K es un $\mathbb{Q}$-e.v.

Recuerdo: K cpo $\begin{cases} \rightarrow \mathbb{Q} \subset K & car(K)=0 \\ \text{o bien } p \text{ primo t.q. } \mathbb{F}_p = \mathbb{Z}/p \subset K. & car(K)=p \end{cases}$

Nos interesa $\boxed{\dim_{\mathbb{Q}}(K) = [K:\mathbb{Q}] < \infty}$ (*). $([K:\mathbb{F}_p] < \infty)$

Def: $K \subset L$, $[L:K] = \dim_K L$.

Vimos: si vale (*), todo $\alpha \in K$ es raíz de $p(x) \in \mathbb{Q}[x]$.

Def: Si $\mathbb{Q} \subset K$, un elemento $\alpha \in K$ se dice algebraico si existe $p(x) \in \mathbb{Q}[x]$ tal que $p(\alpha) = 0$.

Def: Una extensión K de $\mathbb{Q}$ ($\mathbb{Q} \subset K$ y ambos son cuerpos) se dice algebraica si todo elemento $\alpha \in K$ es algebraico sobre $\mathbb{Q}$.

$\Rightarrow$ Si $[K:\mathbb{Q}] < \infty \Rightarrow$ es algebraica.

Comentario: π no es algebraico sobre $\mathbb{Q}$. Más aún los números algebraicos en $\mathbb{C}$ son "pocos".

Ejercicio: si $\mathbb{Q} \subset K$, $\alpha \in K$, son equivalentes:

1. α es algebraico.
2. $\mathbb{Q}[\alpha] \subset K$, $\mathbb{Q}[\alpha] = \{\sum_{n=0}^{N} a_n \alpha^n, a_n \in \mathbb{Q}\}$, $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] < \infty$
3. $\mathbb{Q}[\alpha]$ es un cuerpo.

Obs: 1. Si $p(x) \in \mathbb{Q}[x]$ irreducible, $K = \mathbb{Q}[x]/_{p(x)}$ es algebraica.

Vimos: si α es raíz de $a_0 + a_1 x + \cdots + a_n x^n$, $\mathbb{K} = \mathbb{Q}[\alpha] =$

$\mathbb{Q}[x]/p(x)$ es algebraica y conocemos un polinomio

que tiene a α como raíz. $\beta \in K \rightsquigarrow$ ¿cómo hallar

un polinomio que lo tenga como raíz? $\leq [K:\mathbb{Q}]$

$\beta \in K$ es algebraica, $\mathbb{Q}[\beta] \subset K$, $\dim_{\mathbb{Q}} \mathbb{Q}[\beta] < \infty$

$\Rightarrow$ β raíz de un polinomio. $\quad \deg(m_\beta)$

Ejemplo: $x^3 - 2$, $\alpha = \sqrt[3]{2}$, $K = \mathbb{Q}[\alpha] \ni \sqrt[3]{2} + \sqrt[3]{4} + 1 = \beta$

base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

Problema: hallar un polinomio que lo tenga como raíz.

$\{1, \beta, \beta^2, \beta^3\}$ no son l.i.

2. Dado $p(x) \in K[x]$ irreducible, $L = K[x]/(p(x))$ cuerpo. $\supset K$

$\bar{x}$ es una raíz de $p(x)$ $\quad p(\bar{x}) = 0$

En L agregamos una raíz de $p(x)$ (a saber $\bar{x}$)

A priori, sólo agregamos una.

Ejemplos: 1. $p(x) = x^3 - 2$ irreducible, $L = \mathbb{Q}[x]/(x^3-2) \simeq \mathbb{Q}[\sqrt[3]{2}]$

$\bar{x} \to \sqrt[3]{2}$

En $\mathbb{C}$, $x^3 - 2$ tiene raíces: $\{\sqrt[3]{2}, \xi_3\sqrt[3]{2}, \xi_3^2\sqrt[3]{2}\} \not\subset \mathbb{R}$

