§ Descomposición e inercia

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt[3]{19}, \zeta_3) & \\ \mathbb{Q}(\sqrt[3]{18}) & & \\ & & \mathbb{Q}(\zeta_3) \\ & \mathbb{Q} & \end{array}$$

$L / k / \mathbb{Q}$.

$\mathfrak{p} \subset \mathcal{O}_k \rightsquigarrow \boxed{\mathfrak{p}\mathcal{O}_L} = \prod_{\mathfrak{q} | \mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$

$f(\mathfrak{q}|\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_k/\mathfrak{p}]$
$= [k(\mathfrak{q}) : k(\mathfrak{p})]$

$$\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p}) \cdot f(\mathfrak{q}|\mathfrak{p}) = [L : k].$$

$$\begin{array}{c} L \\ | \\ k \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{ccccc} \mathfrak{q} & \subset & \mathcal{O}_L & \longrightarrow & k(\mathfrak{q}) \\ | & & | & & |\, f(\mathfrak{q}|\mathfrak{p}) \\ \mathfrak{p} & \subset & \mathcal{O}_k & \longrightarrow & k(\mathfrak{p}) \\ | & & | & & |\, f(\mathfrak{p}|p) \\ p & \in & \mathbb{Z} & \longrightarrow & \mathbb{F}_p \end{array}$$

$$f(\mathfrak{q}|p) = f(\mathfrak{q}|\mathfrak{p}) \cdot f(\mathfrak{p}|p).$$
$$e(\mathfrak{q}|p) = e(\mathfrak{q}|\mathfrak{p}) \cdot e(\mathfrak{p}|p).$$

acción transitiva

$\boxed{L/k \text{ es Galois}} \Rightarrow \operatorname{Gal}(L/k) \curvearrowright \{\mathfrak{q} \mid \mathfrak{p}\}$

$\mathfrak{q} \subset \mathcal{O}_L, \quad \mathfrak{p} \subset \mathcal{O}_k.$

Usando transitividad
$f(\mathfrak{q}|\mathfrak{p}), \; e(\mathfrak{q}|\mathfrak{p})$ son los mismos
$\forall \; \mathfrak{q} | \mathfrak{p}$.

$$e(\mathfrak{q}|\mathfrak{p}) \cdot f(\mathfrak{q}|\mathfrak{p}) \cdot g_{\mathfrak{p}} = [L : k].$$

Si L/k es Galois,

def Para $\mathfrak{p} \subset \mathcal{O}_k$, $\mathfrak{q} \subset \mathcal{O}_L$, $\mathfrak{q} | \mathfrak{p}$,
el **grupo de descomposición**:

$$D(\mathfrak{q}|\mathfrak{p}) = \{ \sigma \in \operatorname{Gal}(L/k) \mid \sigma(\mathfrak{q}) = \mathfrak{q} \}.$$

$$\sigma \in D(\mathfrak{q}|\mathfrak{p}) \rightsquigarrow \bar{\sigma} \in \operatorname{Gal}(k(\mathfrak{q}) / k(\mathfrak{p}))$$

$$\begin{tikzcd}
 & & \mathcal{O}_K \arrow[dll, bend right] \arrow[dl] \arrow[d] \\
\mathcal{O}_L \arrow[r, "\sigma"] \arrow[d] & \mathcal{O}_L \arrow[d] & k(\mathfrak{p}) \arrow[dll, bend right] \arrow[dl] \\
k(\mathfrak{q}) \arrow[r, "\bar{\sigma}", "\cong"'] & k(\mathfrak{q}) &
\end{tikzcd}$$

$$\left[\begin{array}{ccc} D(\mathfrak{q}|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \\ \sigma & \longmapsto & \bar{\sigma} \end{array}\right.$$

<u>def</u> Para $\mathfrak{q}|\mathfrak{p}$ como antes, el <u>grupo de inercia</u> viene dado por

$$I(\mathfrak{q}|\mathfrak{p}) = \ker\left(\begin{array}{ccc} D(\mathfrak{q}|\mathfrak{p}) & \to & \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \\ \sigma & \longmapsto & \bar{\sigma} \end{array}\right)$$

$$= \{ \underbrace{\sigma \in \mathrm{Gal}(L/K)}_{\mathrm{Gal}(L/K)} \mid \sigma(\alpha) \equiv \alpha \ (\mathfrak{q}) \ \forall \alpha \in \mathcal{O}_L \}$$

$$\begin{array}{ccccc} I(\mathfrak{q}|\mathfrak{p}) & \hookrightarrow & D(\mathfrak{q}|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \\ & & \sigma & \longmapsto & \bar{\sigma} \end{array}$$

