הרצאה יד

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

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

אז $(g)=(c_1,c_2,\dots,c_n)$.

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

1) $\det A=1$

2) העמודה הראשונה של A היא $\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$.

<u>מסקנה</u> יהי M מודול מעל R. תהי
$(m_1,m_2,\dots,m_n)$ 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- $\gcd(c_1,\dots,c_n)=1$. אז 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 $\mathbb{Z}^2$:

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

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

<u>הוכחה של ההבחנה</u> לפי הטענה מן הקורס הקודמת קיימת מטריצה $A\in M_n(R)$, $A=(a_{ij})$ כך ש-

$\det(A)=1$ וגם העמוד הראשון של A הינו $\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$, כלומר $a_{i1}=c_i$ לכל $1\le i\le n$. נגדיר

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

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- $BA = I_n$. נובע 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

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

כאשר: $r, s \geq 0$, ולכל $1 \leq i \leq s$, האיבר

$0 \neq d_i \in R$ איבר לא הפיך וגם $d_1 | d_2$

$d_2 | d_3$

$\vdots$

$d_{s-1} | d_s$.

המספרים 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

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

כאשר $d_i \in R$ איברים לא הפיכים ושם $d_1 | d_2$, ..., $d_{n-1} | d_n$. (תזכורת: $r | 0$ לכל $r \in R$, כי $r \cdot 0 = 0$). גם כן, ה-d_i-ים יחידים. $(n = r + s)$

מן המשפט הקודם

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

<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

$$\mathrm{Ann}_R(m) = \{r \in R : rm = 0\} \lhd R$$

אידאל (נניח שלא אפסי).

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.

R הוא תחום ראשי, לכן תפ"י. אם $d_1 \neq 0$, אזי $d_1 = p_1 p_2 \cdots p_t$ מפורק 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 $M_1 = Rm_1$

$M_2 = Rm_2 \times \cdots \times Rm_n$.

תג - טענה $M \cong M_1 \times M_2$.

אג - 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 $\underbrace{h}_{c_1 \text{ חזק}} m_1 = xc_1m_1 = \underbrace{xc_2}_{c_2 \text{ חוש}} m_2 + \cdots + xc_nm_n$

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

ויהיו $c_i = gc_i'$. אזי $\gcd(c_1', \dots, c_n') = 1$.

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

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

יהי $(d_1') = Ann_R(m_1')$, נשים לב כי

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

לכן, $g \in Ann_R(m_1') \Rightarrow d_1' | g \Rightarrow d_1' | g | c_1 | d_1$

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', g, c_1, d_1 כולם חברים, בפרט

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

ולכן $c_1m_1 = c_2m_2 + \dots + c_nm_n = 0$.

לכן $M_1 \cap M_2 = (0)$ והוכחנו את הגגל-לרינה
הלורינג כי $M \simeq M_1 \times M_2$.

נוכיח את הקיום של הפירוק של M.

M_2 נוצר על ידי $n-1$ יוצרים, ולכן

באינדוקציה $M_2 \simeq R/(d_2) \times \dots \times R/(d_n)$

כאשר $d_2 | d_3$

$\vdots$

$d_{n-1} | d_n$

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

נשאר רק להוכיח כי $d_1 | d_2$.

יהי

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

יהי
$$m' = c_2m_2 + \cdots + c_nm_n$$
כאשר $c_2,\dots,c_n \in R$.

נשים לב כי $r \in \mathrm{Ann}_R(m') \iff$
$$(r+(d_2), 0+(d_3), \dots, 0+(d_n)) = (0+(d_2),\dots, 0+(d_n))$$
$\iff r \in (d_2)$. לכן $\mathrm{Ann}_R(m') = (d_2)$.

בנוסף, $\gcd(c_2,\dots,c_n)=1$, כי אלם היה מחלק משותף h שלא הפיך, היה קיים $m'' \in M_2$ כך ש- $hm''=m'$. בפרט, יש

$$m'' \leftrightarrow (r_2+(d_2),\dots, r_n+(d_n)) \in R/(d_2) \times \cdots \times R/(d_n)$$
כך ש-
$$(hr_2+(d_2),\dots,hr_n+(d_n)) = m' = (1+(d_2), 0+(d_3),\dots)$$

בפרט,

$$\underbrace{d_1}_{a_1} m_1 = d_2 m' = \underbrace{d_2 c_2}_{a_2} m_2 + \dots + d_2 c_n m_n$$

הוכחנו כבר כי d_1 הינו חבר של

$$g = \gcd(d_1, d_2c_2, \dots, d_2c_n)$$

לכן d_1 מחלק את $d_2c_2, \dots, d_2c_n$, לכן

$$d_1 \mid \gcd(d_2c_2, \dots, d_2c_n) = d_2$$

כיון שכן $\gcd(c_2, \dots, c_n) = 1$.