הרצאה 8

סיום של ההוכחה שכל תחום ראשי הינו תפ"י. כבר הוכחנו שקיימים פירוקים לאי-פריקים. נשאר להוכיח את היחידות.

תזכורת R תחום ראשי. אזי

$a\in R$ אי-פריק $\iff$ (a) מקסימלי $\iff$ (a) ראשוני

$\Updownarrow$

a ראשוני.

הוכחה יהי R תחום ראשי. $0\neq a\in R$ לא הפיך. נניח שני פירוקים

$$a=p_1p_2\cdots p_r=q_1\cdots q_s$$

אינדוקציה על r. אם $r=1$, אזי $a=p_1$ אי-פריק. אם $a=p_1=q_1q_2\cdots q_s$.

אזי a אי-פריק $\Leftarrow$ a ראשוני (כי R תחום ראשי). לכן $a|q_1q_2\cdots q_s$ $\Leftarrow$ $a|q_i$ עבור i מסוים. זה אומר $q_i\in(a)$ $\Leftarrow$ $(q_i)\subseteq(a)$

אך q_i גם אי-פריק. לכן (a), (q_i) אידיאלים מקסימליים $\Leftarrow (q_i)=(a) \Leftarrow q_i, a$ חברים.

q_i ו- $q_1 q_2 \cdots q_r = q_i$ (שאר ה-q_j)

מייצרים אותו האידיאל (a). לכן הם הפיכים, (שאר ה-q_jים) הפיכה.

אך מכפלה של קבוצה לא ריקה של אי-פריקים לא הפיכה, לכן זו מכפלה ריקה. לכן $s=1$. לכן $a=p_1=q_1$.

אז נניח שיחידות הפירוק ידועה ל-r. ויהי

$$a = p_1 p_2 \cdots p_r p_{r+1} = q_1 \cdots q_s$$

אזי p_r ראשוני, לכן $p_{r+1} | q_1 \cdots q_s \Leftarrow p_{r+1} | q_i$ לאיזה i. עד כדי מספור מחדש, נניח $p_{r+1} | q_s$.

כמו קודם $(q_s) \subseteq (p_{r+1}) \underset{\text{שניהם אי-פריקים}}{\Leftarrow} (q_s) = (p_{r+1}) \Leftarrow$

$q_s = u p_{r+1}$ עבור $u \in R$ הפיך.

R תחום שלמות, אז אפשר לצמצם אי פריק:

$$p_1p_2\cdots p_r = q_1q_2\cdots(q_{s-1}u)$$

באינדוקציה $r=s-1 \Leftarrow s=r+1$, וגם p_i, q_i חברים לכל $1\le i\le r$ עד כדי שינוי בסדר ה-q_i-ים.

<u>הגדרה</u> יהי R חוג חילופי. תת $S\subseteq R$ תת-קבוצה כך ש:

1) $0\notin S$
2) S סגורה לכפל ($ab\in S \Leftarrow a,b\in S$)
3) $1\in S$

נגדיר את החוג $S^{-1}R=\left\{\frac{r}{s} : r\in R,\ s\in S\right\}$.

$\left(\frac{r}{s}=\frac{rc}{sc}\right)$.

הגדרה פורמלית: נגדיר קודם יחס שקילות על $R\times S$ ($\frac{r}{s} \rightsquigarrow (r,s)$).

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

זה יחס שקילות: רפלקסיביות, סימטריות קלות.

טרנז': נניח $(r_1,s_1)\sim(r_2,s_2)$

$(r_2,s_2)\sim(r_3,s_3)$

אז קיימים $t_1,t_2\in S$ כך ש- $t_1(r_1s_2-r_2s_1)=0$

$t_2(r_2s_3-r_3s_2)=0$

לכן:

$$0=s_3t_2t_1(r_1s_2-r_2s_1)+s_1t_1t_2(r_2s_3-r_3s_2)$$

$$=r_1s_2s_3t_1t_2-\cancel{r_2s_1s_3}t_1t_2+r_2\cancel{s_1s_3}t_1t_2-r_3s_1s_2t_1t_2$$

$$=\underbrace{s_2t_1t_2}_{\in S}(r_1s_3-r_3s_1)\Rightarrow(r_1,s_1)\sim(r_3,s_3).$$

ותהי $S^{-1}R$ הקבוצה של מחלקות השקילות.

