Repaso: $K/\mathbb{Q}$ finita, vimos

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ es entero algebraico}\}$$

$\exists\, p(x) \in \mathbb{Z}[x]$ mónico, $p(\alpha) = 0$.

$\mathcal{O}_K$ es un anillo. ¿Cómo calcularlo? (dar un cjto de generadores como $\mathbb{Z}$-módulo) ¿Vale que $\mathcal{O}_K$ es un $\mathbb{Z}$-mód.f.g.?

La última clase: $d = [K:\mathbb{Q}]$, dados $\{\alpha_1, \dots, \alpha_d\}$ en K,

discriminante $\boxed{\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det(\sigma_i(\alpha_j))^2 = \det(\operatorname{Tr}(\alpha_i \alpha_j))}$

donde $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_d\}$

Si α entero algebraico, $\operatorname{Tr}(\alpha) \in \mathbb{Z} \to \{\alpha_1, \dots, \alpha_d\}$ son enteros

$\operatorname{disc}(\alpha_1, \dots, \alpha_d) \in \mathbb{Z}$. Además,

(1°) $\operatorname{disc}(\alpha_1, \dots, \alpha_d) = 0 \iff \{\alpha_1, \dots, \alpha_d\}$ es l.d.

(2°) $\operatorname{disc}(\alpha/n, \alpha_2, \dots, \alpha_d) = \frac{1}{n^2} \operatorname{disc}(\alpha_1, \dots, \alpha_d)$

$\rightsquigarrow$ Teo: $\mathcal{O}_K$ es un $\mathbb{Z}$-mód. libre de rango d.

D/ $\{\alpha_1, \dots, \alpha_d\}$ base de K como $\mathbb{Q}$-e.v., α_i enteros algebraicos. Si $\langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Z}} \subsetneq \mathcal{O}_K$, $\exists\, \beta \in \mathcal{O}_K \setminus \langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Z}}$

$$\langle \alpha_1, \dots, \alpha_d, \beta \rangle_{\mathbb{Z}} = \langle \gamma_1, \dots, \gamma_d \rangle_{\mathbb{Z}}$$

$|\operatorname{disc}(\gamma_1, \dots, \gamma_d)| < |\operatorname{disc}(\alpha_1, \dots, \alpha_d)|$. ∎

Obs: $\beta \in K = \langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Q}}$, $\beta = \frac{a_1\alpha_1 + \dots + a_d\alpha_d}{k}$

$k \times a_i$, $a_i \in \mathbb{Z}$. $\rightsquigarrow$ $\operatorname{disc}(\gamma_1, \dots, \gamma_d) = \frac{\operatorname{disc}(\alpha_1, \dots, \alpha_d)}{k^2}$

Luego $\operatorname{disc}(\alpha_1, \dots, \alpha_d) = A^2 \cdot B$, $A, B \in \mathbb{Z}$, los únicos denominadores que podían faltar agregar dividen a A.

Ejemplos: 1). K cuerpo cuadrático, $K = \mathbb{Q}(\sqrt{m})$

$m \in \mathbb{Z}$, libre de cuadrados. Vimos:

$$\mathcal{O}_K = \begin{cases} \langle 1, \sqrt{m} \rangle & \text{si } m \not\equiv 1 \ (4) \quad \operatorname{disc}(\mathcal{O}_K) = 4m \\ \langle 1, \frac{1+\sqrt{m}}{2} \rangle & \text{si } m \equiv 1 \ (4) \quad \operatorname{disc}(\mathcal{O}_K) = m. \end{cases}$$

$$\operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}(1, \sqrt{m}) = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = (-2\sqrt{m})^2 = 4m.$$

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} = 4m.$$

$$\operatorname{disc}\left(1, \tfrac{1+\sqrt{m}}{2}\right) = \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = \left(\left(\tfrac{1-\sqrt{m}}{2}\right) - \left(\tfrac{1+\sqrt{m}}{2}\right)\right)^2$$

$$= (-\sqrt{m})^2 = m$$

En cualquier caso, $\boxed{\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \left(\frac{D + \sqrt{D}}{2}\right)}$, $D \equiv 0, 1 \ (4)$ el discriminante de $\mathcal{O}_K$.

Def: si $K/\mathbb{Q}$ finita, definimos el discriminante de K

como $\operatorname{disc}(\mathcal{O}_K) = \Delta(\mathcal{O}_K) = \operatorname{disc}(\alpha_1, \dots, \alpha_d)$, donde $\mathcal{O}_K = \langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Z}}$. $(d = [K:\mathbb{Q}])$.

Prop: el discriminante está bien definido.

