מודולים מעל תחום ראשי - הסיפור הכמעט מלא

נניח ש-R הוא תחום ראשי, ו-M הוא מודול נוצר סופית מעל R. ניקח קבוצת יוצרים $x_1, \dots, x_n$ של M. מפה אפשר להגדיר הומומורפיזם של מודולים $\varphi \colon R^n \to M$ לפי $\varphi(e_i) = x_i$, שהוא למעשה אפימורפיזם. ממשפט האיזומורפיזם הראשון,

$$M \cong {}^{R^n}\!/_{\ker\varphi}.$$

הגרעין $\ker\varphi$ הוא תת-מודול של R^n.

משפט 1. אם R הוא תחום ראשי, כל תת-מודול של R^n הוא חופשי עם בסיס המכיל לכל היותר n איברים.

הוכחה. נוכיח את הטענה באינדוקציה על n. אם $n = 0$, $R^n = 0$, והטענה ברורה. נניח שהטענה נכונה לאיזשהו $n \geq 0$, ויהי $N \leq R^{n+1}$ איזשהו תת-מודול. אפשר לחשוב על $R^{n+1} = R^n \times R$, ותהי $\pi : R^{n+1} \to R^n$ ההטלה על n הקואורדינטות הראשונות. אז $\pi(N)$ הוא תת-מודול של R^n, ומהנחת האינדוקציה הוא חופשי ויש לו בסיס $y_1, \dots, y_m \in \pi(N)$ עבור $m \leq n$. π הוא אפימורפיזם, לכן אפשר לכתוב $y_i = \pi(x_i)$ לכל $1 \leq i \leq m$.

מצד שני, $\ker(\pi|_N)$ הוא תת-מודול של N, וכן $\ker(\pi|_N) = N \cap (\{0\}^n \times R)$ (זהו החיתוך בין N לתת-המודול של R^{n+1} שכל n הקואורדינטות הראשונות שלו הן 0). אבל אז אפשר לחשוב עליו כעל תת-מודול של R ממש (לפי הקואורדינטה האחרונה), וכל תת-מודול של R נוצר על ידי איבר אחד וגם חופשי (כי הוא איזומורפי ל-R כמודול מעל R). נניח ש-x_0 יוצר על $\ker(\pi|_N)$.

נראה ש-$x_0, x_1, \dots, x_m$ בסיס של N. ההכלה $\sum_{i=0}^m Rx_i \subseteq N$ ברורה. לכיוון ההפוך, יהי $a \in N$. אפשר לכתוב

$$\pi(a) = \sum_{i=1}^m r_i y_i = \sum_{i=1}^m r_i \pi(x_i) = \pi\left(\sum_{i=1}^m r_i x_i\right),$$

לכן $a - \sum_{i=1}^m r_i x_i \in \ker(\pi|_N)$. אבל אז אפשר לכתוב $a - \sum_{i=1}^m r_i x_i = r_0 x_0$ לאיזשהו $r_0 \in R$, ונקבל הצגה של a כצירוף לינארי של $x_0, x_1, \dots, x_m$. כדי להראות שהם בת"ל, נניח $\sum_{i=0}^m r_i x_i = 0$. נפעיל את π ונקבל $\sum_{i=1}^m r_i y_i = \sum_{i=0}^m r_i \pi(x_i) = 0$. אבל $y_1, \dots, y_m$ בסיס, לכן בת"ל, כלומר $r_1 = \cdots = r_m = 0$. לכן קיבלנו $r_0 x_0 = 0$, ומכך ש-x_0 בסיס ל-$\ker(\pi|_N)$ נקבל ש-$r_0 = 0$. □

כמסקנה מהמשפט, אפשר לראות שכל תת-מודול M של R^n אפשר לכתוב בצורה $A \cdot R^n$: ניקח איזשהו בסיס של M, נשים אותו בעמודות מטריצה, ואם יש פחות מ-n איברי בסיס נוסיף עמודות אפסים.

מסקנה 2. כל מודול נוצר סופית M מעל תחום ראשי R הוא מהצורה $M_A \cong R^n/A\cdot R^n$ לאיזושהי $A \in M_n(R)$. המטריצה A נקראת **מטריצת היחסים** של M.

נגדיר יחס שקילות על מטריצות באופן הבא: מטריצות $A, B \in M_n(R)$ הן **דומות**, אם קיימות מטריצות הפיכות $P, Q \in \mathrm{GL}_n(R)$ שעבורן $B = PAQ$. בשפה של אלגברה לינארית, שתי מטריצות הן דומות אם ורק אם אפשר להגיע מאחת לשנייה על ידי פעולות שורה ועמודה. ראינו שכל מטריצה אפשר להביא ככה לצורה אלכסונית קנונית, כלומר צורה אלכסונית $\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$ שעבורה $d_1 \mid \cdots \mid d_n$. אפשר להוכיח שהצורה האלכסונית הקנונית יחידה עד כדי חברות ישירות או כתוצאה של משפט המיון.

