Repaso: $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = L$

$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$

$\mathbb{Q}$

$p \in \mathbb{Z}$ primo, $p \cdot \mathcal{O}_L =$
- $\mathfrak{P}_1 \cdot \mathfrak{P}_2$, $f = 2$, $D(\mathfrak{P}_i | p) = \mathbb{Z}/2$
- ⊛ $\mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3 \cdot \mathfrak{P}_4$, $D(\mathfrak{P}_i | p) = 3$, $f = 1$

no ramificado.

Ejemplo: $\mathbb{Q}(\sqrt{3}, \sqrt{7})$

$\mathbb{Q}(\sqrt{3}, \sqrt{7})$

$\mathbb{Q}(\sqrt{7})$ $\quad$ $\mathbb{Q}(\sqrt{3})$

$\mathbb{Q}$

p se parte $\Leftrightarrow \left(\frac{3}{p}\right) = 1$

se parte $\Leftrightarrow \left(\frac{7}{p}\right) = 1$

Cota	1000	...	10^6
# p	166		78496
⊛ # partes	35		19536
·1.	21,08		24,91 $\sim 1/4$

$|D(\mathfrak{P}_i | p)| = 1$

$\#\mathrm{Gal}(L/\mathbb{Q}) = 4$

Ejemplo 2: $K = \mathbb{Q}$, $L = \mathbb{Q}[x]/(x^3 - x + 2) = f(x)$

$p \in \mathbb{Z}$ no ramificado, $p \cdot \mathcal{O}_L =$
- $\mathfrak{P}$ primo $f(\mathfrak{P}|p) = 1, 2$
- $\mathfrak{P}_1 \cdot \mathfrak{P}_2$
- $\mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3$

$\mathrm{disc}(K) = -2^3 \cdot 13$

$\rightsquigarrow$ $L/\mathbb{Q}$ no es Galois.

Cota	1000	10.000
[#1, #2, #3]	[61, 81, 24]	.. -
%	[36,74%, 48,78%, 14,45%]	33%, 50%, 16%.

$\rightsquigarrow$ ¿[1/3, 1/2, 1/6]? (3) (2) (1) Obs: ¿cómo si L/K no es Galois?

$$6 \begin{cases} \mathcal{O}_f \quad p\cdot\mathcal{O}_{\mathcal{O}_f} = \mathfrak{P}_1\cdots\mathfrak{P}_3 & \mathrm{Gal}(\mathcal{O}_{\mathcal{O}_f}/\mathcal{O}) \simeq S_3 \\ \quad 2\,|\,1 \\ \quad\ \mathcal{O}_2 \quad p\cdot\mathcal{O}_2 = \mathfrak{P}_1\cdots\mathfrak{P}_r \\ \quad 3\,|\,1 \\ \quad\ \mathcal{O} \quad p \end{cases} \qquad p\cdot\mathcal{O}_{\mathcal{O}_f} = \begin{cases} \mathfrak{P}_1\cdots\mathfrak{P}_6 & f=1 \\ \mathfrak{P}_1\cdots\mathfrak{P}_3 & f=2 \\ \mathfrak{P}_1\cdot\mathfrak{P}_2 & f=3 \end{cases}$$

↑ no ramificado

Si L/K Galois

$e\cdot f\cdot r = [L:K] \Rightarrow f = 1, 2, 3, \cancel{6}$

↑ $\mathfrak{P}\,|\,p$, $p\cdot\mathcal{O} = P$

$D(\mathfrak{P}|p) \rightsquigarrow \mathrm{Gal}\left(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p\right)$

$\mathbb{F}_p = (\mathcal{O}/\mathfrak{P})$ $\quad \mathrm{Gal}(\mathcal{O}_f/\mathcal{O}) \simeq S_3$ $\quad$ cíclico, de orden f

$f=1,\ D(\mathfrak{P}_i|p) = \{id\}$ $\quad id. \rightarrow 1/6$

$f=2,\ D(\mathfrak{P}_i|p) = \mathbb{Z}/2$ ← 2-ciclo $\quad (12)(13)(23) \rightarrow 3/6 = 1/2$

$f=3,\ D(\mathfrak{P}_i|p) = \mathbb{Z}/3$ ← 3-ciclo $\quad (123)(132) \rightarrow 2/6 = 1/3$

Pregunta: ¿conocer la factorización en $\mathcal{O}_f/\mathcal{O}$, qué nos dice sobre la factorización en $L/\mathcal{O}$?

