Repaso: $K/\mathbb{Q}$ finita, un elemento $\alpha \in K$ se dice entero algebraico si:

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

$K \subset \mathbb{C} \rightarrow$ $\exists$ MCD, $\mathbb{Z}$-mód. f.g. (grupo abeliano f.g.) tf. $\alpha \in M$, d.MCM.

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

$\mathcal{O}_K$ es un anillo, anillo de enteros de K.

($\mathbb{Z}$-módulo)

Problema: ¿ $\mathcal{O}_K$ es f.g. como grupo abeliano? Sí

Objetivo: dado K, calcular $\mathcal{O}_K \hookrightarrow \{\alpha_1, \dots, \alpha_n\} \in \mathcal{O}_K$ t.q. $\mathcal{O}_K = \langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Z}}$.

F/K finita, definimos dos funciones:

$$\begin{cases} Tr_{F/K} : (F, +) \to (K, +) & \text{(morfismo)} \\ Nm_{F/K} : (F^\times, \cdot) \to (K^\times, \cdot) & \text{(morfismo)} \end{cases}$$

$\alpha \in F$, $m_\alpha : F \to F$, $a \mapsto \alpha \cdot a$, K-t.l., elegida una base $\mathcal{B}$ de F como K-e.v.

$$m_\alpha \rightsquigarrow [m_\alpha]_{\mathcal{B}} \in M_{n \times n}(K), \quad n = [F : K]$$

$$Tr \swarrow \qquad \searrow \det$$

$$Tr_{F/K}(\alpha) \qquad Nm_{F/K}(\alpha)$$

$\alpha, \beta \in F$, • $m_{\alpha+\beta} = m_\alpha + m_\beta$ $\quad ((\alpha+\beta)\cdot a = \alpha \cdot a + \beta a)$

$$[m_{\alpha+\beta}]_{\mathcal{B}} = [m_\alpha]_{\mathcal{B}} + [m_\beta]_{\mathcal{B}}$$

$$\Rightarrow Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta).$$

- $\alpha \cdot \beta$, $m_{\alpha\cdot\beta} = m_\alpha \circ m_\beta \Rightarrow [m_{\alpha\beta}]_{\mathcal{B}} = [m_\alpha]_{\mathcal{B}} \cdot [m_\beta]_{\mathcal{B}}$

$$\overset{\text{def.}}{\Rightarrow} Nm(\alpha\cdot\beta) = Nm(\alpha)\cdot Nm(\beta)$$

Obs/ejercicio: Si $\alpha \in k$, ¿$Tr_{F/k}(\alpha)$, $Nm_{F/k}(\alpha)$?

Si $\alpha \in k$, $[m_\alpha]_{\mathcal{B}} = \begin{pmatrix} \alpha & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix}$

Otra definición de norma y traza: k/ℓ finita, $d = [k:\ell]$,

$\#\, Hom_\ell(k, \mathbb{C}) \leq d$ y valía el igual si k/ℓ es separable.

vale siempre.

Si $k = \ell[x]/p(x)$ (irreducible) $\quad \sigma \in Hom_\ell(k, \mathbb{C})$

σ queda determinado por $\sigma(\bar{x}) \in \{\text{raíces de } p(x)\}$ (hay d elementos)

$\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{d-1}\}$ $\quad d = gr(p(x))$

Fijemos $\{\sigma_1, \dots, \sigma_d\} = Hom_\ell(k, \mathbb{C})$

Teo: $\cdot\, Tr_{k/\ell}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha)$. ← fijo por σ_j, $1 \leq j \leq d$

$\cdot\, Nm_{k/\ell}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha)$. ←

Demo: 1°) Supongamos que $k = \mathbb{Q}[\alpha] \longleftrightarrow \underbrace{\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}}_{\mathcal{B}}$ base de k como $\mathbb{Q}$-e.v.

