אלגברה מופשטת 2 – תרגיל כיתה 11

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

הגדרה

יהי M מודול מעל R. עבור $a \in M$, $Ra = \{r \cdot a : r \in R\}$ הוא המודול הציקלי הנוצר ע"י a וזהו תת מודול של M.

דוגמא

R^n הוא מודול ציקלי מעל החוג $M_n(R)$, כי $M_n(R)e_{11} \cong R^n$.

הגדרה

אם קיימת תת קבוצה $\{a_j\}_{j \in I} \subseteq M$ כך שלכל $m \in M$ קיימים $r_1, \dots, r_n \in R$ כך ש $m = \sum_{i=1}^{n} r_i a_i$, אז נאמר ש M נפרש ע"י $\{a_j\}_{j \in I}$, ואם $\sum_{i=1}^{n} r_i a_i = 0 \leftarrow r_1 = r_2 = \dots = r_n = 0$ אז $\{a_j\}_{j \in I}$ נקרא בסיס ו M נקרא מודול חופשי.

דוגמאות

1. יהי R חוג, נסתכל על R כמודול מעל עצמו אז R הוא ציקלי, כי לכל $m \in R$ מתקיים $m = m \cdot 1$ ולכן $\{1\}$ יוצר את R.
2. R^n הוא חופשי – נוצר ע"י $\{e_i\}_{i=1}^{n}$.
3. ל $\mathbb{Z}_n$ כמודול מעל $\mathbb{Z}$ אין בסיס. אם הייה אז מהדרישה $r \cdot x = 0$ $(r \in \mathbb{Z}, x \in \mathbb{Z}_n)$ היה צריך לנבוע ש $r = 0$ אבל ניתן לקחת את $r = n$, מצד שני $\{1\}$ הוא כן קבוצה יוצרת ל $\mathbb{Z}_n$.

טענה

כל מודול נוצר סופית הוא תמונה הומומורפית של מודול חופשי.

הוכחה

נניח ש M נוצר ע"י $\{a_1,...,a_n\}$. נסתכל על R^n הנוצר ע"י $\{e_i\}$ ונגדיר הומומורפיזים

$e_i \to a_i$ אז $\sum_{i=1}^{n} r_i e_i \to \sum_{i=1}^{n} r_i a_i$ ו $M \cong R^n/\ker f$.

הגדרה

1. יהי M מודול מעל R, ויהי $x \in M$. נגדיר $Ann(x)=\{r \in R : r \cdot x = 0\}$.
   נשים לב ש $Ann(x) \triangleleft R$.
2. הפיתול של M מוגדר להיות
   $Tor_R(M)=Tor(M)=\{m \in M : \exists (0 \neq r) \in R : r \cdot m = 0\}$.
3. אם $Tor(M)=M$ נאמר ש M מפותל.

דוגמאות

1. יהי $R=\mathbb{Z}, M=\mathbb{Z}_6$ $Tor_{\mathbb{Z}}(\mathbb{Z}_6)=\{x \in \mathbb{Z}_6 : \exists (0 \neq z) \in \mathbb{Z} : z \cdot x = 0_{\mathbb{Z}_6}\}=\mathbb{Z}_6$. וזאת מכיוון שלכל $x \in \mathbb{Z}_6$ ניתן לקחת $z=6$.
2. יהי R תחום שלמות ונסתכל על R כמודול מעל עצמו, אז $Tor(R)=\{0\}$, כי אין מחלקי אפס. באותו אופן R^n (R תחום שלמות) כמודול מעל R חסר פיתול.
3. $R=M=\mathbb{Z}_6$ $Tor_{\mathbb{Z}_6}(\mathbb{Z}_6)=\{0,2,3,4\}, Ann(3)=\{0,2,4\}$.
4. אם R תחום שלמות, אז $R/\langle a \rangle$ הוא מודול מפותל מעל R. כי אם $r+\langle a \rangle \in R/\langle a \rangle$, אז $a \cdot r + \langle a \rangle \in \langle a \rangle = 0_{R/\langle a \rangle}$.
5. תהיי $(G,+)$ חבורה אבלית סופית, אז G בתור מודול מעל $\mathbb{Z}$ מפותלת. לכל $a \in G$ נקבל ש $|G| \cdot a = 0$.

טענה

יהי R תחום שלמות. $Tor(M)$ הוא תת מודל של M.

