הרצאה 4

R חוג, $I,J \lhd R$ אידיאלים. הגדרנו

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

$$IJ=\{a_1 i_1 j_1+\cdots+a_r i_r j_r : a_k\in R,\ i_k\in I,\ j_k\in J\}$$

נוצר ע"י מכפלות ij.

<u>דוגמא</u> $R=\mathbb{Z}$

$$I=n\mathbb{Z}$$
$$J=m\mathbb{Z}$$

$$I+J=\{nx+my : x,y\in\mathbb{Z}\}=$$
$$\{x\in\mathbb{Z} : d|x\}=d\mathbb{Z}.$$

$d=\gcd(n,m)$

$$I+J=\underbrace{(n,m)}_{\text{אידיאל נוצר}}=d\mathbb{Z}$$

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

<u>הגדרה</u> R חוג, $I,J\lhd R$ אידיאלים. I,J נקראים זרים אם $I+J=R$.

<u>משפט</u> (משפט השאריות הסיני) R חוג חילופי. I,J אידיאלים זרים. אזי $R/IJ\cong R/I\times R/J$.

<u>הוכחה</u> נגדיר הומ' של חוגים

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

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

מה הגרעין?

$$r \in \ker f \iff f(r) = (0_{R/I},\ 0_{R/J}) \iff$$

$$\left.\begin{array}{l} r+I = 0+I \iff r\in I \\ r+J = 0+J \iff r \in J \end{array}\right\} \iff r\in I\cap J.$$

כלומר, נקבל $\ker f = I\cap J$. נוכיח שני טענות

1) f על

2) $I\cap J = IJ$.

ואז נקבל את המשפט (בנוסף על משפט האיזומורפיזם הראשון)

<u>f-על</u> לפי הנתון, $1\in R = I+J$.

כלומר יש $i\in I$, $j \in J$ כך ש- $1 = i+j$.

$i-0 = i\in I$ $\quad f(i) = (i+I,\ i+J) = (0_{R/I},\ 1_{R/J})$

$$1-i = j\in J \Rightarrow i+J = 1+J \in 1_{R/J}$$

$$f(j) = (1_{R/I},\ 0_{R/J})$$

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

$$f(r_2 i + r_1 j) = f(r_2)f(i) + f(r_1)f(j) =$$
$$(r_2+I, r_2+J)(0,1) + (r_1+I, r_2+J)(1,0) =$$
$$(0, r_2+J) + (r_1+I, 0) = (r_1+I, r_2+J)$$

לכן f על.

2) צריך להוכיח $IJ = I\cap J$,

$IJ \subseteq I \cap J$ תמיד נכון.

יהי $r \in I\cap J$. אזי

$$r = r\cdot 1 = r(i+j) = \underbrace{ri}_{\substack{r\in J \\ ri\in IJ}} + \underbrace{rj}_{\substack{r\in I \\ rj\in IJ}} \in IJ.$$

לכן $IJ = I\cap J$.

<u>מסקנה</u> יהי R חוג חילופי, $I_1,\dots,I_n \triangleleft R$ זרים בזוגות, כלומר $I_i + I_j = R$ לכל i,j שונים. אזי

$$R/I_1 I_2\cdots I_n \cong R/I_1 \times R/I_2 \times\cdots\times R/I_n$$

<u>הוכחה</u> אינדוקציה על n.

$n=2$ עכשיו הוכחנו את המשפט ונניח עבור $n-1$. צריך להוכיח $I_1I_2\cdots I_{n-1},\ I_n$

זרים. אם כן, אזי

$$R/I_1 I_2 \cdots I_n \simeq R/I_1 I_2 \cdots I_{n-1} \times R/I_n$$

$$\simeq R/I_1 \times \cdots \times R/I_{n-1} \times R/I_n.$$

לפי ההנחה, לכל $1 \leq k \leq n-1$, האידאלים I_k, I_n זרים. לכן קיימים $x_k \in I_k$ כך ש- $y_k \in I_n$ $.x_k + y_k = 1$

אזי

$$1 = (x_1+y_1)(x_2+y_2)\cdots(x_{n-1}+y_{n-1}) =$$

$$\underbrace{x_1 x_2 \cdots x_{n-1}}_{\in I_1 I_2 \cdots I_{n-1}} + \underbrace{(\text{המון מחוברים, בכל אחד מהם יש איזה } y)}_{\text{כל מחובר ב- } I_n}$$

$$\in I_1 I_2 \cdots I_{n-1} + I_n$$

לכן

$$I_1 I_2 \cdots I_{n-1} + I_n = R$$

שני האידאלים אכן זרים.

<u>דוגמה</u> $n \in \mathbb{Z}$ $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

פירוק לגורמים ראשוניים. לפי המשפט,

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r}$$

הגדרה R חוג, איבר $a\in R$ נקרא הפיך אם קיים $b\in R$ כך ש- $ab=ba=1$.

חבורה לכפל $R^* = \{a\in R :$ הפיך $a\}$

ברור כי $(R\times S)^* = R^* \times S^*$

בפרט, $\underbrace{\left(\mathbb{Z}/n\mathbb{Z}\right)^*}_{U_n} \simeq \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^* \times \cdots \times \left(\mathbb{Z}/p_r^{e_r}\mathbb{Z}\right)^*$

העוצמה של $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ היא $\varphi(n)$.

$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_r^{e_r})$.

