הרצאה 13

הגדרה 1) M R-מודול נקרא נוצר סופית אם יש אוסף סופי של איברים $m_1,m_2,\dots,m_n\in M$ כך ש- $M=Rm_1+Rm_2+\dots+Rm_n$

כלומר ניתן להציג כל $m\in M$ (לא בהכרח באופן יחיד) בצורה $m=r_1m_1+r_2m_2+\dots+r_nm_n$ כאשר $r_1,\dots,r_n\in R$.

2) $R\subset S$ חוגים, איבר $s\in S$ נקרא שלם מעל R אם הוא שורש של פולינום מתוקן מעל R, כלומר קיימים $n\geq 1$, $r_0,r_1,\dots,r_{n-1}\in R$ כך ש-

$$s^n+r_{n-1}s^{n-1}+\dots+r_1s+r_0=0_S$$

דוגמא $R=\mathbb{Z}$, $S=\mathbb{Q}$ תרגיל: $s\in\mathbb{Q}$ שלם מעל $\mathbb{Z}$ $\iff$ $s\in\mathbb{Z}$

$ns-m=0 \Leftarrow s=\frac{m}{n}$.

משפט יהיו $R\subset S$ חוגים חילופיים. יהי $s\in S$.
הטענות הבאות שקולות:

1) s שלם מעל R.

2) תת-חוג $R[s]\subseteq S$ הינו R-מודול נוצר סופית.

3) קיים תת-חוג $R\subseteq R[s]\subseteq T\subseteq S$ כך ש- T הינו R-מודול נוצר סופית.

4) קיים $R[s]$-מודול נאמן M כך ש- M נוצר סופית כמודול מעל R.

__הוכחה__ $2)\Rightarrow 3)\Rightarrow 4)$ קל.

__$1)\Rightarrow 2)$__ (הוכחנו גם בסוף השיעור הקודם).

$$R[s]=\left\{r_0+r_1s+r_2s^2+\dots+r_ns^n \;\middle|\; \begin{matrix} n\in\mathbb{N} \\ r_i\in R\end{matrix}\right\}$$

לכאורה: $R=R\cdot1+R\cdot s+R\cdot s^2+R\cdot s^3+\dots$

לא ברור מדוע זה יהיה נוצר סופית.

__אבל__ אם s שלם, אזי

$$s^n+a_{n-1}s^{n-1}+\dots+a_1s+a_0=0$$

עבור $a_i\in R$, n מינימום. אפשר לבטא
כל החזקות של s כ"צירוף ליניארי" של $1,s,s^2,\dots,s^{n-1}$

לדוגמא: $s^n = -a_0\cdot 1 - a_1\cdot s - \dots - a_{n-1}s^{n-1}$

לכן $R[s] = R\cdot 1 + R\cdot s + \dots + R\cdot s^{n-1}$

נוצר סופית!

<u>$4 \Rightarrow 1$</u> יהי M מודול-$R[s]$ נאמן שנוצר סופית

כמודול מעל R. זה אומר שיש $m_1,\dots,m_n \in M$

כך ש- $M = Rm_1 + \dots + Rm_n$.

רוצים להוכיח כי s שלם מעל R.

כיוון ש-M הינו מודול-$R[s]$, $sm_i \in M$

לכן קיימים $r_{ij} \in R$ כך ש-

$$sm_i = r_{i1}m_1 + r_{i2}m_2 + \dots + r_{in}m_n$$

לכל $1 \le i \le n$. כאן r_{ij} לאו בהכרח יחידים,

אך זה בסדר. אז:

$$\begin{pmatrix} sm_1 \\ \vdots \\ sm_n \end{pmatrix} = \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

נזכיר שניתן לתת ל- $M^n = M\times\cdots\times M$
מבנה של $M_n(R[s])$-מודול.

$$sI_n\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \underbrace{\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix}}_{B}\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

$$\underbrace{(sI_n - B)}_{\in M_n(R[s])}\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0_M \\ \vdots \\ 0_M \end{pmatrix} \qquad (*)$$

אז $(\mathrm{adj}\, B)\in M_n(R)$ המטריצה המצורפת:

$(\mathrm{adj}\, B)_{ij} = (-1)^{i+j}\det\Big($ המטריצה $(n-1)\times(n-1)$ שמקבלים כאשר מוחקים שורה j-ית ועמודה i-ית של B $\Big)\in R$

<u>משפט מלינארית</u>

$$B(\mathrm{adj}\, B) = (\mathrm{adj}\, B)B = (\det B)\, I_n.$$

זה עובד גם לחוגים.

