הרצאה 2

תרגיל הבית: בחוג, $a+b=b+a$ נובע משאר האקסיומות.

<u>הגדרה</u> חוג-לב (near-ring) הינו כמו חוג-בלי-יחידה

אלא ש: 1) לא דורשים חילופיות של החיבור.

2) דורשים רק פילוג מימין $(a+b)c=ac+bc$

אין לנו משמאל (או להיפך)

כל חוג (בלי יחידה) הינו חוג-לב.

<u>דוגמא</u> G חבורה כלשהי. $N=\{f: G\to G\}$ פונקציות

פעולה על G

$$(f_1+f_2)(g) = f_1(g) \cdot f_2(g)$$

כפל: הרכבה.

אז 1) N מקיים פילוג מימין אך לא משמאל,

כמו שראינו בשיעור הקודם.

2) החיבור ב-N חילופי $\Leftrightarrow$ G אבלית.

<u>הגדרה</u> יהי R חוג. תת-קבוצה $\emptyset\neq S\subseteq R$ נקראת

תת-חוג אם: 1) לכל $a,b\in S$, גם $a-b\in S$.

(סגירות לחיסור)

$S\leq R$ 2) לכל $a,b\in S$, גם $ab\in S$

(סגירות לכפל)

3) $1_R\in S$.

<u>הגדרה</u> יהי R חוג בלי יחידה. תת-קבוצה $\emptyset\neq S\subseteq R$

סגורה לחיסור ולכפל נקראת תת-חוג-בלי-יחידה.

<u>דוגמאות</u> 1) $R=\mathbb{Z}$, $S=n\mathbb{Z}$, $n\geq 1$.

S תמיד תת-חב"י. (חב"י = חוג בלי יחידה)

rng = חג

S תת-חוג רק כאשר $n=1 \Leftarrow R=S$.

__הערה__ כל תת-חוג-בלי-יחידה של R, הינו תת-חבורה של $(R,+)$.

כל המבנים של $\mathbb{Z}$ הן $n\mathbb{Z}$, לכן גם מצאנו את כל התת-חוגים-בלי-יחידה של $\mathbb{Z}$.

2) R חוג עצמו, לא-טריוויאלי, $S=\{0\}$ תת-חב"י לא תת-חוג.

3) R חוג, $A=M_n(R)$

$$B=T_n(R)=\left\{\begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix}\right\}$$ תת-חוג.

4) $R[x]$ חוג של פולינומים. נבחר $a\in R$

$S=\{f\in R[x]:\ f(a)=0\}$ [תרגיל: כדי להוכיח ש-S סגור לכפל, צריך $a\in Z(R)$] ($\overline{a\in Z(R)}$)

תת-חוג-בלי-יחידה, אף פעם לא תת-חוג (אם R לא-טריוויאלי)

5) S קבוצה, $R=\mathcal{P}(S)=\{A:\ A\subseteq S\}$

$A+B=(A\setminus B)\cup(B\setminus A)$

$AB=A\cap B$

תהי $B\subseteq S$ תת-קבוצה.

$R'=\mathcal{P}(B)=\{A\subseteq B\subseteq S\}$

אם $B\subsetneq S$, אזי זה תת-חוג-בלי-יחידה אך לא תת-חוג.

R' הינו חוג (האיבר $B\in R'$ הינו יחידה בכללית)

לכן: תת-חוג של R $\not\Leftrightarrow$ תת-קבוצה שהיא חוג תחת חיבור וכפל של R

6) שוב, $R=P(S)$ שוב, יהי $B\subsetneq S$.

$$R'=\{A\subseteq S \mid B\subseteq A \text{ או } A\cap B=\emptyset\}$$

אזי R' תת-חוג.

7) R חוג כל שהוא. המרכז של R

$$Z(R)=\{a\in R \mid ar=ra \text{ לכל } r\in R\}$$

צ"ל תת-חוג

1) $a,b\in Z(R)$

$$(a-b)r \overset{\text{תוכיחו!}}{=} ar-br=ra-rb=r(a-b)$$

לכן $a-b\in Z(R)$.

2) $(ab)r=a(br)=a(rb)=(ar)b=(ra)b=r(ab)$

3) כמובן, $1\in Z(R)$

8) יהי R חוג, $a\in R$. המרכז של a הינו

$C_R(a)=\{b\in R : ab=ba\}$ תת-חוג.

9) $$Z(R)=\bigcap_{a\in R} C_R(a)$$

באופן יותר כללי. אם $S,T\le R$ תת-חוגים,

אזי $S\cap T\le R$ תת-חוג

לכל אוסף $\{S_i\}_{i\in I}$, של תת-חוגים,

$\bigcap_{i\in I} S_i$ תת-חוג.

הגדרה. יהיו R,S שני חוגים. הומומורפיזם של חוגים

הינו העתקה $f:R\to S$ כך ש-

1) $f(a+b)=f(a)+f(b)$ לכל $a,b\in R$

+ של R חיבור של S

2) $f(a\cdot b)=f(a)\cdot f(b)$ לכל $a,b\in R$.

3) $f(1_R)=1_S$.

<u>הגדרה</u> R,S חוגים בלי יחידה. הומו' של חוגים בלי יחידה הינו העתקה $f:R\to S$ שמקיימת 1, 2.

<u>דוגמאות</u> 1) יהי R חוג בלי יחידה, $S\subseteq R$ תת-חוג. ההכלה $i:S\hookrightarrow R$ הינו הומו' של חוגים בלי יחידה.

