Álgebra III - 2do C. 2020 - Clase 20 - 13/11/2020

Resumen y más

Sea E/K finita y *normal*, $G = \mathrm{Gal}(E/K)$.

- $E = E_s E_i = E_i(\alpha)$ Galois finita $/E_i$,
  $E_i = E^G$, $[E : E_i] = |G| =: r$,
  $f(\alpha, E_i) = (X - \alpha_1) \cdots (X - \alpha_r) \in E_i[X]$

- $K = E_s \cap E_i$ y $E_s = K(\beta)$ Galois finita $/K$,
  $[E_s : K] = [E : E_i] = r$,
  $f(\beta, K) = (X - \beta_1) \cdots (X - \beta_r) \in K[X]$
  (¡Ojo! sin relación entre α y β)

- E/E_s y E_i/K p.i.,
  $[E : E_s] = [E_i : K] = p^e$ para algún $e \in \mathbb{N}_0$.

- $E_s \cap K(\alpha) = K(\alpha)_s$

- $f(\alpha, K) = \big((X - \alpha_1) \cdots (X - \alpha_r)\big)^{p^k}$ para algún $k \leq e$
  y $f(\alpha, E_s) = (X - \alpha)^{p^k}$ (mismo k).

  (¡Ojo! puede ser $k < e$: α no tiene por qué ser elemento primitivo de E/K)

Ejemplo que muestra esto último

$K = \mathbb{F}_p(t, u)$ y $E = K(\sqrt[p]{t}, \sqrt[p]{u})$:
Vimos que E/K no es simple y $[E : K] = p^2$.
Además, E/K es p.i., y normal, con $G = \{\mathrm{id}_E\}$.
$E = E_i = E_i(\alpha)$, $\forall\, \alpha \in E$
Pero $E \neq K(\alpha)$...
Y $E_s = K = K(\beta)$, $\forall\, \beta \in K$.

13.7 Norma y traza en extensiones finitas

Definición 13.7.1 (Norma y traza)
Sea E/K *finita y sea* $\alpha \in E$.

- *La* traza de α en E/K *es*

$$\mathrm{Tr}_{E/K}(\alpha) := [E:K]_i \sum_{\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)} \sigma(\alpha).$$

  Si $E = K(\alpha)$, *se conviene la notación* $\mathrm{Tr}(\alpha) := \mathrm{Tr}_{K(\alpha)/K}(\alpha)$.

- *La* norma de α en E/K *es*

$$\mathrm{N}_{E/K}(\alpha) := \Big(\prod_{\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)} \sigma(\alpha) \Big)^{[E:K]_i}.$$

  Si $E = K(\alpha)$, *se conviene la notación* $\mathrm{N}(\alpha) := \mathrm{N}_{K(\alpha)/K}(\alpha)$.

Observaciones

- En principio, $\mathrm{Tr}_{E/K}(\alpha),\ \mathrm{N}_{E/K}(\alpha)\ \in \overline{K}$.
- Si E/K es finita *separable*, entonces

$$\mathrm{Tr}_{E/K}(\alpha) := \sum_{\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)} \sigma(\alpha) \quad \text{y} \quad \mathrm{N}_{E/K}(\alpha) := \prod_{\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)} \sigma(\alpha).$$

- Si E/K es finita *no separable*, con $\mathrm{car}(K) = p$, entonces

$$\mathrm{Tr}_{E/K}(\alpha) = 0,\ \forall\, \alpha \in E, \quad \text{pues} \quad [E:K]_i = p^e = 0 \ \text{ en } \ E.$$

Teorema 13.7.2 $(\mathrm{Tr}_{E/K}(\alpha),\ \mathrm{N}_{E/K}(\alpha)\ \in K)$
Sea E/K *finita. Entonces*

1. $\mathrm{Tr}_{E/K} : E \to K$ *es una* K*-transformación lineal.*

   En particular $\mathrm{Tr}_{E/K}(\alpha)\ \in K$, $\forall\, \alpha \in E$.

2. $\mathrm{N}_{E/K} : E^\times \to K^\times$ *es un morfismo de grupos multiplicativos.*

   En particular $\mathrm{N}_{E/K}(\alpha)\ \in K$, $\forall\, \alpha \in E$.

Prueba.–

Vamos a hacer la demostración por pasos. La parte menos obvia es probar que $\mathrm{Tr}_{E/K}(\alpha)\ , \mathrm{N}_{E/K}(\alpha)\ \in K\,,\ \forall\,\alpha \in E\,.$ La linealidad de la traza y la multiplicatividad de la norma son triviales como vemos en el siguiente lema, que se deja para demostrar.

