הרצאה 10

בפעם שעברה: אם R תפ"י, אזי $R[x]$ גם תפ"י.

איך נבדוק האם פולינום אי-פריק?

יהי R תפ"י, $f(x)\in R[x]$, יהי d ה-gcd של המקדמים של f. אזי $f=d\cdot g(x)$ כאשר $g(x)$ פרימיטיבי. הפירוק של d זו שאלה על R ולא על פולינומים. אז נניח $f(x)$ פרימיטיבי. טוב כן, לפי הלמה של גאוס, $f(x)$ אי-פריק ב-$R[x]$ $\iff$ $f(x)$ אי-פריק ב-$F[x]$, כאשר $F=\mathrm{Frac}\,R$ שדה השברים.

<u>טענה</u> יהי F שדה, $f(x)\in F[x]$, אזי יש ל-f גורם (אי-פריק) ממעלה 1 $\iff$ יש ל-f שורש ב-F, כלומר $\alpha\in F$ כך ש- $f(\alpha)=0$.

הוכחה ⇐) יהי $f(x)=g(x)h(x)$ כאשר

$g(x)=ax+b$ ממעלה 1. יהי $\alpha=-\frac{b}{a}\in F$.

אזי $f(\alpha)=\overset{0}{\cancel{g(\alpha)}}h(\alpha)=0 \Leftarrow \alpha$ הינו שורש של f.

⇒) יהי α שורש. נזכור ש-$F[x]$ הינו תחום אוקלידי, ניתן לחלק עם שארית:

$$f(x)=q(x)\cdot(x-\alpha)+r(x)$$

כאשר $\deg r<\deg(x-\alpha)=1 \Leftarrow \deg r=0 \Leftarrow$

r קבוע.

$$f(x)=q(x)\cdot(x-\alpha)+r$$
$$f(\alpha)=q(\alpha)\cdot(\alpha-\alpha)+r=r$$

היות $f(\alpha)=0 \Leftarrow r=0 \Leftarrow f(x)=q\cdot(x-\alpha)$,

לכן יש ל-f גורם לינארי.

מסקנה יהי F שדה, $f(x)\in F[x]$ פולינום ממעלה 2 או 3. אזי f פריק $\Leftrightarrow$ יש לו שורש ב-F.

טענה: יהי R תחום גאוס, יהי

$f(x)=a_nx^n+\dots+a_1x+a_0\in R[x]$.

יהי $\frac{r}{s}=\alpha\in F=\mathrm{Frac}\,R$ שבר מצומצם (כלומר $r,s\in R$, $\gcd(r,s)=1$). אם α הינו שורש של $f(x)$, אזי $r|a_0$ וגם $s|a_n$.

הוכחה: נניח כי $\alpha=\frac{r}{s}$ הינו שורש, ולכן:

$$f(\alpha)=\frac{a_nr^n}{s^n}+\frac{a_{n-1}r^{n-1}}{s^{n-1}}+\dots+\frac{a_1r}{s}+a_0=0$$

נכפיל ב-s^n:

$$a_nr^n+a_{n-1}r^{n-1}s+\dots+a_1rs^{n-1}+a_0s^n=0$$

בפרט:

$$a_0s^n=-r(a_nr^{n-1}+\dots+a_1s^{n-1})$$

$$a_nr^n=-s(a_{n-1}r^{n-1}+\dots+a_0s^{n-1})$$

לכן: $r|a_0s^n$. אבל, r זר ל-s, לכן ל-s^n. לכן כל המחלקים הא"פ-פריקים של r מופיעים ב-a_0 $\Leftarrow$ $r|a_0$.

כמו כן: $s|a_nr^n$ $\Leftarrow$ $s|a_n$.

דוגמא: $f(x)=x^3+5x^2-11x+4\in\mathbb{Z}[x]$ אי-פריק.

הוכחה לפי הטענה, המועמדים להיות שורש ב-$\mathbb{Q}$ הם $\pm4, \pm2, \pm1$. בודקים שאף אחד מאלה אינו שורש.

טענה יהי R חוג שלמות, $I\triangleleft R$ אידיאל ראשוני. אזי העתקה הטבעית $\varphi: R\to R/I$ משרה הומ' $\varphi: R[x]\to (R/I)[x]$
$f(x)\mapsto \bar{f}(x)$.

