הרצאה 9

26/12/18

$N = *, **$ הפתרון -

$$\forall \alpha \in \mathcal{O}_K \exists \beta \in \mathbb{Z}[\omega] : \alpha - \beta \in \mathfrak{p} \iff \forall (x,y) \neq (0,0) \in \mathbb{Z}[\omega] : |N(x+\omega y)| > p \quad (*)$$

$\mathbb{Z}[\omega]/\mathfrak{p}$ סופי. נסמן $N = p^2$. אז $\mathbb{Z}[\omega]/\mathfrak{p}$ שדה עם p^2 איברים. לכן $\mathbb{Z}[\omega]/\mathfrak{p}^\times$ חבורה מסדר p^2-1. לפי משפט לגראנז' לכל $\alpha \in \mathbb{Z}[\omega]/\mathfrak{p}^\times$ מתקיים $\alpha^{p^2-1} = 1$, כלומר α שורש של $x^{p^2-1}-1$. לכן $\mathbb{Z}[\omega]/\mathfrak{p}$ מכיל לפחות p^2-1 שורשים של $x^{p^2-1}-1$. אבל $x^{p^2-1}-1$ יש לכל היותר p^2-1 שורשים, ולכן $\mathbb{Z}[\omega]/\mathfrak{p}^\times$ מכיל בדיוק p^2-1 שורשים של $x^{p^2-1}-1$. מכאן $\mathbb{Z}[\omega]/\mathfrak{p}^\times$ מכיל בדיוק p^2-1 איברים שונים מאפס, ולכן $\mathbb{Z}[\omega]/\mathfrak{p}$ מכיל בדיוק p^2 איברים.

$$\mathbb{Z}[\omega]/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$$

$\mathbb{Z}[\omega]/\mathfrak{p}$ מכיל בדיוק p איברים מהצורה $x + \mathfrak{p}$ עבור $x \in \mathbb{Z}$. נסמן $\mathbb{Z}/p\mathbb{Z} = \{0+\mathfrak{p}, 1+\mathfrak{p}, \dots, (p-1)+\mathfrak{p}\}$. נראה ש-$\mathbb{Z}/p\mathbb{Z}$ הוא שדה. יהי $x \in \mathbb{Z}$ כך ש-$x + \mathfrak{p} \neq 0 + \mathfrak{p}$. אז $x \notin \mathfrak{p}$, כלומר $p \nmid N(x) = x^2$. מכיוון ש-p ראשוני, $p \nmid x$. לכן $\gcd(x,p) = 1$, ולכן קיימים $a, b \in \mathbb{Z}$ כך ש-$ax + bp = 1$. אז $ax \equiv 1 \pmod{p}$, כלומר $a + \mathfrak{p}$ הוא ההופכי של $x + \mathfrak{p}$ ב-$\mathbb{Z}/p\mathbb{Z}$. לכן $\mathbb{Z}/p\mathbb{Z}$ הוא שדה.

$\mathbb{Z}[\omega]/\mathfrak{p}$ הוא מרחב וקטורי מעל $\mathbb{Z}/p\mathbb{Z}$ ממימד 2. יהי $\{1+\mathfrak{p}, \alpha+\mathfrak{p}\}$ בסיס. אז $\mathbb{Z}[\omega]/\mathfrak{p} = \{a + b\alpha + \mathfrak{p} : a, b \in \mathbb{Z}/p\mathbb{Z}\}$. מכאן $|\mathbb{Z}[\omega]/\mathfrak{p}| = p^2$

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

כאשר -

$$\Delta_1 = \Delta(u_1, \dots, u_{i_1})$$

$$\Delta_2 = \Delta(u_{i_1+1}, \dots, u_{i_2})$$

$$\vdots$$

$$\Leftarrow \quad \Omega \Delta(\bar{u}) = \prod_{i=1}^{k} \Omega \Delta_i(\bar{u})$$

↓

דטרמיננטה של מטריצה המקיימת את $\mathbb{F}_q/\Omega$ מעל

q/Ω - לא מעניין!

נניח בה"כ, לקבע -

$$\Delta(u_1, \dots, u_n) = d^2 = (\det(u_i^{j-1}))^2 \Delta$$

כאשר $\det(\text{מטריצת הוונדרמונד}) = d \neq 0$.