בדוגמא 5 למעלה $i:P(A)\hookrightarrow P(S)$ <u>אינו</u> הומו' של חוגים, למרות שגם $P(A)$ וגם $P(S)$ חוגים.

2) יהי R חוג כלשהו. $f:\mathbb{Z}\to R$

$$f(n)=\underbrace{1_R+1_R+\dots+1_R}_{n \text{ פעמים}}$$

הינו ההומו' היחיד בין שני החוגים האלה.

מסמן $f(n)=[n]_R$

<u>הגדרה</u> יהי R חוג. המאפיין של R הינו

$\mathbb{N}=\{1,2,3,\dots\}$ $\min\{n\in \mathbb{N} : [n]_R=0_R\} = \text{char } R$

אומרים כי $\text{char } R=0$ אם הקבוצה הנ"ל ריקה.

<u>אבחנה</u> $f:R\to S$ הומו' של חוגים בלי יחידה. אזי $f(0_R)=0_S$, כי $f:(R,+)\to(S,+)$ הומו' של חבורות אבליות.

3) נכון. $f:\mathbb{Z}\to\mathbb{Z}_m$, $m\geq 1$.

$$f(n)=[n]$$

$$\text{char}\ \mathbb{Z}_m = m$$

4) יהי R חוג, $b\in Z(R)$ (נכון, אם R חוג חילופי, $b\in R$ כלשהו) הומ' הצבה.

$$ev_b : R[x]\longrightarrow R$$

$$ev_b(f)=f(b)$$

$$f(x)=\sum_{i=0}^{N} a_i x^i,\qquad f(b)=\sum_{i=0}^{N} a_i b^i\in R$$

זה הומ' של חוגים (תרגיל!)

אם $b\notin Z(R)$, אזי ev_b לא בהכרח מכבד כפל.

אכן, יהי $f=ax$, $a\in R$. $f\cdot f=a^2x^2$

$$ev_b(f)\cdot ev_b(f)= abab \overset{???}{\neq} \underset{aabb}{a^2b^2} = ev_b(f\cdot f)$$

5) $f:R\to S$ הומ' של חוגים. מקבלים הומ' של חוגים

$$f_n : M_n(R)\longrightarrow M_n(S)$$

$$\begin{pmatrix} a_{11} & \cdots & a_{1n}\\ \vdots & & \vdots\\ a_{n1} & \cdots & a_{nn}\end{pmatrix}\longmapsto\begin{pmatrix} f(a_{11}) & \cdots & f(a_{1n})\\ \vdots & & \vdots\\ f(a_{n1}) & \cdots & f(a_{nn})\end{pmatrix}$$

אכן, אקסיומות 1), 2) ברורות. תהיינה $A,B\in M_n(R)$

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

$$(f_n(AB))_{ij} = f\Big(\sum_{k=1}^{n} a_{ik}b_{kj}\Big)=\sum_{k=1}^{n} f(a_{ik})f(b_{kj}) = (f_n(A)\cdot f_n(B))_{ij}$$

לכן, $f_n(AB)=f_n(A)\cdot f_n(B)$

6) יהי $f: G\to H$ הומ' של חבורות. יהי R חוג.

מקבלים הומ' של חוגי חבורה.

$$\varphi: R[G]\longrightarrow R[H]$$

$$\underbrace{\varphi\Big(\sum_{g\in G} a_g\cdot g\Big)}_{\text{סכום סופי}} = \sum_{g\in G} a_g\cdot f(g)\in R[H].$$

<u>הגדרה</u> יהי $f:R\to S$ הומ' של חוגים-בלי-יחידה.

הגרעין של f הינו

$$\ker f=\{a\in R:\ f(a)=0_S\}$$

<u>טענה</u> $\ker f$ הינו תת-חוג-בלי-יחידה.

<u>טענה</u> f חד-חד-ערכי $\Leftrightarrow$ $\ker f=\{0_R\}$

<u>הוכחה</u> $f:(R,+)\to(S,+)$ הומ' של חבורות.

<u>טענה</u> $f:R\to S$ הומ' של חוגים. אזי

$f(R)=\{f(r):\ r\in R\}\subseteq S$ הינו תת-חוג של S.

<u>הוכחה</u> יהיו $a,b\in f(R)$,
$a=f(r_1)$
$b=f(r_2)$

$$a-b=f(r_1-r_2)\Rightarrow a-b\in f(R)$$
$$ab=f(r_1r_2)\Rightarrow ab\in f(R)$$
$$1_S=f(1_R)\Rightarrow 1_S\in f(R).$$

<u>הגדרה</u> יהי R חוג. תת-קבוצה $\emptyset\neq I\subseteq R$ נקראת

אידיאל שמאלי אם:

1) $a+b\in I$ לכל $a,b\in I$.

2) $ra\in I$ לכל $a\in I$ ולכל $\underline{r\in R}$.

I הינה אידיאל ימני אם

1) $a+b\in I$ לכל $a,b\in I$.

2) $ar\in I$ לכל $r\in R$, $a\in I$.

I נקרא אידיאל דו-צדדי (או סתם "אידיאל") אם הוא אידיאל ימני וגם שמאלי.

Dummit, Foote "Abstract Algebra"

L. Rowen, "Groups, Rings, Fields"

L. Rowen "Rin Theory"