הרצאה 18

R תחום ראשי, M מודול נוצר סופית מעל R.

אזי

$$(*) \quad M \simeq R/(d_1) \times R/(d_2) \times \dots \times R/(d_n)$$

כאשר $d_1 | d_2 | \dots | d_n$ איברים לא הפיכים

$$(\Leftrightarrow) \quad (d_1) \supseteq (d_2) \supseteq \dots \supseteq (d_n) \quad (**)$$

אידאלים אמיתיים של R) יתרה מזו,

האידאלים $(d_1),\dots,(d_n)$ המקיימים $(*)$ ו-$(**)$ מוגדרים באופן יחיד.

בפעם שעברה הוכחנו כי M כנ"ל אכן מכפלה ישרה של n מודולים ציקליים, כאשר n הינו מספר היוצרים המינימלי הנדרש בשביל לייצר את M. נשאר להוכיח $d_1 | d_2 | \dots | d_n$.

אינדוקציה על n

<u>n=1</u> M ציקלי. הוכחנו בשיעור הקודם כי $M \cong R/(d_1)$ והאידאל (d_1) יחיד, כי $(d_1) = Ann_R(M)$.

<u>n כללי</u> נניח שידוע שכל M מודול שנוצר (מינימלית) על ידי n-1 איברים, אזי

$$M \simeq R/(d_1) \times \dots \times R/(d_{n-1})$$

כאשר $d_1 | d_2 | \dots | d_{n-1}$.

יהי M מודול שנוצר על ידי n איברים

$m_1,\dots,m_n$ ויהי

$$(d_1) = Ann_R(m_1) = \{r\in R : rm_1 = 0_M\}$$

הוכחנו בפעם שעברה שאם

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

כאשר $c_i \in R$ ומתקיים $c_1 | d_1$, אזי

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

הנחנו כי ל-d_1 מספר מינימלי של גורמים אי-פריקים בין כל היוצרים בכל קבוצת יוצרים

כמו בשיעור הקודם, $M_1 = \langle m_1\rangle$

$$M_2 = \langle m_2,\dots,m_n\rangle$$

$$M_1 \simeq R/(d_1)$$

באינדוקציה,

$$M_2 \simeq R/(d_2) \times R/(d_3) \times \dots \times R/(d_n)$$

כך ש- $d_2 | d_3 | \dots | d_n$. נשאר להוכיח כי $d_1 | d_2$.

שהרי הוכחנו בפעם הקודמת כי $M \simeq M_1 \times M_2$.

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

נגדיר איברים $\left(d_2\tilde m_2 = (d_2+(d_2),\ 0+(d_3),\dots) = 0_M\right)$

$$\tilde m_2 = (1+(d_2),\ 0+(d_3),\dots,\ 0+(d_n))$$
$$\tilde m_3 = (0+(d_2),\ 1+(d_3),\dots,\ 0+(d_n))$$
$$\vdots$$
$$\tilde m_n = (0+(d_2),\ 0+(d_3),\dots,\ 1+(d_n))$$

(רואים שוב באינבריאנטים של M_2 גורם האינ' הנ"ל).

אני טוען כי $M_2 = \langle \tilde{m}_2, \ldots, \tilde{m}_n \rangle$. אכן,

יהי $m \in M_2 = R/_{(d_2)} \times \cdots \times R/_{(d_n)}$

אזי $r_i \in R$ $\quad m = (r_2 + (d_2), r_3 + (d_3), \ldots, r_n + (d_n))$

$= r_2 \tilde{m}_2 + r_3 \hat{m}_3 + \cdots + r_n \tilde{m}_n.$

אזי $\{m_1, \tilde{m}_2, \ldots, \tilde{m}_n\}$ עדיין יוצרים את M

והנתונים על d_1 עדיין מתקיימים, כי לא נגענו ב-m_1.

