

תוכנית 8

יהי $\text{ord}_p f$ מספר האיבריין של f במרחב $K[x]$

משפט: יהי $f \in K[x]$, $f \neq 0$. אפשר לכתוב $f = c \prod p_i^{a_i}$ כאשר $c \in K$

p_i הם פרימים איבריניים. c הקבוע והמספרים a_i (הקבועים) $\text{ord}_p f$

הוא מספר האיבריין של f .

כאשר c הוא הקבוע האיבריני של f : $\text{ord}_p f = a(p) \iff a(p) \in \mathbb{N}$

יחידות c בחוג. לפי צריך רק להוכיח את $*$

משפט 2: יהיו $f, g \in K[x]$, $g \neq 0$. אז קיימים $q, r \in K[x]$ כך ש- $f = pq + r$ ($\deg r < \deg g$)

(הוכחה: אינדוקציה II. (אנטיקווריה...))

דוגמה: $f(x) = 2x^3 + 7x^2 + 5$, $g(x) = x - 1$. האיבריין!

הצגה: $\text{gcd}(f, g)$ הוא האיבריין המשותף הגדול ביותר של f ו- g . $\text{gcd}(f, g) \mid f$ ו- $\text{gcd}(f, g) \mid g$

זה האיבריין המשותף.

אם c איבריני של fg ומחלק את d , נניח $c \mid fg$ ומחלק את d . $c = d$

אז $c = d$ ו- $c \mid d$, $d = uc$ ו- $c = vd$

$1 - u = 0$ או $d \neq 0$, $d(1 - u) = 0$. $u \in K$ או $u = 1$

$d = c \iff 1 = u \iff c \mid d$, $d = uc$, $u \in K$

כך $\text{gcd}(f, g)$ יחיד!

כעת אפשר לכתוב $\text{gcd}(f, g)$ כקומונטה של f ו- g .

$$\text{gcd}(f, g) = a(x)f(x) + b(x)g(x)$$

הצגה: אפשר לכתוב $\text{gcd}(f, g) = 1$ אם $f, g \in K[x]$ ו- $\text{gcd}(f, g) = 1$

אם f, g זרים ו- $1 \mid f, g$ אז $f \mid h$ ו- $g \mid h$

הוכחה: $lf + mg = 1$, $lfh + mgh = h$

\square

מספרים

מספרות 1: אם $\gcd(f, g) = 1$ אז $\text{ord}_p(fg) = \text{ord}_p f + \text{ord}_p g$!
 (הוכחה - כמו עבור \mathbb{Z})

אפשר להניח ש- p מתוקן אז $\gcd(p, f) = 1$ או $p \mid f$.
 אז $\text{ord}_p f = 1$ אם $\gcd(p, f) = 1$ ו- $\text{ord}_p f = \text{ord}_p p$ אם $p \mid f$.

מספרות 2: אם p מתוקן אז $f, g \in \mathbb{Z}$, $f, g \neq 0$ אז $\text{ord}_p(fg) = \text{ord}_p f + \text{ord}_p g$.
 (הוכחה - כמו עבור \mathbb{Z})

(הוכחת המשפט) (המרת חזרה)

יהי $q(x)$ פולינום אי-רציונלי מתוקן. אנו מחשבים $\text{ord}_q f$ ו- $f = c \prod p_i^{a_i}$

$$\text{ord}_q f = \text{ord}_q c + \sum e_i a_i \text{ord}_q p_i = a(q)$$

$\text{ord}_q c = 0$
 $\text{ord}_q p_i = \begin{cases} 0 & p_i \neq q \\ 1 & p_i = q \end{cases}$

שורשים פרימיטיביים:

הפינוק $\rightarrow \cup (\mathbb{Z}/n\mathbb{Z}) \cong \cup (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \dots \times \cup (\mathbb{Z}/p_r^{a_r}\mathbb{Z})$, $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$

Δ שמהי האם $\cup (\mathbb{Z}/n\mathbb{Z})$ חקורה ציקלית?

$\forall x \in \mathbb{Z}$ הוא נורמט פרימיטיבי עבור n אם x זר $n-1$ אז $x+n\mathbb{Z}$ הוא יוצר של $\cup (\mathbb{Z}/n\mathbb{Z})$.

האם $\cup (\mathbb{Z}/p^2\mathbb{Z}) = (\mathbb{Z}/p^2\mathbb{Z})^\times$ ציקלית ?
 האם $\cup (\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^\times$ ציקלית ?

בזמא: \mathbb{F}_5^\times ציקלית , $\bar{2} \in \mathbb{F}_5^\times$: $1 \rightarrow \bar{2} \rightarrow \bar{4} \rightarrow \bar{8} = \bar{3} \rightarrow \bar{1}$ הוא שורש פרימיטיבי למד 5.
 $\cup (\mathbb{Z}/8\mathbb{Z}) = \{ \bar{1}, \bar{3}, \bar{5}, \bar{7} \}$ *
 $\bar{3}^2 = \bar{1}$
 $\bar{5}^2 = \bar{1}$
 $\bar{7}^2 = \bar{1}$

$\cup (\mathbb{Z}/m\mathbb{Z})$ חקורה ציקלית \Leftrightarrow קיים שלם מוביל u

עוזב בראשית של חקורת \mathbb{Z} ציקליות:

אילו מורפוזם $\cup (\mathbb{Z}/2\mathbb{Z}) \times \cup (\mathbb{Z}/2\mathbb{Z}) = \cup (\mathbb{Z}/4\mathbb{Z})$, $\bar{1}$, $(\mathbb{Z}/m\mathbb{Z}, +)$

$(0,0) \mapsto \bar{1}$
 $(1,0) \mapsto \bar{3}$
 $(0,1) \mapsto \bar{5}$
 $(1,1) \mapsto \bar{7}$

$(0,0) + (0,1) = (0,1)$
 $(1,1) + (1,1) = (0,0)$

המשך תחום 8 :

משפט 1: יהי $f \in K[x]$, K שדה ויהי $f \neq 0$, $\deg f = n$ אז יש n שורשים.
 (יותר מ שורשים).

הוכחה - אינדוקציה על n .

$n=0$, $n=1$ טריוויאלים. נניח שהמשפט נכון עבור $n-1$. אז אין f שורשים K -אז f אי-פולינומיאלי.

ישורשים K -אז f סיימן. אז יש $\alpha \in K$ שורש f , סתמים $f(x) = q(x)(x-\alpha) + r$

$$f(x) = q(x)(x-\alpha) + r \quad \text{כאשר } r = f(\alpha) = 0 \quad \text{כי } \alpha \text{ שורש } f$$

$$\deg q = n-1 \quad \text{כי } \beta \neq \alpha \quad \text{אז } \beta \text{ שורש } f$$

$$\beta \text{ שורש } q \Leftrightarrow q(\beta) = 0 \Leftrightarrow f(\beta) = q(\beta)(\beta-\alpha) = 0$$

לפי הנ"ל יש $n-1$ שורשים f ב- K , נכון f יש n שורשים. $(n-1)+1 = n$

■ שיום

סתים: אם $f, g \in K[x]$, $\deg f = \deg g = n$ אז $f(\alpha_i) = g(\alpha_i)$ עבור $n+1$ אברים

שונים $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$. אז $f=g$.

הוכחה: נסתם $f-g \in K[x]$ או $f-g=0$ או $\deg f-g \leq n$

אבל יש $n+1$ שורשים שונים α_i נכון $f-g=0$ ■ $f=g$