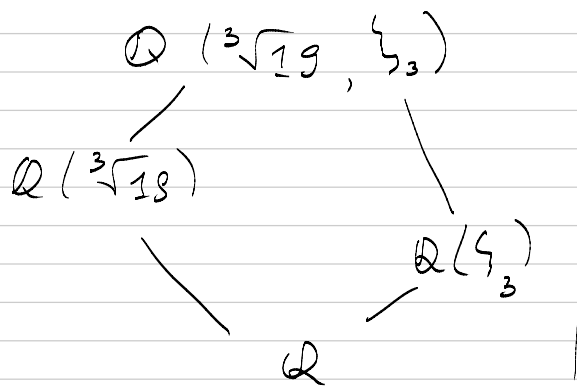


f Descomposición e inercia

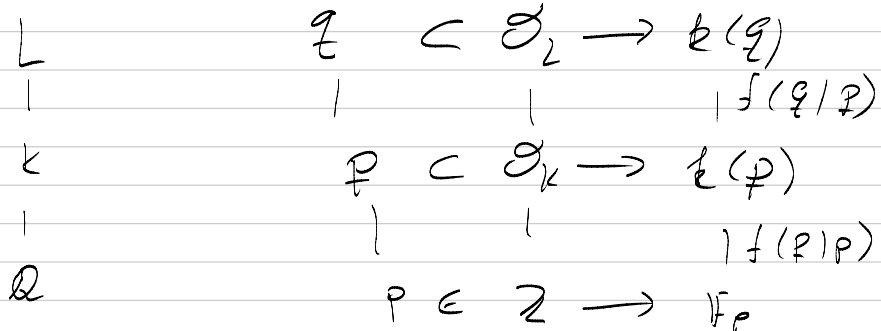


$L/K/\mathbb{Q}$.

$$P \subset \mathcal{O}_K \rightsquigarrow \underbrace{[\mathcal{O}_L / P \mathcal{O}_L]}_{\mathbb{F}} = \prod_{\mathfrak{q}} \mathbb{F}_{\mathfrak{q}} \quad e(\mathfrak{q}|P)$$

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

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



$$f(\mathfrak{q}|P) = f(\mathfrak{q}|F) \cdot f(F|P)$$

$$e(\mathfrak{q}|P) = e(\mathfrak{q}|F) \cdot e(F|P)$$

$|L/K \text{ es Galois}| \Rightarrow \text{Gal}(L/K) \simeq \{ \mathfrak{q} | P \}$
 $\mathfrak{q} \subset \mathcal{O}_L, \quad F \subset \mathcal{O}_K.$

Usando transitividad,

$f(\mathfrak{q}|F), e(\mathfrak{q}|F)$ son los mismos $\forall \mathfrak{q}|P.$

$$e(\mathfrak{q}|F) \cdot f(\mathfrak{q}|F) \cdot g_F = [L : K].$$

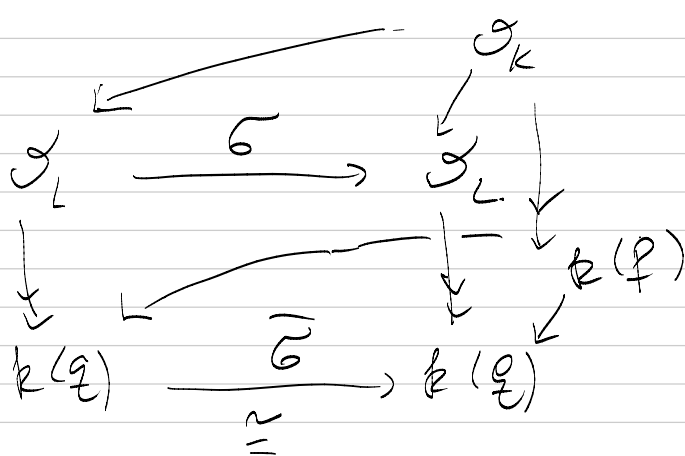
Si L/K es Galois,

def Para $P \subset \mathcal{O}_K, \mathfrak{q} \subset \mathcal{O}_L, \mathfrak{q}|P,$

el grupo de descomposición:

$$D(\mathfrak{q}|P) = \{ \sigma \in \text{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q} \}$$

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



$$\left[\begin{array}{ccc}
 D(q|P) & \longrightarrow & \text{Gal}(k(q)|k(P)) \\
 \cong & \longmapsto & \bar{\sigma}
 \end{array} \right]$$