טענה R חוג, $I\triangleleft R$ אידיאל. אזי $I=R$ אם ורק אם I מכיל איבר הפיך.

הוכחה $\Leftarrow$) $I=R \Leftarrow 1\in I$, אך 1 הפיך.

$\Rightarrow$) יהי $u\in R$ הפיך, יהי $uv=vu=1$.

אזי $u\in I \Leftarrow 1=uv\in I \Leftarrow$ לכל $r\in R$, $r=r\cdot 1\in I$

$\Leftarrow R=I$

מסקנה יהי R חוג עם חילוק (כל איבר לא-אפס הינו הפיך). אזי האידיאלים היחידים של R הם $R, (0)$.

__טענה__ יהי R חוג חילופי. אזי R שדה אם ורק אם האידאלים היחידים שלו הם $R, (0)$.

__הוכחה__ $\Leftarrow$) כבר הוכחנו.

$\Rightarrow$) נניח אין אידאלים מלבד $R, (0)$.

יהי $0 \neq a \in R$. אזי $Ra = R$.

לכן $1 \in Ra \Leftarrow$ קיים $b \in R$ כך ש- $ab = ba = 1$.

__מסקנה__ יהי R חוג עם יחידה, כל הומ' $f: R \to S$ של חוגים הינו חח"ע. $(S \neq 0)$

__הוכחה__ $\ker f \trianglelefteq R$, אך $1 \notin \ker f$ כי $f(1_R) = 1_S \neq 0_S$. אזי $\ker f \neq R \Leftarrow \ker f = \{0_R\} \Leftarrow f$ חח"ע.

__הגדרה__ יהי R חוג. אידאל אמתי $M \trianglelefteq R$ נקרא מקסימלי אם $M \leq I \trianglelefteq R \Leftarrow I = M$ או $I = R$.

__טענה__ R חוג. יהי $I \trianglelefteq R$ אידאל. אזי קיים $M \trianglelefteq R$ מקסימלי כך ש- $I \leq M$.

__הוכחה__ הלמה של צורן. ניקח

$I \in S = \{$כל האידיאלים האמיתיים של R שמכילים את $I\}$

__הלמה של צורן__: $S \neq \emptyset$ קבוצה מסודרת חלקית. אם לכל שרשרת $C \subseteq S$ (C שרשרת $\Leftrightarrow$ לכל $a, b \in C$ מתקיים $a \leq b$ או $b \leq a$) יש חסם מלעיל (איבר $x \in S$ כך ש $a \leq x$ לכל $x \in C$) אזי ל-S יש איבר מקסימלי.

עלינו להוכיח שלכל שרשרת של אידיאלים אמיתיים יש חסם מלעיל. תהי C שרשרת.

נגדיר $\bigcup_{I\in C} I = J$. אני טוען כי $J\in S$.

J <u>סגור לחיבור</u> יהיו $a,b\in J$. $a\in I_1\in C$, $b\in I_2$.

בלי הגבלת הכלליות, $I_1\subseteq I_2 \Rightarrow a,b\in I_2 \Rightarrow$ $a+b\in I_2\subseteq J$.

יהי $a\in J$, $r\in R$. אזי קיים $I\in C$ כך ש- $a\in I$.

אזי $ra\in I\subseteq J$, הוכחנו כי J אידיאל.

וכן $1\notin J$, כי J איחוד של <u>אידיאלים אמיתיים</u>.

לכן J אמיתי ויש לנו את כל התנאים של הלמה של צורן.

<u>טענה</u> R חוג חילופי, $I\triangleleft R$ אידיאל. אזי I מקסימלי אם ורק אם R/I הינו שדה,

<u>הוכחה</u> לפי משפט האיזו' הרביעי מן השיעור הקודם, יש התאמה

$$\left\{ \begin{matrix} \text{אידיאלים} \\ I \subseteq J \trianglelefteq R \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{אידיאלים של} \\ R/I \end{matrix} \right\}$$

ההתאמה $f: J \longrightarrow f(J)$

I מקסימלי $\Longleftrightarrow$ $J=I$ או $J=R$ $\Longleftrightarrow$ $\{(0_{R/I}), R/I\}$ הם כל האידיאלים

$\Updownarrow$

R/I שדה (R/I חילופי כי R היה חילופי)

שיעור הראשון באינפי 1.

בתורת הקבוצות, בנינו את $\mathbb{Z}$.

$$\mathbb{Q} = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\} / \sim$$

$$(a,b) \sim (c,d) \Longleftrightarrow ad = bc$$

$$\frac{a}{b} = \frac{c}{d}$$

איך להגדיר $\mathbb{R}$?

סדרה (a_n) של איברים של $\mathbb{Q}$ נקראת סדרת קושי אם לכל $0<\varepsilon\in\mathbb{Q}$ קיים N כך שלכל $n,m \geq N$ מתקיים $|a_n - a_m| < \varepsilon$.

R החוג של סדרות קושי.

$$(a_n)+(b_n)=(a_n+b_n)$$

$$(a_n)\cdot(b_n)=(a_nb_n).$$

סדרת קושי נקראת אפסה אם לכל $0<\varepsilon\in\mathbb{Q}$ קיים N כך שלכל $N\le n$ מתקיים $|a_n|<\varepsilon$.

$$I=\{\text{סדרות אפסות}\}\triangleleft R$$

הגדרה $\mathbb{R}=R/I$

<u>תרגיל</u> I אידאל מקסימלי. $\Leftarrow$ $\mathbb{R}$ שדה.