<u>def</u> Para $D = D(\mathfrak{q}|\mathfrak{p})$, $I = I(\mathfrak{q}|\mathfrak{p})$,

$$\begin{array}{ll} L & \\ | & \\ L^I & \sim \text{campo de inercia} \\ | & \\ L^D & \sim \text{campo de descomposición} \\ | & \\ K & \end{array}$$

$$\left.\begin{array}{l} D(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma D(\mathfrak{q}|\mathfrak{p})\sigma^{-1} \\ I(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma I(\mathfrak{q}|\mathfrak{p})\sigma^{-1} \end{array}\right] \Rightarrow$$ L^I, L^D están definidos salvo $\cong$ por $\mathfrak{p}$

En gral, si $H \subseteq Gal(L|K)$, podemos tomar

$$K \leq L^H \leq L \rightsquigarrow (\mathcal{O}_L)^H = L^H \cap \mathcal{O}_L$$

$$\mathfrak{q} \subset \mathcal{O}_L \rightsquigarrow \mathfrak{q}^H = \mathfrak{q} \cap (\mathcal{O}_L)^H$$

$$\begin{array}{ccccc} \mathfrak{q} & \subset & \mathcal{O}_L & \twoheadrightarrow & k(\mathfrak{q}) \\ | & & | & & | \\ \mathfrak{q}^H & & (\mathcal{O}_L)^H & \twoheadrightarrow & k(\mathfrak{q}^H) \\ | & & | & & | \\ \mathfrak{p} & \subset & \mathcal{O}_K & \twoheadrightarrow & k(\mathfrak{p}) \end{array}$$

Teorema $L|K$ - extn de Galois, $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{q} \subset \mathcal{O}_L$ t.q. $\mathfrak{q}|\mathfrak{p}$.
$D = D(\mathfrak{q}|\mathfrak{p})$, $I = I(\mathfrak{q}|\mathfrak{p})$.
Sea g el número de primos $\mathfrak{q}|\mathfrak{p}$.

1)

$$\begin{array}{ll} L & \\ \mid \; e(\mathfrak{q}|\mathfrak{p}) & e(\mathfrak{q}|\mathfrak{q}^I) = e(\mathfrak{q}|\mathfrak{p}) \qquad f(\mathfrak{q}|\mathfrak{q}^I) = 1 \\ L^I & e(\mathfrak{q}^I|\mathfrak{q}^D) = 1 \qquad f(\mathfrak{q}^I|\mathfrak{q}^D) = f(\mathfrak{q}|\mathfrak{p}) \\ \mid \; f(\mathfrak{q}|\mathfrak{p}) & \\ L^D & e(\mathfrak{q}^D|\mathfrak{p}) = 1 \qquad f(\mathfrak{q}^D|\mathfrak{p}) = 1 \\ \mid \; g & \\ K & \end{array}$$

2) $[G:D] = g$ y $|I| = e(\mathfrak{q}|\mathfrak{p})$

3) Sucesión exacta corta de grupos.

$$1 \to I(\mathfrak{q}|\mathfrak{p}) \to D(\mathfrak{q}|\mathfrak{p}) \to Gal(k(\mathfrak{q})/k(\mathfrak{p})) \to 1.$$

en particular, si $e(\mathfrak{q}|\mathfrak{p}) = 1 \implies$

$$D(\mathfrak{q}|\mathfrak{p}) \simeq Gal(k(\mathfrak{q})/k(\mathfrak{p})).$$

Dem. 2) $[G:D] = g. \rightsquigarrow [L^D : K] = g.$

$G \curvearrowright X \rightsquigarrow$ teorema de órbitas y estabilizadores.

