תזכורת:

אם R תחו"י, אזי $R[x]$ גם תחו"י

איך נדע האם פולינום הוא אי פריק?

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

טענה:

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

הוכחה:

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

אזי $f(\alpha)=g(\alpha)h(\alpha)=0h(\alpha)=0 \Leftarrow \alpha$ הוא שורש של f.

($\Longrightarrow$) יהי α שורש. כיוון ש-$F[x]$ הוא תחום אוקלידי, ניתן לחלק עם שארית: $f(x)=q(x)(x-\alpha)+r(x)$. כאשר $\deg r<\deg(x-\alpha)=1 \Leftarrow \deg(r)=0 \Leftarrow r$ קבוע

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

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

הנחנו $f(\alpha)=0 \Leftarrow r=0 \Leftarrow f(x)=q(x-\alpha)$, לכן יש ל-$f$ גורם לינארי.

תוצאה:

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

טענה:

יהי R תפ"י, יהי $f(x)=a_nx^n+\ldots+a_1x+a_0\in R[x]$. יהי $\frac{r}{s}=\alpha\in F=Frac R$ 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 ונציב:

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

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 של r מופיעים ב-$a_0 \Rightarrow r|a_0$. כמו כן: $s|a_nr^n \Rightarrow s|a_n$ (המקרה בו יש את אותו גורם כמה פעמים - תרגיל)

דוגמא:

$f(x)=x^3+5x^2-11x+4\in \mathbb{Z}[x]$ א"פ

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

טענה:

יהי R תחום שלמות, $I\triangleleft R$ אידיאל ראשוני. אזי העתקה הטבעית $\varphi:R\to(R/I)[x]$

$f(x)\mapsto\bar{f}(x)$

יהי $f(x)\in R[x]$ פולינום מתוקן (מקדם עליון $=1$) ו- $\deg f\geq1$. אם $\bar{f}\in(R/I)[x]$ מתפרק למכפלה של שני גורמים עם מעלה נמוכה יותר אזי $f(x)\in R[x]$ א"פ.

הוכחה:

נניח שלא, אזי $f(x)$ פריק. יהי $f(x)=g(x)h(x)$ פירוק. אזי R תחום שלמות, לכן המכפלה של המקדמים העליונים של g,h = המקדם העליון של $f=1$. לכן המקדמים העליונים של h,g הפיכים, לכן לא שייכים ל-I. לכן $\deg\bar{g}=\deg g$, $\deg\bar{h}=\deg h$

בנוסף, g,h לא קבועים (כי פולינום קבוע עם מקדם עליון הפיך הוא הפיך), לכן, $\deg h<\deg f$, $\deg g$. גם $\deg\bar{f}=\deg f$ לכן הפירוק $\bar{f}(x)=\bar{g}(x)\bar{h}(x)$

הוגו פירוק לגורמים ממעלה נמוכה יותר, בסתירה להנחה

דוגמא:

$f=x^3+81x^2-231x+1444\in\mathbb{Z}[x]$ אי פריק

ואז ניקח $I=3\mathbb{Z}$

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

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

הערה: ההפך של הטענה לא נכון: $f(x)=x^2+3x+83\in\mathbb{Z}[x]$ אי פריק.

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

דוגמאות נוספות:

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

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

טענה (קריטריון של אייזנשטיין):

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

$$\left(IJ=\{r_1i_1j_1+\dots+r_ni_nj_n : r_k\in R,\ i_k\in I,\ j_k\in J\},\quad P^2=P\cdot P\right)$$

הוכחה:

נפעיל את הטענה הקודמת במקרה $I=P$ מספיק להוכיח שלרדוקציה $\bar{f}\in\left(R/P\right)[x]$ אין פירוק לגורמים ממעלה נמוכה יותר. אבל $\bar{f}=x^n$. נניח בשלילה שקיים פירוק $\bar{f}=\bar{g}\cdot\bar{h}$, אך R/P תחום שלמות (כי P ראשוני). לכן,

$$0=\left(\text{מקדם חופשי של } \bar{f}\right)=\left(\text{מקדם חופשי של } \bar{g}\right)\left(\text{מקדם חופשי של } \bar{h}\right)$$

לכן אחד מהמקדמים החופשיים של $\bar{h},\bar{g}$ (ונניח של $\bar{g}$) הוא 0. נטען כי המקדם החופשי של $\bar{h}$ גם 0. אחרת:

(המונום ממעלה ה.כ' נמוכה) $\ell>0$ $a_\ell\neq 0$

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

אזי $x^n = \bar{f} = \bar{g}\bar{h} = x^n + \underbrace{a_\ell b_0}_{} x^\ell$ בסתירה.

