חוגים – הרצאה 1

הגדרה חוג בלי יחידה: כמו חוג, אלא לא דורשים את קיום של 1. (rng)

תת-חוג R חוג, $S \subseteq R$ תת-קבוצה היא תת-חוג אם
1) סגורה לחיסור
2) סגורה לכפל
3) $1 \in S$.

S הוא תת-חוג-בלי-יחידה אם 1), 2) מתקיימים.

דוגמאות 1) $R=\mathbb{Z}$ $S=n\mathbb{Z}$, אז S תת-חוג בלי יחידה.
תת-חוג $\iff n=1$.

אבחנה אלה כל התת-חוגים-בלי-יחידה של $\mathbb{Z}$.

2) $R=M_2(\mathbb{R})$ $S=\left\{\begin{pmatrix} a & a \\ b & b \end{pmatrix} : a,b\in\mathbb{R}\right\}$.

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix} - \begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} a-c & a-c \\ b-d & b-d \end{pmatrix}$$

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} a(c+d) & a(c+d) \\ b(c+d) & b(c+d) \end{pmatrix}$$

יהי $\begin{pmatrix} x & x \\ y & y \end{pmatrix} \in S$ כאשר $x+y=1$.

לכל $\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$ לכן $\begin{pmatrix} x & x \\ y & y \end{pmatrix}$ יחידה מימין

לא יחידה משמאל

$$\begin{pmatrix} x & x \\ y & y \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2x & 2x \\ 2y & 2y \end{pmatrix}$$

<u>הגדרה</u> הומומורפיזם של חוגים הינו העתקה $f: R \to S$ כך ש-

1) $f(a+b) = f(a) + f(b)$

2) $f(ab) = f(a)f(b)$

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

הומומורפיזם של חוגי-בלי-יחידה: ללא דרישה 3).

<u>דוגמאות</u> 1) R חוג, S תת-חב׳ שלו (תת-חוג).

ההכלה $f: S \hookrightarrow R$ הינו הומ׳ של חב׳.

2) R חוג כלשהו. קיים הומ׳ יחיד (של חוגים) $f: \mathbb{Z} \to R$.

$f(1) = 1_R$.

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

נסמן $n_R = f(n)$.

טענה: $f:R\to S$ הומ' של חוגים. אזי

1) $f(0_R)=0_S$

2) $f(-a)=-f(a)$ לכל $a\in R$.

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

3) $f:\mathbb{Z}\to\mathbb{Z}_n$

$$f(a)=[a]$$

הגדרה: המאפיין (char R) של R הינו $n\in\mathbb{N}$ המינימלי כך ש- $n_R=0_R$. אם n כזה לא קיים, אומרים $\text{char } R=0$.

$$\text{char } \mathbb{Z}_n=n$$

4) R חוג חילופי. ויהי $b\in R$. הומ' ההצבה:

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

$$a_nx^n+\dots+a_1x+a_0\longmapsto a_nb^n+\dots+a_1b+a_0$$

אם R לא חילופי זה עלול לא לשמור כפל:

$$ev_b(ax)\,ev_b(ax)=abab\overset{?}{=}a^2b^2=ev_b(a^2x^2)$$

ג) $f: R \to S$ הומו' של חוגים.

$$M_n(f): M_n(R) \to M_n(S)$$

$$a_{ij} \in R \qquad \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mapsto \begin{pmatrix} f(a_{11}) & \cdots & f(a_{1n}) \\ \vdots & & \\ f(a_{n1}) & \cdots & f(a_{nn}) \end{pmatrix}$$

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

$$(M_n f(A) M_n f(B))_{ij} = \sum_{k=1}^{n} f(a_{ik}) f(b_{kj}) = f\left(\sum a_{ik} b_{kj}\right) = M_n f(AB)_{ij}.$$

<u>דוגמה</u> $f: \mathbb{Z} \to \mathbb{Z}_p$, p ראשוני: ($\mathbb{Z}_p$ שדה)

$$M_n(f): M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$$

אז $M_n(f)(A)$ הפיכה $\Longleftrightarrow$ $p \nmid \det A$.

ד) אין הומו' של חוגים $f: \mathbb{Z}_n \to \mathbb{Z}$.

<u>הוכחה</u> נניח ש"ש $f([1]) = 1$

$$f([n]) = f([1] + \dots + [1]) = 1 + \dots + 1 = n$$

$$f([0]) = 0$$

f לא מוגדר היטב.

6) $f: R \to S$ הומ' של חוגים בלי יחידה

$f(a)=0_S$ ההומ' הטריוויאלי.

7) $f: \mathbb{C} \to \mathbb{C}$ הצמדה

$f(a+bi)=a-bi$. הומ' של חוגים.

