(1) 15/5/08

לינארית 2 - הרצאה 3

הגדרנו: $\varphi: M_n(R)[x] \to M_n(R[x])$

הוכחנו - φ חח"ע $\quad (\varphi(\sum_{\mu=0}^{\infty} A_\mu x^\mu))_{ij} = \sum_{\mu=0}^{\infty} (A)_{ij} x^\mu$

φ על: תהי $C \in M_n($. אזי לכל i,j

$(C)_{ij} = c^{(0)}_{ij} + c^{(1)}_{ij}x + \ldots \in R[x]$. נגדיר לכל μ, $A_\mu \in M_n(R)$: $(A_\mu)_{ij} = c^{(\mu)}_{ij}$

עבור μ גדול מספיק אזי $c^{(\mu)}_{ij} = 0$, לכל i,j, ולכן $A_\mu = 0$

לכן: $\sum_{\mu=0}^{\infty} A_\mu x^\mu$ פולינום ומתקיים $\quad (\varphi(\sum_{\mu=0}^{\infty}$

$$(\varphi(\sum_{\mu=0}^{\infty} A_\mu x^\mu))_{ij} = \sum_{\mu=0}^{\infty} c^{(\mu)}_{ij} x^\mu = (C)_{ij}$$

לכן $\varphi(\sum A_\mu x^\mu) = C$

φ שומרת חיבור: $\sum A_\mu x^\mu, \sum B_\mu x^\mu \in M_n(R)[x]$

(שני פולינומים עם מקדמים של מטריצות)

$$(\varphi(\sum_\mu A_\mu x^\mu + \sum_\mu B_\mu x^\mu))_{ij} = \varphi(\sum_\mu (A_\mu + B_\mu)x^\mu)_{ij} =$$

$$= \sum_\mu (A_\mu + B_\mu)_{ij} x^\mu = \sum_\mu ((A_\mu)_{ij} + (B_\mu)_{ij}) x^\mu = \sum_\mu (A_\mu)_{ij} x^\mu + \sum_\mu (B_\mu)_{ij} x^\mu =$$

$$= (\varphi(\sum_\mu A_\mu x^\mu))_{ij} + (\varphi(\sum_\mu B_\mu x^\mu))_{ij} = (\varphi(\sum_\mu A_\mu x^\mu) + \varphi(\sum B_\mu x^\mu))_{ij}$$

זה לכל i,j, לכן $\varphi(\sum A_\mu x^\mu + \sum B_\mu x^\mu) = \varphi(\sum A_\mu x^\mu) + \varphi(\sum B_\mu x^\mu)$

φ שומרת כפל: יהיו $\sum A_\mu x^\mu, \sum_\mu B_\mu x^\mu \in M_n(R)[x]$

$$\varphi((\sum A_\mu x^\mu)(\sum_\nu B_\nu x^\nu)) \underset{\text{חוק הפילוג}}{=} \varphi(\sum_\mu \sum_\nu A_\mu B_\nu x^{\mu+\nu}) \xleftarrow{\ =\ } \text{φ שומרת חיבור}$$

$$= \sum_\mu \sum_\nu \varphi(A_\mu B_\nu x^{\mu+\nu})$$

מצד שני,

$$\varphi(\sum_\mu A_\mu x^\mu)\,\varphi(\sum_\nu B_\nu x^\nu) \overset{\text{φ שומרת חיבור}}{=} (\sum_\mu \varphi(A_\mu x^\mu))(\sum_\nu \varphi(B_\nu x^\nu))$$

$$= \sum_\mu \sum_\nu \varphi(A_\mu x^\mu)\,\varphi(B_\nu x^\nu)$$

לכן די להוכיח:

$$\varphi(A_\mu B_\nu x^{\mu+\nu}) = \varphi(A_\mu x^\mu)\,\varphi(B_\nu x^\nu)$$

