הרצאה 12

יהי R תפ"י, בהינתן פולינום $f(x)\in R[x]$ איך נוכל לדעת מתי f אי-פריק.

הוכחנו בפעם שעברה:

טענה יהי F שדה. לפולינום $f(x)\in F[x]$ יש גורם לינארי אם ורק אם יש לו שורש.

מסקנה יהי R תפ"י, $f(x)\in R[x]$ פולינום פרימיטיבי ממעלה 2 או 3.
אזי $f(x)$ אי-פריק $\iff$ אין לו שורש ב- $F=\mathrm{Frac}\,R$.

הוכחה $f(x)$ פרימיטיבי. לכן, לפי הלמה של גאוס,
$f(x)$ פריק ב- $R[x]$ $\iff$ $f(x)$ פריק מעל $F[x]$
$\iff$ יש לו פירוק $f(x)=g(x)h(x)$ לגורמים לא
הפיכים, לכן $\deg g\geq 1$, $\deg h\geq 1$. אבל אם $\deg f(x)\leq 3$,

אזי $\deg g=1$ או $\deg h=1$ $\iff$ ל- $f(x)$ ב- $F[x]$
יש גורם לינארי $\iff$ יש לו שורש.

<u>דוגמא:</u> 1) $f(x)=6x^2-x-1 \in \mathbb{Z}[x]$

$$f\left(\tfrac{1}{2}\right)=6\cdot\tfrac{1}{4}-\tfrac{1}{2}-1=0$$

ואכן $f(x)=(2x-1)(3x+1)$ והשורשים הם $\frac{1}{2},-\frac{1}{3}\in \mathbb{Q}\setminus\mathbb{Z}$.

לכן צריך לחפש שורשים ב-F ולא רק ב-R.

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

$$x^4+5x^2+6 \in \mathbb{Z}[x]$$

הוא פריק אבל אין לו שורשים ב-$F=\mathbb{Q}$.

לכן הטענה הקודמת לא נכונה עבור פולינומים ממעלה 4 או יותר.

<u>שאלה:</u> בהינתן פולינום, איך נמצא האם יש לו שורש?

<u>הערה:</u> יהי R גפ"י. נניח כי $c|ab$. אם $\gcd(c,a)=1$ אזי $c|b$.

<u>טענה:</u> יהי R גפ"י, יהי $f(x)=a_nx^n+\dots+a_1x+a_0\in R[x]$ פולינום. יהי $\alpha=\frac{r}{s}\in F$ שורש. נניח שזה שבר מצומצם, כלומר $\gcd(r,s)=1$: אזי $r|a_0$ וגם $s|a_n$.

<u>הוכחה</u> נציב את α בתוך $f(x)$:

$$0 = f(\alpha) = a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \dots + a_1\left(\frac{r}{s}\right) + a_0$$

נכפול את שני האגפים ב-s^n ונעביר אגף:

$$-a_0 s^n = a_n r^n + a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} =$$
$$r\left(a_n r^{n-1} + \dots + a_1 s^{n-1}\right)$$

אגף ימין מתחלק ב-r, לכן אגף שמאל גם כן. אז
$r|a_0 \Leftarrow \gcd(r,s)=1$ לפי ההערה הקודמת.

$$-a_n r^n = a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} + a_0 s^n =$$
$$s\left(a_{n-1} r^{n-1} + \dots + a_0 s^{n-1}\right)$$

לכן $s|(-a_n r^n)$ אך $s|a_n \Leftarrow \gcd(r,s)=1$.

<u>דוגמא</u> $f(x) = x^5 + 4x^4 - 3x^3 + 16x^2 - 17x + 1 \in \mathbb{Z}[x]$

לפי הטענה, אם יש שורש ב-$\mathbb{Q}$ הוא חייב
להיות $\frac{r}{s}$ כאשר $\begin{matrix} r|1 \\ s|1 \end{matrix} \Leftarrow \begin{matrix} r=\pm1 \\ s=\pm1 \end{matrix} \Leftarrow \frac{r}{s}=\pm1$

בודקים כי ±1 לא שורשים, לכן אין כלל שורשים.

