**Repaso:** $R$ dedekind ($R = \mathcal{O}_K$, $K/\mathbb{Q}$ finita)
$\Rightarrow$ ideales para $R$ tienen fact. única, o sea

$$\mathfrak{a} \subsetneq \mathcal{O}_K,\ \mathfrak{a} \neq 0,\ \mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \text{ forma única.}$$

- **T.C.R:** $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$,

$$\mathcal{O}_K/\mathfrak{a} \xrightarrow{\sim} \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$$

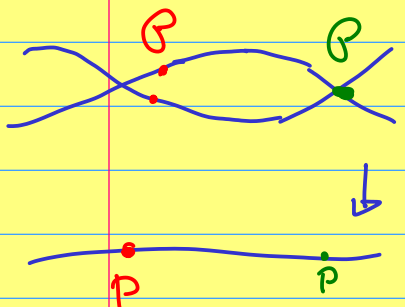
- Si $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a} = \langle \alpha, \beta \rangle_{\mathcal{O}_K}$ (dos generadores bastan)

- Si $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a} \neq 0$, $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$, cumple:

  (1°) Multiplicativa: $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$

  (2°) Si $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, $N((\alpha)) = |\mathcal{O}_K/(\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|$ ($K/\mathbb{Q}$ finita)

## Primos en extensiones




$$\begin{array}{ccc} L & \mathcal{O}_L & \mathfrak{P} \\ | & | & \text{al menos uno } \{ \ | \ \} \text{ único} \\ K & \mathcal{O}_K & \mathfrak{p} \end{array}$$

entender los primos de $L$ en términos de los de $K$.

**Def:** decimos que $\mathfrak{P}$ está sobre $\mathfrak{p}$ o que $\mathfrak{p}$ está debajo de $\mathfrak{P}$ si $\mathfrak{P} \mid \mathfrak{p}.\mathcal{O}_L$ ($\Leftrightarrow \mathfrak{p}.\mathcal{O}_K \subset \mathfrak{P}$)

**Teo:** todo primo no nulo de $\mathcal{O}_L$ está sobre un único ideal primo no nulo de $\mathcal{O}_K$. Recíprocamente, todo primo de $\mathcal{O}_K$ tiene (al menos) un primo de $\mathcal{O}_L$ sobre él.

Demo: (1º) $\mathfrak{P} \cap \mathcal{O}_K = p$, queremos ver que $p$ es primo

$p \neq 0, \mathcal{O}_K$.

· Si $p = \mathcal{O}_K$, $1 \in p \subset \mathfrak{P} \Rightarrow \mathfrak{P} = \mathcal{O}_L$ ✓

· Si $\mathfrak{P} \subset \mathcal{O}_L$, $\alpha \in \mathfrak{P}$, $N_{L/\mathbb{Q}}(\alpha) \in \mathfrak{P}$

$\Rightarrow \mathfrak{P} \cap \mathbb{Z} \neq \{0\} \Rightarrow \mathfrak{P} \cap \mathcal{O}_K \neq \{0\}$ ✓

· $p$ es primo: si $\alpha, \beta \in \mathcal{O}_K$: $\alpha \cdot \beta \in p \Rightarrow \alpha \in p$ ó $\beta \in p$.

$\alpha \cdot \beta \in p \subset \mathfrak{P}$ primo $\Rightarrow \alpha \in \mathfrak{P} \cap \mathcal{O}_K = p$ ✓

(2º) Si $p \subsetneq \mathcal{O}_K$ primo, $p \cdot \mathcal{O}_L$ si es propio,

$p \cdot \mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \Rightarrow \mathfrak{P}_i \mid p \cdot \mathcal{O}_L$

primos arriba de $p$.

¿ $p \cdot \mathcal{O}_L \subsetneq \mathcal{O}_L$? Recordar: $p \subsetneq \mathcal{O}_K$, $\exists \alpha \in K \setminus \mathcal{O}_K$

t.q. $\alpha \cdot p \subset \mathcal{O}_K$. Luego si $p \cdot \mathcal{O}_L = \mathcal{O}_L$,

$(\alpha \cdot p)\mathcal{O}_L \subset \mathcal{O}_K \cdot \mathcal{O}_L = \mathcal{O}_L \Rightarrow \alpha \cdot \mathcal{O}_L = \mathcal{O}_L \Rightarrow \alpha \in \mathcal{O}_L$

$\alpha \cdot (p\mathcal{O}_L)$

$\alpha \cdot \mathcal{O}_L$

en particular es entero algebraico.