נשאיר את u_1 ונחליף את u_2 ב- $u_2 + cu_1$. כלומר

$\Delta(u_1, u_2 - u_1, \dots) = 0$. כי $i=j$ ולכן $u_2 - u_1 = 0$ בשדה

$u_2 \in \mathbb{F}_q$ לכן u_1 הוא אחד השורשים של הפולינום

כי $u_1 = u_j$ עבור $j \neq 1$ ולכן $\Delta = 0$ הפולינום $\Rightarrow (u_1 - u_j) \mid \Delta$.

$$\Delta(u) = \det \begin{pmatrix} \mathrm{Tr}(u_1 u_1) & \cdots & \mathrm{Tr}(u_1 u_n) \\ * & & \end{pmatrix} =$$

$$= \det \begin{pmatrix} 0 & \cdots & 0 \\ * & & \end{pmatrix} = 0$$

$$\Leftarrow \quad \Delta(u) = 0 \iff \Delta(\bar{x}) = 0$$

משמע כל $i=j$ עבור $\mathbb{F}_q/\Omega$ לא פחות, אז אי

$\Delta(\bar{x}) = 0$. לא (מפני כי הקבוע הזה של ההתלות

הפולינומי. עבור איזה שהוא מהן לא הפולינום - אי הוא

הוא u_1 -

$\mathbb{Z}[x]/(p)$ הוא שדה סופי עם p^n איברים, כאשר $n = \deg f$ ו-f אי-פריק מעל $\mathbb{Z}$.

$$\begin{array}{ccc} & \mathbb{Z}[x]/(p) & \\ \swarrow & & \searrow \\ \mathbb{Z}[x]/(p^2) & \longrightarrow & \mathbb{Z}/p^2\mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z}[x]/(p) & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \end{array}$$

על-פי המשולש הזה, כל $\mathbb{Z}[x]/(p^2)$ הוא הרחבה של $\mathbb{Z}/p^2\mathbb{Z}$ ושל $\mathbb{Z}[x]/(p)$. מכיוון שהמימד של $\mathbb{Z}[x]/(p)$ הוא 1 יותר מהמימד של $\mathbb{Z}/p\mathbb{Z}$, נובע שהמימד של $\mathbb{Z}[x]/(p^2)$ הוא 1 יותר מהמימד של $\mathbb{Z}/p^2\mathbb{Z}$.

$$\begin{array}{ccc} \mathbb{Z}[x]/(p^2) & \cong & \mathbb{Z}/p^2\mathbb{Z}[x]/(\bar{f}) \\ \downarrow & & \downarrow \\ \mathbb{Z}[x]/(p) & \cong & \mathbb{Z}/p\mathbb{Z}[x]/(\bar{f}) \end{array}$$

$$\left(\mathbb{Z}[x]/(p^2)\right)[\,] \overset{\text{CRT}}{\cong} \mathbb{Z}/p^2\mathbb{Z}[x]/(\bar{f}) \overset{\text{(משפט הרחבות)}}{\cong} \mathbb{Z}/p^2\mathbb{Z}$$

לכן,

$$\mathbb{Z}[x]/(p^2) = \mathbb{Z}/p^2\mathbb{Z}[x]/(\bar{f}) = \mathbb{Z}/p^2\mathbb{Z}$$

הוכחה: כיוון ש-$\mathbb{Z}/p^2\mathbb{Z}$ הוא חוג, אם נוכיח ש-$\mathbb{Z}/p\mathbb{Z}$ הוא שדה נקבל את הנדרש, שכן $\mathbb{Z}/p^2\mathbb{Z}$ הוא הרחבה של $\mathbb{Z}/p\mathbb{Z}$.

$$[\mathbb{Z}/p^2\mathbb{Z} : \mathbb{Z}/p\mathbb{Z}] = \deg f = d$$

$$f = f_1^{e_1} \cdots f_g^{e_g}$$

לכל $\bar{f}_i \in \mathbb{Z}/p\mathbb{Z}[x]$ אי פריק שונה. שקיים $h_i \in \mathbb{Z}[x]$ עבורו $\bar{h}_i = \bar{f}_i$.

נניח ש-$\bar{f} \in \mathbb{Z}/p\mathbb{Z}[x]$ הפולינום שלו דומה. ~~[illegible]~~

$\forall 0 \neq f \in \mathbb{Z}/p^2\mathbb{Z}[x]$ כך ש-$\deg f < d$, נראה שהמכפלה $f \cdot \mathbb{Z}/p^2\mathbb{Z}[x]$ היא מחלקת אפס.

