Repaso: supongamos L/k Galois, $Gal(L/k)$ su grupo de Galois.

$$\begin{array}{ccc} L & \mathcal{O}_L & \mathfrak{P} \\ | & | & | \\ k & \mathcal{O}_k & \mathfrak{p} \end{array} \qquad \mathfrak{p}\cdot\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}$$

$\sigma \in Gal(L/k)$ actúa en la factorización, o sea

$$\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{P}_1)^{e_1}\cdots\sigma(\mathfrak{P}_r)^{e_r}$$

(los anteriores permutados)

$$\sigma\{\mathfrak{P}_1,\dots,\mathfrak{P}_r\} = \{\mathfrak{P}_1,\dots,\mathfrak{P}_r\}$$

Vimos: la acción es transitiva, o sea dado $\mathfrak{P}_i, \mathfrak{P}_j$, $\exists\ \sigma$ t.q. $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.

Corolario: $\cdot\ e = e(\mathfrak{P}_i|\mathfrak{p})$ es siempre el mismo.

$\cdot\ f = f(\mathfrak{P}_i|\mathfrak{p})$ "

$\cdot\ [L:k] = efr$.

Def: Si $\mathfrak{P}|\mathfrak{p}$, definimos el grupo de descomposición de $\mathfrak{P}|\mathfrak{p}$,

$$D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in Gal(L/k) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

El grupo de inercia $I(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in Gal(L/k) : \sigma(x) \equiv x \pmod{\mathfrak{P}}\ \forall x \in \mathcal{O}_L\}$

Obs: 1. $D(\mathfrak{P}|\mathfrak{p})$ y $I(\mathfrak{P}|\mathfrak{p})$ son subgrupos de $Gal(L/k)$

2. $I(\mathfrak{P}|\mathfrak{p}) \overset{\text{subgrupo}}{<} D(\mathfrak{P}|\mathfrak{p})$

Si $\sigma \in I(\mathfrak{P}|\mathfrak{p})$, $x \in \mathcal{O}$, $\sigma(x) \equiv x \pmod{\mathfrak{P}} \Rightarrow \sigma(x) \in \mathfrak{P} \Rightarrow \sigma \in D(\mathfrak{P}|\mathfrak{p})$

Ejemplo: $K = \mathbb{Q}$, $L = \mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$, $\mathcal{O}_L = \mathbb{Z}[i]$ (enteros de Gauss)

Si p es primo, ¿cómo se factoriza $p\cdot\mathbb{Z}[i]$?

Toda ext. cuadrática es monogénica, $m_i(x) = x^2+1$

Dado p, ¿cómo se factoriza x^2+1 mód p? $-1 \equiv \square \bmod p$

Decidir si $\exists\, a \in \mathbb{F}_p$ t.f. $a^2 \equiv -1\ (p)$, $\left(\frac{-1}{p}\right) = 1$ o -1

Def: dado p primo, $a \in \mathbb{Z}$, $p \nmid a$, definimos el símbolo cuadrático

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \equiv \square \bmod p \\ -1 & \text{si } a \not\equiv \square \bmod p \end{cases}$$

Vale (ejercicio): $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

Como $\mathbb{F}_p^\times$ es cíclico,
$\langle g \rangle$, g tiene orden $p-1$ $(p \neq 2)$

$$\underbrace{-1}_{\text{orden } 2} = g^{\frac{p-1}{2}} \equiv \square\ (\bmod p) \iff \frac{p-1}{2} \text{ es par}$$

$$\iff p \equiv 1\ (4)$$

Obs: Si k es un cuerpo, hay a lo sumo un único elemento $a \neq 1$ t.f. $a^2 = 1$ (x^2-1)

Luego: p es inerte en $\mathbb{Z}[i]$ ($p\cdot\mathbb{Z}[i]$ es primo)

$\Leftrightarrow p \equiv 3 (4)$. Un primo p se parte en $\mathbb{Z}[i] \Leftrightarrow$

