$\boxed{07/05/20}$ § **Norma y traza**

def $A \subset B$ - extn. de anillos t.q B es libre de rango finito n sobre A. Para $\beta \in B$ consideremos

$$\left.\begin{array}{l}\mu_\beta : B \to B \\ x \mapsto x\beta\end{array}\right\} \Rightarrow \begin{array}{l} N_{B/A}(\beta) = \det \mu_\beta \\ T_{B/A}(\beta) = \operatorname{tr} \mu_\beta \end{array}$$

Si $e_1, \dots, e_n \in B$ es una base de B como A-módulo,

$$\beta \cdot e_i = \sum_j a_{ij} e_j \rightsquigarrow N(\beta) = \det(a_{ij}) \quad T(\beta) = \operatorname{tr}(a_{ij}) = \sum_{1 \le i \le n} a_{ii}$$

Si $T \in GL_n(A)$ es matriz de cambio de base.

$$\det(T M T^{-1}) = \det(T) \cdot \det(M) \cdot \det(T)^{-1} = \det M.$$

$$\operatorname{tr}(T M T^{-1}) = \operatorname{tr}(T^{-1} T M) = \operatorname{tr}(M)$$

El pol. característico: $f^\beta_{B/A}(x) = \det(x I_n - M)$

$$= x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$a_0 = (-1)^n \cdot N_{B/A}(\beta), \quad a_{n-1} = -T_{B/A}(\beta)$$

$$N(\beta \cdot \beta') = N(\beta) \cdot N(\beta')$$

$$T(a\beta) = a \cdot T(\beta) \qquad T(\beta + \beta') = T(\beta) + T(\beta')$$

Si $a \in A$, $N(a) = a^n$ $\quad T(a) = na$.

Proposición Para $\mathbb{K}/\mathbb{Q}$ extn. finita existen $n = [\mathbb{K} : \mathbb{Q}]$ encajes $\sigma_1, \dots, \sigma_n : \mathbb{K} \hookrightarrow \mathbb{C}$, y

$$N_{\mathbb{K}/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha) \qquad T_{\mathbb{K}/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha).$$

Dem Si $\mathbb{K} = \mathbb{Q}(\alpha)$, entonces $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$ está definido por $\sigma(\alpha)$, que debe ser una raíz de $f^\alpha_{\mathbb{Q}}$.

$$\deg f^\alpha_{\mathbb{Q}} = n, \quad f^\alpha_{\mathbb{Q}} = \prod_{\sigma : \mathbb{K} \hookrightarrow \mathbb{C}} (x - \sigma(\alpha))$$

En gral,

$$\begin{tikzcd} \mathbb{K} \arrow[r, dashed] & \mathbb{C} \\ \mathbb{Q}(\alpha) \arrow[u, dash] \arrow[ur] & \\ \mathbb{Q} \arrow[u, dash] & \end{tikzcd}$$

$\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ admite $[\mathbb{K} : \mathbb{Q}(\alpha)]$ extensiones a $\mathbb{K} \hookrightarrow \mathbb{C}$.

$$f^\alpha_{\mathbb{K}/\mathbb{Q}} = \left(f^\alpha_{\mathbb{Q}}\right)^{[\mathbb{K} : \mathbb{Q}(\alpha)]} = \prod_{\sigma : \mathbb{K} \hookrightarrow \mathbb{C}} (x - \sigma(\alpha))$$

$$a_0 = (-1)^n N_{K/\mathbb{Q}}(\alpha) = (-1)^n \sigma_1(\alpha)\cdots\sigma_n(\alpha).$$

$$a_{n-1} = -T_{K/\mathbb{Q}}(\alpha) = -(\sigma_1(\alpha)+\cdots+\sigma_n(\alpha)) \qquad \boxtimes$$

Nota Si $K/\mathbb{Q}$ es una extn de Galois,

$$\{K \hookrightarrow \mathbb{C}\} \longleftrightarrow Gal(K/\mathbb{Q}).$$

Proposición Si $\alpha \in \mathcal{O}_K$, entonces $N_{K/\mathbb{Q}}(\alpha), T_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$

Dem $\alpha_1, \dots, \alpha_n$ - raíces de $f^{\alpha}_{K/\mathbb{Q}} \Rightarrow \alpha_i$ son enteros algebraicos.

$N(\alpha) = \alpha_1\cdots\alpha_n, \qquad T(\alpha) = \alpha_1+\cdots+\alpha_n.$

$$\left.\begin{array}{l} \bullet) \text{ Son enteros algebraicos.} \\ \bullet) \ N_{K/\mathbb{Q}}(\alpha), T_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q} \end{array}\right\} N(\alpha), T(\alpha) \in \mathbb{Z}.$$

$\boxtimes$

Proposición $\mathcal{O}_K^{\times} = \{\alpha \in \mathcal{O}_K \mid N(\alpha) = \pm 1\}$

Dem $\alpha \in \mathcal{O}_K^{\times} \Rightarrow \underbrace{N(\alpha)\cdot N(\alpha^{-1})}_{\in\mathbb{Z}} = N(\alpha\alpha^{-1}) = 1$

