Álgebra III - 2do C. 2020 - Clase 3 - 8/9/2020

2.4 Cuerpo generado por

Así como en espacios vectoriales está la noción de "generado por", el menor espacio vectorial que contiene ciertos vectores, aquí pasa lo mismo. Vamos de a poco para foguearnos, pero todo es lo natural y que tiene sentido.

Definición 2.4.1 (Cuerpo generado por)
Sea E/K una extensión de cuerpos.

- *Sea $\alpha \in E$. Entonces $K[\alpha] := \big\{f(\alpha) : \ f \in K[X]\big\} \subset E$ es un dominio íntegro, y*

  $$K(\alpha) := \Big\{\frac{f(\alpha)}{g(\alpha)} : \ f, g \in K[X] \ \ \text{con} \ \ g(\alpha) \neq 0\Big\}$$

  es el cuerpo generado por α sobre K.

  Se tiene que $K(\alpha)$ es el menor cuerpo que contiene a K y a α,

  $$K(\alpha) = \bigcap \{F \ \text{cuerpo}\ , \ K \subset F \ \text{y}\ \alpha \in F\} \ \subset \ E.$$

  Pregunta molesta: ¿por qué nos tomamos el trabajo de especificar que $K \subset E$ y $\alpha \in E$?

- *Sean $\alpha_1, \dots, \alpha_n \in E$. Entonces*

  $$K[\alpha_1, \dots, \alpha_n] := \big\{f(\alpha_1, \dots, \alpha_n) : \ f \in K[X_1, \dots, X_n]\big\} \ \subset E$$

  es un dominio íntegro, y

  $$K(\alpha_1, \dots, \alpha_n) := \Big\{\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : \ f, g \in K[X_1, \dots, X_n] \ \ \text{con} \ \ g(\alpha_1, \dots, \alpha_n) \neq 0\Big\}$$

  es el cuerpo generado por $\alpha_1, \dots, \alpha_n$ sobre K.

  Se tiene que $K(\alpha_1, \dots, \alpha_n)$ es el menor cuerpo que contiene a K y a $\alpha_1, \dots, \alpha_n$, no importa el orden de los α_i, y $K(\alpha_1, \dots, \alpha_n)$ se puede pensar como una torre ya que

  $$K(\alpha_1, \dots, \alpha_n) = \big(K(\alpha_1, \dots, \alpha_m)\big)(\alpha_{m+1}, \dots, \alpha_n), \quad 1 \leq m < n.$$

- *Sea* $S \subset E$. *Entonces* $K[S]$ *es el dominio íntegro en* E *compuesto por evaluaciones en elementos de* S *de polinomios en cualquier número (finito) de variables con coeficientes en* K, *y*

$$K(S) := \Big\{ \frac{\beta}{\gamma} : \ \beta, \gamma \in K[S] \ \ \textit{con} \ \gamma \neq 0 \Big\} \ = \ \bigcap \big\{ F : K, S \subset F \big\} \ \subset \ E$$

  es el cuerpo generado por S sobre K.

  Se tiene que si $S, T \subset E$, *entonces* $K(S \cup T) = K(S)(T) = K(T)(S)$.

Ejemplos

- $\mathbb{Q}(\sqrt{2}) = \big\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} : \ f, g \in \mathbb{Q}[X], g(\sqrt{2}) \neq 0 \big\}$. ¿Se puede escribir más simple?
  ¡Sí! $\mathbb{Q}(\sqrt{2}) = \big\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}} : \ a, b, c, d \in \mathbb{Q}, c \neq 0 \text{ o } d \neq 0 \big\}$. ¿Y aún más simple?
  ¡Sí claro! Se pueden tomar $a, b, c, d \in \mathbb{Z}$... Claro.... ¿Pero aún más simple?

  Conclusión:

- $\mathbb{Q}(\sqrt[4]{2}) = \big\{ \frac{f(\sqrt[4]{2})}{g(\sqrt[4]{2})} : \ f, g \in \mathbb{Q}[X], g(\sqrt[4]{2}) \neq 0 \big\} \ = \ ?????$

- $\mathbb{Q}(\pi)$??????????????