(1) Si $f=1$ (en $\mathcal{O}_f/\mathcal{O}$), $f(\mathfrak{P}_i|p) = 1\ \forall\, \mathfrak{P}_i \subset \mathcal{O}_L$

$$3 = \sum_{i=1}^{r} \overbrace{e(\mathfrak{P}_i|p)}^{1}\overbrace{f(\mathfrak{P}_i|p)}^{1} \Rightarrow (r=3) \leftarrow$$

$D(\mathfrak{P}_1|p)$ $D(\mathfrak{P}_2|p)$ $D(\mathfrak{P}_3|p)$ $H < Gal(L/\mathbb{Q})$

(12) (13) (23) (12)

(2) $f=2$, $p\cdot\mathcal{O}_L = \mathfrak{P}_1\cdot\mathfrak{P}_2\cdot\mathfrak{P}_3$, $Gal(\mathcal{O}_f/L) \simeq \mathbb{Z}/2$

Luego, $Gal(\mathcal{O}_f/L) = D(\mathfrak{P}_1|p)$ (abuso, digamos $\mathfrak{P}_1$)

$\mathfrak{P}_1 \cap L = \mathfrak{Q}_1$.

$D(\mathfrak{P}_1|\mathfrak{Q}_1) = \{\sigma \in Gal(\mathcal{O}_f/L) : \sigma(\mathfrak{P}_1) = \mathfrak{P}_1\} = D(\mathfrak{P}_1|p) \cap H$ ($\sigma \in D(\mathfrak{P}_1|p)$; $\langle(12)\rangle$, H, $\langle(12)\rangle$)

$= H = Gal(\mathcal{O}_f/L) \rightsquigarrow \#D(\mathfrak{P}_1|\mathfrak{Q}_1) = 2$

$\langle(13)\rangle$ $\langle(12)\rangle$

$D(\mathfrak{P}_2|\mathfrak{Q}_2) = D(\mathfrak{P}_2|p) \cap H = \{id\} \Rightarrow \#D(\mathfrak{P}_2|\mathfrak{Q}_2) = 1$

$\mathfrak{P}_2 \cap L$ $f(\mathfrak{P}_2|\mathfrak{Q}_2)$

$\cdot\ D(\mathfrak{P}_3|\mathfrak{Q}_3) = \{id\} \rightsquigarrow p\cdot\mathcal{O}_L = \mathfrak{Q}_1\cdot\mathfrak{Q}_2$

$p\cdot\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ $f(\mathfrak{P}_1|\mathfrak{Q}_1) = 2 \Rightarrow f(\mathfrak{Q}_1|p) = 1$

$2\ 1\ 1/1$ $f(\mathfrak{P}_2|\mathfrak{Q}_2) = 1 \Rightarrow f(\mathfrak{Q}_2|p) = 2$

$p\cdot\mathcal{O}_L = \mathfrak{Q}_1\cdot\mathfrak{Q}_2$ (2) $\mathfrak{P}_2 \cap \mathcal{O}_L = \mathfrak{P}_3 \cap \mathcal{O}_L$

$2\ 1/2$

$p\cdot\mathbb{Z}$ p

(3) $f=3$, $p\cdot\mathcal{O}_L = \mathfrak{P}_1\cdot\mathfrak{P}_2$ $D(\mathfrak{P}_1|p) = \langle(123)\rangle$

$D(\mathfrak{P}_2|p) = \langle(132)\rangle$

$\mathfrak{Q}_i = \mathfrak{P}_i \cap \mathcal{O}_L$, $D(\mathfrak{P}_i|\mathfrak{Q}_i) = \langle(123)\rangle \cap \langle(12)\rangle = \{id\}$

$\rightsquigarrow f(\mathfrak{Q}_i|p) = 3 \Rightarrow$ $p\cdot\mathcal{O}_L$ es primo. (3)

Idea de por qué funcionan estas cuentas

Supongamos L/K Galois, $\mathfrak{P} \subset \mathcal{O}_L$ no ramificado en L/K.

