Álgebra III - 2do C. 2020 - Clase 5 - 15/9/2020

Proposición 3.3.7 (K-endo $\Rightarrow$ K-auto en extensiones finitas)
Sea E/K extensión finita *y σ un K-endormorfismo de E. Entonces σ es un K-automorfismo de E.*

Prueba.–
Como σ es un endomorfismo del K-ev E, $\sigma(E)$ es subespacio de E, pero $\sigma(E) \simeq E$, tiene la misma dimensión que E, por lo tanto $\sigma(E) = E$.

■

---

(2) *Unicidad:* Continuamos con la demostración de la unicidad del cuerpo de descomposición.

En la proposición 3.3.6 tomamos $E_1 = F_1 = K$ con el isomorfismo id_K. Entonces existen $\sigma : E \to F$ y $\psi : F \to E$ K-morfismos. Por lo tanto, $\psi \circ \sigma$ y $\sigma \circ \psi$ son K-endos de E y F respectivamente, luego K-autos por la proposición 3.3.7.

¡Esto implica que $\sigma : E \to F$ es un isomorfismo! (Ver los detalles, obvio)

Pregunta: dado que en esta prueba $E_1 = F_1$ ¿por qué me tomé el trabajo de enunciar la proposición 3.3.6 en forma tan complicada y no simplemente con el mismo cuerpo de base?

■

Comentarios interesantes sobre cuerpo de descomposición

Sea $K(f) = K(\alpha_1, \ldots, \alpha_n)$ cuerpo de descomposición de $f \in K[X]$ de grado n sobre K. Entonces

- Para todo $\sigma : K(f) \underset{K}{\hookrightarrow} \overline{K}$, σ permuta las raíces $\alpha_1, \ldots, \alpha_n$ de f.

  (O sea es un K-endo de $K(f)$, o sea un K-auto.)

  ¿En realidad las raíces de quiénes?

  ¿Cualquier permutación de raíces da un endormorfismo?

- $[K(f) : K] \leq n!$

  Pensar si sale $[K(f) : K] \mid n!$

Notaciones generales

- $\mathrm{Hom}(E/K, F/K) := \{\sigma : E \underset{K}{\hookrightarrow} F,\ K\text{-inmersión}\}$
- $\mathrm{End}(E/K) := \{\sigma : E \underset{K}{\hookrightarrow} E,\ K\text{-endomorfismo}\}$
- $\mathrm{Gal}(E/K) := \{\sigma : E \underset{K}{\hookrightarrow} E,\ K\text{-automorfismo}\}$

3.4 Clausura algebraica

Ya vimos la existencia y unicidad de un cuerpo que contiene las raíces de un polinomio, veamos ahora la existencia y unicidad de un cuerpo que contiene las raíces de todos los polinomios.

Definición-Proposición 3.4.1 (Cuerpo algebraicamente cerrado)
Sea E un cuerpo. Son equivalentes

1. $\forall f \in E[X]$ *con* $\mathrm{gr}(f) \geq 1$, E *contiene al menos una raíz* α *de* f
2. $\forall f \in E[X]$ *con* $\mathrm{gr}(f) \geq 1$, f *se factoriza linealmente en* $E[X]$
3. *Sea* L/E *una extensión algebraica, entonces* $L = E$.

En cualquiera de estos casos, se dice que E es algebraicamente cerrado.

Prueba.–

(1 $\Rightarrow$ 2) Por inducción en $\mathrm{gr}(f)$.

(2 $\Rightarrow$ 3) Sea $\alpha \in L$ y sea $f = f(\alpha, E) \in E[X]$. Ent. $f = (X - \alpha_1)\cdots(X - \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in E$ pero es irreducible, o sea $f = X - \alpha$ y por lo tanto $\alpha \in E$.

(3 $\Rightarrow$ 1) Sea $f \in E[X]$ y L cuerpo de descomposición de f sobre E. Entonces $L = E$ implica que todas las raíces de f pertenecen a E.

∎

Ejemplos

- $\mathbb{C}$ es algebraicamente cerrado
- $\overline{\mathbb{Q}}$ es algebraicamente cerrado. ¿Por qué?

Definición 3.4.2 (Clausura algebraica)
Se dice que un cuerpo E extensión de K es una clausura algebraica de K *cuando se cumplen*

1. *E es algebraicamente cerrado,*
2. *E/K es algebraica.*

Observación 3.4.3
Sea E/K algebraica tal que $\forall\, f \in K[X]$ con $\operatorname{gr}(f) \geq 1$, f tiene todas sus raíces en E. *Entonces E es algebraicamente cerrado (es una clausura algebraica de K).*

Prueba.– Sea $g \in E[X]$ y sea α en el cuerpo de descomposición de g sobre E. Entonces α es algebraico sobre E y por lo tanto sobre K: existe $f \in K[X]$ tal que α es raíz de f, y f tiene todas sus raíces en E!

