

26/12/18

7 תשובות

(2.933) נתון O_L/O_K , n איברי L/K $x_1, \dots, x_n$ נבחרים
- נבחרים

$$\Delta(x_1, \dots, x_n) = \det(T_{L/K}(x_i, x_j))_{i,j}$$

$$\Delta(O_L/O_K) = \sum_{\substack{L/K \text{ איברי} \\ x_1, \dots, x_n \in O_L}} \Delta(x_1, \dots, x_n) \cdot x_i \in O_L \Rightarrow \Delta(x) \in O_K$$

- יש $x_1, \dots, x_n \in O_K$ שהם איברי O_L ו- $O_L = O_K$ הם איברי O_L

$$\Delta(O_L/O_K) = \Delta(x) O_K$$

$$\Delta(O_L/O_K) \in \mathbb{P} \Leftrightarrow O_L \text{ איברי } \mathbb{P} \text{ ו- } O_K \text{ איברי } \mathbb{P}$$

הערה: $O_K = \mathbb{P}$ - $\mathbb{P}$ איברי $\mathbb{P}$

$O_K = \mathbb{P}$ - $\mathbb{P}$ איברי $\mathbb{P}$ ו- O_K איברי $\mathbb{P}$

יש $x_1, \dots, x_n \in O_K$ שהם איברי O_L ו- $O_L = O_K$

יש $x_1, \dots, x_n \in O_K$ שהם איברי O_L ו- $O_L = O_K$

$$\Delta(O_L/O_K) = \Delta(x) O_K$$

$$O_L = \bigoplus x_i O_K$$

, $\mathbb{P}$

, $\mathbb{P}$

$$\bigoplus O_L/\mathbb{P} O_L = \bigoplus \bar{x}_i O_K/\mathbb{P}$$

יש $x_i \in O_K$ שהם איברי O_L ו- $O_L = O_K$

יש $x_i \in O_K$ שהם איברי O_L ו- $O_L = O_K$

$$y x_i = \sum_{j=1}^n a_{ij}(y) x_j$$

- יש $\mathbb{P} O_L$ איברי $\mathbb{P}$

$$\left[\begin{array}{c} \text{איברי} \\ \mathbb{P} O_L \end{array} \right]$$

$$\bar{y} x_i = \sum_{j=1}^n \bar{a}_{ij}(y) \bar{x}_j$$

יש $\bar{x}_1, \dots, \bar{x}_n$ שהם איברי $\bar{y}$ ו- $\bar{y}$ איברי $\bar{y}$

יש $\bar{x}_1, \dots, \bar{x}_n$ שהם איברי $\bar{y}$ ו- $\bar{y}$ איברי $\bar{y}$

יש $\bar{x}_1, \dots, \bar{x}_n$ שהם איברי $\bar{y}$ ו- $\bar{y}$ איברי $\bar{y}$

$$\text{Tr}(\bar{y}) = \sum a_{ii}(y) = \sum \bar{a}_{ii}(y) = \text{Tr}_{L/K}(y)$$

יש $y = x_i x_j$ שהם איברי $\mathbb{P}$ ו- $y \in O_L$ איברי $\mathbb{P}$

$$\Delta(x_1, \dots, x_n) = \det(T_{L/K}(x_i, x_j)) = \det(T_{L/K}(\bar{x}_i, \bar{x}_j)) = \Delta(\bar{x}_1, \dots, \bar{x}_n)$$

$$A(Q|O_K) \in P \stackrel{*}{\Leftrightarrow} A(x_1, \dots, x_n) \in \beta \Leftrightarrow A(\bar{x}_1, \dots, \bar{x}_n) = 0$$

2.3) נוסח O_L/P נגזר על ידי $p \in O_L = \beta_1 e_1 + \dots + \beta_g e_g$

$$O_L / p O_L \cong \bigoplus_{i=1}^g O_L / \beta_i e_i$$

CRT

2.4) נוסח $u_1, \dots, u_n$ נגזר על ידי $u_1, \dots, u_n = \bar{u}_1, \dots, \bar{u}_n$

