roy@benari.com

תרגיל מס' 1 – אלגברה 3

משפט 1: F שדה, $p \in F[x]$, $\deg p \leq 3$ אז p פריק אמ"מ יש לו שורש (בשדה).

הערה: אם r שארית $\Leftarrow$ p פריק.

אם λ שורש אז נוכל לכתוב את p כמכפלה $p(x) = (x-\lambda)\cdot q(x) + r(x)$

כאשר $\deg(r(x)) < \deg(x-\lambda)$.

$\deg(r(x)) \leq 0$ (לוגי)

$p(\lambda) = 0 \Rightarrow r(\lambda) = 0 \Leftarrow r = 0$

$p(x) = (x-\lambda)\, q(x)$ ∴

משפט 2: $p = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$, $t = \frac{r}{s} \in \mathbb{Q}$ כך ש- $\gcd(r,s) = 1$

$p(t) = 0 \Rightarrow a_m \mid s$, $a_0 \mid r$.

הערה: הוכח ש- $f = 8x^3 - 6x - 1$ אי-פריק מעל $\mathbb{Z}[x]$.

פתרון: נניח בשלילה שכן f שורשים רציונליים $\Rightarrow$ הוא פריק מעל $\mathbb{Q}$

$\Rightarrow$ הוא פריק מעל $\mathbb{Z}$.

(נשתמש במשפט 2 כדי להוכיח שאין לו שורשים.

אם יש שורש $\frac{s}{r}$ של $\mathbb{Q}$ אזי $8 \mid s$ ו- $1 \mid r$

$s = \pm 1, \pm 2, \pm 4, \pm 8$ $\quad$ $r = \pm 1$

$\Rightarrow$ מצאנו מועמדים שאין שורשים.

משפט 3: יהי F שדה.

$p \in F[x]$ אי-פריק $\Leftrightarrow$ $p(ax+b)$ הוא פריק ($\exists q, a \neq 0, b \in F$).

משפט 4: (קריטריון אייזנשטיין)

$f \in \mathbb{Z}[x]$, $f = \sum_{i=0}^{n} a_i x^i$.

f אי-פריק אם $\exists p \in \mathbb{Z}$ (ראשוני) $p \mid a_i$ $\forall i: 0 \leq i < n$, $p \nmid a_n$, $p^2 \nmid a_0$

מעל $\mathbb{Q}$.

תרגיל: $f = x^{p-1} + x^{p-2} + \cdots + 1$. הוכח: f אי-פריק מעל $\mathbb{Z}$.

הערה: יהי משפט 3 מספק לפונקציה $f(1+x)$ אי-פריק

$$\varphi(x) = (x-1)f(x) = x^p - 1$$

$$\varphi(1+x) = xf(1+x) = (1+x)^p - 1 =$$

$$= \underbrace{\left(\sum_{i=0}^{p} \binom{p}{i} x^i\right)}_{} - 1 = x^p + \binom{p}{p-1} x^{p-1} + \ldots + \binom{p}{2} x^2 + \binom{p}{1} x + \cancel{1} - \cancel{1} =$$

$$= \sum_{i=1}^{p-1} \binom{p}{i} x^i + x^p = x\left(\binom{p}{1} + \binom{p}{2} x + \ldots + \binom{p}{p-1} x^{p-2} + x^{p-1}\right) =$$

$$= x\left[\sum_{i=1}^{p-1} \binom{p}{i} x^{i-1} + x^{p-1}\right]$$

$$\Rightarrow \quad f(x+1) = \underbrace{\sum_{i=1}^{p-1} \binom{p}{i} x^{i-1} + x^{p-1}}_{\text{(*)}}$$

$\Leftarrow$ p מחלק את x

$p \mid \binom{p}{i}$, $1 \le i \le p-1$ כל המקדמים חלים ב-p

$p \mid (*)$ ו- $p^2 \nmid (*)$ אי-פריק מעל $\mathbb{Z}$. $\Rightarrow f(x+1)$

משפט 5: (שיטת הרדוקציה)

R תחום (לא בהכרח שדה), F שדה.

יהי φ הומו' חח"ע מ- $R \to F$, שמשרה את ה-

הומו' חח"ע $\varphi_* : R[x] \to F[x]$ כך: $\sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} \varphi(a_i) x^i$

הומו' זו שומרת, כלומר לכל $f \in R[x]$,

f אי-פריק ב- $F[x]$ $\Leftarrow$ $\varphi_*(f)$ אי-פריק ב- $R[x]$.

מסקנה: $\mathbb{F}_p = F$.

דוגמה: הראו כי $f(x) = 8x^3 - 6x + 1$ אי-פריק מעל $\mathbb{Z}$ בשיטת הרדוקציה.

$$\varphi_p(x) = x \pmod p$$

$$\deg = 3 \quad \varphi_2^*(f) = 1$$

$$\deg = 3, \quad \varphi_3^*(f) = 2x^3 + 2$$

$\Leftarrow$ שורה $\Leftarrow$ פריק $\Leftarrow$ לכן אזכר לו

$$\varphi_5^*(f) = 3x^3 + 4x + 4$$

(כנ"ל $x = 0, 1, \ldots, 4$ ונראה כאלו שורשים ... שקולה שהפולינום לא פריק