Sea $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Q}$.

$$[mult_\alpha]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & & -a_0 \\ 1 & 0 & & -a_1 \\ 0 & 1 & 0 & -a_2 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 1 & -a_{d-1} \end{pmatrix}$$

(desarrollo por acá)

$m_\alpha(\alpha) = 0$

$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0$

$\alpha^d = -a_{d-1}\alpha^{d-1} - \cdots - a_1\alpha - a_0$

⊛ $\operatorname{Tr}([mult_\alpha]_{\mathcal{B}}) = -a_{d-1} = \sum_{i=1}^{d} \sigma_i(\alpha)$

⊛ $\det([mult_\alpha]_{\mathcal{B}}) = 0 \cdot \det(\ ) + 0 \cdot \det(\ ) + \cdots + (-1) \cdot (-a_0) \cdot \det\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$= (-1)^d \cdot a_0 = \prod_{i=1}^{d} \sigma_i(\alpha)$

Por otro lado, $m_\alpha(x) = \prod_{i=1}^{d} (x - \sigma_i(\alpha)) = x^d - x^{d-1}\underbrace{\left(\sum_{i=1}^{d} \sigma_i(\alpha)\right)}_{-a_{d-1}} + \cdots + \underbrace{(-1)^d \cdot \prod_{i=1}^{d} \sigma_i(\alpha)}_{a_0}$

2° caso: Si $\mathbb{Q}[\alpha] \subsetneq k$ $\quad [k:\mathbb{Q}] = m.n$

$$\begin{matrix} k \\ | \ m \\ \mathbb{Q}[\alpha] \\ | \ n \\ \mathbb{Q} \end{matrix}$$

$\#\operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}[\alpha], \mathbb{C}) = n$ $\quad \{\sigma_1, \ldots, \sigma_n\}$ cada una se extiende de m formas distintas.

$\#\operatorname{Hom}_{\mathbb{Q}}(k, \mathbb{C}) = n.m$

$\operatorname{Hom}_{\mathbb{Q}}(k, \mathbb{C}) = \{\underbrace{\sigma_1^{(1)}, \ldots, \sigma_1^{(m)}}_{\text{extienden a } \sigma_1}, \sigma_2^{(1)}, \ldots, \sigma_2^{(m)}, \ldots, \sigma_n^{(1)}, \ldots, \sigma_n^{(m)}\}$

Todos los $\sigma_i^{(j)}\Big|_{\mathbb{Q}[\alpha]}$ son iguales al variar j.

$\mathcal{B}' = \{1, \alpha, \dots, \alpha^{n-1}\}$ base de $\mathbb{Q}[\alpha]$ como $\mathbb{Q}$-e.v.

Sea $\{\gamma_1, \dots, \gamma_m\}$ base de K como $\mathbb{Q}[\alpha]$-e.v. Luego,

$\mathcal{B} = \{\gamma_1, \alpha\gamma_1, \alpha^2\gamma_1, \dots, \alpha^{n-1}\gamma_1, \gamma_2, \alpha\gamma_2, \dots, \alpha^{n-1}\gamma_2, \dots, \alpha^{n-1}\gamma_m\}$ base de K como $\mathbb{Q}$-e.v.

$$[m_{1+\alpha}]_{\mathcal{B}} = \begin{pmatrix} [m_{1+\alpha}]_{\mathcal{B}'} & & 0 \\ & [m_{1+\alpha}]_{\mathcal{B}'} & \\ 0 & & \ddots \end{pmatrix}$$

$$\mathrm{Tr}\left([m_{1+\alpha}]_{\mathcal{B}}\right) = \sum \mathrm{Tr}\left([m_{1+\alpha}]_{\mathcal{B}'}\right) = m \cdot \mathrm{Tr}\left([m_{1+\alpha}]_{\mathcal{B}'}\right)$$

$$\det\left([m_{1+\alpha}]_{\mathcal{B}}\right) = \det\left([m_{1+\alpha}]_{\mathcal{B}'}\right)^m$$

caso anterior

$$\sum \sigma_i^{(j)}(\alpha) = m \sum_{i=1}^{n} \sigma_i(\alpha) = \mathrm{Tr}\left([m_{1+\alpha}]_{\mathcal{B}}\right) = \mathrm{Tr}_{\mathbb{Q}}(\alpha)$$

$$\prod \sigma_i^{(j)}(\alpha) = \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^m = \det\left([m_{1+\alpha}]_{\mathcal{B}}\right) = N_{\mathbb{Q}}(\alpha)$$

∎

Ejercicio: Probar que si $K \subset L \subset M$ finitas, entonces

- $\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{M/L}(\alpha)\right)$
- $N_{M/K}(\alpha) = N_{L/K}\left(N_{M/L}(\alpha)\right)$