$p \equiv 1 (4)$. $\quad Gal(\mathbb{Q}[i]/\mathbb{Q}) = \{1, \tau\}$
τ conj. compleja

- $p=3$, 3 inerte , $3\mathbb{Z}[i]$ es primo,

$$D(3|3) = \{1, \tau\}, \quad I(3|3) = \{1\}$$

$\{\sigma : \sigma(x) \equiv x (3) \ \forall x \in \mathbb{Z}[i]\}$ $\quad \tau(i) = -i$, $i \not\equiv -i (3) \Leftrightarrow 2i \not\in (3)$

- $p=5$, 5 se parte, $(5) = (2+i)(2-i)$

$$D((2+i)|5) = \{1\}, \quad I((2+i)|5) = \{1\}$$

- $p=2$, $(2) = (1+i)^2$, ramifica.

$$D((1+i)|2) = \{1, \tau\}, \quad I((1+i)|2) = \{1, \tau\}.$$

$\{\tau(x) \equiv x (1+i) \ \forall x \in \mathbb{Z}[i]\}$

τ basta con verificarlo en una base de $\mathbb{Z}[i]$

Basta ver con $x = i$: $-i \equiv i (1+i)$, pues $2i \in (1+i)$

Recordar: $disc(\mathbb{Z}[i]) = \det\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = -4$

Un primo p ramifica en $\mathbb{Q}[i]/\mathbb{Q} \Leftrightarrow p \mid disc(\ ) \quad -4$

Si $\mathcal{P}|p$ fijo, $D(\mathcal{P}|p) \ni \sigma$, $\sigma(\mathcal{P}) = \mathcal{P}$
$\sigma(\mathcal{Q}) = \mathcal{Q}$

$$\mathcal{O}_L \xrightarrow{\sigma} \mathcal{O}_L \quad \rightsquigarrow \quad \mathcal{O}_L/\mathfrak{P} \xrightarrow{\bar{\sigma}} \mathcal{O}_L/\mathfrak{P}$$
$$\mathfrak{P} \xrightarrow{\sigma} \mathfrak{P} \qquad [\alpha] \to [\sigma(\alpha)]$$

por otro lado, $\sigma|_{\mathcal{O}_K} = id$

$$\begin{array}{ccc} F_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P} & \xrightarrow{\bar{\sigma}} & \mathcal{O}_L/\mathfrak{P} \\ | & & | \\ F_p = \mathcal{O}_K/p & \xrightarrow{id} & \mathcal{O}_K/p \end{array} \quad \rightsquigarrow \bar{\sigma} \in Gal\left(\frac{(\mathcal{O}_L/\mathfrak{P})}{(\mathcal{O}_K/p)}\right)$$

Luego tenemos $\psi : D(\mathfrak{P}|p) \to Gal(F_{\mathfrak{P}}/F_p)$ (morfismo de grupos)

$$\sigma \to \bar{\sigma}$$

$$N\ddot{z}(\psi) = \{\sigma \in D(\mathfrak{P}|p) \;/\; \bar{\sigma}(\bar{\alpha}) = \bar{\alpha} \;\forall\, \bar{\alpha} \in \mathcal{O}_L/\mathfrak{P}\}$$

$$\text{“}I(\mathfrak{P}|p)\text{”} \qquad \text{“}\sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \;\forall \alpha \in \mathcal{O}_L\text{”}$$

$$0 \to I(\mathfrak{P}|p) \xrightarrow{\psi} D(\mathfrak{P}|p) \to Gal(F_{\mathfrak{P}}/F_p)$$

Obs: 1. $I(\mathfrak{P}|p) \triangleleft D(\mathfrak{P}|p)$ (es normal).

2. $Gal(F_{\mathfrak{P}}/F_p)$ es cíclico (en particular abeliano)

luego si $\mathfrak{P}$ es tal que $I(\mathfrak{P}|p) = \{1\}$, $D(\mathfrak{P}|p)$ es cíclico (abeliano)

Objetivo: probar que ψ es sobreyectiva.

