הרצאה 17

היום נוכיח את משפט המיון של מודולים נוצרים סופית מעל תחום ראשי.

ההוכחה הסטנדרטית, לדוגמא בספר Atiyah-Macdonald

אנחנו נראה הוכחה שמשתמשת במושגים אנלוגיים לאלגברה לינארית.

<u>הגדרה</u> מודול M נקרא ציקלי אם הוא נוצר על ידי איבר אחד: קיים $m\in M$ כך ש- $M=Rm$.

הוכחנו M ציקלי $\Longleftrightarrow$ קיים אידיאל שמאלי $I\trianglelefteq R$ כך ש- $M\simeq R/I$ כ-R-מודולים

<u>אבחנה</u> יהי R חוג חילופי. יהי M R-מודול ציקלי. אזי $M\simeq R/\mathrm{Ann}_R(M)$.

<u>הוכחה</u> לפי השימוש שעבר, $M\simeq R/I$, כאשר $I\trianglelefteq R$ אידיאל שמאלי ולכן דו-צדדי, כי R חילופי.

לכל $r\in R$, אזי $r\in I \Longleftrightarrow r(1+I)=r+I=0_M \Longleftarrow r\in\mathrm{Ann}_R(M)$

אזי $\mathrm{Ann}_R(M)\subseteq I$ הכיוון השני ברור כי לכל $a\in I$ ולכל $r\in R$, $a(r+I)=\underbrace{ar}_{\in I}+I=0_M$

$I=\mathrm{Ann}_R(M)$.

<u>בפרט</u>: $M\simeq R/I$ עבור אידיאל <u>יחיד</u> $I\trianglelefteq R$. (*)

עכשיו, ולהמשך השיעור, יהי R תחום ראשי.
בפרט, R הינו תפ"י, לכן לכל שני איברים
יש gcd. נזכור: $d=\gcd(a,b)$ אם (d)
הינו האיבר המינימלי היחיד של הקבוצה

$$\left\{ I \;\middle|\; \begin{matrix} I \trianglelefteq R \text{ אידיאל ראשי} \\ I \supseteq (a,b) \end{matrix} \right\}$$

אך במקרה שלנו, (a,b) כבר ראשי (כי כל
אידיאל ב-R ראשי) ולכן $(d)=(a,b)$.

<u>מסקנה</u> יהי R תחום ראשי ויהיו $a,b\in R$.
יהי $d=\gcd(a,b)$. אזי קיימים $x,y\in R$ כך ש-

$$d=xa+yb$$

<u>הוכחה</u> $(d)=(a,b)$, לכן $d\in(a,b)$.

<u>טענה</u> R תחום ראשי, יהי $n\geq 2$. ויהיו $c_1,\dots,c_n\in R$ כך ש-
$\gcd(c_1,c_2,\dots,c_n)=1$. אזי קיימת מטריצה
$A\in M_n(R)$ כך ש- 1) $\det A=1$.
2) העמודה הראשונה של A הינה $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$.

<u>הוכחה</u> אינדוקציה על n:

$n=2$ אזי $1=\gcd(c_1,c_2)$

לכן $1 = xc_1+yc_2$ עבור $x,y\in R$ מתאימים.

ניקח $A=\begin{pmatrix} c_1 & -y \\ c_2 & x \end{pmatrix}$

עכשיו נניח שהטענה ידועה עבור $n-1$. יהי

$g=\gcd(c_2,\dots,c_n)$.

אזי: $\gcd(g,c_1)=1$, לכן $c_1x+gy=1$ עבור $x,y\in R$ מתאימים.

יהי $c_i = gc_i'$ לכל $2\le i\le n$.

מהאינדוקציה קיימת $A'\in M_{n-1}(R)$ כך ש- $\det A'=1$

$$A'=\begin{pmatrix} c_2' & \\ \vdots & * \\ c_n' & \end{pmatrix}$$

ניקח

$$A=\begin{pmatrix} c_1 & 0 & \cdots & 0 & (-1)^{n-1}y \\ c_2 & & & & (-1)^n x c_2' \\ \vdots & & \text{העמודות } n-2 \text{ האחרונות של } A' & & \vdots \\ c_n & & & & (-1)^n x c_n' \end{pmatrix}$$

<u>מסקנה</u> יהי M מודול נוצר סופית מעל R (תחום ראשי).

