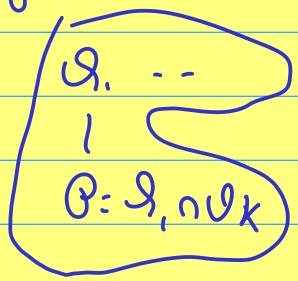


Entender primos en extensiones

$\mathcal{O}_L$ L ← ¿cómo son estos primos?

| |

$\mathcal{O}_K$ K ← conocemos estos primos



Teo: $\mathcal{O}_K[\alpha] \subset \mathcal{O}_L$ ($K[\alpha]=L$) (no vale igualdad en general). $[\mathcal{O}_L : \mathcal{O}_K[\alpha]] = \left|\mathcal{O}_L / \mathcal{O}_K[\alpha]\right|$

α entero en $\mathcal{O}_L$; índice

Sea $\mathfrak{P} \subset \mathcal{O}_K$ t.f. si $N(\mathfrak{P}) = p^r$, $\mathfrak{P}\cap\mathbb{Z}=(p)$

$p \times [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. $\mathfrak{P}\cdot\mathcal{O}_L =$ factorización

↕

factorizar $m_\alpha(x)$ módulo $\mathfrak{P}$

$\bar{g}(x)$

- $g(x) \in \mathcal{O}_K[x]$ (α entero, otras raíces son enteras $(x-\alpha)(x-\alpha_2)\cdots(x-\alpha_r)$ → coef's son enteros)

$$\overline{g(x)} \equiv \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r} \pmod{\mathfrak{P}} \qquad \mathcal{O}_K/\mathfrak{P} = \mathbb{F}_{p^t}$$

Entonces $\mathfrak{P}\cdot\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, donde $\mathfrak{q}_i = \langle \mathfrak{P}, g_i(\alpha)\rangle_{\mathcal{O}_L}$

(elijo $g_i(x) \in \mathcal{O}_K[x]$ t.q. al reducir sea $\bar{g}_i$), y

además, $f(\mathfrak{q}_i|\mathfrak{P}) = \deg(\bar{g}_i)$.

Demo: $g_i \in \mathcal{O}_K[x]$ / $g_i \equiv \bar{g}_i \pmod{\mathfrak{P}}$

$\mathcal{O}_i = \langle P, g_i(\alpha) \rangle = P \cdot \mathcal{O}_K + (g_i(\alpha))_{\mathcal{O}_L}$

$x \longrightarrow \alpha$

$\varphi: \mathcal{O}_K[x] \longrightarrow \mathcal{O}_L \longrightarrow \mathcal{O}_L / \langle P, g_i(\alpha) \rangle$

$N_{\mathcal{O}}(\mathcal{O}) \supseteq \langle P, g_i(x) \rangle$

$\mathrm{Im}(\varphi) \cong \mathcal{O}_K[x] / \langle P, g_i(\alpha) \rangle = \overbrace{\left(\mathcal{O}_K[x]/P\right)/\bar{g}_i(x)}^{\text{cuerpo.}}$

$\bar{g}_i$ irreducible

$\rightarrow$ $N_{\mathcal{O}}(\mathcal{O}) = \langle P, g_i(\alpha) \rangle$ mxl $\Rightarrow$ primo (en particular

$\hookrightarrow$ $N_{\mathcal{O}}(\mathcal{O}) =$ todo $\langle P, g_i(\alpha) \rangle = \mathcal{O}_L$ $\left[f(\bar{g}_i \mid \bar{P}) = g_r(g_i) \right)$

Partimos $\{\mathcal{O}_1, \dots, \mathcal{O}_r\} = \{\mathcal{O}_1, \dots, \mathcal{O}_t\} \cup \{\mathcal{O}_{t+1}, \dots, \mathcal{O}_r\}$

primos todos

Vale: ① $\mathcal{O}_i + \mathcal{O}_j = \mathcal{O}_L$ (coprimos) $1 \le i, j \le t$