■

Problema para ir investigando y respondiendo durante toda la materia
En la observación anterior, ¿alcanzará pedir que $\forall\, f \in K[X]$ con $\operatorname{gr}(f) \geq 1$, f tiene *al menos una raíz en E*?
(Creo que en algún momento aparece en la práctica pero no vale preguntarlo sino que me gustaría que cada tanto lo retomen a ver qué pueden probar en función de los resultados teóricos que vamos obteniendo.)

Teorema 3.4.4 (Existencia y unicidad de la clausura algebraica)
Sea K un cuerpo. Entonces

1. *Existe una clausura algebraica de K.*
2. *Dos clausuras algebraicas de K son K-isomorfas.*

Por eso denotaremos con $\overline{K}$ la *clausura algebraica de K.*

Prueba.–
(1) *Existencia:* Alcanza con probar que existe L/K algebraicamente cerrado, pues después se toma $E := \{\alpha \in L : \ \alpha \text{ alg}/K\}$. O se alcanza con producir un cuerpo L tal que para todo $f \in L[X]$, f tiene al menos una raíz en L.
Esta demostración muy ingeniosa se debe a Émile Artin, 1898-1962, quien es el que puso en lenguaje moderno toda la teoría de cuerpos.
Asocio a cada polinomio $f \in K[X]$ mónico con $\operatorname{gr}(f) \geq 1$ una variable X_f, y considero el anillo (conmutativo) de polinomios en todas esas infinitas variables:

$$P := K[X_f : \ f \in K[X] \ \text{ mónico con } \mathrm{gr}(f) \geq 1].$$

Sea $\mathcal{A}$ el ideal de P generado por todos los $f(X_f)$:

$$\mathcal{A} := \langle f(X_f) : \ f \in K[X] \ \text{ mónico con } \mathrm{gr}(f) \geq 1 \rangle \ \subset \ P.$$

Afirmación: $\mathcal{A}$ es un ideal propio de P.

Por el absurdo. Supongamos $1 \in \mathcal{A}$. Entonces existen finitos de los generadores $f_1(X_{f_1}), \dots, f_s(X_{f_s})$ y $g_1, \dots, g_s \in P$ tq se tiene la identidad de Bézout

$$1 = g_1 f_1(X_{f_1}) + \cdots + g_s f_s(X_{f_s}),$$

(donde los polinomios g_i son cada uno en finitos X_f, $f \in K[X]$).

Vamos a utilizar un argumento muy común en teoría de polinomios ¡la evaluación!

Sea E cuerpo de descomposición de $f_1 \cdots f_s \in K[X]$ sobre K y sean $\alpha_1, \dots, \alpha_s \in E$ tales que $f_1(\alpha_1) = 0, \dots, f_s(\alpha_s) = 0$. Entonces evaluando $X_{f_1} \mapsto \alpha_1, \dots, X_{f_s} \mapsto \alpha_s$ ¿qué obtendríamos en la identidad de Bézout de arriba?¿Qué se concluye?

Con lo cual, como $\mathcal{A}$ es un ideal propio, existe un ideal maximal $\mathcal{M} \subset P$ tal que $\mathcal{A} \subset \mathcal{M}$.

¿Qué implica esto para $P/\mathcal{M}$?

¿Qué es natural querer probar entonces?

Claro, el sueño es querer probar que todo polinomio $f \in P/\mathcal{M}[X]$ tiene al menos una raíz en $P/\mathcal{M}$, o que todo polinomio $f \in K[X]$ tiene *todas* sus raices en $P/\mathcal{M}$... Pero tan directo no es.

Lo que seguro podemos probar es que todo polinomio $f \in K[X]$ tiene al menos una raíz en $P/\mathcal{M}$, pues ¿quién es esa raíz?

¡Sí! como $\mathcal{A} \subset \mathcal{M}$, se tiene $f(\overline{X_f}) = \overline{f(X_f)} = \overline{0}$, luego $\overline{X_f}$ es raíz de f en $P/\mathcal{M}$.

O sea lo que obtuvimos es un cuerpo $L_1 := P/\mathcal{M}$ extensión de K donde cada polinomio $f \in K[X]$ tiene al menos una raíz. ¡Se repite el procedimiento!

Sea L_2/L_1 tal que cada polinomio en $L_1[X]$ tiene al menos una raíz en L_2, y dado L_i, sea L_{i+1}/L_i tal que cada polinomio en $L_i[X]$ tiene al menos una raíz en L_{i+1}.

¿Quién es entonces la extensión L/K que nos va a servir? (o sea que satisface que es una extensión de K donde cada polinomio en $L[X]$ tiene al menos una raíz en L?)

Esto demuestra la existencia. Para la unicidad salvo K-isomorfismo, usaremos nuevamente un argumento de extensión de morfismos, que es fundamental en esta materia.