Si $\mathfrak{Q} \subset \mathcal{O}_K$, $\mathfrak{Q} | \mathfrak{P}$,

ext. de cpos finitos

$D(\mathfrak{Q}|\mathfrak{P}) \xrightarrow[\varphi]{\sim} Gal(\mathbb{F}_{\mathfrak{Q}}/\mathbb{F}_{\mathfrak{P}})$

$Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ no sólo es cíclica, sino que tiene un generador canónico, $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle Frob_q \rangle$

$$x \longrightarrow x^{N(\mathfrak{p})} \quad \text{en } \mathbb{F}_{q^n}.$$

En particular, $\exists\, \sigma \in D(\mathfrak{P}|\mathfrak{p}) \mid \varphi(\sigma) = Frob_q$ (↑ $Frob_{\mathfrak{p}}$)

Caracterizado: $Frob_{\mathfrak{p}}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_L$

⇝ Ejercicio: Si $\mathfrak{P}_2 | \mathfrak{p} \Rightarrow Frob_{\mathfrak{P}_2} = \sigma\, Frob_{\mathfrak{P}}\, \sigma^{-1}$, donde $\sigma \in Gal(L/K)$, $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

Obs: Si L/K es abeliana, $Frob_{\mathfrak{P}} = Frob_{\mathfrak{P}_2} \longrightarrow Frob_{\mathfrak{p}}$ tiene sentido. ψ : {ideales no ramif. de K} $\longrightarrow Gal(L/K)$, $\mathfrak{p} \longrightarrow Frob_{\mathfrak{p}}$ (mapa de Artin) morfismo de grupos.

Si L/K no es abeliano,

$$\psi : \left\{ \begin{array}{l} \text{ideales primos} \\ \text{de } K \text{ no ramif. en } L \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{clases de conjug.} \\ \text{ción de } Gal(L/K) \end{array} \right\}$$

$$\mathfrak{p} \rightsquigarrow \left[Frob_{\mathfrak{P}} \right] \qquad (\uparrow\, Gal(L/K))$$

$\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{P}|\mathfrak{p}$

En $Gal(L/K)$ defino $\sim$, $\sigma \sim \tau$ si $\exists\, \eta \in Gal(L/K)$ t.q. $\eta \sigma \eta^{-1} = \tau$. ⊛

Teo (Tchebotarev): ψ es suryectiva, y más aún,

$$\frac{\#\{\mathfrak{P} \subset \mathcal{O}_K \mid N(\mathfrak{P}) \le X : \varphi(\mathfrak{P}) = [c]\}}{\#\{\mathfrak{P} \subset \mathcal{O}_K \mid N(\mathfrak{P}) \le X\}} \xrightarrow[X \to \infty]{} \frac{\#[c]}{\#G}$$

Problema: ¡es difícil acotar el error! (no es efectivo)

Reciprocidad cuadrática

Obs: $K \subset L$ Galois, $K \subset K' \subset L$, $K' = L^H$, $H < G$ "$\mathrm{Gal}(L/K)$"

$$\begin{array}{ccc} G & \left[\begin{array}{c} L \\ | \\ K' \\ | \\ K \end{array}\right]_H & \left[\begin{array}{c} \mathfrak{P} \\ | \\ \mathfrak{P}' = \mathfrak{P} \cap K' \\ | \\ p \end{array}\right] \end{array}$$

$$D(\mathfrak{P} \mid \mathfrak{P}') = \{\sigma \in \mathrm{Gal}(L/K') : \sigma(\mathfrak{P}) = \mathfrak{P}\} =$$

$$\mathrm{Gal}(L/K') < \mathrm{Gal}(L/K) \quad \Big| \quad \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\} \cap \mathrm{Gal}(L/K')$$

$$\rightsquigarrow \boxed{D(\mathfrak{P} \mid \mathfrak{P}') = D(\mathfrak{P} \mid p) \cap H}$$

$$\boxed{I(\mathfrak{P} \mid \mathfrak{P}') = I(\mathfrak{P} \mid p) \cap H}$$

Teo: $K \subset L$ Galois, $p \subset \mathcal{O}_K$, $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{P}' = \mathfrak{P} \cap K'$.

$$\begin{array}{ccc} L & & \mathfrak{P} \\ | & & | \\ L^{I(\mathfrak{P}\mid p)} & & \mathfrak{P}^I \\ | & & | \\ L^{D(\mathfrak{P}\mid p)} & & \mathfrak{P}^D \\ | & & | \\ K & & p \end{array}$$

$e(\mathfrak{P} \mid p) = e$, $f(\mathfrak{P} \mid p) = f$

1. $L^{D(\mathfrak{P}\mid p)}$ es el cuerpo más grande entre $K \subset K' \subset L$ que cumplen $e(\mathfrak{P}' \mid p) = f(\mathfrak{P}' \mid p) = 1$ $(K' \subset L^{D(\mathfrak{P}\mid p)})$
2. $L^{D(\mathfrak{P}\mid p)}$ es la extensión más chica de las ext. K' tales que $\mathfrak{P}$ es el único primo arriba de $\mathfrak{P}' = \mathfrak{P} \cap K'$.

