הרצאה 5

משפט (פרמה, 1640) יהי p ראשוני. אזי $p=a^2+b^2$ אם ורק אם $p\not\equiv 3 \mod 4$.

יהי $K=\mathbb{Q}(\sqrt{-1})$.

הוכחה: $p=a^2+b^2 \iff p=N_{K/\mathbb{Q}}(a+b\sqrt{-1}) \iff$ קיים איבר של $\mathcal{O}_K=\mathbb{Z}[\sqrt{-1}]$ בעל נורמה p

$\iff$ קיים אידיאל $I \triangleleft \mathcal{O}_K$ עם $N(I)=p$

כי $\mathcal{O}_K$ תחום ראשי. אזי, הוכחנו $Cl_K=\{e\}$

(שם הוכחנו בחוגים כי $\mathcal{O}_K$ תחום אוקלידי). $\iff$

$p\mathcal{O}_K$ לא ראשוני, לכן, $p^2=|N_{K/\mathbb{Q}}(p)| = N(p\mathcal{O}_K)$. אם

הוא לא ראשוני, הוא מתפצל, הנורמות של הגורמים $p\mathcal{O}_K=P_1^{e_1}\cdots P_r^{e_r}$

חייבים להיות p כי הנורמה כפלית.

לפי המשפט מן השיעור הקודם, כדי לחקור את הפירוק של $p\mathcal{O}_K$: ניקח $\theta=\sqrt{-1}$, אזי $\mathcal{O}_K=\mathbb{Z}[\theta]$,

לכן $\mathfrak{f}_\theta = B = \mathcal{O}_K$

הפולי' המינימלי של θ הינו x^2+1. לכל p ראשוני

$p \nmid \mathfrak{f}_\theta$, ולכן נחקור את הפירוק של $x^2+1\in\mathbb{F}_p[x]$.

1) $p=2$: $(x^2+1)\equiv(x+1)^2 \mod 2 \in \mathbb{F}_2[x]$ לכן $2\mathcal{O}_K=P^2$, $P=(1+\theta,2)=(1+\sqrt{-1},2)=(1+\sqrt{-1})$, $2=(1+\sqrt{-1})(1-\sqrt{-1})$

לכן, 2 מסתעף ב- $K/\mathbb{Q}$.

2) $p\equiv 1 \bmod 4$. אזי לפולינום x^2+1 יש שורש מודולו p.

כי $\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, אך $4\mid(p-1)$ לכן יש איבר $a\in\mathbb{F}_p^*$ מסדר 4, אזי $o(a^2)=2 \Rightarrow a^2=-1$. לכן, $-a$ גם שורש,

$$x^2+1=(x-a)(x+a)\in\mathbb{F}_p[x]$$

מכפלה של גורמים אי-פריקים שונים.

לכן

$$p\mathcal{O}_K = P_1 P_2$$

$$P_1=(p,\ a+\sqrt{-1}),\quad P_2=(p,\ a-\sqrt{-1})$$

האידיאלים ראשיים, אבל עלול להיות לא-טריוויאלי למצוא יוצר.

3) $p\equiv 3 \bmod 4$. אזי לפולינום x^2+1 אין שורש מודולו p, כי אין איברים מסדר 4 ב- $\mathbb{F}_p^*$.

לכן $p\mathcal{O}_K = P$ ראשוני.

סיכום 1) $p\mathcal{O}_K$ ראשוני $\iff p\equiv 3 \bmod 4$.

2) p מסתעף ב- $K/\mathbb{Q}$ $\iff p=2$. מתרגילי הבית: $d_K=-4$.

דוגמה נוספת: יהי $K=\mathbb{Q}(\sqrt{d})$ כאשר d חופשי מריבועים.
איך מתפצלים ראשוניים $p\mathcal{O}_K$?