משפט: (קיומי)

יהי p ראשוני ו-n טבעי, אזי קיים שדה $\mathbb{F}_{p^n}$ בעל p^n איברים.

$$\mathfrak{p}_i^{e_i}/(f(x)) \cong \mathfrak{P}_j^{e_j} \bmod p$$

לכן $e_i = e(\mathfrak{P}_j|p)$. $\square$

הערה: נניח $\mathcal{O} = \mathbb{Z}[\alpha]$. אז $\mathcal{O}$ מכיל את כל השורשים של f שהם שלמים ב-K.

משפט קרונקר – תהי $f \in \mathbb{Z}[x]$ מתוקנית פרידית

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

ואי-פריקה מעל $\mathbb{Q}$. יהי p ראשוני כך ש-$p \nmid \Delta(f)$. אז $f/(\mathbb{Z}/p\mathbb{Z})$ פריק מעל $\mathbb{Z}/p\mathbb{Z}$ אם ורק אם $\mathcal{O}_K/p\mathcal{O}_K$ אינו שדה.

משפט: תהי $\mathcal{O}$ סדר כך ש-$\mathcal{O}_K/\mathcal{O} = \mathbb{Z}/n\mathbb{Z}$. אזי $(n,\Delta) = 1$

משמ"ש –

(1) $\mathcal{O}_K \subseteq \frac{1}{n}\mathcal{O} \subseteq \mathbb{Z}_K$

(2) יש $\alpha \in \mathcal{O}$ כך ש-$\mathbb{Z}[\alpha] = \mathcal{O}$, $\Delta(\alpha) = \Delta(\mathcal{O})$, $\Delta(\alpha) \neq 0$

$$\mathcal{O}_K = \mathbb{Z}[\alpha] + \frac{1}{n}\mathcal{O}$$

הוכחה: ① ברור $\mathcal{O} \subseteq \mathcal{O}_K$. נראה $\mathcal{O}_K \subseteq \frac{1}{n}\mathcal{O}$. יהי $\beta \in \mathcal{O}_K$. אזי $\beta = \sum_{i=1}^{n} a_i \omega_i$, $a_i \in \mathbb{Z}$ עבורם $\mathcal{O} = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. נסמן $A = (a_{ij})$ – מטריצת המעבר

$$\begin{pmatrix} \beta \\ \beta' \\ \vdots \\ \beta^{(n-1)} \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}$$

לכן $\det A = \pm\sqrt{\Delta(\mathcal{O})} \neq 0$. נסמן $B = A^{-1} \in GL_n(\mathbb{Q})$. אזי (b_{ij})

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = B \begin{pmatrix} \beta \\ \beta' \\ \vdots \\ \beta^{(n-1)} \end{pmatrix}$$

נשים לב כי $\mathbb{Z}[\beta] \subseteq \mathcal{O}_K$ ולכן $\mathbb{Z}[\beta]$ הוא $\mathbb{Z}$-מודול נוצר. נסמן $\mathbb{Z}[\beta] = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_n$. נסמן $\gamma_i = \sum_{j=1}^{n} c_{ij}\omega_j$, $c_{ij} \in \mathbb{Z}$. נסמן $C = (c_{ij})$ – מטריצת המעבר

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = C \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}$$

נשים לב כי $\det C \neq 0$ כי $\mathbb{Z}[\beta]$ הוא תת-חבורה של $\mathcal{O}_K$ מאינדקס סופי. לכן $\det C \in \mathbb{Z}\setminus\{0\}$. נסמן $\det C = m$. אזי $m\mathcal{O}_K \subseteq \mathbb{Z}[\beta]$. נסמן $\mathcal{O}_K \subseteq \frac{1}{m}\mathbb{Z}[\beta]$. נסמן $\mathbb{Z}[\beta] \subseteq \mathcal{O}_K \subseteq \frac{1}{m}\mathbb{Z}[\beta]$. נסמן $\mathbb{Z}[\beta] = \mathcal{O}$. נסמן $\mathcal{O}_K = \frac{1}{m}\mathcal{O}$. נסמן $\mathcal{O}_K/\mathcal{O} = \mathbb{Z}/m\mathbb{Z}$. נסמן $n = m$. נסמן $(n,\Delta) = 1$.