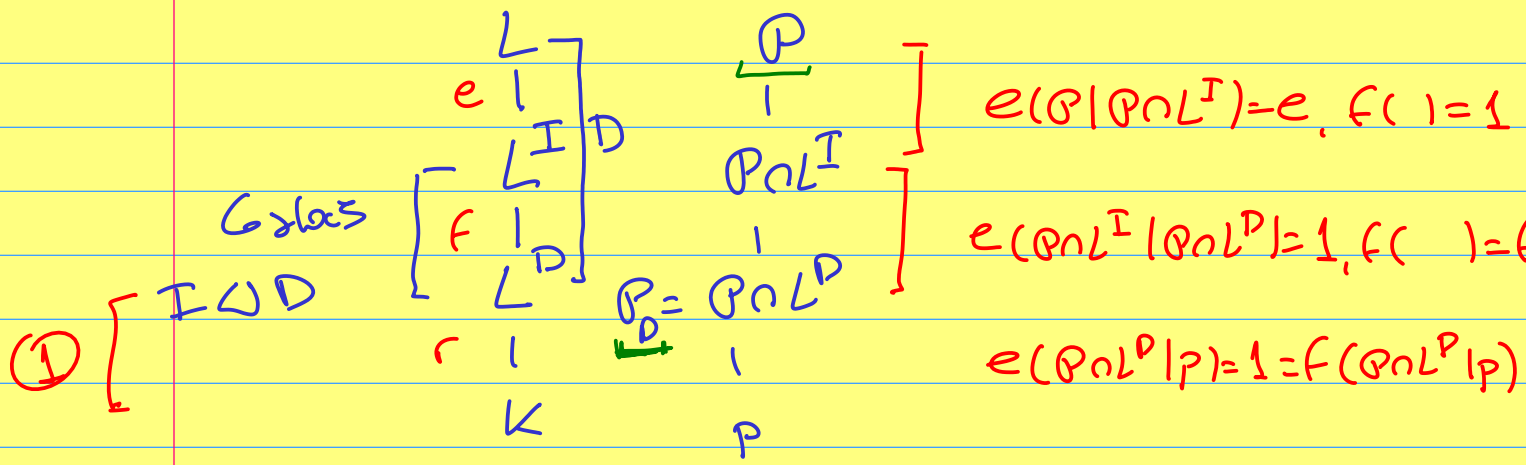
Obs: si $\mathfrak{P}_1, \mathfrak{P}_2$ dos primos arriba de p,

¿ qué relación hay entre $D(\mathcal{P}_1|p)$, $D(\mathcal{P}_2|p)$? Son conjugados

Existe $\sigma \in Gal(L/k)$ t.q. $\sigma(\mathcal{P}_1) = \mathcal{P}_2$

$D(\mathcal{P}_2|p) = \sigma D(\mathcal{P}_1|p) \sigma^{-1}$ (meditar)

Teorema: $\mathcal{P}|p$ como antes, $I = I(\mathcal{P}|p)$ $p\mathcal{O}_L = \mathcal{P}_1^e \cdots \mathcal{P}_r^e$
$D = D(\mathcal{P}|p)$ $f = f(\mathcal{P}|p)$



Demo: $Gal(L/k) \subset \{\mathcal{P}_1, \dots, \mathcal{P}_r\}$ transitiva.