$\Rightarrow N(\alpha), N(\alpha^{-1}) = \pm 1.$

Ahora si $N(\alpha) = \pm 1 \Rightarrow \alpha_1\cdots\alpha_n = \pm 1.$
$(\alpha_1 = \alpha)$

$$\alpha^{-1} = \pm \underbrace{\alpha_2\cdots\alpha_n}_{\text{entero algebraico}} \in \mathcal{O}_K. \qquad \boxtimes$$

Ejemplo $K = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

Base$/\mathbb{Q}$: $1, \sqrt{d}$. $\qquad \alpha = a + b\sqrt{d}$.

$$M_\alpha = \begin{pmatrix} a & db \\ b & a \end{pmatrix} \qquad N(\alpha) = a^2 - db^2 = (a+b\sqrt{d})(a-b\sqrt{d})$$

$$T(\alpha) = 2a = (a+b\sqrt{d}) + (a-b\sqrt{d}).$$

§ Recordatorio de álgebra lineal

Sea V un esp. vect. de dim. finita n sobre k.
Consideremos una forma bilineal simétrica
$\langle\cdot,\cdot\rangle : V\times V \longrightarrow k$.

Sea $e_1,\ldots,e_n$ una base de V/k. El **discriminante**:

$$\Delta(e_1,\ldots,e_n) = \det(\langle e_i, e_j\rangle)_{i,j}.$$

En gral, si $f_1,\ldots,f_e \in V$, donde $f_i = \sum_j a_{ij} e_j$

$$\langle f_k, f_e\rangle = \left\langle \sum_i a_{ki} e_i, \sum_j a_{ej} e_j \right\rangle$$

$$= \sum_{i,j} a_{ki} \cdot \langle e_i, e_j\rangle \cdot a_{ej}$$

$$(\langle f_k, f_e\rangle)_{k,e} = (a_{ij}) \cdot (\langle e_i, e_j\rangle)_{ij}\, (a_{ij})^t.$$

$$\det(\langle f_k, f_e\rangle)_{k,e} = \det(a_{ij})^2 \cdot \Delta(e_1,\ldots,e_n).$$

$$(f_1,\ldots,f_n) \text{ es una base} \iff \det(a_{ij}) \neq 0.$$

Fijando $v \in V$, se obtiene una forma lineal

$$\langle v,\cdot\rangle : V \longrightarrow k$$
$$x \longmapsto \langle v, x\rangle$$

Se dice que $\langle\cdot,\cdot\rangle$ es **no degenerada**:

1) el discriminante $\Delta(e_1,\ldots,e_n) \neq 0$.
(respecto a cualquier base).

$\Updownarrow$

2) $\langle\cdot,\cdot\rangle$ induce isomorfismo

$$\varphi : V \xrightarrow{\sim} V^\vee := \mathrm{Hom}_k(V, k)$$
$$v \longmapsto (x \mapsto \langle v, x\rangle)$$

en este caso:
tenemos
$e_1^*,\ldots,e_n^*$ – base de $V^\vee$,
$e_i^*(e_j) = \delta_{ij}$.

$e_i' := \varphi^{-1}(e_i^*)$.

$e_1',\ldots,e_n'$ – base de V
t.q. $\langle e_i', e_j\rangle = \delta_{ij}$.

§ Emparejamiento de traza

def Para $A \subset B$, donde $rk_A B = n$,

$$\langle \cdot , \cdot \rangle : B \times B \longrightarrow A$$
$$(x, y) \longmapsto T_{B/A}(xy).$$

Si $e_1, \dots e_n$ es una base de B/A, el discriminante

$$\Delta(e_1, \dots, e_n) = \det(\langle e_i, e_j \rangle)_{i,j} = \det(T_{B/A}(e_i e_j))$$

Si $f_1, \dots f_n \in B$, $f_i = \sum_j a_{ij} e_j$,

$$\Delta(f_1, \dots f_n) = [\det(a_{ij})]^2 \cdot \Delta(e_1, \dots, e_n).$$

Si $f_1, \dots f_n$ es una base $\Longleftrightarrow$ $\det(a_{ij}) \in A^\times$

Si $A = \mathbb{Z}$ $\Rightarrow$ $(\mathbb{Z}^\times)^2 = 1$.

Def Si R es un anillo de # que es un $\mathbb{Z}$-módulo f.g., entonces

$$\Delta(R) = \Delta(e_1, \dots, e_n) \in \mathbb{Z}$$ donde $e_1, \dots, e_n$ es alguna base de $R/\mathbb{Z}$.