הוכחה

יהי $x \in Tor(M)$, צ"ל ש $r \cdot x \in Tor(M)$ לכל $r \in R$. מכיוון ש $x \in Tor(M)$ אז קיים $s \in R$ כך ש $sx=0$, ולכן $s \cdot (rx) = r \cdot (sx) = 0$ ז"א $rx \in Tor(M)$.

אם $x,y\in Tor(M)$ אז קיימים $s,s'\in R$ כך ש $sx=s'y=0$ ולכן

$ss'(x-y)=s'(sx)-s(s'y)=0 \rightarrow x-y\in Tor(M)$.

<u>טענה</u>

$M/Tor(M)$ הוא חסר פיתול כמודל מעל R.

<u>הוכחה</u>

$M/Tor(M)=\{m+Tor(M):m\in M\}$. נניח בשלילה שעבור $m\notin Tor(M)$ קיים $0\neq r\in R$

כך ש $r(m+Tor(M))=rm+Tor(M)=0_{M/Tor(M)}=Tor(M)$ ז"א $rm\in Tor(M)$ ולכן קיים

$0\neq s\in R$ כך ש $s(rm)=0\rightarrow (sr)m=0\rightarrow m\in Tor(M)$ וקיבלנו סתירה.

<u>הערה</u>

כל מודול M מעל תחום שלמות R ניתן לפרק ל $M=Tor(M)\oplus M'$ כש $M'\cong M/Tor(M)$.

<u>דוגמא</u>

יהי $M=\mathbb{Z}^2\times\mathbb{Z}_4$ מודול מעל $\mathbb{Z}$ אז $Tor(M)=\mathbb{Z}_4$ $M/Tor(M)=\mathbb{Z}^2$.

<u>הגדרה</u>

המאפס של M הוא $Ann(M)=\{r\in R:r\cdot M=0\}$. אם $Ann(M)=\{0\}$ אז M נקרא נאמן.

תרגיל בית: להראות ש $Ann(M)\lhd R$.

<u>הערה</u>

כל מודול חסר פיתול הוא נאמן.

<u>תרגיל בית</u>

הוכיחו שלכל $\frac{m}{n}+\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}$ קיים $a\in\mathbb{Z}$ כך ש $a\cdot\left(\frac{m}{n}+\mathbb{Z}\right)\in 0_{\mathbb{Q}/\mathbb{Z}}$ (ז"א $Tor\left(\mathbb{Q}/\mathbb{Z}\right)=\mathbb{Q}/\mathbb{Z}$)

אבל לכל $a\in\mathbb{Z}$ ניתן למצוא איבר $x\in\mathbb{Q}/\mathbb{Z}$ כך ש $a\cdot x\neq 0_{\mathbb{Q}/\mathbb{Z}}=\mathbb{Z}$ (ז"א $Ann\left(\mathbb{Q}/\mathbb{Z}\right)=\{0\}$)

<u>דוגמאות</u>

1. אם $M=\mathbb{Z}_n$, $R=\mathbb{Z}$, $Ann(\mathbb{Z}_n)=n\mathbb{Z}$.

2. קיימים מודולים נאמנים ומפותלים. $R=\mathbb{Z}, M={}^{\mathbb{Q}}\!\big/_{\mathbb{Z}}$.

תרגיל

M הוא מודול מעל ${}^{R}\!\big/_{Ann(M)}$.

פתרון

יהי $r+Ann(M)\in {}^{R}\!\big/_{Ann(M)}$.

נוכיח שלכל $m\in M$ הפעולה $(r+Ann(M))\cdot m=rm$ מוגדרת היטב ואת שאר הדרישות למודול נשאיר לתרגיל בית. נניח ש $r_1+Ann(M)=r_2+Ann(M)$ ז"א $r_1-r_2\in Ann(M)$ ולכן קיים $r_0\in Ann(M)$ כך ש $r_1=r_2+r_0$. אזי

$$r_1m=(r_1+Ann(M))m=(r_2+r_0+Ann(M))m=(r_2+r_0)m=r_2m.$$

לכן, אם $I\subseteq Ann(M)$, $I\triangleleft R$, אז M הוא מודול מעל ${}^{R}\!\big/_{I}$.

