הרצאה 9

<u>תזכורת</u> R חוג חילופי, $a\in R$. אזי a אי-פריק אם בכל פירוק $a=bc$ אחד הגורמים הפיך.

תזכורת: a אי-פריק ו-u הפיך $\Leftarrow$ au אי-פריק

$I\trianglelefteq R$ אידיאל, $R[x] \trianglerighteq I[x] = \{$ פולינומים עם מקדמים ב-I $\}$

אזי $(R/I)[x] \cong R[x]/I[x]$ בפרט, $I\trianglelefteq R$ ראשוני $\Leftarrow$ $I[x]\trianglelefteq R[x]$ ראשוני.

בכל השיעור: R יהיה תחום שלמות.

$F=\mathrm{Frac}\,R$ שדה השברים

$$F=\left\{ \frac{r}{s} : r,s\in R,\ s\neq 0 \right\}$$

<u>טענה</u> (הלמה של גאוס) יהי R תחום פריקות יחידה. יהי $0\neq f\in R[x]\leq F[x]$,

אם f פריק כאיבר של $F[x]$, אזי הוא פריק ב-$R[x]$.

דוגמא $R=\mathbb{Z}$

$$x^3-2x^2+3x-6=\left(\frac{3}{2}x-3\right)\left(\frac{2}{3}x^2+2\right)$$

פירוק ב-$\mathbb{Q}[x]$.

$$=(x-2)(x^2+3)$$

הערה ב-$F[x]$, כל פולינום קבוע לא אפס

הינו הפיך. $1=\frac{s}{r}\cdot\frac{r}{s}$.

הוכחה יהי $f(x)=g(x)h(x)$ פירוק

ב-$F[x]$, לגורמים לא-הפיכים. לפי ההערה,

h, g לא קבועים. נשים לב שקיימים $a,b\in R$

כך ש- $ag(x),\ bh(x)\in R[x]$. לדוגמא,

תהי a המכפלה של המכנים של המקדמים

של $g(x)$ וכו'. יהי $d=ab$. אזי

$$d f(x)=\underbrace{ag(x)}_{\tilde{g}(x)}\cdot\underbrace{bh(x)}_{\tilde{h}(x)}\in R[x]$$

יהי $d=p_1p_2\cdots p_r$ פירוק של $d\in R$

לגורמים אי-פריקים. (קיים כי R תפ"י)

ברור כי כל מקדם של $df(x)$ מתחלק ב-d,

ב-p_r. לכן $df(x) \in (p_r)[x] \triangleleft_{R[x]}$, וגו'

$$\varphi : R[x] \to \left(R/(p_r)\right)[x] \cong R[x]/(p_r)[x]$$

$$\varphi(\tilde{g})\cdot\varphi(\tilde{h}) = \varphi(df(x)) = 0$$

כי R תפ"י

אבל p_r אי-פריק $\Leftarrow$ p_r ראשוני $\Leftarrow$ $(p_r) \triangleleft R$ ראשוני $\Leftarrow$

$(p_r)[x] \triangleleft R[x]$ ראשוני $\Leftarrow$ $\left(R/(p_r)\right)[x]$ תחום שלמות $\Leftarrow$

$\varphi(\tilde{g})=0$ או $\varphi(\tilde{h})=0$. אם $\varphi(\tilde{g})=0$,

אזי כל מקדם של $\tilde{g}(x)$ מתחלק ב-p_r.

$$p_1 p_2 \cdots p_{r-1} f(x) = \frac{df(x)}{p_r} = \underbrace{\frac{\tilde{g}(x)}{p_r}}_{\in R[x]} \cdot \tilde{h}(x)$$

ממשיכים כך ונפטרים מכל ה-$p_1 p_2 \cdots p_{r-1}$.

ומקבלים פירוק של $f(x)$ לגורמים

ב-$R[x]$. שני הגורמים של $g(x), h(x)$

עד כדי סקלר. אך שני הגורמים לא

קבועים ובפרט לא הפיכים. לכן f פריק

ב-$R[x]$.

הגדרה יהי R גפ"י. פולינום $f\in R[x]$
נקרא פרימיטיבי אם ה-gcd של המקדמים
הינו 1 (הפיך).

טענה יהי R גפ"י, יהי $f\in R[x]$ פרימיטיבי.
אזי f אי-פריק ב-$R[x]$ $\iff$ הוא אי-פריק
ב-$F[x]$.

הוכחה $\Leftarrow$) למה של גאוס.

$\Rightarrow$) נניח f אי-פריק ב-$F[x]$,
אבל פריק ב-$R[x]$: $f(x)=\underbrace{g(x)\cdot h(x)}_{\text{ללא הפיכים}}$.
אזי $g(x),h(x)$ גם פרימיטיביים, כי
אם לכל המקדמים של g או h היה
מחלק משותף d, אזי d גם היה מחלק
של כל המקדמים של f, בסתירה
לפרימיטיביות. אבל, פולינום פרימיטיבי
קבוע הינו הפיך. לכן $g(x),h(x)$
לא קבועים, לכן לא הפיכים ב-$F[x]$,
בסתירה לאי-פריקות של f ב-$F[x]$.