Lema 13.7.3

Sean E/K finita y $\alpha, \beta \in E\,.$ Entonces

$$\mathrm{Tr}_{E/K}(\alpha+\beta) = \mathrm{Tr}_{E/K}(\alpha) + \mathrm{Tr}_{E/K}(\beta) \quad y \quad \mathrm{N}_{E/K}(\alpha\beta) = \mathrm{N}_{E/K}(\alpha)\mathrm{N}_{E/K}(\beta).$$

■

Vamos entonces a probar que $\mathrm{Tr}_{E/K}(\alpha)\ , \mathrm{N}_{E/K}(\alpha)\ \in K\,,\ \forall\,\alpha \in E\,,$ en casos:

(1) *Caso $E = K(\alpha)$ con α separable/K :*

Sea

$$\begin{aligned} f(\alpha, K) &= \prod_{\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)} \big(X - \sigma(\alpha)\big) \\ &= (X-\alpha_1)\cdots(X-\alpha_r) \ = \ X^r + a_{r-1}X^{r-1} + \cdots + a_0 \ \in \ K[X]. \end{aligned}$$

Entonces

- $\mathrm{Tr}(\alpha) = \displaystyle\sum_{\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)} \sigma(\alpha) \ = \ \alpha_1 + \cdots + \alpha_r \ = \ -a_{r-1} \ \in \ K\,.$
- $\mathrm{N}(\alpha) = \displaystyle\prod_{\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)} \sigma(\alpha) \ = \ \alpha_1 \cdots \alpha_r \ = \ (-1)^r a_0 \ \in \ K\,,$

  y si $\alpha \neq 0\,,\ \sigma(\alpha) \neq 0\,,\ \forall\,\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K) \ \Rightarrow \ \mathrm{N}(\alpha) \in K^\times\,.$

(2) *Caso E/K finita separable:*

Dado que todo $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$
es (en forma única) de la forma $\sigma = \overline{\psi} \circ \tau$
con $\overline{\psi}$ extensión fijada a $\overline{K}$
de $\psi \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)\,,$
y $\tau \in \mathrm{Hom}(E/K(\alpha), \overline{K}/K(\alpha))\,,$ tenemos

$$\bullet\ \mathrm{Tr}_{E/K}(\alpha) \;=\; \sum_{\sigma\in \mathrm{Hom}(E/K,\overline{K}/K)} \sigma(\alpha) \;=\; \sum_{\substack{\tau\in \mathrm{Hom}(E/K(\alpha),\overline{K}/K(\alpha))\\ \psi\in \mathrm{Hom}(K(\alpha)/K,\overline{K}/K)}} \overline{\psi}\circ\tau(\alpha)$$

$$= \sum_{\psi} \overline{\psi}\big(\sum_{\tau}\tau(\alpha)\big) \underset{\tau(\alpha)=\alpha}{=} \sum_{\psi}\overline{\psi}\big([E:K(\alpha)]\alpha\big)$$

$$\underset{\overline{\psi}(\alpha)=\psi(\alpha)}{=} [E:K(\alpha)]\sum_{\psi}\psi(\alpha) \;=\; [E:K(\alpha)]\mathrm{Tr}(\alpha) \;\in\; K$$

$$\bullet\ \mathrm{N}_{E/K}(\alpha) \;=\; \prod_{\sigma\in \mathrm{Hom}(E/K,\overline{K}/K)} \sigma(\alpha) \;=\; \prod_{\substack{\tau\in \mathrm{Hom}(E/K(\alpha),\overline{K}/K(\alpha))\\ \psi\in \mathrm{Hom}(K(\alpha)/K,\overline{K}/K)}} \overline{\psi}\circ\tau(\alpha)$$

$$= \prod_{\psi} \overline{\psi}\big(\prod_{\tau}\tau(\alpha)\big) \underset{\tau(\alpha)=\alpha}{=} \prod_{\psi}\overline{\psi}\big(\alpha^{[E:K(\alpha)]}\big)$$

$$\underset{\overline{\psi}(\alpha)=\psi(\alpha)}{=} \prod_{\psi}\psi(\alpha)^{[E:K(\alpha)]} \;=\; \mathrm{N}(\alpha)^{[E:K(\alpha)]} \;\in\; K^{\times} \;\text{ si } \alpha\in E^{\times}.$$

(3) *Caso E/K finita arbitraria:*

- Si E/K no es separable, $\mathrm{Tr}_{E/K}(\alpha)=0\in K$ y si E/K separable, $\mathrm{Tr}_{E/K}\in K$.
- Para la norma, para $\alpha\neq 0$:

$$\mathrm{N}_{E/K}(\alpha) \;=\; \big(\prod_{\sigma\in \mathrm{Hom}(E/K,\overline{K}/K)}\sigma(\alpha)\big)^{[E:K]_i} \;=\; \prod_{\sigma\in \mathrm{Hom}(E/K,\overline{K}/K)}\sigma(\alpha^{[E:K]_i})$$

$$\underset{\alpha^{[E:K]_i}\in E_s}{=} \prod_{\sigma\in \mathrm{Hom}(E_s/K,\overline{K}/K)}\sigma(\alpha^{[E:K]_i}) \;=\; \mathrm{N}_{E_s/K}(\alpha^{[E:K]_i}) \;\in\; K^{\times}$$

pues $\alpha^{[E:K]_i}\neq 0$ si $\alpha\neq 0$.

