09/09/20

Lema R - $\mathbb{Z}$-mód libre de rango n, $R = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$.

$M = \mathbb{Z}\langle \beta_1, \dots, \beta_n \rangle \subset R$. $\qquad \beta_i = \sum_j a_{ij}\alpha_j$

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

Dem $R \cong \mathbb{Z}^n$ $\qquad M \subset R \longleftrightarrow A = (a_{ij}) \qquad A: \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$

$\alpha_i \mapsto e_i \qquad M \longleftrightarrow A(\mathbb{Z}^n)$

•) Si $\det A = 0 \implies \operatorname{rk} M < n \implies \#(R/M) = \infty$.

•) Forma normal de Smith: (Cohen, "A Course in computational ANT")

$$UAV = B = \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{pmatrix}, \qquad U, V \in GL_n(\mathbb{Z})$$

$U, V : \mathbb{Z}^n \xrightarrow{\cong} \mathbb{Z}^n$

$$[\mathbb{Z}^n : A(\mathbb{Z}^n)] = [\mathbb{Z}^n : B(\mathbb{Z}^n)] = \#(\mathbb{Z}/b_1 \times \cdots \times \mathbb{Z}/b_n)$$
$$= |\det B| = |\det(UAV)|$$
$$= |\det(A)|. \qquad \boxtimes$$

§ Cálculos de $\Delta(R)$ y $\mathcal{O}_K$

$\sigma_i : K \longrightarrow \mathbb{C}$, $\quad n = [K:\mathbb{Q}]$

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

$\langle \alpha_1, \dots, \alpha_n \rangle = R \subset K$

$$\begin{array}{ccc} R & \subset & K \\ |n & & |n \\ \mathbb{Z} & — & \mathbb{Q} \end{array}$$

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

Si $R = \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \cdots \oplus \alpha^{n-1}\mathbb{Z}$. $\qquad K = \mathbb{Q}(\alpha) \xrightarrow{\sigma_i} \mathbb{C}$

$\qquad \alpha \longmapsto \alpha_i$.

$$\Delta(\mathbb{Z}[\alpha]) = \det\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ - & - & - & - & - \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^2 \quad \text{Matriz de Vandermonde.}$$

$$= \prod_{i<j} (\alpha_i - \alpha_j)^2, \quad \text{donde } f^\alpha_\mathbb{Q} = (x-\alpha_1)\cdots(x-\alpha_n).$$

Def Para $f \in \mathbb{Q}[x]$ mónico,

$f = (x-\alpha_1)\cdots(x-\alpha_n)$, el discriminante es

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Proposición Si $K = \mathbb{Q}(\alpha)$ α entero,

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f^\alpha_\mathbb{Q}).$$

Nota: la fórmula para $\Delta(f)$ es simétrica respecto a permutación de α_i. $\underset{\text{t. de Galois.}}{\Longrightarrow}$ $\Delta(f) \in \mathbb{Q}$.

Por otra parte, si $\alpha \in \mathcal{O}_K$ $\Rightarrow$ los α_i son enteros algebraicos.
$\Delta(f) \in \mathbb{Z}$.

Def Para
$$f = a(x-\alpha_1)\dots(x-\alpha_m)$$
$$g = b(x-\beta_1)\dots(x-\beta_n)$$
el **resultante**

$$\mathrm{Res}(f,g) = \boxed{a^n \cdot g(\alpha_1)\dots g(\alpha_m)}$$
$$= (-1)^{mn}\, b^m f(\beta_1)\cdots f(\beta_n)$$
$$= a^n b^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} (\alpha_i - \beta_j)$$

Prop. Para $f = (x-\alpha_1)\dots(x-\alpha_n)$ tenemos
$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \cdot \mathrm{Res}(f, f').$$

Dem •) Si f tiene raíces múltiples $\Rightarrow$ $\Delta(f) = 0$.
$\mathrm{Res}(f,f') = 0$.

