הרצאה 9

תזכורת: R חוג חילופי, איבר $a\in R$ לא הפיך נקרא אי-פריק אם בכל פירוק $a=bc$, בהכרח אחד מן הגורמים b,c הינו הפיך.

תחום פריקות יחידה (תפ"י) הינו תחום שלמות בו ניתן להציג כל איבר $a\neq 0$ ולא הפיך כמכפלה

$$a=p_1\cdots p_n$$

של איברים אי-פריקים, ואם $a=p_1\cdots p_n=q_1\cdots q_m$ שני פירוקים, אזי $n=m$ וקיימת תמורה $\sigma\in S_n$ כך ש- $p_i, q_{\sigma(i)}$ חברים לכל $n\geq i\geq 1$.

<u>משפט</u> כל תחום ראשי הינו תחום פריקות יחידה.

<u>הוכחה</u> יהי R תחום ראשי, $a\neq 0$ לא הפיך.

הוכחנו בסוף השיעור הקודם כי יש ל-a מחלק אי-פריק p_1 (כלומר קיים p_1 אי-פריק כך ש- $a=p_1b_1$ עבור איזה $b_1\in R$).

<u>שלב 2</u> ניתן לפרק את a למכפלה של אי-פריקים.

<u>הוכחה</u> ידוע מן השלב הקודם כי $a=p_1b_1$.

אם b_1 הפיך, אז סיימנו כי a עצמו אי-פריק (ואז $a=a$ הינו פירוק).

אם b_1 לא הפיך, אז לפי השלב 1, $b_1=p_2b_2$ כאשר p_2 אי-פריק $\Leftarrow$ $a=p_1p_2b_2$

אם b_2 הפיך, אז סיימנו, כי $a=p_1(p_2b_2)$
(תרגיל: החבר של אי-פריק הינו אי-פריק).

וכן ממשיכים $b_2 = p_3 b_3$

$a = p_1 p_2 p_3 b_3$ ....

צריך להוכיח שהתהליך הזה מסתיים, כלומר עבור N נקבל b_{N+1} הפיך. אכן:

$$(a) \subseteq (b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \dots$$

אם כל ה-b_n-ים לא הפיכים, מקבלים שרשרת של אידיאלים אמיתיים. אבל R תחום ראשי. לכן נותרי, לכן השרשרת מתייצבת $\Leftarrow$ $(b_N) = (b_{N+1})$ $\Leftarrow$ b_{N+1}, b_N חברים כי יוצרים אותו אידיאל ראשי בתחום שלמות:

$$b_N = u b_{N+1} = p_{N+1} b_{N+1}$$

$\Leftarrow$ $u = p_{N+1}$

בסתירה להנחה כי p_{N+1} אי-פריק ולכן לא הפיך.

__שלב 3__ יחידות הפירוק.

נניח $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ בלי הגבלת הכלליות, $n \leq m$.

__אינדוקציה על n__ אם $n=1$, אז a אי-פריק.

אם $1<m$, אז $a = q_1 (q_2 \cdots q_m)$ היה פירוק של a לגורמים לא-הפיכים, בסתירה. לכן בהכרח $1=n=m$, ושני הפירוקים זהים.

נניח שהטענה נכונה עבור $n-1$.

$$a = p_1 p_2 \cdots p_n = q_1 \cdots q_m$$

אז, $a \in (p_n)$, הוכחנו בשיעור הקודם שהאידיאל (p_n) מקסימלי (כי נוצר ע"י איבר אי-פריק בתחום ראשי) ולכן ראשוני.

אז $q_1q_2\cdots q_m \in (p_n) \Rightarrow q_i \in (p_n)$ עבור i מסוים. (כי (p_n) ראשוני)

אבל: q_i אי-פריק, לכן האידיאל (q_i) מקסימלי, לכן

$q_i \in (p_n) \Rightarrow (q_i)\subseteq(p_n) \Rightarrow (q_i)=(p_n) \Rightarrow q_i, p_n$ חברים.

$q_i = p_n u$ ו-u הפיך

נמספר מחדש את ה-q-ים ונניח $m=i$, אז נצמצם ונקבל

$$p_1\cdots p_{n-1} = q_1\cdots q_{m-2}(\underbrace{q_{m-1}u}_{\text{אי-פריק}})$$

ובאינדוקציה, $n-1=m-1$ והגורמים הנשארים חברים...

$\Downarrow$

$n=m$.

מוטיבציה בהינתן חוג חילופי R, רוצים להגדיר חוג של שברים $\frac{r}{s}$, אבל צריך לחשוב:

1) איזה מכנים מותרים.
2) הכל מוגדר היטב.

