ALGEBRA 3 2017
CLASE 8
8/9/17

Definición (Elto separable, extensión separable)
E/K extensión

① Sea $\alpha \in E$. α es separable $/K$ si α es algebraico$/K$ y $f(\alpha, K) \in K[X]$ es separable

② E/K separable si $\forall \alpha \in E$, α es separable$/K$
(en particular E/K algebraica)

Observación:

Sea K / car$(K)=0$. Entonces $\forall\, E/K$ algebraica, se tiene que E/K es separable

Por ahora nos vamos a dedicar a extensiones separables

Observación:

$E/F/K$: E/K separable $\Rightarrow$ E/F y F/K separables

(pues si $\alpha \in E$, $f(\alpha, F) \mid f(\alpha, K)$ y $\alpha \in F \subset E$)

Proposición (IMPORTANTE)

~~Sea E/K finita. Entonces~~

Sea $\alpha \in \overline{K}$

① α separable$/K$ $\Leftrightarrow$ $\# \mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = [K(\alpha):K]$

Y en ese caso, $f(\alpha, K) = \prod\limits_{\sigma: K(\alpha) \xrightarrow[K]{} \overline{K}} (X - \sigma(\alpha))$

En particular $\prod\limits_{\sigma: K(\alpha) \xrightarrow[K]{} \overline{K}} (X - \sigma(\alpha))$ es un polinomio irreducible de $K[X]$

② α separable $/K$ $\Leftrightarrow$ $K(\alpha)/K$ separable

Demostración

① ~~Este~~ $\# \operatorname{Hom}(k(\alpha)/k : \bar{k}/k) \leq [k(\alpha):K]$

y se tiene igualdad $\iff$ $f(\alpha,k)$ tiene todas raíces simples

Las raíces de $f(\alpha,k)$ son exactamente los $\{\sigma(\alpha),\ \sigma\in \operatorname{Hom}(k(\alpha)/k : \bar{k}/k)\}$

y por lo tanto

$$f(\alpha,k) = \prod_{\sigma\in \operatorname{Hom}(k(\alpha)/k,\ \bar{k}/k)} (X-\sigma(\alpha)) \quad \text{minimal de } \alpha/K$$

② $(\Leftarrow)$ ✓

$(\Rightarrow)$ Sea $\beta\in k[\alpha]$.

~~K(α)/K(β) es separable~~

$$\begin{array}{l} K[\alpha] \\ \quad | \\ k[\beta] \\ \quad | \\ k \end{array}$$

α sep/ $k[\beta] \Rightarrow$

$$\# \operatorname{Hom}(k(\alpha)/k(\beta) : \bar{k}/k(\beta)) = [K(\alpha):k(\beta)]$$

α sep/ $k \Rightarrow$

$$\# \operatorname{Hom}(K(\alpha)/k : \bar{k}/k) = [K(\alpha):k]$$

y $\# \operatorname{Hom}(k(\beta)/k, \bar{k}/k) \leq [k(\beta):k]$

$\Rightarrow$ dado que $\# \operatorname{Hom}(k(\alpha)/k, \bar{k}/k) = \# \operatorname{Hom}(k(\alpha)/k(\beta), \bar{k}/k(\beta))\cdot$

$\# \operatorname{Hom}(k(\beta)/k, \bar{k}/k)$

se tiene que cumplir la igualdad pues

$$[K[\alpha]:k] = [k(\alpha):k(\beta)][k(\beta):k]$$

Así que $[K[\beta]:k] = \# \operatorname{Hom}(k(\beta)/k, \bar{k}/k)$

y por lo tanto β separable $/k$

$\boxtimes$

Teorema Sea E/K finita

E/K separable $\Leftrightarrow [E:K] = \# \operatorname{Hom}(E/K, \overline{K}/K)$

Demostación $(\Leftarrow\!\!\Rightarrow)$ Por inducción en $[E:K]$

- $[E:K] = 1$ ✓
- $[E:K] > 1$ y $\alpha \in E - K$ / $[K(\alpha):K]$ min

$$[E:K] > \begin{array}{c} E \\ | \\ K[\alpha] \\ | \\ K \end{array}$$

separable $\Leftrightarrow \# \operatorname{Hom}(E/K[\alpha], \overline{K}/K[\alpha]) = [E:K[\alpha]]$

$K[\alpha]/K$ separable $\Leftrightarrow \# \operatorname{Hom}(E/K[\alpha], \overline{K}/K[\alpha]) = [K[\alpha]:K]$

$\boxtimes$

Consecuencia E/K algebraica

1. $E = K[\alpha_1, .., \alpha_n]$ sep / $K \Leftrightarrow \alpha_1, .., \alpha_n$ sep/K
   (por torres)

