14/05

$$\begin{array}{ccccc} \mathbb{Z}[\alpha] & \subset & \mathcal{O}_K & \subset & K = \mathbb{Q}(\alpha) \\ n\,| & & n\,| & & | n \\ \mathbb{Z} & \subset & \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

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

Proposición Sea $R \subset K$ subanillo $R = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_n$

$R \subseteq \mathcal{O}_K \subseteq \frac{1}{d} R$, donde $d = \Delta(R)$

Dem $\alpha \in \mathcal{O}_K \Rightarrow \alpha = x_1\beta_1 + \cdots + x_n\beta_n$, $x_i \in \mathbb{Q}$.

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

$$\left.\begin{array}{l} \sigma_1(\alpha) = x_1\sigma_1(\beta_1) + \cdots + x_n\sigma_1(\beta_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \sigma_n(\alpha) = x_1\sigma_n(\beta_1) + \cdots + x_n\sigma_n(\beta_n) \end{array}\right\}$$

Regla de Cramer: $x_i = \frac{\gamma_i}{\delta}$, $\delta = \det\begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{pmatrix}$

$d = \Delta(R) = \delta^2$ $\quad x_i = \frac{\gamma_i \delta}{d}$ $\quad \gamma_i\delta = d \cdot x_i \in \mathbb{Q}$.

$\gamma_i\delta$ es un entero algebraico.

$\Rightarrow \gamma_i\delta \in \mathbb{Z}$.

$$\alpha \in \frac{\beta_1}{d}\mathbb{Z} \oplus \cdots \oplus \frac{\beta_n}{d}\mathbb{Z}. \qquad \square$$

Comentario .) $R \subset \mathcal{O}_K \Rightarrow$ todo $\alpha + \frac{1}{d}R \in \frac{1}{d}R/R$ o consiste en enteros algebraicos, o no contiene ninguno.

.) $d = [\mathcal{O}_K : R]^2 \cdot \Delta_K \Rightarrow$ suficiente considerar $\frac{1}{m}R/R$. donde $m^2 \mid d$.

.) $\#\left(\frac{1}{d}R/R\right) = d^n \Rightarrow$ podemos ocupar el resultado arriba si d es "pequeño".

Ejemplo $K = \mathbb{Q}(\sqrt[3]{15})$ $\quad \alpha = \sqrt[3]{15}$

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(x^3 - 15) = -27 \cdot 15^2 = -3^3 \cdot 15^2 = d$$

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K \subseteq \frac{1}{d}\mathbb{Z}[\alpha].$$

$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1, 3, 15, 3 \cdot 15 = m$

$\frac{a}{m} + \frac{b}{m}\alpha + \frac{c}{m}\alpha^2$ — cuándo son enteros algebraicos?

$a, b, c \in \mathbb{Z}$

los únicos elementos enteros de esta forma son

$$0,\ \underbrace{\frac{1}{3}+\frac{1}{3}\alpha+\frac{1}{3}\alpha^2}_{\beta},\ \underbrace{\frac{2}{3}+\frac{2}{3}\alpha+\frac{2}{3}\alpha^2}_{2\beta}.$$

$f_{\mathbb{Q}}^{\beta} = x^3 - x^2 - 6x - 12.$

Conclusión: $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.

$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3.$

$\Delta_K = -3 \cdot 19^2.$ ☒

§ Kummer–Dedekind

$R = \mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(f).$

$pR = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \longleftrightarrow \bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_s^{e_s}$ en $\mathbb{F}_p[x]$

si los $\mathfrak{p}_i$ son invertibles.

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

$$p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \Rightarrow \mathbb{Z}[\alpha]/(p) \xrightarrow{\simeq} \mathcal{O}_K/(p)$$

Dem $m = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

$$\begin{array}{ccccc} m\mathcal{O}_K & \hookrightarrow & \mathbb{Z}[\alpha] & \hookrightarrow & \mathcal{O}_K \\ \downarrow & & \downarrow & & \downarrow \\ m\mathcal{O}_K/(p) & \longrightarrow & \mathbb{Z}[\alpha]/(p) & \twoheadrightarrow & \mathcal{O}_K/(p) \\ m\mathcal{O}_K/(p) & \longrightarrow & \mathcal{O}_K/(p) & & \simeq \end{array}$$

es sobreyectivo. $p \nmid m \Rightarrow \exists\, m'$ t.q. $mm' \equiv 1 \ (p)$.

$x + (p) \in \mathcal{O}_K/(p) \rightsquigarrow x + (p) = xmm' + (p) \in m\mathcal{O}_K/(p)$.

$\Rightarrow m\mathcal{O}_K/(p) \simeq \mathcal{O}_K/(p)$.

$$\#(\mathbb{Z}[\alpha]/(p)) = \#(\mathcal{O}_K/(p)) = p^n.$$

$\Rightarrow \mathbb{Z}[\alpha]/(p) \simeq \mathcal{O}_K/(p)$. ☒

Ejemplo $K = \mathbb{Q}(\sqrt[3]{19})$. $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$,

$\alpha = \sqrt[3]{19}$, $\beta = \frac{1}{3}(1 + \alpha + \alpha^2)$.