$(L^{D(\mathcal{Q}|\mathcal{P})} \subset K')$

3. $L^{I(\mathcal{Q}|\mathcal{P})}$ es la ext. más grande de las ext. K' tales que $e(\mathcal{Q}'|\mathcal{P}) = 1$.

4. $L^{I(\mathcal{Q}|\mathcal{P})}$ es la ext más chica de las ext. K' tales que $\mathcal{Q}$ es totalmente ramificado sobre $\mathcal{Q}'$.

Demo: Vimos que $L^{D(\mathcal{Q}|\mathcal{P})}$, $L^{I(\mathcal{Q}|\mathcal{P})}$ satisfacen las propiedades.

Supongamos dada $K \subset K' \subset L$ que cumple que $\mathcal{Q}$ es el único primo arriba de $\mathcal{Q}' = \mathcal{Q} \cap K'$. Por teoría de Galois, $K' = L^H$; por otro lado, si $\mathcal{Q}$ es el único primo arriba de $\mathcal{Q}'$, $D(\mathcal{Q}|\mathcal{Q}') = Gal(L/K') = H =$

$= D(\mathcal{Q}|\mathcal{P}) \cap H \Rightarrow H \subset D(\mathcal{Q}|\mathcal{P}) \Rightarrow L^H \supset L^{D(\mathcal{Q}|\mathcal{P})}$

$K'' \qquad \Rightarrow 2v$

(1) Si K' / $e(\mathcal{Q}'|\mathcal{P}) = 1$, $f(\mathcal{Q}'|\mathcal{P}) = 1$

L^H $\qquad \Downarrow \qquad \Downarrow$

$e(\mathcal{Q}|\mathcal{Q}') = e \qquad f(\mathcal{Q}|\mathcal{Q}') = f$

$e(\mathcal{Q}|\mathcal{Q}') \cdot f(\mathcal{Q}|\mathcal{Q}') = |D(\mathcal{Q}|\mathcal{Q}')| = |D(\mathcal{Q}|\mathcal{P}) \cap H|$

$e \cdot f = |D(\mathcal{Q}|\mathcal{P})| \Rightarrow D(\mathcal{Q}|\mathcal{P}) \subset H \Rightarrow L^D \supset K'$

(4) $K' = L^H$, $\mathcal{Q}' = \mathcal{Q} \cap K'$ cumple $\mathcal{Q}|\mathcal{Q}'$ es tot. ramif.

de. Luego $H = I(\mathcal{Q}|\mathcal{Q}') = I(\mathcal{Q}|\mathcal{P}) \cap H \Rightarrow H \subset I(\mathcal{Q}|\mathcal{P})$

$\Rightarrow K' \supset L^{I(\mathcal{Q}|\mathcal{P})}$

③ $K' = L^H$ tq $e(\mathcal{P}'|p) = 1 \Rightarrow e(\mathcal{P}|\mathcal{P}') = e$

$$e(\mathcal{P}|\mathcal{P}') = |I(\mathcal{P}|\mathcal{P}')| = |I(\mathcal{P}|p) \cap H|$$
$$e = |I(\mathcal{P}'|p)| \Rightarrow I(\mathcal{P}|p) \subset H$$
$$\Rightarrow L^I \supset K' \qquad \square$$

Teo (reciprocidad cuadrática): Si p y q son primos impares distintos,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \ (8) \\ -1 & \text{si } p \equiv \pm 3 \ (8) \end{cases}$$ → práctica 4

Demo: $K = \mathbb{Q}$, $L = \mathbb{Q}(\xi_p)$, $\xi_p^p = 1$.

$$Gal(\mathbb{Q}(\xi_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p)^\times \simeq \mathbb{Z}/p-1$$

Si $\sigma \in$ ↑ $\sigma(\xi_p) = \xi_p^a \longrightarrow a$

Vimos: $\mathcal{O}_L = \mathbb{Z}[\xi_p]$, sólo p ramifica.

Problema: ¿cómo descompone q en L?