$d = [k:\mathbb{Q}]$

Def: Si $K/\mathbb{Q}$ finita, $\{\alpha_1, \dots, \alpha_d\}$ elts de K, definimos el **discriminante** de $\{\alpha_1, \dots, \alpha_d\}$, como:

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det\left(\sigma_i(\alpha_j)\right)^2$$

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

Obs: no depende del orden ($\{\alpha_1, \dots, \alpha_d\}$)

Teo: $\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det\left(\overbrace{\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)}^{\in \mathbb{Q}}\right) \in \mathbb{Q}$

Demo: $\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det\left(\sigma_i(\alpha_j)\right)^2 = \det\left(\left(\sigma_i(\alpha_j)\right)\left(\sigma_i(\alpha_j)\right)\right) =$

$$= \det\left(\left(\sigma_i(\alpha_j)\right)\left(\sigma_i(\alpha_j)\right)^t\right) = \det\left(\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_d(\alpha_1) \\ \vdots & & \\ \sigma_1(\alpha_d) & \cdots & \sigma_d(\alpha_d) \end{pmatrix}\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_d(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_d) & \cdots & \sigma_d(\alpha_d) \end{pmatrix}\right)$$

$$= \det\begin{pmatrix} \overbrace{\sigma_1(\alpha_1)\sigma_1(\alpha_1) + \cdots}^{\sigma_1(\alpha_1^2)} & \overbrace{\sigma_1(\alpha_1)\sigma_2(\alpha_1) + \cdots}^{\sigma_2(\alpha_1^2)} & \overbrace{\sigma_1(\alpha_1)\sigma_1(\alpha_2) + \cdots}^{\sigma_1(\alpha_1\alpha_2)} & \overbrace{\sigma_1(\alpha_1)\sigma_2(\alpha_2) + \cdots}^{\sigma_2(\alpha_1\alpha_2)} & \cdots \\ & & \vdots & & \end{pmatrix}$$

$$= \det\begin{pmatrix} \operatorname{Tr}(\alpha_1\alpha_1) & \operatorname{Tr}(\alpha_1\alpha_2) & \cdots & \operatorname{Tr}(\alpha_1\alpha_d) \\ \vdots & & & \\ \operatorname{Tr}(\alpha_d\alpha_1) & - & - & \operatorname{Tr}(\alpha_d\alpha_d) \end{pmatrix} \qquad \square$$

Coro: $\operatorname{disc}(\alpha_1, \dots, \alpha_d) \in \mathbb{Q}$. Además, si $\{\alpha_1, \dots, \alpha_d\}$ son enteros algebraicos, $\operatorname{disc}(\alpha_1, \dots, \alpha_d) \in \mathbb{Z}$.

D/ $\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det\left(\overbrace{\operatorname{Tr}(\alpha_i\alpha_j)}^{\in \mathbb{Q}}\right) \in \mathbb{Q}$.

Si $\{\alpha_1, \dots, \alpha_d\}$ enteros algebraicos, $\alpha_i \cdot \alpha_j$ es entero algebraico, para todo par (i,j).

Obs: Si α entero algebraico, $N_{m}(\alpha), Tr(\alpha) \in \mathbb{Z}$. ✗

Luego $Tr(\alpha_i \alpha_j) \in M_{d\times d}(\mathbb{Z}) \Rightarrow \det(Tr(\alpha_i\alpha_j)) \in \mathbb{Z}$ ✓

Obs: la clase pasada calculamos $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$,

$a+bi \rightsquigarrow$ minimal

Tr ✓ Nm

$2a$ $\quad a^2+b^2$

pedimos enteros. ✓

Lema: Si $r \in \mathbb{Z}$, $r \neq 0$, $disc(\alpha_1, \dots, \alpha_d/r) = disc(\alpha_1, \dots, \alpha_d) \cdot \frac{1}{r^2}$

Demo: $disc(\alpha_1, \dots, \alpha_d/r) = \det\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_d(\alpha_1) \\ \vdots & & \\ \sigma_1(\frac{\alpha_d}{r}) & \cdots & \sigma_d(\frac{\alpha_d}{r}) \end{pmatrix}^2 =$

$$\det\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_d(\alpha_1) \\ \vdots & & \\ \frac{\sigma_1(\alpha_n)}{r} & \cdots & \frac{\sigma_d(\alpha_d)}{r} \end{pmatrix}^2 = \frac{1}{r^2} \cdot \det\left(\sigma_i(\alpha_j)\right)^2 =$$

$$= 1/r^2 \cdot disc(\alpha_1, \dots, \alpha_d) \quad ✓$$

Teo dados $\{\alpha_1, \dots, \alpha_d\}$ en K, $disc(\alpha_1, \dots, \alpha_d) = 0 \iff$

$\{\alpha_1, \dots, \alpha_d\}$ son l.d. sobre $\mathbb{Q}$.