<u>טענה</u> יהי R תחום שלמות, יהי I אידיאל (אמתי) <u>ראשוני</u>.

יהי $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in R[x]$ פולינום מתוקן

נסמן את ההומ' $\varphi : R[x] \longrightarrow (R/I)[x]$

ויהי $\bar{f} = \varphi(f) = x^n + \bar{a}_{n-1}x^{n-1} + \dots + \bar{a}_0 \in (R/I)[x]$.

אם $\bar{f}$ אי-פריק, אזי f גם אי-פריק.

<u>הערה</u> צריך להניח כי $f(x)$ מתוקן. אחרת ניקח

$$f(x) = (2x+1)(x+1) = 2x^2 + 3x + 1 \in \mathbb{Z}[x]$$

ניקח $R = \mathbb{Z}$, $I = 2\mathbb{Z}$

$$\bar{f} = x+1 \in (\mathbb{Z}/2\mathbb{Z})[x]$$

אי-פריק, למרות ש-f היה פריק.

<u>דוגמה</u> אם $\bar{f}$ פריק, זה לא אומר כי f אי-פריק.

לדוגמה,

$f(x) = x^2 + 3x - 19 \in \mathbb{Z}[x]$ אי-פריק.

$$\bar{f} = x^2 - 1 = (x-1)(x+1) \in (\mathbb{Z}/3\mathbb{Z})[x]$$

<u>תרגיל</u> 1) $f(x) = x^4 + 1 \in \mathbb{Z}[x]$ אי-פריק אבל הרדוקציה מודולו כל אידיאל ראשוני לא-אפסי פריק.

2) $f(x) = x^4 - 72x^2 + 4 \in \mathbb{Z}[x]$ אי-פריק אך הרדוקציה מודולו כל אידיאל לא-אפסי פריקה.

הוכחה נניח בשלילה כי $\bar{f}$ אי-פריק אך f פריק.

יהי $f(x)=g(x)h(x)$ פירוק לגורמים לא הפיכים.

אזי המקדמים העליונים של g,h הפיכים.

$$g(x)=b_m x^m+\dots$$
$$h(x)=c_\ell x^\ell+\dots$$

$g(x)h(x)=b_m c_\ell x^{m+\ell}+\dots$ כי R תחום שלמות.

לכן $b_m c_\ell=1$, אזי b_m, c_ℓ הפיכים. לכן,

$\deg g \geq 1$
$\deg h \geq 1$
כי אחרת יהיו הפיכים.

נפעיל את ההומומורפיזם $\varphi: R[x] \to (R/I)[x]$

$\bar{f}=\bar{g}\bar{h}$

$$\left.\begin{aligned}\deg \bar{g} &= \deg g\\ \deg \bar{h} &= \deg h\end{aligned}\right\}$$
כי המקדמים העליונים הפיכים. לכן לא שייכים ל-I

הנחנו כי I ראשוני, לכן R/I תחום שלמות, לכן $\left((R/I)[x]\right)^* = (R/I)^*$, לכן $\bar{g},\bar{h}$ לא הפיכים. בסתירה להנחה ש-$\bar{f}$ היה אי-פריק.

טענה (הקריטריון של אייזנשטיין) יהי R תחום שלמות, $P \triangleleft R$ אידיאל ראשוני, ויהי $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0\in R[x]$ פולינום מתוקן כך ש- $\overset{\deg f \geq 1}{\frown}$ $a_0,a_1,\dots,a_{n-1}\in P$, $a_0\notin P^2$ אזי $f(x)$ אי-פריק.