¿Cuál es la diferencia entre estos ejemplos?

Definición 2.4.2 (Elementos algebraicos y trascendentes)
Sea E/K *extensión de cuerpos.*

- $\alpha \in E$ *es* algebraico sobre K *si existe* $f \in K[X]$ no nulo *tal que* $f(\alpha) = 0$.

- $\alpha \in E$ *es* trascendente sobre K *en caso contrario, es decir si para* $f \in K[X]$ *se tiene* $f(\alpha) = 0$, *entonces* $f = 0$.

(Esto depende siempre del cuerpo de base. Cuando se habla de algebraico o trascendente a secas, es sobre $\mathbb{Q}$.)

Definición-Proposición 2.4.3 (Polinomio minimal)
Sea E/K extensión de cuerpos y $\alpha \in E$ algebraico sobre K. El polinomio minimal *de α sobre K es el único polinomio mónico $f \in K[X]$ que satisface*

- $f(\alpha) = 0$ *y f tiene grado mínimo con esa propiedad,*

o equivalentemente,

- $f(\alpha) = 0$ *y si $g \in K[X]$ es tal que $g(\alpha) = 0$, entonces $f \mid g$ en $K[X]$,*

o equivalentemente,

- $f(\alpha) = 0$ *y f es irreducible en $K[X]$.*

Notaremos $f(\alpha, K)$ el polinomio minimal de α sobre K.

Prueba.– A cargo del lector

$\blacksquare$

Observación $f(\alpha, K)$ tiene grado 1 $\Leftrightarrow$ $\alpha \in K$.

Ejemplos

- $f(\sqrt{2}, \mathbb{Q}) = X^2 - 2$
- $f(\sqrt[4]{2}, \mathbb{Q}) =$
- $f(\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})) =$
- $f(\sqrt{2} + \sqrt{3}, \mathbb{Q}) =$
- $f(\sqrt{3}, \mathbb{Q}(\sqrt{2})) =$
- $f(\xi_p, \mathbb{Q}) =$

Observaciones

- α algebraico$/ K \quad \Leftrightarrow \quad K[\alpha] = K(\alpha)$

  Prueba.–

  $(\Rightarrow)$ $(\subseteq)$ OK

  $(\supseteq)$ Se trata de ver si $\frac{1}{g(\alpha)}$ con $g(\alpha) \neq 0$ se puede escribir como un polinomio en α:

  Sea $f := f(\alpha, K)$ que sabemos que es irreducible. Como $g(\alpha) \neq 0$, entonces f y g son polinomios coprimos. ¿Sí? Por lo tanto

  $$\exists\, r, s \in K[X] \text{ tq } r\,f + s\,g = 1 \underset{f(\alpha)=0}{\Rightarrow} s(\alpha)g(\alpha) = 1 \quad \Rightarrow \quad \frac{1}{g(\alpha)} = s(\alpha).$$

  $(\Leftarrow)$

  $$K[\alpha] = K(\alpha) \Rightarrow \frac{1}{\alpha} = g(\alpha) \in K[\alpha] \Rightarrow g(\alpha)\alpha - 1 = 0 \Rightarrow \alpha \text{ es algebraico}$$

  (¿Por qué ese polinomio que anula a α es no nulo?)

  $\blacksquare$

- α algebraico$/ K \quad \Rightarrow \quad K(\alpha)/K$ es finita y $[K(\alpha) : K] = \operatorname{gr}(f(\alpha, K))$.

  Prueba.– Si $f(\alpha, K) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ que es irreducible, entonces ¿quién es base de $K(\alpha) = K[\alpha]$ como K-ev?

  $\blacksquare$

- $E/F/K$ y $\alpha \in E$ algebraico sobre K, entonces α es algebraico sobre F y $f(\alpha, F) \mid f(\alpha, K)$ en $F[X]$.

  Prueba.–

  $\blacksquare$

3 Extensiones algebraicas

3.1 Generalidades

Definición 3.1.1 (Extensión algebraica)
Sea E/K extensión de cuerpos. Se dice que E/K es algebraica *si para todo $\beta \in E$, se tiene que β es algebraico sobre K.*

Proposición 3.1.2 (Finita $\Rightarrow$ algebraica)
Sea E/K extensión. Entonces E/K finita $\Rightarrow$ E/K algebraica.

