Álgebra III - 2do C. 2020 - Clase 4 - 11/9/2020

3.2 Compuesto de cuerpos

Este concepto es general y lo podríamos haber visto después de "Cuerpo generado por" pero lo pongo ahora porque tenemos más herramientas para hacer ejemplos y ver propiedades.

Definición 3.2.1 (Compuesto de cuerpos)

Sean $K \subset F, L \subset E$. El compuesto de F y L es

$$\begin{aligned} FL &:= K(F \cup L) = F(L) = L(F) \\ &= \left\{ \frac{\sum_{i=1}^n s_i t_i}{\sum_{j=1}^m s'_i t'_i} :\ s_i, s'_j \in F, t_i, t'_j \in L, \sum_{j=1}^m s'_i t'_i \neq 0 \right\} \\ &= \left\{ \frac{f(t_1, \dots, t_n)}{g(t'_1, \dots, t'_m)} : f, g \text{ pols con coeftes en } F, t_i, t'_j \in L, g(\underline{t}') \neq 0 \right\}, \end{aligned}$$

el menor cuerpo que contiene tanto a F como a L.

¿Qué otro cuerpo se puede meter en forma natural en ese diagrama?

Ejemplos

- $F = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{3})$: $FL = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] =$

  $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) =$

- $F = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\xi_3)$: $FL = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$.

  $[\mathbb{Q}(\sqrt[3]{2}, \xi_3) : \mathbb{Q}] =$

  $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\xi_3) =$

- $F = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\sqrt[3]{2}\xi_3)$: $FL = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi_3) =$

  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi_3)) : \mathbb{Q}] =$

Proposición 3.2.2 *Sean $K \subset F, L \subset E$. Entonces*

1. *F/K algebraica $\Rightarrow$ FL/L algebraica, y $FL = L(F) = L[F]$*
2. *F/K finita $\Rightarrow$ FL/L finita, más aún $[FL : L] \leq [F : K]$*

   (En realidad alcanza $F/F \cap L$ finita, y vale $[FL : L] \leq [F : F \cap L]$)

   ¿Tiene que valer necesariamente la igualdad $[FL : L] = [F : F \cap L]$?

Prueba.–

1. El conjunto F es algebraico sobre K implica que el conjunto F es algebraico sobre L, y por lo tanto $FL = L(F) = L[F]$ es algebraico sobre L.
2. Si $\{v_1, \dots, v_n\}$ es base de F como K-ev, entonces $\{v_1, \dots, v_n\}$ genera $FL = L[F]$ (finita $\Rightarrow$ algebraica) como L-ev:

   Pues sea $f(s_1, \dots, s_n m) \in L[F]$ con $f \in L[X_1, \dots, X_m]$ y $s_1, \dots, s_m \in F$. Se tiene
   $$f(s_1, \dots, s_m) = \sum_a \underbrace{c_a}_{\in L} \underbrace{s_1^{a_1} \cdots s_m^{a_m}}_{\in F}$$
   donde cada monomio $s_1^{a_1} \cdots s_m^{a_m}$ es entonces combinación lineal de $v_1, \dots, v_n$ sobre K, o sea $f(s_1, \dots, s_m)$ termina siendo combinación lineal de $v_1, \dots, v_n$ sobre L.

■

Proposición 3.2.3 (Extensiones finitas/algebraicas y compuestos)
Sean $K \subset F, L \subset E$. Entonces

1. $$FL/K \text{ finita } \Leftrightarrow F/K \text{ y } L/K \text{ finitas,}$$
   y en ese caso, $[FL : K] \leq [F : K]\,[L : K]$.
2. $$FL/K \text{ algebraica } \Leftrightarrow F/K \text{ y } L/K \text{ algebraicas.}$$

Prueba.–

1. ($\Rightarrow$) OK pues F/K y L/K son subextensiones de FL/K.

   ($\Leftarrow$) $[FL : L] \leq [F : K] < \infty$ implica
   $$[FL : K] \; = \; [FL : L]\,[L : K] \; \leq \; [F : K]\,[L : K] \; < \; \infty$$
2. ($\Rightarrow$) OK pues F/K y L/K son subextensiones de FL/K.

   ($\Leftarrow$) F/K alg. $\Rightarrow$ FL/L algebraica, y L/K algebraica, implican FL/K algebraicas como torre de algebraicas.

