מבנים אלגבריים תרגול 13

23 ביוני 2021

תרגילים:

1. יהי $f \in \mathbb{F}[x]$ פולינום ממעלה חיובית.

(א) הוכיחו שניתן להציגו כקבוע כפול פולינומים ראשוניים מתוקנים. כלומר, קיימים $c \in \mathbb{F}$ וכן $p_1, \ldots, p_k$ פולינומים ראשוניים מתוקנים כך ש־ $f = c \cdot \prod_{i=1}^{k} p_i$.

(ב) הצגה זו יחידה, עד כדי סדר הגורמים.

פתרון: א. נוכיח באינדוקציה על מעלת הפולינום $\deg f = n$. עבור $n = 1$, אז $f = cx - a = c(x - \frac{a}{c})$ והוא כמובן אי־פריק (כי פירוק לגרומים ממעלה חיבית ייתן שמכפלתם ממעלה 2 לפחות).

נניח נכונות לכל $1 \leq k \leq n$ ונוכיח עבור $n + 1$:

יהי $f = \sum_{i=0}^{n+1} a_i x^i$ פולינום ממעלה $n + 1$. אם הוא ראשוני אז סיימנו $f = a_{n+1} \cdot \left(\sum_{i=0}^{n+1} \frac{a_i}{a_{n+1}} x^i \right)$ (פשוט נתקן אותו וזה הכפל בקבוע). אחרת, הוא פריק, כלומר קיימים g, h עם $1 \leq \deg(g) \leq \deg(h) \leq n$ כך ש־ $f = gh$. כעת נוכל להשתמש בהנחת האינדוקציה, לפיה יש $c_1, c_2 \in \mathbb{F}$ וכן פולינומים ראשוניים מתוקנים $p_1, \ldots p_k, q_1, \ldots, q_m$ כך ש־

$$g = c_1 \prod p_i, h = c_2 \prod q_i$$

וביחד:

$$f = \underbrace{c_1 c_2}_{=c \in \mathbb{F}} \cdot \prod_{i=1}^{k} p_i \cdot \prod_{i=1}^{m} q_i$$

ב. נניח

$$c_1 \prod_{i=1}^{t} p_i = f = c_2 \cdot \prod_{i=1}^{s} q_i$$

אז נראה ש־ p_1 הוא אחד הגורמים במכפלה הימנית, ואז אחרי שמחלקים בגורם הזה, אפשר להמשיך באינדוקציה. אכן, $p_1 | f = c_2 \cdot \prod_{i=1}^{s} q_i$, ולכן מכיון שהוא

ראשוני הוא מחלק לפחות אחד מהם (לפי הגדרת ראשוני). כלומר, קיים j כך ש־ $p_1|q_j$, זאת אומרת שיש פולינום a עבורו $q_j = p_1 a$ אבל q_j ראשוני ולכן אי־פריק, לכן $a = 1$ (כי חייב להיות קבוע, וכיון ששניהם מתוקנים, הקבוע צריך להיות 1) מה שאומר $p_1 = q_j$.

2. נתבונן בחוג המנה

$$\mathbb{Z}_2[x]/\langle x^2+1\rangle$$

כאשר $\langle x^2+1\rangle = \{g(x^2+1) \mid g \in \mathbb{Z}_2[x]\}$ זוהו אידאל ראשי. איבר בחוג המנה הוא מהצורה:

$$[f] = \{f + g \mid g \in \langle x^2+1\rangle\} = f + \langle x^2+1\rangle$$

הערה: זו בעצם מחלקת שקילות תחת היחס $f \equiv g \iff f - g \in \langle x^2+1\rangle$.
פעולות:

$$[f] + [g] = [f+g]$$

$$[f] \cdot [g] = [fg]$$

איבר האפס הוא $[0] = 0 + \langle x^2+1\rangle = \langle x^2+1\rangle$.
איבר היחידה הוא $[1] = 1 + \langle x^2+1\rangle$. למשל שימו לב ש־ $x^2 \equiv x^2 + 2 = 1 + (x^2+1) \in 1 + \langle x^2+1\rangle$ מה שאומר $[1] = [x^2]$.
האם זהו שדה?
פתרון: ראיתם בהרצאה: חוג מנה מהצורה $\mathbb{F}[x]/\langle h\rangle$ הוא שדה אמ"ם h אי־פריק. האם x^2+1 אי־פריק מעל $\mathbb{Z}_2[x]$? בתרגיל הבית תראו שפולינום ממעלה 2,3 הוא אי־פריק אמ"ם אין לו שורש בשדה. ואילו לפולינום שלנו יש שורש:

$$1^2 + 1 = 2 \equiv 0(\mod 2)$$

ואכן ניתן לפרק אותו:

$$x^2 + 1 \equiv x^2 + 2x + 1 = (x+1)^2$$

בסה"כ חוג המנה $\mathbb{Z}_2[x]/\langle x^2+1\rangle$ לא שדה.
כעת, לשם הדוגמא, נמצא בו איבר לא הפיך.
טענה: $[x+1] = (x+1) + \langle x^2+1\rangle$ לא הפיך. הוכחה: נשים לב שמתקיים:

$$[x] \cdot [x+1] = [x(x+1)] = [x^2+x] = [x^2] + [x]$$

אבל ראינו לעיל $[x^2] = [1]$ ולכן נקבל:

$$= [1] + [x] = [x + 1]$$

כלומר:

$$[x][x + 1] = [x + 1]$$

אילו $[x + 1]$ היה הפיך אז היה $[g]$ כך ש־ $[x + 1][g] = [1]$ ואז אחרי הכפלה של השיוויון ב־$[g]$ היינו מקבלים:

$$[x] = [1]$$

וזה לא יכול להיות כי אז $x - 1 \in \langle x^2 + 1 \rangle$ אבל האיברים באידאל זה (למעט פולינום האפס) הם ממעלה שנייה לפחות (בסתירה).