D/ Si $\mathcal{O}_K = \langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Z}} = \langle \beta_1, \dots, \beta_d \rangle_{\mathbb{Z}}$.
(α: base, β: base)

Sea M la matriz de "cambio de base", $M \in M_{d\times d}(\mathbb{Z})$.

$M = C_{\beta'\beta}$, además, $M^{-1} = C_{\beta\beta'} \in M_{d\times d}(\mathbb{Z})$

Luego $M \in GL_d(\mathbb{Z})$. En particular, $\det(M) = \pm 1$.
pues $M \cdot M^{-1} = Id \Rightarrow \underbrace{\det(M)}_{\in\mathbb{Z}} \cdot \underbrace{\det(M)^{-1}}_{\in\mathbb{Z}} = \det(Id) = 1$

$$\operatorname{disc}(\beta_1, \dots, \beta_d) = \det \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_d(\beta_1) \\ \vdots & & \\ \sigma_1(\beta_d) & \cdots & \sigma_d(\beta_d) \end{pmatrix}^2 = \det\left(M \cdot \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_d(\alpha_1) \\ \vdots & & \\ \sigma_1(\alpha_d) & \cdots & \sigma_d(\alpha_d) \end{pmatrix}\right)^2$$

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix} = M \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix}, \quad \sigma_i \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}), \qquad \det(M)^2 \cdot \det(\sigma_i(\alpha_j))^2 = \operatorname{disc}(\alpha_1, \dots, \alpha_d)$$

$$\beta_i = \underbrace{a_1}_{\in\mathbb{Z}}\alpha_1 + \cdots + \underbrace{a_d}_{\in\mathbb{Z}}\alpha_d \qquad \sigma_i(\beta_i) = a_1\sigma_i(\alpha_1) + \cdots + a_d\sigma_i(\alpha_d)$$

Def: decimos que $\mathcal{O}_K$ es monogénica si $\exists\, \alpha \in \mathcal{O}_K$ t.q.

$\mathcal{O}_K = \mathbb{Z}[\alpha]$, o sea $\mathcal{O}_K = \langle 1, \alpha, \dots, \alpha^{d-1} \rangle_{\mathbb{Z}}$.

Ejemplo: cuerpos cuadráticos.

Prop: si $\alpha \in K$ que genere $K/\mathbb{Q}$ ($K = \mathbb{Q}[\alpha]$),

$m_\alpha(X)$ es mínimal, entonces

$$\operatorname{disc}(1, \alpha, \dots, \alpha^{d-1}) = \varepsilon \, N_{K/\mathbb{Q}}(m'_\alpha(\alpha)), \text{ donde}$$

$$\varepsilon = \begin{cases} 1 & \text{si } d \equiv 0, 1 \ (4) \\ -1 & \text{si } d \equiv 2, 3 \ (4). \end{cases}$$

Demo: $\operatorname{disc}(1, \dots, \alpha^{d-1}) \det\begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^{d-1} \\ \vdots & & & \\ \sigma_d(1) & \sigma_d(\alpha) & \cdots & \sigma_d(\alpha)^{d-1} \end{pmatrix}^2$

$\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_d\}$

↑ Vandermonde.

$$= \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \boxed{\prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha))} (-1)^r$$

donde $r = \frac{d(d-1)}{2}$, $(-1)^r = \begin{cases} 1 & \text{si } d \equiv 0, 1 \ (4) \\ -1 & \text{si } d \equiv 2, 3 \ (4) \end{cases}$

$$m_\alpha(X) = \prod_{i=1}^{d} (X - \sigma_i(\alpha)) \Rightarrow m'_\alpha(X) = \sum_{i=1}^{d} \prod_{\substack{j=1 \\ j \neq i}}^{d} (X - \sigma_j(\alpha))$$

$$N_{K/\mathbb{Q}} m'_\alpha(\alpha) = \prod_{i=1}^{d} \underbrace{\sigma_i(m'_\alpha(\alpha))}_{\| \ m'_\alpha(\sigma_i(\alpha))} = \prod_{i=1}^{d} \prod_{\substack{j=1 \\ j \neq i}}^{d} (\sigma_i(\alpha) - \sigma_j(\alpha)) \overset{\circledast}{=}$$

Supongamos $\sigma_1(\alpha) = \alpha$.

$$\circledast = \boxed{\prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha))}. \qquad \blacksquare$$

Ej (2) Extensiones ciclotómicas. p primo, $K = \mathbb{Q}[\xi_p]$

donde ξ_p es una raíz p-ésima de la unidad. ($e^{2\pi i/p}$)

$$X^p - 1 = (X-1)(1 + X + \cdots + X^{p-1})$$

irreducible $= m_{\xi_p}(X)$

$\mathbb{Q}[\xi_p]$

$p-1$ | Galois. ξ_p^2 también es raíz.

