הרצאה 3

<u>הגדרה</u> יהי R חוג. תת-קבוצה I לא-ריקה נקראת אידיאל שמאלי (בהתאמה, ימני) אם

1) I הינה תת-חבורה של $(R,+)$
($\Leftrightarrow$ I סגורה לחיסור)

2) לכל $a\in I$ ולכל $r\in R$ מתקיים $ra\in I$
(בהתאמה, $ar\in I$).

<u>הגדרה</u> I נקרא אידיאל (או אידיאל דו-צדדי) אם הוא גם אידיאל שמאלי וגם ימני.

<u>הערה</u> 1) אם R חילופי, אזי אידיאל שמאלי = אידיאל ימני = אידיאל.

2) R חוג כלשהו. כל אידיאל שמאלי/ימני הינו תת-חוג-בלי-יחידה.

3) אפשר להגדיר כך אידיאלים שמאליים/ימניים של חוג בלי יחידה. (ההגדרה לא משתמשת ב-1).

4) יהי R חוג, $I\subseteq R$ אידיאל שמאלי/ימני.
אזי $I=R \Leftrightarrow 1\in I$.

<u>הוכחה</u> $\Leftarrow$) אם I (נניח שמאלי) וגם $1\in I$.
אזי לכל $r\in R$, $r\cdot 1 = r\in I$.

<u>דוגמאות</u> 1) R חוג בלי יחידה. $I=R$ אידיאל דו-צדדי.

באופן כללי, כשנדבר על אידיאלים, נתכוון לאידיאלים אמיתיים.

0) R חוג בלי יחידה, $I=\{0\}$ הינו אידיאל.

סימון: $I \trianglelefteq R \iff I$ אידיאל ב-R.

1) יהי $f: R\to S$ הומומורפיזם של חוגים בלי יחידה. אזי $\ker f=\{r\in R: f(r)=0\}\trianglelefteq R$.

הוכחה f הומו' בפרט של חבורות אבליות, אנחנו יודעים כי הגרעין הינו תת-חבורה.

יהי $a\in \ker f$, $r\in R$. אזי

$f(ra)=f(r)\cdot f(a)=f(r)\cdot 0=0 \implies ra\in \ker f$.

$f(ar)=f(a)\cdot f(r)=0\cdot f(r)=0 \implies ar\in \ker f$.

2) יהי R חוג בלי יחידה, יהי $a\in R$.

$Ra=\{ra: r\in R\}$ הינו אידיאל שמאלי

הוא נקרא האידיאל השמאלי הנוצר ע"י a,

הוא האידיאל השמאלי הכי קטן שמכיל את a.

צריך לבדוק כי Ra סגור לחיסור:

$ra-sa=(r-s)a\in Ra$ ע"י פילוג.

2') כמו כן, $aR=\{ar: r\in R\}$

האידיאל הימני הנוצר ע"י a.

2) מהו האידיאל (הדו-צדדי) הנוצר על ידי a?

$$RaR = \left\{ \sum_{i=1}^{n} r_i a s_i \;\middle|\; n\in\mathbb{N},\ r_i, s_i \in R \right\} \trianglelefteq R$$

<u>דוגמא של דוגמא</u>

S חוג כלשהו.

$$a = \begin{pmatrix} 0 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}, \quad R = M_n(S)$$

$Ra = \{$ כל המטריצות ב-R עם עמוד ראשון $\begin{pmatrix}0\\ \vdots \\ 0\end{pmatrix}$ $\}$

$aR = \{$ כל המטריצות עם שורה ראשונה $(0 \dots 0)$ $\}$

$$RaR = R$$

בתרגיל הבית השני הוכחנו שאם $J \trianglelefteq M_n(S)$ אזי קיים $I \trianglelefteq S$ כך ש- $J = M_n(I)$

$$RaR \ni a = \begin{pmatrix} 0 & & 0 \\ & 1 & \\ 0 & & \ddots\ 1 \end{pmatrix}$$

לכן, $RaR = M_n(I) = \{A = (a_{ij}) \in M_n(S) : a_{ij} \in I\}$,

לכן $1 \in I \Rightarrow I = S \Rightarrow RaR = M_n(I) = R$.

3) יהי R חוג בלי יחידה, $A \subseteq R$ תת-קבוצה.

