הרצאה 19

תזכורת: F שדה.

$$d(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1 x + a_0 \in F[x]$$

המטריצה מלווה של d היא מטריצה $m\times m$

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

תרגיל הפולינום האופייני של C_d הוא d.

תזכורת מודול מעל $F[x]$ $\Longleftrightarrow$

מרחב וקטורי V מעל F יחד העתקה

לינארית $T: V\to V$.

(V מקבל את הכפל הסקלרי ב-F)

$T(v) = x\cdot v$.

משפט תהי $A\in M_n(F)$ מטריצה. אזי A דומה

למטריצה מן הצורה

$$\begin{pmatrix} C_{d_1} & & & \\ & C_{d_2} & & \\ & & \ddots & \\ & & & C_{d_n} \end{pmatrix}$$

כאשר $d_1|d_2|d_3|\cdots|d_n \neq 0$ והפולינומים $d_i\in F[x]$
מתוקנים ויחידים.

<u>הוכחה</u> A מייצגת העתקה לינארית $T:F^n\to F^n$
(ביחס לאיזשהו בסיס שבחרנו). המ"ו $\underbrace{F^n}_{\text{סוף-מימדי}}$
עם T ניתן $F[x]$-מודול M.
$F[x]$ תחום ראשי, לפי משפט המ"ו

$$M\cong \cancel{F[x]^m}\times F[x]/(d_1)\times\cdots\times F[x]/(d_n)$$

כאשר $d_1|d_2|\cdots|d_n\neq 0$. הוכחנו כי $m=0$.

נבחר את הבסיס

$$1+(d_i),\ x+(d_i),\ \ldots,\ x^{m_i-1}+(d_i)$$

של $F[x]/(d_i)$, כאשר $m_i=\deg d_i$. בעצם

בהינתן בסיס חשב של M, והמטריצה

של העתקה $T: v \mapsto xv$ ביחס לבסיס זה

אז היא צמודה ל-A. הפעולה של x

על $F[x]/_{(d_i)}$ היא:

$$1+(d_i) \longmapsto x+(d_i)$$

$$x+(d_i) \longmapsto x^2+(d_i)$$

$$\vdots$$

$$x^{m_i-2}+(d_i) \longmapsto x^{m_i-1}+(d_i)$$

$$x^{m_i-1}+(d_i) \longmapsto x^{m_i}+(d_i) =$$

$$x^{m_i}-d_i+(d_i) =$$

$$-a_0-a_1x-\dots-a_{m_i-1}x^{m_i-1}+(d_i)$$

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & \vdots & -a_1 \\ 0 & 1 & \cdots & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & 1 & -a_{m_i-1} \end{pmatrix} = C_{d_i}$$

לכן המטריצה של T ביחס לבסיס החשב של $M=V$ היא

צמודה/דומה ל-A $\rightarrow$ $\begin{pmatrix} C_{d_1} & & \\ & \ddots & \\ & & C_{d_n} \end{pmatrix}$

הצורה הרציונלית הקנונית של A.

הגורמים האינוו' d_i מוגדרים עד כדי חברות, לכן אם דורשים d_i מתוקנים אז הם מוגדרים היטב. והתנאי $d_1|d_2|\dots|d_n$ וגם היחידות נובעים ישירות ממשפט המיון.

<u>הגדרה</u> תהי A מטריצה כנ"ל. הפולינומים $d_1,\dots,d_n$ נקראים גורמים אינווריאנטיים של A.

<u>מסקנה</u> הפולי' האופייני של A הינו $d_1(x)\cdot d_2(x)\cdots d_n(x)$.

<u>מסקנה</u> (משפט קיילי-המילטון). תהי $A\in M_n(F)$ מטריצה. יהי

$$f_A(x)=x^n+b_{n-1}x^{n-1}+\dots+b_0$$

הפולי' האופייני. אזי

$$f_A(A)=A^n+b_{n-1}A^{n-1}+\dots+b_1A+b_0\in M_n(F)$$
$$=0.$$

הוכחה יהי M ה-$F[x]$-מודול המתאים ל-T.
יהי $v\in V$

$$(f_A(A))v = (x^N + b_{N-1}x^{N-1} + \dots + b_0)\cdot v$$

לכן, $f_A(A)=0 \iff f_A\cdot v = 0$ לכל $v\in V$

$\iff f_A \in Ann_{F[x]}(M)$. אבל הוכחנו

בפעם הקודמת כי $Ann_{F[x]}(M) = (d_n)$

הגורם האינ' האחרון = הפולי' המינימלי של A.

אז לכן $f_A = d_1 d_2 \cdots d_n \in (d_n) = Ann_{F[x]}(M)$.

שוב, תהי $A\in M_N(F)$ מטריצה, נניח כי F מכיל את כל הערכים העצמיים של A $\Leftarrow$ הפולי' האופייני מתפרק למכפלה של פולינומים לינאריים מעל F, לכן הגורמים האינ' מתפרקים כך (כי הפולי' האופייני הינו $d_1 d_2 \cdots d_n$).