נשתמש במשפט הזה: נפעיל את $\mathrm{adj}(sI_n - B)$
על שני האגפים של $(*)$

$$\operatorname{adj}(sI_n-B)\cdot(sI_n-B)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\underbrace{(\det(sI_n-B)\cdot I_n)}_{\in M_n(R[s])}\underbrace{\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}}_{\in M^n} = \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}_{\in M^n}$$

$$\begin{pmatrix} \underbrace{\det(sI_n-B)}_{\in R[s]}\cdot m_1 \\ \det(sI_n-B)\cdot m_2 \\ \vdots \\ \det(sI_n-B)\cdot m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

לכן, לכל $m\in M$, $\underbrace{\det(sI_n-B)}_{\in R[s]}\cdot m = 0_M = 0_{R[s]}\cdot m$

$\det(sI_n-B) = 0_{R[s]} = 0_s \Leftarrow$ נאמן M

$$\det\begin{pmatrix} s-r_{11} & -r_{12} & \cdots & -r_{1n} \\ -r_{21} & s-r_{22} & \cdots & -r_{2n} \\ \vdots & & & \\ -r_{n1} & -r_{n2} & \cdots & s-r_{nn} \end{pmatrix} =$$

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$$

עבור $a_i\in R$ מתאימים. לכן s שלם מעל R.

מסקנה יהיו $R<S$ חוגים חילופיים.

יהי $R' = \{ s\in S \mid s$ שלם מעל $R \}$

אזי R' הינו תת-חוג של S.

דוגמה $R=\mathbb{Z}$, $S=\mathbb{C}$

$R' = \overline{\mathbb{Z}} = \{$השלמים האלגבריים$\}$

$= \{ s\in\mathbb{C} \mid$ זה שורש של פולינום מתוקן עם מקדמים ב-$\mathbb{C}\}$

הוא חוג.

הוכחה יהיו $s_1, s_2 \in R'$. זה אומר לפי ההוכחה של $(1)\Rightarrow(2)$

$$R[s_1] = R\cdot 1 + \dots + R\cdot s_1^{n_1-1}$$

$$R[s_2] = R\cdot 1 + \dots + R\cdot s_2^{n_2-1}$$

אזי:

$R[s_1,s_2] = \{ \sum_{i,j} r_{ij} s_1^i s_2^j \mid$ מספר סופי של $r_{ij}\neq 0 \}$

נוצר מעל R ע"י $s_1^i s_2^j$, $0\le i\le n_1-1$, $0\le j\le n_2-1$

$M=R[s_1,s_2]$ הינו $R[s_1+s_2]$-מודול
$R[s_1s_2]$-מודול [נאמן]

שנוצר סופית מעל R. לפי תנאי 4),
s_1+s_2, s_1s_2 שלמים מעל R.

<u>הערה</u> יהי R חוג חילופי. אזי
$A\in M_n(R)$ הפיכה אם ורק אם
$\det A\in R$ הפיכה (כאיבר של R).

<u>הוכחה</u> $\Leftarrow$) אם A הפיכה, אזי קיימת
$B\in M_n(R)$ כך ש- $AB=I_n$.

$$(\det A)(\det B)=\det I_n=1_R$$

לכן $\det A\in R$ הפיכה.

$\Rightarrow$) אם $\det A$ הפיכה, אזי

$$\underbrace{\frac{1}{\det A}(\mathrm{adj}\,A)}_{\in M_n(R)}\cdot A = I_n$$

כי $\det A$ הפיכה.

