# הרצאה 4

## העשרה: דוגמאות של חוגים בלי יחידה ללא אידיאלים מקסימליים

1) תהי $G$ חבורה אבלית כלשהי. ניתן להפוך אותה לחוג בלי יחידה ע"י הכפל $ab=0$ לכל $a,b\in G$.

בחוג כזה, אידיאל $\iff$ תת-חבורה.

ניקח $G=(\mathbb{Q},+)$. לחבורה הזאת אין תת"ח אמיתית מקסימלית. תרגיל: נניח $H\leq G$ תת"ח.

$H\leq G$ תת-חבורה אמיתית. אז יש $n\in\mathbb{N}$ כך ש- $\frac{1}{n}\notin H$, ולכן גם $\frac{1}{n^a}\notin H$ לכל $a\in\mathbb{N}$.

ניקח $H\subsetneq\langle H,\frac{1}{n}\rangle\subsetneq G$.

לכן, לחוג $\mathbb{Q}$ עם כפל אפס, אין אידיאלים מקסימליים.

2)
$$S=\left\{\frac{f(x)}{g(x)}:\ f,g\in\mathbb{R}[x],\ \underset{\text{ל-}g\text{ איבר חופשי לא אפס}}{g(0)\neq 0}\right\}$$

חיבור וכפל רגילים של פונקציות.

תרגיל:
$$R=\left\{\frac{f(x)}{g(x)}\in S:\ f(0)=0\right\}\lhd S$$

$R$ הינו האידיאל המקסימלי היחיד של $S$, כי כל איבר $\frac{f}{g}\in S\setminus R$ הינו הפיך).

אבחנה: $R$ אידיאל, לכן חוג בלי יחידה, ואין לו אידיאלים מקסימליים.

חוגים לבונית הרגילה:

<u>הגדרה</u> $R$ חוג בלי יחידה, $I \triangleleft R$ אידיאל דו-צדדי.

הגדרנו יחס שקילות על $R$: $r \sim s \iff r-s \in I$.

$R/I$ הקבוצה של מחלקות השקילות, שכולן מן הצורה $r+I$ כאשר $r$ הינו נציג של המחלקה.

הגדרנו חיבור וכפל של מחלקות

$$[r] = r+I$$
$$[r]+[s] = [r+s]$$
$$[r]\cdot[s] = [rs]$$

זה נותן ל-$R/I$ מבנה של חוג בלי יחידה.

אם $R$ היה חוג, אזי $[1]=1+I$ הינה איבר יחידה של $R/I$, לכן $R/I$ גם חוג.

<u>טענה</u> יהי $f: R \to S$ הומ' של חוגים בלי יחידה. הוכחנו $\ker f = \{r \in R : f(r) = 0_S\} \triangleleft R$.

יהי $r \in R$, יהי $s = f(r)$. אזי

$$f^{-1}(s) = \{x \in R : f(x) = s\} = r + (\ker f).$$

<u>הוכחה</u> יהי $x \in r+(\ker f)$, אזי $x \sim r \Rightarrow x - r \in \ker f \Rightarrow 0 = f(x-r) = f(x) - f(r) \Rightarrow f(x) = f(r) = s \Rightarrow x \in f^{-1}(s)$.

הכיוון השני: יהי $x \in f^{-1}(s)$ אזי $f(x) = s = f(r)$,

לכן $f(x-r)=f(x)-f(r)=0 \Leftarrow x-r\in\ker f \Leftarrow$

$x\sim r \Leftarrow x+(\ker f)=r+(\ker f) \Leftarrow x\in r+(\ker f)$.

<u>משפט</u> (משפט האיזומורפיזם הראשון עבור חוגים).

יהי $f:R\to S$ הומומורפיזם של חוגים

בלי יחידה. אזי $f(R)=\{s\in S: \exists r\in R,\ s=f(r)\}$ התמונה,

שהיא תת-חבורה של $S$. אזי

$$R/(\ker f)\simeq f(R).$$

אם $f$ הומו' של חוגים, אזי ↑ הינו איזו' של <u>חוגים</u>.

