הרצאה 17

R תחום ראשי. יהיו $c_1,\dots,c_n\in R$

$g=\gcd(c_1,\dots,c_n)$.

אזי $(g)=(c_1,c_2,\dots,c_n)$.

הוכחנו בסוף השיעור הקודם: R תחום ראשי, $n\geq 2$ $c_1,\dots,c_n\in R$ איברים כך ש- $\gcd(c_1,\dots,c_n)=1$.

אזי קיימת מטריצה $A\in M_n(R)$ כך ש-

1) $\det A=1$

2) העמוד הראשון של A הינו $\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$.

<u>מסקנה</u> יהי M מודול מעל R. יהי $(m_1,m_2,\dots,m_n)$ קבוצת יוצרים של M,

כלומר $M=Rm_1+Rm_2+\dots+Rm_n$.

(בפרט, M נוצר סופית). יהיו $c_1,c_2,\dots,c_n\in R$

כך ש- $\gcd(c_1,\dots,c_n)=1$. אזי קיימת

קבוצת יוצרים אחרת של M,

$(m_1',m_2',\dots,m_n')$ מאותו גודל n, וכך ש-

$m_1'=c_1m_1+c_2m_2+\dots+c_nm_n$.

<u>הערה</u> אפשר לחשוב על הטענה הקודמת כגירסה חלשה מאוד של למת ההחלפה של שטייניץ מלינארית.

הלמה הנ-ל לא נכונה מעל חוגים.

לדוגמא:

<u>תרגיל</u> שני בסיסים של $\mathbb{Z}^2$:

$B_1=\{(5,3),(3,2)\}$ $\quad$ $B_2=\{(7,-4),(-5,3)\}$.

אבל אין שום בסיס מן הצורה $\{b_1,b_2\}$ כאשר $b_1\in B_1$, $b_2\in B_2$.

<u>הוכחה של הגבלה</u> לפי הטענה מן הפעם הקודמת קיימת מטריצה $A\in M_n(R)$ $=(a_{ij})$ כך ש-: $\det(A)=1$ וגם העמודה הראשונה של A היא $\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$, כלומר $a_{i1}=c_i$ לכל $1\le i\le n$. נגדיר

$$m_j' = a_{ij}m_1+a_{2j}m_2+\dots+a_{jn}m_n\in M.$$

ויהי $M'=Rm_1'+\dots+Rm_n'$ תת-מודול של M. צריך להוכיח כי $M'=M$.

בשביל זה מספיק להראות כי $m_i \in M'$ לכל i.

כיוון ש- $\det A = 1$ הפיכה ב- R,
המטריצה A הינה איבר הפיך של החוג
$M_n(R)$. לכן קיימת מטריצה $B \in M_n(R)$ כך
ש- $BA = I_n$. גורמים כי

$$m_j = b_{1j} m_1' + b_{2j} m_2' + \dots + b_{nj} m_n' \in M'.$$

<u>משפט</u> (מיון של מודולים נוצרים סופית
מעל תחום ראשי). יהי R תחום ראשי.
יהי M R-מודול נוצר סופית. אזי

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

כאשר: $0 \leq r, s$, ולכל $1 \leq i \leq s$, האיבר
$0 \neq d_i \in R$ איבר לא הפיך וגם $d_1 | d_2$
$d_2 | d_3$
$\vdots$
$d_{s-1} | d_s$.
המספר r והאידיאלים
$(d_1), \dots, (d_s)$ יחידים.
כלומר, d_i מוגדרים היטב
עד כדי חברות.

<u>הערה</u> נשים לב כי $R \simeq R/(0)$. לכן ניתן
לנסח את המשפט כך: יהי M מודול נוצר
סופית מעל תחום ראשי R. אזי

$$(*) \qquad M \simeq R/(d_1) \times \dots \times R/(d_n)$$

כאשר $d_i \in R$ איברים לא הפיכים וגם
$d_1 | d_2, \dots, d_{n-1} | d_n$. (כזכור: $r|0$ לכל
$r \in R$, כי $r \cdot 0 = 0$). כמו כן, ה-d_i-ים יחידים.

