§ Teoremas de Brill y Stickelberger.

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array} \rightsquigarrow \mathcal{O}_K \rightsquigarrow \Delta(\mathcal{O}_K) = \Delta_K \in \mathbb{Z}$$

$$p \mid \Delta_K \iff p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}, \quad e_i > 1.$$

def $K/\mathbb{Q}$, $\quad \sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$

$\sigma_i(K) \subset \mathbb{R} \Rightarrow \sigma_i$ **real**

$\sigma_i(K) \not\subset \mathbb{R} \Rightarrow \sigma_i$ **complejo** $\quad \overline{\sigma_i}$ es tb. complejo.

$$\underbrace{r_1}_{\text{el \# de encajes reales}} + \underbrace{2 \cdot r_2}_{\text{encajes complejos}} = n = [K:\mathbb{Q}].$$

(r_1, r_2) — la **signatura** de $K/\mathbb{Q}$.

Nota Si $K = \mathbb{Q}(\alpha)$, $\quad f = f_{\mathbb{Q}}^{\alpha}$.

r_1 = el # de raíces reales de f,

$2r_2$ = el # de raíces complejas de f.

Proposición (Brill) $\quad sgn\, \Delta_K = (-1)^{r_2}$

Dem. $K = \mathbb{Q}(\alpha)$, α entero algebraico

$\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, $\qquad \Delta(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K$

$$\Delta(f_{\mathbb{Q}}^{\alpha}) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

ejercicio:

$$sgn \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{r_2}, \qquad 2r_2 = \text{el } \# \text{ de raíces complejas}$$

$\boxtimes$

Ejemplos

	r_1	r_2	Δ_K
·) $\mathbb{Q}(\sqrt{d})$	$\begin{cases} 2, & d>1 \\ 0, & d<0 \end{cases}$	$\begin{cases} 0, & d>1 \\ 1, & d<0 \end{cases}$	d ó $4d$
·) $\mathbb{Q}(\sqrt[3]{2})$	1	1	$-2^2 \cdot 3^3$
·) $\mathbb{Q}(\alpha)$, $\alpha^3 - 3\alpha + 1 = 0$	3	0	$+3^4$
·) $\mathbb{Q}(\zeta_p)$	0	$\frac{\varphi(p)}{2}$	$(-1)^{\frac{p-1}{2}} \cdot p^{p-2}$

Proposición (Stickelberger) $\quad \Delta_K \text{ mód } 4 \equiv 0$ ó 1

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

$\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C} \qquad \Delta_K = \det(\sigma_i(\alpha_j))^2$.

$$\Delta_K = \left(\sum_{\rho \in S_n} sgn(\rho) \cdot \sigma_{\rho(1)}(\alpha_1) \cdots \sigma_{\rho(n)}(\alpha_n) \right)^2$$

$$= (\underset{\substack{\uparrow \\ sgn\,\rho = +1}}{P} - \underset{\substack{\uparrow \\ sgn\,\rho = -1}}{N})^2 = (P+N)^2 - 4 \cdot PN \equiv 0 \text{ ó } 1 \pmod 4$$

$P+N, \quad P \cdot N \in \mathbb{Z}$

$\boxtimes$

§ Campos linealmente disjuntos

def $K/\mathbb{Q}$, $K'/\mathbb{Q}$.

$$\begin{tikzcd} & \overline{\mathbb{Q}} \arrow[d, dash] & \\ & K\cdot K' & \\ K \arrow[ur, dash] & & K' \arrow[ul, dash] \\ & \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

compuesto KK' = el campo
(compositum) más pequeño que contiene a K y K'.

def K y K' son **linealmente disjuntos** si

> Morandi, §20.

a) $K \otimes_{\mathbb{Q}} K' \longrightarrow KK'$ es un iso.
$x \otimes y \longmapsto xy$.

b) Si $\alpha_1, \ldots, \alpha_n$ es una base de K sobre $\mathbb{Q}$, entonces esta es linealmente independiente sobre K'.

c) Si $\{\alpha_i\}$, $\{\alpha'_j\}$ son bases de K y K' resp., entonces $\{\alpha_i \alpha'_j\}$ es una base KK'.

d) $[KK' : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [K' : \mathbb{Q}]$.

Prop. Si K, K' son linealm. disjuntos,

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

$$\mathcal{O}_{K'} = \alpha'_1 \mathbb{Z} \oplus \cdots \oplus \alpha'_{n'} \mathbb{Z}.$$

Si $\operatorname{mcd}(\Delta_K, \Delta_{K'}) = 1$, entonces

1) $\alpha_i \alpha'_j$ es una base de $\mathcal{O}_{KK'}$.