$\mathbb{Q}$ $\quad\vdots\quad$ ξ_p^{p-1} .. ..

$Gal(\mathbb{Q}[\xi_p]/\mathbb{Q}) \stackrel{?}{=}$ raíces de $m_{\xi_p}(X) = \{\xi_p, \xi_p^2, \dots, \xi_p^{p-1}\}$

$\sigma \in Gal(\mathbb{Q}[\xi_p]/\mathbb{Q})$, $\sigma(\xi_p) = \xi_p^i$

$\varphi: Gal(\mathbb{Q}[\xi_p]/\mathbb{Q}) \to (\mathbb{Z}/p)^\times$ isomorfismo de grupos.

$\sigma \longrightarrow i$ t.q. $\sigma(\xi_p) = \xi_p^i$

$\varphi(\sigma\tau) \Rightarrow (\sigma\tau)(\xi_p) = \sigma(\tau(\xi_p)) = \sigma(\xi_p^j) =$

$\tau(\xi_p) = \xi_p^j$ $\qquad = \sigma(\xi_p)^j = (\xi_p^i)^j = \xi_p^{ij}$.

$$\varphi(\sigma\tau) = \varphi(\sigma)\cdot\varphi(\tau)$$

En particular, $Gal(\mathbb{Q}[\xi_p]/\mathbb{Q})$ es cíclico de orden $p-1$.

$\mathcal{O}_K = ??$ $\qquad disc(K) = ??$

Teo: $\mathcal{O}_K = \mathbb{Z}[\xi_p]$, $disc(K) = \begin{cases} p^{p-2} & p \equiv 1 (4) \\ -p^{p-2} & p \equiv 3 (4) \end{cases}$

Demo: 1. $\mathbb{Z}[\xi_p] = \mathbb{Z}[1 - \xi_p]$

2. AF: $Nm_{k/\mathbb{Q}}(1-\xi_p) = \prod_{i=1}^{p-1}(1-\xi_p^i) = p.$

$$m_{\xi_p}(X) = \frac{X^p-1}{X-1} = 1 + X + \cdots + X^{p-1} = \prod_{i=1}^{p-1}(X-\xi_p^i)$$

Evaluando en $X=1$: $\quad p = \prod_{i=1}^{p-1}(1-\xi_p^i)$

Veamos que $\mathcal{O}_k = \mathbb{Z}[\xi_p]$. $(\mathbb{Z}[\xi_p] \subset \mathcal{O}_k)$

$$\operatorname{disc}(\mathbb{Z}[\xi_p]) = \varepsilon\, Nm\left(m'_{\xi_p}(\xi_p)\right)$$

$$m_{\xi_p}(X)(X-1) = X^p - 1, \text{ derivando,}$$

$$m_{\xi_p}(X)'(X-1) + m_{\xi_p}(X) = pX^{p-1}$$

$\rightsquigarrow$ evalúo en ξ_p $\quad m'_{\xi_p}(\xi_p)(\xi_p-1) = p\xi_p^{p-1}$

norma $\longrightarrow$ $\quad Nm\left(m'_{\xi_p}(\xi_p)\right).\underbrace{Nm(\xi_p-1)}_{p} = \underbrace{Nm(p)}_{p^{p-1}} \cdot Nm(\xi_p^{p-1})$

$Nm(\xi_p^{p-1}) = \prod_{i=1}^{p-1}\xi_p^i = 1$

$$Nm\left(m'_{\xi_p}(\xi_p)\right) = p^{p-2} \Rightarrow \operatorname{disc}(\mathbb{Z}[\xi_p]) = \begin{cases} p^{p-2} & p\equiv 1(4) \\ -p^{p-2} & p\equiv 3(4) \end{cases}$$

Puedo suponer que

Además, si $\alpha \in \mathcal{O}_k \setminus \mathbb{Z}[\xi_p]$, su denominador es p.

Veamos que esto no puede pasar.