$x \in X \rightsquigarrow Gx \cong G/G_x$

3) $[L^I : L^D] = [D:I]$

$[L^I : L^D] \geq f(\mathfrak{q}^I|\mathfrak{q}^D) = f(\mathfrak{q}|\mathfrak{p})$ ✓

$$1 \to I \to D \to \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \to 1$$

$$D/I \hookrightarrow \underbrace{\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))}_{f(\mathfrak{q}|\mathfrak{p})} \qquad [D:I] \leq f(\mathfrak{q}|\mathfrak{p}).$$

Ejemplo $K = \mathbb{Q}(\zeta_{28})$. $p=2$. se ramifica en K.

$$\Phi_{28} = (x^3+x+1)^2 \cdot (x^3+x^2+1)^2 \pmod 2$$

(Kummer-Dedekind) $\rightsquigarrow 2\mathcal{O}_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$,

- $\mathfrak{p}_1 = (2, 1+\zeta_{28}+\zeta_{28}^3)$
- $\mathfrak{p}_2 = (2, 1+\zeta_{28}^2+\zeta_{28}^3)$.

$f_1 = f_2 = 3$

$$K = \mathbb{Q}(i, \zeta_7) \rightsquigarrow \mathrm{Gal}(K/\mathbb{Q}) \cong \underbrace{(\mathbb{Z}/4\mathbb{Z})^\times}_{\langle 5 \rangle} \times \underbrace{(\mathbb{Z}/7\mathbb{Z})^\times}_{\langle 3 \rangle}.$$

como generadores, tomamos

- $\sigma: i \mapsto -i, \quad \zeta_7 \mapsto \zeta_7$. $\quad \mathrm{ord} = 2$
- $\tau: i \mapsto i, \quad \zeta_7 \mapsto \zeta_7^3$. $\quad \underline{\mathrm{ord}\ \tau = 6}$

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$$

$$\boxed{\begin{aligned} \sigma(\mathfrak{p}_1) &= \mathfrak{p}_1 \\ \sigma(\mathfrak{p}_2) &= \mathfrak{p}_2 \\ \tau(\mathfrak{p}_1) &= \mathfrak{p}_2 \\ \tau(\mathfrak{p}_2) &= \mathfrak{p}_1 \end{aligned}}$$

- $D(\mathfrak{p}_1|\mathfrak{p}) \overset{\text{def}}{=} \{\varphi \in \mathrm{Gal}(K/\mathbb{Q}) \mid \varphi(\mathfrak{p}_1) = \mathfrak{p}_1\}$
$= \langle \sigma, \tau^2 \rangle$

$$\sigma: \zeta_{28} \mapsto \zeta_{28}^{15}$$
$$\tau: \zeta_{28} \mapsto \zeta_{28}^{17}$$

- $I(\mathfrak{p}_1|\mathfrak{p}) = ?!$

$\varphi \in D(\mathfrak{p}_1|\mathfrak{p}) \rightsquigarrow$

$$\begin{tikzcd} \mathcal{O}_K \arrow[r, "\varphi", "\simeq"'] \arrow[d] & \mathcal{O}_K \arrow[d] \\ \mathcal{O}_K/\mathfrak{p}_1 \arrow[r, "\overline{\varphi}", "\simeq"'] & \mathcal{O}_K/\mathfrak{p}_1 \end{tikzcd} \qquad \begin{tikzcd} \mathbb{Z}[\zeta_{28}] \arrow[r, "\varphi"] \arrow[d] & \mathbb{Z}[\zeta_{28}] \arrow[d] \\ \mathbb{Z}[\zeta_{28}]/\mathfrak{p}_1 \arrow[r, "\overline{\varphi}"] & \mathbb{Z}[\zeta_{28}]/\mathfrak{p}_1 \end{tikzcd}$$

$$\mathbb{Z}[\zeta_{28}]/\mathfrak{p}_1 \cong \mathbb{F}_2[x]/(x^3+x+1) \cong \mathbb{F}_8.$$

Tomamos por ejemplo $\sigma \in D(\mathfrak{p}_1|p)$.

$$\sigma : \mathbb{Z}[\zeta_{28}] \longrightarrow \mathbb{Z}[\zeta_{28}] \qquad |\mathbb{F}_8^\times| = 7.$$
$$\zeta_{28} \longmapsto \zeta_{28}^{15} \qquad 15 \equiv 1 \pmod 7)$$

$\bar{\sigma} : k(\mathfrak{p}_1) \longrightarrow k(\mathfrak{p}_1)$ es trivial.