דוגמא

יהי $V=\mathbb{R}^3$, $A=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$, ונסתכל על V כמודול מעל $\mathbb{R}[x]$ המושרה מ A. אז הפולינום האופייני של A הוא $f(t)=|tI-A|=\begin{vmatrix}t&-1&0\\-1&t&0\\0&0&t-1\end{vmatrix}=(t-1)(t^2-1)$ על פי משפט קיילי המילטון, $f(A)=0$ ולכן לכל $u\in V$ $f(x)\cdot u=f(A)\cdot u=0 \leftarrow \langle f\rangle\subset Ann(V)$ ולכן V הוא מודול מעל ${}^{\mathbb{R}[x]}\!\big/_{(t-1)(t^2-1)}$.

תזכורת

יהיו U,V מרחבים וקטורים ממימד n מעל שדה F ונניח ש $V\subseteq U$ אז $V=U$.

דוגמא

נתבונן ב $\mathbb{Z}$ וב $2\mathbb{Z}$ כמודולים מעל $\mathbb{Z}$. אז $\{1\}$ מהווה בסיס ל $\mathbb{Z}$ כמודול מעל עצמו ו $\{2\}$ מהווה בסיס ל $2\mathbb{Z}$ כמודול מעל $\mathbb{Z}$ ולכן המימדים של $\mathbb{Z}$ ושל $2\mathbb{Z}$ שווים, $2\mathbb{Z}\subset\mathbb{Z}$ לא שווים.

יהי R מעתה חוג ראשי.

משפט

1. תת מודול של R^n הוא חופשי מדרגה $\le n$.
2. כל תת מודול של R^n הוא מהצורה $A\cdot R^n$ עבור $A\in M_n(R)$. לכן לכל תת מודול של R^n ניתן למצוא את הבסיס שלו על ידי דירוג המטריצה A (ע"י צמצום שורות).

דוגמא

מצאו בסיס לתת מודול של $\mathbb{Z}^3$ (כמודול מעל $\mathbb{Z}$), הנפרש ע"י $\{(1,0,-1),(2,-3,1),(4,-3,-1)\}$ ניתן לעשות זאת ע"י צמצום השורות של המטריצה (והכפלה בהופכיים של R).

$$\begin{pmatrix}1&0&-1\\2&-3&1\\4&-3&-1\end{pmatrix}\xrightarrow{\substack{R_2-2R_1\to R_2\\R_3-4R_1\to R_3}}\begin{pmatrix}1&0&-1\\0&-3&3\\0&-3&3\end{pmatrix}\xrightarrow{R_3-R_2\to R_3}\begin{pmatrix}1&0&-1\\0&-3&3\\0&0&0\end{pmatrix}$$

ולכן התת מודול נפרש ע"י $(1,0,-1),(0,-3,3)$ ז"א איבריו הם:

$$\{a\cdot(0,-3,3)+b\cdot(1,0,-1):a,b\in\mathbb{Z}\}=\{(b,-3a,3a-b):a,b\in\mathbb{Z}\}\subset\mathbb{Z}^3$$

שימו לב שאסור לחלק את $(0,-3,3)$ ב 3 מכיוון ש 3 לא הפיך ב $\mathbb{Z}$.

דוגמאות

1. נמצא קבוצה פורשת לתת מודול הבא של $\mathbb{Z}^3$ (כמודול מעל $\mathbb{Z}$)

$M=\{(x,y,z):x+2y+3z=0,x+4y+9z=0\}$.

נסמן $A=\begin{pmatrix}1&2&3\\1&4&9\end{pmatrix}$ ונדרג את A:

$\begin{pmatrix}1&2&3\\1&4&9\end{pmatrix}\xrightarrow{R_2-R_1\to R_2}\begin{pmatrix}1&2&3\\0&2&6\end{pmatrix}\xrightarrow{R_1-R_2\to R_1}\begin{pmatrix}1&0&-3\\0&2&6\end{pmatrix}$ מכיוון ש $\mathbb{Z}$ תחום שלמות יש

לפתור את $0=\begin{pmatrix}1&0&-3\\0&1&3\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}$ $\leftarrow$ $\begin{matrix}x=3z\\y=-3z\end{matrix}$ $\leftarrow$ $(x,y,z)=(3z,-3z,z)=z\cdot(3,-3,1)$

ז"א M נפרש ע"י $(3,-3,1)$.

2.באותו אופן, אם $M=\{(x,y)\in\mathbb{Z}^2 : 2x+3y=0\}$ הוא תת מודול של $\mathbb{Z}^2$ אז הוא נפרש ע"י $(3,-2)$. זאת מכיוון שעבור $a\cdot(3,-2)=(3a,-2a)$ מתקיים $2\cdot 3a+3\cdot(-2a)=0$ ומהבסיס $(3,-2)$ אי אפשר להוציא גורם משותף.