המחלקים האלמנטריים של M מחלקים
גורמים אינווריאנטיים, לכן, כל מחלק
אלמ' הינו חזקה של פול' לינ'
$(x-\lambda)^a$, $\lambda \in F$. לפי משפט המיון בצורה
של מחלקים אלמ',

$$M \cong F[x]/((x-\lambda_1)^{a_1}) \times \cdots \times F[x]/((x-\lambda_r)^{a_r})$$

כאשר λ_i לאו בהכרח שונים.
בוחרים את ה-F-בסיס

$$(x-\lambda)^{a-1} + (x-\lambda)^a F[x], \dots, (x-\lambda) + (x-\lambda)^a F[x],$$
$$1 + (x-\lambda)^a F[x] \quad \text{של} \quad F[x]/(x-\lambda)^a.$$

ביחס לבסיס הזה, הפעולה של T (כפל
סקלרי ב-x) על $F[x]/(x-\lambda)^a$ הינה

$I=(x-\lambda)^a F[x]$

אם $0 \le k \le a-2$, אזי

$$(x-\lambda)^k + I \longmapsto x(x-\lambda)^k + I =$$

$$(x-\lambda)^{k+1} + \lambda(x-\lambda)^k + I$$

$$(x-\lambda)^{a-1} + I \longmapsto x(x-\lambda)^{a-1} + I = \lambda(x-\lambda)^{a-1} + I$$

מטריצה $a\times a$

$$\begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \lambda & 1 \\ & & & \lambda \end{pmatrix} \longleftrightarrow J_a(\lambda)$$

לכל A צמודה למטריצה יחידה

עד הסדרה

$$\begin{pmatrix} J_{a_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{a_r}(\lambda_r) \end{pmatrix} \longleftarrow$$

צורה
קנונית של
ז'ורדן.

השלמה של חוגים

יהי R חוג חילופי, יהי $I \trianglelefteq R$, נניח $\bigcap_{n=1}^{\infty} I^n = (0)$. (לדוגמא, $R=\mathbb{Z}\times\mathbb{Z}$, $I=\mathbb{Z}\times(0)$ לא מקיים את התנאי).

נגדיר טופולוגיה על R: בסיס של קבוצות פתוחות יהיה

$$x+I^n=\{x+y : y\in I^n\} \qquad (I^0=R)$$

לכל $x\in R$ ולכל $n\geq 0$. כלומר, קבוצה $U\subseteq R$ פתוחה אם ורק אם לכל $x\in U$ קיים n_x כך ש- $x+I^{n_x}\subseteq U$.

אכן זו טופולוגיה: תהיינה U,V פתוחות. $x\in U\cap V$. אזי קיימים n,m כך ש-

$x+I^n\subseteq U$, $x+I^m\subseteq V$. אזי

$$x+I^{\max\{n,m\}} = (x+I^n)\cap(x+I^m)\subseteq U\cap V.$$

לכן $U\cap V$ פתוחה.

כיוון שהנחנו $\bigcap_{n=1}^{\infty} I^n = (0)$ כי טופ׳ האוסדורף.

אכן, יהיו $x,y\in R$ שונים. אזי קיים

n כך ש- $x-y\notin I^n$ $\Longleftarrow$

$$(x+I^n)\cap(y+I^n)=\emptyset$$

נגדיר פונקציית מרחק: נבחר $0<\tau<1$.

$$d(x,y)=\inf\{\tau^n : x-y\in I^n\}$$

$$=\begin{cases} 0, & x=y \\ \tau^{\max\{n:\ x-y\in I^n\}} & : x\neq y. \end{cases}$$

זו אכן פונקציית מרחק. צריך להוכיח רק

את אי-שוויון המשולש

$$d(x,y)\le d(x,z)+d(z,y)$$

כאן נוכיח אפילו משהו יותר חזק (אי-שוויון

המשולש החזק)

$$d(x,y)\le \max\{d(x,z),\ d(z,y)\}$$

הוכחה: נניח x,y,z כולם שונים, אחרת ברור.

יהי n מקס' כך ש- $x-z\in I^n$

m " " $z-y\in I^m$

$$\Leftarrow\quad x-y=(x-z)+(z-y)\in I^{\min\{n,m\}}$$

$$d(x,y)\le \tau^{\min\{n,m\}}=\max\{\tau^m,\tau^n\}=\max\{d(x,z),\,d(z,y)\}.$$

בודקים שהטופ' הנ"ל הטופ' המטרית.

הגדרה: סדרה $\{a_n\}$ של איברים של R נקראת סדרת קושי אם לכל $\varepsilon>0$ קיים N כך שלכל $m,n\ge N$ מתקיים $d(a_n,a_m)<\varepsilon$ $\Leftrightarrow$ לכל k קיים N_k כך ש- $a_n-a_m\in I^k$ לכל $n,m\ge N_k$.

הגדרה: הסדרה $\{a_n\}$ מתכנסת לגבול $L\in R$ אם לכל $\varepsilon>0$ קיים N כך שלכל $n\ge N$ מתקיים $d(a_n,L)<\varepsilon$ $\Leftrightarrow$ לכל k קיים N_k כך ש- $a_n-L\in I^k$ לכל $n\ge N_k$.

R נקרא שלם ביחס ל-I אם כל סדרת
קושי היא מתכנסת.

<u>דוגמא</u> $R=\mathbb{Z}$ לא שלם.
$p>2$, $I=(p)$

$a_n = 1+p+p^2+\dots+p^n$.

זו סדרת קושי, נשים לב כי

$$(1-p)a_n = 1-p^{n+1} \longrightarrow 1$$

ברור שאם $a_n \to L$ אז
$ra_n \to rL$ לכל $r\in R$.

לכן אם $a_n \to L$ אז
$(1-p)L = 1$ ואין איבר $L\in\mathbb{Z}$
עם התכונה הזאת.