

נתון איברי $\mathcal{O}_L$ Norm $\rightarrow$ איברי $\mathcal{O}_K$ הנמצאים -

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

(איברי) (איברי)

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

כל איברי $\mathcal{O}_L$ הוא איברי $\mathcal{O}_K$

2/1/18

הרצאה 10

משפטים

מניחים $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.
 נניח $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.

$$\mathcal{O}_L = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \text{ או } \mathbb{Z}[\sqrt{d}]$$

נניח $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.
 נניח $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.
 נניח $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.

נניח $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.
 נניח $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.
 נניח $L = \mathbb{Q}(\sqrt{d})$ d איברי $\mathbb{Z}$ אי-ריבועי.

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

כל איברי $\mathcal{O}_L$ הוא איברי $\mathcal{O}_K$

משפט: (רייט)

$$U_p(n) = 0 \text{ (mod } p), p = 3 \text{ (mod } 4) \Leftrightarrow a, b \in \mathbb{Z}, n = a^2 + b^2$$

הוכחה: (1.3.1)

$$\# \{n \leq x \mid \exists a, b \in \mathbb{Z} : n = a^2 + b^2\} \sim \frac{x}{\sqrt{4\pi}} \quad \text{למשל}$$

(1.1) (1.2)

$$b_i = z \in \mathbb{Z}[i], \quad u = \text{Norm}_{\mathbb{Q}(i)/\mathbb{Q}}(z) \Leftrightarrow n = a^2 + b^2 \quad \text{הוכחה: (1.1) (1.2)}$$

$$z \in \mathbb{Z}[i], \quad 0 \leq n \in \mathbb{Z} \quad \text{נניח}$$

$$z \in \mathbb{Z}[i] = \prod p_j^{a_j}$$

$$N(z) = \prod_{j: f(\beta_j)=1} p_j^{a_j} \prod_{j: f(\beta_j)=2} p_j^{2a_j}$$

$$p_j = \beta_j \cap \mathbb{Z}$$

$$p_j = \beta_j \cap \mathbb{Z}$$

$$f(\beta_j) = 1 \Leftrightarrow p_j \equiv 1 \pmod{4}$$

$$f(\beta_j) = 2 \Leftrightarrow p_j \equiv 3 \pmod{4}$$

$$p \in \mathbb{Z} \text{ ראשוני} \quad p \equiv 1 \pmod{4} \Leftrightarrow p = f(\beta_j) \Leftrightarrow p_j = p \quad \text{למשל}$$

$$p \equiv 3 \pmod{4} \quad \text{לא ניתן לכתוב כסכום של שני ריבועים}$$

$$x^2 + 1 \equiv 0 \pmod{p} \Leftrightarrow f(\beta) = 2 \quad \text{יש קשר}$$

$$p \equiv 1 \pmod{4} \Leftrightarrow p = f(\beta) \Leftrightarrow p_j = p \quad \text{למשל}$$

הוכחה: (1.3.1) - הוכחה של הנוסחה

$$p = a^2 + b^2 \Leftrightarrow p \equiv 1 \pmod{4} \quad \text{למשל}$$

$$p \equiv 3 \pmod{4} \quad \text{לא ניתן לכתוב כסכום של שני ריבועים}$$

$$p \equiv 1 \pmod{4} \Leftrightarrow p = f(\beta) \Leftrightarrow p_j = p \quad \text{למשל}$$

$$n = [1: k] \quad \text{למשל}$$

$$m = |\Delta(\theta)|, \quad S = \left\{ \frac{1}{m} \sum_{i=0}^{m-1} a_i \theta^i \mid 0 \leq a_i \leq m-1 \right\}$$

$$z = \frac{1}{m} \sum_{i=0}^{m-1} b_i \theta^i \quad \text{למשל}$$

$$b_i = a_i + m k_i \quad \text{למשל}$$

$$z = \frac{1}{m} \sum_{i=0}^{m-1} a_i \theta^i + \sum_{i=0}^{m-1} k_i \theta^i$$

$$|S| = m^m \quad \text{למשל}$$

$$S_p = \left\{ \frac{1}{p} \sum_{i=0}^{p-1} a_i \theta^i \mid 0 \leq a_i \leq p-1 \right\} \quad \text{למשל}$$

$$O_L = \mathbb{Z}[\theta] \quad \text{למשל}$$

הוכחה: (1.3.1)

