14/10 § El automorfismo de Frobenius

L/K $\mathfrak{p} \subset \mathcal{O}_K$ $\mathfrak{q} \subset \mathcal{O}_L$ $\mathfrak{q} \mid \mathfrak{p} \rightsquigarrow \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$

$e(\mathfrak{q}|\mathfrak{p}) = 1.$

$$1 \to I(\mathfrak{q}|\mathfrak{p}) \to D(\mathfrak{q}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \to 1$$
$$\sigma \longmapsto \overline{\sigma}$$

$$D(\mathfrak{q}|\mathfrak{p}) \simeq \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$$
$$\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \longmapsto (x \longmapsto x^{\#k(\mathfrak{p})})$$

Def Si $\mathfrak{q} \mid \mathfrak{p}$, $e(\mathfrak{q}|\mathfrak{p})$, entonces el elemento de $\mathrm{Gal}(L/K)$ que se reduce a $x \mapsto x^{\#k(\mathfrak{p})}$ mód $\mathfrak{q}$ se llama el Frobenius y se denota por $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$

Note: 1) $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}(\alpha) \equiv \alpha^{\#k(\mathfrak{p})} \pmod{\mathfrak{q}}$
$\forall \alpha \in \mathcal{O}_L$

2) Si tomamos otro ideal $\sigma(\mathfrak{q}) \mid \mathfrak{p}$ para $\sigma \in \mathrm{Gal}(L/K)$

$$\mathrm{Frob}_{\sigma(\mathfrak{q})|\mathfrak{p}} = \sigma\, \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}\, \sigma^{-1}$$

3) En particular, si $\mathrm{Gal}(L/K)$ es abeliano $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ depende solamente de $\mathfrak{p}$.

$\mathrm{Frob}_{\mathfrak{p}}$

$$\mathrm{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^{\#k(\mathfrak{p})} \pmod{\mathfrak{q}} \quad \forall\, \mathfrak{q} \mid \mathfrak{p}$$

$\Longrightarrow$ t.c.d.R $\quad \mathrm{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^{\#k(\mathfrak{p})} \pmod{\mathfrak{p}\mathcal{O}_L}$

Ejemplo $K = \mathbb{Q}(\sqrt{d})$ $\quad K/\mathbb{Q}$.

Si p es un primo no ramificado en K.

- $\left(\frac{d}{p}\right) = +1 \Rightarrow p\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2$.
  $D(\mathfrak{p}_1|p) = 1 \Rightarrow \mathrm{Frob}_p = 1.$

•) $\left(\frac{d}{p}\right) = -1 \Rightarrow$ p es inerte

$D(p\mathcal{O}_L \mid p) = Gal(K/\mathbb{Q}) = \{1, \sigma\}$.

$Frob_p : \sqrt{d} \longmapsto -\sqrt{d}$.

$Frob_p : \sqrt{d} \longmapsto \left(\frac{d}{p}\right)\sqrt{d}$.

Ejemplo $K = \mathbb{Q}(\zeta_n)$ $p \nmid n$ no se ramifica en K.

$Frob_p : \zeta_n \longmapsto \zeta_n^p$.

$\alpha \in \mathbb{Z}[\zeta_n] \Rightarrow \alpha = \sum_i a_i \zeta_n^i$ $a_i \in \mathbb{Z}$

$\alpha^p \equiv \sum_i a_i^p \cdot \zeta_n^{ip} \equiv \underbrace{\sum_i a_i \zeta_n^{ip}}_{= Frob_p(\alpha)}$ (mód p)

□

$\text{ord } Frob_{\mathfrak{q}|\mathfrak{p}} = [k(\mathfrak{q}) : k(\mathfrak{p})] = f(\mathfrak{q}|\mathfrak{p}) = f$

$p\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_g$, donde $f(\mathfrak{q}_i|\mathfrak{p}) = f$.

$g = [L:K]/f$.

En particular,

$Frob_{\mathfrak{q}|\mathfrak{p}} = 1 \iff p\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_g$, donde $g = [L:K]$

"$\mathfrak{p}$ se escinde completamente en L".

