הרצאה 11

R תחום פריקות יחידה (תחום שלמות שבו המשפט היסודי של אריתמטיקה נכון).

$F = \mathrm{Frac}\, R$ שדה השברים (איברים של F הם שברים $\frac{r}{s}$, $r,s\in R$, $s\neq 0$).

<u>משפט</u> (הלמה של גאוס) יהי $f(x)=a_nx^n+\dots+a_0\in R[x]\subseteq F[x]$ פולינום פרימיטיבי (ה-gcd של המקדמים $a_0,a_1,\dots,a_n$ הינו 1 $\Longleftrightarrow$ אין $d\in R$ לא-הפיך כך ש- $d|a_i$ לכל i).

אזי $f(x)$ אי-פריק בחוג $R[x]$ $\Longleftrightarrow$ הוא אי-פריק בחוג $F[x]$.

<u>הערה</u> למה זה לא טריוויאלי? מצד אחד, ב-$F[x]$ יותר אברים. לא יותר אפשרויות לפירוק. מצד שני, ב-$R[x]$ יש איברים לא הפיכים (קבועים לא הפיכים ולא אפסים מחוג R) שנהיים הפיכים ב-$F[x]$ (בו קיים $\frac{1}{r}$) לכן פירוק לגורמים לא-הפיכים מעל $R[x]$ עלול להפוך לפירוק <u>עם</u> גורם הפיך ב-$F[x]$).

<u>הוכחה</u> $\Leftarrow$) נניח כי $f(x)$ פריק ב-$F[x]$. אזי $f(x)=g(x)h(x)$.

הבעיה: לפולינומים g,h עלולים להיות מקדמים שברים;

ואם כן הגורמים לא ב-$R[x]$ קיימים $a,b\in R$ $\tilde{g}=a\cdot g(x)\in R[x]$
$\tilde{h}=b\cdot h(x)\in R[x]$

יהי $d=ab=p_1p_2\cdots p_r\in R$

כי R גפ"י

קיבלנו פירוק $d\cdot f(x)=\tilde{g}(x)\cdot\tilde{h}(x)$ ב-$R[x]$ אבל לא של הפולינום שרצינו. הרעיון שניתן להיפטר מן ה-p_i-ים:

לכל p_i, אחד הגורמים מתחלק ב-p_i.

<u>הערה</u> 1) בהוכחה של הכיוון $\Leftarrow$ לא השתמשנו בפרימיטיביות של f.

2) הוכחנו שאם $f(x)=g(x)h(x)$ פירוק ב-$F[x]$ אזי קיים $\frac{r}{s}\in F^*$ כך ש- $f(x)=\left(\frac{r}{s}g(x)\right)\left(\frac{s}{r}\cdot h(x)\right)$ פירוק ב-$R[x]$.

$$x^3-2x^2+3x-6=\overbrace{\left(\tfrac{3}{2}x-3\right)}^{g}\overbrace{\left(\tfrac{2}{3}x^2+2\right)}^{h}$$
$$=\underbrace{(x-2)}_{\frac{2}{3}g}\underbrace{(x^2+3)}_{\frac{3}{2}h}$$

($\Rightarrow$) נניח כי $f(x)$ פריק ב-$R[x]$, צריך להוכיח שהוא פריק ב-$F[x]$. יהי $\boxed{f(x)=g(x)}\,h(x)$ פירוק ב-$R[x]$. נשים לב כי $\deg g,\deg h\geq 1$. אכן, אם $g(x)=d$ או $h(x)=d$ קבוע, אזי כל המקדמים של $f(x)$ מתחלקים ב-d בסתירה לפרימיטיביות.

לכן, $g(x),h(x)$ לא קבועים, לכן לא הפיכים ב- $F[x]$

כי $F^*=((F[x])^*)$. לכן הפירוק $f(x)=g(x)h(x)$ הינו

גם פירוק לגורמים לא הפיכים ב- $F[x]$, לכן $f(x)$

פריק ב- $F[x]$.

<u>הערה</u> הכיוון $(\Leftarrow)$ לא נכון אם $f(x)$ לא

פרימיטיבי. לדוגמא $R=\mathbb{Z}$

$$2x+2=2(x+1)$$

כל אחד מן הגורמים לא הפיך ב- $\mathbb{Z}[x]$.

אבל 2 כן הפיך ב- $\mathbb{Q}[x]$.

אכן, $2x+2$ כן אי-פריק ב- $\mathbb{Q}[x]$.

<u>הערה</u> הלמה של גאוס נכונה גם אם R תחום gcd

ולאו בהכרח תפ"י אך ההוכחה קצת מסובכת יותר.

<u>טענה</u> יהי R תפ"י. תהי $f(x)=g(x)h(x)$ ב- $R[x]$.