הגדרה יהי R חוג חילופי. תת-קבוצה $S\subseteq R$ נקראת תת-קבוצה כפלית אם היא מקיימת את התנאים הבאים:

1) $0\notin S$
2) $1\in S$
3) S סגורה לכפל: אם $a,b\in S$, אז $ab\in S$.

דוגמאות 0) R חוג כלשהו, לא-טריוויאלי, $S=\{1\}$.

1) R תחום שלמות, $S=R\setminus\{0\}$.

2) R חוג חילופי, $P\triangleleft R$ אידיאל ראשוני, $S=R\setminus P$.

3) $R=\mathbb{Z}$, $S=\{1,n,n^2,n^3,n^4,\dots\}$, $0\neq n\in\mathbb{Z}$

4) $R=\mathbb{Z}$ $\quad S=\left\{n\in\mathbb{Z} \;\middle|\; \text{אם } p|n\text{, } p \text{ ראשוני, אזי } p\in\{2,3\}\right\}$

$$=\{1,2^i3^j\}$$

5) $R=\mathbb{Z}/6\mathbb{Z}$ $\quad S=\{[1],\underbrace{[2],[4]}_{\text{מחלקי אפס}}\}$

נזכיר שבריה: $\frac{r}{s}=\frac{ra}{sa}$, אז צריך להגדיר יחס שקילות מתאים.

נגדיר יחס על $R\times S$: $(r_1,s_1)\sim(r_2,s_2)$ אם קיים $t\in S$ כך ש־ $t(r_1s_2-r_2s_1)=0$.

<u>טענה</u> זה יחס שקילות. רפלקסיבי, סימטרי: ברורים.

טרנזיטיביות: נניח $(r_1,s_1)\sim(r_2,s_2)$, $(r_2,s_2)\sim(r_3,s_3)$ אזי

קיימים $t_1,t_2\in S$ כך ש־

$$t_1(r_1s_2-r_2s_1)=0 \qquad t_2(r_2s_3-r_3s_2)=0$$

$$0=s_3t_2\underbrace{t_1(r_1s_2-r_2s_1)}_{=0}+s_1t_1\underbrace{t_2(r_2s_3-r_3s_2)}_{=0}=$$

$$r_1s_2s_3t_1t_2-r_2s_1\cancel{s_3t_1}t_2+r_2s_1\cancel{s_3t_1}t_2-r_3s_1s_2t_1t_2$$

$$=\underbrace{s_2t_1t_2}_{\in S}(r_1s_3-r_3s_1)$$

לכן $(r_1,s_1)\sim(r_3,s_3)$.

<u>הערה</u> אם R תחום שלמות, אזי $(r_1,s_1)\sim(r_2,s_2)$

אם ורק אם $r_1s_2-r_2s_1=0$

כי $t(r_1s_2-r_2s_1)=0$, אך $t\in S$, לכן $t\neq0$, לכן $r_1s_2-r_2s_1=0$.

<u>הגדרה</u> יהי R חוג חילופי, $S\subseteq R$ תת-קבוצה
כפלית. המיקום של R ב-S הינו:
הקבוצה $S^{-1}R$ של מחלקות השקילות
על היחס הנ"ל, עם הפעולות:

$$\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1s_2+r_2s_1}{s_1s_2} \qquad \frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}$$

$$(r_1,s_1)+(r_2,s_2)=(r_1s_2+r_2s_1,s_1s_2)$$
$$(r_1,s_1)\cdot(r_2,s_2)=(r_1r_2,s_1s_2)$$

$[(r,s)]=\frac{r}{s}$

<u>תרגיל</u> 1) הפעולות האלה מוגדרות היטב.
2) $S^{-1}R$ עם הפעולות האלה הינו חוג,
$0_{S^{-1}R}=(0,1)=\frac{0}{1}$ $\qquad$ $1_{S^{-1}R}=\frac{1}{1}$.

<u>הערה</u> $f:R\to S^{-1}R$ הינו הומו של חוגים.
$f(a)=\frac{a}{1}$

אם R לא תחום שלמות, f לאו חד-חד-ערכי.

אכן,
$$\ker f=\{a\in R:\ \frac{a}{1}=\frac{0}{1}\}=$$
$$\{a\in R:\ \exists t\in S,\ \ t(a\cdot1-0\cdot1)=ta=0\}$$

אם S מכיל מחלקי אפס, זה יכול לקרות.

<u>הוכחנו</u> $f:R\to S^{-1}R$, $a\mapsto\frac{a}{1}$ חח"ע אם ורק אם
בקבוצה S אין מחלקי אפס.