Si $\alpha \in \mathcal{O}_k$, $\quad \alpha = \dfrac{a_0 + a_1(1-\xi_p) + a_2(1-\xi_p)^2 + \cdots + a_{p-2}(1-\xi_p)^{p-2}}{p}$ $\quad a_0 \in \{0,\dots,p-1\}$

$\Rightarrow \quad p \mid a_i \,, \; 0 \le i \le p-2 .$

Supongamos fc no, a_i es el primero no divisible por p.

$$\alpha = \frac{a_i(1-\xi_p)^i + \cdots + a_{p-2}(1-\xi_p)^{p-2}}{p} \cdot p \times a_i .$$

$\in \mathcal{O}_K$; $\in \mathcal{O}_K$

$$\Rightarrow \underbrace{\frac{p\cdot\alpha}{(1-\xi_p)^{i+1}}}_{\in \mathcal{O}_K} = \underbrace{\frac{a_i}{(1-\xi_p)}}_{\in \mathcal{O}_K} + \underbrace{\frac{a_{i+1} + a_{i+2}(1-\xi_p) + \cdots + a_{p-2}(1-\xi_p)^{*}}{\in \mathcal{O}_K}}$$

AF: $(1-\xi_p)^i \mid p$ en $\mathbb{Z}[1-\xi_p]$ $\quad (p = (1-\xi_p)^i \cdot \square)$

$0 \le i \le p-1$

12] $\prod_{i=1}^{p-1} |1-\xi_p^i| = p$

$1-\xi_p \mid 1-\xi_p^i$, pues $1-\xi_p^i = (1-\xi_p)(1+\xi_p+\cdots+\xi_p^{i-1})$

$$\Rightarrow \underbrace{\prod_{i=1}^{p-1}(1-\xi_p)}_{(1-\xi_p)^{p-1}} \mid \prod_{i=1}^{p-1}(1-\xi_p^i) = p$$

Luego $\frac{a_i}{(1-\xi_p)} \in \mathcal{O}_K$, $\quad Nm\left(\frac{a_i}{(1-\xi_p)}\right) = \frac{a_i^{p-1}}{p} \in \mathbb{Z}$

$\Rightarrow p \mid a_i^{p-1} \Rightarrow p \mid a_i$ Abs!.

Obs: cómo calcular $\mathcal{O}_K$.

1º] Hallar $\{\alpha_1, \ldots, \alpha_d\}$ base de $K/\mathbb{Q}$, α_i enteros alg.

[2°] $\operatorname{disc}\{\alpha_1, \dots, \alpha_d\} = A^2 \cdot B$, $A, B \in \mathbb{Z}$.

[3°] Para cada $p \mid A$, mirar $\dfrac{a_0 \alpha_1 + \dots + a_{d-1}\alpha_d}{p}$

con $0 \le a_i \le p-1$, y ver si son enteros algebraicos.

→ alguno sí, agrego. (bajó disc. en p^2)

→ ninguno, tiro p, y sigo.

Obs: Al mirar ξ_n, $n \in \mathbb{N}$, vale:

$$\begin{array}{c} \mathbb{Q}[\xi_n] \\ \Big| \\ \mathbb{Q} \end{array} \qquad \phi(n) = \#\{i : 1 \le i \le n : \operatorname{mcd}(i, n) = 1\}$$

$$X^n - 1 = 0 \qquad \sigma(\xi_n) = \xi_n^i \quad \operatorname{mcd}(i, n) = 1.$$

$$\operatorname{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n)^\times$$

Abeliano (no cíclico en general)

$$\mathcal{O}_K = \mathbb{Z}[\xi_n].$$

Obs: no todos los anillos de enteros son monogénicos (práctico).

Ahora conocemos el análogo de $\mathbb{Z}$ en $\mathbb{Q}$ ($\mathcal{O}_K \subset K$) y cómo calcularlo. ¿Hay factorización única?

Rta: en general no.

Ejemplo: $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

irreducibles.

2 irred: $2 = \alpha \cdot \beta \Rightarrow Nm(2) = Nm(\alpha) \cdot Nm(\beta)$

$4 \quad \textcircled{2} \quad \textcircled{2}$

Obs: $\alpha \in \mathcal{O}_K$, $Nm(\alpha) = 1 \Rightarrow \alpha^{-1} \in \mathcal{O}_K$ $(\alpha^{-1} = \bar{\alpha})$

$Nm(a+b\sqrt{-5}) = a^2 + 5b^2 \stackrel{?}{=} 2$ no puede ser.

$= 3$ idem.

¿Qué sucede? $(2) = \langle 2, 1+\sqrt{-5} \rangle^2$

$(3) = \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle$

$$(6) = \overbrace{\langle 2, 1+\sqrt{-5} \rangle^2}^{(2)} \overbrace{\langle 3, 1-\sqrt{-5} \rangle \langle 3, 1+\sqrt{-5} \rangle}^{(3)}$$

$\textcircled{2} \quad \square \quad \square \quad \textcircled{3}$

$= (1+\sqrt{-5})(1-\sqrt{-5})$