האידיאל השמאלי הנוצר ע"י A הינו

$$RA = \left\{ \sum_{i=1}^{n} r_i a_i : n\in\mathbb{N},\ r_i \in R,\ a_i \in A \right\}$$

קל לבדוק שזה אכן אידיאל שמאלי.

כמו כן

$$AR=\left\{\sum_{i=1}^{n} a_i r_i : \ n\in\mathbb{N}, \ a_i\in A, \ r_i\in R\right\}$$

אידיאל ימני שנוצר ע"י A.

4) R <u>חוג</u> חילופי, $I\triangleleft R$. נגדיר את הרדיקל של I:

$$\sqrt{I}=\{a\in R : \ \exists n\in\mathbb{N}, \ a^n\in I\} \qquad \mathbb{N}=\{1,2,3,\dots\}$$

<u>טענה</u> $\sqrt{I}\triangleleft R$.

<u>הוכחה</u>: 1) סגירות לכפל: יהי $a\in\sqrt{I}$, $r\in R$. אזי קיים n טבעי כך ש- $a^n\in I$ אזי

$$(ra)^n = rara\cdots ra \underset{R \text{ חילופי}}{=} r^n \underbrace{a^n}_{\in I} \in I$$

לכן $ra\in\sqrt{I}$

2) סגירות לחיבור: יהיו $a,b\in\sqrt{I}$. אזי קיימים טבעיים n,m כך ש- $a^n\in I$, $b^m\in I$.

$$(a+b)^{n+m-1} = \underbrace{\sum_{k=0}^{n+m-1}\binom{n+m-1}{k} a^k b^{n+m-1-k}}_{\underbrace{a^k b^{n+m-1-k} + \dots + a^k b^{n+m-1-k}}_{\binom{n+m-1}{k} \text{ פעמים}}}$$

הצלחתי להציג את $(a+b)^{n+m-1}$ כסכום של 2^{n+m-1} מחוברים, כולם מן הצורה $a^k b^{n+m-1-k}$.

אם $n \geq k$, אזי המחובר הינו

$$\underbrace{a^n}_{\in I}\left(a^{k-n} b^{n+m-1-k}\right) \in I$$

אם $k<n$. אזי $n+m-1-k \geq m$, אז המחובר "מתחלק" ב- b^m ולכן מוכל ב-I

$$a^k b^{n+m-1-k} = \left(a^k b^{n-1-k}\right) b^m \in I$$

בכל מקרה, $(a+b)^{n+m-1} \in I$. $\Longleftarrow$ $a+b \in \sqrt{I}$.

הנחנו כי R חוג, לכן אם $a \in \sqrt{I}$ אזי $a^n \in I$

$-a = -1 \cdot a$ $\Longleftarrow$ $(-a)^n = (-1)^n \cdot \underbrace{a^n}_{\in I} \in I$.

5) R חוג. אידיאל I (שמאלי/ימני) נקרא מקסימלי, אם I אידיאל (שמאלי/ימני) אמיתי ואם J הוא אידיאל (שמאלי/ימני) אמיתי שמקיים $I \subseteq J$, אזי $I = J$.

(I אמיתי $\Longleftrightarrow$ $I \neq R$).

<u>טענה</u> יהי R חוג. אידיאלים (שמאליים/ימניים) מקסימליים קיימים.

<u>טענה</u> "הלמה של צורן" תהי $\mathcal{A}$ קבוצה עם סדר חלקי. נניח שכל שרשרת

$a_1 \leq a_2 \leq a_3 \leq a_4 \leq \dots$ $(a_i \in \mathcal{A})$

חסומה מלעיל, כלומר שקיים $b\in S$ כך ש-
$a_i \leq b$ לכל i.
אזי ל-S יש איבר מקסימלי (קיים $m\in S$
כך שאם $c\in S$ מקיים $m\leq c$ אזי $m=c$).

"<u>הוכחה</u>" הלמה של צורן שקולה לאקסיומת
הבחירה.

<u>הוכחה של הטענה</u> R חוג. רוצים להוכיח
שקיים אידאל שמאלי מקסימלי:

$$S = \{ I \leq R : \text{אידאל שמאלי (אמיתי)}\ I \}$$

עם יחס ההכלה. תהי

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

שרשרת של אידאלים שמאליים. נוכיח כי
$\bigcup_{n=1}^{\infty} I_n$ אידאל (אזהרה: איחוד של אידאלים
בגון כלל לא אידאל!)

