~~Habíamos visto~~

$\cancel{\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})}$

$\cancel{\mathbb{Q}(\pi), \mathbb{Q}(X)}$ ~~con X indeterminada~~

<u>Definición</u> (Cuerpo generado por)

① $K(\alpha)$

② Sea E/K ext de cpos y $\alpha_1, .., \alpha_s \in E$

$$K[\alpha_1, .., \alpha_s] = \{ f(\alpha_1, .., \alpha_s),\ f \in K[X_1, .., X_s] \} \subseteq E \text{ anillo (di)}$$

$$K(\alpha_1, .., \alpha_s) = \left\{ \frac{f(\alpha_1, .., \alpha_s)}{g(\alpha_1, .., \alpha_s)},\ f, g \in K[X_1, .., X_s],\ g(\alpha_1, .., \alpha_s) \neq 0 \right\}$$

menor cuerpo que contiene a K y a $\alpha_1, .., \alpha_s$.

Se tiene $K(\alpha_1, .., \alpha_s) = K(\alpha_1)(\alpha_2) \dots (\alpha_s)$ etc...

③ $S \subseteq E$

$K[S] = \{$ expresiones polinomiales evaluadas en (finitos) eltos de $S \} \subseteq E$

$$K(S) = \left\{ \frac{f(s_1, .., s_n)}{g(t_1, .., t_m)},\ f, g \text{ pols},\ s_i, t_j \in S,\ g(\underline{t}) \neq 0 \right\} \subseteq E$$

Se tiene $K(S \cup T) = K(S)(T) = K(T)(S)$

es el menor cuerpo que contiene a K, y S.

Habíamos visto

$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}[\sqrt[4]{2}] = \mathbb{Q}(\sqrt[4]{2})$

$\mathbb{Q}(\pi)$, $\mathbb{Q}(X)$ con X indeterminada

Ejemplos

1) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$ d.i.

$\mathbb{Q}(\sqrt{2}) = \{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = a' + b'\sqrt{2},\ a, b \in \mathbb{Q}\}$ *

$= \mathbb{Q}[\sqrt{2}]$ es cuerpo.

2) X indeterminada / $\mathbb{Q}$:

$\mathbb{Q}(X) = \{ \frac{f(x)}{g(x)},\ g \neq 0 \}$

ANTES: Hoja 0

3) π trascendente $s/\mathbb{Q}$ = ...

Definición (eltos algebraicos y trascendentes)

Sea E/K extensión de cuerpos

1) $\alpha \in E$ es algebraico sobre K si $\exists f \in K[X]$ no nulo tq $f(\alpha) = 0$

2) $\alpha \in E$ es trascendente sobre K si $\nexists$ $f(\alpha) = 0 \Rightarrow f = 0$

(Depende siempre del cuerpo de base)

Proposición (Pol. minimal)

Sea E/K extensión de cuerpos y sea
Si $\alpha \in E$ es algebraico / K.
Entonces el minimal de α sobre K es el único polinomio mónico $f \in K[X]$ que satisface

① $f(\alpha) = 0$

② f tiene grado mínimo

o equivalentemente

① $f(\alpha) = 0$

② si $g \in K[X]$ satisface $g(\alpha) = 0$, entonces $f \mid g$

o equivalentemente

① $f(\alpha)=0$

② f es irreducible en $K[X]$

Demostración

$\exists g$ mónico y de grado ≥ 1 / $f(\alpha)=0$ — dominio de ideales ppales

Sea $I = \langle g \in K[X] / g(\alpha)=0 \rangle = \langle f \rangle$ con f mónico

e irreducible pues si $f = gh$ ent. $g(\alpha)=0$ ó $h(\alpha)=0$

y es único en c/caso

Ejemplos $f(\sqrt{2}, \mathbb{Q}) = X^2 - 2$

$f(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = X^4 - 10X^2 + 1$

$f(\xi_p, \mathbb{Q}) = X^{p-1} + \dots + 1$ (irreducible como consecuencia de Eisenstein)

Observaciones

① α algebraico$/K \iff K[\alpha] = K(\alpha)$

$(\Rightarrow)$ $\subseteq$ ✓

$\supseteq$ $\quad \dfrac{1}{g(\alpha)} = s(\alpha)$?