$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3$

$[\mathcal{O}_K : \mathbb{Z}[\beta]] = 2.$

$f_{\mathbb{Q}}^{\beta} = x^3 - x^2 - 6x - 12.$

$3\mathcal{O}_K = \mathfrak{P}_1^2 \cdot \mathfrak{P}_2 \longleftrightarrow \overline{f}^{\mathfrak{P}} = x^2(x-1)$ en $\mathbb{F}_3[x]$.

Para $p \neq 3$, hay que factorizar $f = x^3 - 19$ mód p.

Por ejemplo, $\overline{f} = (x+1)(x^2+x+1)$ en $\mathbb{F}_2[x]$.

·) $p = 19 \Rightarrow \overline{f} = x^3$.

·) $p \equiv 2\ (3) \Rightarrow x \mapsto x^3$ es un autom. de $\mathbb{F}_p^\times$.

$\Rightarrow \exists!\ a$ t.q. $a^3 \equiv 19\ (p)$

$f = (x-a)\cdot$(cuadrático irred.)

·) $p \equiv 1\ (3) \Rightarrow \zeta \in \mathbb{F}_p^\times$ t.q. $\zeta \neq 1$, $\zeta^3 = 1$.

/ Si 19 no es un cubo mód p. $\Rightarrow$ $\overline{f}$ es irreducible en $\mathbb{F}_p[x]$.

\ Si 19 es un cubo mód $p \Rightarrow$

$\overline{f} = (x-a)(x-\zeta a)(x-\zeta^2 a)$ en $\mathbb{F}_p[x]$.

Conclusión:

·) $3\mathcal{O}_K = \mathfrak{P}_1^2 \cdot \mathfrak{P}_2$ $\quad f_1 = 1 \quad f_1 = 1$.

·) $19\mathcal{O}_K = \mathfrak{P}^3$

·) $p \equiv 1\ (3)$, $p \neq 19 \Rightarrow$

$\mathbb{Q}(\sqrt[3]{19})$

/ Si 19 es un cubo mód p, $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$.

\ Si 19 no es un cubo mód p, $p\mathcal{O}_K$ es primo.

·) $p \equiv 2\ (3) \Rightarrow p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$, $f_1 = 1$, $f_2 = 2$.

§ Ramificación

Def $K/\mathbb{Q}$ campo de #, $p \in \mathbb{Z}$ primo.

$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}$

e_i = índices de ramificación

f_i = grados de campos resid.

$\mathcal{O}_K/\mathfrak{P}_i \simeq \mathbb{F}_{p^{f_i}}$

Se dice que $\mathfrak{p}$ **se ramifica** si $e_i > 1$ para algún i.

Teorema $\sum_i e_i f_i = n = [K:\mathbb{Q}]$.

Def. para $K/\mathbb{Q}$, $\forall\, 0 \neq I \subset \mathcal{O}_K$, la **norma**

$$N_{K/\mathbb{Q}}(I) = \#(\mathcal{O}_K/I)$$

Lema 1) $N(I\mathcal{J}) = N(I)\cdot N(\mathcal{J})$

2) $N_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$

Dem. 1) $I = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_s^{e_s}$ t.c.d.r. $\Rightarrow N(I) = N(\mathfrak{P}_1^{e_1})\cdots N(\mathfrak{P}_s^{e_s})$.

Hay que ver que $N(\mathfrak{P}^e) = N(\mathfrak{P})^e$.

Hemos visto que en gral. para un ideal primo invertible $\mathfrak{P} \subset R \subset K$.

$$\#(R/\mathfrak{P}^e) = \#(R/\mathfrak{P})^e.$$

2) $\alpha\mathcal{O}_K$ es la imagen de la apl. $\mathbb{Z}$-lineal.

$$\mu_\alpha : \mathcal{O}_K \longrightarrow \mathcal{O}_K$$
$$x \longmapsto \alpha x.$$

$$[\mathcal{O}_K : \alpha\mathcal{O}_K] = |\det \mu_\alpha| = |N_{K/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|. \quad \boxtimes$$

Demostración del teorema

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_s^{e_s}.$$

$$\left.\begin{aligned} N(p\mathcal{O}_K) &= p^n \\ N(\mathfrak{P}_i^{e_i}) &= N(\mathfrak{P}_i)^{e_i} = p^{f_i e_i} \end{aligned}\right\} \Rightarrow p^n = p^{\sum f_i e_i}.$$

$$\sum_i f_i e_i = [K:\mathbb{Q}] \qquad \boxtimes$$

§ Ramificación y discriminante.

Sea α un entero algebraico, $f = f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[x]$.

$p \in \mathbb{Z}$ primo.

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

$p \mid \Delta(\mathbb{Z}[\alpha]) \Rightarrow \bar{f}$ tiene raíz múltiple en $\overline{\mathbb{F}_p}[x]$.

$\Rightarrow \bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_s^{e_s}$ en $\mathbb{F}_p[x]$ donde $e_i > 1$ para algún i.