נשים לב כי $d_2 \tilde{m}_2 = 0_M$. לכן

$$d_1 m_1 = d_2 \tilde{m}_2 + 0\tilde{m}_3 + \cdots + 0\tilde{m}_n \ (=0_M)$$

לפי מה שהוכחנו בפרק הקודם מקבלים כי

$d_1 \mid g = \gcd(d_1, d_2)$ (המסומן בירוק)

אך $g \mid d_2$ ולכן $d_1 \mid d_2$.

נשאר להוכיח את היחידות של $((d_i))$

ה-d_i נקראים גורמים אינווריאנטיים של M.

טענה יהי R חוג (חילופי). נניח כי $R^m \simeq R^n$ כ-R-מודולים.

אזי $m=n$. $\left(R^n \simeq \underbrace{R\times R\times\cdots\times R}_{n \text{ פעמים}}\right)$

הגדרה יהי M מודול מעל חוג R. יהי (בלי הנחה חילופי) $I \triangleleft_\ell R$ אידיאל שמאלי! - אין צורך

$$IM = \left\{ a_1m_1+\dots+a_rm_r \;\middle|\; \begin{matrix} a_i\in I \\ m_i\in M \end{matrix} \right\} \subseteq M$$

ברור שזה תת-מודול.

הוכחה של הטענה

יהי $\varphi: R^n \xrightarrow{\sim} R^m$ איזומורפיזם.

אזי לכל אידיאל $I \triangleleft R$ מתקיים $\varphi(IR^n)=IR^m$.

לכן, מקבלים איזומורפיזם

$$R^n/IR^n \xrightarrow{\sim} R^m/IR^m$$

$$(r_1,\dots,r_n)+IR^n \longmapsto \varphi(r_1,\dots,r_n)+IR^m$$

יהי I אידיאל מקסימלי. במצב זה, $F=R/I$ הינו שדה. אני טוען כי

תת-טענה 1 יהי $I \triangleleft R$ אידיאל כלשהו.

$$IR^n = \{(a_1,\dots,a_n) : a_i\in I \ \forall i\}$$

הוכחה $\supseteq$)

$$(a_1,\dots,a_n) = a_1(1,0,\dots,0)+\dots+a_n(0,0,\dots,1) \in IR^n$$

$\subseteq$)

$$\underset{r_i\in R}{\overset{a\in I}{}} \; a(r_1,\dots,r_n) = (ar_1,\dots,ar_n) \in I^n$$

<u>תת-טענה 2</u> יהי I אידיאל מקסימלי

$$R^n / IR^n \simeq F^n$$

כאשר $F \simeq R/I$.

<u>תת-הוכחה</u> נגדיר הומומורפיזם

$$\varphi: R^n \longrightarrow F^n$$

$$\varphi(r_1, \ldots, r_n) = (r_1 + I, \ldots, r_n + I)$$

ברור כי φ על וכי $\ker \varphi = I^n = IR^n$.

עכשיו משפט האיזו' הראשון.

<u>הוכחה של הטענה</u> נניח $R^n \simeq R^m$.

יהי I אידיאל מקסימלי. יהי F השדה R/I.

אז $F^n \simeq R^n / IR^n \simeq R^m / IR^m \simeq F^m$

אך $F^n \simeq F^m \Leftarrow n=m$, כי המימד של מרחב וקטורי מוגדר באופן יחיד.

<u>דיון</u> יהי M מודול נוצר סופית מעל תחום ראשי R. ידוע לנו כי

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

כאשר $d_1 | \ldots | d_s$ לא הפיכים ולא אפסים.

__מסקנה__ נזכור כי

$$\mathrm{Tor}(M)=\left\{m\in M \;\middle|\; \begin{array}{l} \text{קיים } 0\neq a\in R \\ \text{כך ש- } am=0_M \end{array}\right\}$$

אזי

$$\mathrm{Tor}(M)\simeq R/(d_1)\times\cdots\times R/(d_s)$$

(d_s הורג כי איבר של $R/(d_1)\times\cdots\times R/(d_s)$)

__מסקנה 2__

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

__תוצאה__ בכל ביטוי

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

הטבעי r מוגדר באופן יחיד.