Como $\bar{g}_i$ y $\bar{g}_j$ son distintos (e irreducibles)

$\Rightarrow$ generan todo $\mathcal{O}_{K/P}[x]$, $1 = \bar{g}_i \bar{f} + \bar{g}_j \cdot \bar{h}$

$1 = g_i f + g_j h$ módulo $P \Rightarrow \mathcal{O}_i + \mathcal{O}_j = \mathcal{O}_L$

② $P \cdot \mathcal{O}_L \mid \mathcal{O}_1^{e_1} \cdots \mathcal{O}_r^{e_r}$. Recordar de dividir

contener. Luego $\langle p, \mathfrak{q}_1 \rangle^2 = \langle \underbrace{p^2}_{\in \mathfrak{P}\mathcal{O}_L}, p\cdot\mathfrak{q}_1, \mathfrak{q}_1^2 \rangle$

$$\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} = \langle \mathfrak{P}, g_1(\alpha) \rangle^{e_1} \cdots \langle \mathfrak{P}, g_r(\alpha) \rangle^{e_r}$$

$$\subset \langle \mathfrak{P}, \underbrace{g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r}}_{g(\alpha) \bmod \mathfrak{P}} \rangle \subset \mathfrak{P}\mathcal{O}_L$$

Luego, $\mathfrak{P}\cdot\mathcal{O}_L = \mathfrak{q}_1^{\alpha_1} \cdots \mathfrak{q}_t^{\alpha_t}$, $0 \le \alpha_i \le e_i$

$$n = [L:K] = \sum_{i=1}^{t} \alpha_i \cdot f(\mathfrak{q}_i|\mathfrak{P}) \le \sum_{i=1}^{t} e_i \deg(\bar{g}_i(\alpha))$$

$$\le \sum_{i=1}^{r} e_i \cdot \deg(g_i(x)) = n \rightsquigarrow \boxed{t = r} \quad \boxed{\alpha_i = e_i}$$ ∎

Recordar (vez pasada) $K = \mathbb{Q}$, $L = \mathbb{Q}[x]/(x^3 - x + 2)$

$\mathcal{O}_L = \mathbb{Z}[\alpha]$, α raíz de $x^3 - x + 2$

$p = 11$, $x^3 - x + 2 \equiv (x+3)(x^2 + 8x + 11)$

$(11)\cdot\mathcal{O}_L = \langle 11, \alpha + 3 \rangle \cdot \langle 11, \alpha^2 + 8\alpha + 11 \rangle$

$f = 1$ $\quad$ $f = 2$

Veremos: esto implica $L/\mathbb{Q}$ no es Galois.

Teo: Si $K/\mathbb{Q}$ finita, $p \in \mathbb{Z}$, p ramifica en K $\iff$ $p \mid \mathrm{disc}(K)$. En particular, hay un número finito de primos ramificados.

Obs: si $\mathcal{O}_K = \mathbb{Z}[\alpha] \rightsquigarrow \operatorname{disc}(\mathcal{O}_K) = \pm N_{K/\mathbb{Q}}(m'_\alpha(\alpha))$

$\operatorname{disc}(m_\alpha(X))$

$= \prod (\alpha_i - \alpha_j)^2$. si $p \in \mathbb{Z}$, $p\cdot\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots$

$e_i > 1 \iff$ al factorizar $\bar{m}_\alpha(X)$ hay raíces repetidas (alguno) en $\overline{\mathbb{F}_p}$

$\iff \operatorname{disc}(\bar{m}_\alpha(X)) = 0$. Pero $\operatorname{disc}(\bar{m}_\alpha(X)) \equiv \operatorname{disc}(m_\alpha(X))(p)$

Demo (Teo): si $p\cdot\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, por el T.C.R.

