הרצאה 18

משפט יהי R תחום ראשי. יהי M R-מודול נוצר סופית. אזי

$$M \simeq R/(d_1) \times R/(d_2) \times \cdots \times R/(d_n)$$

כאשר

1) n הוא הגודל המינימלי של קבוצה יוצרת של M.

2) $d_i \in R$ לא הפיכים (אבל אולי 0) שמקיימים $d_1 | d_2 | d_3 | \cdots | d_n$.

ה-d_i-ים הללו אפסיים נקראים הגורמים האינווריאנטיים של M.

$$M \simeq R^{n-r} \times R/(d_1) \times \cdots \times R/(d_r)$$

כאשר $d_1, \ldots, d_r$ הגורמים האינווריאנטיים.

בנוסף, האיברים $d_1, d_2, \ldots, d_n$ הם יחידים עד כדי חברות.

בפעם הקודמת הוכחנו את הקיום של הפירוק של M, נשאר להוכיח את היחידות.

<u>משפט</u> (מיון של מודולים נוצרים סופית מעל תחום ראשי על ידי מחלקים אלמנטריים).

יהי R תחום ראשי, M R-מודול נוצר סופית אזי

$$M \cong R^t \times R/_{(p_1^{a_1})} \times R/_{(p_2^{a_2})} \times \dots \times R/_{(p_s^{a_s})}$$

כאשר $t \geq 0$, ה-p_i הם איברים אי-פריקים לאו בהכרח שונים לא אפסיים של R, $a_i \geq 1$. המספר t נקרא הדרגה של החלק החופשי של M.

האיברים $p_1^{a_1}, \dots, p_s^{a_s}$ נקראים המחלקים האלמנטריים של M. בהינתן M, המספר t והמחלקים האלמנטריים (עד כדי חברות) יחידים.

<u>טענה</u> שני המשפטים שקולים.

הוכחה אם $M \simeq R^m \times R/(d_1) \times \dots R/(d_r)$

$d_1 | d_2 | \dots | d_r \neq 0$, ויהי $d_i = p_{i1}^{a_{i1}} p_{i2}^{a_{i2}} \cdots p_{ir_i}^{a_{ir_i}}$

הפירוק של d_i לגורמים אי-פריקים (R הוא תפ"י) כאשר ה-p_{ij} (עבור i נתון) שונים. לפי משפט השאריות הסיני

$$R/(d_i) \simeq R/(p_{i1}^{a_{i1}}) \times \dots \times R/(p_{ir_i}^{a_{ir_i}})$$

לכן ניתן להציג את M בצורה של המשפט השני. הכיוון השני גם נכון.

לדוגמא,

$$\mathbb{Z}^4 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\underline{2}\mathbb{Z} \times \mathbb{Z}/\underline{4}\mathbb{Z} \times \mathbb{Z}/\underline{3}\mathbb{Z} \times \mathbb{Z}/\underline{9}\mathbb{Z} \times \mathbb{Z}/\underline{5}\mathbb{Z}$$

$$\simeq \mathbb{Z}^4 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

לכן כל מודול המוצג בצורה של מחלקים אלמנ' ניתן להציג גם בצורה של גורמים אינוו', באופן יחיד. (וגרגיל)

אז כדי להוכיח את שני המשפטים נשאר רק להוכיח שהדרגה של M בצורה של מחלקים אלמ' יחידה.

<u>טענה 1</u> יהי R חוג ראשי, $I \triangleleft R$ אידאל.

אם $(R/I)^m \simeq (R/I)^n$, אז $n=m$.

<u>הוכחה</u> אם I מקסימלי, אז R/I שדה, ואז זה ידוע מלינארית (F שדה.. אז $F^n \simeq F^m$ $\Leftarrow$ $m=n$ כי המימד של מרחב וקטורי מוגדר היטב). עכשיו נטפל במקרה הכללי:

יהי $P \triangleleft R$ אידאל מקסימלי שמכיל את I.

R חוג ראשי $\Leftarrow$ $P=(p)$. אם

$$(R/I)^n \xrightarrow[\sim]{f} (R/I)^m$$

$$\boxed{\text{אז } \frac{(R/I)^n}{p\,(R/I)^n} \simeq \frac{(R/I)^m}{p\,(R/I)^m}}$$

$pM = \{pm : m \in M\}$ גם-מודול

סלם $f: M \xrightarrow{\sim} N$ איזו' של R-מודולים,

איזו' $f: pM \xrightarrow{\sim} pN$ ולכן

$$f: M/pM \xrightarrow{\sim} N/pN$$

$$f(m+pM) = f(m) + pN$$

אז $\left(R/I\right)^n \big/ p\left(R/I\right)^n \overset{\text{גרעין}}{\cong}$

$$\left(\left(R/I\right) \big/ \left(pR/I\right) \right)^n = \left(\left(R/I\right) \big/ \left(P/I\right) \right)^n \underset{\uparrow}{\cong} \left(R/p\right)^n$$

איזו' 3.