■

Antes observamos que si la extensión es no separable, entonces la traza es nula, o sea que si la traza es no nula, entonces la extensión es separable. De hecho podemos probar que es un si y solo si.

Proposición 13.7.4 (La traza es no nula $\Leftrightarrow$ E/K es separable)
Sea E/K finita. Entonces

$$\mathrm{Tr}_{E/K}: E\to K \;\; \textit{es una t.l. no nula} \;\Longleftrightarrow\; E/K \;\; \textit{es separable.}$$

Prueba.–
Solo falta probar que si E/K es separable, entonces $\mathrm{Tr}_{E/K} \neq 0$.
Sea $\theta \in E$ tal que $E = K(\theta)$ con minimal de grado n
y sea $\mathrm{Hom}(E/K, \overline{K}/K) = \{\sigma_1, \ldots, \sigma_n\}$.
Miremos entonces la traza sobre la base $(1, \theta, \ldots, \theta^{n-1})$ de E/K.

$$\begin{aligned}
&\mathrm{Tr}(1) = 1 + \cdots + 1 = n \quad \text{(que puede ser 0 si } \mathrm{car}(K) \,|\, n) \\
&\mathrm{Tr}(\theta) = \sigma_1(\theta) + \cdots + \sigma_n(\theta) \\
&\quad \vdots \\
&\mathrm{Tr}(\theta^{n-1}) = \sigma_1(\theta^{n-1}) + \cdots + \sigma_n(\theta^{n-1}) = \sigma_1(\theta)^{n-1} + \cdots + \sigma_n(\theta)^{n-1}
\end{aligned}$$

¿Pueden ser todos nulos? ¿Puede ser

$$\begin{pmatrix} 1 & \ldots & 1 \\ \sigma_1(\theta) & \ldots & \sigma_n(\theta) \\ \vdots & & \vdots \\ \sigma_1(\theta)^{n-1} & \ldots & \sigma_n(\theta)^{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} ?$$

¿'Qué es esto? ¡La matriz de la izquierda es una matriz de Vandermonde! con determinante

$$\prod_{1 \leq i < j \leq n} \big(\sigma_j(\theta) - \sigma_i(\theta)\big) \;\neq\; 0 \;\text{ pues } \sigma_i(\theta) \neq \sigma_j(\theta) \text{ para } i \neq j.$$

O sea multiplicar por esa matriz es una transformación lineal inversible.... ¡No puede dar 0!

∎

La proposición siguiente establece el comportamiento de la traza y la norma bajo inmersiones e incluye grados de separabilidad e inseparabilidad que podríamos haber visto antes.

Proposición 13.7.5 (Traza y norma vs. inmersiones)
Sea E/K finita, $\tau \in \mathrm{Hom}(E/K, \overline{K}/K)$ y $\alpha \in E$. Entonces

1. $[\tau(E) : K]_s = [E : K]_s \quad y \quad [\tau(E) : K]_i = [E : K]_i$
2. $\mathrm{Tr}_{\tau(E)/K}(\tau(\alpha)) = \mathrm{Tr}_{E/K}(\alpha) \quad y \quad \mathrm{N}_{\tau(E)/K}(\tau(\alpha)) = \mathrm{N}_{E/K}(\alpha)$

Prueba.–
(1) $[\tau(E):K]_s = \#\mathrm{Hom}(\tau(E)/K, \overline{K}/K) = \#\mathrm{Hom}(E/K, \overline{K}/K) = [E:K]_s$,
pues $E \simeq \tau(E)$ implica que hay una biyección entre
$\{\sigma : E \underset{K}{\hookrightarrow} \overline{K}\}$ y $\{\psi : \tau(E) \underset{K}{\hookrightarrow} \overline{K}\}$.
Además $[\tau(E):K] = [E:K]$ pues $\tau(E)$ y E son isomorfos como K-e.v.
Estas dos cosas implican $[\tau(E):K]_i = [E:K]_i$.
(2)

$$\begin{aligned}\mathrm{Tr}_{\tau(E)/K}(\tau(\alpha)) &= [\tau(E):K]_i \sum_{\psi \in \mathrm{Hom}(\tau(E)/K, \overline{K}/K)} \psi(\tau(\alpha)) \\ &= [E:K]_i \sum_{\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)} \sigma(\alpha) \;=\; \mathrm{Tr}_{E/K}(\alpha).\end{aligned}$$

Idem para la norma.

