מבנים אלגבריים תרגול 13

22 ביוני 2021

תרגילים:

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

(א) ניתן להציג את f כקבוע כפול מכפלה של פולינומים ראשוניים מתקונים.

(ב) ההצגה יחידה עד כדי סדר הפולינומים.

פתרון: א. באינדוקציה על מעלה n. עבור $n = 1$ אכן מקבלים פולינום $x - a$ והוא אי־פריק.

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

יהי f פולינום ממעלה $n + 1$. אם הוא ראשוני סיימנו כי נציג אותח ע"י $f \cdot 1$. אחרת, קיימים $g, h \in \mathbb{F}[x]$ עם $1 \le \deg(g) \le \deg(h) \le n$ כך ש־ $f = gh$ (עדיין לא ידוע על g, h שהם אי־פריקים). מהנחת האינדוקציה קיימים $p_1, \ldots, p_k$ פולינומים ראשוניים וקבוע c_1 עד ש־ $g = c_1 \cdot \prod_{i=1}^{k} p_i$, וכן קיימים $q_1, \ldots, q_m$ פולינומים ראשוניים וקבוע c_2 כך ש־ $h = c_2 \cdot \prod_{i=1}^{m} q_i$. בסה"כ:

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

וקיבלנו הצגה כמכפלת ראשוניים כפול קבוע.

ב. נניח שיש 2 הצגות

$$d_1 \cdot \prod_{i=1}^{k} p_i = f = d_2 \cdot \prod_{i=1}^{m} q_i$$

נתבונן בפולינום p_1. מתקיים: $p_1 | \prod_{i=1}^{m} q_i$ ולכן לפי הגדרת ראשוני, הוא מחלק לפחות אחד מהגורמים. נניח שהוא מחלק את q_j. כלומר, $q_j = p_1 \cdot g$ אבל מאי־פריקות של q_j נקבל $g = 1$. בסה"כ קיבלנו $p_1 = q_j$. אחרי שמוציאים את שני הגורמים, ניתן להמשיך באינדוקציה.

2. נתבונן בחוג המנה $R = \mathbb{Z}_2[x]/\langle x^2+1\rangle$. איבר כללי, בהינתן $f \in \mathbb{Z}_2[x]$ אז בחוג המנה הוא

$$[f] = f + \langle x^2+1\rangle = \left\{ f + g(x^2+1) \mid g \in \mathbb{Z}_2[x] \right\}$$

האם זה שדה?

פתרון: ראיתם בהרצאה שחוג מנה $\mathbb{F}[x]/\langle h\rangle$ הוא שדה אמ"ם h אי־פריק. אצלנו: בשיעורי הבית תוכיחו שפולינום ממעלה 2,3 הוא אי־פריק אמ"ם אין לו שורש. נבדוק:

$$0^2 + 1 = 1 \not\equiv 0$$

$$1^2 + 1 = 2 \equiv 0 \pmod 2$$

אצלנו יש לו שורש, ולכן הוא פריק, ולכן R לא שדה. ניתן לראות $[x^2] = [1]$:

$$x^2 + \langle x^2+1\rangle = [x^2] = [1] = 1 + \langle x^2+1\rangle \iff x^2 - 1 \in \langle x^2+1\rangle$$

אבל $x^2 - 1 = x^2 + 1$ כי מעל $\mathbb{Z}_2$, ואכן $x^2 + 1 \in \langle x^2+1\rangle$:

$$[x][x+1] = [x^2+x] = [x^2] + [x] = [1] + [x] = [x+1]$$

בסה"כ:

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

נב"ש $[x+1]$ הפיך, אז יש $[g]$ כך ש־ $[x+1][g] = [1]$, ואז נכפיל את השיווין ב־ $[g]$ ונקבל:

$$[x]\underbrace{[x+1][g]}_{=[1]} = \underbrace{[x+1][g]}_{=[1]}$$

$$[x] = [1]$$

אבל $[x] \neq [1]$ כי $x - 1 = x + 1 \notin \langle x^2+1\rangle$.