1) $d\equiv 2,3 \bmod 4$. אזי $\mathcal{O}_K=\mathbb{Z}[\sqrt{d}]$, ניקח $\theta=\sqrt{d}$, אזי $\mathfrak{f}_\theta=\mathcal{O}_K$.

לכן, לכל p הפירוק של $p\mathcal{O}_K$ נקבע ע"י הפירוק של x^2-d מודולו p.

$\sum e_i f_i = 2$

הינה נניח: p מסתעף $\Leftrightarrow p\mid d_K \overset{=4d}{} \Leftrightarrow p\mathcal{O}_K=\mathfrak{p}^2$

$\mathcal{O}_K/\mathfrak{p}\simeq\mathbb{F}_p$.

אם $p\nmid 4d$, אזי $p\mathcal{O}_K=\mathfrak{p}_1\mathfrak{p}_2 \Leftrightarrow$ יש שורש של x^2-d מודולו p

$p\mathcal{O}_K=\mathfrak{p}$ ראשוני $\Leftrightarrow$ אין שורש.

הגדרה: יהי q ראשוני, יהי $(a,q)=1$. הסימן של לג'נדר (Legendre) הינו

$$\left(\frac{a}{q}\right)=\begin{cases}1, & \text{קיים פתרון לחפיפה } x^2\equiv a \bmod q\\ -1, & \text{לא קיים}\end{cases}$$

תכונה: $\left(\frac{ab}{q}\right)=\left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$. לכן מספיק לקבוע $\left(\frac{-1}{q}\right)$ ואת $\left(\frac{p}{q}\right)$ כאשר p ראשוני!

$$\left(\frac{-1}{q}\right) = \begin{cases} -1, & q \equiv 3 \mod 4 \\ 1, & q \equiv 1,2 \mod 4 \end{cases}$$

הדדיות ריבועית של גאוס (1797): יהיו $p,q \geq 3$ ראשוניים.

אזי $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

איך זה עוזר לנו: אנחנו רוצים לקבוע האם יש שורש של x^2-d מודולו p, כלומר לחשב $\left(\frac{d}{p}\right)$, לכל p.

הבעיה: יש אינסוף p-ים.

הפתרון: $\left(\frac{d}{p}\right)$ נקבע על ידי $\left(\frac{q}{p}\right)$ כאשר $q|d$ ראשוני,

אלה נקבעים על ידי הסימנים $\left(\frac{p}{q}\right)$, יש רק

מספר סופי של מחלקות

מודולו q.

<u>דוגמה</u> $K=\mathbb{Q}(\sqrt{3})$. איך $p\mathcal{O}_K$ מתפרק?

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

$d_K = 12$. לכן $p=2,3 \iff p\mathcal{O}_K = P^2$.

נניח $p \geq 5$. רוצים לחשב $\left(\frac{3}{p}\right)$.

הדדיות ריבועית: $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}}$

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right), & p \equiv 1 \mod 4 \quad (\text{זוגי } \tfrac{p-1}{2}) \\ -\left(\frac{p}{3}\right), & p \equiv 3 \mod 4 \quad (\text{אי-זוגי } \tfrac{p-1}{2}) \end{cases}$$

מהו $\left(\frac{p}{3}\right)$

$\left(\frac{1}{3}\right) = 1$

$\left(\frac{2}{3}\right) = -1$

x (mod 3)	x^2
1	1
2	1

טבלה

p mod 12	p mod 3	p mod 4	$\left(\frac{p}{3}\right)$	$\left(\frac{3}{p}\right)$
1	1	1	1	1
5	2	1	-1	-1
7	1	3	1	-1
11	2	3	-1	1

לסיכום

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & p \equiv 1, 11 \mod 12 \\ -1, & p \equiv 5, 7 \mod 12 \end{cases}$$

סך הכל

$$p\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \begin{cases} P^2, & p = 2, 3 \\ P_1 P_2, & p \equiv 1, 11 \mod 12 \\ P, & p \equiv 5, 7 \mod 12 \end{cases}$$

2) אם $d\equiv 1 \mod 4$, אזי אם ניקח $\theta=\frac{1+\sqrt{d}}{2}$, אזי

$\mathcal{O}_K=\mathbb{Z}[\theta]$, $\mathfrak{f}_\theta=\mathcal{O}_K$.