אזי: יהיו $a,b\in \bigcup I_n$, אזי $a\in I_n$, $b\in I_m$.

זה אומר $\underset{I_m, I_n}{\overset{\cup|}{a,b\in I_{\max\{m,n\}}}}$. לכן $a-b\in I_{\max\{m,n\}}$
לכן $a-b\in \bigcup I_n$.

בנוסף, אם $a\in \bigcup I_n$ אזי $a\in I_n$ עבור n מתאים.
לכל $r\in R$, $ra\in I_n \Rightarrow ra\in \bigcup I_n$.

אז $1\notin I_n$ לכל n. לכן

$1\notin \bigcup_{n=1}^{\infty} I_n$, לכן $\bigcup_{n=1}^{\infty} I_n \in \mathcal{A}$, ולכל שרשרת

יש חסם מלעיל. לפי הלמה של צורן,

קיים איבר מקסימלי של $\mathcal{A}$ שהוא יהיה

אידיאל (שמאלי) מקסימלי של R.

<u>הגדרה</u> יהי R חוג בלי יחידה. יהי $I \trianglelefteq R$.

(אידיאל דו-צדדי). נגדיר יחס על R.

$r,s\in R$, נגיד $r\sim s$ אם $r-s\in I$.

<u>טענה</u> זה יחס שקילות.

1) רפלקסיבי: $r-r=0\in I \Rightarrow r\sim r$.

2) סימטרי: אם $r\sim s \Rightarrow r-s\in I \Rightarrow s-r=-(r-s)\in I \Rightarrow s\sim r$

$$r-s+(s-r)=0$$

3) טרנזיטיבי: $\begin{matrix} r\sim s \\ s\sim t \end{matrix} \Rightarrow \begin{matrix} r-s\in I \\ s-t\in I \end{matrix} \Rightarrow r-t=(r-s)+(s-t)\in I \Rightarrow r\sim t$

נסמן R/I הקבוצה של מחלקות השקילות.

כל מחלקה הינה מן הצורה

$a+I=\{a+b: b\in I\}$, $a\in R$.

נגדיר חיבור וכפל של מחלקות:

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

<u>טענה</u> הפעולות האלה מוגדרות היטב, ו-R/I עם הפעולות האלה הינו חוג בלי יחידה (חוג אם R היה חוג)

<u>הוכחה</u> יהיו a_1,a_2 / b_1,b_2 נציגים שונים של המחלקות:

$$a_1+I = a_2+I$$
$$b_1+I = b_2+I.$$

R/I הינה הקבוצה של הקוסטים של התת"ח I בחבורה $(R,+)$. $(R,+)$ אבלית, לכן I תת"ח נורמלית, והחיבור של קוסטים מוגדר היטב.

לפי ההגדרה, $a_2=a_1+c$, $c\in I$.
$b_2=b_1+d$, $d\in I$

לכן

$$a_2b_2=(a_1+c)(b_1+d)=a_1(b_1+d)+c(b_1+d)=$$
$$a_1b_1+\underbrace{a_1d}_{\in I}+\underbrace{cb_1}_{\in I}+\underbrace{cd}_{\in I}$$

כי I אידיאל שמאלי. כי I אידיאל ימני.

$$=a_1b_1+(\text{איבר של } I)$$

ולכן $a_2b_2+I=a_1b_1+I$.
ה.נ. קריטי ש-I היה אידיאל דו-צדדי!

<u>דוגמא</u> $R=\mathbb{Z}$
כל התת-חוגים בלי יחידה הם $n\mathbb{Z}$.
ברור כי $n\mathbb{Z}$ הינו אידיאל לכל n.
(ז.א. אידיאל הנוצר ע"י n). ניקח $I=n\mathbb{Z}$
$R/I=\mathbb{Z}/n\mathbb{Z}$ עם חיבור וכפל של מחלקות מודולו n.

אם $n=1$, אזי $n\mathbb{Z}=I=\mathbb{Z}$

תרגיל 1) אם $I=R$, אזי R/I הינו החוג הטריוויאלי!

2) $R\cong R/(0)$.

תרגיל: אימתי $I\trianglelefteq\mathbb{Z}$ הינו מקסימלי $\Longleftrightarrow$ $I=p\mathbb{Z}$

כאשר p ראשוני!