$\Rightarrow |Gal(L/k)| = r \cdot |D(\mathcal{P}_1|p)| \Rightarrow |D(\mathcal{P}_1|p)| = e \cdot f$

$\|$
$e \cdot f \cdot r$

Luego $[L^D : k] = [Gal(L/k) : D(\mathcal{P}|p)] = r$ (1)

La extensión L/L^D es Galois, $Gal(L/L^D) = D$

que fija a $\mathcal{P}$ sobre $\mathcal{P}_D = \mathcal{P} \cap L_D$

Como $Gal(L/L^D)$ actúa transitivamente en el cjto
$\|$
$D(\mathcal{P}|p)$

de primos arriba de $\mathfrak{P}_D$, y a la vez, $\sigma(\mathfrak{P}) = \mathfrak{P}$

$\forall \sigma \in D(\mathfrak{P}|p) \Rightarrow$ hay un único primo arriba de $\mathfrak{P}_D$.

$$e.f = [L : L^D] = e(\mathfrak{P}|\mathfrak{P}_D).f(\mathfrak{P}|\mathfrak{P}_D) \leq e.f$$

$$e = e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{P}_D).e(\mathfrak{P}_D|p) \quad (e(\mathfrak{P}_D|p) \geq 1)$$

$$f = f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{P}_D).f(\mathfrak{P}_D|p) \quad (f(\mathfrak{P}_D|p) \geq 1)$$

$$\Rightarrow e(\mathfrak{P}|\mathfrak{P}_D) \leq e \;,\; f(\mathfrak{P}|\mathfrak{P}_D) \leq f$$

$$\Rightarrow \boxed{e(\mathfrak{P}_D|p) = 1 = f(\mathfrak{P}_D|p)} \qquad \boxed{\begin{array}{l} e(\mathfrak{P}|\mathfrak{P}_D) = e \\ f(\mathfrak{P}|\mathfrak{P}_D) = f \end{array}}$$

$\mathfrak{P}_I = \mathfrak{P} \cap L^I$, Afirmo: $\boxed{f(\mathfrak{P}|\mathfrak{P}_I) = 1}$ $\quad [F_{\mathfrak{P}} : F_{\mathfrak{P}_I}]$

Sea $\mathcal{O}_L/\mathfrak{P} = \mathcal{O}_{L^I}/\mathfrak{P}_I$ $\quad (F_{\mathfrak{P}} \;\; F_{\mathfrak{P}_I})$

Miremos $Gal\left(F_{\mathfrak{P}}/F_{\mathfrak{P}_I}\right) = \{id\}$ listo.

σ, $\bar{\alpha} \in F_{\mathfrak{P}}$, $\alpha \in \mathcal{O}_L$ un levantado.

L/L^I es Galois, $Gal(L/L^I) = I$

$$g(X) = \prod_{\sigma \in I} (X - \sigma(\alpha)) \in L^I[X]$$ y α es raíz.

(en realidad en $\mathcal{O}_{L^I}$)

$\bar{g}(x) \in \mathbb{F}_{p^I}[x]$ tiene a $\bar{\alpha}$ como raíz.

$\Rightarrow m_{\bar{\alpha}}(x) \mid \bar{g}(x)$, pero $\bar{g}(x) = \prod_{\sigma \in I} (x - \overline{\sigma(\alpha)}) \bmod p$

$= (x-\bar{\alpha})^{|I|}$

Si $\sigma \in I$, $\sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \ \forall \alpha \rightsquigarrow \overline{\sigma(\alpha)} = \bar{\alpha}$

$\Rightarrow$ $m_{\bar{\alpha}}(x)$ tiene una única raíz en $\mathbb{F}_{\mathfrak{p}}$

Recordar: las ext. de cpos finitos son separables

$\Rightarrow m_{\bar{\alpha}}(x) = x - \bar{\alpha} \Rightarrow \bar{\alpha} \in \mathbb{F}_{p^I}$ ✓

Luego, $\boxed{f(\mathfrak{P}_I \mid \mathfrak{P}_D) = f}$ (por ser multiplicativo).

