מבוא לחוגים ומודולים - תרגול 12

יהי R תחום ראשי, ויהי M מודול נוצר סופית מעל R. ראינו שאפשר לפרק

$$M\cong R^n/A\cdot R^n \cong R/\langle d_1\rangle \times\cdots\times R/\langle d_n\rangle$$

כאשר $d_1|\cdots|d_n$ הגורמים האינווריאנטים. הם יחידים עד כדי חברות.

ברמת המטריצות, זה שקול לכך ש- $A=P\begin{pmatrix}d_1&&\\&\ddots&\\&&d_n\end{pmatrix}\cdot Q$

עבור $P,Q\in GL_n(R)$.

לקחנו $R=F[x]$, $V=F^n$, העתקה לינארית $T:V\longrightarrow V$,

והגדרנו על V מבנה של $F[x]$-מודול (סימון V_T):

$$x\cdot v=T(v),\quad f(x)\cdot v=f(T)(v)$$

אם בוחרים מטריצה מייצגת A של T,

$$V_T\cong F[x]^n/(xI-A)F[x]^n \cong F[x]/\langle d_1(x)\rangle\times\cdots\times F[x]/\langle d_n(x)\rangle$$

$d_1(x)|\cdots|d_n(x)$.

$d_n(x)=$ הפולינום המינימלי של T. $d_1(x)\cdot\ldots\cdot d_n(x)=$ הפולינום האופייני של T.

אז ראינו

$$f(x)=x^n-a_{n-1}x^{n-1}-\cdots-a_0$$

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

$$A\overset{\text{דומה}}{\sim}\begin{pmatrix}C_{d_1(x)}&&&\\&C_{d_2(x)}&&\\&&\ddots&\\&&&C_{d_n(x)}\end{pmatrix}$$

מצד שני, הייתה גרסה למשפט המיון עם מחלקים ראשוניים:

$$M\cong R/\langle p_1^{e_1}\rangle\times\cdots\times R/\langle p_t^{e_t}\rangle$$

כאשר $p_1,\dots,p_t \in R$ אי־פריקים וראשוניים (לא בהכרח שונים), $e_i > 0$.

נניח ש־F מכיל את כל הע"ע של T, כלומר הפולינום האופייני של T מתפרק למכפלה של גורמים לינאריים $(x-\lambda_1)^{k_1}\cdots(x-\lambda_t)^{k_t}$.

המחלקים הראשוניים של V_T הם בדיוק $(x-\lambda_i)^{k_i}$ שמופיעים בפירוקים של $d_1,\dots,d_n$. (λ_i לא בהכרח שונים)

$$V_T \cong F[x]/\langle (x-\lambda_1)^{k_1}\rangle \times \dots \times F[x]/\langle (x-\lambda_t)^{k_t}\rangle$$

אם נבחר בסיס B_i של $F[x]/\langle (x-\lambda_i)^{k_i}\rangle$, $B = B_1 \cup \dots \cup B_t$,

איחוד במובן של לוו לעיבוב רכיבים

$$[T]_B^B = \begin{pmatrix} \boxed{[T]_{B_1}^{B_1}} & & \\ & \ddots & \\ & & \boxed{[T]_{B_t}^{B_t}} \end{pmatrix}$$

אפשר לשים לב ש־$F[x]/\langle (x-\lambda)^k\rangle \cong \{v\in V \mid (T-\lambda I)^k(v)=0\}$. "המרחב העצמי המוכלל"

<u>טענה:</u>

תהי $T: F^k \to F^k$ העתקה לינארית שביחס אליה $V_T \cong F[x]/\langle (x-\lambda)^k\rangle$.

