Recordar: $Gal\begin{bmatrix} L \\ | \\ F \\ | \\ K \end{bmatrix} Gal$) depende ✓ normal y separable

Teo: (Galois) L/K Galois, hay una biyección entre

$$\{K \subset F \subset L\} \longleftrightarrow H < Gal(L/K) = Aut_K(L)$$

$$F \longrightarrow Aut_F(L)$$

$$L^H \longleftarrow H$$

Además, L^H/K es Galois $\Leftrightarrow$ H es un subgrupo normal de $Gal(L/K)$

Recordar: 1. L/K separable si $\alpha \in L$, $m_\alpha(x)$ tiene todas sus raíces distintas.

2. L/K es normal si $p(x) \in K[x]$ irreducible t.q. tiene una raíz en $L \Rightarrow$ tiene todas.

(L = cuerpo de descomposición $p(x) \in K[x]$)

3. G grupo, H subgrupo. H se dice normal si cumple que para todo $g \in G$, $gHg^{-1} = \{ghg^{-1} : h \in H\} = H$.

Ejemplo: 1. $G = S_3$, $H = \langle (12) \rangle = \{id, (12)\}$

$1 \to 2$, $2 \to 1$, $3 \to 3$

H no es normal, $(13) \in G$

$1 \to 3$, $2 \to 2$, $3 \to 1$

$(13)(12)(13) = (123)$: $1 \to 3$, $2 \to 3$, $3 \to 2$ $\notin H$

2. $G = S_3$, $H = \langle (123) \rangle = \{id, (123), (132)\}$

$1 \to 2$, $2 \to 3$, $3 \to 1$

$1 \to 3$, $2 \to 1$, $3 \to 2$

H es normal $\quad gHg^{-1} = H \ \forall g \in G$

Obs: si $g \in H$ (orden 2), $gHg^{-1} = H$ (orden 3)

$S_3 = \langle (12), (123) \rangle$, luego basta ver que

$(12)\, H\, (12) = H$ $\qquad (12)(123)(12) = (132) \in H$

$(12)(132)(12) = (123) \in H$ ✓

Demo (Teo) biyección clase pasada.

Tomemos $\sigma \in Gal(L/k)$, H subgrupo de $Gal(L/k)$,

Afirmo: $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$ $\qquad \sigma^{-1}H\sigma$ es otro subgrupo de $Gal(L/k)$

Ejercicio: ver que $\sigma^{-1}H\sigma$ es subgrupo.

Demo (afirmación) $\subseteq$) $\beta \in \sigma(L^H)$, o sea $\exists \alpha \in L^H =$

$\{ \gamma \in L : \tau(\gamma) = \gamma \ \forall \tau \in H \}$ y $\beta = \sigma(\alpha)$

q.v.q. $\beta \in L^{\sigma H \sigma^{-1}} \iff \sigma \tau \sigma^{-1}(\beta) = \beta \ \forall \tau \in H$

$\beta = \sigma(\alpha)$ $\qquad \sigma \tau \sigma^{-1}(\sigma(\alpha)) = \sigma(\alpha)$ ✓

$\sigma \tau(\alpha)$

$\sigma(\alpha)$ porque $\alpha \in L^H$

$\supseteq$) $\beta \in L^{\sigma H \sigma^{-1}}$, q.v.q. $\sigma^{-1}(\beta) \in L^H \iff \tau\sigma^{-1}(\beta) = \sigma^{-1}(\beta)$

$\forall \tau \in H \iff \sigma \tau \sigma^{-1}(\beta) = \beta \ \forall \tau \in H$ ✓

El teo dice L^H normal $\iff$ H es subgrupo normal

L^H es normal $\Leftrightarrow \sigma \in Gal(L/K)$, $\sigma(L^H) = L^H$

($L^{\sigma H \sigma^{-1}}$)

$\Leftrightarrow \sigma H \sigma^{-1} = H \quad \forall \sigma \in Gal(L/K)$ ($\Leftrightarrow$ H subgrupo normal ☑)

Ejemplo: $K = \mathbb{Q}$, $p(x) = x^3 - 2$, L = cpo desc. $= \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi_3)$
$= \mathbb{Q}(\xi_3, \sqrt[3]{2})$

$Gal(L/\mathbb{Q}) = S_3$

Subgrupos:
- $\{id\}$
- $\langle (12) \rangle$, $\langle (13) \rangle$, $\langle (23) \rangle$ (orden 2)
- $\langle (123) \rangle$ (orden 3)
- S_3

