5.5.08 (1)

אלגברה לינארית 2 - שיעור 1

דן הרן ת.ז. 6408849
שחיבר 203
havan@post.tau.ac.il

חוגים

<u>הגדרה:</u> חוג הוא קבוצה R שעליה מוגדרות 2 פעולות: חיבור $(+)$ וכפל $(\cdot$, או ללא סימון$)$ אשר מקיימות את החוקים הבאים:

(ח 0) סגירות החיבור - לכל $a,b\in R$ יש $c\in R$ יחיד כך ש $a+b=c$.

(ח 1) חוק הקיבוץ: $(a+b)+c=a+(b+c)$, לכל $a,b,c\in R$

(ח 2) קיום איבר האפס: יש איבר $0\in R$ יחיד כך ש- $a+0=a=0+a$ לכל $a\in R$

(ח 3) קיום נגדי: לכל $a\in R$ יש $-a\in R$ יחיד כך ש $a+(-a)=0=(-a)+a$

(ח 4) חוק החילוף: $a+b=b+a$ לכל $a,b\in R$.

(כ 0) סגירות הכפל - לכל $a,b\in R$ יש $c\in R$ יחיד כך ש $a\cdot b=c$.

(כ 1) חוק הקיבוץ: $(a\cdot b)c=a\cdot(b\cdot c)$ לכל $a,b,c\in R$,

(3) פילוג $a(b+c)=ab+ac$ לכל $a,b,c\in R$

$(b+c)a=ba+ca$

<u>הגדרה:</u> חוג R יקרא <u>חוג עם יחידה</u> אם יש איבר $1\in R$ כך ש- $a=a\cdot 1=1\cdot a$ לכל $a\in R$.

חוג R יקרא <u>חילופי</u>, אם $ab=ba$ לכל $a,b\in R$.
חוג R נקרא <u>תחום שלמות</u> אם הוא חילופי, עם 1, ולכל $a,b\in R$ שונים מ-0, גם $ab\neq 0$.

<u>דוגמאות:</u> (1) $\mathbb{Z}$ - תחום שלמות

(2) $2\cdot\mathbb{Z}$ $(\mathbb{Z}_{even})$ - חוג חילופי, ללא 1.

(3) כל שדה הוא חוג ואפילו תחום שלמות (שדה הוא חוג חילופי עם יחידה ולכל $0\neq a\in R$ יש הופכי - ולכן גם תמיד אם $a,b\neq 0 \Rightarrow ab\neq 0$ כי נוכל לכפול בהופכי של a ולקבל ש $b=0$).
בפרט $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ חוגים.
ראשוני

(4) $\mathbb{Z}/n\mathbb{Z}$ = חוג השארית לאחר חילוק ב-n.

(למשל, אם $n=7$ אז $[2]\cdot[6]=[5]=[-2]$, $[2]+[6]=[1]$)

לגבי חוג חילופי עם יחידה, הוא תחום שלמות $\Leftrightarrow$ הוא שדה $\Leftrightarrow$ n ראשוני
(זה משפט שלא נוכיח כעת).

(5) אם R חוג, יהי $R[X]=\{a_0X^0+a_1X^1+a_2X^2+\dots \mid a_1,a_2,\ldots\in R$ כמעט כולם 0$\}$

כלומר, $R[X]=\{\sum_{i=0}^{\infty} a_iX^i \mid a_1,a_2\ldots\in R$ כמעט כולם 0$\}$

נגדיר חיבור וכפל ב- $R[X]$

$$\sum_{i=0}^{\infty} a_iX^i+\sum_{i=0}^{\infty} b_iX^i=\sum_{i=0}^{\infty}(a_i+b_i)X^i$$

$$\left(\sum_{i=0}^{\infty} a_iX^i\right)\left(\sum_{i=0}^{\infty} b_iX^i\right)=\sum_{k=0}^{\infty} C_kX^k$$ (כאשר $C_k=\sum_{i+j=k} a_ib_j$)

<u>נשים לב</u>: אם k מספיק גדול ו- $i+j=k$ אז $a_i=0$ או $b_j=0$ ולכן $a_ib_j=0$ (תמיד).