אז קיים בסיס B של V_T שביחס אליו המטריצה המייצגת של T היא

$$[T]_B^B = \begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} = J_k(\lambda)$$

<u>הוכחה:</u>

נסמן $I = \langle (x-\lambda)^k\rangle$. ניקח את הבסיס

$$B = \{(x-\lambda)^{k-1}+I, (x-\lambda)^{k-2}+I, \dots, 1+I\}$$

נסמן $b_i=(x-\lambda)^i+I$.

$$T(b_{k-1})=x\cdot b_{k-1}=x\left((x-\lambda)^{k-1}+I\right)=x(x-\lambda)^{k-1}+I=$$
$$=\left(\lambda+(x-\lambda)\right)(x-\lambda)^{k-1}+I=\lambda(x-\lambda)^{k-1}+(x-\lambda)^k+I=$$
$$=\lambda(x-\lambda)^{k-1}+I=\lambda b_{k-1}$$

$$T(b_{k-2})=x\cdot b_{k-2}=x(x-\lambda)^{k-2}+I=\left(\lambda+(x-\lambda)\right)(x-\lambda)^{k-2}+I=$$
$$=\lambda(x-\lambda)^{k-2}+(x-\lambda)^{k-1}+I=\lambda b_{k-2}+b_{k-1}$$

אפשר לחשב באופן דומה שלכל $0\le i\le k-2$, $T(b_i)=\lambda b_i+b_{i+1}$.

לכן

$$[T]_B^B=\begin{pmatrix}\lambda & 1 & & 0\\ 0 & \lambda & \ddots & \\ \vdots & 0 & \ddots & 1\\ 0 & 0 & \cdots 0 & \lambda\end{pmatrix}=J_k(\lambda)$$

$B=\{b_{k-1},\dots,b_0\}$

□

מסקנה:

נניח ש-F שדה, V מרחב וקטורי ממימד סופי מעל F, $T:V\to V$ העתקה לינארית, ונניח שהפולינום האופייני של T מתפרק למכפלה של גורמים לינאריים מעל F. אזי קיים בסיס B של V שבו

$$[T]_B^B=\begin{pmatrix}J_{k_1}(\lambda_1) & & 0\\ & \ddots & \\ 0 & & J_{k_t}(\lambda_t)\end{pmatrix}$$

זו צורת ז'ורדן הקנונית של T. יש יחידות עד כדי סדר הבלוקים.

דוגמה:

אם $A=\begin{pmatrix}-1&-2&6\\-1&0&3\\-1&-1&4\end{pmatrix}$, ראינו שהגורמים האינווריאנטים הם $1,\ \overset{J_1(1)}{1-x},\ \overset{J_2(1)}{(1-x)^2}$.

לכן צורת ז'ורדן היא

$$\left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 1 \\ 0 & 0 & 1 \end{array}\right)$$

<u>דוגמה:</u>

נניח שצורת ז'ורדן היא

$$J_3(1) \oplus J_3(5) \oplus J_4(1) \oplus J_3(-4) \oplus J_3(1) \oplus J_1(-4) \oplus J_2(-4) \oplus J_2(5) \oplus J_5(1)$$

איך חוזרים לגורמים האינווריאנטים? קודם חוזרים למחלקים האלמנטריים

$$(x-1)^3,\ (x-5)^3,\ (x-1)^4,\ (x+4)^3,\ (x-1)^3,\ x+4,\ (x+4)^2,\ (x-5)^2,\ (x-1)^5$$

כדי לחזור לגורמים האינווריאנטים, נשים בטבלה לפי ע"ע ונמיין לפי החזקות:

$(x-1)^5$	$(x-5)^3$	$(x+4)^3$
$(x-1)^4$	$(x-5)^2$	$(x+4)^2$
$(x-1)^3$	1	$x+4$
$(x-1)^3$	1	1

נכפול כל שורה וכך נקבל את הגורמים האינווריאנטים:

$$(x-1)^5(x-5)^3(x+4)^3 \longleftarrow \text{הפולינום המינימלי}$$

$$(x-1)^4(x-5)^2(x+4)^2$$

$$(x-1)^3(x+4)$$

$$(x-1)^3$$

איברים אלגבריים ואיברים שלמים

הגדרה:

יהיו $R\subseteq S$ חוגים חילופיים.

- איבר $s\in S$ הוא אלגברי מעל R, אם s הוא שורש של פולינום לא אפסי מעל R, כלומר קיים $f(x)\in R[x]$, $f(x)=a_nx^n+\cdots+a_0 \neq 0$ שעבורו $f(s)=a_ns^n+\cdots+a_1s+a_0=0$.
- איבר $s\in S$ הוא שלם מעל R, אם הוא שורש של פולינום מתוקן מעל R.

דוגמה:

$\sqrt{3}$ שלם מעל $\mathbb{Z}$, כי הוא מתאפס ע"י הפולינום x^2-3.

