5/12/18 הרצאה 7

חבורת מחלקה

הגדרה: יהי B חוג דדקינד, $K=Frac(B)$.

1) אידאל שברי הוא B-תת-מודול של K, שהוא נוצר סופית.

2) אם $0\neq m$ אידאל שברי, נגדיר $m^{-1}=\{x\in K \mid xm\subseteq B\}$. ברור ש-$m^{-1}$ תת B-מודול של K, אך לא ברור שהוא נ"ס.

אידאלים של B הם בפרט אידאלים שבריים. אם נרצה להדגיש שאידאל שברי הוא אידאל נאמר שהוא אידאל שלם.

דוגמאות:

1) אם $0\neq x\in K$, אז Bx אידאל שברי. אידאלים כאלה נקראים ראשיים ומתקיים $(Bx)^{-1}=Bx^{-1}$.

2) m^{-1}, עבור m אידאל שברי, הוא אידאל שברי. די לבדוק ש-m^{-1} נ"ס. ניקח $0\neq x\in m$. אזי, $m^{-1}x\subseteq B$. לכן $m^{-1}x$ נ"ס כי B נתרי. אבל, כמודולים מעל B, $m^{-1}x\cong m^{-1}$. לכן m^{-1} נ"ס.

הגדרה: אידאל שברי m נקרא הפיך אם $B=m^{-1}m$. כמו כן, אם m_1,m_2 אידאלים שבריים, מגדירים -

$$m_1m_2=\left\{\sum_{i=1}^{k} m_{i1}m_{i2} \mid m_{i1}\in m_1, m_{i2}\in m_2\right\}$$

ביחס לכפל הנ"ל B הוא יחידה, וכן $Bx\cdot m=mx$.

נרצה להוכיח שכל אידאל שברי הוא הפיך.

למה: יהא $0\neq a\subseteq B$ אידאל שלם. אז a הפיך.

הוכחה: נסמן $b=aa^{-1}\subseteq B$ אידאל שלם.

ברור גם ש-$a\subseteq b$. (כי $1\in a^{-1}$)

נבדוק לוקלית ש-$B=b$. יהי P מקסימלי.

[illegible]

תרגיל: אם $\mathfrak{m}$ אידאל שברי של B, אז $\mathfrak{m}_p = B_p\mathfrak{m}$ אידאל שברי של B_p, $(\mathfrak{m}\mathfrak{n})_p = \mathfrak{m}_p\mathfrak{n}_p$, $(\mathfrak{m}^{-1})_p = \mathfrak{m}_p^{-1}$.

וגם,

$$\mathfrak{b}_p \subseteq \mathfrak{a}_p\mathfrak{a}_p^{-1} \subseteq R_p$$

כיוון ש- B_p הוא PID כי הוא תחום דדקינד (3) יש $\mathfrak{a}_p = B_p x$, ולכן $\mathfrak{a}_p^{-1} = B_p x^{-1}$. משמע $\mathfrak{b}_p = B_p x x^{-1} = B_p$. לכן $\mathfrak{b} = B$. □

משפט: יהי $\mathfrak{m} \neq 0$ אידאל שברי. אז יש פירוק יחיד (עד כדי סדר) $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ כאשר $0 \neq e_1, \dots, e_r \in \mathbb{Z}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ראשוניים שונים, וכן, $k > 0$, $\mathfrak{p}_i^{-k} := (\mathfrak{p}_i^{-1})^k$.

מסקנה: כל אידאל שברי $\neq 0$ הפיך. כי -

$$\mathfrak{m}^{-1} = \mathfrak{p}_1^{-e_1} \cdots \mathfrak{p}_r^{-e_r}$$

$$\Rightarrow \mathfrak{m}\mathfrak{m}^{-1} = \underbrace{(\mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_1^{-e_1})}_{=R} \cdots \underbrace{(\mathfrak{p}_r^{e_r} \cdot \mathfrak{p}_r^{-e_r})}_{=R} = R$$

הוכחת המשפט:

ניקח $0 \neq x \in \mathfrak{m}^{-1} \cap R$. נניח כך $\mathfrak{m}x \subseteq R$. ולכן יש פירוק לראשוניים,

$$\mathfrak{m}x = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s}, \quad a_i \geq 0$$

וכן,

$$Bx = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_s^{b_s}, \quad b_i \geq 0$$

(דקוש - כדאי להבין ההוכחה של $\mathbb{Q}, \mathbb{Z}$)

עכשיו,

$$(Bx)^{-1} = \mathfrak{p}_1^{-b_1} \cdots \mathfrak{p}_s^{-b_s}, \quad b_i \geq 0$$

ואז,

$$\mathfrak{m} = (\mathfrak{m}Bx)(Bx^{-1}) = \prod \mathfrak{p}_i^{a_i - b_i}$$

והוכחנו קיום פירוק.

הוכחת יחידות, אם -

$$\mathfrak{m} = \prod \mathfrak{p}_i^{\alpha_i} \prod \mathfrak{q}_j^{-\beta_j} = \prod \mathfrak{p}_i^{\gamma_i} \prod \mathfrak{q}_j^{-\delta_j}$$

$$(\alpha_i, \beta_j, \gamma_i, \delta_j \geq 0)$$

$$\Leftarrow \quad \prod \mathfrak{p}_i^{\alpha_i} \prod \mathfrak{q}_j^{\delta_j} = \prod \mathfrak{p}_i^{\gamma_i} \prod \mathfrak{q}_j^{\beta_j}$$

ואז מיחידות הפירוק בראשוניים אשר (עד סדר) - יש רק שוויון בכל מקום $\delta_j = \beta_j$, $\alpha_i = \gamma_i$.

<u>הגדרה:</u> $I(B) = \{$ חבורת האידיאלים השברים $\neq 0 \}$ - זו חבורה (כפלית): עם B איבר יחידה. למעשה זו חבורה חופשית אבלית, עם קבוצת הראשוניים המקסימליים כבסיס.

<u>הגדרה:</u> נסמן -

$$I(B) \supseteq P(B) = \{ \text{אידיאלים ראשיים} \}$$

נשים לב ש- $P(B) = I(B)$ אמ"מ B הוא PID.
נגדיר את <u>חבורת המחלקה</u> של B להיות המנה,

$$C(B) = I(B)/P(B)$$

<u>משפט:</u> (שנוכיח אח"כ)
אם B חוג שלמים (הסגור השלם של $\mathbb{Z}$ בהרחבה סופית של $\mathbb{Q}$) אז $|C(B)|<\infty$.

במקרה כזה נאמר ש- $|C(B)|$ הוא <u>מספר המחלקה</u>.

[יש משפט Claborn משנות ה-60 שאומר שלכל חבורה אבלית A יש חוג דדקינד B כך ש- $C(B)\cong A$]

<u>חוגי דדקינד בהרחבות</u>

תהי L/K הרחבה סופית ספרבילית. יש לה העתקת העקבה -

$$Tr_{L/K} : L \to K$$

שמגדירה תבנית ביליניארית, <u>תבנית העקבה</u>,

$$T_{L/K}(x,y) : L\times L \to K$$
$$(x,y) \mapsto tr_{L/K}(xy) := \langle x,y \rangle$$

תזכורת - תבנית ביליניארית היא <u>לא מנוונת</u> אם
כלומר $T(\cdot,x)\not\equiv 0$ לכל $x\neq 0$.

לה ג.מ.ח המטריצה המייצגת לא מנוונת.

<u>משפט:</u> L/K פרידה $\iff$ התבנית העקבה לא מנוונת.