2.5) נוסח O_L / β_i

2.6) נוסח O_L / β_i נגזר על ידי O_L / β_i נגזר על ידי O_L / β_i

$$T_i : O_L / \beta_i \rightarrow O_K / p$$

2.7) נוסח O_L / β_i נגזר על ידי O_L / β_i

2.8) נוסח O_L / β_i נגזר על ידי O_L / β_i

$$\left(\begin{array}{c} \boxed{\Gamma_{\mu_1, \mu_2, \mu_3}} \\ \boxed{\Gamma_{\mu_4, \mu_5}} \end{array} \right)$$

$$Tr(\bar{y}) = Tr_1(y_1) + \dots + Tr_g(y_g)$$

2.9) נוסח O_L / p נגזר על ידי O_L / p

$$\Delta(u_1, \dots, u_n) = \prod \Delta_i$$

- זהו

$$\Delta_1 = \Delta(u_1, \dots, u_{f_1})$$

$$\Delta_2 = \Delta(u_{f_1+1}, \dots, u_{f_1+f_2})$$

;

$$\Delta(u) = \prod_{i=1}^g \Delta_i$$

$\Leftarrow$

הנה $\mathbb{C}/\beta_i$ זהו המרחב $\mathbb{C}/\beta_i$ של המרחב $\mathbb{C}/\beta_i$

$$\mathbb{C}/\beta_i$$

- זהו המרחב $\mathbb{C}/\beta_i$

$$\Delta(\bar{x}_1, \dots, \bar{x}_n) = \det \Delta(u_1, \dots, u_n)$$

$$0 \neq \det \begin{pmatrix} \beta_1 & \beta_2 \\ \beta_3 & \beta_4 \end{pmatrix}$$

- זהו המרחב $\mathbb{C}/\beta_i$ של המרחב $\mathbb{C}/\beta_i$

$$0 = \Delta(\bar{x}_1, \dots, \bar{x}_n)$$

הנה $\mathbb{C}/\beta_i$ זהו המרחב $\mathbb{C}/\beta_i$ של המרחב $\mathbb{C}/\beta_i$

$$0 = \text{Tr}(u_i u_j) \Leftrightarrow u_i u_j = 0, u_i^2 = 0$$

$$\Delta(u) = \det \begin{pmatrix} \text{Tr}(u_1 u_1) & \dots & \text{Tr}(u_1 u_n) \\ \vdots & & \vdots \\ \text{Tr}(u_n u_1) & \dots & \text{Tr}(u_n u_n) \end{pmatrix} =$$

$$= \det \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} = 0$$

$$\Rightarrow \Delta(u) = 0 \Rightarrow \Delta(\bar{x}) = 0$$

הנה $\mathbb{C}/\beta_i$ זהו המרחב $\mathbb{C}/\beta_i$ של המרחב $\mathbb{C}/\beta_i$

$$\Delta(\bar{x}) = 0$$

הנה $\mathbb{C}/\beta_i$ זהו המרחב $\mathbb{C}/\beta_i$ של המרחב $\mathbb{C}/\beta_i$

הנה $\mathbb{C}/\beta_i$ זהו המרחב $\mathbb{C}/\beta_i$ של המרחב $\mathbb{C}/\beta_i$

משפט: (קרויבר)

יהי p מספר ראשוני, $\mathcal{O}_K$ תת-בנייה של $\mathbb{Q}$, ו- L תת-בנייה של $\mathcal{O}_K$.
 אז, $\mathcal{O}_{K,p}$ הוא תת-בנייה של $\mathcal{O}_K$ ו- $\mathcal{O}_L$ הוא תת-בנייה של $\mathcal{O}_{K,p}$.
 אם $f \in \mathcal{O}_K[x]$ הוא פולינום, אז $f \pmod{p}$ הוא פולינום ב- $\mathcal{O}_K/p\mathcal{O}_K$.
 אם $f \in \mathcal{O}_K[x]$ הוא פולינום, אז $f \pmod{p}$ הוא פולינום ב- $\mathcal{O}_K/p\mathcal{O}_K$.

$$\bar{f} = \varphi_1^{e_1} \cdots \varphi_g^{e_g}$$

אם $\mathcal{O}_{K,p}[x] \ni \varphi_i$ אז φ_i הוא פולינום ב- $\mathcal{O}_{K,p}$.

$$p = \beta_1^{e_1} \cdots \beta_g^{e_g}$$

$$f_i = f(\beta_i) = \deg \varphi_i$$

$$= [\mathcal{O}_K/\beta_i : \mathcal{O}_K/p]$$

כל φ_i הוא פולינום ב- $\mathcal{O}_K/p$.