דוגמה:

$\frac{1}{2}$ אלגברי שאינו שלם מעל $\mathbb{Z}$.

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$$

$$f\left(\tfrac{1}{2}\right)=\frac{1}{2^n}+\frac{a_{n-1}}{2^{n-1}}+\cdots+a_0=0 \quad /\cdot 2^n$$

$$\underbrace{1+2\cdot a_{n-1}+\cdots+2^n a_0}_{\text{אי-זוגי}}=0$$

טענה:

יהיו $R\subseteq S$ חוגים חילופיים. התנאים הבאים שקולים:

א. s שלם מעל R.

ב. החוג $R[s]\subseteq S$ נוצר סופית כ-R-מודול.

ג. קיים תת-חוג $R[s]\subseteq T\subseteq S$ שהוא נוצר סופית כ-R-מודול.

ד. קיים $R[s]$-מודול נאמן M כך ש-M נוצר סופית כ-R-מודול.

מסקנה:

אוסף האיברים ב-S שהם שלמים מעל R הוא תת-חוג של S.

תרגיל:

יהי F שדה, ויהיו $a,b\in F$. מצאו פולינום המאפס את $a^{\frac{1}{3}}+b^{\frac{1}{3}}$, והסיקו שהוא שלם מעל F.

[דמיינו את $\sqrt[3]{2}+\sqrt[3]{5}$]

פתרון:

נסמן $x=a^{\frac{1}{3}}+b^{\frac{1}{3}}$.

$$x^2=a^{\frac{2}{3}}+2a^{\frac{1}{3}}b^{\frac{1}{3}}+b^{\frac{2}{3}}$$

$$x^3=a+3a^{\frac{2}{3}}b^{\frac{1}{3}}+3a^{\frac{1}{3}}b^{\frac{2}{3}}+b=a+b+3a^{\frac{1}{3}}b^{\frac{1}{3}}(a^{\frac{1}{3}}+b^{\frac{1}{3}})=$$
$$=a+b+3a^{\frac{1}{3}}b^{\frac{1}{3}}x$$

$$x^3-a-b=3a^{\frac{1}{3}}b^{\frac{1}{3}}x$$

$$(x^3-a-b)^3=27abx^3$$

ואם נפתח את הסוגריים נקבל פולינום מתוקן שמאפס את x. (ממעלה 9)
$$(x^3-a-b)^3-27abx^3$$

הגדרה:

יהיו $R\subseteq S$ חוגים חילופיים.

א. אומרים ש-S הוא <u>הרחבה שלמה</u> של R אם כל איבר של S שלם מעל R.

ב. אומרים ש-R <u>סגור בשלמות ב-S</u> אם כל איבר של S שהוא שלם מעל R נמצא ב-R.

R <u>סגור בשלמות</u> אם הוא סגור בשלמות ב-$\mathrm{Frac}(R)$.

הערה:

אם S הרחבה שלמה של R ו-$R\subseteq T\subseteq S$ אז גם T הרחבה שלמה של R.

דוגמאות:

א. כל תחום שלמות פריקות ראשי (UFD) הוא סגור בשלמות (בשדה השברים שלו)

בפרט $\mathbb{Z}$ סגור בשלמות ב-$\mathbb{Q}$.

ב. $\mathbb{Z}[\sqrt{2}]$ הרחבה שלמה של $\mathbb{Z}$. אכן, אם $x=a+b\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$,

$$x-a=b\sqrt{2}$$
$$(x-a)^2=2b^2$$

לכן $a+b\sqrt{2}$ שורש של הפולינום $x^2-2ax+(a^2-2b^2)$.

תרגיל:

יהי R חוג שאין בו נילפוטנטים $\underbrace{\text{נילפוטנטים}}_{\exists n\geq 1:\ a^n=0}$ שונים מאפס. הוכיחו ש-R סגור בשלמות ב-$R[x]$.

פתרון:

יהי $f(x)\in R[x]$ איבר שלם מעל R. אז קיימים $a_0,\dots,a_{n-1}\in R$ שעבורם

$$f(x)^n+a_{n-1}f(x)^{n-1}+\dots+a_1f(x)+a_0=0$$

אם $f(x)$ לא היה קבוע, נניח שהמונום המוביל שלו הוא bx^k, $b\neq 0$.