■

3.3 Cuerpos de descomposición

Proposición 3.3.1 (Existencia de cuerpo con raíz)
Sea $f \in K[X]$ no constante. Entonces existe un cuerpo E extensión de K que contiene (al menos) una raíz de f.

Prueba.–
Spg podemos suponer $f \in K[X]$ irreducible.
Entonces $K[X]/\langle f\rangle$ es un cuerpo por ser $\langle f\rangle$ un ideal maximal de $K[X]$.
En $K[X]$ tenemos la relación de equivalencia módulo f que define las clases:

$$\overline{g} = \overline{h} \;\Leftrightarrow\; f \mid g - h.$$

(En particular $\overline{g} = \overline{r}_f(g)$, el resto de dividir a g por f.)
Sabemos que el mapa

$$\begin{array}{rccc} \pi_f : & K[X] & \to & K[X]/\langle f\rangle \\ & g & \mapsto & \overline{g} \end{array}$$

es un homomorfismo de anillos pues

- $\pi_f(g+h) = \pi_f(g) + \pi_f(h)$
- $\pi_f(g\,h) = \pi_f(g)\pi_f(h)$
- $\pi_f(1_K) = \overline{1}$.

<u>Afirmación:</u> $K \hookrightarrow K[X]/\langle f\rangle$ y $\overline{X}$ es raíz de f en $K[X]/\langle f\rangle$:
Dados $a, b \in K$ se tiene

$$\pi_f(a) = \pi_f(b) \;\Leftrightarrow\; \overline{a} = \overline{b} \;\Leftrightarrow\; f \mid a - b \;\Leftrightarrow\; a = b.$$

Así, $K \simeq \pi_f(K) \subset K[X]/\langle f\rangle$, y de esa forma, dado $g = \sum_i a_i X^i$, se tiene

$$\pi_f(g) = \overline{g} = \overline{\sum_i a_i X^i} = \sum_i \overline{a_i}\,\overline{X}^i = \sum_i a_i \overline{X}^i,$$

es decir $\overline{g} = g(\overline{X})$ en $K[X]/\langle f\rangle$.
En particular, $f(\overline{X}) = \overline{f} = \overline{0}$.
Concluimos que $\overline{X}$ es raíz de f en la extensión $K[X]/\langle f\rangle$ de K.

∎

Observación *(Isomorfismo de cuerpos con raíz)*

1. Sea E/K una extensión de cuerpos y sea $\alpha \in E$ una raíz de $f \in K[X]$ irreducible. Entonces $K[X]/\langle f \rangle \simeq K(\alpha)$ con un isomorfismo σ tq $\sigma(\overline{X}) = \alpha$ y $\sigma(a) = a$, $\forall\, a \in K$.

2. Sean E/K, F/K extensiones de cuerpos y sean $\alpha \in E, \beta \in F$ raíces de $f \in K[X]$ irreducible. Entonces $K(\alpha) \simeq K(\beta)$ con un isomorfismo σ tq $\sigma(\alpha) = \beta$ y $\sigma(a) = a$, $\forall\, a \in K$.

Prueba.–

1. Sea $\Phi : K[X] \to K[\alpha] = K(\alpha) \subset E$ la evaluación en α definida por $X \mapsto \alpha$, o sea $\Phi(g) = g(\alpha)$, $\forall\, g \in K[X]$.

   Entonces $\mathrm{Nu}(\Phi) = \{g \in K[X] : g(\alpha) = 0\} = \langle f \rangle$ pues f irreducible.

   Así,
   $$K[X]/\langle f \rangle \underset{\sigma}{\simeq} K[\alpha]$$
   con $\sigma := \overline{\Phi}$ que satisface lo indicado.

2. Tenemos
   $$K(\alpha) \underset{\sigma_\alpha^{-1}}{\simeq} K[X]/\langle f \rangle \underset{\sigma_\beta}{\simeq} K(\beta).$$

■

Intermezzo
K-inmersiones

Definición 3.3.2 (K-inmersión)
Sean E/K, F/K extensiones. Un morfismo de cuerpos $\sigma : E \to F$ que satisface además $\sigma(a) = a$, $\forall\, a \in K$, es decir $\sigma|_K = \mathrm{id}_K$, se llama un K-morfismo, o mejor una K-inmersión *(para recalcar el hecho que es un monomorfismo).*
Vamos a notar una K-inmersión σ por $E \underset{K}{\hookrightarrow} F$.