En esta situación, si $rk\, R = n$, y $\beta_1, \dots, \beta_n \in R$, $\beta_i = \sum_j a_{ij} e_j$, entonces

$$M = \mathbb{Z}\langle \beta_1, \dots, \beta_n \rangle.$$

$$[R : M] = \begin{cases} \infty, & \text{si } \det(a_{ij}) = 0. \\ \|\det(a_{ij})\|, & \text{si } \det(a_{ij}) \neq 0. \end{cases}$$

Proposición Si $M = \mathbb{Z}\langle \beta_1, \dots, \beta_m \rangle$, $rk\, M = n$,

$$\Delta(M) = [R : M]^2 \cdot \Delta(R).$$

Dem. $\Delta(\beta_1, \dots, \beta_n) = \det(a_{ij})^2 \cdot \Delta(R).$ $\boxtimes$

§ Generación finita de $\mathcal{O}_K$

Lema (independencia lineal de caracteres)

Dado un gpo abeliano G y un campo F, si $\chi_1, \dots, \chi_n : G \to F^\times$ son caracteres (multiplicativos),

$$\chi_i \neq \chi_j, \quad i \neq j, \quad y$$

$$c_1\chi_1 + \dots + c_n\chi_n = 0 \quad \text{para } c_1, \dots, c_n \in F$$

$\Rightarrow \quad c_1 = \dots = c_n = 0.$

Dem En mis apuntes.

Lema Sea $K/\mathbb{Q}$ campo de #,

$\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ diferentes encajes.

Entonces,

$$\Delta(\alpha_1, \dots, \alpha_n) = \det\left(T_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)$$
$$= \det\left(\sigma_i(\alpha_j)\right)^2_{i,j}.$$

Demostración Usar la fórmula $T_{rK/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$. $\boxtimes$

Prop.

$$\langle \cdot, \cdot \rangle : K \times K \to \mathbb{Q}$$
$$(\alpha, \beta) \longmapsto T_{K/\mathbb{Q}}(\alpha\beta)$$

es una forma no degenerada.

Dem Si $\alpha_1, \dots, \alpha_n$ es una base de $K/\mathbb{Q}$, hay que ver que $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$.

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$$

$\det(\sigma_i(\alpha_j)) \neq 0$, por la independencia lineal de $\sigma_i : K^\times \to \mathbb{C}^\times$. $\boxtimes$

Teorema $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango $n = [K : \mathbb{Q}]$.

Dem. Sea $\alpha_1, \dots, \alpha_n \in K$ una base de $K/\mathbb{Q}$. al multiplicar los α_i por $N \in \mathbb{Z}$, $N \gg 0$, podemos asumir que $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$.

El emp. de traza $\langle \cdot, \cdot \rangle$ es no degenerado $\Rightarrow$ existe base dual $\alpha_1', \dots, \alpha_n' \in K$.

$$\langle \alpha_i, \alpha_j' \rangle = \delta_{ij}.$$

Todo $\alpha \in \mathcal{O}_K$ puede ser expresado como

$$\alpha = \sum_i \underbrace{a_i}_{\in \mathbb{Q}} \alpha_i'$$

$$a_i = \sum_j a_j \cdot \delta_{ij} = \sum_j a_j \cdot \langle \alpha_i, \alpha_j' \rangle = \langle \alpha_i, \sum_j a_j \alpha_j' \rangle$$
$$= \langle \alpha_i, \alpha \rangle.$$

$\alpha_i, \alpha \in \mathcal{O}_K \Rightarrow \langle \alpha_i, \alpha \rangle = T(\alpha_i \alpha) \in \mathbb{Z}$

$a_i \in \mathbb{Z}$,

$$\underbrace{\alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n}_{rk\ n.} \subseteq \mathcal{O}_K \subseteq \underbrace{\alpha_1' \mathbb{Z} \oplus \cdots \oplus \alpha_n' \mathbb{Z}.}_{rk\ n}$$

$rk\, \mathcal{O}_K = n.$ $\boxtimes$

Corolario $\mathcal{O}_K$ es el subanillo de K más grande t.q. es f.g. como $\mathbb{Z}$-módulo.

Dem 1) $rk\, \mathcal{O}_K = n = [K : \mathbb{Q}]$

2) Si $R \subset K$, $\mathbb{Z} \subset R$ con R f.g. ($<\infty$) $\Rightarrow$ los elementos de R son enteros $/\mathbb{Z}$.

$\Rightarrow R \subseteq \mathcal{O}_K$ $\boxtimes$

Def Para un campo de # $K/\mathbb{Q}$, el **discriminante** es

$$\Delta_K \overset{def}{=} \Delta(\mathcal{O}_K) = \det(T_{K/\mathbb{Q}}(\alpha_i\alpha_j)).$$

$$\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}.$$

Ejemplo Si $K = \mathbb{Q}(\sqrt{d})$.

$d \equiv 2,3\ (4)$: $\quad \mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \sqrt{d}\,\mathbb{Z}$

$$\Delta(\mathcal{O}_K) = \det\begin{pmatrix} T(1) & T(\sqrt{d}) \\ T(\sqrt{d}) & T(d) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

$d \equiv 1\ (4)$: $\quad \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} \oplus \frac{1+\sqrt{d}}{2}\mathbb{Z}.$

$$\Delta(\mathcal{O}_K) = \det\begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d.$$

Conclusión: $\Delta_K = \begin{cases} 4d, & d \equiv 2,3\ (4) \\ d, & d \equiv 1\ (4). \end{cases}$