מגדירים חיבור וכפל: $\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1s_2+r_2s_1}{s_1s_2}$

$$\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}$$

כלו' מגדירים $(r_1,s_1)+(r_2,s_2)=(r_1s_2+r_2s_1,\ s_1s_2)$

$(r_1,s_1)\cdot(r_2,s_2)=(r_1r_2,\ s_1s_2).$

תרגיל: זה נותן פעולות מוגדרות היטב על $S^{-1}R$.

וכי $S^{-1}R$ הינו חוג חילופי עם $\frac{1}{1}$ ו-$\frac{0}{1}$

הפעולות האלה.

דוגמאות 1) R תחום שלמות.

$S=R\setminus\{0\}$ סגור לכפל.

במקרה הזה, $S^{-1}R$ הינו שדה.

$$\frac{r}{s}=\frac{0}{1} \iff t(r\cdot 1-0\cdot s)=0 = tr \Rightarrow r=0$$

R תחום שלמות, $t\in S$, $t\neq 0$

לכן, אם $\frac{r}{s}\neq 0$ ב-$S^{-1}R$,

אזי $r\neq 0$, ואז $\frac{r}{s}\cdot\frac{s}{r}=\frac{rs}{rs}=\frac{1}{1}$

במקרה הזה, $S^{-1}R$ נקרא שדה השברים של R, מסומן $\mathrm{Frac}\,R$.

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

2) R חוג חילופי. $S=\{$כל האיברים הרגולריים$\}$

$S^{-1}R =$ חוג השברים של R.

הערה אם R תחום שלמות, $S=R\setminus\{0\}$ ומקבלים $\mathrm{Frac}\,R$.

3) $R=\mathbb{Z}$, $S=\{1,2,4,8,16,32,\dots\}$

$$S^{-1}R=\left\{\frac{a}{b}\in\mathbb{Q} : b=2^k\right\}\subseteq\mathbb{Q}$$

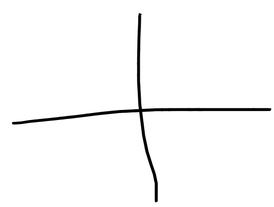
<u>מינוח</u> $S^{-1}R$ נקרא המיקום של R ב-S.

4) R חוג חילופי, P אידיאל ראשוני.

$S=R\setminus P$.

$$S^{-1}R=\left\{\frac{r}{s} : s\notin P\right\}.$$

$\mathbb{R}^2$

$\mathbb{R}[x,y] \longleftrightarrow$ 

$P=I(V)=(x,y) \longleftrightarrow$ V אי-פריקה $(0,0)$

ראשוני

$S=\mathbb{R}[x,y]\setminus P$,

$S^{-1}R=\left\{\text{פונקציות רציונליות מעל } \mathbb{R}\ \frac{f(x,y)}{g(x,y)} \text{ שמוגדרות ב-} (0,0)\right\}$,

יש הומו' של חוגים $R \longrightarrow S^{-1}R$

$r \longmapsto \frac{r}{1}$.

אם R לא תחום שלמות, ההומו' הנ"ל עלול לא להיות חד-חד-ערכי.

<u>הגדרה</u> R חוג חילופי. יהיו $a,b\in R$.
d הינו מחלק משותף של a,b אם $d|a$ וגם $d|b$ $\Longleftrightarrow$ $a,b\in(d)$.

הוא נקרא מחלק משותף מקסימלי (gcd) אם לכל מחלק משותף c אחר של a,b מתקיים $c|d$.
כלומר, (d) הינו האידאל הראשי המינימלי שמכיל את $I=(a,b)$.

<u>תוצאה</u> אם R תחום שלמות, אז gcd של שני איברים מוגדר היטב עד כדי חברות, אם הוא קיים.

ה-gcd של שני איברים לאו בהכרח קיים.