מונום
לא אפסי ממעלה
חיובית

לכן המקדמים החופשיים של g,h שניהם 0. נניח בשלילה כי $f(x)$ פריק. $f(x)=\tilde{g}(x)\tilde{h}(x)$.

אזי $x^n=\bar{f}=\bar{\tilde{g}}\cdot\bar{\tilde{h}}$. לפי מה שהוכחנו, גם ל-$\bar{\tilde{g}}$ וגם ל-$\bar{\tilde{h}}$ יש מקדם חופשי 0 $\Leftarrow$

$\Leftarrow$ המקדמים החופשיים של $\tilde{g},\tilde{h}$ שייכים ל-P $\Leftarrow$ a_0 הוא המכפלה של המקדמים החופשיים של $\tilde{g},\tilde{h}$ $\Leftarrow$ $a_0\in P^2$ בסתירה

דוגמה:

$x^4+1\in\mathbb{Z}[x]$ אי פריק.

יהי $g(x)=(x+1)^4+1$. ברור כי $g(x)$ אי פריק $\Leftrightarrow$ x^4+1 אי פריק.

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

אבל $g(x)=x^4+4x^3+6x^2+4x-2\in\mathbb{Z}[x]$ - מקיים את הקריטריון של אייזנשטיין עבור

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

תזכורת:

יהי R חוג (לאו בהכרח חילופי). R נקרא נותרי משמאל (מימין) אם כל שרשרת עולה של אידיאלים שמאליים (ימניים) $I_1\subseteq I_2\subseteq I_3\subseteq\dots$ מתייצבת, כלומר קיים N כך ש $I_N=I_{N+1}=I_{N+2}=\dots$

אם R חילופי, אז נותרי משמאל = נותרי מימין, ואומרים פשוט נותרי

ראינו בתרגול: R נותרי משמאל/מימין $\Leftrightarrow$ כל אידאל שמאלי/ימני של R נוצר סופית

טענה:

יהי R חוג נותרי משמאל/מימין. אזי R/I נותרי משמאל/מימין

הוכחה:

לפי משפט האיזו' הרביעי, אם יש שרשרת עולה לא מתייצבת של אידיאלים של R/I, נוכל להפוך אותה לשרשרת לא מתייצבת של אידיאלים של R שמכילים את I, בסתירה לנותריות של R.

משפט (משפט הבסיס של הילברט):

יהי R נותרי משמאל/מימין. אזי $R[X]$ גם נותרי משמאל/מימין

הוכחה:

כדי לא לכתוב מימין/משמאל, נכתוב הוכחה עבור R חילופי (אותה הוכחה נכונה במקרה הכללי). יהי $I \lhd R[x]$ אידאל. רוצים להוכיח שהוא נוצר סופית. נגדיר:

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

לכל $n \in \mathbb{N}$:

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

נטען כי J, J_n כולם אידאלים של R.

סגירות לחיבור של J_n: יהיו $a, b \in J_n$. קיימים $f, g \in I$, $\deg f, \deg g \le n$ כך ש

$f(x) = ax^m + \dots \quad , g(x) = bx^l + \dots$

נניח, בלי הגבלת הכלליות, כי $l \le m$. אזי $I \ni f(x) + g(x) \cdot x^{m-l} = (a+b)x^m + \dots$

לכן $a+b \in J_n$. כמו כן לכל $r \in R$, $I \ni r f(x) = rax^m + \dots \Leftarrow ra \in J_n$.

כמו כן $J_1 \subseteq J_2 \subseteq J_3 \subseteq \dots$ לכן $J = \bigcup_{n=1}^{\infty} J_n$ גם אידאל.

שלב ב: לפי ההנחה, R נותרי, לכן J נוצר סופית. יהי $J = (r_1, \dots, r_k)$. יהיו $f_1, \dots, f_k \in I$ עם מקדמים מובילים $r_1, \dots, r_k$. נבחר $N > \max\{\deg f_1, \dots, \deg f_k\}$

לכל $1 \le j \le N$ יהי $J_j = (r_{1j}, r_{2j}, \dots, r_{kj}) \lhd R$

יהיו $f_{1j}, \dots, f_{kj} \in I$ כך שהמקדמים המובילים הם r_{ij}, וגם $\deg f_{ij} \le j$

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

המטרה היא להוכיח כי $I = I'$, ולכן I נוצר סופית. ברור כי $I' \subseteq I$