הוכחה: נניח $\mathcal{O}_K$ הוא תת-בנייה של $\mathbb{Q}$, אז $\mathcal{O}_K$ הוא תת-בנייה של $\mathbb{Z}$.
 אז $\mathcal{O}_K$ הוא תת-בנייה של $\mathbb{Z}$.
 $\mathcal{O}_L = \mathcal{O}_K[x] = \mathcal{O}_K[x]/\langle f(x) \rangle$

$$\mathcal{O}_L/p\mathcal{O}_L \cong \mathcal{O}_K[x]/\langle f(x) \rangle \cong \mathcal{O}_K[x]/\langle \bar{f}(x) \rangle \cong \prod (\mathcal{O}_K[x]/\langle \varphi_i^{e_i} \rangle)$$

כיוון ש- $\mathcal{O}_K[x]/\langle \varphi_i^{e_i} \rangle$ הוא תת-בנייה של $\mathcal{O}_K[x]/\langle \varphi_i \rangle$, אז $\mathcal{O}_L/p\mathcal{O}_L$ הוא תת-בנייה של $\mathcal{O}_K[x]/\langle \varphi_i \rangle$.
 אז $\mathcal{O}_L/p\mathcal{O}_L$ הוא תת-בנייה של $\mathcal{O}_K[x]/\langle \varphi_i \rangle$.

$$\mathcal{O}_L \longrightarrow \mathcal{O}_L/p\mathcal{O}_L \longrightarrow \mathcal{O}_K[x]/\langle \varphi_i \rangle$$

$$\mathcal{O}_L/p\mathcal{O}_L \cong \mathcal{O}_K[x]/\langle \varphi_i \rangle \pmod{p}, \quad \beta_i = \alpha_i \pmod{p}$$

$$\beta_i^r \bmod p \approx \psi_i^r k(p)(x) / \psi_i^r e_i$$

□

$$e(\beta_i) = e_i \quad \text{אם } N \text{ זוגי}$$

$$\text{כעת נניח } \beta_i = 0 \text{ ונניח } \beta_i = 0 \text{ ונניח } \beta_i = 0 \text{ ונניח } \beta_i = 0 \text{ ונניח } \beta_i = 0$$

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

$$N \geq \max \{ |a_i| \} \quad \text{אם } 50\% < 70\%$$

$$L = \mathbb{Q}[x]/f, \quad \text{כעת נניח } \beta_i = 0 \text{ ונניח } \beta_i = 0$$

$$(g \text{ ו } f \text{ זוגי})$$

$$L = k(\theta) \text{ ו } \theta \in \mathbb{Q}_L \text{ ו } \Delta(\theta) = \Delta(\theta) \text{ ו } \Delta(\theta) = \Delta(\theta) \text{ ו } \Delta(\theta) = \Delta(\theta)$$

$$\mathbb{Q}_k[\theta] \subseteq \mathbb{Q}_L \subseteq \frac{1}{\Delta(\theta)} \mathbb{Q}_k[\theta] \quad (1)$$

$$\Delta(\theta) \notin p \text{ ו } \Delta(\theta) \in p \text{ ו } \Delta(\theta) \in p \text{ ו } \Delta(\theta) \in p$$

$$\mathbb{Q}_L \mathbb{Q}_{k,p} = \mathbb{Q}_{k,p}[\theta]$$

$$\mathbb{Q}_k[\theta] \subseteq \mathbb{Q}_L \text{ ו } \mathbb{Q}_k[\theta] \subseteq \mathbb{Q}_L \text{ ו } \mathbb{Q}_k[\theta] \subseteq \mathbb{Q}_L$$

$$\Delta(\theta) \mathbb{Q}_L = \bigcap_p \mathbb{Q}_{k,p}[\theta] = \mathbb{Q}_k[\theta]$$

$$\mathbb{Q}_{k,p} \rightarrow \mathbb{Q}_L \text{ ו } \mathbb{Q}_{k,p} \rightarrow \mathbb{Q}_k \text{ ו } \mathbb{Q}_{k,p} \rightarrow \mathbb{Q}_k$$

$$\theta^{i-1} = \sum_{j=1}^n a_{ij} x_j, \quad a_{ij} \in \mathbb{Q}_k$$

$$A = (a_{ij})$$

$$B = A^{-1} \in GL_n(k) \text{ ו } \det A = d \neq 0 \text{ ו } \det B = d^{-1}$$

$$X_n = \sum_{i=1}^n b_i \otimes i^{-1}$$

ה'תשס"ב י"ג

$$y = \sum_{k=0}^n r_k x_k = \sum_{i,k=1}^n r_k b_{ik} \theta^{i-1}$$

1561

$$dy = \sum_{i,k} \underbrace{r_{ik}}_{\in \mathbb{O}_n} \underbrace{d \cdot b_{ik}}_{\in \mathbb{O}_n} \cdot \underbrace{0^{i-1}}_{\in \mathbb{O}_n \setminus \{0\}}$$

$$\Rightarrow dy \in \mathcal{O}_K[0]$$

$\Rightarrow$ für $\Delta(x) = \Delta^2(x) - c$ (25)

$$\Delta(\varnothing) \cdot y = d^2 \Delta(x) y = d \Delta(x) \cdot dy \in \mathcal{O}_K[\varnothing]$$

日

$p-2$ n $1-n$ 0 1 2

: $\Delta(0)$ $\rho_{1/2}$

משפט: תהי $L = L(\phi)$ הריחוק סכימטי k, n של ϕ .