② נסמן $\mathcal{O}_K = \mathbb{Z}[\alpha] + \frac{1}{n}\mathcal{O}$. נסמן $\Delta(\alpha) = \Delta(\mathcal{O})$. נסמן $\Delta(\alpha) \neq 0$. נסמן $\mathbb{Z}[\alpha] = \mathcal{O}$. נסמן $\mathcal{O}_K = \mathbb{Z}[\alpha] + \frac{1}{n}\mathcal{O}$.

$$\mathcal{O}_K = \mathbb{Z}[\alpha] + \frac{1}{n}\mathcal{O}$$

$$\mathcal{O}_K = \mathbb{Z}[\alpha] + \frac{1}{n}\mathcal{O}$$

$$X_k = \sum_{i=1}^{n} b_{ik}\theta^{i-1}$$

ולכן אם נרצה למצוא k כך ש

$$y = \sum_{i=1}^{n} r_k X_k = \sum_{i=1}^{n} r_k b_{ik} \theta^{i-1}$$

ולכן,

$$\underbrace{\sum_{i=1}^{n} r_k b_{ik}}_{\vec{Q}_k \cdot \vec{b}_i} \theta^{i-1} = p$$

$$\Leftarrow \quad L[\theta]\vec{Q}_k \ni p$$

כלומר, $\exists \vec{r}_k$ כך ש $L[\theta]\vec{r}_k = p$, אזי f מקיימת

$$L[\theta]\vec{Q}_k \ni p \cdot (\theta)\vec{v} = f(x)\vec{v}^{\,2} p = f \cdot (\theta)\vec{v}$$

$$L[\theta]\vec{Q}_k \ni p \cdot (x)\vec{v} p = f(x)\vec{v}^{\,2} p = f \cdot (\theta)\vec{v}$$

$$L[\theta]\vec{Q}_k \quad (\theta]\vec{Q}_k$$

ומכאן ש $r = 1$.

(2) נניח $n-1$ כשמתקיים d. $\square$

לשלב n:

משפט: יהי f פולינום ממעלה n, שמקיים $f(x) = 0$ ו $f'(x) \neq 0$ לכל x ב $\mathbb{R}$. אזי,

$$(f'(\theta))^{n+1} \operatorname{Norm} \prod_{i=1}^{n} (-1)^{\frac{i(i-1)}{2}} = (\theta)\vec{v}$$

הוכחה: נסמן $\theta_0, \dots, \theta_n = \Theta$ כך ש Θ הוא שורש של f. אזי,

$$f(x) = \prod_{i=1}^{n} (\theta_i - x)$$

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

$$\Rightarrow \quad (f'(\theta_j))^{n+1} = \prod_{j=1}^{n} \prod_{i \neq j} (\theta_j - \theta_i)^2$$

כלומר,

$$f'(\theta_j) = \prod_{i \neq j} (\theta_j - \theta_i) (-1)^{\binom{n}{2}}$$

$N \geq 33$ שלם,

$$\Delta(\Theta) = \det VV^T = (\det T)^2 = \prod_{i<j}(\theta_i - \theta_j)^2$$

$V = V(\theta_1, \ldots, \theta_n)$
מטריצת ונדרמונד

תזכורת: ① יהי Θ שורש של $f = x^n - b$ (ללא f פרידה)

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

$N(\Theta) = (-1)^{\frac{n(n-1)}{2}} b^{n-1}$

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

② $\Theta = \sqrt[3]{2}$, $f = x^3 - 2$, $\mathbb{Q}(\Theta) = K$. מתקיים $[K:\mathbb{Q}] = 3$

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

יהי d ראשוני, p לא מחלק את d, יהי $\mathbb{Z}_p[\Theta] = \mathbb{Z}[\Theta]/p\mathbb{Z}[\Theta]$

יהי $\mathbb{Q}$ הרחבה של $\mathbb{Q}$ ממעלה n ויהי Θ איבר פרימיטיבי של K עם $f = x^3 - 2$ מינימלי של Θ.

פירוק של p ב-$\mathcal{O}_K$	פירוק של f מעל $\mathbb{Z}_p$	p
$p\mathcal{O}_K = \mathfrak{P}$	$x^3 - 2$	7
$p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$, $f_1 = 1$, $f_2 = 2$	$(x+3)(x^2+4x+1)$	23
$p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$	$(x+1)(x-4)(x-5)$	31

p ראשוני $\Leftarrow$ כל הגורמים הראשוניים של $\Delta(\Theta)$

$d = -23$ ראשוני $\mathbb{Z}[\Theta]$ ($\Theta \in \mathcal{O}_K$) יהי

$$\mathbb{Z}[\Theta] \subseteq \mathcal{O}_K \subseteq \frac{1}{2}\mathbb{Z}[\Theta]$$

נרצה ל-

$$2\mathcal{O}_K = \mathcal{O}_K\Theta^3 = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

$$2\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

עבור $\sum e_i f_i = 3$. כל אלו $g = 1$, $e_i = f_i = 1$.