$\alpha \in K$ y es entero algebraico $\Rightarrow \alpha \in \mathcal{O}_K$, Abs! ∎

Def: Si $p \subset \mathcal{O}_K$ no nulo, $\mathfrak{P} \mid p\mathcal{O}_L$, el índice de ramificación de $\mathfrak{P}$ sobre $p$, denotamos $e(\mathfrak{P}|p)$, es el exponente de $\mathfrak{P}$ en la factorización de $p \cdot \mathcal{O}_L$.

$e(\mathfrak{P}_i|p)$

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

Decimos que un primo $p$ ramifica en $L/K$ si $\exists\, \mathfrak{P}$ arriba de él tal que $e(\mathfrak{P}|p) > 1$.

Ejemplos: $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{3})$, $\mathcal{O}_L = \mathbb{Z}[\sqrt{3}]$, $\mathcal{O}_K = \mathbb{Z}$

- 3 en $\mathbb{Z}$, $3.\mathbb{Z}[\sqrt{3}] = (\sqrt{3})^2_{\mathcal{O}_L}$ ← ramifica.
  $f(\sqrt{3}|3) = 1$
- 5 en $\mathbb{Z}$, $\boxed{5.\mathbb{Z}[\sqrt{3}]}$ es primo. $\mathbb{Z}[\sqrt{3}]/\langle 5, 5\sqrt{3}\rangle_{\mathbb{Z}} \simeq$

$\{5, \dots, 5\} \simeq \mathbb{Z}/5[t]/(t^2-3)$ ¿$t^2-3$ irreducible en $\mathbb{F}_5[t]$?

Sí: no tiene raíces.

no ramifica

$f(5\mathcal{O}_L|5) = 2$

- 11 en $\mathbb{Z}$, $11.\mathbb{Z}[\sqrt{3}] = \underbrace{(1+2\sqrt{3})}_{\mathfrak{P}}\,\underbrace{(1-2\sqrt{3})}_{\overline{\mathfrak{P}}}$

no ramifica. $f(1+2\sqrt{3}|11) = 1 = f(1-2\sqrt{3}|11)$

- 2 en $\mathbb{Z}$, $2.\mathbb{Z}[\sqrt{3}] = (1+\sqrt{3})(1-\sqrt{3}) = (1+\sqrt{3})^2$

ramifica. $= -(1-\sqrt{3})\boxed{(2+\sqrt{3})}$ unidad. $f(2+\sqrt{3}|2) = 1$

Siguiendo la misma notación:

$$\begin{array}{ccccc} L & \supset & \mathcal{O}_L & \supset & \mathfrak{P} \\ | & & | & & | \\ K & \supset & \mathcal{O}_K & \supset & p \end{array}$$

$\mathcal{O}_K \hookrightarrow \mathcal{O}_L \twoheadrightarrow \mathcal{O}_L/\mathfrak{P}$ induce $\varphi: \mathcal{O}_K \to \mathcal{O}_L/\mathfrak{P}$

$N_{\mathcal{O}}(\mathfrak{P}) = \mathfrak{P} \cap \mathcal{O}_K = p \Rightarrow \tilde{\varphi}: \mathcal{O}_K/p \hookrightarrow \mathcal{O}_L/\mathfrak{P}$ (cuerpos finitos)

( $B_1 \subset B_2$ finitos $|B_2| = |B_1|^{[B_2 : B_1]}$ )

En particular, podemos mirar $[\mathcal{O}_L/\mathcal{P} : \mathcal{O}_K/p] = f(\mathcal{P}|p)$

llamamos el grado de inercia del primo.