Sea $f = f(\alpha, K)$ irred. Como $g(\alpha) \neq 0$, $f \perp g$

$\exists r, s / \ r f + s g = 1$

$\Rightarrow \quad s(\alpha)\, g(\alpha) = 1$

$(\Leftarrow)$ $K[\alpha] = K(\alpha) \Rightarrow \dfrac{1}{\alpha} = g(\alpha)$

$\Rightarrow g(\alpha).\alpha - 1 = 0 \Rightarrow \alpha$ es algebraico.

② α algebraico$/K \Rightarrow K[\alpha]/K$ es finita y $[K(\alpha):K] = \text{gr}(f(\alpha,K))$

Si $f(\alpha, K) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ (irred) en $K[X]$

entonces $K[\alpha]$ tiene como base, como K-e.v por

$\{1, \alpha, \dots, \alpha^{n-1}\}$ [illegible]

③ $E/F/K$ y $\alpha \in E$ alg$/K$. Entonces $f(\alpha, F) \mid f(\alpha, K)$

Extensiones algebraicas

Definición (Extensión algebraica)

Sea E/K una extensión de cuerpos.

E/K es algebraica $\iff \forall \beta \in E$, β es alg$/K$

Proposición E/K finita $\Rightarrow$ E/K algebraica

Demostración Sea $[E:K]=n$

Dado $\beta \in E$, $1, \beta, \ldots, \beta^n$ no pueden ser li

$\Rightarrow \exists$ un polinomio no nulo que anula a β

RECÍPROCA ?

Observación: Si α es alg.$/K$, entonces $K[\alpha]$ es algebraica

pues $\forall \beta \in K[\alpha]$, $K[\beta]/K$ es finita.

Sea son equivalentes para $\alpha \in E/K$:

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

PROPOSICIÓN: Dados $\alpha_1, \ldots, \alpha_s \in E/K$. Son equivalentes

1. $\alpha_1, \ldots, \alpha_s$ alg$/K$
2. $[K(\alpha_1, \ldots, \alpha_s):K] < \infty$
3. $K(\alpha_1, \ldots, \alpha_s)$ alg$/K$
4. $K[\alpha_1, \ldots, \alpha_s] = K(\alpha_1, \ldots, \alpha_s)$

Demostración

$(1 \Rightarrow 2)$ $K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1, \ldots, \alpha_{s-1})(\alpha_s)$ y

$$[K(\alpha_1, \ldots, \alpha_s):K] = \underbrace{[K(\alpha_1, \ldots, \alpha_s) : K(\alpha_1, \ldots, \alpha_{s-1})]}_{< \infty} \underbrace{[K(\alpha_1, \ldots, \alpha_{s-1}) : K]}_{< \infty \text{ (HI)}}$$

pues α_s alg$/ K(\alpha_1, \ldots, \alpha_{s-1})$

(2) $\Rightarrow$ (3) ✓ (3) $\Rightarrow$ (1) ✓

(1) $\Rightarrow$ (4): $K(\alpha_1,..,\alpha_s) = K(\alpha_1,..,\alpha_{s-1})(\alpha_s) = K(\alpha_1,..,\alpha_{s-1})[\alpha_s]$

Por inducción en s

(4) $\Rightarrow$ (1): EJERCICIO (Difícil)

[redacted]

→

<u>Corolario</u> (Caracterización de extensiones finitas)

Sea E/K extensión.

Entonces: E/K finita $\Leftrightarrow$ $\exists\ \alpha_1,..,\alpha_s \in E$ alg$/K$

tq $E = K(\alpha_1,..,\alpha_s) = K[\alpha_1,..,\alpha_s]$

<u>Demostración</u>:

($\Rightarrow$) E/K finita $\Rightarrow$ $\exists$ base finita como K-ev,

$\alpha_1,..,\alpha_s$ y son todos algebraicos

$E = K(\alpha_1,..,\alpha_s)$ (hay de más pero no importa)

($\Leftarrow$) $E = K(\alpha_1,..,\alpha_s)$ con $\alpha_1,..,\alpha_s$ alg $\Rightarrow$