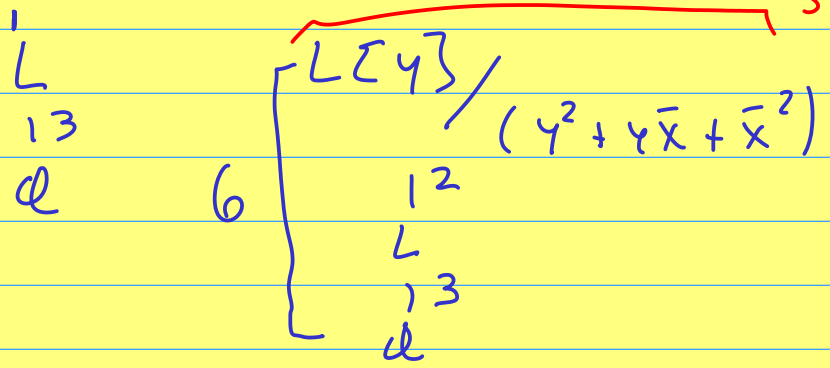
Miremos $y^3 - 2$ en $L = \mathbb{Q}[x]/(x^3-2)$

$y^3 - 2 = (y - \bar{x})(y^2 + y\bar{x} + \bar{x}^2)$ en $L[y]$

irreducible en L.

Pregunta: ¿qué hago si quiero construir un cuerpo donde $p(x)$ se factorice linealmente?

acá gané.



2. $p(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ irreducible.

$L = \mathbb{Q}[x]/p(x)$, $[L : \mathbb{Q}] = 3$, Afirmo: $p(x)$ en L se factoriza linealmente.

Demo: Si α es raíz de $p(x) \Rightarrow \alpha^2 - 2$ y $1 - \alpha - \alpha^2$ también son raíces.

$$(\alpha^2-2)^3 + (\alpha^2-2)^2 - 2\cdot(\alpha^2-2) - 1 = \alpha^6 - 6\alpha^4 + 12\alpha^2 - 8$$

$$+ \alpha^4 - 4\alpha^2 + 4 - 2\alpha^2 + 4 - 1 = \alpha^6 - 5\alpha^4 + 6\alpha^2 - 1 =$$

$$(\alpha^3 + \alpha^2 - 2\alpha - 1)(\alpha^3 - \alpha^2 - 2\alpha + 1) = 0.$$

$\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$

Luego $y^3 + y^2 - 2y - 1 = (y - \bar{x})(y - (\bar{x}^2 - 2))(y - (1 - \bar{x} - \bar{x}^2))$

Obs: Los cuerpos K que contienen a $\mathbb{Q}$ que construimos son de la forma $\mathbb{Q}[x]/p(x)$, $p(x)$ irreducible.

Pregunta: ¿son todos $K \supset \mathbb{Q}$, $[K : \mathbb{Q}] < \infty$ así?

Teo: Si $\mathbb{Q} \subset K$, $[K:\mathbb{Q}] < \infty \Rightarrow \exists\, p(x) \in \mathbb{Q}[x]$ irred. tal que $K \simeq \mathbb{Q}[x]/(p(x))$

Obs: Lo mismo vale para $\mathbb{F}_p$. (Demo para otro curso).

Ejemplo: $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{ \sum a_{ij} \sqrt{2}^i \sqrt{3}^j \} = \langle 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \rangle_{\mathbb{Q}}$

$[K:\mathbb{Q}] = 4$, $4 \begin{cases} K \\ \mathbb{Q}[\alpha] \\ \mathbb{Q} \end{cases}$ $\begin{matrix} 1 \\ 4 \end{matrix}$ $\sqrt{2}+\sqrt{3}$ sirve.

$\alpha^2 = (\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6}$ $\quad \{1, \sqrt{2}+\sqrt{3}, 5+2\sqrt{6}\}$ son l.i.

$\Rightarrow \alpha$ es raíz de un polinomio de grado 2.

↓ mónico.

Def: Si k cuerpo, $p(x) \in k[x]$, un cuerpo de descomposición de $p(x)$ es un cuerpo L tal que:

1. $k \subset L$
2. $p(x) = (x-\gamma_1) \cdots (x-\alpha_n)$, $\alpha_i \in L$ (raíces están en L)
3. $L = k[\alpha_1, \dots, \alpha_n]$ (es lo más chico posible).

$$\{ \sum_i q_{\vec{i}}\, \alpha^{\vec{i}} \,.\, q_{\vec{i}} \in k,\ \vec{i} \in (\mathbb{N} \cup \{0\})^n \}$$

Ejemplos:

- $x + a \in \mathbb{Q}[x]$, un cuerpo de descomposición es $\mathbb{Q}$.
- $p(x) = x^2 + 1$, $L = \mathbb{Q}[i] \simeq \mathbb{Q}[x]/(x^2+1)$ $\quad \overline{x} \leftrightarrow i$
- $p(x) = x^3 + x^2 - 2x - 1$, un cpo de desc. es $\mathbb{Q}[x]/(p(x))$
- $p(x) = x^3 - 2$, un cpo de desc. es $\mathbb{Q}[x,y]/(x^3-2,\ y^2+xy+x^2) =$

$$= \left(\mathbb{Q}[X]/(X^3-2) \right)[Y]/(Y^2+YX+X^2) \simeq \mathbb{Q}[\sqrt[3]{2}, \underline{\underline{\xi_3}}]$$