אם R תחום שלמות, אזי f חח"ע לכל S

דוגמאות 1) R תחום שלמות, $S=R\setminus\{0\}$

טענה אזי $S^{-1}R$ הינו שדה.

הוכחה $\frac{r}{s}=\frac{0}{1} \iff r=r\cdot 1=0\cdot s=0 \iff r=0$

יהי $0\neq x\in S^{-1}R$ אזי $x=\frac{r}{s}$, $r\neq 0$, אזי $r\in S$.

ולכן $\frac{s}{r}\in S^{-1}R$, והוא ההפכי כפלי ל-x.

הגדרה R תחום שלמות, $S=R\setminus\{0\}$. השדה $S^{-1}R$ נקרא שדה השברים של R, מסומן $\mathrm{Frac}\,R$

טענה $\mathrm{Frac}\,R$ הינו השדה הכי קטן שמכיל את R.

כלומר, יהי F שדה כלשהו, אם קיים שיכון של חוגים $f:R\hookrightarrow F$, אזי קיים שיכון $\varphi:\mathrm{Frac}\,R\hookrightarrow F$ כך ש- $f(r)=\varphi(\frac{r}{1})$ לכל $r\in R$.

הוכחה נגדיר $\varphi(\frac{r}{s})=f(r)\cdot f(s)^{-1}$.

תרגיל: φ מוגדר היטב והינו הומ' של חוגים.

מדוע φ מוגדר היטב? נניח $\frac{r_1}{s_1}=\frac{r_2}{s_2}$.

אזי $r_1s_2-r_2s_1=0$ (כי R תחום שלמות)

לכן $r_1s_2=r_2s_1 \Rightarrow f(r_1)f(s_2)=f(r_2)f(s_1)$

אבל $f(s_1),f(s_2)\in F$ ונכפיל ב- $f(s_1)^{-1}\cdot f(s_2)^{-1}$

ונקבל $f(r_1)f(s_1)^{-1}=f(r_2)\cdot f(s_2)^{-1}$.

לכן φ מוגדר היטב.

דוגמא $\mathrm{Frac}\,\mathbb{Z}=\mathbb{Q}$.

הערה יהי R חוג אם קיים שדה F
ושיכון $f: R \hookrightarrow F$, אזי R תחום שלמות.

הוכחה R חילופי: $f(ab) = f(a)\cdot f(b) \underset{F \text{ חילופי}}{=} f(b)\cdot f(a) = f(ba)$

f חח"ע $\Leftarrow$ $ab = ba$ לכל $a,b \in R$.

אם $a,b \in R$, $ab = 0$ $\Leftarrow$ $0 = f(ab) = f(a)\cdot f(b)$

$\Leftarrow$ (בשדה אין מחלקי אפס) $f(a) = 0$ או $f(b) = 0$ $\Leftarrow$

$a = 0$ או $b = 0$ כי f חח"ע

דוגמא 2 $R = \mathbb{Z}[i]$ השלמים של גאוס: נשים לב
כי $\mathbb{Z}[i] \subseteq \mathbb{C}$, שדה, לכן $\mathbb{Z}[i]$ תחום שלמות.

טענה $\operatorname{Frac} R = \mathbb{Q}(i)$
$= \{a+bi : a,b \in \mathbb{Q}\}$.

$a,b,c,d \in \mathbb{Z}$

אכן $\dfrac{a+bi}{c+di} = \dfrac{(a+bi)(c-di)}{(c+di)(c-di)} = \dfrac{(ac+bd)+(bc-ad)i}{c^2+d^2} =$

$$\frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \in \mathbb{Q}(i)$$

לכן, $\operatorname{Frac} \mathbb{Z}[i] \subseteq \mathbb{Q}(i)$, אך

$$\frac{a}{b} + \frac{c}{d}i = \frac{ad+bci}{bd+0i} \in \operatorname{Frac} \mathbb{Z}[i]$$

לכן, $\operatorname{Frac} \mathbb{Z}[i] = \mathbb{Q}(i)$

הערה באופן כללי, $\frac{r}{s} \in S^{-1}R$ הינו סימון פורמלי.
כיוון שעכשיו מוכל כי $\mathbb{Z}[i] \subseteq \mathbb{C}$, לכן $\operatorname{Frac} \mathbb{Z}[i] \subseteq \mathbb{C}$,
ונוכל לעבוד בתוך $\mathbb{C}$, ואז $\frac{r}{s}$ באמת חילוק של מספרים מרוכבים