דוגמא: $R=\mathbb{Z}[\sqrt{-5}]$ זה תחום שלמות.

$$N(a+b\sqrt{-5})=a^2+5b^2 = |a+b\sqrt{-5}|^2$$

$$\alpha=6$$
$$\beta=2(1+\sqrt{-5})$$

$$N(\alpha)=36, \quad N(\beta)=24$$

$$c=2$$
$$d=1+\sqrt{-5}$$

שניהם מחלקים משותפים של α,β.

$$\alpha=6=(1+\sqrt{-5})(1-\sqrt{-5}).$$

אם היה קיים gcd של α,β, נניח לו g, אזי $c|g$ וגם $d|g$ $\Leftarrow$

$$4=N(c)\,|\,N(g)$$
$$6=N(d)\,|\,N(g)$$
$$\Rightarrow 12=\mathrm{lcm}(4,6)\,|\,N(g).$$

מצד שני, $g|\alpha$, $g|\beta$ $\Rightarrow$ $N(g)|N(\alpha)=24$, $N(g)|N(\beta)=36$ $\Rightarrow$ $N(g)|\gcd(24,36)=12.$

לכן $N(q)=12$. אבל $12 \neq a^2+5b^2$ $a,b\in\mathbb{Z}$

לכן ב-$\mathbb{Z}[\sqrt{-5}]$ אין איברים עם נורמה 12!

ל-α,β אין gcd.

<u>תרגיל</u> אם R הוא גפ"י, אזי לכל

זוג α,β של איברים לא אפסיים יש gcd.

$$\alpha = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

$$\beta = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

p_i אי-פריקים לא חברים, $0 \le e_i, f_i$.

$$\gcd(\alpha,\beta) = p_1^{\min\{e_1,f_1\}} \cdots p_r^{\min\{e_r,f_r\}}.$$

$$\{\text{שדות}\} \subsetneq \left\{\begin{matrix}\text{תחומים}\\ \text{אוקלידיים}\end{matrix}\right\} \subseteq \left\{\begin{matrix}\text{תחומים}\\ \text{ראשיים}\end{matrix}\right\} \subseteq \{\text{גפ"י}\}$$

$$\subseteq \left\{\begin{matrix}\text{תחומי}\\ \gcd\end{matrix}\right\} \subseteq \left\{\begin{matrix}\text{תחומי}\\ \text{שלמות}\end{matrix}\right\} \subseteq \left\{\begin{matrix}\text{חוגים}\\ \text{חילופיים}\end{matrix}\right\}$$

הערות 1) R תחום שלמות $\iff$ $R[x]$ תחום שלמות.

$\Rightarrow$) אם $ab=0$, נחשוב על a,b כפולינומים קבועים.

$\Leftarrow$) $f(x)g(x)=0$, יהי $f(x)=ax^n+$(חזקות יותר גבוהות)

$a\neq 0$

$$g(x)=bx^m+O(x^{m+1})$$

$b\neq 0$

$$f(x)g(x)=abx^{n+m}+O(x^{m+n+1})$$

$$\Rightarrow ab=0.$$

2) יהי $I\lhd R$, יהי $I[x]\lhd R[x]$ הוכיחו

של כל הפולינומים עם מקדמים ב-I.

נזכיר שבהינתן הומו' $f:R\to S$

מקבלים הומו' $f:R[x]\to S[x]$

$$f(a_nx^n+\dots+a_0)=f(a_n)x^n+\dots+f(a_0).$$

בפרט, אם $f: R \to R/I$ אזי

$$f(r) = r + I$$

מקבלים $f: R[x] \to (R/I)[x]$ זה על.

$$\ker f = I[x]$$

לפי משפט איזו' הראשון, $R[x]/I[x] \cong (R/I)[x]$.

<u>מסקנה</u> $I \triangleleft R$ אידיאל ראשוני $\iff$
$I[x] \triangleleft R[x]$ אידיאל ראשוני.

<u>הוכחה</u> $I \triangleleft R$ ראשוני $\iff$ R/I תחום שלמות

$\iff$ $(R/I)[x]$ תחום שלמות $\iff$

$R[x]/I[x]$ תחום שלמות $\iff$ $I[x]$ ראשוני.