Repaso: K cuerpo, $p(x) \in K[x]$, construir un cuerpo L, $K \subset L$ $([L:K] < \infty)$ t.f.

- $p(x)$ tiene todas sus raíces en L ó
- $p(x)$ se factoriza linealmente en $L[x]$

y además

- $L = K[\alpha_1, \dots, \alpha_n]$ si las raíces de $p(x)$ son $\{\alpha_1, \dots, \alpha_n\}$

Def: un tal L se llama un cuerpo de descomposición de $p(x)$.

Ejemplos: 1. $p(x) = x^3 - 2$ irred en $\mathbb{Q}[x]$

$K_1 := \mathbb{Q}[x]/(x^3-2)$ ← $y^3 - 2$ en K_1 se factoriza como

$\mathbb{Q}$, $[3]$

$y^3 - 2 = (y - \bar{x})(y^2 + \bar{x}y + \bar{x}^2)$ (irred.)

$L = K_1[x_2]/(x_2^2 + \bar{x}x_2 + \bar{x}^2)$ $\quad [L:\mathbb{Q}] = 6$.

$[2]$

K_1

$[3]$

$\mathbb{Q}$

② Si $p(x) = x^3 + x^2 - 2x - 1$ en $\mathbb{Q}[x]$,

$K_1 := \mathbb{Q}[x]/(p(x))$. $\quad y^3 + y^2 - 2y - 1 = (y - \bar{x}) \cdot (y - (\bar{x}^2 - 2))$

$(y - (1 - \bar{x} - \bar{x}^2))$

$[3]$

$\mathbb{Q}$

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

1. Existe L cuerpo de descomposición de $p(x)$
2. L es "único", salvo isomorfismo (biyectivo, de anillos)

En concreto, si L_1 y L_2 son dos cpos de descomposición $\Rightarrow$ existe $\sigma: L_1 \to L_2$ isomorfismo de cuerpos t.q. $\sigma(k) = k \ \forall k \in K$ ($\sigma|_K = id$)

Def: Si L_1 y L_2 son extensiones de K ($K \subset L_1$, $K \subset L_2$), un K-morfismo es un morfismo de cuerpos $\sigma: L_1 \to L_2$ cuya restricción a K es la identidad.

Demo (Teo): **Existencia:** como en el ejemplo. $K_1 = K[x]/(p(x))$

Unicidad: por hip. L_1, L_2 dos cpos de desc. de K

$L_1 = K[\alpha_1, \dots, \alpha_n]$ ("polinomios"), $L_2 = K[\beta_1, \dots, \beta_n]$

Para Dar $\sigma: L_1 \to L_2$ basta definirla en α_i.

$K[\alpha_1] \simeq K[x]/(p(x)) \simeq K[\beta_1]$ ($\alpha_1 \to$ raíces)

i red. σ_1 $\qquad \sigma_1(\alpha_1) = \beta_1$

Miramos cómo se factoriza $p(x)$ en $K[\alpha_1][x]$

$p(x) = (x-\alpha_1) \cdot (p_2(x)) \cdots p_r(x)$

Mismo en $K[\beta_1][x]$, $p(x) = (x-\beta_1) \cdot (\tilde{p}_2(x)) \cdots \tilde{p}_n(x)$ $\quad \not\ni \sigma_1$

$$x \longrightarrow x$$

$$\sigma_1 : k[\alpha_1][x] \longrightarrow k[\beta_1][x]$$

$$\sigma_1(p(x)) = p(x) = (x-\beta_1)\cdot \tilde{p}_2(x) \cdots \tilde{p}_n(x)$$

$$(x-\beta_1)\cdot \sigma_1(p_2(x)) \cdots \sigma_1(p_r(x)) \Rightarrow \tilde{p}_2(x) = \sigma(p_2(x))$$

Extiendo σ_1: si α_2 raíz de $p_2(x)$,

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

Si β_2 es raíz de $\tilde{p}_2(x)$

Observaciones: si $p(x)$ es irreducible, L es un cpo de descomposición de $p(x) \Rightarrow [L:k] \leq d!$

$$k \overset{d}{\subset} k[x_1]/p_1(x) \overset{d-1}{\subset} k_1[x_2]/p_1(x) \subset \cdots$$