$\Rightarrow$ $[E:K] < \infty$

<u>Corolario</u>

α, β alg$/K$ $\Rightarrow$ $\alpha \pm \beta$, $\alpha\beta$ alg $/K$

α/β alg $/K$

pues son una subextensión de $K[\alpha,\beta]$

(1) $\mathbb{C}/\overline{\mathbb{Q}}/\mathbb{Q}$

$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} / \alpha$ es alg $/K\}$ es un cuerpo

(2) E/K. $K_E: \{\alpha \in E / \alpha$ es alg$/K\}$ es subcuerpo de E que contiene a K

$\overline{\mathbb{Q}}/\mathbb{Q}$ es infinita: Considerar por ejemplo $\sqrt[n]{2}$ en $\overline{\mathbb{Q}}$: grado de la extensión

Ojo con $S \subseteq E$ (S ∞)

Proposición

1. S algebraico$/K \iff K(S)$ algebraico$/K$

2. $[K(S):K] < \infty \Rightarrow K(S)/K$ algebraico

   Pero no vale la vuelta: $\overline{\mathbb{Q}}/\mathbb{Q}$ alg pero ∞

3. S algebraico $\Rightarrow K(S) = K[S]$

   Pero $\Leftarrow$ Falso: $\mathbb{Q}[\mathbb{C}] = \mathbb{C} = \mathbb{Q}(\mathbb{C})$

   pero $\mathbb{C}$ no alg$/\mathbb{Q}$

Demostración

1. ($\Rightarrow$) $\alpha \in K(S)$: $\alpha = \dfrac{f(s_1,.., s_n)}{g(t_1,.., t_m)} \in K(S)$

$\Rightarrow \alpha \in K(s_1,.., s_m, t_1,.., t_m)$ con $s_1,.., s_m, t_1,.., t_m$ alg$/K$

$\Rightarrow \alpha$ es alg$/K$ pues $K(s_1,.., s_m, t_1,.., t_m)$ alg$/K$

($\Leftarrow$) obvio.

2. finito $\Rightarrow$ alg siempre

3. Siempre reducir a finitos eltos:

($\Rightarrow$) Quiero probar que $\dfrac{1}{g(s_1,.., s_m)} \in K[S]$, o sea se escribe como un pol en eltos de S.

Pero $\dfrac{1}{g(s_1,.., s_m)} \in K(s_1,.., s_m) = K[s_1,.., s_m] \subseteq K[S]$ $\boxtimes$

Proposición Sea $E/F/K$ una torre de extensiones. Entonces

E/K algebraica $\iff E/F$ y F/K algebraicas

Demostración

$(\Longrightarrow)$ $\alpha \in E$ alg$/K \Rightarrow \alpha \in E$ alg$/F$

(recordar $f(\alpha, F) \mid f(\alpha, K)$ en $F[X]$)

$\alpha \in F \subseteq E \Rightarrow \alpha$ alg$/K$

$(\Longleftarrow)$ Sea $\alpha \in E$.

Entonces α alg$/F$:

Sea $f := f(\alpha, F) = X^m + b_{m-1} X^{m-1} + \dots + b_0$, $b_i \in F$

$\Rightarrow f \in K(b_0, .., b_{m-1})[X]$ con $b_0, .., b_{m-1}$ alg$/K$.

o sea α alg$/K(b_0, .., b_{m-1})$ que es finita

$\Rightarrow \alpha \in K(b_0, .., b_{m-1})(\alpha)$

con $[K(b_0, .., b_{m-1})(\alpha) : K]$ finita pues

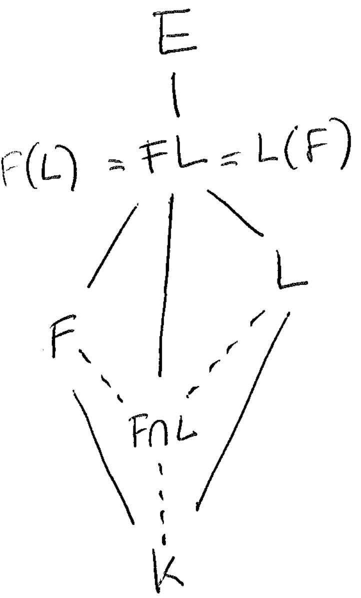
$K(b_0, .., b_{m-1})/K$ y $K(b_0, .., b_{m-1})(\alpha)/K(b_0, .., b_{m-1})$