$\sum e_i f_i = n$

מתקיים $2 = \text{Norm}$ ראשוני.

מציאו $p=3$ ראשוני שעבורו x^3-2 פולינום אי-פריק מעל $\mathbb{Z}$ ($\mathbb{Z}[\alpha]=\mathbb{Z}[\alpha]$ שלם). נשים $\alpha=\alpha$ ונקבל שעבור

$$x^3-2=(x-1)^3-3x^2+3x-3$$

נראה שזה פולינום אי-פריק מעל $\mathbb{Z}$. [הערה: אי-פריקות אינה תלויה בבסיס הנתון]

$$\Leftarrow \quad 3\mu=\alpha^3 \qquad (\mu=\alpha^2-\alpha+1)$$

לכן,

$$3^3 \mathrm{Norm}(\mu)=\mathrm{Norm}(\alpha^3)=3^3$$

$$\Rightarrow \quad \mathrm{Norm}(\mu)=1$$

אבל,

$$1=\mathrm{Norm}\,\mu=\mu\cdot\overline{\mu}$$

(כאשר $\overline{\mu}$ מצמוד). לכן, μ הפיך. לכן,

$$\mathcal{O}_\alpha=\mathcal{O}_{3\alpha}$$

$\Leftarrow$ $\mathcal{O}_\alpha$ מושלם (כמו קודם) לכן 3 מוצף ראשוני.

נוכיח את הטענה הבאה שנראה שעבורה $\mathcal{O}_\alpha$ אי-פריק שקול. $\mathcal{O}_\alpha=\mathcal{O}_{3\alpha}$ אי-פריק אף. (בהמשך-

$\mathrm{Norm}_{L/k}(\mathcal{O}_L)=\langle \mathrm{Norm}_{L/k}(a) \mid a\in\mathcal{O}_L\rangle$ (כאשר $\mathcal{O}_L$ שלם)

הוכחה – **טענות עזר.**

① אם $\mathcal{O}_L=a\mathcal{O}_L$, אז, $\mathrm{Norm}_{L/k}(\mathcal{O}_L)=\mathcal{O}_k\mathrm{Norm}_{L/k}(a)$.

② אם $\mathcal{O}_k\ni c$ כלשהו, אז

$$\mathrm{Norm}(a\mathcal{O}_L)=\mathrm{Norm}(a)\cdot\mathcal{O}_k$$

③ $\mathrm{Norm}_{L/k}(\mathcal{O}_L)\cdot\mathrm{Norm}_{L/k}(H)=\mathrm{Norm}_{L/k}(H\mathcal{O}_L)$

הערה: ③ לעיתים משתמשים ב-p. זה $\mathcal{O}_K$ הוא יחיד, $\mathcal{O}$ הוא בדקונג ולא מס' טבעי אך משתמשים לפעמים + 2,1.

$\Leftarrow$ $\mathcal{O}$ הוא PID. ואין הטענה נובעת — אינה נכונה

ב מצב 3 נניח לרגע את הטענה ונוכיח לאחר מכן

שכיוון $I = \frac{p_1^{a_1} \cdots p_r^{a_r}}{q_1^{b_1} \cdots q_s^{b_s}} \Rightarrow N(I) = \frac{N(p_1)^{a_1} \cdots N(p_r)^{a_r}}{N(q_1)^{b_1} \cdots N(q_s)^{b_s}}$

טענה: יהי β השייך ל $\mathcal{O}$, $N(p)$ ו α_K, אז $\alpha = \prod \beta_i^{a_i}$, $f = f(\beta/p)$ אז, $p^f = \text{Norm}(\beta)$. ואז, $\text{Norm}(\alpha) = \prod p_i^{a_i f_i}$

הוכחה: נשים ב- $K/\mathbb{Q}$ שהוא $G = \text{Gal}(K/\mathbb{Q})$.

$\forall \sigma \in G$. $\text{Norm}(\beta) = \text{Norm}(\sigma\beta)$ — ברור.