משפט 3. לכל $A, B \in M_n(R)$, $A \sim B$ אם ורק אם $M_A \cong M_B$.

הוכחה. $\boxed{\Leftarrow}$ נניח $B = PAQ$ לאילושהן $P, Q \in \mathrm{GL}_n(R)$. נשים לב שמתקיים השוויון $B \cdot R^n = (PAQ) \cdot R^n = (PA) \cdot (Q \cdot R^n) = PA \cdot R^n$ (המעבר האחרון נכון כי המטריצה Q הפיכה). לכן בעצם $M_B = M_{PA}$. את האיזומורפיזם $M_A \cong M_{PA}$ אפשר להראות על ידי ההעתקה $\varphi : M_A \to M_{PA}$ המוגדרת לפי $\varphi(v) = Pv + (PA \cdot R^n)$ היא איזומורפיזם של מודולים (ודאו שאתם יודעים להוכיח את זה. שימו לב שצריך גם להראות שהיא מוגדרת היטב).

$\boxed{\Rightarrow}$ נניח $M_A \cong M_B$. אפשר לדרג את A ולהביא אותה לצורה אלכסונית קנונית $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$. לפי החלק הראשון של הטענה,

$$M_A \cong M_D \cong R/\langle d_1\rangle \times \cdots \times R/\langle d_n\rangle.$$

אבל אז גם $M_B \cong M_A \cong R/\langle d_1\rangle \times \cdots \times R/\langle d_n\rangle$. מהיחידות של הגורמים האינווריאנטים, נקבל ש-D היא הצורה האלכסונית קנונית של B, ובפרט $B \sim D$. לכן $A \sim D \sim B$, כלומר $A \sim B$. $\square$

מסקנה 4. יהי M תת-מודול של R^n. אז אפשר למצוא בסיס $y_1, \ldots, y_n$ של R^n וסקלרים $d_1, \ldots, d_m \in R$ כך ש-$d_1 y_1, \ldots, d_m y_m$ בסיס של M.

הוכחה. נכתוב $M = A \cdot R^n$ לאיזושהי $A \in M_n(R)$. נדרג את A לצורה אלכסונית קנונית $A \sim D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$. אנחנו יודעים שקיים איזומורפיזם של R-מודולים

$\varphi : R^n \to R^n$ כך ש-$\varphi(A \cdot R^n) = D \cdot R^n$: אם $D = PAQ$, אפשר לקחת $\varphi(v) = Pv$. קל לוודא שזהו איזומורפיזם של מודולים מעל R, וכן $\varphi(Av) = PAv = (PAQ)Q^{-1}v = DQ^{-1}v$. אבל ל-$D \cdot R^n$ יש בסיס $d_1e_1, \dots, d_me_m$ (כאשר m הוא האינדקס המקסימלי שעבורו $d_m \neq 0$), ואם נסתכל על $\varphi^{-1}(e_1), \dots, \varphi^{-1}(e_n)$ נקבל את הבסיס הדרוש לטענה. □

מודולים מעל $F[x]$

כעת נניח ש-F שדה, וניקח את $R = F[x]$, שראינו שהוא תחום ראשי. ראינו איך נראים מודולים מעל R: מרחב וקטורי V מעל F יחד עם העתקה לינארית $T : V \to V$.

ניקח $V = F^n$ בתור המרחב הווקטורי, וניקח $T : V \to V$ העתקה לינארית המיוצגת על ידי מטריצה A. שימו לב שאם B דומה ל-A, אז B היא המטריצה המייצגת של T אם נחליף את הבסיסים של V בתחום ובטווח. קיבלנו פה מבנה של V כמבנה של $F[x]$-מודול, שנסמן V_T: הפעולה של $f(x) \in F[x]$ על $v \in V$ היא $f(x) \cdot v = f(A)v$.

אמרנו בתרגול ש-V_T לעולם אינו חופשי מעל $F[x]$, ולמעשה אינו נאמן: אם $m_A(\lambda)$ הוא הפולינום המינימלי של A, אז $m_A(x) \cdot v = m_A(A)v = 0$ לכל $v \in V$.

אם היינו רוצים לכתוב את V_T בצורה M_B לאיזושהי מטריצה B, מי היא הייתה צריכה להיות? מחפשים מטריצה $B \in M_n(F[x])$ שתהיה מטריצת היחסים של המודול. נלך לפי ההגדרה: נבחר בסיס $v_1, \dots, v_n$ של V מעל F כך ש-A היא המטריצה המייצגת של T ביחס לבסיס הזה, ואז $v_1, \dots, v_n$ יוצרים את V_T מעל $F[x]$. נסמן על ידי $e_1, \dots, e_n$ את וקטורי היחידה ב-$F[x]^n$, ואז יש הומומורפיזם $\varphi : F[x]^n \to V_T$ לפי $\varphi(e_i) = v_i$. רוצים ללמוד את הגרעין של φ.