משפט יהי R חוג חילופי. אזי R תפ"י $\Leftrightarrow$ $R[x]$ תחום פריקות יחידה.

הוכחה ($\Leftarrow$) ברור (נחשוב על $a\in R$ כפולינום (קבוע)).

($\Rightarrow$) יהי R תפ"י. יהי $f(x)\in R[x]$. אם f קבוע, הטענה ברורה. אז נניח f לא קבוע.

יהי d ה-gcd של המקדמים. אזי

$$f = d\cdot g(x)\ ,\quad d\in R,\quad g(x)\in R[x]$$

כאשר $g(x)$ פרימיטיבי. מספיק להוכיח של-$g(x)$ יש פירוק יחיד לגורמים אי-פריקים (פולינום לא-קבוע לא-פרימיטיבי לא יהיה אי-פריק).

אך $F[x]$ חוג פולינומים מעל שדה, לכן תפ"י (אפילו תחום אוקלידי) אזי

$$g(x) = p_1(x)\cdot p_2(x)\cdots p_r(x)$$

כאשר $p_i(x)$ אי-פריקים ב-$F[x]$. לפי הלמה של גאוס, $g(x)=q_1(x)\cdots q_r(x)$ כאשר $q_i\in R[x]$ הינו כפל סקלארי של $p_i(x)$, לכל $1\le i\le r$.

כל סקלאר לא אפסי ב-$F[x]$ הינו הפיך.
לכן כל $q_i(x)$ עדיין אי-פריק ב-$F[x]$. אז
$q(x)$ פרימיטיבי $\Leftarrow$ כל ה-$q_i(x)$ פרימיטיביים
$\Leftarrow$ כל ה-$q_i(x)$ גם אי-פריקים ב-$R[x]$ לפי הטענה הקודמת.

נשאר להוכיח יחידות. נניח שיש שני פירוקים

$$q = q_1 q_2 \cdots q_r = q_1' q_2' \cdots q_s',$$

$$q_i, q_i' \in R[x]$$

אז q פרימיטיבי $\Leftarrow$ q_i, q_i' גם פרימיטיביים, לכן אי-פריקים ב-$F[x]$. ב-$F[x]$ יש יחידות של הפירוק
לכן, עד כדי מספור מחדש של ה-q_i-ים, $r=s$, וגם q_i חבר של q_i' (ב-$F[x]$) לכל $1 \le i \le r$. ההפיכים של $F[x]$ הם הסקלרים הלא אפסיים, לכן $q_i'(x) = \frac{r_i}{s_i} q_i(x)$ לכל i:

לכן $\underbrace{s_i q_i'(x)}_{\text{gcd של המקדמים הינו } s_i} = \underbrace{r_i q_i(x)}_{\text{gcd של המקדמים הינו } r_i}$ שוויון של פולינומים ב-$R[x]$.

(q_i, q_i' פרימיטיביים).

לכן s_i, r_i הם gcd של אותה קבוצה של איברים של R (המקדמים של אותו פולינום).

ה-gcd מוגדר עד כדי חברות $\Leftarrow$ s_i, r_i חברים ב-R $\Leftarrow$ $r_i = s_i u$ כאשר $u \in R$ הפיך,

לכן $q_i' = \frac{r_i}{s_i} q_i = u q_i$ חברים גם ב-$R[x]$.

הוכחנו כי $R[x]$ הינו תחום פריקות יחידה.

מסקנה R תפ"י $\Leftarrow$ $R[x_1, \dots, x_n]$ גם תפ"י.

הוכחה אינדוקציה. $R[x,y] = (R[x])[y]$

$$x^2 y + x^6 y^3 - x^5 y = (x^6) \cdot y^3 + (x^2 - x^5) y$$

מסקנה R תפ"י $\Leftarrow$ $R[x_1, x_2, x_3, \dots]$ (חוג פולינומים באינסוף של נעלמים) גם תפ"י.

הוכחה $$S = \underbrace{R[x_1, x_2, \dots]}_{\text{לכל איבר יש מספר סופי של מונומים.}} = \bigcup_{n=1}^{\infty} R[x_1, \dots, x_n]$$

תרגיל: אם $f \in R[x_1, \dots, x_n]$ אי-פריק אזי f אי-פריק גם כאיבר של S.

יהי $f\in S$. אזי קיים n מינימלי

כך ש- $f\in R[x_1,\dots,x_n]$. אזי החוג

הנ"ל הוא תפ"י, לכן יש ל-f פירוק יחיד

לאי-פריקים של $R[x_1,\dots,x_n]$, לכן של S.

<u>תוצאה</u> תפ"י לא בהכרח חוג נתרי.

הוכחה $S=\mathbb{R}[x_1,x_2,x_3,\dots]$.

אזי S תפ"י לפי הנ"ל, אבל

$$(x_1)\underset{x_2}{\subsetneq}(x_1,x_2)\underset{x_3}{\subsetneq}(x_1,x_2,x_3)\subseteq\dots$$

שרשרת עולה אינסופית של אידיאלים של S,

לכן S לא נתרי.