$p(x) = (x-\bar{x}_1)\cdot \underbrace{\text{irred}}_{p_1(x)}$, $d = gr(p(x))$

Ejemplo 1 vale $=$, ejemplo 2 no

Ejemplo: $\mathbb{F}_p[t]$ anillo de polinomios $\rightsquigarrow$ cuerpo de fracciones de $\mathbb{F}_p[t] = \mathbb{F}_p(t) = K = \left\{ \frac{p(t)}{q(t)} : p(t), q(t) \in \mathbb{F}_p[t], q \neq 0 \right\}/\sim$

$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$. cuerpo.

$p(x) = x^p - t \in K[x]$, irreducible (Eisenstein).

($p \in \mathbb{Z}$ primo, $q(x) = a_n x^n + \cdots + a_1 x + a_0$, $p \nmid a_n$, $p \mid a_i$ $\forall\, 0 \leq i \leq n-1$

y $p^2 \nmid a_0 \Rightarrow g(x)$ es irreducible). x^3+2 irred.

(t) es primo en $\mathbb{F}_p[t]$, pues $\mathbb{F}_p[t]/(t) \simeq \mathbb{F}_p$ cpo.

Aplico criterio de Eisenstein con (t).

¿Quién es el cpo de descomposición de $\underline{x^p - t}$?

$$L = K[x]/(x^p - t), \quad y^p - t \overset{\text{en } L}{=} (y - \bar{x})^p$$

Demo: $(a+b)^p \overset{\text{Newton}}{=} a^p + \binom{p}{1}a^{p-1}b^1 + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$

$p \mid \binom{p}{1}$, $p \mid \binom{p}{2}$, $p \mid \binom{p}{p-1}$

$\Rightarrow (a+b)^p = a^p + b^p$ si $\mathrm{car}(K) = p$.

$[(ab)^p = a^p \cdot b^p]$ ↑ siempre.

En $\mathbb{F}_p(t)$ hay polinomios irreducibles con una única raíz repetida

Def: un polinomio $p(x) \in K[x]$ se dice **separable** si ningún factor irreducible de él admite raíces múltiples (en un cuerpo de descomposición).

Prop: si $p(x) \in K[x]$ irreducible y no constante. Son equivalentes:

1. $p(x)$ tiene alguna raíz repetida.
2. $\mathrm{car}(K) = p$ y existe $g(x) \in K[x]$ t.q. $p(x) = g(x^p)$
3. $p(x)$ tiene todas sus raíces repetidas.

Demo: $3 \Rightarrow 1$ ✓

$2. \Rightarrow 3.$ $g(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ en un cpo de desc.

de $g(x) \Rightarrow P(x) = g(x^p) = (x^p - a_1) \cdot \ldots \cdot (x^p - a_n)$

K_1 $= (x - \sqrt[p]{a_1})^p \cdots (x - \sqrt[p]{a_n})^p$

1. $\Rightarrow$ 2. $p'(x) \in K[x] \longrightarrow p'(x) = 0$

$\rightarrow$ $p'(x) \neq 0$, $\quad gr(p'(x)) < gr(p(x))$

Obs: si a es raíz múltiple de $p(x) \Rightarrow p'(a) = 0$. pues

$(x-a)^2 \mid p(x) \Rightarrow p(x) = (x-a)^2 h(x)$.

$p'(x) = 2(x-a)h(x) + (x-a)^2 h'(x)$

$p'(a) = 0 + 0 = 0$.

en a

$mcd(p(x), p'(x)) = p(x) \cdot q(x) + p'(x) \cdot b(x)$

Luego, $mcd(p(x), p'(x))(a) = 0$

$mcd(p(x), p'(x)) \mid p(x)$, como $p(x)$ es irr.

debe, $mcd(p(x), p'(x)) = 1$ Absurdo

Luego, $p'(x) = 0$. $\quad p(x) = a_n x^n + \cdots + a_1 x + a_0$, $\quad n \geq 1$.