Prueba.– Supongamos que $[E : K] = n$, y sea $\beta \in E$. ¿Qué pasa con $1, \beta, \ldots, \beta^n$?

■

¿Vale la recíproca?

Corolario 3.1.3 *Si α es algebraico sobre K, entonces la extensión $K(\alpha)/K$ es algebraica.*

O sea son equivalentes:

1. α es algebraico sobre K
2. $[K(\alpha) : K] < \infty$
3. $K(\alpha)/K$ es algebraica
4. $K(\alpha) = K[\alpha]$

Proposición 3.1.4 *Sea E/K una extensión de cuerpos y sean $\alpha_1, \ldots, \alpha_s \in E$. Son equivalentes*

1. *$\alpha_1, \ldots, \alpha_s$ son algebraicos sobre K,*
2. *$[K(\alpha_1, \ldots, \alpha_s) : K] < \infty$*
3. *$K(\alpha_1, \ldots, \alpha_s)/K$ es algebraica*
4. *$K(\alpha_1, \ldots, \alpha_s) = K[\alpha_1, \ldots, \alpha_s]$*

Prueba.–
El caso $s = 1$ está hecho. Es natural entonces probar esto por inducción en s.

(1 ⇒ 2) $K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1, \ldots, \alpha_{s-1})(\alpha_s)$ donde $\alpha_1, \ldots, \alpha_{s-1}$ son algebraicos sobre K y α_s es algebraico sobre $K(\alpha_1, \ldots, \alpha_{s-1})$

Luego, por HI, $K(\alpha_1, \ldots, \alpha_{s-1})/K$ es finita, y por el caso 1, $K(\alpha_1, \ldots, \alpha_s)/K(\alpha_1, \ldots, \alpha_{s-1})$ es finita, y por lo tanto $K(\alpha_1, \ldots, \alpha_s)/K$ es finita como torre de finitas.

(2 ⇒ 3) OK por la proposición 3.1.2

(3 ⇒ 4) $K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1, \ldots, \alpha_{s-1})(\alpha_s) = K(\alpha_1, \ldots, \alpha_{s-1})[\alpha_s]$ por el caso 1, y $K(\alpha_1, \ldots, \alpha_{s-1}) = K[\alpha_1, \ldots, \alpha_{s-1}]$ por HI. Además $K[\alpha_1, \ldots, \alpha_s] = K[\alpha_1, \ldots, \alpha_{s-1}][\alpha_s]$.

(4 ⇒ 1) Es cierto pero al parecer no sale así con cuentitas... Es bastante más complicado y conceptual. Así que los dejo para que lo busquen, investiguen y resuelvan durante todo el semestre.

■

Corolario 3.1.5 (Caracterización de extensiones finitas)
Sea E/K una extensión de cuerpos. Entonces

$$E/K \text{ es finita} \iff \exists\, \alpha_1, \ldots, \alpha_s \in E \;\; alg/K \;\; tq \;\; E = K(\alpha_1, \ldots, \alpha_s)$$

Prueba.–

(⇒) E/K finita tiene una base finita $\{\alpha_1, \ldots, \alpha_s\}$ como K-ev, y son todos algebraicos. Entonces $E = K(\alpha_1, \ldots, \alpha_s)$ (¡hay elementos de más que generan pero no importa!)

(⇐) $E = K(\alpha_1, \ldots, \alpha_s)$ con $\alpha_1, \ldots, \alpha_s$ algebraicos/ K ⇒ $[E : K] < \infty$ por la proposición 3.1.4.

■

Corolario 3.1.6 *Sea E/K una extensión de cuerpos. Entonces*

$$\{\alpha \in E : \; \alpha \;\; \text{es algebraico sobre} \;\; K\} \subset E$$

es una subextensión de cuerpos de E, que contiene a K.