Teorema de densidad de Chebotarëv

Para $K/\mathbb{Q}$ extn de Galois con $Gal(K/\mathbb{Q}) = G$, sea C una clase de conjugación en G.

$X = \{p \in \mathbb{Z} \mid Frob_{\mathfrak{q}|p} \in C\}$.

$d(X) = \#C/\#G$.

$d(X)$ = densidad analítica (de Dirichlet)

o densidad natural.

Corolario Hay un $\#$ infinito de primos que se escinden completamente en K, su densidad es $1/\#G$.

Ejemplo $K = \mathbb{Q}(\zeta_n)$. $p \nmid n$. $\#G = \varphi(n)$.

$\mathrm{Frob}_p \longleftrightarrow p \bmod n$.

$\zeta_n \mapsto \zeta_n^p$

Chebotarëv: $d(p \mid p \equiv a \ (n)) = \frac{1}{\varphi(n)}$.

(t. de Dirichlet)

Ejemplo $K = \mathbb{Q}(\sqrt[3]{15}, \zeta_3)$

$\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

$\sigma: \sqrt[3]{15} \mapsto \zeta_3 \sqrt[3]{15}$

$\tau: \zeta_3 \mapsto \zeta_3^2$.

Clases de conjugación:

$C = \{1\}$ $C' = \{(12), (13), (23)\}$ $C'' = \{(123), (132)\}$

·) Primos con $\mathrm{Frob}_p \in C \iff p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_6$ $p \equiv 1 \ (3)$ y 15 es un cubo mód p. $d(x) = \frac{1}{6}$

·) Primos con $\mathrm{Frob}_p \in C'$ $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. $p \equiv 2 \ (3)$ $d(x) = \frac{1}{2}$

$\frac{\#C'}{\#G}$

·) Primos con $\mathrm{Frob}_p \in C''$ $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. $p \equiv 1 \ (3)$ t.q. 15 no es un cubo mód p. $d(x) = \frac{1}{3}$

§ Caso no-Galois

L/K - la cerradura de Galois.

$\mathrm{Gal}(L/K) = G$. $K = L^H$, $H \subseteq G$.

$\mathfrak{P} \in \mathcal{O}_F$, $\mathfrak{P}$ no se ramifica en L

$Q \subset \mathcal{O}_L$ un primo t.q. $Q \mid \mathfrak{P}$

$F = \mathrm{Frob}_{Q|\mathfrak{P}}$ $\langle F \rangle = D(Q|\mathfrak{P})$

$\langle F \rangle \cap \{\text{clases laterales } H\sigma, \sigma \in G\}$

$H\sigma \longmapsto H\sigma F$.

las órbitas: $\{H\sigma_1, H\sigma_1 F, H\sigma_1 F^2, \dots, H\sigma_1 F^{n_1-1}\}$,

$\dots\dots$

$\{H\sigma_s, H\sigma_s F, H\sigma_s F^2, \dots, H\sigma_s F^{n_s-1}\}$

n_i es el # más pequeño t.q. $H\sigma_i F^{n_i} = H\sigma_i$.

$\sum_i n_i = [G:H] = [K:F]$.

Teorema Se tiene $\mathfrak{p}\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, $\mathfrak{q}_i = \sigma_i(Q) \cap \mathcal{O}_K$.

$f(\mathfrak{q}_i|\mathfrak{p}) = n_i$.

Dem $\mathfrak{q}_i \mid \mathfrak{p}$

·) $\mathfrak{q}_i \neq \mathfrak{q}_j$ para $i \neq j$.

Si $\mathfrak{q}_i = \mathfrak{q}_j \Rightarrow \sigma_i(Q)$ y $\sigma_j(Q)$ son primos en $\mathcal{O}_L$ sobre el mismo ideal $\mathfrak{q}_i = \mathfrak{q}_j \subset \mathcal{O}_K$.

$\exists \sigma \in H$ t.q. $\sigma_i(Q) = \sigma\sigma_j(Q)$.