$R[X]$ חוג, נקרא <u>חוג פולינומים מעל R</u>. אם R חילופי אז גם $R[X]$ חילופי.

<u>הערה</u>: אם יש $1\in R$ אז $X:=0X^0+1\cdot X^1+0\cdot X^2+\dots$ מתחלף בכפל עם כל איברי $R[X]$ (כי $1,0$ מתחלפים בכפל עם כל איברי R). (שאר מקדמי הפולינום X)

<u>סימון</u>: בדר"כ מזניחים בכתיבת הפולינום מחוברים מהצורה $0\cdot X^i$, רושמים X^i במקום $1\cdot X^i$ ורושמים a_0 במקום $a_0\cdot X^0$. לכן פולינום נראה כך: $2+3X+7X^3$.

שימו לב $R[x]$ חוג, איבר ה-0 שלו הוא $0\cdot X^0+0\cdot X^1+0\cdot X^2+\dots=0$ (פולינום ה-0).
לכל $f\in R[X]$ מגדירים מעלה $\deg f$ כך:

אם $f=\sum a_iX^i\neq 0$ אז $\deg f=\max\{i \mid a_i\neq 0\}$
ואם $\deg 0=-\infty$.

<u>דוגמאות</u>: $\deg(1+X^3)=3$, $\deg(8)=0$.

<u>קל לראות</u>: $\deg(f+g)\le\max(\deg f,\deg g)$

$\deg(f\cdot g)\le\deg f+\deg g$ ⊛ אם R הוא תחום שלמות אז יש הסימן מחייב שוויון. לכן, במקרה כזה, גם $R[X]$ תחום שלמות.

<u>ספרות</u>: אלגברה לינארית של האוניברסיטה הפתוחה
" של סדרת שאום.
מתמטיקה של סדרת שאום.
אלגברה א': עמי צבר

(6) אם R חוג, אז $M_n(R)$ חוג המטריצות מסדר $n\times n$ מעל R עם פעולות החיבור $(A+B)_{ij}=(A)_{ij}+(B)_{ij}$

$$(AB)_{ij}=\sum_{k=1}^{n}(A)_{ik}(B)_{kj}$$

בדר"כ $M_n(R)$ אינו חילופי, אפילו אם R חילופי. אם R חוג עם 1 אז יש יחידה ב- $M_n(R)$ והוא $I=I_n=\begin{pmatrix}1&&0\\&\ddots&\\0&&1\end{pmatrix}$

בפרט: $M_n(R)[X]$ הוא חוג שבדר"כ אינו חילופי.

5.5.08 ③ אלגברה לינארית 2 - שיעור 1

(ד) אם V מ"ו ממימד סופי מעל שדה F אז $L(V,V)$ (= קבוצת ההעתקות הלינאריות מ- V ל- V) היא חוג ביחס לכפל = הרכבה. יש בו יחידה (העתקת הזהות), הוא בדר"כ לא חילופי.

<u>הגדרה:</u> יהיו R,S שני חוגים. העתקה $\varphi: R\to S$ נקראית הומומורפיזם אם היא שומרת חיבור וכפל. כלומר $\varphi(a+b)=\varphi(a)+\varphi(b)$ לכל $a,b\in R$. וכן $\varphi(ab)=\varphi(a)\cdot\varphi(b)$ לכל $a,b\in R$.

הומומורפיזם שהינו חח"ע ועל הינו איזומורפיזם.

<u>הערה:</u> אם φ הומומורפיזם $\varphi(0)=0$, אכן $\varphi(0)=\varphi(0+0)=\varphi(0)+\varphi(0)$. מוסיפים $(-\varphi(0))$ לשני האגפים מימין:

$$\varphi(0)+(-\varphi(0)) = 0 = \varphi(0)+\varphi(0)+(-\varphi(0)) = \varphi(0)$$

לא תמיד $\varphi(1)=1$. למשל $\varphi:\mathbb{Z}\to\mathbb{Z}$ המוגדרת $\varphi(k)=0$ לכל $k\in\mathbb{Z}$ היא הומומורפיזם.