יהי $f(x)\in R[x]$ פולינום מתוקן (מקדם עליון $=1$) וכי $\deg f\geq 1$. אם $\bar{f}\in (R/I)[x]$ לא מתפרק למכפלה של שני גורמים עם מעלה נמוכה יותר אזי $f(x)\in R[x]$ אי-פריק.

הוכחה נניח שלא, אזי $f(x)$ פריק. יהי $f(x)=g(x)h(x)$ בירור לגורמים לא הפיכים. R חוג שלמות, לכן המכפלה של המקדמים העליונים של g,h = מקדם העליון של f $=1$. לכן המקדמים העליונים של g,h הינם הפיכים.

לכן לא שייכים ל-I. לכן $\deg \bar{g} = \deg g$
$\deg \bar{h} = \deg h$

בנוסף, g, h לא יחידים (כי פולי' יחידה עם מקדם עליון הפיך הינו הפיך) לכן $\deg g, \deg h < \deg f$. גם $\deg \bar{f} = \deg f$.

לכן הפירוק $\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$ הינו פירוק לגורמים ממעלה נמוכה יותר, בסתירה להנחה.

__דוגמא:__ $f = x^3 + 81x^2 - 231x + 144 \in \mathbb{Z}[x]$ אי-פריק.

אכן, ניקח $I = 3\mathbb{Z}$.

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

לפולינום $\bar{f}$ אין שורשים, לכן f אי-פריק.

__אזהרה:__ ההפך של הטענה לא נכון.

$f(x) = x^2 + 3x + 83 \in \mathbb{Z}[x]$ אי-פריק.

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

דוגמאות לתרגול נוסף:

1) $x^4+1\in\mathbb{Z}[x]$ אי-פריק, אבל הרדוקציה מודולו כל אידאל ראשוני הינה פריקה.

2) $x^4-72x^2+4\in\mathbb{Z}[x]$ אי-פריק, אבל $\bar{f}$ פריקה לכל אידאל $0\neq I\triangleleft\mathbb{Z}$.

<u>טענה</u> (קריטריון של אייזנשטיין). יהי R תחום שלמות, $P\triangleleft R$ אידאל ראשוני.

יהי $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0\in R[x]$ פולינום מתוקן. אם $a_0,\dots,a_{n-1}\in P$ אך $a_0\notin P^2$, אזי $f(x)$ אי-פריק.

$$P^2=P\cdot P$$

$$IJ=\left\{r_1i_1j_1+\dots+r_ni_nj_n : \begin{array}{l} r_k\in R \\ i_k\in I,\ j_k\in J\end{array}\right\}$$

<u>הוכחה</u> נפעיל את הטענה הקודמת במקרה $I=P$. מספיק להוכיח שלרדוקציה $\bar{f}\in(R/P)[x]$ אין פירוק לגורמים ממעלה נמוכה יותר.

אך $\bar{f} = x^n$. נניח בשלילה שקיים פירוק

$\bar{f} = g \cdot h$, אך R/p תחום שלמות, כי

p ראשוני. לכן,

$0 =$ (מקדם החפשי של $\bar{f}$) $=$ (מקדם החפשי של g)(מקדם החפשי של h)

לכן אחד מן המקדמים החפשיים של g,h

(נניח של g) הינו 0. אני טוען כי המקדם

החפשי של h גם 0. אחרת:

$$g = x^k + \dots + \underbrace{a_\ell x^\ell}, \quad h = x^{n-k} + \dots + \underbrace{b_0}_{\neq 0}$$

$0<\ell$, ש-$\neq 0$

המונום ממעלה הכי נמוכה.

אך

$$x^n = \bar{f} = gh = x^n + \underbrace{a_\ell b_0}x^\ell$$

מונום לא אפסי

ממעלה $n>\ell$.

סתירה.

לכן המקדמים החפשיים של g,h שניהם 0.

נניח בשלילה כי $f(x)$ פריק

אזי $f(x)=\tilde{g}(x)\cdot\tilde{h}(x)$.

$x^n=\bar{f}=\bar{\tilde{g}}\cdot\bar{\tilde{h}}$. לפי מה שעשינו

הוכחנו גם ל- $\bar{\tilde{g}}$ וגם ל $\bar{\tilde{h}}$ יש מקדם

חפשי 0 $\Leftarrow$ הגורמים החופשיים של $\tilde{h},\tilde{g}$

שייכים ל- P $\Leftarrow$ a_0 שהוא המכפלה של

הגורמים החופשיים של $\tilde{g},\tilde{h}$ $\Leftarrow$ $a_0\in P^2$,

סתירה.