Prueba.– Alcanza con comprobar que si $\alpha, \beta \in E$ son algebraicos sobre K, entonces $\alpha \pm \beta$, $\alpha \cdot \beta$ y α/β (si $\beta \neq 0$) son algebraicos sobre K. ¿Por qué vale esto?

■

Problema práctico interesante: Teniendo $f(\alpha, K)$ y $f(\beta, K)$, ¿cómo se puede calcular un polinomio en $K[X]$ que anula a $\alpha + \beta$?

Ejemplo ($\overline{\mathbb{Q}}$)

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \ \alpha \ \text{ es algebraico (sobre } \mathbb{Q})\}$$

es el cuerpo de números algebraicos.
¿Es una extensión finita o infinita de $\mathbb{Q}$?

Veamos ahora la versión infinita de la Proposición 3.1.4.

Proposición 3.1.7 *Sea E/K una extensión de cuerpos y sea $S \subset E$. Entonces*

1. *S algebraico sobre K $\Leftrightarrow$ $K(S)/K$ algebraica*
2. *$[K(S) : K] < \infty$ $\Rightarrow$ $K(S)/K$ algebraica*

   ¿Vale la recíproca?
3. *S algebraico sobre K $\Rightarrow$ $K(S) = K[S]$*

   ¿Vale la recíproca?

Prueba.–
Siempre se trata de reducirse al caso finito donde valen todas las equivalencias.

1. ($\Rightarrow$)

$$\begin{aligned} \alpha \in K(S) \ &\Rightarrow \ \alpha = \frac{f(s_1, \ldots, s_n}{g(t_1, \ldots, t_m)} \ \text{ con } \ s_i, t_j \in S \\ &\Rightarrow \ \alpha \in K(s_1, \ldots, s_n, t_1, \ldots, t_m) \ \text{ con } \ s_i, t_j \ \text{ algebraicos sobre } \ K \\ &\Rightarrow \ \alpha \ \text{ alg. sobre } K \text{ pues } K(s_1, \ldots, s_n, t_1, \ldots, t_m)/K \ \text{ alg.} \end{aligned}$$

   ($\Leftarrow$) Obvio ¿no?

2. Finito $\Rightarrow$ Algebraica siempre. ¿Qué pasa con la vuelta?

3. Alcanza con probar que $\dfrac{1}{g(t_1,\ldots,t_m)} \in K[S]$ para $t_1,\ldots,t_m \in S$, o sea se escribe como un polinomio evaluados en elementos de S. Pero

$$\frac{1}{g(t_1,\ldots,t_m)} \in K(t_1,\ldots,t_m) = K[t_1,\ldots,t_m] \subset K[S]$$

¿Qué pasa con la vuelta?

■

Proposición 3.1.8 (Extensiones algebraicas y torres)
Sea $E/F/K$ una torre de cuerpos. Entonces

$$E/K \text{ algebraica } \Leftrightarrow E/F \text{ y } F/K \text{ algebraicas}$$

Prueba.–

$(\Rightarrow)$

- E/F algebraica: $\alpha \in E$ alg/K $\Rightarrow$ $\alpha \in E$ alg/F.
  (Y de paso, ¿qué le pasaba a $f(\alpha,F)$ con respecto a $f(\alpha,K)$?)

- F/K algebraica: $\alpha \in F \subset E$ $\Rightarrow$ α alg/K.

$(\Leftarrow)$ Sea $\alpha \in E$. Qpq α es algebraico sobre K sabiendo que E/F y F/K son algebraicas. Siempre intentar reducirse al caso finito donde todo vale...

Sabemos que α alg. sobre F: Sea

$$f := f(\alpha,F) = X^m + b_{m-1}X^{m-1} + \cdots + b_0 \in F[X]$$

Entonces $f \in K(b_0,\ldots,b_{m-1})[X]$ donde $b_0,\ldots,b_{m-1} \in F$ son algebraicos sobre K. O sea en realidad α es algebraico sobre $K(b_0,\ldots,b_{m-1})$ que es una extensión algebraica (finita) de K.

En definitiva, $\alpha \in K(b_0,\ldots,b_{m-1})(\alpha)$ que es finita, con lo cual α es algebraico sobre K

■