•) Si f no tiene raíces múltiples,
$$\mathrm{Res}(f,f') = f'(\alpha_1)\dots f'(\alpha_n)$$
$$f = \prod (x-\alpha_i) \Rightarrow f' = \sum_i \prod_{j\neq i} (x-\alpha_j) \Rightarrow f'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$$
$$\mathrm{Res}(f,f') = \prod_i \prod_{j\neq i} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$
$$= (-1)^{\frac{n(n-1)}{2}} \cdot \Delta(f) \qquad \boxtimes$$

Corolario Si $K = \mathbb{Q}(\alpha)$, α - entero algebraico, $f \in \mathbb{Z}[x]$ - pol. mínimo de α
$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f) = (-1)^{\frac{n(n-1)}{2}} \cdot N_{K/\mathbb{Q}}(f'(\alpha))$$

Dem $\mathrm{Res}(f,f') = f'(\alpha_1)\dots f'(\alpha_n) = f'(\sigma_1(\alpha))\cdots f'(\sigma_n(\alpha))$
$$= \sigma_1(f'(\alpha))\cdots\sigma_n(f'(\alpha))$$
$$= N_{K/\mathbb{Q}}(f'(\alpha)) \qquad \boxtimes.$$

Ejemplo $K = \mathbb{Q}(\zeta_p)$, p primo (impar)

$$\mathcal{O}_K = \mathbb{Z}[\zeta_p] \qquad \Delta_K = \Delta(\mathbb{Z}[\zeta_p]) = (-1)^{\binom{p}{2}} N(\Phi_p'(\zeta_p))$$

$$\Phi_p(x) = \frac{x^p - 1}{x-1}. \qquad x^p - 1 = (x-1)\Phi_p.$$

$$p x^{p-1} = \Phi_p(x) + (x-1)\Phi_p'(x)$$

$$p \cdot \zeta_p^{p-1} = (\zeta_p - 1)\cdot \Phi_p'(\zeta_p).$$

$$N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p)) = \frac{N_{K/\mathbb{Q}}(p)\cdot N_{K/\mathbb{Q}}(\zeta_p)^{p-1}}{N_{K/\mathbb{Q}}(\zeta_p - 1)} = \frac{p^{p-1}}{p} = p^{p-2}$$

(**Ejercicio:** $N(\zeta_{p-1}) = \Phi_p(1) = p$)

Conclusión: $\Delta_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p(p-1)}{2}} \cdot p^{p-2}.$

Nota: el resultante $\mathrm{Res}(f,g)$ puede ser calculado usando la matriz de Sylvester.

$$f = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

$$g = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0.$$

Matriz de $(n+m)\times(n+m)$.

$$\mathrm{Res}(f,g) = \det \begin{array}{c} n\left\{ \begin{matrix} \\ \\ \\ \end{matrix}\right. \\ m\left\{ \begin{matrix} \\ \\ \\ \end{matrix}\right. \end{array} \begin{pmatrix} a_m & a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & \cdots & a_1 & a_0 & \cdots & 0 \\ & & & & \cdots & & & & \\ \hline b_n & b_{n-2} & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ & & & & \cdots & & & & \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & \cdots & b_1 & b_0 \end{pmatrix}$$

Ejemplo

•) $f = x^2 + ax + b$. $\qquad f' = 2x + a$

$$\Delta(f) = -\mathrm{Res}(f,f') = -\det\begin{pmatrix} 1 & a & b \\ 2 & a & 0 \\ 0 & 2 & a \end{pmatrix} = a^2 - 4b.$$

•) $f = x^3 + ax + b$, $\qquad f' = 3x^2 + a$

$$\Delta(f) = -\mathrm{Res}(f,f') = -\det\begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix} = -(4a^3 + 27b^2)$$

Ejemplo $\Delta(\mathbb{Z}[\sqrt{d}]) = \Delta(x^2-d) = 4d.$

$d \equiv 1\ (4)$: $\Delta\left(\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]\right) = \Delta\left(x^2 - x - \frac{d-1}{4}\right) = d.$ $\boxtimes$

Prop. Sea $K/\mathbb{Q}$ un campo de #. $\alpha \in \mathcal{O}_K$ t.q. $K = \mathbb{Q}(\alpha)$.

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f_{\mathbb{Q}}^{\alpha}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K.$$

Ejemplo Si $d \equiv 1\ (4)$. $K = \mathbb{Q}(\sqrt{d})$ $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

$$\underset{4d}{\underset{\shortparallel}{\Delta(\mathbb{Z}[\sqrt{d}])}} = \underbrace{[\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]]}_{=2}{}^2 \cdot \underbrace{\Delta_K}_{=d}$$

Ejemplo $K = \mathbb{Q}(\alpha)$, $\alpha^3 + \alpha - 1 = 0.$

$$\left.\begin{array}{l} \Delta(\mathbb{Z}[\alpha]) = \Delta(x^3+x-1) = -31 \\ \shortparallel \\ [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K \end{array}\right\} \quad \begin{array}{l} \mathcal{O}_K = \mathbb{Z}[\alpha], \\ \Delta_K = -31 \end{array}$$