ואכן

$$(\varphi(AB x^{\mu+\nu}))_{ij} = (AB)_{ij} x^{\mu+\nu} = \sum_{k=1}^{n} (A)_{ik}(B)_{kj} x^{\mu+\nu} =$$

$$= \sum_{k=1}^{n} \underbrace{(A)_{ik} x^\mu}\ \underbrace{(B)_{kj} x^\nu} = \sum_{k=1}^{n} (\varphi(Ax^\mu))_{ik} (\varphi(Bx^\nu))_{kj} =$$

$$= (\varphi(Ax^\mu)\,\varphi(Bx^\nu))_{ij}$$ מ"ל

<u>סימון</u>: אם R חוג, אז $R^\times = \{a\in R \mid a \text{ הפיך}\}$ (יש לו הופכי)

למשל, אם F שדה אז $(F[x])^\times = F^\times = F\setminus\{0\}$

<u>פריקות בחוגים</u>

<u>הגדרה</u>: יהי R חוג עם 1. קבוצה $I\subseteq R$ נקראת <u>אידיאל</u> אם

(א) $0\in I$ (ב) $a,b\in I \Rightarrow a+b\in I$

(ג) אם $a\in I$, $r\in R$ אז $ar, ra\in I$, בפרט $-a=(-1)\cdot a\in I$.

דוגמאות: א) אם R חוג חילופי עם 1 ו- $a\in R$ אז

$$(a):=\{ra \mid r\in R\}=\{b\in R \mid a|b\}$$

אידיאל ב-R, נקרא האידיאל הנוצר ע"י a.

אידיאל מהצורה (a) נקרא ראשי.

ב) יהי $\varphi: R\to S$ הומומורפיזם של חוגים עם 1 אז $\ker\varphi=\{r\in R \mid \varphi(r)=0\}$ אידיאל ב-R.

ג) $\{0\}$ הוא אידיאל

<u>למה</u>: יהי F שדה. אז כל אידיאל I ב- $R=F[x]$ הוא ראשי.

יתר על כן, אם $I\neq\{0\}$ אז

(א) קיים $g\in F[x]$ מתוקן (= בעל מקדם עליון 1) יחיד כך ש- $I=(g)$

(ב) g הוא הפולינום היחיד המתוקן ב-I ממעלה

$$m=\min\{\deg(h) \mid 0\neq h\in I\}$$

<u>הוכחה</u>: אם $I=\{0\}$, אז I ראשי, $I=(0)$. נניח $I\neq\{0\}$

אזי יש $g\in I$ ממעלה m.

טענה: $I=(g):=\{rg \mid r\in R\}$

אכן, "$\supseteq$" נובע, כי I סגור תחת כפל באיברי R.

"$\subseteq$": יהי $f\in I$. לפי החילוק עם שארית, $q,r\in R, \deg r<m$, $f=gq+r$

$$r=\underset{\in I}{f}-\underset{\in I}{g}q\in I$$

לפי ההגדרה של m, $r=0$. לכן $f=gq\in(g)$

בלי הגבלת הכלליות g מתוקן, אחרת אם $c\in F^\times$ המקדם העליון של g, אז $c^{-1}g$ מתוקן, מאותה המעלה m כמו g, וקל לראות ש- $(g)=(c^{-1}g)$

היחידות ב-(א): אם g' מתוקן, $I=(g)=(g')$ אז $g|g'$ וגם $g'|g$ ומכאן $g=g'$ (תרגיל: אם $g,g'\in F[x]$ מתוקנים, $g'|g$, $g|g'$ אז $g=g'$)

(3)

הוכחה ב-(ב): אם גם $g' \in I$ מתוקן ממעלה m, אז לפי ההוכחה, $I=(g')$, ולכן, לפי (א), $g=g'$.

<u>הגדרה</u>: יהי R תחום שלמות. יהי $0 \neq q \in R$, לא הפיך.

