www.math.tau.ac.il/~haran

12/05/08 ליניארית-שעור

המשך-תת חוגים:

תת חוג S של R: $0\in S$, S סגורה תחת החיסור והכפל.

דוגמא:

אם R חוג, $S=\{\alpha I_n \mid \alpha\in R\} \subseteq M_n(R)$ תת חוג

יש איזומורפיזם $S\to R$ הנתון ע"י $\alpha I_n \to \alpha$

נזהה את S עם R ונאמר ש-R תת חוג של $M_n(R)$

דוגמא נוספת:

אם R חוג חילופי עם 1, ו- $A\in M_n(R)$

$R[A]=\{a_0I_n+a_1A+a_2A^2+\dots \mid a_i\in R \text{ וכמעט כולם } 0\}$

הוא תת חוג של $M_n(R)$, חילופי (כי החזקות של A מתחלפות בכפל)

משפט: יהי R תחום שלמות, אז קיים שדה F כך ש-R תת חוג של F.
בפרט אם F שדה, אז $F[x]$ הוא תת חוג של שדה.

חילוק:

הגדרה: יהי R חוג עם 1. יהי $a\in R$, איבר $b\in R$ נקרא הופכי של a, אם $ab=1=ba$.

אם הופכי קיים אז הוא יחיד:

נניח שגם $ac=1=ca$, אז $b=b1=b(ac)=(ba)c=1\cdot c=c$.

ואז ההופכי של a מסומן a^{-1}. a נקרא הפיך, אם יש לו הופכי.

תרגיל: יהי R חוג עם יחידה, ויהיו $f,g\in R[x]$ שונים מ-0. אם המקדם העליון של g הפיך אז $\deg(f\cdot g)=\deg(f)+\deg(g)$

משפט: (חילוק עם שארית).

יהי R חוג עם 1, $f,g\in R[x]$, $b_i\in R$, $g=b_mx^m+\dots+b_1x+b_0$

b_m הפיך, אז: (א) קיימים $q,r\in R[x]$ יחידים כך ש- $\deg r<\deg g=m$, $f=gq+r$

(ב) קיימים $q',r'\in R[x]$ יחידים כך ש- $\deg r'<\deg g=m$, $f=q'g+r'$

הוכחה של א':

<u>קיום</u>: באינדוקציה על $\deg f$.

אם $\deg f < m$, ניקח $q=0$, $r=f$

נניח כי $n := \deg f \geq m$, אז $f = a_n x^n + \dots + a_0$, $(a_n \neq 0)$

ואנחנו מניחים שהטענה נכונה לפולינומים ממעלה $< n$.

אז $f = g(b_m^{-1} a_n x^{n-m}) + f_1$

כאשר,
$$f_1 = f - g(b_m^{-1} a_n x^{n-m}) =$$
$$= (a_n x^n + \dots + a_0) - (b_m b_m^{-1} a_n x^{n-m+m} + \dots)$$
$$= (a_n x^n + \dots) - (a_n x^n + \dots)$$

ולכן $\deg f_1 < n$.

ולכן לפי הנחת האינדוקציה יש $q_1, r \in R[x]$ כך ש-

$\deg r < m$, $f_1 = g q_1 + r$, אז,
$$f = g(b_m^{-1} a_n x^{n-m}) + g q_1 + r$$
$$= g(\underbrace{b_m^{-1} a_n x^{n-m} + q_1}_{=q}) + r = gq + r$$

<u>יחידות</u>: נניח ש- $f = gq + r = gq_0 + r_0$, $\deg r, \deg r_0 < m$.
$$g(q_0 - q) = r - r_0$$

אם $q_0 = q$, אז גם $r = r_0$.

אם $q_0 \neq q$ אז $q_0 - q \neq 0$, לפי התרגיל:
$$m \leq \deg g + \deg(q_0 - q) = \deg g \cdot (q_0 - q) = \deg(r - r_0) < m$$

וזו סתירה. ∎

<u>מסקנה</u>:

יהי R חוג עם 1, יהי $\alpha \in R$, ויהי $f \in R[x]$

אז $f(\alpha) = 0$ אם ורק אם קיים $q \in R[x]$ כך ש- $f(x) = q(x) \cdot (x - \alpha)$

<u>הוכחה</u>: לפי הטענה יש $q', r' \in R[x]$ יחידים, כך ש-

(*) $f = q'(x) \cdot (x - \alpha) + r'$, $\deg r' < \deg(x - \alpha) = 1$

אבל $\deg r' < 1$, פירוש, $\deg r' \leq 0$, כלומר $r' \in R$ (ולכן $r'(\alpha) = r'$).

נציב α בשני האגפים של (*). $f(\alpha) = q'(\alpha - \alpha) + r' = r'$ (כאן השתמשנו בכך

ש-α מתחלף עם המקדמים של $x-\alpha$, ולכן ההצבה שומרת כפל).

ולכן $f=q'(x)(x-\alpha)+f(\alpha)$

כעת אם $f(\alpha)=0$ אז זו ההצגה המבוקשת,

להיפך, אם $q\in R[x]$ כך ש-

$f=q(x)(x-\alpha)$ אזי

לפי היחידות בטענה, $q=q'$ ו- $f(\alpha)=0$ <u>מש"ל</u>.

הגדרה: יהי R חוג חילופי, ויהיו $a,b\in R$.

נאמר ש-"a מחלק את b" (ונסמן $a|b$),

אם יש $c\in R$ כך ש- $b=a\cdot c$.

מסקנה: יהי F שדה, יהי $\alpha\in F$, ויהי $f\in F[x]$.