ה-n ב-$(*)$ הוא גודל מינימלי של קבוצה יוצרת של M. $(n = r + s)$

מן הניסוח הקודם

<u>הגדרה</u> האיברים $d_1, d_2, \dots, d_n$ (עד כדי חברות) נקראים הגורמים האינווריאנטיים של M.

<u>הוכחה של הקיום</u> של פירוק של M למכפלה ישרה של מודולים ציקליים.

תזכורת של הגדרה: יהי $m \in M$,
המאפס $Ann_R(m) = \{r \in R : rm = 0\} \lhd R$
אידאל ניתן שלא אמצעי).

נבחר קבוצה יוצרת $(m_1, m_2, \ldots, m_n)$ של M בעלת שתי התכונות הבאות:

1) n מינימלי.

2) יהי $(d_1) = Ann_R(m_1)$. אזי מספר הגורמים האי-פריקים של d_1 מינימלי בין כל קבוצות היוצרים מגודל n.

כי R הוא תחום ראשי, לכן תפ"י. אם $d_1 \neq 0$, אזי $d_1 = p_1 p_2 \cdots p_t$ מפירוק לאי-פריקים, t הוא מספר הגורמים האי-פריקים.
אם $d_1 = 0$, אומרים שיש לו ∞ גורמים אי-פריקים.

נוכיח את המשפט באינדוקציה על n.

<u>$n=1$</u> אזי $M = Rm_1$ והוכחנו בשיעור הקודם כי $M \cong R/Ann_R(m_1) = R/(d_1)$ כ-R-מודולים.

<u>$n>1$</u> יהיו $M_1 = Rm_1$
$M_2 = Rm_2 \times \cdots \times Rm_n$.

ג.ג - טענה $M \cong M_1 \times M_2$.

ג.ג - הוכחה לפי טענה מן השיעור הקודם, צריך להוכיח שני דברים:

א) $M = M_1 + M_2$.

ב) $M_1 \cap M_2 = (0)$.

א) ברור, כי $\{m_1, m_2, \dots, m_n\}$ קבוצה יוצרת של M. לכן ניתן להציג כל $m \in M$ בצורה

$$m = \underbrace{r_1 m_1}_{\in M_1} + \underbrace{r_2 m_2 + \dots + r_n m_n}_{\in M_2}$$

לכן $M = M_1 + M_2$. אז נוכיח כי $M_1 \cap M_2 = (0)$.

יהי

$$c_1 m_1 = c_2 m_2 + \dots + c_n m_n$$

איבר של החיתוך, כאשר $c_1, \dots, c_n \in R$.

יהי $h = \gcd(c_1, d_1)$

$d_1 m_1 = 0 \Leftarrow (d_1) = Ann_R(m_1)$. אז קיימים $x, y \in R$ כך ש: $h = c_1 x + d_1 y$. לכן,

$$h m_1 = c_1 x m_1 + y \cancel{d_1 m_1}^{0} = x c_1 m_1.$$

לכן $\underbrace{hm_1}_{c_1 \text{ חזק}} = xc_1m_1 = \underbrace{xc_2}_{c_2 \text{ חזל}}m_2 + \cdots + xc_nm_n$

וניתן להניח בלי הגבלת הכלליות כי $c_1|d_1$.

אז יש לנו $c_1m_1 = c_2m_2 + \cdots + c_nm_n$

כאשר $c_1|d_1$. יהי $g=\gcd(c_1,\dots,c_n)$.

ויהי $c_i = gc_i'$. אז $\gcd(c_1',\dots,c_n')=1$.