2. $E = K(S)$ separable $\Leftrightarrow S$ sep/K
   ($K(S) = K[S]$ por ser alg y reducción a finitos eltos)

3. E/K sep $\Leftrightarrow E/F$ y F/K sep ~~(Torres ?)~~
   (llevar al caso finito) ~~(por el teo de # Hom e igualdad en ambos miembros)~~

4. E/K sep $\Rightarrow EF/F$ separable (pues $EF = F(E) = F[E]$ y c/generador de E es separable $/K \Rightarrow$ separable $/F$)

5. E/K, F/K sep $\Leftrightarrow EF/K$ sep

Corolario: El cpo de descomposición de un pol separable es una extensión separable de K

Proposición

Sea E/K separable y $\alpha \in E$.

Entonces $$f(\alpha, K) = \prod_{1 \le i \le n} (X - \sigma_i(\alpha))$$

donde $\{\sigma_1(\alpha), .., \sigma_n(\alpha)\} = \{\sigma(\alpha),\ \sigma \in \mathrm{Hom}(E/K, \overline{K}/K)\}$

(o sea los σ_i recorre todos los valores $\neq$ tomados por $\sigma(\alpha)$)

Demostración

$$f(\alpha, K) = \prod_{\tau \in \mathrm{Hom}(K(\alpha)/K,\ \overline{K}/K)} (X - \tau(\alpha))$$

pero cada τ es la restricción de algún σ. $\square$

Ejemplo:

$$\begin{array}{c} \mathbb{Q}[\sqrt[3]{2}, \zeta_3] \\ | \\ \mathbb{Q} \end{array}$$

$\sigma_1 = id$

$\sigma_2: \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3,\ \zeta_3 \mapsto \zeta_3$

$\sigma_3: \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2,\ \zeta_3 \to \zeta_3$

$\sigma_4: \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \zeta_3 \mapsto \zeta_3^2$

$\zeta_5: \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3,\ \zeta_3 \mapsto \zeta_3^2$

$\zeta_6: \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2,\ \zeta_3 \mapsto \zeta_3^2$

? $\sqrt[3]{2} + \zeta_3$:

$\sigma_1: \sqrt[3]{2} + \zeta_3 \mapsto \sqrt[3]{2} + \zeta_3$

$\sigma_2: \sqrt[3]{2} + \zeta_3 \mapsto \sqrt[3]{2}\zeta_3 + \zeta_3$

$\sigma_3: \sqrt[3]{2} + \zeta_3 \mapsto \sqrt[3]{2}\zeta_3^2 + \zeta_3$

$\sigma_4: \sqrt[3]{2} + \zeta_3 \mapsto \sqrt[3]{2}\,\cancel{\zeta_3} + \zeta_3^2$

$\sigma_5: \sqrt[3]{2} + \zeta_3 \mapsto \sqrt[2]{2}\zeta_3 + \zeta_3^2$

$\sigma_6: \sqrt[3]{2} + \zeta_3 \mapsto \sqrt[2]{2}\zeta_3^2 + \zeta_3^2$

todos distintos (se puede ver)

$$\Rightarrow f(\sqrt[3]{2} + \zeta_3, \mathbb{Q}) = \prod_{1 \le i \le 6} (X - \sigma_i(\sqrt[3]{2} + \zeta_3))$$

(5)

$= x^6 + 3x^5 + 6x^4 + 3x^3 + x^2 + 9x + 9$

(si hice las cuentas bien)

En particular

$$\left.\begin{array}{c} \mathbb{Q}[\sqrt[3]{2}, \zeta_3] \\ |\ 1 \\ \mathbb{Q}[\sqrt[3]{2}+\zeta_3] \\ |\ 6 \\ \mathbb{Q} \end{array}\right\} \Rightarrow \mathbb{Q}[\sqrt[3]{2}, \zeta_3] = \mathbb{Q}[\sqrt[3]{2}+\zeta_3]$$

Es lo que se llama un elto primitivo de la extensión

Se tiene para $\theta = \sqrt[3]{2} + \zeta_3$,

$$f(\theta, \mathbb{Q}) = \prod_{1 \le i \le 6} \left(x - \sigma_i\left(\sqrt[3]{2} + \zeta_3\right)\right) = x^6 + 3x^5 + 6x^4 + 3x^3 + x^2 + 9x + 9$$

Minimales E/K separable finita

(1)

$$\begin{tikzcd} E \arrow[d, dash, "\tau"] \\ K[\alpha] \arrow[d, dash, "\psi"] \\ K \arrow[uu, dash, bend left, "\sigma"] \end{tikzcd}$$

$$f(\alpha,K) = \prod_{\psi \in \mathrm{Hom}(K(\alpha)/K,\ \bar{K}/K)} (X - \psi(\alpha))$$

$$= \prod_{\substack{\sigma_i \in \mathrm{Hom}(E/K,\ \bar{K}/K) \\ \sigma_i(\alpha) \neq \sigma_j(\alpha) \text{ para } i \neq j}} (X - \sigma_i(\alpha))$$

Notar que hay exactamente $[E : K(\alpha)]$ inmersiones $\sigma : E \xrightarrow[K]{} \bar{K}$ que extienden a una $\psi : K[\alpha] \xrightarrow[K]{} \bar{K}$ dada.