גירסה שקולה של משפט המיון:

(מחלקות אלמנטריות)

__משפט__ יהי M מודול נוצר סופית מעל תחום ראשי R. אזי

$$M\simeq R^r\times R/(p_1^{a_1})\times R/(p_2^{a_2})\times\cdots\times R/(p_s^{a_s})$$

כאשר p_i איברים אי-פריקים (לאו בהכרח שונים), $a_i\in\mathbb{N}$. האיברים $p_i^{a_i}$ מוגדרים באופן יחיד עד כדי חברות.

טענה שני הניסוחים של משפט המיון שקולים.

הוכחה יהי $d_i = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$

הפירוק של d_i (R תחום ראשי לכן גאוסי)

לפי משפט השאריות הסיני (כאשר q_i שונים)

$$R/(d_i) \simeq R/(q_1^{b_1}) \times \cdots \times R/(q_t^{b_t})$$

לפי הגירסה של גורמים אינווריאנטיים,

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

אז כל $R/(d_i)$ מפרקים כנ"ל.

בכיוון השני

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

$$\simeq \left(\mathbb{Z}/2\mathbb{Z}\right) \times \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\right) \times \left(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\right)$$

$$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

לפי הרעיון הזה, בהינתן ביטוי של M במחלקים אלמנטריים ניתן לקבל גורמים אינווריאנטיים.

אין עניין לא הוכחנו את היחידות.
והיום לא נוכיח אותה, נוכיח בפעם הבאה. בינתיים נניח את היחידות ונחקור מה אומר משפט המיון על $F[x]$-מודולים.

<u>תזכורת</u> F שדה, $F[x]$ - תחום ראשי.

הוכחנו שכדי להגדיר $F[x]$-מודול צריך להגדיר: 1) מרחב וקטורי V מעל F.
2) העתקה לינארית $T: V \to V$ שהיא הכפל הסקלרי ב-x.

$$x \cdot v = T(v)$$

$$(a_n x^n + \dots + a_0) \cdot v = a_n T^n(v) + \dots + a_1 T(v) + a_0 v.$$

יהי M מודול נוצר סופית מעל $F[x]$.
לפי משפט המיון (גירסה של גורמים אינווריאנטיים) נקבל

$$M \simeq F[x]^r \times F[x]/(d_1) \times \dots \times F[x]/(d_s)$$

כאשר d_i פולינומים לא קבועים
כך ש- $d_s | \dots | d_2 | d_1$. (לא הפיכים ולא אפסים)

נחקור את $F[x]/(g(x))$ כאשר $g(x)$ פולינום
לא קבוע. עד כדי חברות אפשר להניח כי
$g(x)$ מתוקן.

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

ה-$F[x]$-מודול הציקלי $F[x]/(g)$ הוא
גם F-מודול.

<u>טענה</u> הקבוצה $\{1+(g), x+(g), \dots, x^{n-1}+(g)\}$
הינה בסיס של $F[x]/(g)$ בתור F-מודול.

<u>הוכחה</u> <u>בת"ל</u> נניח כי
$$z_0(1+(g)) + z_1(x+(g)) + \dots + z_{n-1}(x^{n-1}+(g)) = 0$$
עבור $z_i \in F$.

$$(z_0 + z_1 x + \dots + z_{n-1}x^{n-1}) + (g) = (0)$$

כלומר $g \mid (z_0 + z_1 x + \dots + z_{n-1}x^{n-1})$

אך $\deg g = n > \deg(z_0 + \dots + z_{n-1}x^{n-1})$

לכן $z_i = 0$ לכל i.

פורש $F[x]$ תחום אוקלידי!