$p'(x) = n \cdot a_n x^{n-1} + \cdots + a_1 = 0$

$\Rightarrow car(K) \neq 0$, $(p \nmid n)$, además, $p(x) = \sum a_i x^i$

$p'(x) = \sum i a_i x^{i-1}$

$p'(x) = 0 \Rightarrow p \mid i \cdot a_i \ \forall i \rightarrow$ si $a_i \neq 0$, $p \mid i$

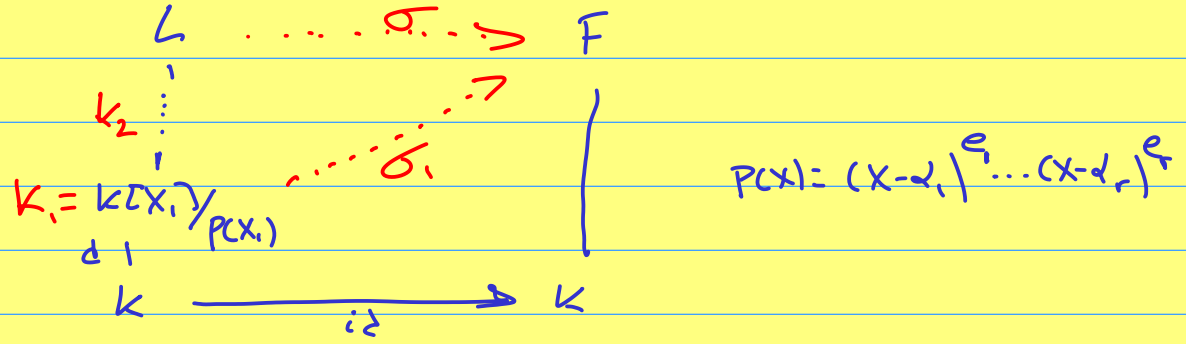
$\Updownarrow$

si $p \nmid i$, $a_i = 0$. ∎

Obs: si $car(K) = 0$, todos los polinomios son separables.

Lema: Si $p(x) \in k[x]$ irreducible, L el cuerpo de descomposición de $p(x)$ y F un cuerpo donde $p(x)$ se factoriza linealmente.
Entonces $\#\{\sigma: L \to F,\ k\text{-morfismo}\} \leq [L:k]$
y vale la igualdad $\Leftrightarrow$ $p(x)$ es separable.

Demo: Por construcción de L:



Si $\sigma_1 : k_1 \to F$, k-morfismo, basta decir donde va a parar $\bar{X}_1$ y $\sigma_1(\bar{X}_1) = \alpha_i$, $1 \leq i \leq r$

$\Rightarrow \#\{\sigma_1 : k_1 \to F\} = \#\{\text{raíces de } p(X)\} \leq gr(p(x))$

Sigue inductivamente, o sea $p(X) = (X - \bar{X}_1) P_2(X) \cdots P_r(X)$ en $k_1[X]$.

Elegimos el siguiente factor irreducible, $k_2 = k_1[X_2]/P_2(X)$

Para extender σ_1, basta definir donde va $\bar{X}_2$, raíz de $P_2(X)$ en F. ∎

Obs: Si $F = L$ (cpo de descomposición $p(X)$), $[L:k] < \infty$.

$$Aut_k(L) = \{\sigma: L \to L \quad k\text{-morfismo}\}$$

(morfismo de cuerpos $\Rightarrow$ σ inyectiva $\Rightarrow$ suryectiva)

$\# Aut_k(L) \leq [L:k]$ y es un igual $\Leftrightarrow$ $p(x)$ es separable.

Lema: $Aut_K(L)$ es un grupo con la composición. ($\sigma \cdot \tau = \sigma \circ \tau$)

D/ Veamos que la operación está bien definida:

$\sigma, \tau \in Aut_K(L) \Rightarrow \sigma \circ \tau \in Aut_K(L)$

- $\sigma \circ \tau$ es morfismo de anillos $(\sigma(\tau(a+b)) = \sigma(\tau(a)+\tau(b)) = \sigma(\tau(a)) + \sigma(\tau(b)))$.
- $(\sigma \circ \tau)(k) = \sigma(\tau(k)) = \sigma(k) = k$ ✓

Grupo:
- Asociativa ✓
- Neutro: id_L, $id(a) = a$.
- Inverso: σ, biyectiva, $\sigma^{-1}: L \to L$ ✓

(ver que σ^{-1} es morfismo).

