25/12/18

**הרצאה 18**

**משפט:** כמו בסימונים לעיל, יהיו -

$$e_i = e(\mathfrak{P}_i/\mathfrak{p}),\quad f_i = f(\mathfrak{P}_i/\mathfrak{p}),\quad n=[L:K]$$

(1) מתקיים -

$$\sum_{i=1}^{g} e_i f_i = \dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$$

(2) בפרט,

$$\sum e_i f_i \le n$$

(3) אם $M=\mathcal{O}_K \setminus \mathfrak{p}$, וכן $\mathcal{O}_{L,M}$ נוצר סופית כמודול מעל $\mathcal{O}_{K,\mathfrak{p}}$ אזי -

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

**הוכחה:** ממשפט השאריות הסיני, $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \bigoplus_{i=1}^{g} \mathcal{O}_L/\mathfrak{P}_i^{e_i}$. לכן, מספיק להראות כי -

$$\dim_{k(\mathfrak{p})}(\mathcal{O}_L/\mathfrak{P}_i^{e_i}) = e_i f_i$$

כמרחב מעל $k(\mathfrak{P}_i)$,

$$\mathcal{O}_L/\mathfrak{P}_i^{e_i} = \bigoplus_{a=0}^{e_i-1} \mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$$

אכן, הגרעין של ההעתקה:

$$\mathfrak{P}_i^a/\mathfrak{P}_i^{a+2} \longrightarrow \mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$$

הוא -

$$\mathfrak{P}_i^{a+1}/\mathfrak{P}_i^{a+2}$$

לכן, $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+2} \cong \mathfrak{P}_i^{a+1}/\mathfrak{P}_i^{a+2} \oplus \mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$

ונוכל להמשיך באינדוקציה.

אם נראה כי, זה נכונה - $1=\dim_{k(\mathfrak{P}_i)}(\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1})$ אזי נקבל $\dim_{k(\mathfrak{p})}(\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1})=f_i$. עם יס"מ. אכן, $\mathcal{O}_{L,\mathfrak{P}_i}$ הוא PID;

וכן, $\mathcal{O}_{L,\mathfrak{P}_i}/\mathfrak{P}_i^b\mathcal{O}_{L,\mathfrak{P}_i} \cong \mathcal{O}_L/\mathfrak{P}_i^b$ לכל $b$; לכן, $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ - מ"ש.

ולכן היוצר שלו יוצר את $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ כמרחב וקטורי מעל $k(\mathfrak{P}_i)$. הסעיף השני נובע, שכן הראינו כבר כי $\dim_{k(\mathfrak{p})}\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \le n$.

נניח כעת ש- $\mathcal{O}_{L,M}$ נוצר סופית מעל $\mathcal{O}_{K,M}$. אזי, משום ש- $\mathcal{O}_{K,M}$ הוא PID, ~~[illegible]~~

ול-$\mathcal{O}_{L,M}$ אין פיתול, ועל כן $\mathcal{O}_{L,M}$ חופשי מעל $\mathcal{O}_{K,M}$. בסיס של $\mathcal{O}_{L,M}$ מעל $\mathcal{O}_{K,M}$ הוא גם בסיס של $L$ מעל $K$; לכן ניתן לכתוב -

$$\mathcal{O}_{L,M} = \bigoplus_{i=1}^{n} \mathcal{O}_{K,M} x_i$$

$$p\mathcal{O}_{L,M} = \bigoplus_{i=1}^{n} p\,\mathcal{O}_{K,M} x_i$$

ולכן,

$$\mathcal{O}_L/p\mathcal{O}_L \cong \mathcal{O}_{L,M}/p\mathcal{O}_{L,M} \cong \bigoplus_{i=1}^{n} (\mathcal{O}_{K,M}/p\mathcal{O}_{K,M})x_i \cong$$

$$\cong \bigoplus_{i=1}^{n} (\mathcal{O}_{K,M}/p)\, x_i$$

לכן, $\dim_{\mathcal{O}_{K,M}/p}(\mathcal{O}_L/p\mathcal{O}_L) = n$ - וסיימנו. □

<u>מסקנה:</u> אם ההרחבה $L/K$ ספרבילית, אזי $n = \sum e_i f_i$ !