$\sigma_i^{-1}\sigma\sigma_j(Q) = Q \Rightarrow \sigma_i^{-1}\sigma\sigma_j \in D(Q|\mathfrak{p}) = \langle F \rangle$

$\sigma_i^{-1}\sigma\sigma_j = F^k$ para algún k.

$\sigma\sigma_j = \sigma_i F^k \Rightarrow H\sigma_j = H\sigma_i F^k$

están en la misma órbita

$\Rightarrow j = i$.

·) Falta ver que los $\mathfrak{q}_i$ son todos los ideales t.q. $\mathfrak{q}_i \mid \mathfrak{p}$.

$$\sum_i n_i = \sum_{\mathfrak{q}\mid\mathfrak{p}} f(\mathfrak{q}|\mathfrak{p}) = [K:F].$$

Basta ver que $f(\mathfrak{q}_i|\mathfrak{p}) \geq n_i \quad \forall i$.

$$\begin{array}{ccccc} \sigma_i(Q) & \subset & \mathcal{O}_L & \twoheadrightarrow & k(\sigma_i(Q)) \\ | & & | & & | \\ \sigma_i(Q)\cap\mathcal{O}_K = \mathfrak{q}_i & \subset & \mathcal{O}_K & \twoheadrightarrow & k(\mathfrak{q}_i) \\ | & & | & & | \\ \mathfrak{p} & \subset & \mathcal{O}_i & \twoheadrightarrow & k(\mathfrak{p}) \end{array}$$

$$H \Rightarrow \underbrace{\mathrm{Frob}_{\sigma_i(Q)\mid \mathfrak{q}_i}}_{} = \left(\mathrm{Frob}_{\sigma_i(Q)\mid \mathfrak{p}}\right)^{f(\mathfrak{q}_i\mid\mathfrak{p})}$$

$$= \left(\sigma_i \underbrace{\mathrm{Frob}_{Q\mid\mathfrak{p}}}_{=F} \sigma_i^{-1}\right)^{f(\mathfrak{q}_i\mid\mathfrak{p})}$$

$$= \sigma_i F^{f(\mathfrak{q}_i\mid\mathfrak{p})} \cdot \sigma_i^{-1}$$

$$\sigma_i F^{f(\mathfrak{q}_i\mid\mathfrak{p})} \sigma_i^{-1} \in H$$

$$H\sigma_i = H\sigma_i F^{f(\mathfrak{q}_i\mid\mathfrak{p})}$$

$$\Longrightarrow \quad f(\mathfrak{q}_i\mid\mathfrak{p}) \geq n_i.$$

∎

Ejemplo $K = \mathbb{Q}(\sqrt[4]{2})$ $K/\mathbb{Q}$ no es Galois.

$L = \mathbb{Q}(\sqrt[4]{2}, i)$ — cerradura de Galois.

$G = \mathrm{Gal}(L\mid\mathbb{Q})$

$\sigma : \sqrt[4]{2} \longmapsto i\sqrt[4]{2}$

$\tau : i \longmapsto -i.$

$G = \langle \sigma, \tau \rangle \simeq D_4$

$= \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$

$K = \mathbb{Q}(\sqrt[4]{2}) = L^H, \quad H = \langle \tau \rangle.$

Clases laterales: $H, \; H\sigma, \; H\sigma^2, \; H\sigma^3.$

$p \neq 2$ no se ramifica en L

Sea $\mathfrak{q} \subset \mathcal{O}_L$ un primo t.q. $\mathfrak{q} \mid \mathfrak{p}$.

$F = \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \in Gal(L/K)$.

Por ejemplo, $F = \tau$.

$H\tau = H$, $H\sigma\tau = H\tau\sigma^3 = H\sigma^3$, $H\sigma^2\tau = H\sigma^2$

$\{H\}, \{H\sigma, H\sigma^3\}, \{H\sigma^2\}$.

$\Rightarrow \quad \mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$. $\quad f_1 = f_2 = 1$

$f_3 = 2$.

Ejercicio: Ver otros casos para F.