$\mathcal{O}_K/p\mathcal{O}_K \simeq \overbrace{\mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}}^{d}$ es un $\mathbb{Z}/p$-módulo ($\overline{\mathbb{F}_p}$)

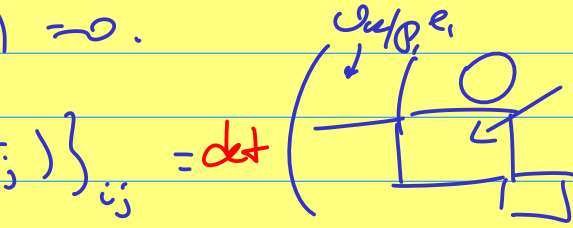
$\operatorname{disc}(\mathcal{O}_K/p\mathcal{O}_K) = \prod_{i=1}^{r} \operatorname{disc}(\mathcal{O}_K/\mathfrak{p}_i^{e_i})$

$\operatorname{disc}(\mathcal{O}_K)\ (p)$ $\qquad$ $\uparrow$ $\overline{\mathbb{F}_p}$-e.v.

$\{v_1 \to v_t\}$ de $\mathcal{O}_K/\mathfrak{p}_1^{e_1} \rightsquigarrow$ en $\mathcal{O}_K/p\mathcal{O}_K$

$\{w_1, \ldots, w_s\}$ base de $\mathcal{O}_K/\mathfrak{p}_2^{e_2} \to$ $(v_1, 0, \ldots 0)$, $(v_2, 0, \to 0)$, $\{0, w_2, 0 \ldots 0)$, $(0, w_2, 0, \ldots 0)$

$\operatorname{Tr}(v_i \cdot w_j) = 0$.

$\{\operatorname{Tr}(v_i v_j)\}_{ij} = \det$ 

$=$

$\det(\operatorname{Tr}(v_i^{(1)} \cdot v_j^{(1)})) \cdot \det(\operatorname{Tr}(v_i^{(2)} \cdot v_j^{(2)}) \cdots$

$\operatorname{disc}(\mathcal{O}_K/\mathfrak{p}_1^{e_1})$ $\qquad$ $\operatorname{disc}(\mathcal{O}_K/\mathfrak{p}_2^{e_2}) \cdots$

$\mathbb{F}_p$-e.v.

$\Leftarrow$) Si $e_1 = 1$, $\operatorname{disc}\left(\mathcal{O}_K/\mathfrak{p}_1^{e_1}\right) = \operatorname{disc}\left(\mathcal{O}_K/\mathfrak{p}_1\right) \neq 0$

cuerpo

$\mathbb{F}_p$

pues $\begin{cases} \to \text{hicimos } \circledast \\ \to L = \mathcal{O}_K/\mathfrak{p}_1 \text{ cpo finito.} \Rightarrow \operatorname{disc}(\,) = \end{cases}$

$\mathbb{F}_p[t]/f(t)$ c. irred.

$N_{L/K}(f'(t)) \neq 0.$

$\neq 0$ por ser separable.

$\operatorname{disc}(\mathcal{O}_K \bmod \mathfrak{p})$.

$\Rightarrow \operatorname{disc}\left(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K\right) \neq 0.$

$\circledast$ L/K ext. de cuerpos, $n = [L:K]$,

$\operatorname{disc}(\{v_1, \dots, v_n\}) = 0 \iff \{v_1, \dots, v_n\}$ son l.d.

$\Rightarrow$) $\operatorname{disc}\left(\mathcal{O}_K/\mathfrak{p}^r\right) = 0$. si $r > 1$.

si $r>1$, tiene elementos nilpotentes.

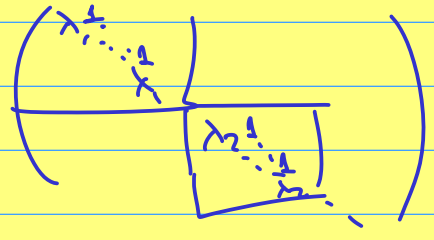
$(\pi \neq 0$ t.f. $\pi^N = 0)$, $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, $\pi \neq 0, \pi^2 = 0$.

Si π es nilpotente $\Rightarrow a \cdot \pi$ es nilpotente $\forall a$.