<u>הוכחה:</u> אכן, כש-$L/K$ ספרבילית ראינו ש-$\mathcal{O}_L$ נ"ס כ-$\mathcal{O}_K$ מודול; לכן גם הלוקליזציה, ונפ"י. □

<u>דוגמה:</u> יהי $L = \mathbb{Q}(\sqrt{d})$, $d \neq 1$ חסר ריבועים. אז יש רק 3 אפשרויות -

① $p\mathcal{O}_L = \mathfrak{P}$ - במקרה כזה נאמר ש-$p$ <u>אינרטי</u>.

② $p\mathcal{O}_L = \mathfrak{P}\mathfrak{Q}$ כאשר $\mathfrak{P} \neq \mathfrak{Q}$. במקרה כזה נאמר ש-$p$ <u>מתפצל</u>.

③ $p\mathcal{O}_L = \mathfrak{P}^2$ - במקרה כזה נאמר ש-$p$ מסתעף.

<u>משפט:</u> תהא $L/K$ הרחבה גלואה, $\mathfrak{p} \neq 0$ ראשוני של $\mathcal{O}_K$. אזי,

$$p\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

הפירוק לראשוניים של $p$ ב-$\mathcal{O}_L$. יתר על כן,

$$f := f(\mathfrak{P}_1|p) = \ldots = f(\mathfrak{P}_g/p)$$

ובפרט, $efg = n$. יתר על כן, בסימון $D = D(\mathfrak{P}_1/p)$, $I = I(\mathfrak{P}/p)$,

בלי הנחת שדה השאריות פרפקטי:
$g = [G:D]$
$f = [D:I]$
$e = |I|$

<u>הערה:</u> מסקנה חשובה ש- מה שקובע אחרי הכל על $p$. ואכן, $G$ פועל טרנזיטיבית על ראשוני $\mathcal{O}_L$, המונחים מעל $p$.

הוכחה (המשך): היות ו-G ~~המרחב~~ המ"ג של β פועלה על
ולכן אם ניקח נציגים $s \in \Sigma$, אזי $s\beta$ לכל $s \in \Sigma$:
הם הראשוניים המונחים מעל $\mathfrak{p}$ וכולם שונים.
לכן $g = |\Sigma| = [G:D]$
ממשפט, $\mathcal{O}/\beta$ - הרחבה נורמלית עם חבורה $\cong D/I$.
בפרט, $f = [D:I]$. באשר לראשוניים האחרים, שווים:

$$f(s\beta/p) = [D_{s\beta} : I_{s\beta}] = [sDs^{-1} : sIs^{-1}] = [D:I] = f$$

כדי לסיים, נשתמש במה שכבר הוכחנו להרחבה $L/L^I$ עם הראשוניים $\beta$, $\beta^I = \beta \cap L^I$. מלמה קודמת, (עם הדיאגרמה)

$$Gal(L/L^I) = D_{\beta/\beta^I} = I_{\beta/\beta^I}$$

לומר $\beta$ הוא הראשוני היחיד מעל $\beta^I$, עם דרגה יחסית 1; לכן, $e(\beta/\beta^I) = [L:L^I] = |I|$. כך גם לראשוניים האחרים בגלל הפעולה של G. לבסוף בבירור ב-$L^I/L$ רק ה-$\beta^I$ מונח מעל $p$. □

**הגדרה:** נאמר ש-$p$ ~~מפוצל~~ מפוצל לחלוטין אם $g=n$, $e=f=1$
" — " אינרטי לחלוטין אם $f=n$, $e=g=1$ והרחבת שדה השאריות מקסימלית
" — " מסועף לחלוטין אם $e=n$, $f=g=1$

**מסקנה:** בסימונים הקודמים,
$L/L^I$ - מסועף לחלוטין
$L^I/L^D$ - אינרטי לחלוטין
$L^D/K$ - מפוצל
עם הראשוניים המתאימים.

כרגיל תהי $L/K$ הרחבה ספרבילית סופית, עם תחומי דדקינד מתאימים $\mathcal{O}_L, \mathcal{O}_K$.