<u>משפט</u>

כל מודול M נוצר סופית מעל R הוא מהצורה $M_A = {R^n}/{A\cdot R^n}$.

הסבר: ניתן להגדיר $f:R^n\to M$ ואז $Kerf=A\cdot R^n$, כש $A=(a_{ij})$ ו $\sum a_{ij}e_i$ פורשת את $Kerf$.

<u>דוגמא</u>

נניח ש $A=\begin{pmatrix} m & & & \\ & \cdot & & \\ & & \cdot & \\ & & & m\end{pmatrix}$, $m\in\mathbb{Z}$. למה איזומורפי $M_A={\mathbb{Z}^n}/{A\mathbb{Z}^n}$?

נשים לב:

$$M_A=\{(a_1,...,a_n)+m\cdot\alpha : \alpha\in\mathbb{Z}^n, a_i\in\mathbb{Z}\}=\{(a_1,...,a_n)(\operatorname{mod} m) : a_i\in\mathbb{Z}\}\cong\mathbb{Z}_m\times...\times\mathbb{Z}_m$$

<u>הגדרה</u>

$A,B\in M_n(R)$ $A\sim B$ אם קיימים $P,Q\in GL_n(R)$ כך ש $B=PAQ$.

<u>טענה</u>

$$A\sim B\leftrightarrow M_A\cong M_B$$

ע"י כפל במטריצות הפיכות ניתן להביא כל מטריצה (מעל תחום ראשי R) למטריצה אלכסונית $\begin{pmatrix} d_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & d_n\end{pmatrix}$, כש $d_1|d_2....|d_n$. צורה זו נקראת סדורה קנונית ו d_i נקראים הגורמים האינווריאנטים לכן, אם $A\sim diag(d_1,...,d_n)$ אז $M_A\cong\oplus {R}/{d_iR}$.

כפל במטריצות הפיכות מתאים לפעולות הבאות:

1. הוספת כפולה של עמודה/שורה לעמודה/שורה אחרת.
2. החלפת שורות/עמודות.
3. כפל בהופכי.

<u>דוגמא</u>

מהו הסדר של $G=\left\langle (a,b,c) \middle| \begin{matrix} 2a+4b+3c=0 \\ a+2b+3c=0 \\ a+4b+9c=0 \end{matrix} \right\rangle$?

G נוצר ע"י שלוש יוצרים e_1,e_2,e_3 כמודול מעל $\mathbb{Z}$, ולכן ניתן להתייחס ל G כמודול

$\mathbb{Z}^3 / A\mathbb{Z}^3$ כש $A=\begin{pmatrix} 2 & 4 & 3 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix}$ נעביר את A לצורה אלכסונית.

$$A=\begin{pmatrix} 2 & 4 & 3 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \\ 2 & 4 & 3 \end{pmatrix} \xrightarrow[R_3-2R_1\to R_3]{R_2-R_1\to R_2} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 6 \\ 0 & 0 & -3 \end{pmatrix} \xrightarrow[C_3-3C_2\to C_3]{C_2-2C_1\to C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 6 \\ 0 & 0 & -3 \end{pmatrix} \xrightarrow{C_3-3C_2\to C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{pmatrix}$$

ולכן $G\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \leftarrow |G|=6$.

שימו לב שזו אינה הצורה הקנונית. הצורה הקנונית היא $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{pmatrix}$.

<u>הערה</u>

1. אם ל M יש בסיס $\{v_1,...,v_n\}$ אז $M\cong Rv_1\oplus...\oplus Rv_n$.

   ההפך לא בהכרח נכון, אם M איזומורפי לסכום ישר אין זה אומר שיש לו בסיס.

   למשל: $M=\mathbb{Z}_2\oplus\mathbb{Z}_2$ כמודול מעל $\mathbb{Z}$. ל M אין בסיס כי אחרת עבור (a,b) (איבר

   בבסיס) נקבל $2\cdot(a,b)=(0,0) \leftarrow 2=0_{\mathbb{Z}}$ סתירה.

2. לא כל תת מודול של מודול חופשי הוא גם חופשי.

   נתייחס ל $R=\mathbb{Z}\times\mathbb{Z}$ כמודול מעל עצמו אז $\mathbb{Z}\times\{0\}$ הוא תת מודול של R אבל הוא לא

   חופשי מעל R.