מודולים

הגדרות

- M חופשי = יש לו בסיס
- M נוצר סופית = נפרש על ידי קבוצה סופית
- "חופשי" + "נוצר סופית" $\Leftarrow$ יש בסיס סופי $\Leftrightarrow$ $M \cong R^n$

הערה

לכל מודול חופשי נוצר סופית יש בסיס סופי.

הוכחה

תהי $x_1, \dots x_n$ קבוצה פורשת(אולי אינה ב"ת). יהי $B = \{b_i\}$ בסיס של המודול(אולי אינסופי).

נציג כל x_i כצירוף לינארי של איברים מהבסיס B, ונסמן בB' את האיברים של B המשתתפים בהצגות האלו.

M נפרש ע"י B', ומכיוון ש$B' \subseteq B$, B' ב"ת. לכן B' בסיס סופי של M.

הערה

מודול M הוא מנה של איזשהו R^n $\Leftrightarrow$ M נוצר סופית.

הוכחה

$\Leftarrow$ נניח $M = {}^{R^n}/_{P}$. $\{e_i + P\}$ פורשת את M.

$\Rightarrow$ נניח שM נפרש על ידי $x_1, \dots x_n$. נגדיר הומומורפיזם $M \to R^n$ לפי $e_i \mapsto x_i$. ברור שזה על.

דוגמה

כל חבורה אבלית נוצרת סופית היא מנה של $\mathbb{Z}^n$.

לדוגמה:

$$\varphi : \mathbb{Z}^2 \to {}^{\mathbb{Z}}/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}/_{4\mathbb{Z}}$$

נוצרת על ידי

$$\begin{array}{ccc} e_1 & \mapsto & (1,0) \\ e_2 & \mapsto & (0,1) \\ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} & \mapsto & (a_1, a_2) \end{array}$$

הגרעין של φ כולל את $\begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \end{pmatrix}$. קל להוכיח ש

$$\ker \varphi = \mathbb{Z} \begin{pmatrix} 3 \\ 0 \end{pmatrix} + \mathbb{Z} \begin{pmatrix} 0 \\ 4 \end{pmatrix}$$

לסיכום,

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}^2 / \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} \mathbb{Z}^2$$

$$\begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 3a \\ 4b \end{pmatrix}$$

משפט

יהי R תחום ראשי.
אז כל תת־מודול של R^n הוא מודול חופשי מדרגה$\leq n$.

הערה

כל תת מודול של R(=אידאל(שמאלי)) הוא מודול חופשי מדרגה≤ 1(=נוצר על ידי איבר אחד)

הוכחה

נסמן תת־מודול $N \leq R^n$. נסמן $M = R^n$.
נגדיר:

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$$

לפי

$$M_k = Re_1 + \cdots + Re_k$$

נסמן $N_k = N \cap M_k$. לכן

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq N_n = N$$

מכיוון שR ראשי, הטענה מתקיימת ל$n = 1$. לכן N_1 הוא מודול חופשי מדרגה≤ 1.
נמשיך באינדוקציה. נניח שלN_k יש בסיס בגודל$\leq k$(נבנה בסיס לN_{k+1})

דוגמה:

$$N=\left\{\begin{pmatrix}a\\b\end{pmatrix}\middle|a+b\equiv 0 \pmod 2\right\}\subseteq\mathbb{Z}^z=M_2$$

$$0\subset M_1=\begin{pmatrix}*\\0\end{pmatrix}\subset M_2=\begin{pmatrix}*\\ *\end{pmatrix}$$

$$0\subset\underbrace{\left\{\begin{pmatrix}2c\\0\end{pmatrix}\middle|c\in\mathbb{Z}\right\}}_{=\mathbb{Z}\cdot\begin{pmatrix}2\\0\end{pmatrix}}\subset N$$

נסמן

$$I=\{c\in R|ce_{k+1}\in N+M_k\subseteq R\}$$

נוכיח ש$I\lhd R$:

- סגור לחיבור ־ נניח ש$c,c'\in I$. אז

$$ce_{k+1},c'e_{k+1}\in N+M_k$$

$$\Downarrow$$

$$(c\pm c')\,e_{k+1}\in N+M_k$$

- סגור לכפל בסקלר ־ אם $c\in I$ ו$a\in R$ אז

$$ce_{k+1}\in N+M_k$$

$$\Downarrow$$

$$(ac)\,e_{k+1}\in N+M_k$$

$$\Downarrow$$

$$ac\in I$$

מכיוון ש-R ראשי, $I = Rc_0$. אם $c_0 = 0$ אז $N_{k+1} = N_k$, אחרת $c_0 \neq 0$ ומכיוון ש-$c_0 \in I$ קיימים $v \in N, y \in M_k$ כך ש-$c_0 e_{k+1} = v - y$.

נוכיח שהוספת הווקטור $\overbrace{e_{k+1}}^{=v} + y$ לבסיס של N_k שכבר בנינו נותנת בסיס ל-N_{k+1}. הקבוצה אכן ב"ת כי אם יש צירוף לינארי שמתאפס המקדם של e_{k+1} בצירוף שווה למקדם של v ולכן הוא אפס. מה שנותר הוא צ"ל של איברי הבסיס הישן, הקבוצה הפורשת את N_{k+1} כי לכל $w \in N_{k+1}$ הרכיב c של e_{k+1} שייך לפי ההגדרה ל-I ולכן הוא כפולה של c_0, לכן

$$w - \frac{c}{c_0} \cdot v \in N_k$$

מסקנה

יהי R תחום ראשי.

כל מודול נוצר סופית מעל R איזומורפי למודול מהצורה $M_A = {}^{R^n}\!/_{AR^n}$ כאשר $A \in M_n(R)$.

הוכחה

יהי M מודול נוצר סופית, עם קבוצה פורשת בגודל n.

אז יש אפימורפיזם $\varphi : R^n \to M^{\sum Rw_i}$, $\varphi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum x_i w_i$.

נסמן $K = \ker \varphi$. ברור ש-$M \cong {}^{R^n}\!/_K$ ו-$K \leq R^n$. לפי המשפט קיימים $v_1, \dots v_n \in R^n$ הפורשים את K. נסמן:

$$A = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}$$

לכל $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in R^n$

$$Ax = \begin{pmatrix} & | & \\ - & v_i & - \\ & | & \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum x_i v_i$$

$\Leftarrow$

$$K = \left\{ \sum x_i v_i \middle| x_i \in R \right\} = \{Ax | x \in R^n\} = A \cdot R^n$$

$\Leftarrow$

$$M \cong {}^{R^n}\!/_{AR^n} = M_A$$

הערה

A נקראת מטריצת היחסים של M.

אלגוריתם לחישוב מטריצת היחסים של מודול M נוצר סופית

1. נבחר קבוצה פורשת $x_1,\dots x_n$ של M.
2. נגדיר $\varphi : R^n \to M$ לפי $\varphi\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix} = \sum \alpha_i x_i$.

לker φ יש קבוצה פורשת $\left\{\sum\limits_{i=1}^{n} a_{ij}e_i\right\}_{i=1,\dots n}$. $A=(a_{ij})$ היא מטריצת היחסים.

דוגמה

נתאר את $\mathbb{Z}/2\mathbb{Z}$ כמודול מעל $\mathbb{Z}$.

$\mathbb{Z}/2\mathbb{Z}$ נפרש ע"י $2\mathbb{Z}$ ו$2\mathbb{Z}+1$. לכן יש אפימורפיזם $\mathbb{Z}^2 \to \mathbb{Z}/2\mathbb{Z}$ ע"י

$$\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} \mapsto \alpha_1+\alpha_2 \pmod 2$$

$$\ker(\varphi) = \left\{ \begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} \middle| \alpha_1+\alpha_2 = 0 \pmod 2 \right\} \le \mathbb{Z}^2 =$$

$$= \mathbb{Z}\begin{pmatrix}2\\ 0\end{pmatrix} + \mathbb{Z}\begin{pmatrix}1\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}\mathbb{Z}^2$$

$$\mathbb{Z}/2\mathbb{Z} \cong M_{\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}} = \mathbb{Z}^2/\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}\mathbb{Z}^2$$