לכל p, הפירוק של $p\mathcal{O}_K$ נקבע על ידי הפירוק של הפולינום המינימלי של θ מודולו p:

$$2\theta = 1+\sqrt{d}$$

$$2\theta-1=\sqrt{d}$$

$$4\theta^2-4\theta+1=d$$

$$4\theta^2-4\theta+(1-d)=0$$

$$\theta^2-\theta+\frac{1-d}{4}=0$$

לכן הפול' המינימלי הינו $x^2-x+\frac{1-d}{4}$.

אם $p=2$, יש לבדוק את הפירוק מודולו 2.

$d_K=d$, לכן 2 לא מסתעף. הוא פוצל $\iff 2 \mid \frac{1-d}{4}$

$\iff d\equiv 1 \mod 8$

$\iff x^2-x+\frac{1-d}{4}\equiv x(x-1) \mod 2$

$\iff 2\mathcal{O}_K = P_1P_2$

אם $d \equiv 5 \mod 8$, אז $2\mathcal{O}_K = P$ ראשוני.

אם $2<p$, אז אפשר לעשות השלמה לריבוע.

אז, ניקח $\theta = \sqrt{d}$. אז $\mathbb{Z}[\theta] \subsetneq \mathcal{O}_K$. אבל,

$2 \nmid p \iff p$ זר ל- f_θ. $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

$2 \in f_\theta$

לכן ניתן לחקור את x^2-d מודולו p כמו במקרה הקודם.

נחזור למשפטים מן השבוע שעבר: A תחום דדקינד

$K = \mathrm{Frac}\ A$

L/K סופית, ספרבילית

B סגור השלם של A ב-L.

יהי $\beta_1, \dots, \beta_n$ בסיס של L מעל K, נניח $\beta_1, \dots, \beta_n \in B$. (קיימים כאלה כי כל איבר של L מן הצורה $\frac{b}{a}$, $\left(\begin{smallmatrix} b\in B \\ a\in A\end{smallmatrix}\right)$.

הדיסקרימיננטה $d(\beta_1, \dots, \beta_n) = \det\left(\mathrm{Tr}_{L/K}(\beta_i\beta_j)\right) \in A$

הגדרה הדיסקרימיננטה $d_{L/K}$ הינה האידיאל של A הנוצר על ידי האיברים $d(\beta_1,\dots,\beta_n)$ לכל K-בסיס $\{\beta_1,\dots,\beta_n\}\subseteq B$ של L.

הערה אם נבחר בסיס אחר $\{\beta_1',\dots,\beta_n'\}$, אזי

$$d(\beta_1',\dots,\beta_n') = d(\beta_1,\dots,\beta_n)\det(M)^2$$

כאשר M המטריצה המעבירה בין הבסיסים.

לכן התנאי $d(\beta_1,\dots,\beta_n)=0$ עבור בסיס אחד $\iff$ $d(\beta_1',\dots,\beta_n')=0$ לכל בסיס.

הערה ההגדרה הנ"ל של $d_{L/K}$ עובדת גם כאשר A לא תחום ראשי ואין בסיסים שלמים.

תרגיל יהי A תחום ראשי. אזי

$$d_{L/K} = (d(\beta_1,\dots,\beta_n))$$

לכל בסיס שלם $\beta_1,\dots,\beta_n$.

משפט תהי L/K הרחבה של שדות מספרים. יהי $\mathfrak{q}\trianglelefteq O_K=A$ אידיאל ראשוני. אזי $\mathfrak{q}$ מסתעף ב-L/K $\iff$ $\mathfrak{q}\mid d_{L/K}$.