finitas $\boxtimes$

$\Rightarrow \alpha$ alg$/K$

Compuestos de cuerpos

Definición: Sean $K \subseteq F, L \subseteq E$



$$FL := K(F \cup L) = F(L) = L(F)$$

menor cuerpo que contiene a F y a L

$$= \left\{ \frac{\sum_{i=1}^{m} a_i b_i}{\sum_{j=1}^{n} a'_j b'_j},\ a_i, a'_j \in F,\ b_i, b'_j \in L \right\}$$

$$= \left\{ \frac{f(b_1,..,b_n)}{g(b'_1,..,b'_m)},\ f, g \in F[x_1,..,x_n,...] \right\}$$

Proposición

① F/K algebraica $\Rightarrow$ LF/L algebraica y $LF = L(F) = L[F]$

② F/K finita $\Rightarrow$ $[FL:L] \leq [F:K] < \infty$

Demostración

① Los eltos de $F \subseteq E$ son alg$/K \subseteq L$ $\Rightarrow$ los eltos de F son alg$/L$ $\Rightarrow$ $LF = L(F) = L[F]$

y si $f(b_1,..,b_m) \in LF$ con $f(x_1,..,x_m) \in L[x_1,..,x_m]$ y $b_1,..,b_m \in F$, entonces $f(b_1,..,b_m) \in L[b_1,..,b_m]$ con $b_1,..,b_m$ alg$/L$ $\Rightarrow$ $f(b_1,..,b_m)$ alg$/L$.

② Si $\{v_1,..,v_n\}$ es base de F como K-ev, entonces $\{v_1,..,v_n\}$ genera FL como L-ev.:

Como $FL = L[F]$, si $f(b_1,..,b_n) \in LF$ como arriba y

$f(b_1,.., b_m) = \sum c_{\underline{a}} \underbrace{b_1^{a_1} \cdots b_m^{a_m}}_{\in F}$ y $c_{\underline{a}} \in L$, donde $b_1^{a_1} \cdots b_m^{a_m}$ es cl $/K$ de $v_1,.., v_n$, ent. $f(b_1,.., b_m)$ es cl $/L$ de $v_1,.., v_m$.

De hecho alcanza con $F/F\cap L$ finita: $[FL:L] \leq [F:F\cap L] < \infty$

Pensar si tiene que valer $[FL:K] = [F:F\cap L]$

$$\begin{tikzcd}
 & \mathbb{Q}[\sqrt[3]{2}, \xi_3] = E & \\
F = \mathbb{Q}[\sqrt[3]{2}] \arrow[ur, dash, "2"] & & \mathbb{Q}[\sqrt[3]{2}\xi_3] = L \arrow[ul, dash, "2"'] \\
 & \mathbb{Q} \arrow[ul, dash, "3"] \arrow[ur, dash, "3"'] \arrow[uu, dash, "6"] &
\end{tikzcd}$$

$FL = E$

$F \cap L = \mathbb{Q}$

<u>PROPOSICIÓN</u> $[FL:K] < \infty \iff [F:K]$ y $[L:K] < \infty$

y en ese caso $[FL:K] \leq [F:K][L:K]$

<u>Demostración</u>

$(\Longrightarrow)$ ✓ F/K y L/K subext de FL/K

$(\Longleftarrow)$ $[FL:L] \leq [F:K]$

$\Rightarrow [FL:K] \leq [FL:L][L:K] \leq [F:K][L:K] < \infty$

<u>PROPOSICIÓN</u>

FL/K algebraica $\iff$ F/K y L/K algebraicas

<u>Demostración</u>

$(\Longrightarrow)$ ✓ F/K y L/K subext de FL/K

$(\Longleftarrow)$ $\left.\begin{array}{l} F/K \text{ alg} \Rightarrow FL/L \text{ alg} \\ L/K \text{ alg} \end{array}\right\} FL/K \text{ alg}$

(Torres de algs es alg)