Estas son: $\sigma = \bar{\psi} \circ \tau$, $\tau \in \mathrm{Hom}(E/K(\alpha),\ \bar{K}/K(\alpha))$

donde $\bar{\psi}$ es una fijada:

$\bar{\psi} \circ \tau(\alpha) = \bar{\psi}(\alpha) = \psi(\alpha) = \alpha$ ✓

$\bar{\psi} \circ \tau \neq \bar{\psi} \circ \tau'$ como ya vimos por la inyectividad.

Por lo tanto:

$$\prod_{\sigma \in \mathrm{Hom}(E/K,\ \bar{K}/K)} (X - \sigma(\alpha)) = f(\alpha, K)^{[E : K(\alpha)]}$$

(2)

$$\begin{tikzcd} E = K(\theta) \arrow[d, dash, "\tau"] \\ F \arrow[d, dash, "\psi"] \\ K \arrow[uu, dash, bend left, "\sigma"] \end{tikzcd}$$

$$f(\theta, K) = \prod_{\sigma} (X - \sigma(\theta))$$

$$= \prod_{\psi, \tau} (X - \bar{\psi} \circ \tau(\theta)) = \prod_{\psi, \tau} \bar{\psi}\,(X - \tau(\theta))$$

$$= \prod_{\psi} \Big(\bar{\psi} \Big(\underbrace{\prod_{\tau} (X - \tau(\theta))}_{f(\theta,F) \in F[X]} \Big) \Big) = \prod_{\psi} (\psi(f(\theta, F)))$$

$$\Rightarrow \quad f(\theta, K) = \prod_{\psi \in \mathrm{Hom}(F/K,\ \bar{K}/K)} \psi(f(\theta, F))$$

Ejemplos

$$\begin{array}{ll} & E = \mathbb{Q}(\overset{\theta}{\overbrace{\sqrt[3]{2}+\zeta_3}}) \\ \tau_1 : \zeta_3 \mapsto \zeta_3 & \quad | \\ \tau_2 : \zeta_3 \mapsto \zeta_3^2 & F = \mathbb{Q}(\sqrt[3]{2}) \\ & \quad | \ \psi_1 = id, \psi_2, \psi_3 \\ & \quad \mathbb{Q} \end{array}$$

$\psi_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}$

$\psi_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3$

$\psi_3 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\,\zeta_3^2$

$$f(\theta,\mathbb{Q}) = f(\theta,F)\,\psi_2(f(\theta,F))\,\psi_3(f(\theta,F))$$

$$(X-(\sqrt[3]{2}+\zeta_3))(X-(\sqrt[3]{2}+\zeta_3^2)) = f(\theta,F) \in \mathbb{Q}[\sqrt[3]{2}][X]$$

$$\psi_2(f(\theta,F)) = (X-(\sqrt[3]{2}\zeta_3+\zeta_3))(X-(\sqrt[3]{2}\zeta_3+\zeta_3^2)) \in \mathbb{Q}[\sqrt[3]{2}\zeta_3][X]$$

$$\psi_3(f(\theta,F)) = (X-(\sqrt[3]{2}\zeta_3^2+\zeta_3))(X-(\sqrt[3]{2}\zeta_3^2+\zeta_3^2)) \in \mathbb{Q}[\sqrt[3]{2}\zeta_3^2][X]$$

Observación

Sea E/K separable finita y $\theta \in E$.

Entonces

$$E = K[\theta] \iff \forall \sigma \neq \sigma' : E \xrightarrow[K]{} \bar{K}, \text{ se tiene } \sigma(\theta) \neq \sigma'(\theta)$$

Demostración

$$f(\theta,K) = \prod_{\substack{\sigma(\theta)\neq\sigma'(\theta) \\ \sigma \in Hom(E/K,\bar{K}/K)}} (X-\sigma(\theta))$$

$$\triangleleft \quad \underbrace{\deg f(\theta,K)}_{= [K[\theta]:K]} = \underbrace{\# Hom(E/K,\bar{K}/K)}_{= [E:K]} \iff \begin{array}{c}\sigma(\theta)\neq\sigma'(\theta) \\ \forall \sigma\neq\sigma'\end{array}$$

$$[K[\theta]:K] = [E:K]$$

⊠

Definición (Elemento primitivo)

Sea E/K extensión de cuerpos. Se dice que E es simple$/K$ (monógena) y que $\theta \in E$ es un elto primitivo de E/K si

$$E = K(\theta)$$

Es + fácil trabajar con extensiones simples pues conocemos Hom!

