

### תרגיל 5 מופשטת 3

בכל התרגיל אתם מתבקשים לנמק את צעדיכם ככל האפשר.

1. להלן עובדה שהשתמשתי בה בתרגול ואמרתם לי שלא ראיתם בקורס הקודם:  
יהי  $p$  מספר ראשוני, אזי הפולינום

$$x^{p-1} + x^{p-2} + \dots + 1$$

הוא אי פריק מעל  $\mathbb{Q}$ .  
הוכיחו קביעה זו. הדרכה:

(א) ראשית הוכיחו כי אם  $p$  ראשוני ו  $0 < k < p$  אז

$$p \mid \binom{p}{k}$$

**פתרון:** כזכור

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

נשים לב שהגורמים במכנה הם עצרת של מספרים קטנים מ  $p$  ולכן לא מכילים שום גורם  $p$  לעומת המונה שכן מכיל ולכן הטענה ברורה.

(ב) שימו לב ש

$$x^{p-1} + x^{p-2} + \dots + 1 = \frac{x^p - 1}{x - 1}$$

**פתרון:** שמנו לב.

(ג) החליפו את  $x$  ב  $x + 1$  והשתמשו בקריטריון אייזנשטיין.

**פתרון:** נחליף את  $x$  ב  $x + 1$  ונקבל

$$\frac{(x+1)^p - 1}{x+1-1} = \frac{\sum_{k=0}^p \binom{p}{k} x^k - 1}{x} = \frac{\sum_{k=1}^p \binom{p}{k} x^k}{x} = \sum_{k=1}^p \binom{p}{k} x^{k-1}$$

כעת נשים לב ש

$$p \nmid \binom{p}{p} = 1$$

אבל לכל  $0 < k < p$  אכן מתקיים

$$p \mid \binom{p}{k}$$

ועבור  $k = 1$  (המקדם החופשי) מתקיים

$$p^2 \nmid \binom{p}{1} = p$$

לכן לפי קריטריון אייזנשטיין. הפולינום אי פריק. לכן גם הפולינום המקורי אי פריק.

2. הנה עוד עובדה שחשוב להכיר: יהי  $F$  ממאפיין  $p$  אז מתקיים שלכל  $a, b \in F$

$$(a + b)^p = a^p + b^p$$

דרך אחרת להגיד את זה: הפונקציה  $f(x) = x^p$  היא הומומורפיזם (כי קל להראות שהיא שומרת כפל). הוכיחו טענה זו.

**פתרון:** לפי הבינום של ניטון (שעובד בכל שדה) מתקיים

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}$$

אבל כזכור לכל  $0 < k < p$  מתקיים

$$p \mid \binom{p}{k}$$

ולכן

$$\binom{p}{k} = 0$$

כלומר הביטוי מכיל רק את האיבריים הקיצוניים, דהיינו

$$a^p + b^p$$

כנדרש.

3. האם הפולינומים הבאים ספרביליים?

$$(א) \quad x^3 + x^2 - x - 1 \text{ מעל } \mathbb{Q}.$$

**פתרון:** הנגזרת היא  $3x^2 + 2x - 1$ . נבצע אלגוריתם אוקלידס

$$x^3 + x^2 - x - 1 = \left(\frac{1}{3}x + \frac{1}{9}\right)(3x^2 + 2x - 1) - \frac{8}{9}x - \frac{8}{9}$$

$$3x^2 + 2x - 1 = (3x - 1)(x + 1)$$

הפולינום לא ספרבילי

(ב) מעל  $\mathbb{Q}$   $x^3 + x^2 - x - 2$ .

**פתרון:** הנגזרת היא  $3x^2 + 2x - 1$  נבצע אלגוריתם אוקלידס

$$x^3 + x^2 - x - 2 = \left(\frac{1}{3}x + \frac{1}{9}\right)(3x^2 + 2x - 1) - \frac{8}{9}x - \frac{17}{9}$$

ובחילוק

$$\frac{3x^2 + 2x - 1}{x + \frac{17}{8}}$$

מתקבלת שארית ולכן הפולינום ספרבילי.

(ג) מעל  $\mathbb{Z}_5$   $x^{10} + x^5 + 3$ .

**פתרון:** הנגזרת היא 0 ולכן הפולינום לא ספרבילי.

(ד) מעל  $\mathbb{Z}_{17}$   $x^{17} - x$ .

**פתרון:** הנגזרת היא  $-1$  ולכן הפולינום ספרבילי.

4. תהי  $F \subseteq K$  הרחבת שדות ממימד 2. הראו ש  $K$  שדה פיצול של פולינום כלשהוא ב  $F[x]$ .

**פתרון:** ניקח  $\alpha \in K \setminus F$ . ברור ש  $F(\alpha) = K$  ולכן הפולינום המינימלי של  $\alpha$  מדרגה 2. כלומר

$$f(x) = x^2 + bx + c$$

השורשים הם כמובן

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

היות ש  $\alpha \in K$  קל לראות ש

$$\sqrt{b^2 - 4c} \in K$$

ולכן גם השורש השני ב  $K$ . כלומר  $K$  שדה מפצל של הפולינום. היות שאין עוד שדות בין  $K$  ל  $F$ .  $K$  הוא שדה הפיצול.

בדיעבד אני רואה שהפתרון הזה משתמש בכך שהמאפיין שונה מ 2 וזה לא היה נתון. הנה עדכון שמתאים לכל מאפיין.

$\alpha$  הוא שורש של הפולינום  $f(x)$  שלמעלה. ולכן ב  $K$  מתקיים

$$x - \alpha \mid f(x)$$

אבל  $f(x)$  בסך הכל ממעלה 2 וזה אומר שב  $K$  מתקיים

$$f(x) = (x - \alpha)(x - \beta)$$

ולכן  $\beta \in K$ . ו  $K$  מפצל את  $f(x)$  בנוסף הוא ממש שדה הפיצול כי כל שדה יותר קטן יהיה  $F$  בעצמו.

5. תהי  $F \subseteq K$  הרחבת שדות. נניח ש  $f(x) \in F[x]$  ספרבילי כך ש  $f = g_1 g_2$  עבור  $g_1, g_2 \in K[x]$ . הוכיחו כי

$$\gcd(g_1, g_2) = 1$$

**פתרון:** נניח שיש גורם משותף

$$\gcd(g_1, g_2) = h(x) \in K[x]$$

מדרגה גדולה מאחד. נניח ש

$$g_1 = hh_1, \quad g_2 = hh_2$$

נרחיב את  $K$  לשדה פיצול של  $f(x)$ . בשדה זה מתקיים

$$f = g_1 g_2 = h^2 h_1 h_2$$

ולכן  $f$  לא ספרבילי בסתירה.