Teorema $p \mid \Delta_K \iff p$ se ramifica $\left(p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}, \ e_i > 1 \right)$.

Lema. $\Delta_K \bmod p = \Delta\left(\mathcal{O}_K/(p) \,/\, \mathbb{F}_p\right)$

(Discr. de $\mathcal{O}_K/(p)$ como $\mathbb{F}_p$-álgebra.)

Dem.

$$\begin{array}{ccc} \mathcal{O}_K & \twoheadrightarrow & \mathcal{O}_K/(p) \\ \downarrow N_{K/\mathbb{Q}},\ T_{K/\mathbb{Q}} & \hookrightarrow & \downarrow N_{\mathcal{O}_K/(p)/\mathbb{F}_p},\ T_{\mathcal{O}_K/(p)/\mathbb{F}_p} \\ \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p \end{array}$$

$\mathcal{O}_K/(p) \simeq \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{F}_p$, y las trazas y determinantes conmutan con $\otimes$.

Si $\alpha_1, \dots, \alpha_n$ es una base de $\mathcal{O}_K$ sobre $\mathbb{Z}$.

$\Rightarrow \bar{\alpha}_1, \dots, \bar{\alpha}_n$ es una base de $\mathcal{O}_K/(p)$ sobre $\mathbb{F}_p$.

$$\Delta_K = \Delta(\alpha_1, \dots, \alpha_n) = \det\left(T_{\mathcal{O}_K/\mathbb{Z}}(\alpha_i \alpha_j) \right)$$

$$\Delta_K \bmod p = \det\left(T_{\mathcal{O}_K/(p)/\mathbb{F}_p}(\bar{\alpha}_i \bar{\alpha}_j) \right) = \Delta(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$$

$$= \Delta\left(\mathcal{O}_K/(p) \,/\, \mathbb{F}_p\right)$$

Lema 2 Si A, B son k-álgebras de dim. fin. sobre un campo k, entonces,

$$\Delta(A \times B / k) = \Delta(A/k) \times \Delta(B/k).$$

$\boxtimes$

Dem Sea $a_1, \dots, a_m$ una base de A sobre k.

$b_1, \dots, b_n$ una base de B sobre k

$(a_1, 0), \dots, (a_m, 0), (0, b_1), \dots, (0, b_n)$ - una base de $A \times B$.

$$\Delta(A \times B / k) = \det \begin{pmatrix} T_{A/k}(a_i a_j) & 0 \\ 0 & T_{B/k}(b_k b_\ell) \end{pmatrix} = \det\left(T_{A/k}(a_i a_j)\right) \times \det\left(T_{B/k}(b_k b_\ell)\right)$$

$$= \Delta(A/k) \cdot \Delta(B/k)$$

□

Lema Para $\mathfrak{p} \subset \mathcal{O}_K$ tenemos

$$\Delta(\mathcal{O}_K / \mathfrak{p}^e / \mathbb{F}_p) = 0 \iff e > 1.$$

Dem $A = \mathcal{O}_K / \mathfrak{p}^e$.

Si $e = 1$: $A \simeq \mathbb{F}_p[x] / (g)$

$g = (x - \alpha_1) \cdots (x - \alpha_s)$ en $\overline{\mathbb{F}}_p[x]$.

$\alpha_i \neq \alpha_j$.

$$\Delta(A / \mathbb{F}_p) = \Delta(g) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \neq 0.$$

Si $e > 1$: $A = \mathcal{O}_K / \mathfrak{p}^e$, podemos tomar una base de A sobre $\mathbb{F}_p$ que contiene $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$. En este caso $\bar{\alpha}^e = 0$.

Tenemos un nilpotente $\bar{\alpha} \in A$.

Para cualquier $\bar{\beta} \in A$, $\bar{\alpha}\bar{\beta}$ es t.b. un nilpotente.

$\mu_{\bar{\alpha}\bar{\beta}} : A \to A$, $x \mapsto \bar{\alpha}\bar{\beta}$ es nilpotente $\Rightarrow$

$$T(\mu_{\bar{\alpha}\bar{\beta}}) = 0 = T_{A/k}(\bar{\alpha}\bar{\beta})$$

$$\Delta(A / \mathbb{F}_p) = 0.$$

□

Demostración del teorema

$\left(p \mid \Delta_K \iff \mathfrak{p}_i = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}, \ e_i > 1 \text{ para algún } i. \right)$

t.c.d.s: $\mathcal{O}_K/(p) \simeq \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_s^{e_s}$.

iso de $\mathbb{F}_p$-álgebras.

$$\Delta_K \bmod p = \prod_i \underbrace{\Delta(\mathcal{O}_K/\mathfrak{p}_i^{e_i}/\mathbb{F}_p)}_{=0 \iff e_i > 1}.$$

□

Corolario Hay un # finito de primos $p \in \mathbb{Z}$ que se ramifican en K.

Ejemplo •) $K = \mathbb{Q}(\sqrt{d})$

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

•) $K = \mathbb{Q}(\zeta_p)$ $\quad \Delta_K = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$.

el único p que se ramifica en $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ es el mismo p.