**הגדרה:** נאמר שהראשוני $\beta$ של $\mathcal{O}_L$ מסועף מעל $K$, אם $e(\beta/\beta\cap\mathcal{O}_K) > 1$, או שההרחבה $L(\beta)/K(p)$ לא ספרבילית. אחרת $\beta$ אינו מסועף. נאמר שהראשוני $p$ של $\mathcal{O}_K$ מסועף ב-$\mathcal{O}_L$ אם יש ראשוני מסועף המונח מעליו. אחרת $p$ אינו מסועף.

כדי לקצר את הסימונים נכתוב $T(x)$ במקום $Tr_{L/K}(x)$.

**הגדרה:** יהיו $x_1,\dots,x_n$ ב-$L$, הדיסקרימיננטה של $(x_1,\dots,x_n)$ היא -

$$\Delta(x) = det\left(T(x_i x_j)\right)_{i,j} \in K$$

אם כל ה-$x_i \in \mathcal{O}_L$ אזי $\Delta(x) \in \mathcal{O}_K$.

**הגדרה:** אידאל הדיסקרימיננטה מוגדר להיות -

$$\Delta = \Delta(\mathcal{O}_L/\mathcal{O}_K) = \langle \Delta(x_1,\dots,x_n) \mid x_i \in \mathcal{O}_L,\ x_1,\dots,x_n \text{ בסיס ל-} L/K \rangle$$

**למה:** תהי $S \subseteq \mathcal{O}_K$ קבוצה כפלית. אזי,

$$\Delta(\mathcal{O}_{L,S}/\mathcal{O}_{K,S}) = \Delta(\mathcal{O}_L/\mathcal{O}_K)\mathcal{O}_{K,S}$$

**הוכחה** - ברורה ההכלה $\Delta(\mathcal{O}_L/\mathcal{O}_K) \subseteq \Delta(\mathcal{O}_{L,S}/\mathcal{O}_{K,S})$ לכן צריך רק את הכיוון השני. לשם, ניקח $y=(y_1,\dots,y_n)$ בסיס ל-$L/K$, כך ש-$y_i \in \mathcal{O}_{L,S}$. אזי, קיים $0 \neq s \in S$ כך ש-$sy_i \in \mathcal{O}_L$ עבור $i=1,\dots,n$. לכן,

$$\Delta(sy) = det(T(sy_i sy_j)) = s^{2n} det(T(y_i y_j)) = s^{2n}\Delta(y)$$

לכן,

$$\Delta(y) \in \Delta(\mathcal{O}_L/\mathcal{O}_K)\mathcal{O}_{K,S}$$ □

כאשר $\mathcal{O}_L$ הוא מודול חופשי מעל $\mathcal{O}_K$, אידאל הדיסקרימיננטה הינו ראשי -

**למה:** נניח $x=(x_1,\dots,x_n)$ בסיס של $\mathcal{O}_L$ מעל $\mathcal{O}_K$. אזי,

$$\Delta(\mathcal{O}_L/\mathcal{O}_K) = \Delta(x)\mathcal{O}_K$$

**הוכחה:** נכתוב - $y=(y_1,\dots,y_n)$ בסיס של $L/K$, עם $y_i \in \mathcal{O}_L$ ($i=1,\dots,n$). אזי, ניתן לכתוב -

$$y_i = \sum_j a_{ij} x_j \quad i=1,\dots,n$$

לכן, אם נסמן $A=(a_{ij})$, נקבל -

$$(T(y_i y_j))_{i,j} = A\,(T(x_i x_j))_{i,j}\,A^T$$

$$\Rightarrow \Delta(y) = det A^2 \Delta(x) \in \Delta(x)\mathcal{O}_K$$ □