Nota 1: Una K-inmersión $\sigma : E \underset{K}{\hookrightarrow} F$ se extiende en forma natural a un K-(mono)morfismo de anillos $\sigma : E[X] \to F[X]$ con $\sigma(X) = X$.

Nota 2: Una K-inmersión es en particular una tl de K-ev, o sea un morfismo de K-álgebras, pues para $a \in K$ y $\alpha \in E$ se tiene $\sigma(a\,\alpha) = \sigma(a)\,\sigma(\alpha) = a\,\sigma(\alpha)$.
(Este es entonces el concepto natural de morfismo en extensiones de un cuerpo.)

Nota 3: Así, si $\sigma : E \underset{K}{\hookrightarrow} F$ es una K-inmersión y $f \in K[X]$ se tiene

$$\sigma(f(\alpha)) = f(\sigma(\alpha)), \quad \forall\, \alpha \in E$$

Nota 4: Sea $\sigma : K(\alpha) \underset{K}{\hookrightarrow} F$ una K-inmersión tal que $\sigma(\alpha) = \beta \in F$, entonces σ queda determinada en todo $K(\alpha)$ pues

$$\sigma\Big(\frac{f(\alpha)}{g(\alpha)}\Big) = \frac{f(\beta)}{g(\beta)}$$

donde $g(\beta) \neq 0$ pues $g(\alpha) \neq 0$ y σ inyectiva.

Teorema 3.3.3 (K-isomorfismos)
Sean E/K, F/K extensiones de cuerpos y sean $\alpha \in E, \beta \in F$ algebraicos sobre K. Entonces

$$\exists\, \sigma : \ K(\alpha) \underset{K}{\hookrightarrow} \ K(\beta) \ tq\ \sigma(\alpha) = \beta \iff f(\alpha, K) = f(\beta, K),$$

y en ese caso σ resulta un K-isomorfismo.

Prueba.–

($\Rightarrow$) Sabemos que $\sigma(\alpha) = \beta$ implica $\sigma(f(\alpha)) = f(\beta)$, $\forall\, f \in K[X]$.

Sea entonces $f := f(\alpha, K)$: $f(\beta) = \sigma(f(\alpha)) = \sigma(0) = 0$. Por lo tanto $f(\beta, K) \,|\, f(\alpha, K)$. ¿Sí?

Pero $f(\alpha, K)$ irreducible. Luego $f(\beta, K) = f(\alpha, K)$. ¿Sí?

($\Leftarrow$) OK, ya lo vimos arriba, ¿No?

Definición 3.3.4 (Cuerpo de descomposición)
Sea $f \in K[X]$ *un polinomio no constante. Se dice que* E/K *es un* cuerpo de descomposición de f sobre K *si cumple las dos condiciones siguientes*

1. f *se factoriza linealmente en* $E[X]$*, es decir existen* $\alpha_1, \ldots, \alpha_d \in E$*, no obligatoriamente distinto,s tales que*

$$f = (X - \alpha_1) \cdots (X - \alpha_d)$$

2. *Si* $F \subset E$ *es un cuerpo tal que* f *se factoriza linealmente en* $F[X]$*, entonces* $F = E$*.*

En ese caso E *es un cuerpo "más chico" que contiene todas las raíces de* f*:* $E = K(\alpha_1, \ldots, \alpha_d) = K[\alpha_1, \ldots, \alpha_d]$*, pues la extensión es algebraica, es más, finita.*

Ejemplos

- $f = X^3 - 2 \in \mathbb{Q}[X]$:
- $f = X^d - 1 \in \mathbb{Q}[X]$:
- $f = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$:

Teorema 3.3.5 (Existencia y unicidad del cuerpo de descomposición)
Sea $f \in K[X]$ *no constante. Entonces*

1. *Existe un cuerpo de descomposición de* f *sobre* K*.*
2. *Dos cuerpos de descomposición de* f *sobre* K *son* K*-isomorfos.*

Por eso denotaremos con $K(f)$ el *cuerpo de descomposiicón de* f *sobre* K*.*

Prueba.–
(1) *Existencia:* Naturalmente, por inducción en $\mathrm{gr}(f)$.