אזי $\{m_1,\dots,m_n\}$ קבוצה יוצרת, כלומר

$M= Rm_1+\dots+Rm_n$.

ויהיו $c_1,\dots,c_n\in R$ כך ש- $\gcd(c_1,\dots,c_n)=1$

אזי קיימת קבוצה יוצרת $\{m_1',\dots,m_n'\}$

כך ש- $m_1'=c_1m_1+\dots+c_nm_n$.

<u>הוכחה</u> יהי A המטריצה מן הטענה הקודמת

$$A=(a_{ij})$$

נגדיר

$$m_j'=a_{1j}m_1+a_{2j}m_2+\dots+a_{nj}m_n$$

$$(m_1'=c_1m_1+\dots+c_nm_n)$$

ברור כי $\underbrace{\langle m_1',\dots,m_n'\rangle}_{\text{(תת-מודול) הנוצר ע"י } m_1',\dots,m_n'}\leq M$

יהי $B=\operatorname{adj}(A)$. אזי $BA=(\det A)I_n=I_n$

$B\in M_n(R)$

כשהוכחנו את זה בלינארית לא השתמשנו בחילוק, לכן הטענה נכונה מעל כל חוג.

אזי (פורמלית) $B=(b_{ij})$

$$m_j=b_{1j}m_1'+\dots+b_{nj}m_n'$$

לכן $m_1,\dots,m_n\in\langle m_1',\dots,m_n'\rangle$

לכן $M\subseteq\langle m_1',\dots,m_n'\rangle$

לכן $\{m_1',\dots,m_n'\}$ אכן קבוצה יוצרת.

<u>משפט המיון</u> יהי R תחום ראשי. יהי M מודול נוצר סופית מעל R. אזי

$$M \simeq R^r \times R/(d_1) \times R/(d_2) \times \dots \times R/(d_s)$$

כאשר $0 \le r, s$ וכאשר $d_i \in R$ איברים לא אפסיים ולא הפיכים כך ש- $d_1 | d_2$, $d_2 | d_3$, $\vdots$ $d_{s-1} | d_s$.

השלם r <u>והאידיאלים</u> $(d_1), \dots, (d_s)$ (כלומר האיברים $d_1, \dots, d_s$ עד כדי חברות) מוגדרים באופן יחיד.

בנוסף, $n = r+s$ הינו העוצמה של קבוצת יוצרים מינימלית של M.

(<u>ניתן</u> לייצר את M ע"י n איברים אך לא ו-$n-1$).

הנ"ל הינו הניסוח הקלאסי של המשפט.

אם נאפשר $d_i = 0$ נקבל ניסוח אחיד יותר.

ניסוח שקול של המשפט) יהי R תחום ראשי, M נוצר סופית. אזי

$$M \cong R/(d_1) \times \cdots \times R/(d_n).$$

כאשר (d_i) אידיאלים אמיתיים וכאשר

$$(d_1) \supseteq (d_2) \supseteq (d_3) \supseteq \cdots \supseteq (d_n)$$

כלומר $d_1 | d_2, \dots, d_{n-1} | d_n$.

האידיאלים $(d_1),\dots,(d_n)$ מוגדרים באופן יחיד ונקראים הגורמים האינווריאנטיים של M.

מדוע זה שקול לניסוח הקודם?

יהי $d_{s+1} = \cdots = d_n = 0$. אז $R/(0) \cong R$.

נשים לב כי $0 | r$ לכל $r \in R$ $(0 = r \cdot 0)$

אך 0 מחלק רק את 0.

הוכחה יהי n מספר היוצרים המינימלי של M,

נעשה אינדוקציה על n.

$n=1$ M ציקלי, הוכחנו $M \cong R/(d_1)$

(יתכן $d_1=0$, הוכחנו את היחידות שלו (*) $(d_1) = \mathrm{Ann}_R(M)$.

נניח שהמשפט ידוע עבור $n-1$:

נבחר קבוצת יוצרים $\{m_1,\dots,m_n\}$ של M

כך שבה:

$$(d_1) = \mathrm{Ann}_R(Rm_1) = \{r \in R : rm_1 = 0_M\},$$

כלי מספר הגורמים האי-פריקים של d_1 מינימלי

(R תפ"י — $d_1 = p_1 p_2 \cdots p_t$, כלומר t מינימלי)

בהמשך נסמן $(d_1) = \mathrm{Ann}_R(m_1)$.