Obs: Si L cpo de descomposición de $p(x)$, d raíces distintas.

$$\sigma \in Aut_K(L), \quad L = K[\alpha_1, \dots, \alpha_d] \longrightarrow L$$

Por ser σ morfismo de cuerpos, queda unívocamente determinado por $\sigma(\alpha_i) \in \{\alpha_1, \dots, \alpha_d\}$

$$\sigma \rightsquigarrow S_d = \{\text{permutaciones de los números } \{1, \dots, d\}\}$$
$$= \{f: \{1, \dots, d\} \to \{1, \dots, d\} \text{ biyectivas}\}.$$

$\sigma \longrightarrow f(i) = j$ si $\sigma(\alpha_i) = \alpha_j$. ↑ grupo con la composición.

$$Aut_K(L) \hookrightarrow S_d.$$

Ejemplos: 1. $K = \mathbb{Q}$, $p(x) = x^3 - 2$, L = cpo de descomposición.

$$Aut_{\mathbb{Q}}(L) < S_3 \qquad Aut_{\mathbb{Q}}(L) = S_3.$$

↑ $\{L : \mathbb{Q}\} = 6$ ↑ 6 elementos

$L = k_1[x]/(x^2+\sqrt[3]{2}x+\sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi_3) = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$

$k_1 = \mathbb{Q}[x]/(x^3-2) = \mathbb{Q}(\sqrt[3]{2})$

$\mathbb{Q}$

$x^3-1 = (x-1)(x^2+x+1)$

$\xi_3^3 = 1$

$\vdots$

$-1, \frac{1 \pm \sqrt{-3}}{2}$

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

$\sqrt[3]{2} \to \sqrt[3]{2}\xi_3$

$\to \sqrt[3]{2}\xi_3^2$

$\sigma \in Aut_{\mathbb{Q}}(L)$, $\sigma(\sqrt[3]{2}) = ?$

$\sigma(\xi_3) = ?$

$\xi_3 \to \xi_3$

$\to \xi_3^2$

Estos son los 6 elts de $Aut_{\mathbb{Q}}(L)$

$\sigma: \sqrt[3]{2} \to ?$ ejercicio σ como elto de S_3

$\xi_3 \to ?$

$\sigma(\sqrt[3]{2}) = \xi_3\sqrt[3]{2}$

$\sigma(\xi_3) = \xi_3^2$

$(\sqrt[3]{2}, \sqrt[3]{2}\xi_3, \sqrt[3]{2}\xi_3^2)$

$\downarrow \sigma$

$(\xi_3\sqrt[3]{2}, \xi_3\sqrt[3]{2}\cdot\xi_3^2, \xi_3\sqrt[3]{2}\cdot\xi_3^4)$

$\vdots$

$(\xi_3\sqrt[3]{2}, \sqrt[3]{2}, \xi_3^2\sqrt[3]{2})$

$1 \to 2$

$2 \to 1$ $\boxed{(12)}$

$3 \to 3$

(2) $p(x) = x^3 + x^2 - 2x - 1$, $\# Aut_{\mathbb{Q}}(L) = 3$

$\mathbb{Z}/3 = Aut_{\mathbb{Q}}(L) < S_3$ $\boxed{(123)}$

Def: Si H es un subgrupo de $Aut_K(L)$ (L cpo de desc.) $p(x)$ separable.

$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in H\} \supset K$

Teo: (Galois) Si $K \subset L$ finita y "buena", existe una biyección entre:

$\{k \subset F \subset L\}$ $\xleftrightarrow{\text{biyectiva}}$ $\{H \text{ subgrupos de } Aut_k(L)\}$

extensiones intermedias

$F \longrightarrow Aut_F(L) = \{\sigma : L \to L : \sigma|_F = id\}$

$L^H \longleftarrow H$

$Gal(L/k) = Aut_k(L)$