<u>הוכחה</u> נגדיר העתקה

$$\varphi: R/(\ker f)\longrightarrow f(R)$$

$$\varphi(r+\ker f)=f(r)$$

$\varphi$ מוגדרת היטב כי, לפי הטענה הקודמת,

אם $x+\ker f=r+\ker f$, אז $f(x)=f(r)$.

אני טוען כי $\varphi$ הינו הומו' של חב"י:

1) $\varphi((r+\ker f)(x+\ker f))=$

$\varphi(rx+\ker f)=f(rx)\underset{f\text{ הומו'}}{=}f(r)\cdot f(x)=\varphi(r+\ker f)\varphi(x+\ker f)$

2) $\varphi$ מכבדת חיבור באופן דומה.

<u>הערה</u> אם $f$ הינו הומו' של חוגים

($R,S$ חוגים, $f(1_R)=1_S$) אזי $\varphi(1_{R/\ker f})=$

$\varphi(1+\ker f)=f(1)=1$

ולכן $\varphi$ הומ' של חוגים.
נשאר לבדוק כי $\varphi$ איזו':

1) $\varphi$ על, ברור ($s\in f(R)$ $\Leftarrow$ קיים $r\in R$ כך ש- $s=f(r)$ $\Leftarrow$ $s=\varphi(r+\ker f)$).

2) $\varphi$ חח"ע: $\varphi(r+\ker f)=\varphi(x+\ker f)$ $\Leftarrow$ $f(r)=f(x)$ $\Leftarrow$ $r+\ker f = x+\ker f$ לפי הטענה הקודמת.

<u>הגדרה</u> 1) יהי $R$ חוג, ויהיו $I,J$ אידיאלים שמאליים/ימניים/דו-צדדיים. אפשר להגדיר אידיאל שמאלי/ימני/דו-צדדי

$$I+J=\{i+j : i\in I,\ j\in J\}$$

<u>הערה</u> $I+J$ הינו האידיאל השמאלי/ימני/דו-צדדי המינימלי שמכיל את $I\cup J$.

2) יהי $R$ חוג חילופי, ויהיו $I,J\triangleleft R$.

נגדיר
$$IJ=\Big\{\sum_{k=1}^{n} i_k j_k : i_k\in I,\ j_k\in J,\ \underset{\substack{\Uparrow\\ \text{הסכום הינו סופי}}}{n\in\mathbb{N}}\Big\}\underset{\text{תרגיל}}{\triangleleft} R$$

$$r\Big(\sum i_k j_k\Big)=\sum \underbrace{(r i_k)}_{\in I} j_k \in IJ.$$

<u>הערה</u> לא באמת צריך חילופיות. מספיק:
$I$ אידיאל שמאלי $\Leftarrow$ $IJ$ אידיאל שמאלי.
$J$ ימני $\Leftarrow$ $IJ$ ימני.

**הגדרה** אידיאלים $I,J$ של $R$ נקראים קו-מקסימליים אם $I+J=R$.

**דוגמאות** $R=\mathbb{Z}$, $I=n\mathbb{Z}$, $J=m\mathbb{Z}$

$$IJ = nm\mathbb{Z}$$

**תרגיל** $I+J = g\mathbb{Z}$, $g=\gcd(n,m)$

[אכן, $n\mathbb{Z} \subseteq k\mathbb{Z} \iff k|n$. עבור $kn\in\mathbb{Z}$.]

לכן, $n\mathbb{Z}, m\mathbb{Z}$ קו-מקסימליים $\iff$ $n,m$ זרים.

**משפט השאריות הסיני** יהי $R$ חוג חילופי. יהיו $I,J \triangleleft R$ אידיאלים קו-מקסימליים. אזי יש איזו' של חוגים:

$$R/IJ \simeq R/I \times R/J$$

**הוכחה** נגדיר הומו' של חוגים:

$$f: R \longrightarrow R/I \times R/J$$

$$f(r) = (r+I,\ r+J).$$

קודם כל נראה מהו $\ker f$.

