

אלגברה ב' 2 – תרגול 2

07.03.11

פריקות של פולינומים

R תחום פריקות יחידה. F שדה המנות.

תזכורת. $\sum_{i=0}^{\infty} a_i x^i = f \in R[x]$ יקרא פרימיטיבי אם $1 \in \gcd(a_0, \dots, a_n)$.

טענה. יהיו $f_i \in F[x]$ כך ש- $f_1, f_2 \in R[x]$ מתוקנים אז $f_i \in R[x]$.

הוכחה. נכתוב $f_i = c_i^{-1} p_i$ עבור $c_i \in F^*$ $p_i \in R[x]$ פרימיטיבי. $f_1 f_2 = (c_1 c_2)^{-1} p_1 p_2$.
שוב מהשיעור, בגלל הנתון ש- $f_1, f_2 \in R[x]$ אז $f_1 f_2 = c' p'$ עבור $c' \in R$ $p' \in R[x]$ פרימיטיבי.
לכן

$$(c_1 c_2) c' p' = p_1 p_2$$

כעת $p_1 p_2$ פרימיטיבי מטענה בשיעור, $c_1, c_2 \in R$ כי $c_1, c_2 \in R$ כי f_i מתוקן. לכן
המקדם העליון של p_i הוא c_i . אז $(c_1 c_2) c' \in R$ מחלק את כל המקדמים של $p_1 p_2$. לכן
 $\square$ $(c_1 c_2) c' \in R^*$ לכן $c_1, c_2 \in R^*$.

הטענה נקראת "הלמה של גאוס".

קריטריון איזנשטיין לא"פ

יהי $f \in R[x]$

$$f = a_0 + a_1 x + \dots + a_n x^n$$

ויהי $p \in R$ א"פ כך ש- $p \nmid a_i, p \nmid a_n, 0 \leq i \leq n-1$ אז f אי פריק מעל F .

הוכחה. נכתוב $f = c f_1$ עבור $c \in R$ ו- $f_1 \in R[x]$ פרימיטיבי. אז $\sum_{i=0}^n a_i x^i = c \sum_{i=0}^n \alpha_i x^i$ לכן $p \mid \alpha_i$ לכל $0 \leq i \leq n-1$ כי $a_i = c \alpha_i$ וכן $p \nmid c$ (כי אחרת $p \mid c \alpha_n = a_n$).
 $\underbrace{\sum_{i=0}^n \alpha_i x^i}_{=f_1}$

$p \nmid \alpha_n$ (אחרת שוב $p \mid c \alpha_n = a_n$). $p^2 \nmid \alpha_0$ (אחרת $p^2 \mid a_0$). הזוג (f_1, p) מקיימים את תנאי הקריטריון ו- $f_1 \in R[x]$ אי פריק מעל R $\Leftrightarrow$ f_1 א"פ מעל F $\Leftrightarrow$ f א"פ מעל F $\Leftrightarrow$ $f = c f_1, c \in F^*$ פרימיטיבי f_1

F . כעת אפשר להוכיח את הקריטריון עבור הפולינום f_1, p . די להוכיח f_1 א"פ מעל R .
יהיו $a(x), b(x) \in R[x]$ כך ש- $f_1(x) = a(x)b(x)$ בה"כ $\deg a > 0, \deg b > 0$ (אחרת למשל $a \in R$ ואז $f_1(x) = a \cdot b(x)$ פרימיטיבי, a מחלק את כל מקדמי f_1 ולכן הפיך ב- R ולכן הפירוק טריוויאלי).