המשפט: $L = \mathbb{Q}(\sqrt{2})$, $\Delta = -2^3$ כלומר $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}] - 0$

הטעם, $\mathbb{Z}$ הוא $\mathbb{Z}$ ו- $\mathbb{Z}[\sqrt{2}]$ הוא $\mathbb{Z}[\sqrt{2}]$.
 $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ ו- $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$
 כלומר $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$

$$\left(\frac{0+\sqrt{2}}{2} \right) \text{ נשלב}$$

$$\frac{0+\sqrt{2}}{2} = \frac{\sqrt{2}}{2}$$

$$\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$$

$$\theta \mapsto \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \theta^2 \mapsto \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\Rightarrow \frac{0+\sqrt{2}}{2} \mapsto \begin{pmatrix} 0 & 1 & 1 \\ \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}$$

הזכרנו ש- $\frac{1}{2}$ הוא

$$\frac{1}{2} + \frac{1}{4} = \frac{3}{4} \notin \mathbb{Z}$$

ה- $\mathbb{Z}[\sqrt{2}]$ הוא $\mathbb{Z}[\sqrt{2}]$ ו- $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$
 כלומר $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$

כלומר $L = \mathbb{Q}(\sqrt{2})$ ו- $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$.
 כלומר $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$ ו- $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$

$$y = \frac{1}{4d} (a+b\theta), \quad a, b \in \mathbb{Z}$$

$$(1, 0) : y = 2 \text{ הוא } \frac{1}{4d}$$

$$r_y = \frac{1}{4d} \begin{pmatrix} a & b\theta \\ 1 & a \end{pmatrix}$$

$$x^2 - \frac{a}{2d}x + \frac{a^2 - db^2}{16d^2} = 0$$

$$\frac{a}{2d} \in \mathbb{Z} \Leftrightarrow a \in d\mathbb{Z}$$

$$\frac{a^2 - db^2}{16d^2} \in \mathbb{Z}$$

$$\Rightarrow \frac{a^2 - db^2}{16d^2} = \frac{4d^2 A^2 - db^2}{16d^2}$$

$\frac{d}{dt} = \frac{\partial}{\partial t} + \vec{v} \cdot \nabla$ (המשפט) $\frac{d}{dt} = \frac{\partial}{\partial t} + \vec{v} \cdot \nabla$

- def 61)

1. $\alpha \in \mathbb{R}$ is a root of $x^2 - 1 = 0$ in $\mathbb{R}[x]$ if and only if $\alpha = \pm 1$.

$\beta=1, \alpha=0$ " — " " — "

$f \sim 1$

$$G_2 = \mathbb{Z} \left[\frac{1+\sqrt{5}}{2} \right] \quad \text{vkl.} \quad \text{rkl.} \quad \frac{1+\sqrt{5}}{2} \quad (2)$$

$$x^2 - x + \frac{1-d}{4} \in \mathbb{Z}[x]$$

$$\delta \equiv 1 \quad (\text{mod } 4)$$

$$\otimes_{\mathbb{Q}(\sqrt{5})} = \begin{cases} \mathbb{Z}[\alpha], & j \equiv 2,3 \pmod{4} \\ \mathbb{Z}[\frac{1+\alpha}{2}], & j \equiv 1 \pmod{4} \end{cases} \quad \text{p.d.o}$$

אין אונזערע קינדער וועלכע זענען געווען אין דער שולע!