D/ ($\Leftarrow$) $\{\alpha_1, \dots, \alpha_d\}$ son l.d. / $\mathbb{Q}$ $\sum a_i \alpha_i = 0$, $a_i \in \mathbb{Q}$

$\left[\sigma_i(\alpha_j)\right]$ las columnas son l.d. pues

aplico σ_j: $\quad \sigma_j\left(\sum a_i \alpha_i\right) = 0$

$$\sum \sigma_j(a_i)\,\sigma_j(\alpha_i) = 0 \quad , \; a_i \in \mathbb{Q}, \; \sigma_j(a_i) = a_i$$

$$\sum a_i\,\sigma_j(\alpha_i) = 0.$$

$$[\sigma_i(\alpha_j)] = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_d(\alpha_1) \\ \vdots & & \\ \sigma_1(\alpha_d) & \cdots & \sigma_d(\alpha_d) \end{pmatrix} \begin{matrix} \leftarrow a_1 \\ + \\ \leftarrow a_d \end{matrix}$$

$\Rightarrow$ columnas son l.d. $\Rightarrow \det(\;) = 0$. ✓

$\Leftarrow$) $\operatorname{disc}(\alpha_1, \ldots, \alpha_d) = 0$, (supongamos que $\{\alpha_1, \ldots, \alpha_d\}$ son l.i.)

$$\det \begin{pmatrix} \operatorname{Tr}(\alpha_1\alpha_1) & \cdots & \operatorname{Tr}(\alpha_1\alpha_d) \\ \vdots & & \\ \operatorname{Tr}(\alpha_d\alpha_1) & \cdots & \operatorname{Tr}(\alpha_d\alpha_d) \end{pmatrix} \Rightarrow \text{columnas son l.d./} \mathbb{Q}$$

$\exists$ sea existen $a_1, \ldots, a_d \in \mathbb{Q}$ (no todos nulos) t.q.

(*) $$a_1 \begin{pmatrix} \operatorname{Tr}(\alpha_1\alpha_1) \\ \vdots \\ \operatorname{Tr}(\alpha_1\alpha_d) \end{pmatrix} + a_2 \begin{pmatrix} \operatorname{Tr}(\alpha_2\alpha_1) \\ \vdots \\ \operatorname{Tr}(\alpha_2\alpha_d) \end{pmatrix} + \cdots + a_d \begin{pmatrix} \operatorname{Tr}(\alpha_d\alpha_1) \\ \vdots \\ \operatorname{Tr}(\alpha_d\alpha_d) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Sea $\beta = a_1\alpha_1 + \cdots + a_d\alpha_d \in K$, $\beta \neq 0$ (suposición). $\quad (\beta = 0)$

$f: K \to \mathbb{Q}$, $\gamma \to \operatorname{Tr}(\beta\cdot\gamma)$ es $\mathbb{Q}$-lineal. $f(\gamma_1+\gamma_2) = f(\gamma_1)+f(\gamma_2)$, $f(\lambda\cdot\gamma) = \lambda f(\gamma)$, $\lambda \in \mathbb{Q}$

Afirmo: $f \equiv 0$.

Como $\{\alpha_1, \ldots, \alpha_d\}$ son l.i. y $[K:\mathbb{Q}] = d \Rightarrow$ base, luego basta ver que $f(\alpha_i) = 0$.

$$f(\alpha_1) = Tr(\beta\cdot\alpha_1) = Tr((a_1\alpha_1 + \cdots + a_d\alpha_d)\alpha_1)$$

$$= a_1 Tr(\alpha_1\alpha_1) + \cdots + a_d Tr(\alpha_d\alpha_1) = 0 \text{ por } \circledast$$

$$f(\alpha_2) = a_1 Tr(\alpha_1\alpha_2) + \cdots + a_d Tr(\alpha_d\alpha_2) = 0$$

$$\vdots$$

$$f(\alpha_d) = 0.$$

$\Rightarrow f \equiv 0$, $f(\underline{\beta^{-1}}) = Tr(\beta\cdot\beta^{-1}) = Tr(1) = d \neq 0$ Abs!

