R תחום ראשי לאורך כל ההרצאה

תזכורת:

R תחום ראשי. יהיו $c_1,\dots,c_n\in R$, $g=\gcd(c_1,\dots,c_n)$ אזי $(g)=(c_1,\dots,c_n)$

הוכחנו בסוף השיעור הקודם: R תחום ראשי, $c_1,\dots,c_n\in R$ $(n\geq 2)$ זרים כך ש $\gcd(c_1,\dots,c_n)$

אזי קיימת מטריצה $A\in M_n(R)$ כך ש:

1) $\det A=1$

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

תוצאה:

יהי M מודול מעל R. תהי $(m_1,\dots,m_n)$ קבוצת יוצרים של M. כלומר,

$M=Rm_1+\dots+Rm_n$

(בפרט M נוצר סופית). יהיו $c_1,\dots,c_n\in R$ כך ש $\gcd(c_1,\dots,c_n)=1$. אזי קיימת

קבוצת יוצרים אחרת של M, $(m_1',\dots,m_n')$ מאותו גודל n, וכך ש

$m_1'=c_1m_1+\dots+c_nm_n$

הערה: אפשר לחשוב על הטענה הקודמת כגרסה חלשה (מאוד) של למת ההחלפה של שטייניץ למליניאריות.

הלמה הזאת לא נכונה מעל חוגים. למשל: (תרגיל) שני בסיסים של $\mathbb{Z}^2$: $B_1=\{(5,3),(3,2)\}$

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

אבל אין שום בסיס מהצורה (b_1,b_2) כאשר $b_1\in B_1$, $b_2\in B_2$.

הוכחה: (של התוצאה)

לפי הטענה מהפעם הקודמת קיימת מטריצה $A\in M_n(R)$ כך ש $\det(A)=1$ וגם העמודה

הראשונה שלה היא $\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$. כלומר, $a_{i1}=c_i$ לכל $n\geq i\geq 1$. נגדיר

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

יהי $M'=Rm_1'+\dots+Rm_n'$ 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 היא איבר הפיך של החוג $M_n(R)$. לכן קיימת מטריצה $B\in M_n(R)$ כך ש
$BA=I_n$. בודקים כי $m_j=b_{1j}m_1'+\dots+b_{nj}m_n'\in M'$

משפט (מיון של מודולים נוצרים סופית מעל תחום ראשי):

יהי R תחום ראשי, יהי M R-מודול נוצר סופית. אזי $M\simeq R^r\times R/(d_1)\times\dots\times R/(d_s)$
כאשר $r,s\geq 0$ ולכל $1\leq i\leq s$, האיבר $0\neq d_i\in R$ איבר לא הפיך וגם $d_1|d_2, d_2|d_3,\dots,d_{s-1}|d_s$
המספר r והאידיאלים $(d_1),\dots,(d_s)$ יחידים (כלומר, d_i מוגדרים היטב עד כדי חברות)

הערה: נשים לב כי $R\simeq R/(0)$. לכן ניתן לנסח את המשפט כך: יהי M מודול נוצר סופית
מעל תחום ראשי R. אזי $M\simeq R/(d_1)\times\dots\times R/(d_n)$ כאשר $d_i\in R$ איברים לא הפיכים
וגם $d_1|d_2,\dots,d_{n-1}|d_n$ (תזכורת: $r|0$ לכל $r\in R$ כי $r\cdot 0=0$) גם כאן ה-d_i-ים
יחידים ($n=r+s$ מהניסוח הקודם) * ה-n הוא גודל מינימלי של קבוצה יוצרת של M

הגדרה: האיברים $d_1,\dots,d_n$ (עד כדי חברות) נקראים הגורמים האינווריאנטים של M

תזכורת: יהי $m\in M$, המאפס $Ann_R(m)=\{r\in R: rm=0\}\trianglelefteq R$ אידאל (ויתכן שלא אמיתי)

הוכחה של הקיום:

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

1) n מינימלי

2) יהי $(d_1)=Ann_R(m_1)$. אזי מספר הגורמים הא"י פריקים של d_1 מינימלי בין כל הקבוצות היוצרים מגודל n

(R הוא תחום ראשי, לכן תפ"י. אם $d_1\neq 0$, אזי $d_1=p_1\cdot\ldots\cdot p_t$ מתפרק לא"י פריקים.
t הוא מספר הגורמים. אם $d_1=0$, אומרים שיש לו ∞ גורמים אי פריקים)

נוכיח את המשפט באינדוקציה על n.