<u>דוגמא</u> $x^4+1\in\mathbb{Z}[x]$ אי-פריק

יהי $g(x)=(x+1)^4+1$. ברור כי

$g(x)$ אי-פריק $\Leftrightarrow$ x^4+1 אי-פריק.

$g(x)=h_1(x)h_2(x) \Leftrightarrow x^4+1=h_1(x-1)\cdot h_2(x-1)$

אך $g(x)=x^4+4x^3+6x^2+4x-2\in\mathbb{Z}[x]$

כי מקיים את הקריטריון של אייזנשטיין עבור

$P=2\mathbb{Z}$ $\Leftarrow$ $g(x)$ אי-פריק $\Leftarrow$ x^4+1 אי-פריק

<u>תזכורת</u> יהי R חוג לאו בהכרח חילופי.

R נקרא נתרי משמאל (מימין) אם כל סדרה עולה של אידאלים שמאליים (ימניים)

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

מתייצבת, כלומר קיים N כך ש:

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

אם R חילופי, אזי נתרי מימין = נתרי משמאל, ואומרים פשוט נתרי.

הוכחנו בתרגול: R נתרי משמאל/מימין $\Longleftrightarrow$ כל אידאל שמאלי/ימני של R נוצר סופית.

<u>טענה</u> יהי R חוג נתרי משמאל/מימין. יהי $I \triangleleft R$ אידאל שמאלי/ימני. אזי R/I נתרי משמאל/מימין.

<u>הוכחה</u> לפי משפט האיזו' הרביעי, אם יש סדרה לא-מתייצבת של אידאלים של R/I,

נוכל להביא דוגמה לשרשרת עולה לא מתייצבת של אידאלים של R שמכילים I, בסתירה לנתריות של R.

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

<u>הוכחה</u> כדי לא להגיד מימין/משמאל כל הזמן ניתן הוכחה עבור R חילופי, אותה הוכחה נכונה במקרה הכללי)

יהי $I \trianglelefteq R[x]$ אידאל. רוצים להוכיח שהוא נוצר סופית. נגדיר:

$$J = \{ r \in R \mid r \text{ הינו מקדם עליון של איבר של } I \}$$

לכל $n \in \mathbb{N}$

$$J_n = \{ r \in R \mid r \text{ מקדם עליון של } f \in I,\ \deg f \leq n \}$$

אני טוען כי J, J_n כולם אידאלים של R.

סגירות לחיבור של J_n: יהיו $a, b \in J_n$.

קיימים $f, g \in I$, $\deg f, \deg g \leq n$ כך ש-

$f(x)=ax^m+\cdots$, $g(x)=bx^\ell+\cdots$

נניח בלי הגבלת הכלליות כי $\ell\le m$. אזי

$$I\ni f(x)+g(x)\cdot x^{m-\ell}=(a+b)x^m+\cdots$$

לכן $a+b\in J_n$. כמו כן לכל $r\in R$,

$I\ni rf(x)=rax^m+\cdots \Rightarrow ra\in J_n$.

כמובן $J_1\subseteq J_2\subseteq J_3\subseteq J_4\subseteq\cdots$ לכן

$J=\bigcup_{n=1}^{\infty}J_n$ גם אידיאל

<u>שלב 2</u> לפי ההנחה, R נותרי, לכן J

נוצר סופית. יהי $J=(r_1,\dots,r_k)$. ויהיו

$f_1,\dots,f_k\in I$ עם מקדמים מובילים $r_1,\dots,r_k$.

נבחר $N\ge\max\{\deg f_1,\dots,\deg f_k\}$. לכל $1\le j\le N$

יהי $J_j=(r_{1j},r_{2j},\dots,r_{k_jj})\trianglelefteq R$,

ויהיו $f_{1j},\dots,f_{k_jj}\in I$ כך שהמקדמים

המובילים הם r_{ij}, וגם $\deg f_{ij}\le j$.

נגדיר

$$I' = (f_1, \dots, f_k, f_{ij})_{\substack{1 \le j \le N \\ 1 \le i \le k_j}} \trianglelefteq R$$

המטרה היא להוכיח כי $I = I'$, ולכן

I נוצר סופית. ברור כי $I' \subseteq I$.