$\tau^2 \in D(\mathfrak{p}_1|p) \rightsquigarrow \overline{\tau^2} = \bar{\zeta} \longmapsto \bar{\zeta}^{17^2} = \bar{\zeta}^2$

no trivial.

(el automorfismo de Frobenius de $\mathbb{F}_8$).

$I = \langle \sigma \rangle$.

$$K^I = \mathbb{Q}(i, \zeta_7)^{\langle \sigma \rangle} = \mathbb{Q}(\zeta_7).$$
$$K^D = \mathbb{Q}(i, \zeta_7)^{\langle \sigma, \tau^2 \rangle} =$$

$$\begin{array}{lcl}
 & \mathbb{Q}(\zeta_{28}) & = K \\
e = 2 & | & | \\
 & \mathbb{Q}(\zeta_7) & = K^I \\
f = 3 & | & | \\
 & \mathbb{Q}(\sqrt{-7}) & = K^D \\
g = 2 & | & | \\
 & \mathbb{Q} & \quad \mathbb{Q}
\end{array}$$

$p\mathcal{O}_K = \mathfrak{p}_1^2 \, \mathfrak{p}_2^2$

$f_1 = f_2 = 3.$

$\boxed{e = 2, \ f = 3, \ g = 2.}$

$(e \cdot f \cdot g = \varphi(28) = 12.)$

§ Reciprocidad cuadrática

Sea p primo impar.

$$p^* = (-1)^{\frac{p-1}{2}} \cdot p.$$

$$\begin{array}{c}
L = \mathbb{Q}(\zeta_p) \\
| \\
K = \mathbb{Q}(\sqrt{p^*}) \\
| \\
\mathbb{Q}
\end{array}$$

Proposición Un primo impar $q \neq p$ se escinde en K

$\Updownarrow$

q se factoriza en L en un $\#$ par de primos.

Dem Si q se escinde en $K \Rightarrow$ $q\mathcal{O}_K = \mathfrak{p}\,\sigma(\mathfrak{p})$ para algún $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$

$\mathrm{Gal}(L/\mathbb{Q})$.

$\{Q \subset \mathcal{O}_L$ t.q. $Q \mid q\} \longleftrightarrow$

$$\{Q \mid \mathfrak{q}\} \sqcup \underset{1:1}{\{Q \mid \sigma(\mathfrak{q})\}}.$$

$$\# \{Q \subset \mathcal{O}_L \mid Q \mid q\} = 2 \cdot \# \{Q \mid \mathfrak{q}\} \text{ es par.}$$

Viceversa, supongamos que el número de ideales $Q \subset \mathcal{O}_L$ t.q. $Q \mid q$ es par.

$g = [\mathrm{Gal}(L|\mathbb{Q}) : D(Q|q)]$ es par.

$G = \mathrm{Gal}(L|\mathbb{Q})$ es cíclico de orden $p-1$.

$H \subset G$ - el subgrupo de índice 2 $\Rightarrow$

$$L^H = K = \mathbb{Q}(\sqrt{p^*})$$

$$D = D(Q|q) \subseteq H \rightsquigarrow K \subseteq L^D$$

$$f(Q^D|q) = 1 \Rightarrow f(\underline{Q \cap K} \mid q) = 1.$$

$\Rightarrow$ q se escinde en $\mathcal{O}_K$ en dos ideales $\boxtimes$

q se escinde en $\mathbb{Q}(\sqrt{p^*}) \Longleftrightarrow \left(\frac{p^*}{q}\right) = +1.$

$\Updownarrow$

q se factoriza en g ideales primos en $\mathbb{Q}(\zeta_p)$, g par.

$\Updownarrow$

q se factoriza en $g = \frac{p-1}{f}$, es par, donde $f = $ ord. de q mod p.

$\Updownarrow$

$$f \mid \frac{p-1}{2} \Longleftrightarrow q^{\frac{p-1}{2}} \equiv 1 \ (p) \Longleftrightarrow \left(\frac{q}{p}\right) = +1.$$

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$ — La ley de reciprocidad cuadrática.