קיבלנו $\left(R/p\right)^n \cong \left(R/p\right)^m \Longleftarrow n=m$.

<u>טענה</u> יהי R תחום ראשי, $d \in R$.

נתבונן ב-R-מודול הציקלי $R/(d)$.

יהי $a+(d) \in R/(d)$, כאשר $a \in R$ אזי

$$\mathrm{Ann}_R(a+(d)) = \{r\in R : r(a+(d)) = 0\}$$
$$= \{r\in R : ra\in(d)\} = \left(\frac{d}{\gcd(a,d)}\right).$$

<u>הוכחה</u> תרגיל. במקרה של $R=\mathbb{Z}$, המספר הזה קובע את הסדר של $[a]\in\mathbb{Z}_d$, והוכחנו את המקרה הזה בתרגול א'. אותה ההוכחה עובדת.

<u>תוצאה</u> יהיו

$$m=(a_1+(d_1),\dots,a_n+(d_n))\in R/(d_1)\times\cdots\times R/(d_n)$$

אז

$$\mathrm{Ann}_R(m) = \bigcap_{i=1}^{n}\mathrm{Ann}_R(a_i+(d_i))$$

<u>הערה</u> אם $a,b\in R$, ו-R תחום ראשי, וגם $\gcd(a,b)=1$, אז $(ab)=(a)(b)=(a)\cap(b)$.

<u>תוצאה</u> יהי $M\cong R/(d_1)\times\cdots\times R/(d_n)$ כאשר $d_1|d_2|\cdots|d_n$. אז

$$\mathrm{Ann}_R(M)=\{r\in R : rm=0\ \ \forall m\in M\} = (d_n),$$

הוכחה ברור כי

$$\mathrm{Ann}_R(M)=\bigcap_{i=1}^{n}\mathrm{Ann}_R\left(R/(d_n)\right)$$

אך $\mathrm{Ann}_R\left(R/(d_i)\right)=(d_i)$. אכן,

$$\mathrm{Ann}_R\left(R/(d_i)\right)\subseteq \mathrm{Ann}_R\left(1+(d_i)\right)=(d_i)$$

מצד שני ברור כי $(d_i)\subseteq \mathrm{Ann}_R\left(R/(d_i)\right)$.

לכן,

$$\mathrm{Ann}_R(M)=(d_1)\cap\cdots\cap(d_n)=(d_n).$$

הוכחה של יחידות של המחלקים האלמנטריים:

נניח

$$M\cong R^m\times R/(p_1^{a_1})\times\cdots\times R/(p_r^{a_r})\cong$$

$$R^n\times R/(q_1^{b_1})\times\cdots\times R/(q_s^{b_s}).$$

נזכר כי הגדרנו,

$$\mathrm{Tor}(M)=\{m\in M:\exists r\neq 0 ; rm=0\}=$$

$$\{m\in M:\mathrm{Ann}_R(m)\neq 0\}.$$

כיוון שקיים $f: M \to N$ איזו' של R-מודולים,

אז $\mathrm{Ann}_R(m) = \mathrm{Ann}_R(f(m))$ לכל $m \in M$.

לכן, f מגדיר איזו' $\mathrm{Tor}(M) \simeq \mathrm{Tor}(N)$ ולכן

גם $M/\mathrm{Tor}(M) \simeq N/\mathrm{Tor}(N)$.

ארגיל: בהינתן M כנ"ל,

$$\mathrm{Tor}(M) \simeq R/(p_1^{a_1}) \times \cdots \times R/(p_r^{a_r}) \simeq$$

$$R/(q_1^{b_1}) \times \cdots \times R/(q_s^{b_s}).$$

ולכן,

$$R^m \simeq M/\mathrm{Tor}(M) \simeq R^n$$

ולכן $m=n$ לפי המקרה $I=(0)$ של הטענה 1.

לכן בלי הגבלת הכלליות ניתן להניח כי

M הינו מודול של פיתול, כלומר $M = \mathrm{Tor}(M)$.

יוגם משלה. ןןיח

$$M \simeq R/(p_1^{a_1}) \times \cdots \times R/(p_r^{a_r})$$

יהי $p \in R$ אי-פריק

$$M = R/(p^{c_1}) \times R/(p^{c_2}) \times \cdots \times R/(p^{c_t}) \times$$

(מכפלות של $R/(p_i^{a_i})$ כאשר p_i לא חבר של p).

<u>תרגיל</u>

$$\{m \in M : \exists \alpha \geq 1,\ \mathrm{Ann}_R(m) = (p^\alpha)\} =$$

$$R/(p^{c_1}) \times \cdots \times R/(p^{c_t}).$$

הוכחת יחידות

$$R/(p_1^{a_1}) \times \cdots \times R/(p_r^{a_r}) \simeq R/(q_1^{b_1}) \times \cdots \times R/(q_s^{b_s})$$

שונו על הגבר-מוגדלים הכלל. בלי

הגבלת הכלליות, ניתן להניח

$$M \cong R/(p^{a_1}) \times \dots \times R/(p^{a_r}) \cong R/(p^{b_1}) \times \dots \times R/(p^{b_s})$$

עבור $p \in R$ אי-פריק בלי הגבלת הכלליות,

$1 \le a_1 \le a_2 \le \dots \le a_r$ $\quad (p^{a_1} | p^{a_2} | \dots | p^{a_r})$

$1 \le b_1 \le b_2 \le \dots \le b_s$

צריך להוכיח כי $s = r$ וכי לכל $r \ge i \ge 1$, $a_i = b_i$.