Subgrupo	$\{id\}$	$\langle (12) \rangle$	$\langle (13) \rangle$	$\langle (23) \rangle$
Extensión	L	$\mathbb{Q}(\sqrt[3]{2}\xi_3^2)$	$\mathbb{Q}(\sqrt[3]{2}\xi_3)$	$\mathbb{Q}(\sqrt[3]{2})$

no Galois/$\mathbb{Q}$

$\langle (123) \rangle$	S_3
$\mathbb{Q}(\xi_3)$	$\mathbb{Q}$
2:1 Galois	
$\mathbb{Q}$	

$x^3 - 2$ ~raíces~ $\{\sqrt[3]{2}, \sqrt[3]{2}\xi_3, \sqrt[3]{2}\xi_3^2\}$

(12): $\sqrt[3]{2} \to \sqrt[3]{2}\xi_3$
$\sqrt[3]{2}\xi_3 \to \sqrt[3]{2}$
$\sqrt[3]{2}\xi_3^2 \to \sqrt[3]{2}\xi_3^2$

(123): $\sqrt[3]{2} \to \sqrt[3]{2}\xi_3$
$\sqrt[3]{2}\xi_3 \to \sqrt[3]{2}\xi_3^2$
$\sqrt[3]{2}\xi_3^2 \to \sqrt[3]{2}$

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

$[\mathbb{Q}(\xi_3) : \mathbb{Q}] = 2$ $\quad x^3 - 1 = (x-1)(\underbrace{x^2 + x + 1}_{\text{irred.}})$

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

Obs: $F \longrightarrow Aut_F(L) \qquad [L:L^H] = \#H$
$L^H \longleftarrow H$

Ejercicio: hacer lo mismo para el otro ejemplo.

Cuerpos finitos

Recordemos: K es un cuerpo finito $\Rightarrow \exists p$ primo t.q. $\mathbb{F}_p = \mathbb{Z}/p \hookrightarrow K \Rightarrow \#K = p^n$ (ejercicio).

Pregunta: dado $d \in \mathbb{N}$, ¿existe un cuerpo con p^d elts? (Sí)
¿cuántos hay? uno solo salvo isomorfismos.

Ejemplo: $p=2$, x^2+x+1 es irreducible $\Rightarrow \mathbb{F}_2[X]/_{X^2+x+1} = \mathbb{F}_4$
2^1
$\mathbb{F}_2$

Teo: Si $d \in \mathbb{N}$, p primo, $\exists K$ cuerpo con p^d elts. Además, K es único salvo isomorfismos. ($K = \mathbb{F}_{p^d}$)

Demo: $f(x) = X^{p^d} - X \in \mathbb{F}_p[X]$, sea K un cuerpo de descomposición de $f(x)$.

Obs: 1°. $f(x)$ es simple, $f'(x) = -1$, no hay raíces comunes de f y su derivado.

$K = \mathbb{F}_p[\alpha_1, \dots \alpha_{p^d}]$.

igualdad.
↓
$S = \{ \alpha_1, \ldots, \alpha_{p^d} \} \subset K$

<u>Pues</u>: (1º) $\mathbb{F}_p \in S$, $\alpha \in \mathbb{F}_p$, $\alpha^p = \alpha \Rightarrow \alpha^{p^2} = \alpha^p = \alpha$

$\ldots \Rightarrow \alpha^{p^d} = \alpha \Rightarrow \alpha^{p^d} - \alpha = 0$ ✓

(2º) Si α, β raíces $\Rightarrow \alpha+\beta$ es raíz.

$(\alpha+\beta)^p = \alpha^p + \beta^p$, $(\alpha+\beta)^{p^2} = \alpha^{p^2} + \beta^{p^2} \ldots$

$(\alpha+\beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} \Rightarrow (\alpha+\beta)^{p^d} - (\alpha+\beta) =$

$= \underbrace{\alpha^{p^d} - \alpha}_{\overset{\shortparallel}{0}} + \underbrace{\beta^{p^d} - \beta}_{\overset{\shortparallel}{0}} = 0$

(3º) Si α, β raíces $\Rightarrow \alpha \cdot \beta$ es raíz.