- $\mathrm{gr}(f) = 1$: ¿Quién es en ese caso un cuerpo de descomposición?
- $\mathrm{gr}(f) =: n > 1$: Sea $h \in K[X]$ irreducible tq $h \mid f$, y $K(\alpha_1) := K[X]/\langle h \rangle$ (que contiene una raíz de f).

  Se tiene que $f = (x - \alpha_1)g$ en $K(\alpha_1)[X]$ y $\mathrm{gr}(g) = n - 1$.

  Por lo tanto por HI existe un cuerpo de descomposición E de g sobre $K(\alpha_1)$: $E = K(\alpha_1)(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$ es entonces un cuerpo de descomposición de f sobre K.

Esta fue facil... La unicidad es un poquito más engorrosa pero se demuestra como cada vez que se demuestra unicidad en esquemas parecidos, y como lo han practicado mucho en Álgebra II con los diagramas conmutativos: es consecuencia de probar la existencia de morfismos para un lado y para el otro. En este caso aprovechamos para probar la proposición siguiente, un poco más general, que es importante en sí misma.

Proposición 3.3.6 (Extensión de inmersiones en extensiones finitas)
Sea $\sigma : E_1 \to F_1$ un isomorfismo de cuerpos, y sea $f \in E_1[X]$ no constante.
Sea E un cuerpo de descomposición de f sobre E_1 y sea F cualquier extensión de F_1 donde $\sigma(f)$ se factoriza linealmente. Entonces existe $\overline{\sigma} : E \to F$ morfismo de cuerpos que extiende a σ, i.e. $\overline{\sigma}|_{E_1} = \sigma$.

Prueba.–
Por inducción en $\mathrm{gr}(f)$.

- $\mathrm{gr}(f) = 1$: ¿Quiénes son en ese caso E y $\overline{\sigma}$?
- $\mathrm{gr}(f) =: n > 1$: Como E es cuerpo de descomposición de f sobre E_1, sea $\alpha \in E$ una raíz de $f \in E_1[X]$ y sea $h \mid f$ el factor irreducible de f en $E_1[X]$ que le corresponde a α.

  ¿Qué le pasa entonces a $\sigma(h) \in F_1[X]$? ¿Cómo es? ¿Por qué?

  Sea entonces $\beta \in F$ raíz de $\sigma(h) \in F_1[X]$, y definamos

  $$\tilde{\sigma} : \; E_1(\alpha) = E_1[\alpha] \to F_1(\beta) \subset F, \quad \tilde{\sigma}(g(\alpha)) := \sigma(g)(\beta).$$

  <u>Afirmación:</u> $\tilde{\sigma}$ es un isomorfismo de cuerpos que extiende a σ:

  (Ojo que esto es bastante sutil: no se puede mandar α a cualquier lado porque hay que respetar la relación dada por $h(\alpha) = 0$, pero lo que estamos diciendo es que si la respetamos, entonces sí da un morfismo)

  Considerar

  $$E_1(\alpha) \underset{\sigma_\alpha^{-1}}{\simeq} E_1[X]/\langle h \rangle \qquad ? \qquad F_1[X]/\langle \sigma(h) \rangle \underset{\sigma_\beta}{\simeq} F_1(\beta)$$

  y mostrar que el ? del medio es un isomorfismo de anillos usando el típico diagrama cociente de Álgebra II. Dejo lugar para hacerlo.

Así, $E_1(\alpha)\underset{\tilde{\sigma}}{\simeq}F_1(\beta)$, E cuerpo de descomposición de f sobre E_1 es cuerpo de descomposición de $f/(X-\alpha)$ (que tiene grado $(n-1)$) sobre $E_1(\alpha)$ y F es extensión de $F_1(\beta)$ donde $\tilde{\sigma}(f/(X-\alpha)) = \sigma(f)/(X-\beta)$ se factoriza linealmente.

Estamos en condiciones de aplicar la HI! $\tilde{\sigma} : E_1(\alpha) \to F_1(\beta)$ se extiende a $\overline{\sigma} : E \to F$, y recordemos que $\tilde{\sigma}$ extendía a $\sigma : E_1 \to F_1$. Esto concluye la demostración.

■