2) $\Delta_{KK'} = \Delta_K^{[K':\mathbb{Q}]} \cdot \Delta_{K'}^{[K:\mathbb{Q}]}$

Ejemplo $K = \mathbb{Q}(\sqrt{3})$, $K' = \mathbb{Q}(\sqrt{5})$, $KK' = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

$\Delta_K = 12$ $\qquad \Delta_{K'} = 5$.

$$\mathcal{O}_K = \mathbb{Z} \oplus \sqrt{3}\,\mathbb{Z} \qquad \mathcal{O}_K = \mathbb{Z} \oplus \frac{1+\sqrt{5}}{2}\mathbb{Z}.$$

$$\mathcal{O}_{KK'} = \mathbb{Z} \oplus \sqrt{3}\,\mathbb{Z} \oplus \frac{1+\sqrt{5}}{2}\mathbb{Z} \oplus \frac{\sqrt{3}+\sqrt{15}}{2}\mathbb{Z}.$$

$$\Delta_K = \det \begin{pmatrix} 1 & +\sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix}^2 \qquad \Delta_{K'} = \det \begin{pmatrix} 1 & (1+\sqrt{5})/2 \\ 1 & (1-\sqrt{5})/2 \end{pmatrix}^2$$

$$\Delta_{KK'} = \det \left(\begin{pmatrix} 1 & +\sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix} \otimes \begin{pmatrix} 1 & (1+\sqrt{5})/2 \\ 1 & (1-\sqrt{5})/2 \end{pmatrix} \right)^2$$

$$= \underbrace{12^2 \cdot 5^2 = 2^4 \cdot 3^2 \cdot 5^2}$$

producto de Kronecker

en gral, $\underset{m\times m}{X = (x_{ij})}$, $\underset{n\times n}{Y = (y_{kl})}$.

$$X \otimes Y = \underset{mn \times mn}{\begin{pmatrix} x_{11}Y & x_{12}Y & \cdots & x_{1n}Y \\ \vdots & \vdots & & \vdots \\ x_{n1}Y & x_{n2}Y & \cdots & x_{nn}Y \end{pmatrix}}$$

$$\det(X \otimes Y) = (\det X)^n \cdot (\det Y)^m.$$

§ Anillo de enteros de $\mathbb{Q}(\zeta_n)$. $\quad n = p_1^{e_1} \cdots p_s^{e_s}$.

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{e_1}}) \cdots \mathbb{Q}(\zeta_{p_s^{e_s}})$$

Lema Consideremos $K = \mathbb{Q}(\zeta_{p^e})$.

1) $\Delta(\mathbb{Z}[\zeta_{p^e}]) = \pm p^s$, donde $s = p^{e-1}(pe-e-1)$.

2) el ideal $\mathfrak{p} = (1-\zeta_{p^e})\mathcal{O}_K$ es primo

y se tiene $p\mathcal{O}_K = \mathfrak{p}^{\varphi(p^e)}$, $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$.

Dem. $\Delta(\mathbb{Z}[\zeta_{p^e}]) = \Delta(\Phi_{p^e}) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(\Phi'_{p^e}(\zeta_{p^e}))$

la parte 1) — ejercicio.

(revisar el cálculo para $e=1$)

la parte 2) $\zeta := \zeta_{p^e}$

$$\Phi_{p^e}(1) = \prod_{(k,p^e)=1} (1-\zeta^k) = p \qquad 1-\zeta^k = \underbrace{\frac{1-\zeta^k}{1-\zeta}}_{\in \mathcal{O}_K^\times} \cdot (1-\zeta)$$

$$N\left(\frac{1-\zeta^k}{1-\zeta}\right) = \frac{N(1-\zeta^k)}{N(1-\zeta)} = 1$$

$$1-\zeta^k = \underbrace{\varepsilon_k}_{\in \mathcal{O}_K^\times} \cdot (1-\zeta) \qquad (1-\zeta)^{\varphi(p^e)} = \varepsilon \cdot p.$$

$$p\mathcal{O}_K = \mathfrak{p}^{\varphi(p^e)}, \quad \text{donde} \quad \mathfrak{p} = (1-\zeta)\mathcal{O}_K.$$

$$\left.\begin{array}{l} N(p\mathcal{O}_K) = N(\mathfrak{p})^{\varphi(p^e)} \\ \quad \parallel \\ p^{\varphi(p^e)} \end{array}\right\} \begin{array}{l} \Rightarrow N(\mathfrak{p}) = p. \\ \Rightarrow \mathcal{O}/\mathfrak{p} \simeq \mathbb{F}_p. \end{array}$$