$(\alpha\beta)^{p^d} - \alpha\beta = \alpha^{p^d}\beta^{p^d} - \alpha\beta = \alpha^{p^d}\beta^{p^d} - \alpha\beta^{p^d} +$

$\alpha\beta^{p^d} - \alpha\beta = \beta^{p^d}(\underbrace{\alpha^{p^d} - \alpha}_{0}) + \alpha(\underbrace{\beta^{p^d} - \beta}_{0}) = 0.$

$\Rightarrow \underset{\overset{\shortparallel}{K}}{\mathbb{F}_p[\alpha_1, \ldots, \alpha_{p^d}]} \subset S \subset K \Rightarrow \boxed{S = K}$

Luego $\# K = p^d$. ∎

$K = \mathbb{F}_p[x]/\varphi(x)$
$\big|\, d$ ← ¿quién es? (irred. de grado d).
$\mathbb{F}_p$

Por construcción raíz de $X^{p^d} - X$

$p = 101$, $d = 3$ ⇝ factorizar un polinomio de grado 101^3

<u>Pregunta</u>: ¿Cuándo $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$?

Lema: $\mcd(X^n-1 : X^m-1) = X^{\mcd(n,m)} - 1$

Demo: Supongamos $n \geq m$, $n = m \cdot q_1 + r_1$

$$X^n - 1 - (X^m-1)X^{n-m} = X^{n-m} - 1 - (X^m-1)X^{n-2m}$$

$$X^n - 1 - (X^m-1)\cdot(X^{n-m} + X^{n-2m} + \cdots + X^{n-q_1 m}) = X^{n-2m} - 1$$

$$= X^{r_1} - 1.$$

Por propiedades del mcd $\mcd(X^n-1, X^m-1) = \mcd(X^{r_1}-1, X^m-1)$

$$= \mcd(X^{r_1}-1, X^{r_2}-1) \cdots = \mcd(X^{\mcd(m,n)}-1, X^0-1)$$

$m = r_1 q_1 + r_2$

$$= X^{\mcd(m,n)} - 1 \quad \square$$

Corolario: $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n \mid m$.

D/($\Leftarrow$) si $n \mid m$, $X^{p^n} - X \mid X^{p^m} - X$

$$X(X^{p^n-1} - 1) \mid X(X^{p^m-1} - 1)$$

$$\mcd(p^n-1, p^m-1) = p^{\mcd(n,m)} - 1 = p^n - 1$$

$$p^n - 1 \mid p^m - 1 \Rightarrow X^{p^n-1} - 1 \mid X^{p^m-1} - 1 \quad (\text{Lema})$$

Luego $\mathbb{F}_{p^m}$ cpo de descomposición de $X^{p^m} - X$, contiene al cpo de descomposición de $X^{p^n} - X$. ✓

$\Rightarrow \mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, luego $X^{p^n} - X$ tiene todas las raíces

en $\mathbb{F}_{p^m} = \{\text{raíces de } X^{p^m} - X\} \Rightarrow$

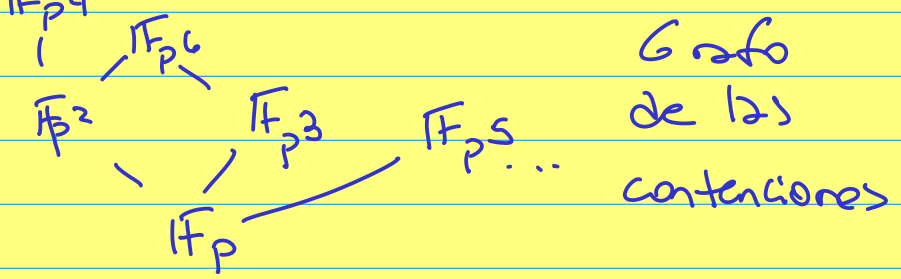
$\{\text{raíces } X^{p^n} - X\} \subset \{\text{raíces de } X^{p^m} - X\}$

$\Rightarrow X^{p^n} - X \mid X^{p^m} - X$ (en $\mathbb{F}_{p^m}$ ambos se factorizan como producto de polinomios de grado 1).

Luego, $(X^{p^n-1} - 1 : X^{p^m-1} - 1) = X^{p^{mcd(n,m)}-1} - 1$

$\Rightarrow p^n - 1 \mid p^m - 1$

$\Rightarrow n \mid m$ ☐



Grafo de las contenciones

Obs: Si $\varphi(x) \in \mathbb{F}_p[X]$ irreducible de grado d,

entonces $\mathbb{F}_p[x]/\varphi(x) \simeq \mathbb{F}_{p^d} \Rightarrow \bar{X}^{p^d} - \bar{X} = 0$

$\Rightarrow p(x) \mid X^{p^d} - X \Rightarrow$ todos aparecen como factores de $X^{p^d} - X$ (problema: tiene grado muy grande)

Problema: dar un algoritmo efectivo para dado p, d hallar un polinomio de grado d en $\mathbb{F}_p[X]$ irreducible.