$X^3-1=0$

$(X-1)(X^2+X+1)$

Obs: no es necesario suponer $p(x)$ es irreducible. En tal caso, si $p(x) = f(x) \cdot g(x)$, basta construir un cpo de descomposición de $f(x)$, y sobre él un cpo de descomposición de $g(x)$.

Teo: Si $p(x) \in K[x]$, entonces:

1. Existe L cuerpo extensión de K ($K \subset L$) cuerpo de descomposición de $p(x)$.
2. El cuerpo L es único salvo isomorfismos.

Obs: Si K y L son cuerpos, $\varphi: K \to L$ morfismo, $N(\varphi) = \{0\}$, pues si $\varphi(a) = 0$, y $a \neq 0$,
$1 = \varphi(1) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = 0$ Abs!

Demo (Teo): podemos suponer $p(x)$ irreducible.

Existencia: $K_1 = K[X_1]/p(X_1)$ cuerpo que contiene a K.

En $K_1[Y]$ factorizo al polinomio $p(Y) = (Y - \overline{X_1}) \cdot P_2(Y) \cdots P_r(Y)$ (mónico, irred.)

Si todos los P_i son de grado 1, listo. Sino, tomo el primer factor de grado mayor que 1 (digamos $P_2(Y)$).

$$K_2 = K_1[X_2]/P_2(X_2)$$

En K_2, $P_2(Y) = (Y - \overline{X_2}) \cdot P_2^{(2)}(Y) \cdots P_2^{(r)}(Y)$, continúo.

Obs: supongamos que en K_2 P_2 se factoriza linealmente.

En el siguiente paso, debo factorizar $P_3(Y), \dots, P_n(Y)$ en k_2.

Unicidad: Sup. $p(x)$ irreducible, L_1, L_2 dos cpos de dex. de $p(x)$.

$$L_1 = k[\alpha_1, \alpha_2, \alpha_3] \overset{?}{\simeq} k[\beta_1, \beta_2, \beta_3] = L_2$$

$$k[\alpha_1] \simeq k[x]/p(x) \simeq k[\beta_1]$$

$$\alpha_1 \to \bar{x} \qquad \sigma_1 : k[\alpha_1] \xrightarrow{\sim} k[\beta_1]$$

$$k \to k$$

$$\alpha_1 \to \beta_1$$

$p(x)$ en $k[\alpha_1]$, $p(x) = (x-\alpha_1) \cdot P_2(x) \cdots P_r(x)$

$p(x)$ en $k[\beta_1]$, $p(x) = (x-\beta_1) \cdot \tilde{P}_2(x) \cdots \tilde{P}_r(x)$

$$\sigma_1 : k[\alpha_1] \xrightarrow{\sim} k[\beta_1] \overset{\text{induce}}{\rightsquigarrow} k[\alpha_1][x] \simeq k[\beta_1][x]$$

$$\sigma_1 \left(\sum a_i x^i \right) = \sum \sigma_1(a_i) x^i$$

$$p(x) = \sigma_1(p(x)) = (x-\beta_1) \cdot \sigma_1(P_2(x)) \cdots \sigma_1(P_r(x)) \text{ en } k[\beta_1][x]$$
$$= (x-\beta_1) \cdot \tilde{P}_2(x) \cdots \tilde{P}_r(x)$$

Puedo suponer que $\sigma(P_2(x)) = \tilde{P}_2(x)$. $(\operatorname{gr}(P_2) > 1)$

Si α_2 es raíz de $P_2(x)$ y β_2 es raíz de $\tilde{P}_2(x)$

$$\sigma_2 : k[\alpha_1, \alpha_2] \to k[\beta_1, \beta_2] \quad \text{que extiende a } \sigma_1$$
$$k \to k$$
$$\alpha_1 \to \beta_1$$

$\alpha_2 \longrightarrow \beta_2$

$$k[\alpha_1, \alpha_2] \simeq k[\alpha_1][x] / p_2(x) \overset{\sigma_1}{\simeq} k[\beta_1][x] / \tilde{p}_2(x) \simeq k[\beta_1, \beta_2]$$

σ_2

Continuamos indutivamente.