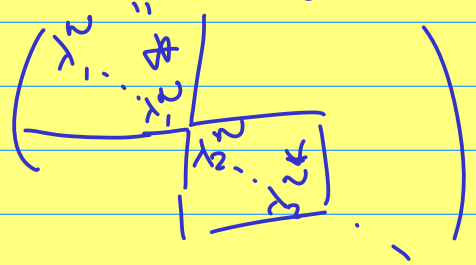
$\operatorname{Tr}_{K/\mathbb{Q}}(\pi) = ?$ $\quad \mathcal{O}_K/\mathfrak{p}^r$ como $\mathbb{F}_p$-e.v.

$m_\pi : \mathcal{O}_K/\mathfrak{p}^r \to \mathcal{O}_K/\mathfrak{p}^r$ (miremos en $\overline{\mathbb{F}_p}$)

$[m_\pi]_{\mathcal{B}} = T$ forma de Jordan



$$[m_\pi]_{\beta}^{N} = [m_{\pi^N}]_{\beta} = 0.$$



$\Rightarrow \lambda_i^N = 0 \Rightarrow \boxed{\lambda_i = 0}$

$\Rightarrow Tr(m_\pi) = 0.$

Luego, si en la base de $\mathcal{O}_K/\mathfrak{p}^r$ hay algún elto nilpotente (v_i), $disc(v_1, \dots, v_t) = \det(Tr(v_i v_j))$

$$= \det\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = 0$$

$\dim_{\mathbb{F}_p} \mathcal{O}_K/\mathfrak{p} \Leftarrow |\mathcal{O}_K/\mathfrak{p}| = p^s$ eltos, $|\mathcal{O}_K/\mathfrak{p}^r| = p^{s \cdot r}$

"s"

En particular, $\{v_1, \dots, v_{s+1}, \dots\}$ base de $\mathcal{O}_K/\mathfrak{p}^r$

$\{v_1, \dots, v_{s+1}\}$ en $\mathcal{O}_K/\mathfrak{p}^r$, mira su reducido módulo $\mathfrak{p}$

$\bar{v}_1, \dots, \bar{v}_{s+1}$ en $\mathcal{O}_K/\mathfrak{p} \Rightarrow$ son l.d., $\bar{v}_1 = \lambda_2 \bar{v}_2 + \cdots + \lambda_s \bar{v}_s$

$\lambda_i \in \mathbb{F}_p$ $\quad \tilde{v}_1 = v_1 - \lambda_2 v_2 - \cdots - \lambda_s v_s$

$\{ \underset{\neq 0}{\tilde{v}_1}, v_2, \dots \}$ pero $\tilde{v}_1 = 0 \bmod \mathfrak{p}$

$\Rightarrow$ nilpotente. ∎

Cono 0: en $K/\mathbb{Q}$ ramifican finitos primos.

Cono: si L/K finita de cuerpos, hay finitos

ideales primos que ramifican.

D/ ramifican finitos primos

$$\begin{array}{ccc} L & \mathcal{O}_L\cdot\mathcal{O}_L = \mathcal{O}_1^{e_1}\cdots\mathcal{O}_r^{e_r} & \text{Si } \mathcal{O} \text{ ramifica en } L/K \\ | & | & \\ K & \mathcal{O} & \Rightarrow \mathcal{O}\cap\mathbb{Z} \text{ ramifica en } L/\mathbb{Q} \\ | & | & \\ \mathbb{Q} & p=\mathcal{O}\cap\mathbb{Z} & \Rightarrow \text{en } L/K \text{ ramifican finitos primos.} \end{array}$$

□

Factorización y teoría de Galois

Supongamos que L/K es Galois. $Gal(L/K)=\{\sigma_1,\dots,\sigma_d\}$

$d=[L:K]$. Si $p\subset\mathcal{O}_K$ primo, $\sigma(p)=p\ \forall\sigma\in Gal(L/K)$

$\sigma(L)=L$, y si α es algebraico, $\sigma(\alpha)$ es algebraico.