<u>הגדרה:</u> <u>הומומורפיזם R חוגים עם יחידה</u> הוא כזה שמקיים $1\to 1$.

<u>דוגמאות:</u> (א) יהי V מ"ו ממימד n מעל שדה F ויהי B בסיס. העתקה $\varphi: L(V,V)\to M_n(F)$ הנתונה ע"י $\varphi(T)=[T]_B^B$ היא איזומורפיזם של חוגים.

(ב) יהי R חוג ויהי $\alpha\in R$. אם $f=\sum_{i=0}^{\infty} a_i x^i\in R[x]$ נגדיר $f(\alpha)=\sum_{i=0}^{\infty} a_i\alpha^i = a_0+a_1\alpha+a_2\alpha^2+\dots\in R$ (הצבה של α ב- f).

* נגדיר העתקה $\varphi: R[x]\to R$ כך $\varphi(f)=f(\alpha)$. האם φ הומומורפיזם.

(1) φ שומרת חיבור: יהיו $g=\sum_{i=0}^{\infty} b_i x^i$, $f=\sum_{i=0}^{\infty} a_i x^i$

$$\varphi(f+g) = \varphi\left(\sum (a_i+b_i)x^i\right) = \sum_{i=0}^{\infty}(a_i+b_i)\alpha^i = \sum_{i=0}^{\infty}\left[(a_i\alpha^i)+(b_i\alpha^i)\right] =$$
$$= \sum_{i=0}^{\infty} a_i\alpha^i + \sum_{i=0}^{\infty} b_i\alpha^i = \varphi(f)+\varphi(g)$$

(2) אם α מתחלף בכפל עם כל מקדמי g אז $\varphi(fg)=\varphi(f)\cdot\varphi(g)$:
יהיו
$$f=\sum a_i x^i \qquad g=\sum b_j x^j$$

$$\varphi(f\cdot g) = \varphi\left(\sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i b_j\right)x^k\right) = \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i b_j\right)\alpha^k = \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i b_j\alpha_k\right)$$

$$\varphi(f)\cdot\varphi(g) = \left(\sum_{i=0}^{\infty} a_i\alpha^i\right)\left(\sum_{j=0}^{\infty} b_j\alpha^j\right) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_i\alpha^i b_j\alpha^j = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_i b_j\alpha^{i+j}$$

$$= \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i b_j\alpha^k\right)$$

הערה, אם α מתחלף בכפל עם כל איברי R, אז φ הומומורפיזם.
(אם יש $a\in R$ כך ש- $a\alpha\neq\alpha a$ אז

$$\left(\ \varphi(X\cdot a)=\varphi(aX)=a\cdot\alpha\neq\alpha\cdot a=\varphi(X)\cdot\varphi(a)\right.$$

<u>הגדרה:</u> יהי R חוג. תת קבוצה $S\subseteq R$ תקרא תת חוג אם:

(1) $0\in S$

(2) אם $a,b\in S$ אז $ab,\ \underbrace{a-b}_{a+(-b)}\in S$

בפרט אם $a,b\in S$ אז $-a\in S$ כי $-a=0+(-a)\in S$

$a,b\in S$ אז $a+b\in S$ כי $-b\in S$ ולכן $a+b=a-(-b)\in S$

בפרט S הוא חוג, ביחס לפעולות ב-R.

<u>דוגמה:</u> $\mathbb{Z}$ תת חוג של $\mathbb{Q}$, וכן $\mathbb{Q}$ תת חוג של $\mathbb{C}$.

אם R חוג, $R[x]\supseteq S=\{a_0+0x+0x^2+\dots|a_0\in R\}$.

זה בעצם כתיבה מסובכת של R, כלומר, הוא גם איזומורפי ל-R
[illegible] ע"י $a_0\to a_0+0\cdot x+\dots$ ולכן אומרים ש-R תת חוג של $R[x]$.