$\boxtimes$

Proposición Para $K = \mathbb{Q}(\zeta_{p^e})$ se tiene
$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}].$$

Dem $\Delta(\mathbb{Z}[\zeta_{p^e}]) = \pm p^s =: d, \quad s = p^{e-1}(pe-e-1)$

$$\mathbb{Z}[\zeta_{p^e}] \subseteq \mathcal{O}_K \subseteq \frac{1}{d}\mathbb{Z}[\zeta_{p^e}].$$

$$p^s \cdot \mathcal{O}_K \subseteq \mathbb{Z}[\zeta_{p^e}] \subseteq \mathcal{O}_K.$$

$$\mathfrak{p} = (1-\zeta_{p^e})\mathcal{O}_K \qquad \mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p \Rightarrow \mathcal{O}_K = \mathbb{Z} + \mathfrak{p}.$$

$$\Rightarrow \quad \mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}] + \mathfrak{p} \qquad (*)$$

$$(*)\cdot\mathfrak{p}: \qquad \mathfrak{p} = \mathfrak{p}\,\mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}^2$$

$$\Rightarrow \quad \mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}\,\mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}^2$$
$$= \mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}^2.$$

etc. .... $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}^t$ para todo $t = 1, 2, 3, \ldots$

en particular, $t = s\cdot\varphi(p^e)$.

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}] + \left(\mathfrak{p}^{\varphi(p^e)}\right)^s = \mathbb{Z}[\zeta_{p^e}] + p^s\mathcal{O}_K$$
$$= \mathbb{Z}[\zeta_{p^e}]. \qquad \boxtimes$$

Teorema para $K = \mathbb{Q}(\zeta_n)$ tenemos

•) $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$

•) $\Delta_K = (-1)^{\varphi(n)/2} \cdot \dfrac{n^{\varphi(n)}}{\prod_{p \mid n} p^{\varphi(n)/(p-1)}}$

Dem Inducción sobre s donde $n = p_1^{e_1} \cdots p_s^{e_s}$

•) $s = 1$: acabamos de ver.

•) $s > 1$. $K_1 = \mathbb{Q}(\zeta_{p_1^{e_1}}), \ldots, K_s = \mathbb{Q}(\zeta_{p_s^{e_s}})$

$\mathbb{Q}(\zeta_n) = K_1 \cdots K_s$, y $K_1 \cdots K_{s-1}$, K_s son linealmente disjuntos.

$\mathcal{O}_{K_1 \cdots K_{s-1}} = \mathbb{Z}[\zeta_{p_1^{e_1}} \cdots \zeta_{p_{s-1}^{e_{s-1}}}]$ — por inducción

$\mathcal{O}_{K_s} = \mathbb{Z}[\zeta_{p_s^{e_s}}]$, $\operatorname{mcd}(\Delta_{K_1 \cdots K_{s-1}}, \Delta_{K_s}) = 1$.

$\mathcal{O}_{K_1 \cdots K_{s-1} K_s} = \mathbb{Z}[\zeta_{p_1^{e_1}} \cdots \zeta_{p_{s-1}^{e_{s-1}}}] \cdot \mathbb{Z}[\zeta_{p_s^{e_s}}]$

$= \mathbb{Z}[\zeta_n]$

$\Delta = \ldots\ldots$ (ejercicio) $\boxtimes$

$\Delta_{K_1 \cdots K_{s-1}}^{[K_s : \mathbb{Q}]} \cdot \Delta_{K_s}^{[K_1 \cdots K_{s-1} : \mathbb{Q}]}$

Ejemplo: $K = \mathbb{Q}(\zeta_{20}) = \underbrace{\mathbb{Q}(\zeta_4)}_{K_1} \cdot \underbrace{\mathbb{Q}(\zeta_5)}_{K_2}$.

$\mathcal{O}_{K_1} = \mathbb{Z}[\zeta_4]$, $\mathcal{O}_{K_2} = \mathbb{Z}[\zeta_5]$.

$\mathcal{O}_K = \mathbb{Z}[\zeta_{20}]$.

$\Delta_K = \Delta_{K_1}^{\varphi(5)} \cdot \Delta_{K_2}^{\varphi(4)} = 2^8 \cdot 5^6$.