Ejemplo $\Delta(x^2 - x + 6) = \Delta(x^3 - x + 1) = -23.$

$K = \mathbb{Q}(\alpha)$, $\alpha^2 - \alpha + 6 = 0.$ $\frac{1+\sqrt{-23}}{2}$

$= \mathbb{Q}(\sqrt{-23})$

$K' = \mathbb{Q}(\alpha)$, $\alpha^3 - \alpha + 1 = 0.$

$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ $\mathcal{O}_{K'} = \mathbb{Z}[\alpha].$

$\Delta_K = \Delta_{K'}$, aunque $K \not\cong K'$.

Ejemplo (Dedekind) $K = \mathbb{Q}(\alpha)$, $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$ (*)

$$\left.\begin{array}{l} \Delta(\mathbb{Z}[\alpha]) = \Delta(x^3 + x^2 - 2x + 8) = -2^2 \cdot 503. \\ \shortparallel \\ [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K. \end{array}\right\} \Rightarrow \begin{array}{l} \mathcal{O}_K = \mathbb{Z}[\alpha] \\ \text{ó} \\ [\mathcal{O}_K : \mathbb{Z}[\alpha]] = 2. \ \checkmark \end{array}$$

$$\left(\frac{2}{\alpha}\right)^3 \cdot (*) \Rightarrow \frac{64}{\alpha^3} - \frac{16}{\alpha^2} + \frac{8}{\alpha} + 8 = 0. \Leftrightarrow \left(\frac{4}{\alpha}\right)^3 - \left(\frac{4}{\alpha}\right)^2 + 2 \cdot \frac{4}{\alpha} + 8 = 0.$$

$\beta = \frac{4}{\alpha} \in \mathcal{O}_K$

$= -\frac{1}{2}\alpha^2 - \frac{1}{2}\alpha + 1 \notin \mathbb{Z}[\alpha]$.

$$\begin{array}{c} \mathcal{O}_K \\ | \\ \mathbb{Z}[\alpha,\beta] \\ | >1 \\ \mathbb{Z}[\alpha] \end{array} \Bigg) 2$$

$\mathcal{O}_K = \mathbb{Z}[\alpha, \beta] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z}$

$\alpha\beta = 4, \quad \alpha^2 = 2 - \alpha - 2\beta$

$\beta^2 = -2 - 2\alpha + \beta$.

$$\Delta(\mathcal{O}_K) = \Delta(\mathbb{Z}[\alpha,\beta]) = \det \begin{pmatrix} T(1) & T(\alpha) & T(\beta) \\ T(\alpha) & T(\alpha^2) & T(\alpha\beta) \\ T(\beta) & T(\alpha\beta) & T(\beta^2) \end{pmatrix}$$

$= -503$.

De hecho, $\mathcal{O}_K$ no es de la forma $\mathbb{Z}[\gamma]$ para $\gamma \in \mathcal{O}_K$.

Primero) en $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ tenemos factorización en ideales primos

$2\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$, donde $\mathfrak{p}_1 = (2 - \alpha - \beta)$

$\mathfrak{p}_2 = (5 - 3\alpha - 2\beta)$

$\mathfrak{p}_3 = (7 - 4\alpha - 3\beta)$.

diferentes ideales primos

Ahora) Supongamos que $\mathcal{O}_K = \mathbb{Z}[\gamma]$ para algún γ.

$\mathcal{O}_K = \mathbb{Z}[\gamma] \simeq \mathbb{Z}[x]/(f)$, f – un pol. cúbico.

Kummer – Dedekind: factorización de $2\mathcal{O}_K$

$\Updownarrow$

factorización de f en $\mathbb{F}_2[x]$.

Los pol. irreducibles en $\mathbb{F}_2[x]$:

deg 1: x, $x+1$.

deg 2: $x^2 + x + 1$.

deg 3: $x^3 + x + 1$, $x^3 + x^2 + 1$

$2\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \longleftrightarrow \bar{f} = \bar{g}_1 \cdot \bar{g}_2 \cdot \bar{g}_3$,

donde $\bar{g}_1, \bar{g}_2, \bar{g}_3$ son <u>diferentes</u> polinomios lineales en $\mathbb{F}_2[x]$.

$\boxed{\text{Contradicción!}}$