$n=1$: אזי $M=Rm_1$ והוכחנו בשיעור הקודם כי $M\simeq R/Ann_R(m_1)\simeq R/(d_1)$ כ-R-מודולים.

$n>1$: יהי $M_1=Rm_1$, $M_2=Rm_2\times\dots\times Rm_n$

תת-טענה: $M \simeq M_1 \times M_2$

הוכחה: לפי טענה מהרצאה הקודמת, צריך להוכיח כי 1) $M=M_1+M_2$, 2) $M_1\cap M_2=(0)$

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

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

2) יהי $c_1m_1=c_2m_2+\dots+c_nm_n$ איבר של החיתוך, כאשר $c_1,\dots,c_n\in R$

יהי $h=gcd(c_1,d_1)$. $d_1m_1=0 \Leftarrow (d_1)=Ann_R(m_1)$. אז קיימים $x,y\in R$ כך ש

$h=c_1x+d_1y$. לכן $hm_1 = xc_1m_1+yd_1m_1 = xc_1m_1$

לכן, $hm_1 = xc_1m_1 = \underbrace{xc_2}_{c_2 \text{ חדש}}m_2+\dots+xc_nm_n$. וניתן להניח בלי הגבלת הכלליות

כי $c_1|d_1$. אז יש לנו $c_1m_1=c_2m_2+\dots+c_nm_n$ כאשר $c_1|d_1$.

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

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

כך ש $m_1' = -c_1'm_1+c_2'm_2\dots+c_n'm_n$. יהי $(d_1')=Ann_R(m_1')$, נשים לב כי

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

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

לפי המינימליות של מספר הגורמים הא"פ 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. $c_1\in(d_1)=Ann_R(m_1)$ ולכן

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

כלומר, $M_1\cap M_2=(0)$

בחזרה להוכחת הקיום של הפירוק של M. M_2 נוצר ע"י $n-1$ יוצרים

אז מהנחת האינדוקציה $M_2\simeq R/(d_2)\times\dots\times R/(d_n)$ כאשר $d_2|d_3,\dots,d_{n-1}|d_n$

($n-1$ הוא הגודל המינימלי של קבוצה של יוצרים של M_2. אם הייתה קבוצת יוצרים קטנה יותר, היינו

יכולים לצרף אליה את m_1 ולקבל קבוצת יוצרים של M, בסתירה למינימליות של n.)

קיבלנו כי $M \simeq M_1 \times M_2 = R/(d_1) \times \dots \times R/(d_n)$. 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 $m' = c_2 m_2 + \dots + c_n m_n$ כאשר $c_2, \dots, c_n \in R$

נשים לב כי $r \in (d_2) \iff (0+(d_2), \dots, 0+(d_n)) = (r+(d_2), \dots, 0+(d_n)) \iff r \in Ann_R(m')$

לכן $Ann_R(m') = (d_2)$. בנוסף, $\gcd(c_2, \dots, c_n) = 1$, כי אם היה מחלק משותף h לא הפיך, היה קיים $m'' \in M_2$ כך ש $m' = hm''$. בפרט יש

$m'' \leftrightarrow (r_2+(d_2), \dots, r_n+(d_n)) \in R/(d_2) \times \dots \times R/(d_n)$

כך ש:

$(hr_2+(d_2), \dots, hr_n+(d_n)) = m' = (1+(d_2), 0+(d_3), \dots) \rightarrow$ נחזור לפה בהמשך

בפרט, $\underbrace{d_1}_{c_1} m_1 = d_2 m' = \underbrace{d_2 c_2}_{c_2} m_2 + \dots + d_2 c_n m_n$ הוכחנו כבר כי d_1 הוא 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 $d_1 | \gcd(d_2c_2, \dots, d_2c_n)$