■

Proposición 13.7.6 (Traza y norma vs. torres)
Sea $E/F/K$ una torre finita y $\alpha \in E$. Entonces

- $\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}\big(\mathrm{Tr}_{E/F}(\alpha)\big)$
- $\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{F/K}\big(\mathrm{N}_{E/F}(\alpha)\big)$

Prueba.–
Es exactamente la misma demostración que hicimos en el caso $F = K(\alpha)$ usando que si $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$ entonces existen únicos $\psi \in \mathrm{Hom}(F/K, \overline{K}/K)$ y $\tau \in \mathrm{Hom}(E/F, \overline{K}/F)$ tal que $\sigma = \overline{\psi} \circ \tau$, y que $[E:K]_i = [E:F]_i [F:K]_i$.
Completarla.

■

Para finalizar, otra forma de ver la traza y la norma en extensiones finitas *separables*.

Proposición 13.7.7 (El morfismo multiplicar por α)
Sea E/K finita y separable*, y sea $\alpha \in E$.*
Definimos $m_\alpha : E \to E$, $x \mapsto \alpha x$ la multiplicación por α en E.
Entonces $m_\alpha \in \mathrm{End}_K(E)$, i.e. es un K-endomorfismo de E como K-e.v, y se tiene

$$\mathrm{tr}(m_\alpha) = \mathrm{Tr}_{E/K}(\alpha) \quad y \quad \det(m_\alpha) = \mathrm{N}_{E/K}(\alpha).$$

Prueba.–
Claramente $m_\alpha \in \mathrm{End}_K(E)$ pues $m_\alpha(x) \in E$, $\forall\, x \in E$, y

- $m_\alpha(x+y) = \alpha(x+y) = \alpha x + \alpha y = m_\alpha(x) + m_\alpha(y)$
- $m_\alpha(ax) = \alpha(ax) = a\alpha x = a m_\alpha(x)$

Probemos las dos afirmaciones, nuevamente por casos.

(1) <u>*Caso* $E = K(\alpha)$*:*</u>
Se tiene $\mathrm{tr}(m_\alpha) = \mathrm{tr}([m_\alpha]_{\mathcal{B}})$ y $\det(m_\alpha) = \det([m_\alpha]_{\mathcal{B}})$
donde $\mathcal{B}$ es cualquier base de E como K-e.v.
Sea $\mathcal{B} = (1, \alpha, \ldots, \alpha^{n-1})$, donde $f(\alpha, K) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$.
Entonces

$$[m_\alpha]_{\mathcal{B}} \;=\; \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \vdots \\ 0 & & 1 & -a_{n-1} \end{pmatrix} \;=\; C_{f(\alpha,K)},$$

la matriz compañera de $f(\alpha, K)$, de la cual sabemos que $\chi_{m_\alpha} = f(\alpha, K)$.
Con lo cual $\mathrm{tr}(m_\alpha) = \mathrm{Tr}(\alpha)$ y $\det(m_\alpha) = \mathrm{N}(\alpha)$.

(2) <u>*Caso* $\alpha \in E$*:*</u>
Sea $(\theta_1, \ldots, \theta_m)$ una base de $E/K(\alpha)$ y como antes $(1, \alpha, \ldots, \alpha^{n-1})$ la base de $K(\alpha)/K$ de modo que

$$\mathcal{B} = (\theta_1, \ldots, \theta_1\alpha^{n-1}, \theta_2, \ldots, \theta_2\alpha^{n-1}, \ldots, \theta_m, \ldots, \theta_m\alpha^{n-1})$$

es base de E/K.
Entonces $[m_\alpha]_{\mathcal{B}}$ es una matriz diagonal en bloques,
compuesta por m bloques iguales a $C_{f(\alpha,K)}$.
Y por lo tanto

$$\chi_{m_\alpha} = f(\alpha, K)^m = (X^n + a_{n-1}X^{n-1} + \cdots + a_0)^m,$$

y usando que $m = [E : K(\alpha)]$, se concluye

$$\begin{aligned} \mathrm{tr}(m_\alpha) &= \text{ coefte de } X^{mn-1} = -m a_{n-1} = \mathrm{Tr}_{E/K}(\alpha), \\ \det(m_\alpha) &= \text{ coefte constante } = ((-1)^n a_0)^m = \mathrm{N}_{E/K}(\alpha). \end{aligned}$$

■