<u>הוכחה:</u> "$\Leftarrow$" נניח ש- L/K פרידה. לכן, $L=K(\theta)$, $\theta\in L$ (משפט ~~השלם~~ היוצר הפרימיטיבי), ולכן $1,\theta,\dots,\theta^{n-1}$ בסיס של L/K.
נחשב את המטריצה המייצגת:

$$\left(Tr(\theta^{i-1}\theta^{j-1})\right)_{i,j=1,\dots,n}$$

נסמן את הצמודים של θ ב- $\theta_1=\theta,\dots,\theta_n$.
אז:

$$Tr_{L/K}(\theta^{i+j-2}) = \sum_{k=1}^{n}\theta_k^{i+j-2}$$

שקול - המטריצה היא -

$$\left(\sum \theta_k^{i+j-2}\right)_{i,j}$$

$$\begin{pmatrix} 1 & \cdots & 1 \\ & \ddots & \\ \theta_1^{n-1} & \cdots & \theta_n^{n-1}\end{pmatrix}\begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1}\end{pmatrix} = V(\theta_1,\dots,\theta_n)V^T(\theta_1,\dots,\theta_n)$$

אז מקבלים שה-דט הינה שונה:

$$\det V(\theta_1,\dots,\theta_n) = \prod_{i<j}(\theta_i-\theta_j) \neq 0$$

כי ההרחבה L/K פרידה.

"$\Rightarrow$" L/K לא פרידה. נפרק -

$$\underbrace{K - K^{sep}}_{\text{פריד}} \underbrace{- L}_{\text{אי-פרידה לגמרי}}$$

לכל $x\in L$, יש $n\geq 1$ כך ש- $x^{p^n}\in K^{sep}$. לכן,

$$x^{p^n} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1\end{pmatrix}$$

$\Rightarrow Tr = 0$

$\square$

תכונת דדקינד — של מנוונת

$\Downarrow$

משמעות של בסיס דואלי.

אם $v_1,\dots,v_n$ בסיס אז יש בסיס דואלי $v_1^*,\dots,v_n^*$ כך ש- $Tr(v_i v_j^*) = \delta_{ij}$.

<u>מסקנה:</u> אם L/K פריד נקבל בסיס $x_1,\dots,x_n\in L$ אז יש בסיס ד.ו. $y_1,\dots,y_n\in L$ כך ש- $Tr(x_i y_j)=\delta_{ij}$.

<u>משפט:</u> יהי B חוג דדקינד עם שדה שברים K, L/K הרחבה סופית. $\tilde{B}$ הסגור השלם, S, של B ב-L - הוא דדקינד.

<u>הוכחה:</u> די להוכיח לפריד ולאי פריד בטהורה. (רמקך

<u>ב</u> בפריד: נניח L/K פרידה.

מהגדרה, S סגור בשלמות. צ"ל S נתרי ממימד קרול $=1$.

הוכחנו ש S לעומת B - נ"ס וגם "ירד",

משאירים את B, ש- S נתרי.

יהי $x_1,\dots,x_n\in S$ בסיס את L. (אם יש לנו בסיס $x_1',\dots,x_n'\in L$ נכפיל במכנה משותף מ-B, כך שיהיו ב-S)

$$Bx_1+\dots+Bx_n \subseteq S$$
$$S\subseteq Kx_1+\dots+Kx_n = L$$

ניקח בסיס דואלי $y_1,\dots,y_n$. ונראה ש- $S\subseteq By_1+\dots+By_n$.

אכן ניקח $x\in S$. נרשום -

$$x = c_1y_1+\dots+c_ny_n,\quad c_i\in K$$

נכפיל ב- x_j וניקח עקבה.

$$B=S\cap K\ni Tr(xx_j)=\sum_{i=1}^n c_i Tr(y_ix_j) = c_j\in B$$

לכן, S נתרי! די להוכיח ש- $\mathfrak{P}\cap B=\mathfrak{p}$ מקסימלי. לכן מספיק להראות $\mathfrak{p}\neq B,0$. הוא $\neq B$ כי לא מכיל את 1, הוא $\neq 0$ כי ניקח $x\in \mathfrak{P}$, $x\neq 0$, וניקח $f(x)$ פולינום המינימלי של x. f אי פריק, לכן $f(0)\neq 0$. ומצד שני, $f(0)\neq 0 = \pm\prod_{i=1}^n x_i \in \mathfrak{P}\cap K = \mathfrak{p}$. לכן סיימנו.