<u>הגדרה</u> יהי F שדה, ונניח V F-אלגברה ממימד סופי.

(V מרחב וקטורי סוף-מימדי מעל F עם כפל שנותן לו מבנה של חוג).

לכל $v\in V$, נגדיר את העקבה $Tr_{V/F}(v)\in F$ להיות העקבה של המטריצה של העתקה ה-F-לינארית

$$V\longrightarrow V$$
$$w\longmapsto vw$$

לכל בסיס $\beta_1,\dots,\beta_n$ של V, נגדיר

$$d(\beta_1,\dots,\beta_n)=\det\left(Tr_{V/F}(\beta_i\beta_j)\right)\in F.$$

גם כאן, התנאי $d(\beta_1,\dots,\beta_n)=0$ לא תלוי בבחירה של הבסיס.

<u>תת-טענה</u> יהיו V_1,V_2 שתי F-אלגבראות עם בסיסים $(\alpha_1,\dots,\alpha_n)$, $(\beta_1,\dots,\beta_m)$ בהתאמה. אזי

$((\alpha_1,0),\dots,(\alpha_n,0),(0,\beta_1),\dots,(0,\beta_m))$ הינו בסיס של $V_1\times V_2$.

אזי $d_{V_1\times V_2/F}(\alpha_1,\dots,\beta_m)=d_{V_1/F}(\alpha_1,\dots,\alpha_n)\cdot d_{V_2/F}(\beta_1,\dots,\beta_m)$

$$d_{V_1\times V_2/F}(\alpha_1,\dots,\beta_m) = \det\begin{pmatrix} Tr_{V_1/F}(\alpha_i\alpha_j) & 0 \\ 0 & Tr_{V_2/F}(\beta_i\beta_j) \end{pmatrix}$$ <u>הבחנה</u>

<u>טענה 2</u> יהי $\mathfrak{p} \triangleleft O_K$ אידאל ראשוני. נסמן $A = O_K$, $B = O_L$. אזי

$$d_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = 0 \iff \mathfrak{p} \mid d_{L/K}$$

לא בהכרח שדה

$$B/\mathfrak{p}B \simeq B/\mathfrak{P}_1^{e_1} \times \dots \times B/\mathfrak{P}_r^{e_r}$$

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$$

<u>תת-הוכחה</u> יהי $\bar\beta_1,\dots,\bar\beta_n$ בסיס של $B/\mathfrak{p}B$ כמרחב וקטורי מעל $A/\mathfrak{p}$.

בשבוע שעבר (בתרגול הבית) הוכחנו

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = n = [L:K]$$

יהיו $\beta_1,\dots,\beta_n \in B$ הרמות של $\bar\beta_i$. אני טוען שזה בסיס של L מעל K (אכן, מספיק להוכיח כי $\beta_1,\dots,\beta_n$ בת"ל מעל K, כי $n = \dim_K L$. אם הם תלויים לינארית מעל K, אזי תלויים לינארית מעל A. ניקח רדוקציה מודולו $\mathfrak{p}$, נקבל תלות של $\bar\beta_i$ מודולו $A/\mathfrak{p}$.
בסתירה.

ברור כי

$$d_{B/\wp B \,/\, A/\wp}(\bar\beta_1,\dots,\bar\beta_n) = \det(\mathrm{Tr}(\bar\beta_i\bar\beta_j)) = \overline{\det(\mathrm{Tr}_{L/K}(\beta_i\beta_j))}$$

לכן, $d_{B/\wp B \,/\, A/\wp}=0 \iff$ לכל בסיס $\beta_1,\dots,\beta_n$

מקיים: $d_{L/K}(\beta_1,\dots,\beta_n)\in\wp \iff \mathfrak{d}_{L/K}\subseteq\wp \iff$

$\wp \mid d_{L/K}$.