אז המונום המוביל של אגף שמאל הוא b^nx^{kn}, ששונה מ-0 כי $b^n\neq 0$

ולכן יכול להצטמצם רק ע"י אף גורם אחר, בסתירה.

לכן $f(x)$ קבוע, כדרוש. $\square$

תרגיל:

יהיו $C\subseteq R'\subseteq R$ חוגים חילופיים, ויהי $a\in R$. נניח ש-a שלם מעל R',

ו-R' הרחבה שלמה של C. אז a שלם מעל C.

כמסקנה מכך, אם R הרחבה שלמה של R', ו-R' הרחבה שלמה של C, אז גם R הרחבה שלמה של C.

הוכחה:

a שלם מעל R', לכן קיימים $b_0,\dots,b_{n-1}\in R'$ שעבורם

$$a^n+b_{n-1}a^{n-1}+\dots+b_1a+b_0=0$$

$$a^n=-b_{n-1}a^{n-1}-\dots-b_1a-b_0$$

לכן a שלם גם מעל $C[b_0,\dots,b_{n-1}]$. לכן $C[b_0,\dots,b_{n-1}][a]$ הוא מודול נוצר סופית מעל $C[b_0,\dots,b_{n-1}]$, אבל $C[b_0,\dots,b_{n-1}]$ מודול נוצר סופית מעל C, כי $b_0,\dots,b_{n-1}$ שלמים מעל C, ולכן גם $C[b_0,\dots,b_{n-1}][a]$ מודול נוצר סופית מעל C. מהתנאים השקולים שכתבנו קודם, a שלם מעל C. $\square$

מסקנה:

נניח $R\subseteq S$, הסגור השלם של R ב-S הוא סגור בשלמות ב-S.

דוגמה חשובה:

$F=\mathbb{Q}[\sqrt{d}]$, ($d\neq 1$ חופשי מריבועים) הסגור השלם הוא

$$\mathcal{O}_d=\begin{cases}\mathbb{Z}[\sqrt{d}], & d\equiv 2,3 \pmod 4\\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d\equiv 1 \pmod 4\end{cases}$$

בחוג הזה אפשר להגדיר נורמה (לא אוקלידית)

$$N(a+b\sqrt{d})=(a+b\sqrt{d})(a-b\sqrt{d})=a^2-db^2$$

N פונקציה כפלית, $x=0 \iff N(x)=0$.

מסקנה:

$N(x)\in\mathbb{Z}$ לכל $x\in\mathcal{O}_d$.

הערה:

יש בדיוק 21 ערכים של d שעבורם $\mathcal{O}_d$ אוקלידי ביחס לפונקצ' הנורמה הנ"ל:

$d>0$ $\quad \{2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}$

$d<0$ $\quad \{-1,-2,-3,-7,-11\}$

תרגיל:

הוכיחו שאם $x|y$ ב-$\mathcal{O}_d$ אז $N(x)|N(y)$ ב-$\mathbb{Z}$.

בפרט, x הפיך ב-$\mathcal{O}_d$ $\iff$ $N(x)=\pm 1$.

הוכחה:

מהכפליות של הנורמה: $y=xz \Rightarrow N(y)=N(x)\cdot N(z)$.

תרגיל:

כמסקנה מהתרגיל הקודם, אפשר להוכיח שאם $N(a)$ אי-פריקה, אז a אי-פריק.

תנו דוגמה ל-a אי-פריק שעבורו $N(a)$ פריקה.

פתרון:

$d=-5$, $a=1+\sqrt{-5}$. $N(a)=1-(-5)=6$ פריקה.

a אי-פריק: נניח $a=bc$

$$\Downarrow$$

$$6=N(a)=N(b)N(c)$$

אם b ו-c לא הפיכים, אז $N(b),N(c)\neq\pm1$, והנורמה חיובית, לכן בה"כ $N(b)=2$.

אבל אין ב-$\mathbb{Z}[\sqrt{-5}]$ איברים מנורמה 2:

$$\alpha^2+5\beta^2=N(\alpha+\beta\sqrt{-5})=2$$

אז בהכרח $\beta=0$, אבל אין פתרונות ל-$\alpha^2=2$.