יהי $r\in\ker f \iff (r+I, r+J) = (0+I, 0+J)$

$\iff r\in I$ וגם $r\in J \iff r\in I\cap J$.

לכן $\ker f = I\cap J$. לפי משפט האיזו' הראשון

$$R/I\cap J \simeq \mathrm{Im}(f) = f(R) \qquad (*)$$

כדי להשלים את ההוכחה צריך להוכיח
שני דברים:

א) $f$ על.

ב) $I \cap J = IJ$

אזי (*) מתפרק ל- $R/IJ \simeq R/I \times R/J$
וזה מה שאנחנו רוצים.

<u>הוכחות</u> א) לפי הנתון, $1 \in R = I + J$,
לכן קיימים $i \in I,\ j \in J$ כך ש- $i + j = 1$.

אזי: $i \in I \Rightarrow i + I = 0 + I$

$i + j = 1 \Rightarrow i + J = 1 + J$

לכן $f(i) = (0 + I,\ 1 + J)$

כמו כן $f(j) = (1 + I,\ 0 + J)$

יהי $(r_1 + I,\ r_2 + J) \in R/I \times R/J$.

אזי
$$f(r_1 j + r_2 i) = f(r_1)f(j) + f(r_2)f(i) = (r_1 + I,\ 0 + J) + (0 + I,\ r_2 + J) = (r_1 + I,\ r_2 + J)$$

לכן $f$ על.

ב) צריך עדיין להוכיח $IJ = I \cap J$.

יהי $x \in IJ$ אזי $x = \sum \underbrace{i_k j_k}_{I \cap J} \in \underbrace{I \cap J}_{I \cap J}$

כי אידיאל ולכן סגור לחיבור.

קיבלנו $J\cap I\subseteq IJ$, זה נכון לכל זוג
של אידיאלים דו-צדדיים,
בכל חב״י.

נוכיח את ההכלה השניה: יהי $x\in J\cap I$.

$$x = x\cdot 1 = x(i+j) = \underbrace{xi}_{\substack{i\in I \\ x\in I\cap J\subseteq J}} + \underbrace{xj}_{\substack{j\in J \\ x\in I}} \in IJ$$

כי $I,J$ קו-מקסימליים

לכן $IJ\subseteq J\cap I$, וסיימנו את
ההוכחה של משפט השאריות הסיני.

דוגמאות נוספות של חוגי מנה:
(חב״י)

1) $\mathbb{Z}/n\mathbb{Z}$

2) $R=S[x]$, $S$ חב״י כלשהו.
$I=x^nR$ עבור $n\geq 1$ טבעי.

$I$ הינו אידיאל דו צדדי. אכן, $x^n$
מתחלף גם עם מקדמים וגם עם
חזקות של $x$. לכן $x^n\in Z(R)$, לכן

$$x^nR = \{f(x)\cdot x^n\}_{f(x)\in R} = \{x^n\cdot f(x)\} = Rx^n.$$

$x^nR = \{$ פולינומים מן הצורה $\sum_{k=n}^{N} s_kx^k :$ $N\in\mathbb{N}$, $s_k\in S\}$

R חוג כלשהו. אם $a \in Z(R)$, אזי

האידיאל $aR = Ra$ דו-צדדי. נסמן אותו $(a)$.

מהו חוג המנה $R/I = S[x]/(x^n)$

שני פולינומים $f(x), g(x) \in R$ שייכים לאותה

מחלקה מודולו $I = (x^n)$ $\iff$ $f(x) - g(x) \in (x^n)$

$\iff$ המקדמים של $1, x, \dots, x^{n-1}$ ב-f וב-g

זהים. כל מחלקה ב- $S[x]/(x^n)$ הינה

מן הצורה

$$\{f(x) \in S[x] : f(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + \text{(משהו עם מעלות גבוהות יותר)}\}.$$

<u>שאלה</u> מהו החוג $\mathbb{Z}[x]/(x^2+1)$

$$= \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$