La extensión $\begin{matrix} L^I \\ | \\ L^D \end{matrix}$ es Galois, pues $I \lhd D$

$f = f(\mathfrak{P}_I \mid \mathfrak{P}_D) \overset{(*)}{\leq} [L^I : L^D]$

"$f(\mathfrak{P}_I \mid \mathfrak{P}_D) \cdot e(\mathfrak{P}_I \mid \mathfrak{P}_D)$"

$$Gal(L^I/L^D) \xrightarrow{\psi} Gal(\mathbb{F}_{p^I}/\mathbb{F}_{p^D})$$

$\#$ $\qquad\qquad\qquad\qquad$ $\#$

$D/I \qquad\qquad\qquad\qquad f$

tiene f elts $\rightarrow$

$Gal(L/L^D) = D$, $Gal(L/L^I) = I$, $I \lhd D$,

$$D \begin{cases} L \\ | \\ L^I \} I \\ | \\ L^D \} D/I \end{cases} \qquad \begin{aligned} D(\mathfrak{P} \mid \mathfrak{P}_D) &= D(\mathfrak{P} \mid p) = D \\ I(\mathfrak{P} \mid \mathfrak{P}_D) &= I(\mathfrak{P} \mid p) = I \end{aligned}$$

Como ψ es sobreyectiva, $|D/I| \leq f$

$f \leq [L^I : L^D] \Rightarrow \boxed{[L^I : L^D] = f}$

$(*)$

$\Rightarrow e(\mathfrak{P}_I|\mathfrak{P}_D)=1$

$\Rightarrow e(\mathfrak{P}|\mathfrak{P}_I)=e$ y terminamos ☐

Cor: ψ isomorfismo.

D/ $|D/I| = |Gal(L^I/L^D)| = e = |Gal((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})|$

$\Rightarrow \psi$ biyectiva. ☐

Cor2: $\mathfrak{p}$ ramifica en $L/K \iff e(\mathfrak{P}|\mathfrak{p})>1$ (para cualquier $\mathfrak{P}|\mathfrak{p}$) $\iff L^I \subsetneq L \iff I(\mathfrak{P}|\mathfrak{p}) \neq \{1\}$

En particular, para todo primo $\mathfrak{p} \subset \mathcal{O}_K$ salvo finitos, $I(\mathfrak{P}|\mathfrak{p})=1$.

Ejemplo: $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})$, d_i libre de cuadrados

d_1/d_2 no es cuadrado

$Gal(L/K) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, $[L:\mathbb{Q}]=4$

Si p primo en $\mathbb{Z}$, ¿$f(\mathfrak{P}|p)=4$? NO

$\mathfrak{P}|p$

Si $f(\mathfrak{P}|p)=4$, $|D(\mathfrak{P}|p)/I(\mathfrak{P}|p)| = f = 4 = Gal(L/\mathbb{Q})$

$\mathbb{Z}/2 \times \mathbb{Z}/2 = D(\mathfrak{P}|p) \not\to Gal(\mathbb{F}_{p^4}/\mathbb{F}_p) \simeq \mathbb{Z}/4$ NO

$\Rightarrow$ $\exists (\mathcal{P}|p| = 1$ ó 2. Si p no ramifica,

$p \cdot \mathcal{O}_L = \begin{cases} \mathcal{P}_1 \mathcal{P}_2 \mathcal{P}_3 \mathcal{P}_4 & \text{e.f. } r=4 \\ \mathcal{P}_1 \mathcal{P}_2 & \text{"} \quad 1 \end{cases}$

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

↔ $|D(\mathcal{P}_i|p)| = 2$

Subgrupos de orden 2, hay 3 ↔ 3/4

" " 1 hay 1 ↔ 1/4

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

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

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

$x^2 - 3$ $\quad$ $\mathbb{Q}$ $\quad$ $x^2 - 7 \equiv (p)$

$\vdots$ $\quad$ (p) $\quad$ $\downarrow$

p se parte en 4 primos ↔ $\left(\frac{7}{p}\right) = 1 = \left(\frac{3}{p}\right)$ (37 ↔ el primero)

PX 2,3,7

Cota	1000	10.000	100.000	10^6
#P	166	1227	9590	78496
#parten	35	298	2353	19536
%	21,08	24,28	24,53	24,91
	(21 ms)	(71 ms)	(444 ms)	(3880 ms)