Luego $\sigma(\mathcal{O}_L)=\mathcal{O}_L \Rightarrow \sigma(p\cdot\mathcal{O}_L)=p\cdot\mathcal{O}_L$

Si $p\cdot\mathcal{O}_L = \mathcal{P}_1^{e_1}\cdots\mathcal{P}_r^{e_r}$

aplico σ

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

Pero, $\sigma:\ \underbrace{\mathcal{O}_L/\mathcal{P}_1}_{\text{cuerpo}} \xrightarrow{\text{biyección}} \underbrace{\mathcal{O}_L/\sigma(\mathcal{P}_1)}_{\text{cuerpo}}$, $\sigma(\mathcal{P}_1)$ ideal primo.

$\Rightarrow \sigma(\mathcal{P}_1)=\mathcal{P}_i$ (alguno de los otros), en particular,

$$e(\mathcal{P}|p)=e(\sigma(\mathcal{P})|p) \quad \text{y} \quad f(\mathcal{P}|p)=f(\sigma(\mathcal{P})|p)$$

Pregunta: ¿es transitiva la acción? dados $\mathfrak{P}_i, \mathfrak{P}_j$ en la factorización de $p.\mathcal{O}_L$, $\exists \sigma \in Gal(L/K)$ t.f. $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.

Teo: la acción de $Gal(L/K)$ en los primos que dividen a $p.\mathcal{O}_L$ es transitiva.

D/ Supongamos que no: $\exists \mathfrak{P}_1, \mathfrak{P}_2$ que dividen a $p.\mathcal{O}_L$ tales que $\sigma(\mathfrak{P}_1) \neq \mathfrak{P}_2 \quad \forall \sigma \in Gal(L/K)$

$\{$ Primos que dividen a $p\mathcal{O}_L \} = \{ \sigma(\mathfrak{P}_1) \} \cup \{\mathfrak{P}_2\} \dots$

Por el T. C. R., $\exists \alpha \in \mathcal{O}_L$ t.f.

$$\begin{cases} \alpha \equiv 0 \ (\mathfrak{P}_2) \leftarrow \\ \alpha \equiv 1 \ (\sigma(\mathfrak{P}_1)) \quad \forall \sigma \in Gal(L/K) \end{cases} \quad (1)$$

$$N_{L/K}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha) \in \mathcal{O}_K$$

Supongamos $\sigma_1 = id$. $\quad \alpha \cdot \prod_{i=2}^{d} \sigma_i(\alpha) \in \mathfrak{P}_2 \cap \mathcal{O}_K = p\mathbb{Z}$

$\alpha \in \mathfrak{P}_2 \quad \prod_{i=2}^{d} \sigma_i(\alpha) \in \mathcal{O}_L \quad \Rightarrow \mathfrak{P}_1$

$(\ p.\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \ \mathfrak{P}_1 \mid p\mathcal{O}_L \Rightarrow p \in \mathfrak{P}_1 \ )$

Luego $\alpha \cdot \sigma_2(\alpha) \cdots \sigma_r(\alpha) \in \mathfrak{P}_1$. Abs! ($\mathfrak{P}_1$ es primo). ☐

$\alpha \notin \mathfrak{P}_1 \quad \sigma_2(\alpha) \notin \mathfrak{P}_1 \quad \sigma_r(\alpha) \notin \mathfrak{P}_1$

Corolario: Si L/K es Galois, $p \in \mathcal{O}_K$ primo,

p. $Q_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_r^e$, y $f = f(\mathfrak{P}_i | p)$ siempre el mismo. En particular,

$$\boxed{d = [L:K] = e_1 f(\mathfrak{P}_1|p) + \cdots + e_r f(\mathfrak{P}_r|p) = e.f.r}$$

Aplicación: La extensión $\mathbb{Q}[X]/X^3 - X + 2$ no es Galois.

D/ 11 se factoriza como $3 = 1 + 2$ (f_1, f_2)