הגדרה יהי F שדה, S חוג, $F\subset S$.
יהי $s\in S$ איבר אלגברי מעל F (= שלם מעל F, כי F שדה). אזי

$$(0)\neq I=\{f\in F[x] : f(s)=0_S\}\trianglelefteq F[x]$$

אידאל. אבל $F[x]$ תחום אוקלידי, לכן תחום ראשי. לכן קיים פולינום לא אפסי $f_s\in F[x]$ כך ש- $I=(f_s)$. להבחילה, f_s מוגדר עד כדי חברות, אך האברים ההפיכים של $F[x]$ הם F^*. לכן אם נדרוש בנוסף כי f_s מתוקן אזי הוא מוגדר היטב.

נקרא f_s **הפולינום המינימלי** של s.

טענה יהי R תפ״י. יהי $F=\mathrm{Frac}\,R$. יהי $R\subset F\subset S$. אזי $s\in S$ שלם מעל R $\Longleftrightarrow$ $f_s\in R[x]$.

__הוכחה__ (⇒) אם $f_s \in R[x]$, אזי f_s הינו
פולינום מתוקן מעל R, s שורש שלו,
לכן s שלם מעל R.

(⇐) נניח s שלם מעל R. אז קיים
$g \in R[x] \subseteq F[x]$ מתוקן כך ש- $g(s)=0$. אז $g \in I$,
לכן $g(x)=f_s(x)h(x)$ כפולינומים ב- $F[x]$.
לפי הלמה של גאוס, קיימים $\tilde{f},\tilde{h} \in R[x]$ כך ש-
$g(x)=\tilde{f}(x)\tilde{h}(x)$ וגם $\tilde{f}=\alpha \cdot f_s$ כאשר $\alpha \in F$.
אבל g מתוקן, המקדם המוביל של $\tilde{f}$
הינו $\alpha \Leftarrow \alpha$ הפיך ב- R. לכן
$f_s(x)=\frac{1}{\alpha} f(x) \in R[x]$.

__מטרה__ לקחת שדה F ולהגדיר בתוכו
"חוג שלמים" O_F כך ש- $F=\mathrm{Frac}\, O_F$
וכן שהזוג (F,O_F) "יתנהג כמו" $(\mathbb{Q},\mathbb{Z})$.

הגדרה שדה ריבועי הינו שדה $\mathbb{Q}\subseteq F$

וכך ש- $\dim_{\mathbb{Q}} F = 2$.

תרגיל קיים $0,1\neq d\in\mathbb{Z}$ חפשי מריבועים

(כלומר d לא מתחלק בשום ריבוע שלם

$(4,9,16,\dots$ כך ש-

$$F=\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d}\mid a,b\in\mathbb{Q}\}\subseteq\mathbb{C}$$

פתרון יהי F שדה ריבועי. יהי

$\{1,\alpha\}$ בסיס מעל $\mathbb{Q}$. אזי $\alpha^2\in F \Leftarrow$

$$\alpha^2=c_1\cdot 1+c_2\cdot\alpha \Leftarrow c_1,c_2\in\mathbb{Q}.$$

$$\alpha^2-c_2\alpha-c_1=0$$

$$\Big(\underbrace{\alpha-\frac{c_2}{2}}_{\in\mathbb{Q}}\Big)^2=\alpha^2-c_2\alpha+\frac{c_2^2}{4}=c_1+\frac{c_2^2}{4}.$$

אבל $\{1,\underbrace{\alpha-\frac{c_2}{2}}_{\beta}\}$ גם בסיס של F מעל $\mathbb{Q}$.

אז $\beta^2=c_1+\frac{c_2^2}{4}\in\mathbb{Q}$. אם נכפיל את

β ב- $r \in \mathbb{Q}$ שנבחר חכם, נקבל

$(r\beta)^2 = \underbrace{r^2\beta^2}_{d} \in \mathbb{Z}$ חפשי מריבועים.

אבל $\{1, \underbrace{r\beta}_{\sqrt{d}}\}$ גם בסיס של F.

<u>תרגיל</u> יהי $F = \mathbb{Q}(\sqrt{d})$, יהי

$\mathcal{O}_F = \{\alpha \in F :$ α שלם מעל $\mathbb{Z}\}$

אזי

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, & d \equiv 2,3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \{a + \frac{b(1+\sqrt{d})}{2} : a, b \in \mathbb{Z}\} & d \equiv 1 \mod 4. \end{cases}$$