עכשיו אנחנו מוכנים להוכיח את הטענה. הוכחה:

$$\wp \mid d_{L/K} \underset{\text{תת-טענה 2}}{\iff} d_{B/\wp B \,/\, A/\wp}=0$$

אבל, לפי תת-טענה 1,

$$d_{B/\wp B \,/\, A/\wp} = \prod_{i=1}^{r} d_{B/P_i^{e_i} \,/\, A/\wp}$$

לכן, מספיק להוכיח לכל אידיאל ראשוני $P \triangleleft B$, $P\mid\wp$,

כי $d_{B/P^e \,/\, A/\wp}=0$ אם ורק אם $e>1$.

כי אז $\mathfrak{p} \mid d_{L/K} \iff$ קיים i כך ש $e_i>1 \iff d_{B/P_i^{e_i} / A/\mathfrak{p}} = 0$ (קיים i)

$\Big(\iff \mathfrak{p}$ מסתעף ב- L/K.

<u>אם $e=1$</u>, אזי B/P שדה. אז $d_{B/P / A/\mathfrak{p}} \neq 0$

כי $B/P \,/\, A/\mathfrak{p}$ הרחבה סופית וספרבילית.

<u>אם $e>1$</u> יהי $x \in P \setminus P^e$ (קיים לפי יחידות הפירוק).

יהי $\bar{x}, \bar{\beta}_2, \ldots, \bar{\beta}_n$ בסיס של B/P^e מעל $A/\mathfrak{p}$.

לכל $\bar{\beta}_j$, $(\bar{x}\bar{\beta}_j)^e = 0$ כי $\bar{x}^e = 0$.

לכן, אם M מטריצה של מכפלה ב- $\bar{x}\bar{\beta}_j$ אזי $M^e = 0$. לכן הערכים העצמיים של M כולם 0,

לכן $\operatorname{Tr}(\bar{x}\bar{\beta}_j) = 0$, לכן

$$d_{B/P^e / A/\mathfrak{p}} = \det \begin{pmatrix} 0 & \cdots & 0 \\ & * & \end{pmatrix} = 0$$

עכשיו נסיים את ההוכחה של משפט היחידות של דיריכלה מלפני שבועיים.

המשפט יהי K שדה מספרים. יהי $n=[K:\mathbb{Q}]$

r המספר של שיכונים ממשיים $\sigma: K \hookrightarrow \mathbb{R}$

s המספר של זוגות של שיכונים לא ממשיים $\tau, \bar{\tau}: K \hookrightarrow \mathbb{C}$

אזי $\mathcal{O}_K^* \simeq \mu(K) \times \mathbb{Z}^{r+s-1}$

הוכחה אז $n=r+2s$. יהיו $\sigma_1,\ldots,\sigma_r : K \hookrightarrow \mathbb{R}$ $\tau_1,\ldots,\tau_s : K \hookrightarrow \mathbb{C}$ נציגים של כל זוג.

$$\theta : K \hookrightarrow V = \mathbb{R}^r \times \mathbb{C}^s$$

$$\alpha \longmapsto (\sigma_1(\alpha),\ldots,\sigma_r(\alpha),\tau_1(\alpha),\ldots,\tau_s(\alpha))$$

לכל $(x_1,\ldots,x_r,y_1,\ldots,y_s) \in V$

נגדיר $N(x_1,\ldots,y_s) = |x_1|\cdots|x_r|\cdot|y_1|^2\cdots|y_s|^2 \in \mathbb{R}$

$N: V \to \mathbb{R}$ רציפה.

$$G = \{(x_1,\ldots,y_s) \in V : N(x_1,\ldots,y_s) = 1\}$$

לכל $\alpha \in K$, $N(\theta(\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$

לכן, $U = \theta(\mathcal{O}_K^*) = G \cap \theta(\mathcal{O}_K)$.

$$V^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$$

$$L : V^* \longrightarrow \mathbb{R}^{r+s}$$

$$L(x_1, \dots, y_s) = (\log|x_1|, \dots, \log|x_r|, 2\log|y_1|, \dots, 2\log|y_s|)$$

$$L(G) = H = \{(z_1, \dots, z_{r+s}) \in \mathbb{R}^{r+s} \mid z_1 + \dots + z_{r+s} = 0\} \simeq \mathbb{R}^{r+s-1}.$$

נשאר להוכיח כי $L(U) \subseteq H$ הוא סריג שלם.