אז α שורש של f אמ"מ f מתחלק ב- $x-\alpha$ בחוג $F[x]$. $(x-\alpha|f)$

מסקנה: יהי F שדה, $0\neq f\in F[x]$, ממעלה n, אז ל- f לכל היותר n שורשים שונים ב- F.

הוכחה: באינדוקציה על n.

אם $n=0$, אז $f\neq 0$ קבוע ב- F ואין לו שורשים.

נניח $n>0$ ונניח נכונות עבור פולינומים ממעלה $n-1$.

אם ל- f אין שורשים - סיימנו.

אם ל- f יש שורש $\alpha\in F$, אז לפי המסקנה $f=(x-\alpha)g$,

כאשר $g\in F[x]$. אז $n=\deg f=\deg(x-\alpha)+\deg g$

ולכן $\deg g=n-1$.

לפי הנחת האינדוקציה, ל- g יש לכל היותר $n-1$ שורשים שונים ב- F.

אבל לכל $\beta\in F$ מתקיים $f(\beta)=(\alpha-\beta)g(\beta)$, לכן β שורש של f

אמ"מ β שורש של g או $\alpha=\beta$.

לכן השורשים של f הם α והשורשים של g, סה"כ יש לכל היותר n שורשים שונים ב- F.

מסקנה: יהי F שדה, יהי $f\in F[x]$ ממעלה $n\geq 0$ ויהי $0\neq c\in F$ המקדם העליון של f. נניח של-f יש n שורשים שונים $\alpha_1,\dots,\alpha_n$ ב-F.

אז- $f=c(x-\alpha_1)\dots(x-\alpha_n)$

הוכחה: $g=c(x-\alpha_1)\dots(x-\alpha_n)$

כיוון ש- $\deg g=n$, והמקדם העליון של g הוא c.

לכן $f-g\in F[x]$ ממעלה קטנה מ-n.

אבל $\alpha_1,\dots,\alpha_n$ שורשים של $f-g$, כי:

$(f-g)(\alpha_i)=f(\alpha_i)-g(\alpha_i)=0-0=0$.

לפי המסקנה הקודמת, $f-g=0$ ולכן $f=g$. ∎

הגדרה: שדה F נקרא סגור אלגברית, אם לכל $f\in F[x]$ ממעלה $n>0$ יש שורש (לפחות אחד) ב-F.

משל: $\mathbb{C}$ סגור אלגברית.

$\mathbb{Q},\mathbb{R}$ אינם סגורים אלגברית, כי ל- $1+x^2$ אין בהם שורש.

משפט: יהי F שדה סגור אלגברית ויהי $f\in F[x]$ ממעלה $n\geq 0$ אזי קיימים $\alpha_1,\dots,\alpha_n\in F$ (לא בהכרח שונים!) וקיים $0\neq c\in F$, כך ש-

$f=c(x-\alpha_1)\dots(x-\alpha_n)$

הוכחה: באינדוקציה על n; אם $n=0$ אז $f=c\in F$ $(c\neq 0)$ את הטענה המבוקשת. נניח $n>0$ ונניח נכונות לפולינומים ממעלה $n-1$.

F סגור אלגברית, לכן יש $\alpha_n\in F$ כך ש- $f(\alpha_n)=0$.

לכן $x-\alpha_n \mid f$. כלומר, יש $g\in F[x]$ כך ש-

$f=g(x)(x-\alpha_n)$

כיוון ש- $\deg g=n-1$. לפי הנחת האינדוקציה יש $\alpha_1,\dots,\alpha_{n-1}\in F$, ו- $0\neq c\in F$, כך ש- $g=c(x-\alpha_1)\dots(x-\alpha_n)$

מכאן

$f=c(x-\alpha_1)\dots(x-\alpha_{n-1})(x-\alpha_n)$ מש"ל.

* דוגמא להומומורפיזם של חוגים:

יהי R חוג,

$$\varphi : \underbrace{M_n(R)[x]}_{\text{פולינומים שהמקדמים שלהם הן מטריצות.}} \longrightarrow \underbrace{M_n(R[x])}_{\text{מטריצות שהאיברים בהן הם פולינומים.}}$$

ע"י:
$$\left(\varphi\left(\sum_{\mu=0}^{\infty} A_\mu x^\mu\right)\right)_{ij} = \sum_{\mu=0}^{\infty} (A_\mu)_{ij} x^\mu \qquad (A_\mu \in M_n(R))$$

למשל:
$$\varphi\left(\begin{pmatrix} 2 & 1 \\ -3 & 0 \end{pmatrix} + \begin{pmatrix} 7 & 0 \\ 1 & 1 \end{pmatrix} x + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x^2 \right) = \begin{pmatrix} 2+7x & 1+x^2 \\ -3+x & x \end{pmatrix}$$

טענה: אז φ איזומורפיזם.

הוכחה: (1) φ חח"ע: נניח:
$$\varphi\left(\sum_{\mu=0}^{\infty} A_\mu x^\mu\right) = \varphi\left(\sum_{\mu=0}^{\infty} B_\mu x^\mu\right)$$

אז לכל i,j:
$$\sum_{\mu=0}^{\infty} (A_\mu)_{ij} x^\mu = \sum_{\mu=0}^{\infty} (B_\mu)_{ij} x^\mu$$

לכן, לכל i,j ולכל μ:
$$(A_\mu)_{ij} = (B_\mu)_{ij}$$

משמע $A_\mu = B_\mu$ לכל μ.

לכן:
$$\sum A_\mu x^\mu = \sum B_\mu x^\mu.$$