אז $f_1(x) = b_0 + b_1 x + \dots + b_m x^m$ כאשר $b_m \neq 0, c_r \neq 0$ $f_1(x) = b_0 + b_1 x + \dots + b_m x^m$ $(c_0 + c_1 x + \dots + c_r x^r)$

נרשום $f_1(x) = \sum_{i=0}^n a_i x^i$. אז $a_n = b_m \cdot c_r$ ו- $a_0 = b_0 \cdot c_0$.
 בה"כ $p \nmid c_0$ וכי אם $p \mid b_0, p \mid c_0$ אז $p^2 \mid a_0$.

$$a_1 = b_1 c_0 + b_0 c_1$$

$p \mid b_1$ אבל $p \nmid c_0$ לכן $p \mid b_1 c_0$ והוא ראשוני. $p \mid a_0$ כי $p \mid a_1, p \mid b_0$.
 באופן כללי $a_i = b_i c_0 + \dots + b_0 c_i$ ל- $i \leq m$ עכשיו $p \mid a_i$ כי $r + m = n$ ולכן $m < n$.
 $p \mid b_0, \dots, b_{i-1}$ באינדוקציה $p \nmid c_0$ ולכן $p \mid b_i$. בפרט, $p \mid b_m$ לכן $p \mid a_n = b_m c_r$ בסתירה. $\square$

שאלה. יהי $p \in \mathbb{Z}$ ראשוני. צ"ל $x^i \in \mathbb{Z}[x]$ $f = \sum_{i=0}^{p-1} x^i$ א"פ מעל $\mathbb{Q}$.

תשובה. $f(x)$ א"פ מעל $\mathbb{Q} \Leftrightarrow f(x+1)$ א"פ מעל $\mathbb{Q}$ (הוא איזומורפיזם $\mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$).
 אז אם $f(x) = a(x)b(x)$ פירוק אז גם $f(x+1) = a(x+1)b(x+1)$ פירוק לא טריוויאלי. נשתמש בזהות הידועה $f(x+1) = \sum_{j=0}^{p-1} \binom{p}{j} x^j + 1$.

$$\underbrace{f(x+1)}_{\mathbb{Q}(x)-\text{ב}} = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \sum_{j=2}^{p-1} \binom{p}{j} x^{j-1} + p$$

$p \mid \binom{p}{j}$ לכל $2 \leq j \leq p-1$, $p \nmid p$.
 $nmid1$ לכן א"פ מעל $\mathbb{Q}$ ולכן גם $f(x)$ כזה.

שאלה. הוכיחו כי $f = x^5 - x^2 + 1$ א"פ מעל $\mathbb{Q}$.

תשובה. נראה ש- f אי פריק מעל $\mathbb{Z}_2[x]$: $\mathbb{Z}_2[x] : \tilde{f} \in \mathbb{Z}_2[x]$ ע"י $f \mapsto \tilde{f}$ $\sum a_i x^i \mapsto \sum (a_i + 2\mathbb{Z})x^i$.
 וזה הומומורפיזם על.

אם f א"פ מעל $\mathbb{Z}$ אז $f = ab$ לא טריוויאלי מעל $\mathbb{Z}$ ואז $\tilde{f} = \tilde{a}\tilde{b}$ אבל f מתוקן לכן a, b מתוקנים אז $\deg \tilde{a} = \deg a, \deg \tilde{b} = \deg b$ פירוק לא טריוויאלי ב- $\mathbb{Z}_2[x]$.
 f פרימיטיבי לכן א"פ מעל $\mathbb{Z}$ שקולה לא"פ מעל $\mathbb{Q}$.

$\tilde{f} = x^5 + x^2 + 1$ אין לו שורש ב- $\mathbb{Z}$ לכן פירוק שלו הוא מעלה 3 כפול מעלה 2 או מעלה 4 כפול מעלה 1 וזה לא יכול להיות כי אין שורש. אז מעלה 3 כפול מעלה 2. לכן הפולינומים האי פריקים ממעלה 2 מעל $\mathbb{Z}_2$ הם:

$$x^2 + x + 1, \quad x^2 + x, \quad x^2 + 1, \quad x^2$$

מתוכם רק $x^2 + x + 1$ א"פ ומבדיקה ישירה לא מחלק את $\tilde{f}$.