$L = \mathbb{Q}[x]/\frac{x^p-1}{x-1}$

$$\frac{X^p-1}{X-1} \equiv (X \not{-1}) \cdot \overline{P_1(X)} \cdots \overline{P_r(X)} \quad (\text{mod } q)$$

$$f(\mathcal{P}|q) = gr(\overline{P_i}(X)), \quad p-1 = f \cdot r.$$

$\sum_{i=1}^{p}$

$\mathbb{F}_q[x]/$ $= \mathbb{F}_q(\xi_p) = \mathbb{F}_q[X]/\overline{P_i(X)}$, f es el más chico tq $q^f \equiv 1$ (mod p)

$\mathbb{F}_q$ contiene una raíz p-ésima de la unidad.

$\mathbb{F}_{q^f}^{\times}$ cíclico de orden q^f-1, contiene un elto de orden $p \iff p \mid q^f-1 \iff q^f \equiv 1 (p) \Rightarrow$ **$f = \mathrm{ord}(q \bmod p)$**

Ejemplo: 5. ¿cómo se factoriza en $\mathbb{Q}(\xi_7)$?

$5^1 \neq 1$, $5^2 \equiv 25 \equiv 4 (7)$, $5^3 \overset{\neq 1}{\equiv} -1 (7)$

$\Rightarrow \mathrm{ord}(5 \bmod 7) = 6 \Rightarrow 5$ es primo.

$r = \frac{p-1}{f}$

Por otro lado, si $d \mid p-1$, $(\mathbb{Z}/p)^{\times} \simeq \mathbb{Z}/p-1$ (cíclico de orden $p-1$), existe un único subgrupo $(\langle d \rangle)$ H_d de orden $\frac{p-1}{d}$

$\mathbb{Q}(\xi_p)$

$\frac{p-1}{d}$ | H_d

$\mathbb{Q}(\xi_p) = F_d$

d |

$\mathbb{Q}$

O sea para cada $d \mid p-1$, $\exists!$ $F_d/\mathbb{Q}$ de grado d.

ejercicio Obs: $F_{d_1} \subset F_{d_2} \iff d_1 \mid d_2$

Problema: ¿cómo se factoriza q en F_d? ↗ $f=1$

Lema: q se parte completamente en $F_d/\mathbb{Q} \iff$

q es una potencia d-ésima módulo p.

Teo

Demo: $\mathfrak{p}$ se parte completamente $\iff e = f = 1 \iff$

$D(\mathfrak{P}|\mathfrak{p}) = G(\mathfrak{P}|\mathfrak{p})$

$F_d \subset L = F_r \iff d \mid r = \frac{p-1}{f}$, $f = \operatorname{ord}(q \bmod p)$

$d \mid \frac{p-1}{f} \iff f \mid \frac{p-1}{d}$

$(\mathbb{Z}/p)^\times = \langle g \rangle$, $q = g^a$, $\operatorname{ord}(q \bmod p) = \frac{p-1}{\operatorname{mcd}(a, p-1)}$

$f = \operatorname{ord}(q \bmod p) \mid \frac{p-1}{d} \iff d \mid \operatorname{mcd}(a, p-1)$

$\frac{p-1}{\operatorname{mcd}(a,p-1)}$ ⇑

q es una potencia d-ésima. ∎

$\left(\frac{q}{p}\right) = 1 \iff q$ es un cuadrado módulo p (*)

$F_2 = ?$ $[F_2 : \mathbb{Q}] = 2$, $F_2 = \mathbb{Q}(\sqrt{d})$, como en

$\mathbb{Q}(\zeta_p)/\mathbb{Q}$ sólo ramifica p, en $F_2/\mathbb{Q}$ sólo ramifica p.

Ejercicio: · si $p \equiv 1 \,(4)$, $F_2 = \mathbb{Q}(\sqrt{p})$

· si $p \equiv 3 \,(4)$, $F_2 = \mathbb{Q}(\sqrt{-p})$

(*) $\iff q$ se parte completamente en F_2

Lema

· si $p \equiv 1 \,(4)$, $F_2 = \mathbb{Q}(\sqrt{p})$ $\quad X^2 - p \equiv$ ($\mathfrak{p}$) tiene raíz.

$\iff \left(\frac{p}{q}\right) = 1 = \left(\frac{q}{p}\right)$

· Si $p \equiv 3(4)$, $F_2 = \mathbb{Q}(\sqrt{-p})$, $x^2 + p \equiv$ (q)

$\Leftrightarrow \left(\frac{-p}{q}\right) = 1$, $\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = 1$

$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}}$ $\qquad (-1)^{\frac{p-1}{2}}$

$(\frac{p-1}{2})(\frac{q-1}{2})$

Todo junto: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)$