Obs: $|\mathcal{O}_L/\mathcal{P}| = |\mathcal{O}_K/p|^{f(\mathcal{P}|p)}$

$N(\mathcal{P}) = N(p)^{f(\mathcal{P}|p)}$

Obs2: Tanto el grado de ramificación como el de inercia son multiplicativos en torres.

$$\begin{array}{ccc} L & \mathcal{O}_L & \mathcal{P} \\ | & | & | \\ M & \mathcal{O}_M & \mathfrak{P} \\ | & | & | \\ K & \mathcal{O}_K & p \end{array}$$

1. $e(\mathcal{P}|p) = e(\mathcal{P}|\mathfrak{P}) \cdot e(\mathfrak{P}|p)$
2. $f(\mathcal{P}|p) = f(\mathcal{P}|\mathfrak{P}) \cdot f(\mathfrak{P}|p)$

2. $[\mathcal{O}_L/\mathcal{P} : \mathcal{O}_K/p] = [\mathcal{O}_L/\mathcal{P} : \mathcal{O}_M/\mathfrak{P}] \cdot [\mathcal{O}_M/\mathfrak{P} : \mathcal{O}_K/p]$

(ejercicio guía 1).

1. $p \cdot \mathcal{O}_M = \mathfrak{P}^{e(\mathfrak{P}|p)} \cdot \ldots$ (otros primos)

$\Rightarrow p \cdot \mathcal{O}_L = (p \cdot \mathcal{O}_M) \cdot \mathcal{O}_L = (\mathfrak{P}^{e(\mathfrak{P}|p)} \cdot \mathcal{O}_L) \cdot \ldots$ (otros primos arriba)

$\mathcal{P}^{e(\mathcal{P}|p)} \cdot \ldots = (\mathcal{P}^{e(\mathcal{P}|\mathfrak{P})})^{e(\mathfrak{P}|p)}$

(otros primos)

por T. U. $e(\mathcal{P}|p) = e(\mathcal{P}|\mathfrak{P}) \cdot e(\mathfrak{P}|p)$ ∎

Teo: si $K \subset L$, $n = [L:K]$, $p$ primo de $\mathcal{O}_K$,

$p \cdot \mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$, $e_i = e(\mathcal{P}_i|p)$

entonces: $e(\mathfrak{P}_1|p).f(\mathfrak{P}_1|p)+\cdots+e(\mathfrak{P}_r|p).f(\mathfrak{P}_r|p)=n.$

Demo: $N(p.\mathcal{O}_L) = N(\mathfrak{P}_1)^{e_1}\cdots N(\mathfrak{P}_r)^{e_r}$ ⊛ =

lema → " $N(p)^{[L:k]}$

$N(\mathfrak{P}_i) = |\mathcal{O}_L/\mathfrak{P}_i| =$

$= |\mathcal{O}_k/p|^{f(\mathfrak{P}_i|p)} = N(p)^{f(\mathfrak{P}_i|p)}$

⊛ $= N(p)^{e(\mathfrak{P}_1|p).f(\mathfrak{P}_1|p)} \cdots N(p)^{e(\mathfrak{P}_r|p).f(\mathfrak{P}_r|p)} =$

$= N(p)^{e(\mathfrak{P}_1|p)f(\mathfrak{P}_1|p)+\cdots+e(\mathfrak{P}_r|p)f(\mathfrak{P}_r|p)}$

$= N(p)^{[L:k]}$ ∎

Lema: Si $\mathfrak{a} \subset \mathcal{O}_k$, $N(\mathfrak{a}.\mathcal{O}_L) = N(\mathfrak{a})^{[L:k]}$

D/ Podemos suponer $\mathfrak{a} = p$ primo. $\mathcal{O}_L/p.\mathcal{O}_L$ es un e.v. sobre $\mathcal{O}_k/p$ = cuerpo. $\Rightarrow |\mathcal{O}_L/p.\mathcal{O}_L| = N(p)^m$

$m = \dim_{\mathcal{O}_k/p}(\mathcal{O}_L/p\mathcal{O}_L)$. Objetivo: $m=[L:K]$.

L ⊃ $\mathfrak{P}$ Como p primo de $\mathcal{O}_k$, $N(p) = q^t$, $t \in \mathbb{N}$,

K ⊃ p primos $q = p.\cap \mathbb{Z}$, $\mathcal{O}_k/p$ es un $\mathbb{Z}/q$-e.v.