Obs: Si K tiene p^d elementos, la función

$$\begin{array}{ccc} K & \longrightarrow & K \\ x & \longrightarrow & x^p \end{array}$$

es un morfismo biyectivo

que se llama el automorfismo de Frobenius ($Frob_p$)

biyectivo: $\longrightarrow$ todo morfismo de cuerpos es inyectivo (como K finito biyectivo)

$N_{-}(f) := \{ \alpha : \alpha^p = 1 \}$

raíces de $X^p - 1 = (X-1)^p$, una única raíz, el 1.

$Aut_{\mathbb{F}_p}(\mathbb{F}_{p^d}) \supset \{Frob_p\}$, $(Frob_p)^d : x \to x^{p^d}$

$(Frob_p)^d = id$ (en K, $x^{p^d} = x$)

Ninguna potencia más chica es la identidad, o sea si

$(Frob_p)^r = id \Rightarrow \{ \alpha^{p^r} - \alpha = 0 \ \forall \alpha \in K \}$

$\Rightarrow K \subset \{$raíces de $X^{p^r} - X\}$ $\Rightarrow r \geq d$

K: p^d ellos; $X^{p^r} - X$: tiene p^r ellos

$\Rightarrow \# \langle Frob_p \rangle = d = [K : \mathbb{F}_p] \Rightarrow Aut_{\mathbb{F}_p}(K) = \langle Frob_p \rangle$

y tiene orden $d = [K : \mathbb{F}_p]$. $\Rightarrow [K : \mathbb{F}_p]$ Galois.

y $Gal(K/\mathbb{F}_p) \simeq \mathbb{Z}/d\mathbb{Z}$.

Recordar: Galois $\begin{cases} L \\ | \\ F \\ | \\ K \end{cases}$ Galois $F = L^H$ Galois $\Leftrightarrow H \triangleleft Gal(L/K)$ normal

$gHg^{-1} = H$, pero si $Gal(L/K)$ es abeliano

↑ vale siempre

Luego si K, L son cuerpos finitos, $K \subset L$, la extensión $\begin{cases} L \\ | \\ K \\ | \\ \mathbb{F}_p \end{cases}$ Galois, $Gal(L/\mathbb{F}_p)$ cíclico ($\Rightarrow$ abeliano)

$\Rightarrow L/K$ es Galois y $Gal(L/K)$ es cíclico.

Ejercicio: si K tiene p^n elementos, $Gal(L/K) = \langle \text{Frob}_p^n \rangle$

Teo: si K es un cuerpo finito, el grupo multiplicativo de K, $(K \setminus \{0\}, \cdot)$ (producto) $= K^\times$ es cíclico.

Demo: por el Teo de estructura, $K^\times \simeq \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$ $(q_1, \ldots, q_r)$

donde $d_1 | d_2 | \cdots | d_r$. Luego todo elemento de $K^\times$ elevado a d_r da 1, $\alpha \in K^\times$, $\alpha^{d_r} = 1$. (todos salvo el 0.)

Luego, $\alpha^{d_r+1} - \alpha = 0$. ↑ para todo $\alpha \in K$

Luego $K \subset \{$raíces de $X^{d_r+1} - X\}$

↑ p^d elts ↑ d_r+1 elts $\Rightarrow p^d \leq d_r + 1$

$p^d - 1 \leq d_r$

y • $d_1 \cdot \ldots \cdot d_r = p^d - 1$ $\Rightarrow \boxed{d_r = p^d - 1}$

↳ $d_r \leq p^d - 1$

□

Cor: dado $d \in \mathbb{N}$, p primo, $\exists\, f(x) \in \mathbb{F}_p[x]$ irred. de grado d.

D/ $\mathbb{F}_{p^d}$, α un generador de $\mathbb{F}_{p^d}^{\times}$

$\Rightarrow \mathbb{F}_p\alpha = \mathbb{F}_p[\alpha]$, $m_\alpha(x) \in \mathbb{F}_p[x]$,

$\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x] / m_\alpha(x)$ $\Rightarrow gr(m_\alpha(x)) = d$.

d | $\mathbb{F}_p$

□

Además, $\mathbb{F}_{p^d}$ es monógena ($\mathbb{F}_p\alpha = \mathbb{F}_p[\alpha]$)