תזכורת:

R תחום חילופי, $a\in R$. אז a אי פריק אם בכל פירוק $a=bc$ אחד האיברים הפיך

אם a אי פריק, u הפיך $\Leftarrow$ au אי פריק

$I\lhd R$ אידיאל, $I[x]\lhd R[x]=\{$פולינומים עם מקדמים מ-$I\}$

אז $R[x]/I[x]\simeq(R/I)[x]$ בפרט, $I\lhd R$ ראשוני $\iff$ $I[x]\lhd R[x]$ ראשוני

בכל השיעור R יהי תחום שלמות. $F=\mathrm{Frac}R$ שדה השברים $F=\{\frac{r}{s}:r,s\in R,s\neq 0\}$

טענה: (הלמה של גאוס)

יהי R תחום פריקות יחידה, יהי $0\neq f\in R[x]\leq F[x]$

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

דוגמה:

$R=\mathbb{Z}$ $\quad x^3-2x^2+3x-6=(\frac{3}{2}x-3)(\frac{2}{3}x^2+2)$ פריק ב-$\mathbb{Q}[x]$ וכן:

$x^3-2x^2+3x-6=(x-2)(x^2+3)$ פריק ב-$\mathbb{Z}[x]$

הערה: ב-$F[x]$, כל פולינום קבוע לא אפסי הינו הפיך $(\frac{r}{s}\cdot\frac{s}{r}=1)$

הוכחה (של הלמה של גאוס):

יהי $f(x)=g(x)h(x)$ פירוק ב-$F[x]$, לגורמים לא הפיכים. לפי ההערה, g,h לא קבועים. נשים לב שקיימים $a,b\in R$ כך ש $ag(x),bh(x)\in R[x]$. לדוגמה: תהי a המכפלה של המכנים של המקדמים של $g(x)$, וכו'. יהי $d=ab$ אז

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

יהי $d=p_1\cdot\ldots\cdot p_r$ פירוק של $d\in R$ לגורמים אי פריקים (קיים כי R תפ"י)

ברור שכל מקדם של $df(x)$ מתחלק ב-d, לכן גם ב-p_r. לכן $df(x)\in(p_r)[x]\lhd R[x]$

יהי $\varphi:R[x]\to(R/(p_r))[x]\simeq R[x]/(p_r)[x]$

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

אבל P_r אי פריק $\Leftarrow$ P_r ראשוני $\Leftarrow$ $(P_r) \triangleleft R$ ראשוני $\Leftarrow$ $(P_r)[x] \triangleleft R[x]$ ראשוני $\Leftarrow$

$\Leftarrow$ $\left(R/_{(P_r)}\right)[x]$ תחום שלמות $\Leftarrow$ $\varphi(\hat{g})=0$ או $\varphi(\tilde{h})=0$. נניח $\varphi(\hat{g})=0$, אזי כל

מקדם של $\hat{g}(x)$ מתחלק ב-P_r

$$P_1\cdot\ldots\cdot P_{r-1} f(x) = \frac{df(x)}{P_r} = \underbrace{\frac{\hat{g}(x)}{P_r}}_{\in R[x]}\cdot \tilde{h}(x)$$

ממשיכים כך ונפטרים מכל $P_1,\ldots,P_{r-1}$ ומקבלים פירוק של $f(x)$ לגורמים ב-$R[x]$.

אזי הגורמים של $g(x),h(x)$ עד כדי סקלר. אז שני הגורמים לא קבועים ובפרט לא הפיכים. לכן f פריק ב-$R[x]$.

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

טענה:

יהי R תפ"י. יהי $f\in R[x]$ פרימיטיבי. אזי f אי פריק ב-$R[x]$ $\Leftrightarrow$ הוא אי פריק ב-$F[x]$

הוכחה:

($\Leftarrow$) למה של גאוס

($\Rightarrow$) נניח f אי פריק ב-$F[x]$, אבל פריק ב-$R[x]$. $f(x)=g(x)\cdot h(x)$

אזי $g(x),h(x)$ גם פרימיטיביים, כי אם לכל המקדמים של g או h היה מחלק משותף d אזי d גם היה מחלק את 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:

($\Rightarrow$) ברור (נחשוב על $a\in R$ כפולינום קבוע)

(⇐) יהי $f(x)\in R[x]$. אם f קבוע, הטענה ברורה. נניח ש-f לא קבוע. יהי d ה-gcd של המקדמים. אזי $f=dg(x)$ כאשר $g(x)$ פרימיטיבי. מספיק להוכיח של-$g(x)$ יש פירוק יחיד לגורמים אי פריקים (כי פולינום לא קבוע לא פרימיטיבי לא יהיה אי פריק).

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

$$g(x)=p_1(x)\cdot\ldots\cdot p_r(x)$$

כאשר $p_i(x)$ אי פריקים ב-$F[x]$. לפי הלמה של גאוס, $g(x)=q_1(x)\cdot\ldots\cdot q_r(x)$ כאשר $q_i\in R[x]$ הוא כפל סקלרי של $p_i(x)$, לכל $1\le i\le r$.
כל סקלר לא אפסי ב-$F[x]$ הינו הפיך. לכן כל $q_i(x)$ עדיין אי פריק ב-$F[x]$. וכן $g(x)$ 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 $g=q_1\cdot\ldots\cdot q_r=q_1'\cdot\ldots\cdot q_s'$ $(q_i,q_i'\in R[x])$ וכן g 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, $\underbrace{s_iq_i'(x)}_{\text{gcd של המקדמים הוא } s_i}=\underbrace{r_iq_i(x)}_{\text{gcd של המקדמים הינו } r_i}$ שוויון של פולינומים ב-$R[x]$ (q_i',q_i פרימיטיביים)

לכן r_i,s_i הם gcd של אותה קבוצה של איברים של R (המקדמים של אותו פולינום) ה-gcd מוגדר עד כדי חברות $\Leftarrow$ r_i,s_i חברים ב-R $\Leftarrow$ $r_i=s_iu$ כאשר $u\in R$ הפיך, לכן $q_i'=\frac{s_i}{r_i}q_i=uq_i$ חברים גם ב-$R[x]$. והוכחנו כי $R[x]$ הוא תחום פריקות יחידה.

תוצאה:

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

הוכחה:

אינדוקציה. $R[x,y]=(R[x])[y]$ $\quad\left(x^2y+x^6y^3-x^5y=(x^6)y^3+(x^2-x^5)y\right)$

תוצאה:

R תפ"י $\Leftarrow$ $R[x_1,x_2,\dots]$ (חוג פולינומים באינסוף 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, אז f אי פריק גם באיבר של S.

פתרון:

יהי $f\in S$. אז קיים n מתאים כך ש $f\in R[x_1,\dots,x_n]$ אז החוג הזה הוא תפ"י,

לכן יש ל- f פירוק יחיד לאי' פריקים של $R[x_1,\dots,x_n]$, לכן של S

תוצאה:

תפ"י לא בהכרח חוג נתרי

הוכחה:

$S=R[x_1,x_2,\dots]$ אז S תפ"י לפי הנ"ל, ואבל

$$(x_1)\subsetneq(x_1,x_2)\subsetneq(x_1,x_2,x_3)\subsetneq\dots$$

שרשרת עולה אינסופית של אידאלים של S. לכן S לא נתרי