Nbcho: $\beta = 0$ pues, $\sigma_1(\beta) = \sum a_i\sigma_1(\alpha_i) = 0$, σ_1 morfismo de cuerpos $\Rightarrow$ inyectivo. ∎

Teo: $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo finitamente generado.

D/ Sea $\{\alpha_1, \ldots, \alpha_d\}$ base de K como $\mathbb{Q}$-e.v. tal que todos los α_i son enteros algebraicos.

$\rightarrow$ $disc(\alpha_1, \ldots, \alpha_d) \in \mathbb{Z}$ no nulo. Sea $n = |disc(\alpha_1, \ldots, \alpha_d)| \in \mathbb{N}$.

Si $\langle \alpha_1, \ldots, \alpha_d \rangle_{\mathbb{Z}} = \mathcal{O}_K$ listo.

Sino, $\exists\, \beta \in \mathcal{O}_K \setminus \langle \alpha_1, \ldots, \alpha_d \rangle_{\mathbb{Z}}$, miremos $\langle \alpha_1, \ldots, \alpha_d, \beta \rangle$

$$\underbrace{\langle \alpha_1, \ldots, \alpha_d \rangle_{\mathbb{Z}}}_{L_1} \subsetneq \underbrace{\langle \alpha_1, \ldots, \alpha_d, \beta \rangle_{\mathbb{Z}}}_{\text{f.g.}} = \underbrace{\langle \gamma_1, \ldots, \gamma_d \rangle_{\mathbb{Z}}}_{L_2}$$

¿Cómo elegirlos?

Vale (Forma Normal de Smith): dada $M \in M_{m\times n}(\mathbb{Z})$ existen $A \in GL_m(\mathbb{Z})$, $B \in GL_n(\mathbb{Z})$ tales que

$$A\cdot M\cdot B = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{pmatrix} \quad d_1 | \cdots | d_r \text{ enteros.}$$

Luego, puedo mirar la matriz de L_1 en L_2

$\alpha_1 = \sum a_{i,1}\gamma_i \quad , \quad a_{i,1} \in \mathbb{Z}$

$\alpha_2 =$

$\vdots$

$$A \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & & \vdots \\ a_{d1} & & a_{dd} \end{pmatrix} B = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_d \end{pmatrix} \quad \lambda_i \in \mathbb{Z}$$

A: cambio de base

$\det \neq 0$

B: cambio de base

$\Rightarrow \lambda_i \neq 0 \quad \lambda_1 \cdots \lambda_d$

Cambio $\{\alpha_1, \ldots, \alpha_d\}$ por $\hookrightarrow \{A\alpha_1, \ldots, A\alpha_d\} = \{\delta_1, \ldots, \delta_d\}$

$\{\gamma_1, \ldots, \gamma_d\}$ por $\{B^{-1}\gamma_1, \ldots, B^{-1}\gamma_d\} = \left\{\frac{\delta_1}{\lambda_1}, \ldots, \frac{\delta_d}{\lambda_d}\right\}$

empecé

Luego $\operatorname{disc}\{\alpha_1, \ldots, \alpha_d\} = \operatorname{disc}\{\delta_1, \ldots, \delta_d\} =$

$= (\lambda_1 \cdots \lambda_d)^2 \cdot \operatorname{disc}\left\{\frac{\delta_1}{\lambda_1}, \ldots, \frac{\delta_d}{\lambda_d}\right\} = \underbrace{(\lambda_1 \cdots \lambda_d)^2}_{>1} \cdot \underbrace{\operatorname{disc}(\gamma_1, \ldots, \gamma_d)}_{\text{siguiente}}$

$\rightsquigarrow$ (discriminante decreció. Al ser natural, el proceso termina $\square$

Lema: Si $\{\alpha_1, \ldots, \alpha_d\}$ y $\{\beta_1, \ldots, \beta_d\}$ generan lo mismo

$\Rightarrow \operatorname{disc}\{\alpha_1, \ldots, \alpha_d\} = \operatorname{disc}(\beta_1, \ldots, \beta_d)$