$\mathbb{Q}$ ⊃ q

$q.\mathcal{O}_k = p^c.\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$ Afirmo: los $\mathfrak{P}_i$'s son todos los ideales primos de norma potencias de q.

Sea $\alpha \in \mathfrak{P}|p^2$, $\alpha \notin \mathfrak{P}_2, \ldots, \alpha \notin \mathfrak{P}_r$ (por T.C.R. existe $(\alpha) \not\subset \mathfrak{P}_2 \Rightarrow \mathfrak{P}_2 \nmid (\alpha)$

un tal elemento). En particular, $\alpha \in \mathfrak{p}$, $(\alpha) \subset \mathfrak{p}$, o sea

$$\mathfrak{p} \mid (\alpha) \Rightarrow (\alpha) = \overline{\mathfrak{p}} \cdot \overbrace{\mathfrak{b}}^{\mathfrak{P}\mathfrak{B}}, \quad \mathfrak{q} \mid N(\mathfrak{B})$$

$$\mathfrak{B} = \tilde{\mathfrak{P}}_1^{e_1} \cdots \tilde{\mathfrak{P}}_r^{e_r}, \quad N(\mathfrak{B}) = N(\tilde{\mathfrak{P}}_1)^{e_1} \cdots N(\tilde{\mathfrak{P}}_r)^{e_r}$$

$\mathfrak{q} \mid N(\tilde{\mathfrak{P}}_1)$, pues, los ideales primos de norma divisible por $\mathfrak{q}$ son $\{\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_r\}$, pero $\mathfrak{P}_2 \mid (\alpha), \dots, \mathfrak{P}_r \mid (\alpha)$

$\Rightarrow \mathfrak{P}_2 \mid \mathfrak{B}, \dots, \mathfrak{P}_r \mid \mathfrak{B}$. A la vez, como $\mathfrak{p}^2 \nmid (\alpha)$, $\mathfrak{p} \mid \mathfrak{B}$.

$$N(\alpha \cdot \mathcal{O}_L) = N(\mathfrak{p} \cdot \mathcal{O}_L \cdot \mathfrak{B}\mathcal{O}_L) = N(\mathfrak{p}\mathcal{O}_L) \cdot N(\mathfrak{B}\mathcal{O}_L)$$
$$\| \qquad \| \qquad \text{coprimo con } \mathfrak{q}$$
$$N(\mathfrak{p})^m \cdot N(\mathfrak{B}\mathcal{O}_L)$$

$$|N_{L/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(N_{L/K}(\alpha))| = |N_{K/\mathbb{Q}}(\alpha^{[L:K]})| =$$

$$= |N_{K/\mathbb{Q}}(\alpha)|^{[L:K]} = |N((\alpha))|^{[L:K]}$$

Miremos la potencia de $\mathfrak{q}$ en ambos lados:

$$v_{\mathfrak{q}}(N(\alpha)^{[L:K]}) = v_{\mathfrak{q}}(N(\mathfrak{p})^m) + v_{\mathfrak{q}}(N(\mathfrak{B}\mathcal{O}_L))$$
$$\| \qquad \| \qquad \| 0$$

$$[L:K]\, v_{\mathfrak{q}}(N(\alpha)) = m \cdot v_{\mathfrak{q}}(N(\mathfrak{p}))$$

En $\mathcal{O}_K$, $\alpha = \mathfrak{p} \cdot \mathfrak{b} \Rightarrow N(\alpha) = N(\mathfrak{p}) \cdot \underbrace{N(\mathfrak{b})}_{\mathfrak{q}\mathbb{X}} \Rightarrow$

$$\Rightarrow \boxed{v_{\mathfrak{q}}(N(\alpha)) = v_{\mathfrak{q}}(N(\mathfrak{p}))} \Rightarrow \boxed{m = [L:K]} \quad \square$$

Obs: similar a $\nearrow$ $S = \mathcal{O}_K \setminus \mathfrak{p}$, $(\mathcal{O}_K)_S$ localizado, es DIP

P. $(\mathcal{O}_K)_S = (d)_{(\mathcal{O}_K)_S}$. $\mathcal{O}_K = \bigcap_P (\mathcal{O}_K)_S$

---

Problema: ¿cómo encontrar primos de manera "eficiente"?