יהי $h(x)+(g) \in F[x]/(g)$. נחלק עם שארית:

$$h(x) = q(x)\cdot g(x) + r(x)$$

כאשר $\deg r < \deg g = n$. אז

$$h(x)+(g) = r(x)+(g)$$

אז $r(x) = c_0 + c_1 x + \dots + c_{n-1}x^{n-1}$, $c_i \in F$

כי $\deg r < n$, ולכן

$$h(x)+(g) = r(x)+(g) = c_0(1+(g)) + \dots + c_{n-1}(x^{n-1}+(g))$$

אזי נביט ההעתקה $T: F[x]/(g) \to F[x]/(g)$

$$T(f(x)+(g)) = x f(x) + (g)$$

ביחס לבסיס הנ"ל?

$$\begin{aligned} T:\ 1+(g) &\to x+(g) \\ x+(g) &\to x^2+(g) \\ &\vdots \\ x^{n-2}+(g) &\to x^{n-1}+(g) \\ x^{n-1}+(g) &\to x^n+(g) = (x^n - g) + (g) = \\ &-a_0(1+(g)) - \dots - a_{n-1}(x^{n-1}+(g)) \end{aligned}$$

כי $x^n - g = -a_0 - a_1 x - \dots - a_{n-1} x^{n-1}$.

אז המטריצה היא

$$\begin{pmatrix} 0 & 0 & & & 0 & -a_0 \\ 1 & 0 & & & & -a_1 \\ 0 & 1 & 0 & & & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & & 0 & 1 & -a_{n-1} \end{pmatrix}$$

המטריצה הזאת נקראת המטריצה המלווה של הפולינום $g(x) = x^n + a_{n-1} x^{n-1} + \dots + a_0$, נסמן אותה C_g.

<u>טענה</u> (צורה קנונית רציונלית של מטריצה)

תהי $A \in M_n(F)$ מטריצה $n \times n$. אזי A דומה למטריצה מן הצורה

$$\begin{pmatrix} C_{d_1} & & & 0 \\ & C_{d_2} & & \\ & & \ddots & \\ 0 & & & C_{d_s} \end{pmatrix}$$

כאשר C_{d_i} היא המטריצה המלווה של פולינום מתוקן d_i, וכאשר $d_1 | d_2 | \dots | d_s$, והפולינומים $d_1, \dots, d_s$ יחידים.

הוכחה יהי $V\simeq F^n$, תהי $T:V\to V$ ההעתקה המתאימה ל-A.

המידע הזה מגדיר לנו $F[x]$-מודול M. הוא נוצר סופית כי F-מודול, קל וחומר כי $F[x]$-מודול. לפי משפט המיון:

$$M\simeq F[x]^r\times F[x]/(d_1)\times\cdots\times F[x]/(d_s).$$

החוג $F[x]$ אינסוף-מימדי כמרחב וקטורי מעל F $\{1,x,x^2,x^3,x^4,\dots\}$.

V סוף-מימדי מעל F $\Leftarrow r=0 \Leftarrow$

$$M\simeq F[x]/(d_1)\times\cdots\times F[x]/(d_s)$$

המטריצה A מבטאת כפל פולי' ב-x עבור הבסיס הסטנדרטי של F^n.

ראינו למעלה שעבור בסיס מתאים

$$(1+(d_i),\dots,x^{\deg(d_i)-1}+(d_i))$$

של $F[x]/(d_i)$, כפל פולי' ב-x מתאים למטריצה

המלווה C_{d_i}: ניקח את הבסיס של V

הניתן על ידי שרשור של הבסיסים של

$F[x]/(d_i)$. אזי הכפל הסקלרי ב-x

הינו

$$\begin{pmatrix} C_{d_1} & & & \\ & C_{d_2} & & \\ & & \ddots & \\ & & & C_{d_s} \end{pmatrix} \text{ - rational canonical form}$$

<u>תרגיל</u> הפולינום האופייני של C_g

הינו $g(x)$.