(א) q נקרא אי פריק אם לכל $a,b \in R$ מתקיים: אם $q=ab$ אז $a \in R^{\times}$ או $b \in R^{\times}$

(ב) q נקרא <u>ראשוני</u> אם לכל $a,b \in R$ מתקיים: אם $q|ab$ אז $q|a$ או $q|b$. (אם q מחלק את a,b זה מחלק אחד מהם)

למשל: $R=\mathbb{Z}$: אי-פריקים $\pm 2, \pm 3, \pm 5, \pm 7, \ldots$ הם גם ראשוניים.

<u>תרגיל</u>: יהי R תחום שלמות

(א) יש כלל הצמצום ב-R, אם $ac=bc$, $c \neq 0$, אז $a=b$

(ב) אם $a|b$ וגם $b|a$ אז יש $u \in R^{\times}$ כך ש-$b=ua$.

<u>תרגיל</u>: יהי R תחום שלמות.

(א) אם q ראשוני אז q אי פריק

(ב) אם q אי פריק, $u \in R^{\times}$, אז גם qu אי פריק.

<u>הוכחה</u>

(א) יהי $a,b \in R$ כך ש $q=ab$ אז $q|ab$ לכן $q|a$ (או $q|b$). נאמר $a=qc$. מכאן $a=abc$. כיוון $a \neq 0$, כי $q \neq 0$, לכן אפשר לצמצם: $1=bc$. לכן b הפיך, כלומר $b \in R^{\times}$. <u>מש"ל</u>

<u>משפט</u>: יהי R תחום שלמות שבו כל אידיאל <u>ראשי</u> (למשל $F[x]$ או $\mathbb{Z}$) (F שדה) יהי $q \in R$ אי פריק אז q ראשוני.

<u>הוכחה</u>: יהיו $a,b \in R$ כך ש-$q|ab$ אז

$I=\{c \in R \mid q|cb\}$ הוא אידיאל ב-R. (לבדוק)

(q מחלק את 0, אם c_1, c_2 נמצאים אז גם הסכום נמצא!

$$q|c_1b,\ q|c_2b \Rightarrow \begin{matrix} c_1b=qd_1 \\ c_2b=qd_2 \end{matrix} \Rightarrow (c_1+c_2)b=q(d_1+d_2)$$ כלומר $q|c_1+c_2$.

וגם לגבי המכפלה) הוא אידיאל ב-R (לבדוק) לכן יש $c_0 \in R$ כך ש-$I=c_0$.

$a \in I$, לכן יש $v \in R$ כך ש-$a=vc_0$.

$q \in I$, לכן יש $u \in R$ כך ש-$q=uc_0$. נתון ש-q אי-פריק,

לכן $c_0 \in R^{\times}$ או $u \in R^{\times}$. אם $c_0 \in R^{\times}$, אז $1=c_0c_0^{-1} \in (c_0)=I$. ואז לפי

הגדרת I, $q|b$.

אז $u\in R^{\times}$: $a=rc_0=rqu^{-1}=q(ru^{-1})$, לכן $q|a$. מש"ל

תרגיל: יהי F שדה ויהי E תת שדה שלו. יהיו $f,g\in E[x]$

נניח כי $g|f$ ב-$F[x]$. הוכח ש-$g|f$ ב-$E[x]$.

הוכחה: לפי החילוק עם שארית ב-$E[x]$ יש $q,r\in F[x]$ כך ש-

$$f=gq+r \ , \ \deg r<\deg g$$

כי הכפולה היחידה של 0 היא 0, לכן g הוא 0

(אחרת $g=0$ ואז זה נכון. נניח $g\neq 0$)

בפרט, $q,r\in F[x]$. אבל גם $f=gq'+0$, $q'\in F[x]$

לפי היחידות של החילוק עם שארית ב-$F[x]$, $r=0$ ו-$q'=q$. בפרט

$q'\in E[x]$