אזי $f(x)$ פרימיטיבי $\iff$ $g(x),h(x)$ שניהם פרימיטיביים.

<u>הוכחה</u> $(\Leftarrow)$ אם המקדמים של $g(x)$ נניח מתחלקים ב- $a\in R$ לא הפיך,

אזי $g(x)=d\cdot\tilde{g}(x)$, לכן $f(x)=d\cdot(\tilde{g}(x)\cdot h(x))$, לכן המקדמים ב $f(x)$ מתחלקים ב-d. לכן, אם g או h לא פרימיטיביים, אזי גם f לא.

($\Leftarrow$ אם f לא פרימיטיבי, אזי $f=d\cdot\tilde{f}(x)$. כאשר d לא הפיך. יהי p גורם אי-פריק של d. כמו בסוף השיעור הקודם, מוכיחים כי $g(x)$ או $h(x)$ מתחלק ב-p ולכן לא פרימיטיבי.

__טענה__ יהי R חוג תולופי. אזי R גפ"י אם ורק אם $R[x]$ גפ"י.

__הוכחה__ ($\Rightarrow$ נניח $R[x]$ גפ"י. יהי $d\in R$ לא הפיך. נתייחס אליו כפולינום קבוע (ממעלה 0) $R[x]$ גפ"י, לכן יש פירוק יחיד $d=p_1p_2\cdots p_r$.

__הערה__ יהי R תחום שלמות. יהיו $g,h\in R[x]$. אזי $\deg(g\cdot h)=\deg(g)+\deg(h)$.

הוכחנו את זה בשיעור הקודם.

אם R לא תחום שלמים זה לא בהכרח נכון

לדוגמא, $R = \mathbb{Z}/6\mathbb{Z}$.

$([2]x+1)([3]x-1) =$

$\cancel{[6]x^2} + x - 1 = x - 1$

לפי ההערה, הגורמים $q_1, q_2, \ldots, q_r$ חייבים להיות ממעלה 0,
כלומר הם קבועים, ולכן נקבל פירוק של d לגורמים
אי-פריקים של R. הוא יחיד כי יחיד ב-$R[x]$.

$\Leftarrow$) יהי R גפ"י, צריך להוכיח כי $R[x]$ גפ"י.

יהי $f(x) = a_n x^n + \dots + a_0 \in R[x]$ פולינום. ויהי $d = \gcd(a_0, \dots, a_n)$

אזי $f(x) = d \cdot \tilde{f}(x)$ כאשר $\tilde{f}(x)$ פרימיטיבי.

ידוע שיש פירוק של d, כי $d \in R$, R גפ"י.

נניח של-$\tilde{f}$ יש פירוק לגורמים אי-פריקים.

יהי $F = \mathrm{Frac}\, R$, החוג $F[x]$ הינו תחום אוקלידי,
לכן תחום ראשי, לכן גפ"י. לכן יש פירוק
$\tilde{f}(x) = q_1(x) \cdots q_r(x)$ ב-$F[x]$.

לפי הלמה של גאוס (אפשר להשתמש בה כי $\tilde{f}$ פרימי')
ניתן לקבל פירוק ב-$R[x]$. לכן יש פירוק

$\tilde{f}(x) = q_1'(x)\cdots q_r'(x)$ פירוק ב-$R[x]$

כאשר $q_i'(x) = \frac{r_i}{s_i} q_i(x)$. כל q_i' חבר של q_i
ב-$F[x]$, לכן אי-פריק ב-$F[x]$. לפי ההערה,
$\tilde{f}$ פרימיטיבי $\Leftarrow$ q_i' פרימיטיביים. לכן לפי הלמה של
גאוס הם אי-פריקים ב-$R[x]$ כי היו אי-פריקים ב-$F[x]$.

לכן קיבלנו פירוק של $f(x)$ לגורמים אי-פריקים
ב-$R[x]$.

נשאר להוכיח שהפירוק יחיד.
נניח כי $f(x)$ פרימיטיבי. יהיו $f(x) = p_1\cdots p_r = q_1\cdots q_s$
שני פירוקים. אזי p_i, q_i כולם פרימיטיביים,
לכן אלה שני פירוקים לגורמים אי-פריקים גם ב-$F[x]$.