קודם כל, לפי אחד התרגילים למעלה,

$$Ann_R(M) = (p^{a_r}) = (p^{b_s})$$

לכן $a_r = b_s$. יהי $n = a_r = b_s$,

נעשה אינדוקציה על n.

$\overline{n=1}$

$$\underbrace{R/(p) \times \dots \times R/(p)}_{r\ \text{פעמים}} \cong \underbrace{R/(p) \times \dots \times R/(p)}_{s\ \text{פעמים}}$$

אז $s = r$ לפי הטענה 1.

$\underline{n \geq 1}$

אזי

$$pM = pR/(p^{a_1}) \times \cdots \times pR/(p^{a_r}) \simeq$$

$$R/(p^{a_1-1}) \times \cdots \times R/(p^{a_r-1})$$

אכן

$$pR/(p^a) \simeq R/(p^{a-1})$$

$$pr + (p^a) \longleftarrow\!\shortmid\; r + (p^{a-1})$$

לכן,

$$pM \simeq R/(p^{a_1-1}) \times \cdots \times R/(p^{a_r-1}) \simeq$$

$$R/(p^{b_1-1}) \times \cdots \times R/(p^{b_s-1})$$

ומסיימים באינדוקציה. לה-a_i-ים הגדולים
מ-1 מתאימים ב-b_i-ים הגדולים מאחד.

M/pM והטענה 1 $\Longleftarrow$ אותו מספר של 1-ים בין ה-a_i
ובין ה-b_i.

יישומים של המיון

0) $R=\mathbb{Z} \Leftarrow$ מיון של חבורות אבליות נוצרות סופית.

1) יהי F שדה. אז חוג הפולינומים $F[x]$ הינו תחום אוקלידי, לכן תחום ראשי.

לפני כמה שיעורים ראינו כי

$F[x]$-מודול $M \longleftrightarrow$ מרחב וקטורי V מעל F

עם אופרטור לינארי

$T: V \to V$

$T(v) = xv$

יהי M $F[x]$-מודול שאנחנו מניחים לגביו סוף-מימדי: $\dim_F V < \infty$.

זה אומר כי M נוצר סופית כ-F-מודול וכן נוצר כ-$F[x]$-מודול.

לפי משפט המיון (גירסה של גורמים אינווריאנטיים)

$$M \simeq F[x]^m \times F[x]/(d_1) \times \dots \times F[x]/(d_r)$$

כאשר $d_1 | d_2 | \dots | d_r \neq 0$.

נשים לב כי $m=0$. אכן $M=V$

$$\dim_F V = m \dim_F F[x] + \sum_{i=1}^{r} \dim_F F[x]/(d_i)$$

אבל $F[x]$ אינסוף-מימדי מעל F.
פולינומים $\Leftarrow$ צירופים לינאריים של F של
$1, x, x^2, x^3, \dots$.

לכן $m=0$, כי אחרת $\dim_F V = \infty$. לכן

$$M = F[x]/(d_1) \times \dots \times F[x]/(d_r)$$

$d_1, \dots, d_r$ מוגדרים עד כדי חברות.
אם נדרוש שיהיו פולי' מתוקנים, הם מוגדרים היטב.

יהי $d \in F[x]$

$$d = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0.$$

$$F[x]/(d) = \{f + (d) : f \in F[x],\ \deg f < n\}.$$

לכן $1+(d),\ x+(d),\ x^2+(d), \dots, x^{n-1}+(d)$

זה בסיס של $F[x]/(d)$ כמ"ו מעל F.

ביחס לבסיס הזה, הכפלה של x

תהיה כמו:

$$\underbrace{\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & \vdots & -a_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}}_{\text{המטריצה המלווה}} = C_d$$

$1 \to x$

$x \to x^2$

$\vdots$

$x^{n-1} \to x^n = -a_0 - a_1 x - \dots - a_{n-1}x^{n-1}$

המטריצה המלווה של $d \in F[x]$.

טענה תהי $A\in M_s(F)$ מטריצה. אזי

A דומה למטריצה מן הצורה

$$\begin{pmatrix} C_{d_1} & & & \\ & C_{d_2} & & \\ & & \ddots & \\ & & & C_{d_n} \end{pmatrix}$$

צורה קנונית רציונלית של A.

כאשר $d_1 | d_2 | d_3 \cdots | d_n$

פולינומים מתוקנים מעל F.

ו-d_i נקראים הגורמים האינווריאנטיים של A והם מוגדרים היטב.