דוגמא $x^7+5x^6-10x^5+125x^4+75x^3-15x^2+625x-10 \in \mathbb{Z}[x]$ אי-פריק, $P=5\mathbb{Z}$

הוכחה נניח בשלילה כי $f(x)$ פריק. $f(x)=g(x)h(x)$ כאשר g,h לא הפיכים.

ניקח רדוקציה מודולו P:

$$g(x)=b_mx^m+\dots+b_0$$
$$h(x)=c_\ell x^\ell+\dots+c_0$$

b_m,c_ℓ הפיכים כמו בהוכחה הקודמת.

R/P תחום שלמות. לכן

$\bar{f}=x^n$ (כאשר המקדמים של f שייכים ל-P) ולכן נקבל ברדוקציה

$$x^n=\bar{f}=\bar{g}\bar{h}=\bar{b}_m\bar{c}_\ell x^{m+\ell}+\dots+\bar{b}_0\bar{c}_0$$

לכן, $\bar{b}_0\bar{c}_0=0$, כי לאגף השמאלי אין איבר חופשי.

אך R/P תחום שלמות כי P ראשוני, לכן $\bar{b}_0=0$ או $\bar{c}_0=0$.

נניח בלי הגבלת הכלליות כי $\bar{b}_0=0$. אני טוען כי $\bar{c}_0=0$.

אחרת, נניח שלא. אזי

$$\bar{g} = \bar{b}_m x^m + \dots + \bar{b}_k x^k, \quad k>0, \quad k<n \qquad m,\ell<n$$
$$\bar{b}_k \neq 0$$

$$\bar{h} = \bar{c}_\ell x^\ell + \dots + \bar{c}_0, \qquad \bar{c}_0 \neq 0$$

$$\bar{f} = \bar{g}\bar{h} = \underbrace{\bar{b}_m \bar{c}_\ell x^{m+\ell}}_{=x^n} + \dots + \underbrace{\bar{b}_k \bar{c}_0 x^k}_{\text{שונה מאפס}} \neq x^n$$

כי $\bar{b}_k \neq 0$, $\bar{c}_0 \neq 0$

אבל $\bar{f} = x^n$, סתירה.

לכן, $\bar{b}_0 = \bar{c}_0 = 0 \Rightarrow b_0 \in P$, $c_0 \in P$. זה אומר כי

$$a_0 = b_0 c_0 \in P^2$$

בסתירה.

<u>טענה</u> יהי R חוג, אזי R נותרי מימין/נותרי משמאל $\iff$ כל אידיאל ימני/שמאלי של R נוצר סופית, כלומר נוצר ע"י מספר סופי של איברים.

הוכחה ($\Rightarrow$) נניח שכל אידיאל שמאלי נוצר סופית. נניח
בשלילה כי R לא נותרי שמאלי. אזי יש
שרשרת עולה של אידיאלים שמאליים

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq I_4 \subsetneq \cdots$$

הראינו כי $I = \bigcup_{n=1}^{\infty} I_n$ הינו אידיאל שמאלי אלמגי. לכן

$I=(a_1,a_2,\dots,a_r)$. לכל a_i קיים $n_i\in\mathbb{N}$

כך ש- $a_i\in I_{n_i}$. יהי $n=\max\{n_1,\dots,n_r\}$.

אזי $a_1,a_2,\dots,a_r\in I_n \Rightarrow I=I_n \Rightarrow$

$$I_n=I_{n+1}=I_{n+2}=\cdots$$

השרשרת מתייצבת בסתירה להנחה.

($\Leftarrow$) נניח שקיים אידיאל I שאינו נוצר סופית.

יהי $0\neq a_1\in I$.

$(a_1)\neq I$ כי I לא נוצר סופית. אז יהי

$a_2\in I\setminus(a_1)$.