O sea dado $p \subset \mathcal{O}_K$ primo, hallar $p\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$

Hipótesis: $\begin{matrix} L & \mathcal{O}_L \\ | & | \\ K & \mathcal{O}_K \supset p \end{matrix}$, $\alpha \in \mathcal{O}_L$ que genere la extensión, $L = K[\alpha]$.

Sea $p \subset \mathcal{O}_K$ primo, $N(p) = q^t$, $q \times [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$

$\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$, no tiene por qué valer la igualdad.

Pero ambos son $\mathbb{Z}$-módulos de igual rango $\Rightarrow \mathcal{O}_L/\mathcal{O}_K[\alpha]$ es finito. $q \times |\mathcal{O}_L/\mathcal{O}_K[\alpha]| = [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$

Sea $g = m_\alpha(X) \in K[X]$, en realidad $m_\alpha(X) \in \mathcal{O}_K[X]$

pues, $m_\alpha(X) = (X-\alpha)\cdot(X-\alpha_2)\cdots$, $\alpha_i = \sigma(\alpha)$,

$\{\sigma_1, \dots, \sigma_d\} = \mathrm{Hom}_K(L, \mathbb{C})$, $\alpha_i$ son enteros algebraicos.

$\Rightarrow m_\alpha(X) = X^d - X^{d-1}\underbrace{(\alpha_1 + \cdots + \alpha_d)}_{\in K \text{ y enteros} \Rightarrow \in \mathcal{O}_K} + X^{d-2}\underbrace{(\sum \alpha_i\alpha_j)}_{\in K \text{ y enteros} \Rightarrow \in \mathcal{O}_K} + \cdots$

Podemos mirar $\overline{g} \equiv \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r} \pmod{p}$ $\mathcal{O}_K/p[X]$ cpo finito.

Sean $g_1, \dots, g_r \in \mathcal{O}_L[x]$, $gr(g_i) = gr(\overline{g}_i)$ y tq

$$g_i \equiv \overline{g}_i \pmod{p}.$$

Teo: en estas hipótesis, sea $\mathcal{O}_i = \langle p, g_i(\alpha) \rangle_{\mathcal{O}_L}$

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

y más aún, $f(\mathcal{O}_i | p) = gr(g_i)$.

Ejemplo: $K = \mathbb{Q}$, $L/K$, $L = \mathbb{Q}[\alpha]$, $\alpha$ raíz de

$g(x) = x^3 - x + 2$. $\mathcal{O}_L \overset{?}{=} \mathbb{Z}[\alpha]$ (¿cuál es el índice?)

$$disc(\mathbb{Z}[\alpha]) = -104 = -2^3 \cdot 13 \qquad disc(\mathbb{Z}[\alpha]) = disc(\mathcal{O}_L)\cdot[\mathcal{O}_L : \mathbb{Z}[\alpha]]^2$$

Luego, $|\mathcal{O}_L / \mathbb{Z}[\alpha]| = 1$ ó $2$.

Podemos mirar $p \neq 2$ (en realidad, $\mathbb{Z}[\alpha] = \mathcal{O}_L$).

- $p = 3$, ¿cómo se factoriza? $x^3 - x + 2 \equiv$ irred. $(\mathrm{mod}\ 3)$

$\Rightarrow (3)$ es primo en $\mathcal{O}_L$ $\quad f(3\mathcal{O}_L | 3) = 3$.

- $p = 11$, en $-3$, $-27 + 3 + 2$

$$\bar{x}^3 - \bar{x} + 2 \equiv (\bar{x}+3)(\bar{x}^2 + 8\bar{x} + 11) \quad (11)$$

$\uparrow$ irred.

Obs: esta factorización implica $L/\mathbb{Q}$ no es Galois.

$\Rightarrow$ $11\cdot\mathcal{O}_L = \langle 11, \alpha + 3\rangle_{\mathcal{O}_L} \cdot \langle 11, \alpha^2 + 8\alpha + 11\rangle_{\mathcal{O}_L}$

$f(11 | 11) = 1 \qquad f(11 | 11) = 2$

$(1\cdot 1 + 2\cdot 1 = 3 = [K : \mathbb{Q}])$.

- $p = 13$? (ejercicio)