$\Gamma_{M:\phi} = \frac{V_{BC}}{\sqrt{3} V_{IN}}$

$\varphi \in K \subseteq M \cap L$ $\Rightarrow$ $M, L \subseteq \mathbb{C}$ $\Rightarrow$ φ is $\mathbb{C}$ -linear
 $\Rightarrow$ φ is $\mathbb{C}$ -linear $\Rightarrow$ φ is $\mathbb{C}$ -linear $\Rightarrow$ φ is $\mathbb{C}$ -linear
 $\Rightarrow$ φ is $\mathbb{C}$ -linear $\Rightarrow$ φ is $\mathbb{C}$ -linear $\Rightarrow$ φ is $\mathbb{C}$ -linear

② $\frac{1}{2}$ מל מל הממלכה ה'א' נאמל, מל מל מל

(3) $W = M \cdot L \leftarrow$ $W = M \cdot L$ (היחסות)

$$3 = [L: \mathbb{Q}] \quad , \quad 2 = [K: L]$$

(10) (11)

מחברת: ח.ל.מ. מלמד: מ.ל.מ. -

2.4. 18 82700 2.4. 18 82700 -342 82700

-XCH₃ alk-122 | 122

$$T_{r_{M/L}}(x) = T_{r_{L/K}}(x)$$

$$\Delta(q/q) \mathcal{O}_N \subseteq \mathcal{O}_L \mathcal{O}_M \subseteq \mathcal{O}_N \quad \text{ist.} \quad \text{--- WJF}$$
$$Y = \{y_1, \dots, y_n\} \quad (1 \times 1) \quad O_K \quad \text{from } 0.07 \text{ to } 0.1 \quad - \text{PID} \quad \text{and } O_K$$

$Tr_{L_k} - \delta \quad ON' > \quad Y - \delta \quad \& R3$

$$\delta_{ij} = \text{Tr}_{\mathcal{H}_k} (y_i y_j^*) = \text{Tr}_{\mathcal{H}_k} (y_j y_i^*)$$

-150 ml

$$D = (Tr(y_i y_j')_{i,j})$$

$$D^{-1} = (W_{Y_k}(y_i; y_j))_{i,j}$$

 σ_c

$$\Delta(\mathcal{O}_L/\mathcal{O}_K) = \Delta(y_1, \dots, y_n) \mathcal{O}_K$$

רצ"מ

$$\text{פרט } D^{-1} \in \frac{1}{\Delta(y)} M_{n \times n}(\mathcal{O}_K) \Leftarrow$$

$$x \in \mathcal{O}_{N \times 2} \quad y_i' \in \frac{1}{\Delta} \mathcal{O}_K \quad \text{ש"י} \quad y_i' = \sum \text{Tr}(y_k' y_i') y_k' \text{ש"י}$$

$$\text{Tr}_{L/K}(y_i x) = \alpha_i \in \mathcal{M}, \quad x = \sum \alpha_i y_i' \quad - \text{רצ"מ}$$

$$\text{רצ"מ} \quad x \in \frac{1}{\Delta} \mathcal{O}_K \text{ש"י}$$

$$\left((\text{Tr}_{L/K}(y_i y_j))_{i,j} \right) \left(\text{Tr}(y_i' y_j') \right)_{i,j} = \quad - \text{כ}$$

$$= \sum_k \text{Tr}(y_i y_k) \text{Tr}(y_k' y_j') =$$

$$\square \quad = \text{Tr} \left(\sum_k \text{Tr}(y_i y_k) y_k' y_j' \right) = \text{Tr}(y_i y_j')$$