Teorema

Sea E/K separable finita. Entonces E es simple $/K$

i.e $\exists\, \theta \in E$ / tq $E = K[\theta]$.

(Más aún si $|K| = \infty$, existen $c_2, \ldots, c_n$ en cualquier subcjto infinito de K tq si $E = K[\alpha_1, \ldots, \alpha_n]$, $\theta = \alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n$)

Demostración

① Caso $|K| = \infty$

Por inducción en # generadores dado que

$E = K[\alpha_1, \ldots, \alpha_n]$ por ser finita.

- Caso clave: $E = K[\alpha, \beta]$ (2 generadores)

Si $f(\alpha, K) = (X - \alpha_1) \ldots (X - \alpha_r)$

$f(\beta, K) = (X - \beta_1) \ldots (X - \beta_t)$

[$\sigma \in Hom(E/K, \overline{K}/K) = \{\sigma_\ell\}$ está determinado por donde manda α y β.

Buscamos $c \in K$ / $\alpha_i + c\beta_j \neq \alpha_{i'} + c\beta_{j'}$ si $(i,j) \neq (i',j')$

pues en ese caso:

$\sigma_\ell(\alpha + c\beta) = \alpha_{\ell_1} + c\,\beta_{\ell_2}$ todos $\neq$ para $(\ell_1, \ell_2) \neq (\ell'_1, \ell'_2)$

Pero $\alpha_i + c\beta_j = \alpha_{i'} + c\beta_{j'} \iff c(\beta_j - \beta_{j'}) = \alpha_{i'} - \alpha_i$

$$\iff c = \frac{\alpha_{i'} - \alpha_i}{\beta_j - \beta_{j'}}$$

Sea entonces $c \in K$ (o en el subcjto infinito de K) tq

$$c \notin \left\{ \frac{\alpha_{i'} - \alpha_i}{\beta_j - \beta_{j'}},\ \cancel{i \neq i', j \neq j'}\ (i,j) \neq (i',j') \right\}$$

Probemos que $\theta = \alpha + c\beta$ es elto primitivo, o sea que

$\sigma(\theta) \neq \sigma'(\theta)$, $\forall\, \sigma, \sigma' \in Hom(E/K, \overline{K}/K)$

$\sigma \neq \sigma' \iff (i,j) \neq (i',j')$

$\sigma(\alpha) = \alpha_i$, $\sigma(\beta) = \beta_j$

$\sigma'(\alpha) = \alpha_{i'}$, $\sigma'(\beta) = \alpha_{j'}$

$(i,j) \neq (i',j')$

luego $\alpha_i + c\beta_j \neq \alpha_{i'} + c\beta_{j'}$.

• En general para $|K| = \infty$

$$\begin{array}{ll} E = K[\alpha_1,.., \alpha_{n-1}](\beta) = K[\theta](\beta) = K(\theta') & \text{Caso (2)} \\ \quad | & \\ F = K[\alpha_1,.., \alpha_{n-1}] = K(\theta) & \text{HI} \\ \quad | & \\ K & \end{array}$$

② Caso $|K| < \infty$

E es una extensión finita de un cuerpo finito

$\Rightarrow$ E es un cuerpo finito.

$\Rightarrow$ $E^\times$ es grupo abeliano finito para • $\vdots$ es cíclico por ser E cuerpo

pues si por el teo de caracterización de los grupos abelianos finitos

$$E^\times \simeq \mathbb{Z}/_{n_1\mathbb{Z}} \oplus .. \oplus \mathbb{Z}/_{n_r\mathbb{Z}} \quad \text{con}$$

$$\simeq G_{n_1} \times .. \times G_{n_r} \quad \text{con } n_1 | n_2 | \cdots | n_r$$

n_r exponente de $E^\times$

$|E^\times| = n = n_1 \times .. \times n_r$

$\forall x \in E^\times$, se tiene $x^{n_r} = 1$

o sea $\forall x \in E^\times$, x es raíz de $X^{n_r} - 1$

pero en un cuerpo, $X^{n_r - 1}$ tiene a lo sumo n_r raíces

luego $n_r = n \Rightarrow E^\times \simeq \mathbb{Z}/_{n\mathbb{Z}}$ cíclico

$\Rightarrow E^\times = \{\theta^k, 0 \le k \le n-1\} \Rightarrow E = K[\theta]$.

$\boxtimes$