צמודים, כולם שלמים ולכן ב-S,

הגדרה: תהא $L/\mathbb{Q}$ הרחבה סופית. נסמן $\mathbb{Z}_L$ או O_L - הסגור השלם של $\mathbb{Z}$ ב-L. אז O_L - חוג דדקינד. חוגים מהצורה הזו נקראים חוגי שלמים.

הרחבה של אידיאלים ראשוניים

יהא O_K חוג דדקינד עם שדה מנות K. תהא L/K הרחבה סופית, O_L - החוג דדקינד של שהוא הסגור השלם של O_K.

ניקח $p \in Spec(O_K)$, $\neq 0$. אזי,

$$pO_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

עם $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ ראשוניים שונים של O_L, $e_i \geq 1$. נאמר ש- $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ הם הראשוניים מעל p.

הגדרה: יהי $\mathfrak{P}$ ראשוני של O_L מעל ראשוני p של O_K. אינדקס הסיעוף של $\mathfrak{P}$ מעל p, המסומן $e(\mathfrak{P}|p)$, זו החזקה של $\mathfrak{P}$ בפירוק של pO_L. המעלה היחסית של $\mathfrak{P}/p$ מוגדרת להיות -

$$f(\mathfrak{P}/p) = [L(\mathfrak{P}) : K(p)]$$

לבסוף, $g(p)$ מוגדר להיות מס' הראשוניים מעל p.

דוגמא: $O_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \sqrt{2}\mathbb{Z}$.

$$2O = (\underbrace{\sqrt{2}\, O}_{\text{ראשוני}})^2$$

כי -

$$\sqrt{2}\, O = \sqrt{2}\mathbb{Z} + 2\mathbb{Z}$$

ואז,

$$O/\sqrt{2}O = \mathbb{Z}/2\mathbb{Z} \text{ - שדה}$$

לכן $\sqrt{2}O$ ראשוני.

אזי, $f=1$, $e=2$, $g=1$.

לא ברור ש- f סופי (א-פריורי) אבל סופיות אני נוכיח מאוחר יותר בכלליות. נבוא בעת ישירות כבר עכשיו. משהו חזק יותר אפילו, ש- $f \leq [L:K]$.

למה: יהי $\mathfrak{a}$ אידאל ב-$\mathcal{O}_L$, כך ש-$\mathfrak{a} \cap \mathcal{O}_K =: \mathfrak{p}$ ראשוני. אז,

$$\dim_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{a}) \le [L:K]$$

בפרט, נקבל -

מסקנה: עבור $\mathfrak{a} = \mathfrak{P}$ נקבל $f \le [L:K]$.

הוכחה (**למה**): נמקם ב-$\mathcal{O}_K - \mathfrak{p}$, ואז $\mathcal{O}_L/\mathfrak{a}, \mathcal{O}_K/\mathfrak{p}$ שמורים, כדי להניח בה"כ ש-$\mathcal{O}_K$ הוא PID.
ניקח $x_1, \dots, x_r \in \mathcal{O}_L$ בת"ל מודולו $\mathfrak{a}$, די להוכיח שהם בת"ל מעל K. אחרת יש צ"ל,

$$a_1x_1 + \dots + a_rx_r = 0$$

עם $a_i \in K$ לא כולם 0. כיוון ש-$\mathcal{O}_K$ הוא PID וגם מקומי, נרשום $a_i = \pi^{\alpha_i}u_i$, $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2, u_i \notin \mathfrak{p}$, $\alpha_i \in \mathbb{Z}$.
נסמן $\beta = \min_{i, a_i \neq 0} \alpha_i$. נכפיל ב-$\pi^{-\beta}$. נקבל:

$$a_1'x_1 + \dots + a_r'x_r = 0$$

כאשר $a_i' = \pi^{\alpha_i - \beta}u_i$ לא כולם ב-$\mathfrak{p}$! ניקח מודולו ונקבל סתירה.

□

המסקנה הכללית -

$$\sum_{i=1}^{g} e_i f_i = [L:K]$$