~~ש"י~~

$$\text{ש"י } \Delta(\mathcal{O}_L/\mathcal{O}_K) \text{ש"י} \quad \text{רצ"מ} \quad \mathcal{O}_L \mathcal{O}_M = \mathcal{O}_{LM} \quad - \text{ש"י} \quad \Delta(\mathcal{O}_M/\mathcal{O}_K) \text{ש"י}$$

$$\mathcal{O}_{LM} \subseteq \Delta(\mathcal{O}_L/\mathcal{O}_K) \mathcal{O}_{LM} + \Delta(\mathcal{O}_M/\mathcal{O}_K) \mathcal{O}_{LM} = \mathcal{O}_L \mathcal{O}_M$$

$$\mathcal{O}_{LM} = \Delta(\mathcal{O}_L/\mathcal{O}_K) \mathcal{O}_{LM} + \Delta(\mathcal{O}_M/\mathcal{O}_K) \mathcal{O}_{LM} = \mathcal{O}_L \mathcal{O}_M \subseteq \mathcal{O}_{LM}$$

$$\square \quad \text{ש"י} \quad \text{רצ"מ}$$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{3}, \sqrt{5})} = \mathbb{Z}[\sqrt{3}, \frac{1+\sqrt{5}}{2}]$$

רצ"מ

$$\frac{3+\sqrt{5}}{5} \text{ש"י}$$

תורת גלואה

הי' $\xi_m \in \mathbb{C}$ שבו $\xi_m^m = 1$ ו- $\gcd(m, m) = 1$ (כלומר m אינו מתחלק ב- m).
 השדה $\mathbb{Q}(\xi_m)$ נקרא השדה הציקלוטומית ה- m -ית.
 נניח $m = 2^k \cdot n$ כאשר n אינו מתחלק ב-2.

זהו שדה ציקלוטומי.
 כל ξ_m הוא שורש של $x^m - 1$.
 כל ξ_m הוא שורש של $x^{m-1} + \dots + x + 1$.

$$\psi(m) = (\mathbb{Z}/m\mathbb{Z})^\times = \text{מספר האיברים הפרימיטיביים}$$

הפולינום (סימטרלי ציקלוטומי)

$$\begin{aligned} \Phi_1(x) &= x - 1 \\ \Phi_m(x) &= \frac{x^m - 1}{\prod_{d|m, d < m} \Phi_d(x)} \end{aligned}$$

תכונות חשובות

$$\Phi_m(x) = \prod_{i \in \mathbb{Z}/m\mathbb{Z}^\times} (x - \xi_m^i) \quad (1)$$

$$\Phi_p(x) = x^{p-1} + \dots + x + 1 \quad (2)$$

$$\begin{aligned} \Phi_{p^a}(x) &= \Phi_p(x^{p^{a-1}}) \quad (3) \\ &= x^{p^{a-1}(p-1)} + \dots + x^{p^{a-1}} + 1 \end{aligned}$$

$$\mathbb{Z}[x] \quad \Phi_m(x) \in \mathbb{Z}[x] \quad (4)$$

למשל $m = p^a$ תורת גלואה

גלואה: $\mathbb{Q} = \mathbb{Q}_L$, $L = \mathbb{Q}(\xi)$, $\xi = \xi_q$, $q = p^a$

$$[L:\mathbb{Q}] = \varphi(q) = \varphi(p^a) \quad (1)$$

$$\Phi_q(x) \text{ הוא הפולינום המינימלי של } \xi \text{ מעל } \mathbb{Q} \quad (2)$$

$$p \nmid q \Rightarrow L \text{ איננה פרימיטיבית} \quad (3)$$

$$\begin{aligned} p \nmid q \Rightarrow \alpha = 1 - \xi, \quad p \nmid q \Rightarrow \alpha = 1 - \xi \\ p \nmid q \Rightarrow \alpha = 1 - \xi \end{aligned} \quad (4)$$

$$p \nmid q \Rightarrow \alpha = 1 - \xi, \quad p \nmid q \Rightarrow \alpha = 1 - \xi \quad (5)$$

$$\begin{aligned} p \nmid q \Rightarrow \alpha = 1 - \xi, \quad p \nmid q \Rightarrow \alpha = 1 - \xi \\ p \nmid q \Rightarrow \alpha = 1 - \xi \end{aligned} \quad (6)$$