נגדיר שני תת-מודולים של M:

$$M_1 = Rm_1$$

$$M_2 = Rm_2 + \dots + Rm_n = \langle m_2,\dots,m_n\rangle$$

<u>תת-טענה</u> $M \simeq M_1 \times M_2$.

<u>תת-הוכחה</u> לפי המשפט הקודם, צריך להוכיח

א) $M_1 + M_2 = M$

ב) $M_1 \cap M_2 = (0)$.

אז ברור כי לכל $m\in M$,

$$m = \underbrace{r_1m_1}_{\in M_1} + \underbrace{r_2m_2+\dots+r_nm_n}_{\in M_2}$$

לכן $M = M_1+M_2$

נוכיח את ב). יהי $m\in M_1\cap M_2$. אזי

$$\boxed{m = r_1m_1 = r_2m_2+\dots+r_nm_n} \quad (**)$$

צריך להוכיח $m=0$, כלומר $r_1m_1=0$.

יהי $h=\gcd(r_1,d_1)$ $\quad (d_1)=\mathrm{Ann}_R(m_1)$

לכן $h = xr_1+yd_1$ עבור $x,y\in R$ מתאימים.

$$(c_1m_1) = hm_1 = (xr_1)m_1 + \cancel{(yd_1)m_1}^{\to 0} = xr_1m_1$$

$(y(d_1m_1)=0)$

יהי $c_1=h$, $c_i = xr_i$ לכל $2\le i\le n$. אזי

$$c_1m_1 = hm_1 = xr_1m_1 = c_2m_2+\dots+c_nm_n$$

נכפול את $(**)$ ב-x.

מה הרעיון?

מספיק להוכיח $c_1m_1=0$, כי $c_1=h$, אך $h|r_1 \Rightarrow$ $hm_1=0$ $\Downarrow$ $r_1m_1=0$

לכן נקבל $\boxed{c_1m_1 = c_2m_2 + \dots + c_nm_n}$ (***)

צריך להוכיח $c_1m_1=0$, עכשיו $\boxed{c_1 | d_1}$ $(*)^4$

$(c_1 = h = \gcd(r_1,d_1))$.

יהי $$g = \gcd(c_1, \dots, c_n)$$

ויהי $$c_i = g c_i'.$$

אזי $$\gcd(c_1', \dots, c_n') = 1.$$

לכן, לפי הטענה הקודמת, יש קבוצ. יוצר. $\{m_1', \dots, m_n'\}$ כך ש-

$$m_1' = -c_1'm_1 + c_2'm_2 + \dots + c_n'm_n.$$

יהי $$\underbrace{(d_1')}_{\text{הגדרה של } d_1'} = \mathrm{Ann}_R(m_1') = \{r \in R : rm_1' = 0_M\}$$

לפי המינימליות של d_1, ידוע מספר הגורמים האי-פריקים של d_1' לא קטן ממספר הגורמים האי-פריקים של d_1.

<u>בפרט</u> אם נוכיח $d_1' | d_1$, נקבל כי d_1, d_1' חברים

(כי אז $d_1 = d_1'y$, אך אם y לא הפיך, הפירוק של d_1 יהיה ארוך מן הפירוק של d_1', בסתירה למינימליות).

נשים לב כי

$$gm_1' = g(-c_1'm_1 + c_2'm_2 + \dots + c_n'm_n) =$$
$$-c_1m_1 + c_2m_2 + \dots + c_nm_n = 0_M \quad (***)$$

לכן $g \in Ann_R(m_1') = (d_1')$, לכן $d_1' | g$. אבל,

$$g | c_1 \Leftarrow g = \gcd(c_1, \dots, c_n)$$

$$(*)^4 \quad c_1 | d_1$$

מסיקים, $d_1' | d_1$, ולכן d_1', d_1 חברים.

לכן $(d_1') = (d_1)$. אז $d_1' | g | c_1$, לכן

$$c_1 \in (d_1') = (d_1) = Ann_R(m_1)$$

לכן $c_1m_1 = 0$. והוכחנו את התת-טענה $M \simeq M_1 \times M_2$.

באינדוקציה:

$$M_2 \simeq R/(d_2) \times \cdots \times R/(d_n)$$

כאשר $d_2 | d_3 | \cdots | d_n$. נשאר להוכיח רק $d_1 | d_2$.