כבר ידוע כי $F[x]$ תפ"י, לכן $r=s$ ו- p_i, q_i
חברים לכל i. האיברים ההפיכים ב- $F[x]$ הם
הקבועים הלא-אפסיים. לכן לכל i קיים $\frac{r_i}{s_i} \neq 0 \in F$
כך ש- $q_i(x) = \frac{r_i}{s_i} p_i(x)$

$$\underbrace{s_i \cdot q_i(x)}_{\text{gcd של המקדמים הינו } s_i} = \underbrace{r_i \cdot p_i(x)}_{\text{gcd הינו } r_i}$$ p_i, q_i פרימיטיביים

ה-gcd ב- R מוגדר היטב עד כדי חברות, כי R תחום
שלמות. לכן, r_i, s_i חברים ב- R, לכן $\frac{r_i}{s_i}$

r_i, s_i חברים $\Rightarrow r_i = s_i u \Rightarrow u = \frac{r_i}{s_i}$, $u \in R^*$

הינו איבר הפיך של R, לכן של $R[x]$, לכן p_i, q_i חברים
גם ב- $R[x]$.

עכשיו, יהי $f(x)$ פולינום לא בהכרח פרימיטיבי.

נשים לב שפולינום אי-פריק ממעלה ≥ 1 חייב להיות
פרימיטיבי. אחרת, אם $g(x)$ לא פרימי, d ה-gcd
של המקדמים, $g(x) = d \cdot \tilde{g}(x)$, שני הגורמים לא הפיכים.
בסתירה לאי-פריקות של g)

לכן, יהי $f(x) = p_1 \cdots p_r \cdot q_1(x) \cdots q_s(x)$

פירוק של $f(x)$, כאשר $\deg p_i = 0$

אזי $\deg q_i \geq 1$ מקבלים את הגורמים האי-פריקים ממעלה 0 ביחד (p_i-ים) וממעלה ≥ 1 ביחד (q_i-ים)

$p_1 \cdots p_r \in R$

$q_1 \cdots q_s$ פרימיטיביים

לכן $\gcd = p_1 \cdots p_r$ של המקדמים של f

$\tilde{f}(x) = q_1 \cdots q_s$ עד כדי חברות

לכן כל פירוק של f מתפרק לפירוק של ה-$\gcd$ ושל $\tilde{f}$ (פרימיטיבי). נגד הנחתנו שה-פירוקים האלה יחידים.

<u>מסקנה</u> יהי R תפ"י. אזי $R[x_1, x_2, \ldots, x_n]$ גם תפ"י.

<u>הוכחה</u> אינדוקציה, שכן $R[x_1,x_2] = (R[x_1])[x_2]$

$2x^2y + 5xy + 6x^5y^3 = (6x^5)y^3 + (2x^2+5x)y$

מסקנה יהי R תחום, אזי $\underbrace{R[x_1,x_2,\dots]}$ לא נתרי.

∞ משתנים

הוכחה

$$R[x_1,\dots] = \bigcup_{n=1}^{\infty} R[x_1,\dots,x_n]$$

בכל פולינום מופיעים רק מספר סופי של משתנים

תרגיל אם $f(x)$ פריק ב- $R[x_1,\dots]$ אזי הוא פריק ב- $R[x_1,\dots,x_n]$ עבור n מספיק גבוה.

מסקנה תחום לא בהכרח נתרי. לדוגמא, $\bar{R}[x_1,x_2,x_3,x_4,\dots]$ כאשר R תחום

$(x_1) \subsetneq (x_1,x_2) \subsetneq (x_1,x_2,x_3) \subsetneq \dots$ שרשרת עולה.

יהי R תחום.

שאלה כיצד נדע מתי פולינום $f(x)\in R[x]$ הינו אי-פריק?

טענה יהי F שדה, $f(x)\in F[x]$. אזי ל- $f(x)$ יש

שורש ($\alpha\in F$ כך ש- $f(\alpha)=0$) אם ורק אם ל- $f(x)$ יש

גורם אי-פריק ממעלה 1.

<u>הוכחה</u> $(\Rightarrow)$ נניח שיש גורם לינארי. אזי

$$f(x) = (ax+b)\,g(x)$$

כאשר $a \neq 0$. יהי $\alpha = -ba^{-1} \in F$. אזי

$$f(\alpha) = (a\alpha+b)\cdot g(\alpha) = (-b+b)\,g(\alpha) = 0$$

לכן α שורש.

$(\Leftarrow$ יהי α שורש. הפולינום $x-\alpha$ אי-פריק ב- $F[x]$.

$F[x]$ תחום אוקלידי; לכן ניתן לחלק את $f(x)$ ב- $(x-\alpha)$ עם שארית:

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

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

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

נציב α:

$$0 = f(\alpha) = \cancel{(\alpha-\alpha)}^{\to 0} q(\alpha) + r = r$$

לכן $r=0 \Rightarrow f(x) = (x-\alpha)q(x)$, לכן $x-\alpha$

הינו גורם אי-פריק של $f(x)$.

<u>מסקנה</u> יהי $f(x)\in R[x]$ פולינום ממעלה 2 או 3.

הוא פריק אם ורק אם יש לו שורש.