def Para $q|P$ como antes, el grupo de inercia viene dado por

$$I(q|P) = \ker(D(q|P) \rightarrow \text{Gal}(k(q)|k(P)))$$

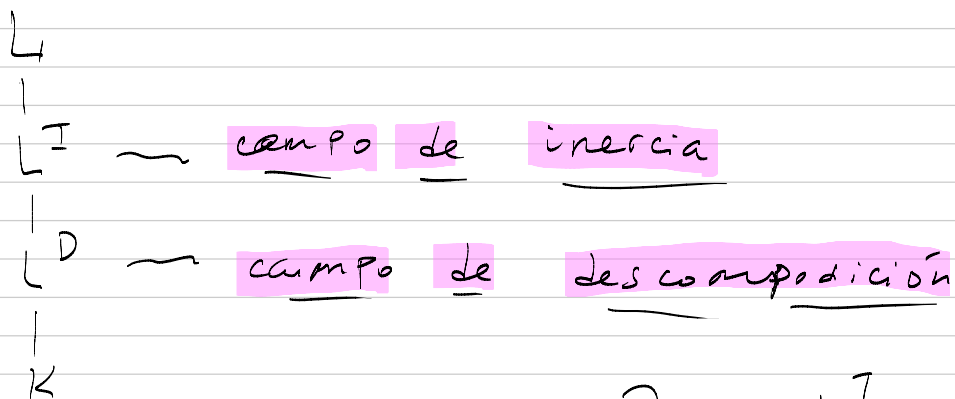
$$\cong \bar{\sigma} \longmapsto \bar{\sigma}$$

$$= \frac{\{ \sigma \in \text{Gal}(L|K) \mid \sigma(\alpha) = \alpha \ (q) \}}{\text{Gal}(L|K)} \quad \{ \forall \alpha \in \mathcal{O}_L \}$$

$$I(q|P) \hookrightarrow D(q|P) \longrightarrow \text{Gal}(k(q)|k(P))$$

$$\cong \bar{\sigma} \longmapsto \bar{\sigma}$$

def Para $D = D(q|P)$, $I = I(q|P)$,



$$\left. \begin{array}{l}
 D(\sigma(q)|P) = \sigma D(q|P) \sigma^{-1} \\
 I(\sigma(q)|P) = \sigma I(q|P) \sigma^{-1}
 \end{array} \right\} \Rightarrow L^I, L^D \text{ están definidos}$$

salvo \cong por P

En geral, si $H \subseteq \text{Gal}(L/K)$, podemos tomar

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

$$\begin{array}{ccc} \mathfrak{q} \subset \mathcal{O}_L & \rightsquigarrow & \mathfrak{q}^H = \mathfrak{q} \cap (\mathcal{O}_L)^H \\ \mathfrak{q} \subset \mathcal{O}_L & \longrightarrow & \mathbb{k}(\mathfrak{q}) \\ \downarrow & & \downarrow \\ \mathfrak{q}^H & (\mathcal{O}_L)^H \longrightarrow & \mathbb{k}(\mathfrak{q}^H) \\ \downarrow & & \downarrow \\ \mathfrak{p} \subset \mathcal{O}_K & \longrightarrow & \mathbb{k}(\mathfrak{p}) \end{array}$$

Teorema L/K - extn de Galois, $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{q} \subset \mathcal{O}_L$ t.q. $\mathfrak{q} | \mathfrak{p}$.

$$D = D(\mathfrak{q} | \mathfrak{p}), \quad I = I(\mathfrak{q} | \mathfrak{p}).$$

Sea g el número de primos $\mathfrak{q} | \mathfrak{p}$.

$$\begin{array}{l} 1) \quad \begin{array}{l} L \\ | \\ e(\mathfrak{q} | \mathfrak{p}) \\ L^I \\ | \\ f(\mathfrak{q} | \mathfrak{p}) \\ L^D \\ | \\ g \\ K \end{array} \quad \begin{array}{l} e(\mathfrak{q} | \mathfrak{q}^I) = e(\mathfrak{q} | \mathfrak{p}) \quad f(\mathfrak{q} | \mathfrak{q}^I) = 1 \\ e(\mathfrak{q}^I | \mathfrak{q}^D) = 1 \quad f(\mathfrak{q}^I | \mathfrak{q}^D) = f(\mathfrak{q} | \mathfrak{p}) \\ e(\mathfrak{q}^D | \mathfrak{p}) = 1 \quad f(\mathfrak{q}^D | \mathfrak{p}) = 1 \end{array} \end{array}$$

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

$$3) \quad \text{Sucesión exacta corta de grupos.} \\ 1 \rightarrow I(\mathfrak{q} | \mathfrak{p}) \rightarrow D(\mathfrak{q} | \mathfrak{p}) \rightarrow \text{Gal}(\mathbb{k}(\mathfrak{q}) / \mathbb{k}(\mathfrak{p})) \rightarrow 1$$

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

$$D(\mathfrak{q} | \mathfrak{p}) \cong \text{Gal}(\mathbb{k}(\mathfrak{q}) / \mathbb{k}(\mathfrak{p})).$$

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

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

$$\alpha \in X \rightsquigarrow G_\alpha \cong G / G_\alpha$$

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

$$[L^I : L^D] \rightsquigarrow f(\mathfrak{q}^I | \mathfrak{q}^D) = f(\mathfrak{q} | \mathfrak{p}) \quad \checkmark$$

$$1 \rightarrow I \rightarrow D \xrightarrow{\vee} \text{Gal}(K(\zeta) / K(F)) \rightarrow 1$$

$$D/I \hookrightarrow \underbrace{\text{Gal}(K(\zeta) / K(F))}_{f(\zeta|F)} \quad [D:I] \leq f(\zeta|F)$$