$a_3\in I\setminus(a_1,a_2)$

$a_4\in I\setminus(a_1,a_2,a_3),\dots$

$$\overset{Ra_1}{(a_1)} \subsetneq \overset{Ra_1+Ra_2}{(a_1,a_2)} \subsetneq (a_1,a_2,a_3) \subsetneq \cdots \quad \text{אזי}$$

שרשור עולה אינסופי של אידאלים ממש,
לכן R לא נתרי ממש.

<u>משפט</u> (משפט הבסיס של הילברט) יהי R חוג נתרי מימין/משמאל. אזי $R[x]$ גם נתרי מימין/משמאל.

<u>מסקנה</u> יהי F שדה. אזי F נתרי "במובן הריק".
אזי $F[x_1,\dots,x_n]$ גם נתרי באינדוקציה.
לכן, תהי $X \subseteq F^n$ יריעה אלגברית, כלומר קבוצה שניתן להגדיר אותה על ידי התאפסות של פולינומים.

$$I = \{f \in F[x_1,\dots,x_n] : f(a_1,\dots,a_n) = 0 \ \forall (a_1,\dots,a_n) \in X\} \trianglelefteq F[x_1,\dots,x_n]$$

החוג נתרי, לכן I נוצר סופית $I=(f_1,\dots,f_r)$

לכן
$$X = \{(a_1,\dots,a_n) \in F^n \mid f_1(a_1,\dots,a_n) = \dots = f_r(a_1,\dots,a_n) = 0\}$$

כלומר ניתן להגדיר את X על ידי התאפסות של מספר סופי של פולינומים.

הוכחה יהי R נותרי. יהי $I \trianglelefteq R[x]$ אידיאל כלשהו!

אנחנו צריכים להוכיח כי I נוצר סופית. לכל $n \geq 0$,

נגדיר

$$J_n = \left\{ a \in R \;\middle|\; \begin{array}{l} a \text{ הינו המקדם המוביל} \\ \text{של } f \in I \text{ כך ש-} \\ \deg f = n \end{array} \right\}.$$

(כולל 0 כמקדם מוביל)

תת-טענה כל J_n הינו אידיאל של R.

תת-הוכחה יהיו $a, b \in J_n$ $\Leftarrow$ קיימים

$$I \ni f(x) = ax^n + a_{n-1}x^{n-1} + \dots + a_0$$

$$I \ni g(x) = bx^n + \dots + b_0$$

אזי $f - g = (a-b)x^n + \dots + (a_0 - b_0) \in I$

ולכן $a - b \in J_n$.

לכל $r \in R \subseteq R[x]$,

$$r \cdot f(x) = rax^n + \dots + ra_0 \in I$$

ולכן $ra \in J_n$.

לכן J_n הינו אידיאל של R.

נשים לב כי $J_n \subseteq J_{n+1}$ לכל n.

כי $a \in J_n$ $\Leftarrow$ יש פולינום $ax^n + \dots + a_0 = f(x) \in I$

ואז $x\cdot f(x) = ax^{n+1}+\dots+a_0 \in I$

לכן $a\in J_{n+1}$.

קיבלנו שרשרת עולה של אידיאלים שמאליים

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$$

R נותרי שמאלי, לכן מתייצבת: קיים N כך ש-

$$J_N = J_{N+1} = J_{N+2} = \dots$$

לכל $N\geq i\geq 0$, נבחר קבוצה סופית של יוצרים

של J_i (אפשר כי R נותרי שמאלי)

$$J_i = Ra_{i1}+\dots+Ra_{ir_i} \qquad r_i\in\mathbb{N}$$

לכל יוצר $a_{ij}\in J_i$ נבחר פולינום $f_{ij}\in I$

ממעלה i ועם מקדם מוביל a_{ij}. נגדיר

$$I' = Rf_{11}+\dots+Rf_{Nr_N} \trianglelefteq_\ell R[x]$$

האידיאל השמאלי הנוצר על ידי כל ה-f_{ij}-ים.

הוא נוצר סופית. <u>טענה</u> $I=I'$ ולכן I נוצר סופית.