ה'תשנ"ח ע"ה

$$\Delta(\mathcal{D}) = (-1)^{n(n-1)/2} \text{Norm}_{L/K} (f'(\theta))$$

הוכחה: (NO) $\Rightarrow$ $\emptyset = \emptyset_1, \dots, \emptyset_n$ $\Rightarrow$ $\emptyset$ קההה $\Rightarrow$ $\emptyset$ $\Rightarrow$ $\emptyset$

$$f(x) = \prod_{j=1}^n (x - \theta_j)$$

$$f'(\theta_i) = \prod_{j \neq i} (\theta_i - \theta_j)$$

$$\Rightarrow \text{N}_{\frac{1}{k}} f'(0) = \prod_{i=1}^n \prod_{j \neq i} (0_i - 0_j)$$

$$N_{L/n} f'(\theta) = (-1)^{\binom{n}{2}} \prod_{i < j} (\theta_i - \theta_j)^2$$

128

33N

$$\Delta(\theta) = \det V V^T = (\det V)^2 = \prod_{i=1}^n (\theta_i - \theta_j)^2$$

$$V = V(\theta_1, \dots, \theta_n)$$

מטריצה סימטרית

משפט 1: $f = x^n - a$ הוא פולינום ב- x מעל $\mathbb{Q}$ אם ורק אם a אינו n -עוצם של מספר רציונלי.

$$f' = nx^{n-1}$$

$$N(\theta) = (-1)^n a^{n-1}$$

$$\Rightarrow N(f'(\theta)) = (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot a^{n-1} = (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot a^{n-1}$$

למשל: $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$, $f = x^3 - 2$, $\theta = \sqrt[3]{2}$

$$\Delta(\theta) = -3^3 \cdot 2^2$$

לפי משפט 1, $\mathbb{Q}(\sqrt[3]{2})$ אינו פולינום ב- x מעל $\mathbb{Q}$.

$$\mathbb{Z}_p[\theta] = \mathbb{Z}_p[x]$$

אם $\mathbb{Q}_L \rightarrow \mathbb{Q}$ הוא פולינום ב- x מעל $\mathbb{Q}$, אז $\mathbb{Q}_L$ אינו פולינום ב- x מעל $\mathbb{Q}$.

מסלול	פולינום ב- x מעל $\mathbb{Q}$	מסלול
$\mathbb{Q}_L = \mathbb{Q}$	$x^3 - 2$	7
$27\mathbb{Q}_L = \mathbb{Q}_1, \mathbb{Q}_2, \mathbb{Q}_3$	$(x+3)(x^3-3x+1)$	27
$31\mathbb{Q}_L = \mathbb{Q}_1, \mathbb{Q}_2, \mathbb{Q}_3$	$(x-4)(x-3)(x+1)$	31

משפט 2: $(\mathbb{Q}_L \supset \mathbb{Q}) \quad \mathbb{Z}[\theta] \cong \mathbb{Z}[x]/(f(x))$

$$2\mathbb{Z}[\theta] = \theta^3 \mathbb{Z}[\theta]$$

למשל: $2\mathbb{Q}_L = \theta^3 \mathbb{Q}_L = \prod_{i=1}^g \mathbb{Q}_i^{e_i}$

$$\theta \mathbb{Q}_L = \mathbb{Q}_1^{e_1} \dots \mathbb{Q}_g^{e_g}$$

משפט 3: $e_i f_i = 1$ (כאן $p \nmid e_i$)

$$\sum_{i=1}^g e_i f_i = 1$$

— נורמל פונקציה α^3 (כ) פונקציה α^3 — $p=3$
 $(\mathbb{Z}[0] = \mathbb{Z}[0])$, $\alpha = 0+1$ נוס . (ד) α^3 נוס