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

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

(Kummer-Dedekind) $\vartheta_K = P_1^2 \cdot P_2^2$

$$\cdot) P_1 = (2, 1 + \zeta_{28} + \zeta_{28}^3)$$

$$\cdot) P_2 = (2, 1 + \zeta_{28}^2 + \zeta_{28}^3)$$

$$f_1 = f_2 = 3$$

$$K = \mathbb{Q}(i, \zeta_7) \rightsquigarrow \text{Gal}(K/\mathbb{Q}) \cong \underbrace{(\mathbb{Z}/4\mathbb{Z})^{\times}}_{\langle \sigma \rangle} \times \underbrace{(\mathbb{Z}/7\mathbb{Z})^{\times}}_{\langle \tau \rangle}$$

como generadores, tomamos

$$\cdot) \sigma: i \mapsto -i, \quad \zeta_7 \mapsto \zeta_7, \quad \text{ord} = 2$$

$$\cdot) \tau: i \mapsto i, \quad \zeta_7 \mapsto \zeta_7^3, \quad \text{ord} \tau = 6$$

$$f \vartheta_K = P_1^2 \cdot P_2^2$$

$$\cdot) D(P_1 | P) \stackrel{\text{def}}{=} \left\{ \varphi \in \text{Gal}(K/\mathbb{Q}) \mid \varphi(P_1) = P_1 \right\}$$

$$= \langle \sigma, \tau^2 \rangle$$

$$\cdot) I(P_1 | P) = ?!$$

$$\varphi \in D(P_1 | P) \rightsquigarrow$$

$$\begin{array}{l} \sigma(P_1) = P_1 \\ \sigma(P_2) = P_2 \\ \tau(P_1) = P_2 \\ \tau(P_2) = P_1 \end{array}$$

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

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

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\varphi} & \mathcal{O}_K \\ \downarrow & & \downarrow \\ \mathcal{O}_K/P_1 & \xrightarrow{\varphi} & \mathcal{O}_K/P_1 \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}[\zeta_{28}] & \xrightarrow{\varphi} & \mathbb{Z}[\zeta_{28}] \\ \downarrow & & \downarrow \\ \mathbb{Z}[\zeta_{28}]/P_1 & \xrightarrow{\varphi} & \mathbb{Z}[\zeta_{28}]/P_1 \end{array}$$

$$\mathbb{F}_2[x] / (x^3 + x + 1) \cong \mathbb{F}_8$$

Tomamos como ejemplo $\sigma \in D(\mathbb{F}_7 | \mathbb{F})$

$$\sigma: \mathbb{Z}[\zeta_{28}] \rightarrow \mathbb{Z}[\zeta_{28}] \quad |\mathbb{F}_8^*| = 7.$$

$$\zeta_{28} \mapsto \zeta_{28}^{15}$$

$$15 \equiv 1 \pmod{7}$$

$\bar{\sigma}: \mathbb{F}(\zeta_7) \rightarrow \mathbb{F}(\zeta_7)$ es trivial.

$$\sigma^2 \in D(\mathbb{F}_7 | \mathbb{F}) \rightsquigarrow \bar{\sigma}^2 = \bar{\sigma} \mapsto \bar{\sigma}^{17^2} = \bar{\sigma}^2$$

no trivial.

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

$$I = \langle \sigma \rangle.$$

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

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

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

$$g \mathcal{D}_K = \mathbb{F}_1^2, \mathbb{F}_2^2$$

$$f_1 = f_2 = 3.$$

$$\overline{(e = 2, f = 3, g = 2.)}$$

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

§ Reciprocidad cuadrática

Sea p primo impar.

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

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



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

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

Dem Si q se escinde en $K \Rightarrow \sigma \in \text{Gal}(K/\mathbb{Q})$
 $\mathcal{D}_K = \mathbb{F} \sigma(\mathbb{F})$ para algún $\sigma \in \text{Gal}(L/\mathbb{Q})$.

$$\{Q \subset \mathcal{O}_L \text{ t.q. } Q|q\} \leftrightarrow$$

$$\{Q|p\} \cup \{Q|6(p)\}$$

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

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

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

$G = \text{Gal}(L/Q)$ es cíclico de orden $p-1$.

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

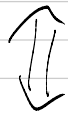
$$L^H = K = Q(\sqrt{p^*})$$

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

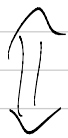
$$f(Q^D|q) = 1 \Rightarrow f(Q \cap K|q) = 1.$$

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

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



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



q se factoriza en $g = \frac{p-1}{f}$ es par.

donde $f = \text{ord. de } q \text{ mod } p$.



$$g \mid \frac{p-1}{2} \iff q^{\frac{p-1}{2}} = 1 \pmod{p} \iff \left(\frac{q}{p}\right) = +1.$$

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