$p\mathcal{O}_K$ ל- p מתאים,

$$\text{Norm}_{K/\mathbb{Q}}(p\mathcal{O}_K) = \left(\prod_{i=1}^{g} (\text{Norm}(P_i))^e\right) = p^n \quad \deg I = n$$

$$\deg(p^n) = n \Rightarrow p\mathcal{O}_K = \prod P_i^e$$

$\Rightarrow \exists f_i = e_i f_i = n \Leftrightarrow f_i = r$. ולכן מה שרצינו.

שאלה: מי $K/\mathbb{Q}$ כאשר יחיד סתור שלהם.

$$p^{f(Q/p)} = \text{Norm}_{K/\mathbb{Q}}(Q) = \cdots =$$

$$= (Q)\,\text{Norm}_{L/\mathbb{Q}}\,\text{Norm}_{K/L} =$$

$$= (\beta\mathcal{O}_K)^{f(\beta\mathcal{O}_K/p)}\,\text{Norm}_{K/\mathbb{Q}} =$$

$$\Leftarrow (\beta\mathcal{O}_K)^{f(\beta\mathcal{O}_K/p)} = (\text{Norm}(\beta))$$

מתקיים — כיוון שקיים β, שמ $f(\beta/p) = r$.

Q	e	f
β_1	1	2
β_2	1	1
p	1	3

שאלה

ניתן להגדיר את Norm גם לאיברים המתלכדים -

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

(ללא הוכחה)

$$\mathrm{Norm}: Cl(\mathcal{O}_L) \longrightarrow Cl(\mathcal{O}_K)$$

כי הנורמה של מחלקה = מחלקה.

הרצאה 10

21/12/18

קבוצת מספרים

מעתה כלל $\mathcal{O}_K = \mathbb{Z}$, $\mathcal{O}_L$. L שדה מספרים $\frac{\mathbb{Q}}{K}$

הכוונה: סופי. (ניתן לשים L ב- $\mathbb{C}$)

כלומר:

$$\mathcal{O}_L \text{ חבורה חופשית מעל } \mathbb{Z} \text{ בדיוק } n \text{ יוצרים} = \mathcal{O}_L \text{ חוג השלמים של } K$$

$$\downarrow$$

$$\mathcal{O}_L \text{ מודול חופשי מעל } \mathbb{Z}$$

נוהגים את אינדקס K של $\mathcal{O}_K$ באינדקס $\mathbb{Q}$ - אל $N_{L/K}(\mathfrak{A})$ אינדקס של $\mathbb{Z}$. זה הוא מה שנקרא $\mathbb{Z}$ אך עתה כאשר.

לשם כך $N(\mathfrak{A}) = |\mathcal{O}_L/\mathfrak{A}|$ - הגדרה המוכללת של $\mathfrak{A}$. כלומר,

$\mathbb{Z}$: $N(\mathfrak{A}) = (\mathfrak{A})^{\mathbb{Q}/\mathbb{Z}}\mathrm{Norm}$, וכן, $0 < |\mathfrak{A}| N$.

ו פעמים, $\rho - (\mathfrak{A})N$ קרוי עתה בשם הפונקציה (Counting Norm)

שכן $|\mathcal{O}_L/\mathfrak{A}| = (\mathfrak{A})N$. (ניתן: כל $\mathbb{Z}$-מ"ו V הינו $\mathbb{Z}^n$ - איזו $\mathbb{Z}$, $\mathfrak{A}$ מושוה $\mathcal{O}_L$. אז, $\mathcal{O}_L/\mathfrak{A}$ מיפוי $\mathbb{Z}$-מודולים $\mathcal{O}_L/\mathbb{Z}$ ו $\mathfrak{A}/\mathbb{Z}$ יוצג (מהעדה) $(\mathfrak{A}/\mathcal{O}_L)\#$.

(נזון $\mathbb{Z}[\mathcal{O}_L : \mathbb{Z}^n]$)

כלים של שני לעיל

כיוון ש- $\mathfrak{A} = p^k\mathcal{O}_L$, נקבל ש-

$$(p^k)N = p^{nk} = \#(\mathcal{O}_L/\mathbb{Z}^n) = \#(\mathcal{O}_L/\mathfrak{A})N$$

משפט: (פרמה)

מספר טבעי p הינו מהצורה x^2+y^2, $x,y \in \mathbb{Z}$ אם"ם $p \equiv 1 \pmod 4$ או $p=2$.