תרגול 12 מבנים אלגבריים

14 ביוני 2021

תרגילים:

1. הוכיחו: אם I_1, I_2 אידאלים בחוג R אז $I_1 + I_2 = \{x + y \mid x \in I_1, y \in I_2\} \trianglelefteq R$.
פתרון: תת־חבורה חיבורית: $0 = 0 + 0 \in I_1 + I_2$. יהיו $a + b, x + y \in I_1 + I_2$, אזי:

$$(a + b) - (x + y) = \underbrace{(a - x)}_{\in I_1} + \underbrace{(b - y)}_{\in I_2} \in I_1 + I_2$$

בליעה: יהיו $r \in R, x + y \in I_1 + I_2$ אזי:

$$r(x + y) = \underbrace{rx}_{\in I_1} + \underbrace{ry}_{\in I_2} \in I_1 + I_2$$

ובאותו אופן:

$$(x + y)r = \underbrace{xr}_{\in I_1} + \underbrace{yr}_{\in I_2} \in I_1 + I_2$$

2. דוגמא לסכום אידאלים: הוכיחו: $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.
פתרון: $\subseteq$: יהי $4a + 6b \in 4\mathbb{Z} + 6\mathbb{Z}$ אזי נקבל:

$$4a + 6b = 2\underbrace{(2a + 3b)}_{\in \mathbb{Z}} \in 2\mathbb{Z}$$

$\supseteq$: יהי $2a \in 2\mathbb{Z}$. מכיון ש־ $2 = gcd(4, 6)$ אזי לפי ההרצאה קיימים $m, n \in \mathbb{Z}$ כך ש־ $2 = 4m + 6n$. ומכאן נקבל:

$$2a = (4m + 6n)a = 4ma + 6na \in 4\mathbb{Z} + 6\mathbb{Z}$$

3. הוכיחו שהקבוצה $I = \{d(x) \in \mathbb{F}[x] \mid d(0) = 0\}$ היא אידאל ראשי.
פתרון: צריך למצוא $f(x) \in \mathbb{F}[x]$ כך ש־ $I = \langle f(x) \rangle = \{g(x) \cdot f(x) \mid g(x) \in \mathbb{F}[x]\}$.
נוכיח:

$$I = \langle x \rangle$$

$\subseteq$: יהי $d \in I$ אז אם $d = 0$ ברור ש־ $d \in \langle x \rangle$. אחרת, $d(0) = 0$ ולכן נקבל שהוא מהצורה:

$$d(x) = \sum_{k=1}^{n} a_k x^k = x \cdot \underbrace{\sum_{k=0}^{n-1} a_{k+1} x^k}_{\in \mathbb{F}[x]} \in \langle x \rangle$$

$\supseteq$: יהי $g(x) = x \cdot f(x) \in \langle x \rangle$, ולכן:

$$g(0) = 0 \cdot f(0) = 0$$

ולפי הגדרה $g \in I$.

4. אנחנו רוצים להוכיח את הכיוון מימין לשמאל של הטענה מההרצאה: $p(x) \in \mathbb{F}[x]$ מדרגה חיובית אי־פריק אמ"ם הוא ראשוני. נעשה בשני שלבים:

(א) נוכיח תחילה טענת עזר: אם $gcd(a(x), c(x)) = gcd(b(x), c(x)) = 1$ אז $gcd(a(x)b(x), c(x)) = 1$.
פתרון: לפי האלגוריתם ניתן יש m_1, n_1, m_2, n_2 כך ש־:

$$m_1(x)a(x) + n_1(x)c(x) = 1 = m_2(x)b(x) + n_2(x)c(x)$$

ולכן:

$$1 = (m_1(x)a(x) + n_1(x)c(x)) \cdot (m_2(x)b(x) + n_2(x)c(x)) =$$

$$(m_1(x)m_2(x))\, a(x)b(x) + (m_1(x)a(x)n_2(x) + n_1(x)m_2(x)b(x) + n_1(x)n_2(x)c(x)) \cdot c(x)$$

קיבלנו

$$1 = m \cdot (ab) + n \cdot c$$

נשים לב שכדי להוכיח $gcd(a(x)b(x), c(x)) = 1$ צריך להוכיח שני דברים:

i. $1|ab, c$. זה ברור, כי 1 מחלק כל פולינום.

ii. שאם $g|ab, c$ אז $g|1$. כעת, אם $g|ab, c$ אז הוא מחלק גם כל צירוף לינארי שלהם, ומכיוון ש־1 צ"ל שלהם נקבל $g|1$.

(ב) ניגש כעת להוכחת הטענה: אם $p(x) \in \mathbb{F}[x]$ מדרגה חיובית אי־פריק אז הוא ראשוני.

פתרון: נתון p אי פריק, וצ"ל שהוא ראשוני. נניח $p|ab$. צ"ל $p|a \vee p|b$.
נסמן $d(x) = gcd(a(x), p(x))$. מכיון ש־ $d(x)|p(x)$ נקבל שיש $q(x)$ כך ש־ $p(x) = d(x) \cdot q(x)$. מכיון שנתון ש־p אי־פריק, נקבל $\deg(d) = 0 \vee \deg(q) = 0$. נחלק למקרים:

i. אם $\deg(q) = 0$ זאת אומרת ש־ $q \in \mathbb{F}$ ולכן הוא הפיך, ולכן נקבל $d(x) = q^{-1}p(x)$, ומכאן $p|d$, ולפי הגדרת ממ"מ $d|a$, ומטרנזיטיביות נקבל $p|a$.

ii. אם $\deg(d) = 0$ אז קיבלנו $1 = gcd(a, p)$. כעת נוכל לעשות את אותו דבר בעזרת הסימון $d'(x) = gcd(b(x), p(x))$, ולקבל $p|b \vee \deg(d') = 0$. אם $p|b$ סיימנו. אחרת, קיבלנו בסה"כ $1 = gcd(a, p) = gcd(b, p)$ ולפי תרגיל קודם: $1 = gcd(ab, p)$. שימו לב שמתקיים $p|ab$ (כי מזה התחלנו), וכמובן $p|p$, ולכן נקבל $p|1 = gcd(ab, p)$, ומכאן ש־ $\deg(p) < 1$ בסתירה לכך שלקחנו פולינום ממעלה חיובית. כלומר, בסה"כ קיבלנו $p|a \vee p|b$ או סתירה (כלומר, יש מקרה שלא יכול להיות בחלוקה למקרים).