כי אז $L(U) \simeq \mathbb{Z}^{r+s-1}$

$$\mathcal{O}_K^* \simeq U \simeq (\ker L|_U) \times L(U) \simeq \mu(K) \times \mathbb{Z}^{r+s-1}.$$

לפי משפט מן השיעור השני, צריך למצוא קבוצה

חסומה $\tilde{B} \subseteq H$ כך ש- $H = \bigcup_{\gamma \in L(H)} (\gamma + \tilde{B})$.

מספיק למצוא קבוצה חסומה $B \subseteq G$ כך ש-

$$G = \bigcup_{u \in U} uB.$$

כי אז $H = L(G) = \bigcup_{u \in U} \underbrace{L(B)}_{\tilde{B}} + L(u)$

נזכור, $V = \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^r \times (\mathbb{R}^2)^s \simeq \mathbb{R}^n$

$$\Theta(\mathcal{O}_K) = \iota(\mathcal{O}_K)$$

$$\iota(\alpha) := (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}\,\tau_1(\alpha), \mathrm{Im}\,\tau_1(\alpha), \dots)$$

הוכחנו לפני שבועיים $\mathrm{vol}(\iota(\mathcal{O}_K)) = \sqrt{|d_K|}$.

תהי $X \subseteq \mathbb{R}^n$ קבוצה קומפקטית, סימטרית, קמורה עם $\mathrm{vol}(X) > 2^n \sqrt{|d_K|}$.

לכל $g \in G$, $\mathrm{vol}(g^{-1}X) = \mathrm{vol}(X)$

$N(g^{-1}X) = N(X)$.

לפי מינקובסקי, $\Theta(\mathcal{O}_K) \cap g^{-1}X \neq (0)$. לכן קיים $0 \neq a_g \in \mathcal{O}_K$,

$\Theta(a_g) \in g^{-1}X$.

אבל N רציפה, לכן $N(g^{-1}X) = N(X) \subseteq \mathbb{R}$ קומפקטית.
אז קיים M, לא תלוי ב-g, כך ש-$|N_{K/\mathbb{Q}}(a_g)| \le M$.

אבל ידוע שיש מספר סופי של אידיאלים I של $\mathcal{O}_K$,
בפרט של אידיאלים ראשיים, כך ש-$N(I) \le M$.

יהיו $\alpha_1,\dots,\alpha_m \in O_K$ כך ש-

$\alpha_1 O_K, \dots, \alpha_m O_K$

הם כל האידיאלים הראשיים עם נורמה $\le M$.

זה אומר $N(a_g O_K) \le M \Leftarrow$ קיים $1 \le i \le m$ כך ש-

$$(a_g) = (\alpha_i)$$

לכן $a_g = \varepsilon \alpha_i$ עבור $\varepsilon \in O_K^*$ מתאים.

$$g^{-1}X \ni \theta(a_g) = \underbrace{\theta(\varepsilon)}_{\in U}\theta(\alpha_i)$$

$$g^{-1}X \cap U\theta(\alpha_i) \neq \emptyset$$

$$X \cap g\theta(\alpha_i)U \neq \emptyset$$

$$\theta(\alpha_i^{-1})X \cap gU \neq \emptyset$$

לכל $g \in G$,

$$gU \cap \underbrace{\left(\bigcup_{i=1}^{m} \theta(\alpha_i^{-1})X\right)}_{B} \neq \emptyset$$

B מכילה נציג של כל מחלקה ב- G/U.

$$G = \bigcup_{u \in U} uB.$$