לפי הטענה הקודמת, קיימת קבוצת יוצרים $(m_1',\dots,m_n')$ מאותו גודל מינימלי n,

כך ש- $m_1' = -c_1'm_1 + c_2m_2' + \cdots + c_n'm_n$, אבל,

יהי $(d_1') = \mathrm{Ann}_R(m_1')$, נשים לב כי

$$gm_1' = -c_1m_1 + c_2m_2 + \cdots + c_nm_n = 0$$

לכן, $g \in \mathrm{Ann}_R(m_1') \Leftarrow d_1'|g \Leftarrow d_1'|g|c_1|d_1$

לפי המינימליות של מספר הגורמים האי-פריקים של d_1, מסיקים כי ל- d_1, d_1' יש אותו מספר של גורמים אי-פריקים,

לכן d_1, d_1' חברים $((d_1)=(d_1'))$

בפרט, d_1, c_1, q, d_1' כולם חברים, בפרט

$c_1 \in (d_1) = \mathrm{Ann}_R(m_1)$

ולכן $c_1 m_1 = c_2 m_2 + \dots + c_n m_n = 0$.

לכן $M_1 \cap M_2 = (0)$ והוכחנו את הנג-לינה הוודאג כי $M \cong M_1 \times M_2$.

נוכיח את הקיום של הפירוק של M.

M_2 נוצר ע"י $n-1$ יוצרים, ולכן באינדוקציה $M_2 \cong R/(d_2) \times \dots \times R/(d_n)$

כאשר $d_2 | d_3$

$\vdots$

$d_{n-1} | d_n$

($n-1$ הינו הגודל המינימלי של קב' יוצרים של M_2. אם הייתה קב' יוצרים של M_2 יותר קטנה, היינו יכולים לצרף אליה את m_1 ולקבל קב' יוצרים של M, בסתירה למינימליות של n)

קיבלנו כי $M \cong M_1 \times M_2 \cong R/(d_1) \times R/(d_2) \times \dots \times R/(d_n)$

נשאר רק להוכיח כי $d_1 | d_2$.

יהי $m' = (1+(d_2), 0+(d_3), \dots, 0+(d_n)) \in R/(d_2) \times \dots \times R/(d_n) \cong M_2$.

יהי $m' = c_2m_2 + \cdots + c_nm_n$

כאשר $c_2,\dots,c_n \in R$.

נשים לב כי $r \in Ann_R(m') \iff$

$$(r+(d_2), 0+(d_3), \dots, 0+(d_n)) =$$
$$(0+(d_2), \dots, 0+(d_n))$$

$\iff r \in (d_2)$. לכן $Ann_R(m') = (d_2)$.

יהיו
$$m' = m_2' \longleftrightarrow (1+(d_2), 0+(d_3), \dots, 0+(d_n))$$
$$m_3' \longleftrightarrow (0+(d_2), 1+(d_3), \dots, 0+(d_n))$$
$$\vdots$$
$$m_n' \longleftrightarrow (0+(d_2), \dots, 0+(d_{n-1}), 1+(d_n))$$

כאשר מגדירים $M' \simeq R/(d_2) \times \cdots \times R/(d_n)$

על ידי קביעת איזומורפיזם של R-מודולים

ביניהם. ברור כי $(m_2', \dots, m_n')$ הינה

קבוצת יוצרים של M_2, שהרי

$$(r_2+(d_2), \dots, r_n+(d_n)) = r_2m_2' + \cdots + r_nm_n'$$

לכל $r_1,\dots,r_n \in R$. לכן קבוצת היוצרים
$(m_1, m_2', \dots, m_n')$ של M מקיימת את
שני התנאים (א),(ב) מתחילת ההוכחה.

לכן, בלי הגבלת הכלליות, $m_1' = m_2$. לכן,

$$d_1 m_1 = 0 = d_2 m_2$$

בתחילת ההוכחה (d_1, d_2 ממלאים את
התפקידים של c_1, c_2 שם) הוכחנו כי
d_1 הינו חבר של $\gcd(d_1,d_2)$, אך זה
אומר כי $d_1 | d_2$ כמו שרצינו!

עד כאן, הוכחנו את קיום הפירוק

$$M \cong R/(d_1) \times \dots \times R/(d_n)$$

כאשר $d_1 | d_2, \dots, d_{n-1} | d_n$. כדי להשלים
את הוכחת המשפט, נשאר להוכיח את
היחידות.