משפט 5. $\ker \varphi = (xI - A)\, F[x]^n$.

הוכחה. נסמן $K = \ker \varphi$, ונוכיח הכלה דו-כיוונית.

$\boxed{\supseteq}$ לכל $1 \leq i \leq n$, נסמן $w_i = (xI - A)e_i$. מספיק להראות שכל $w_i \in K$. אכן, לפי הגדרת מטריצה מייצגת $x \cdot v_i = Av_i = \sum_{j=1}^n A_{ji}v_j$, ולכן

$$\varphi(w_i) = \varphi(x \cdot e_i - \sum_{j=1}^n A_{ji}e_i) = x \cdot v_i - \sum_{j=1}^n A_{ji}v_i = 0.$$

$\boxed{\subseteq}$ נסמן $W = \sum_{i=1}^m Fe_i$. זה רק תת-מרחב וקטורי מעל F, אבל לא בהכרח תת-מודול מעל $F[x]$. הצמצום של φ אל W הוא איזומורפיזם $W \xrightarrow{\sim} V$ (כי זו העתקה לינארית על בין מרחבים וקטוריים מאותו המימד). נשים לב כי $x \cdot e_i = w_i + Ae_i$, ולכן $x \cdot W \subseteq K + W$. באינדוקציה, לכל $k \geq 0$ נקבל $x^k \cdot W \subseteq K + W$, ולכן $F[x]^n = \sum_k x^kW = K + W$. מצד שני, $K \cap W = 0$ כי $v_1, \dots, v_n$ בת"ל מעל F; לכן בעצם $F[x]^n = K \oplus W$. אבל כיוון ש-φ משרה איזומורפיזם מ-W ל-V, נקבל $\ker \varphi \subseteq K$. □

מסקנה 6. מטריצת היחסים של V_T היא $xI-A$. במילים אחרות, או יותר נכון נוסחה אחרת,

$$V_T \cong {}^{F[x]^n}\big/_{(xI-A)F[x]^n}.$$

כעת, ניזכר במושג מאלגברה לינארית: נאמר ששתי מטריצות $A,B\in M_n(F)$ הן **צמודות**, אם קיימת $P\in \mathrm{GL}_n(F)$ שעבורה $B=PAP^{-1}$.

משפט 7. יהיו $A,B\in M_n(F)$. הטענות הבאות שקולות:

א. A ו-B צמודות מעל F.

ב. $xI-A$ ו-$xI-B$ דומות מעל $F[x]$.

ג. A ו-B מגדירות את אותו המבנה של מודול מעל $F[x]$ על F^n.

הוכחה. $\boxed{\text{א} \Leftarrow \text{ב}}$ אם $B=PAP^{-1}$ אז $xI-B=P(xI-A)P^{-1}$.
$\boxed{\text{ב} \Leftarrow \text{ג}}$ אלו מטריצות היחסים של המודולים שמגדירים A ו-B על F^n, ולכן זה נובע ממשפט 3.
$\boxed{\text{ג} \Leftarrow \text{א}}$ כיוון שהן מגדירות את אותו המבנה של מודול, יש איזומורפיזם של מודולים $\varphi:F^n\to F^n$. בפרט הוא מקיים לכל $v\in V$

$$\varphi(Av)=\varphi(x\cdot_A v)=x\cdot_B\varphi(v)=B\cdot\varphi(v).$$

אבל זהו איזומורפיזם של מודולים, בפרט של מרחבים וקטוריים מעל F, ולכן אפשר להציג אותו על ידי מטריצה הפיכה P, כלומר $\varphi(v)=Pv$. נקבל

$$PAv=BPv$$

ומפה $B=PAP^{-1}$. $\square$

מסקנה 8. יהיו $F\subseteq K$ שדות, ויהיו $A,B\in M_n(F)$. אז A ו-B צמודות מעל F אם ורק אם הן צמודות מעל K.

הוכחה. $\boxed{\Leftarrow}$ טריוויאלי.
$\boxed{\Rightarrow}$ למטריצות $xI-A$ ו-$xI-B$ יש צורות אלכסוניות קנוניות D_A ו-D_B מעל $F[x]$. אבל A ו-B צמודות מעל K, לכן $xI-A$ ו-$xI-B$ דומות מעל $K[x]$, ולכן הצורות האלכסוניות הקנוניות שלהן מעל $K[x]$ שוות (עד כדי חברות). אבל הצורות האלו חייבות להיות D_A ו-D_B, בגלל היחידות של הצורה האלכסונית הקנונית. $\square$