \le t-1$

$\{\sigma_1, \ldots, \sigma_t\}$ = set of generators

$\langle \sigma_j \rangle \simeq \mathbb{Z}/m_j\mathbb{Z}$

[Structure theorem was proved in the recitation. Also, its non-trivial part was proved in §34.3 page 4.]

For later purposes, let us record

Cor. $\forall\ \sigma \in G,\ \exists\ \chi \in \operatorname{Hom}_{gps}(G, \mu_m(F))$ s.t

$$\chi(\sigma) \neq 1.$$

(37.5) Proof of Thm (37.3) - II.

We already know that $\forall\ \chi \in \operatorname{Hom}_{gps}(G, \mu_m(F))$ there exists $\alpha \in E^\times$ (unique up to mult. by an element of $F^\times$) s.t. $\chi(\sigma) = \frac{\alpha}{\sigma(\alpha)}$. For such $\alpha \in E^\times$, we also proved that $\alpha^m \in F^\times$. Thus we have a well-defined (injective) map (gp. hom in fact)

$$\operatorname{Hom}_{gps}(G, \mu_m(F)) \longrightarrow A/F^\times$$

where $A = \{\alpha \in E^\times \mid \alpha^m \in F^\times\}$.

Now if $\alpha \in A$, then $\sigma(\alpha^m) = \alpha^m$; i.e.

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)^m = 1 \quad ; \text{ i.e. } \frac{\alpha}{\sigma(\alpha)} \in \mu_m(E) = \mu_m(F)$$

(F has all such elements).

and hence $\sigma \longmapsto \frac{\alpha}{\sigma(\alpha)}$ is a group character.

Thus we have shown that there is an iso. of groups

$$\operatorname{Hom}_{gps}(G, \mu_m(F)) \simeq A/F^\times$$

$\uparrow$ gp. under multiplication of $E^\times$.

(37.6) Proof of Thm 37.3 - III.

Again write $A^* = \alpha_1 F^{\times} \amalg \cdots \amalg \alpha_N F^{\times}$ $(N = |G| = (E:F))$

$a_i = \alpha_i^m \in F^{\times}$.

$E' =$ splitting extn. of $X^m - a_i$ $(1 \le i \le N)$ $\subset E$.

If $E' \neq E$, as E/F is Galois, $\exists\ \sigma \in G$ s.t. $\sigma \neq e$

and $\sigma|_{E'} = Id_{E'}$.

Let $\chi \in \mathrm{Hom}_{gps}(G, \mu_m(F))$ s.t. $\chi(\sigma) \neq 1$. (Cor on page 7)

$\updownarrow$

$\alpha \in A$. So $\chi(\sigma) = \dfrac{\alpha}{\sigma(\alpha)} \neq 1$, i.e. $\sigma(\alpha) \neq \alpha$.

But $\alpha \in A = \alpha_1 F^{\times} \amalg \cdots \amalg \alpha_N F^{\times}$. i.e. $\alpha \in E'$.

This is a contradiction to $\sigma|_{E'} = Id_{E'}$. $\square$