— α ל α^3 נוס
 $(x-1)^3 - 2 = x^3 - 3x^2 + 3x - 3$

אם α^3 נוס פונקציה α^3 נוס
 $[\alpha^3]$ נוס α^3 נוס α^3 נוס

$(u = \alpha^2 - \alpha + 1)$ $\alpha^3 = 3u$ $\Leftarrow$

$3^3 \text{Norm}(u) = \text{Norm}(\alpha^3) = 3^3$, נוס

$\Rightarrow \text{Norm}(u) = 1$

, נוס

$u \cdot \bar{u} = \text{Norm } u = 1$
 $\bar{u} = \alpha^2 + \alpha + 1$

, נוס $u = \alpha^2 - \alpha + 1$, נוס

~~נוס~~

$3\alpha = \alpha^3 \alpha$

פונקציה 3 נוס (α^3) נוס $\alpha \alpha$ $\Leftarrow$
 $\bar{u} = \alpha^2 + \alpha + 1$

נוס α^3 ל α^3 נוס

נוס α^3 נוס α^3 נוס α^3 נוס
 α^3 נוס α^3 נוס α^3 נוס

$\text{Norm}_{L/K}(\sigma) = \langle \text{Norm}_{L/K}(a) \mid a \in \sigma \rangle$ — (over $\mathbb{Q}_K$)
 α^3 נוס α^3 נוס

$\text{Norm}_{L/K}(\sigma) = \mathbb{Q}_K \text{Norm}_{L/K}(\alpha)$, נוס , $\sigma = \mathbb{Q}_K$ אל (1)

(נוס)

α^3 , α^3 , α^3 נוס (2)

$\text{Norm}(a \mathbb{Q}_K) = \text{Norm}(a) \mathbb{Q}_K$

$\text{Norm}_{L/K}(\sigma \tau) = \text{Norm}_{L/K}(\sigma) \text{Norm}_{L/K}(\tau)$ (3)

□

2022-23

$$\pi_N(q_j)^{b_j}$$

$$\sigma = \prod \beta_i^{a_i}$$

$$\mathcal{J} = f(\beta/p)$$

$$G = \text{Gal}(L/K)$$

123115

حصان

6

$$PG_L = \pi$$

$$\leftarrow rge = n - fge \leftarrow$$

710

$$\int \sin x \, dx$$

$p \quad f(Q/p)$

$$= X_{\text{norm}}(Q) = \dots =$$

$$\text{Norm}_{K/k} \text{Norm}_{N/K} (Q) =$$

$$= \text{Norm.}(\beta^{f(\omega|\beta)}) =$$

$$= \frac{f(q|\beta)}{\text{Norm}(\beta)} = p^\top \cdot f(q|\beta)$$

$r = f(p/r)$ (ה'ש'ת, תש"ח) $\in$

נתן אימ' 2 Norm ל Norm אימ' 2 Norm - הנחיה

$$\text{Norm} : I(\mathcal{O}_L) \longrightarrow I(\mathcal{O}_K)$$

(אידיאלים)

$$\text{Norm} : \mathcal{O}_L \longrightarrow \mathcal{O}_K$$

כ' נרמ' $f \in \mathcal{O}_K$ = נרמ' = נרמ'.

2/1/12

הרצאה 10

מספרים

מנחים נרמ' - $\mathcal{O}_K = \mathbb{Z}$, $K = \mathbb{Q}$ - $L = \mathbb{Q}$ מספרים $\mathbb{Q}$ - $L = \mathbb{Q}$ מספרים
הנחיה: נרמ' - (נרמ' ל $L = \mathbb{Q}$ - $\mathbb{Z}$)

$$\mathcal{O}_L = \mathbb{Z} = \mathcal{O}_K \quad \text{הנחיה} \quad \mathcal{O}_L = \mathbb{Z} \quad \mathcal{O}_K = \mathbb{Z}$$

נרמ' ל אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים
אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים
נרמ' $N(\mathcal{O}_L) = \mathcal{O}_K$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים
נרמ' $N(\mathcal{O}_L) = \mathcal{O}_K$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים

(Counting norm) נרמ' - $N(\mathcal{O}_L) = \mathcal{O}_K$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים
נרמ' $N(\mathcal{O}_L) = \mathcal{O}_K$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים
נרמ' $N(\mathcal{O}_L) = \mathcal{O}_K$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים
נרמ' $N(\mathcal{O}_L) = \mathcal{O}_K$ - $\mathcal{O}_K$ אידיאלים $\mathcal{O}_L$ - $\mathcal{O}_K$ אידיאלים

$$\# \mathcal{O}_L / \mathfrak{p}^k = p^{kf} = N(\mathfrak{p}^k) = N(\mathfrak{p})^k$$

סכום ל של אידיאלים

נרמ' (אידיאלים)

$$U_p(m) \equiv 0 \pmod{p^2}, p \equiv 3 \pmod{4} \iff a, b \in \mathbb{Z}, m = a^2 + b^2$$