8) R, S חוגים $f(r,s)=r$ $\quad f: R\times S \to R$

$g(r,s)=s$ $\quad g: R\times S \to S$

9) לאו בהכרח קיים $f: R \to R\times S$

<u>הוכחה</u> הרכבה של הומ' של חוגים היא הומ' של חוגים.

$R \longrightarrow R\times S \xrightarrow{g} S$

$R \longrightarrow S$

10) ההומ' האלכסוני

$f: R \to R^n = R\times R\times \cdots \times R$

$f(a) = (a, a, a, \dots, a)$

11)

$$f: R \longrightarrow R\times S$$

$f(r) = (r,0)$ זו הומו' של חוגים בלי יחידה.

12)

$$f_1 : R \to S_1$$

$$f_2 : R \to S_2$$

$$f: R \longrightarrow S_1 \times S_2$$

$$f(a) = (f_1(a), f_2(a))$$

<u>הגדרה</u> הומו' $f: R\to S$ נקרא איזומורפיזם אם הוא חח"ע ועל.

<u>תרגיל</u> $f^{-1}: S \to R$ גם הומו'.

<u>הגדרה</u> יהי $I \subseteq R$ תת-חוג בלי יחידה. I נקרא אידיאל שמאלי אם $ra\in I$ לכל $a\in I$, $r\in R$.

אידיאל ימני $ar\in I$ לכל $a\in I$, $r\in R$.

אידיאל דו-צדדי (אידיאל) אם I אידיאל ימני ושמאלי.

אם R חילופי, אז אידיאל ימני $\Longleftrightarrow$ אידיאל שמאלי.

<u>דמיון</u> אידיאלים $\longleftrightarrow$ תת"ח נורמליות.

טענה יהי $f: R\to S$ הומו' של חוגים (או חוגים בלי יחידה)

נזכיר $\ker f=\{r\in R: f(r)=0_S\}$ הינו אידאל דו-צדדי.

$a\in\ker f,\ r\in R$

$f(ra)=f(r)f(a)=f(r)\cdot 0_S=0_S \Rightarrow ra\in\ker f$

$f(ar)=0_S\cdot f(r)=0_S \Rightarrow ar\in\ker f$.

הגדרה יהי R חוג, $I\subseteq R$ אידאל דו-צדדי.

נגדיר יחס על R: $x,y\in R$

$x\sim y \iff x-y\in I$.

זה יחס שקילות (זה בדיוק היחס של החבורה $(R,+)$ שמגדיר את המחלקות של I).

יהי R/I הקבוצה של מחלקות השקילות.

הגדרה נסמן $a+I\in R/I$ את המחלקה של $a\in R$.

נגדיר חיבור וכפל של מחלקות

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)(b+I)=ab+I.$$

הטענה הפעולות הללו מוגדרות היטב, ו- R/I עם הפעולות הללו הינה חוג.

הוכחה $a_1+I=a_2+I$ $\quad a_2=a_1+c_1$

$b_1+I=b_2+I$ $\quad b_2=a_2+c_2$

$c_1,c_2\in I$

$$a_2+b_2-(a_1+b_1) = \underbrace{(a_2-a_1)+(b_2-b_1)} =$$

חיבור הינו חילופי | $c_1+c_2\in I$ | לכן $(a_2+b_2)+I = (a_1+b_1)+I$.

כמו כן

$$a_2b_2=(a_1+c_1)(b_1+c_2)=$$
$$a_1b_1+\underbrace{c_1b_1+a_1c_2+c_1c_2}_{\in I}$$

$$a_2b_2+I=a_1b_1+I.$$

<u>דוגמא</u> האידיאלים של $\mathbb{Z}$ הם $n\mathbb{Z}$ לכל $0\le n$.

$R=\mathbb{Z}$

$I=n\mathbb{Z}$

$R/I=\mathbb{Z}_n$.

<u>טענה</u> R חוג, I אידיאל. אז $I=R \iff 1\in I$.

<u>דוגמא</u> R חוג, $R, \{0_R\}$ אידיאלים דו-צדדים.

<u>טענה</u> I מכיל איבר הפיך של R $\iff I=R$.

<u>טענה</u> יהי $f:R\to S$ הומו' של חוגים. יהי $s\in f(R)$. יהי $r\in R$ כך ש $f(r)=s$.

אז $f^{-1}(s)=r+(\ker f)$.

<u>הוכחה</u> $a\in f^{-1}(s) \iff f(a)=f(r) \iff f(a-r)=0_s \iff$
$a-r\in \ker f \iff a\in r+(\ker f)$.

משפט האיזומורפיזם הראשון.

יהי $f:R\to S$ הומ' של חוגים. אזי

קיים איזומורפיזם

$$R/(\ker f) \xrightarrow{\sim} f(S)$$

$$r+(\ker f) \longmapsto f(r)$$