Teorema 3.4.5 (Extensión de inmersiones en extensiones algebraicas)
Sea $\sigma : K \hookrightarrow L$ una inmersión, con L algebraicamente cerrado, y sea E/K una extensión algebraica*.*
Entonces existe $\overline{\sigma} : E \hookrightarrow L$ inmersión que extiende a σ, i.e. $\overline{\sigma}|_K = \sigma$.
"Las inmersiones a un cuerpo algebraicamente cerrado se extienden a cualquier extensión algebraica"

Prueba.–
(Para E/K algebraica finita, ya lo hicimos la clase pasada ¿Sí?)
Para el caso general, vamos a usar el *Lema de (Kuratowski)-Zorn, 1922-1935*:
Sea $S \neq \emptyset$ parcialmente ordenado. Entonces si toda *cadena* (subconjunto totalmente ordenado) en S tiene *cota superior* (un elemento $\geq$ a todos los demás) en S, entonces S tiene *elementos maximales* (eltos que no son menores que ningún otro).

Aquí consideramos

$$S := \{(F, \tau) : K \subset F \ \text{ y } \tau : F \to L \ \text{ tq } \ \tau|_K = \sigma\},$$

ordenado partialmente por $\prec$:

$$(F, \tau) \prec (F', \tau') \ \text{ si } \ F \subset F' \ \text{ y } \ \tau'|_F = \tau.$$

Entonces

- $S \neq \emptyset$ pues
- Sea $\{(F_i, \tau_i) : i \in I\}$ una cadena en S. Entonces ¿quién es una cota superior? ¿qué cuerpo y qué inmersión?

Por lo tanto S admite un elemento maximal (F, τ).

Afirmación: $F = E$.

Pues sino sea $\alpha \in E \setminus F$, entonces, τ se extiende a $F(\alpha) \subset E$ mandando α a una raíz $\beta \in L$ de $\tau(f(\alpha, F))$. (Ya usamos ese argumento en *Extensión de inmersiones en extensiones finitas* ¿se acuerdan?). Y (F, τ) no sería maximal en S.

Se concluye que $F = E$ y τ extiende a σ.

∎

Ya que está aprovechemos para probar la extensión de la Proposición que afirmaba que todo K-endo de una extensión finita es un K-auto. Aunque no va a resultar necesaria para la unicidad de la clausura algebraica, es una propiedad importantísima (y no sé si tan intuitiva).

Proposición 3.4.6 (K-endo $\Rightarrow$ K-auto en extensiones algebraicas)
Sea E/K extensión algebraica *y σ un K-endormorfismo de E. Entonces σ es un K-automorfismo de E.*

Prueba.–

Ya lo probamos (por dimensión) para extensiones finitas. Así que una buena filosofía siempre es intentar reducirse a una extensión finita de K.

Ya sabemos que σ es mono, o sea que solo quiero probar que es epi:
qpq dado $\beta \in E$, existe $\alpha \in E$ tq $\beta = \sigma(\alpha)$.

Sea $f := f(\beta, K) = (X - \beta_1) \cdots (X - \beta_n) \in K(f)[X]$, con $\beta = \beta_1 \in E$,
y sea $\overline{\sigma} : E(\beta_1, \dots, \beta_n) \hookrightarrow \overline{K}$ extensión de σ (que existe por ser extensión algebraica de E).

Numeremos las raíces de modo tal que $\{\beta_1, \dots, \beta_n\} \cap E =: \{\beta_1, \dots, \beta_k\} \neq \emptyset$.

Observemos que al ser K-inmersión, $\overline{\sigma}$ permuta las raíces de f:
$\overline{\sigma}(\{\beta_1, \dots, \beta_n\}) = \{\beta_1, \dots, \beta_n\}$, y por hipótesis, $\overline{\sigma}(E) = \sigma(E) \subset E$. Así,

$$\sigma(\{\beta_1, \dots, \beta_k\}) = \overline{\sigma}(\{\beta_1, \dots, \beta_n\} \cap E) \subset \{\beta_1, \dots, \beta_n\} \cap E = \{\beta_1, \dots, \beta_k\}.$$

Por lo tanto, si $F := K(\beta_1, \dots, \beta_k)$, $\sigma(F) \subset F$, que es una extensión finita de K: el K-endo $\sigma|_F$ resulta ser un K-automorfismo de F, lo que implica que existe $\alpha \in F \subset E$ tal que $\beta = \sigma(\alpha)$.

∎

Observación 3.4.7 *Si E/K no es algebraica, lo anterior es falso (o no siempre cierto). ¿Por?*

(2) *Unicidad:* Sean E, L dos clausuras algebraicas de K. Probemos que $E \underset{K}{\simeq} L$:

Se tiene que $\sigma = \mathrm{id}_K : K \to L$ se extiende a $\overline{\sigma} : E \underset{K}{\hookrightarrow} L$.

Pero $E \simeq \overline{\sigma}(E) \subset L$,

y E alg. cerrado $\Rightarrow$ $\overline{\sigma}(E) \subset L$ alg. cerrado,

pero $L/\overline{\sigma}(E)$ alg. $\Rightarrow$ $L = \overline{\sigma}(E)$.

$\blacksquare$

Convención

Cada vez que diga $\overline{K}/K$ voy a suponer que $\overline{K}$ también es la clausura algebraica de cualquier extensión algebraica de K que esté considerando, para no complicarme.