מבנים אלגבריים תרגול 12

28 ביוני 2021

1 ממ"מ

תרגילים:

1. מצאו את $gcd(a,b)$ עבור: $a(x) = x^6 + x^5 + x^4 + x^2 + 1, b(x) = x^3 + x + 1$,
ורשמו אותו כצ"ל שלהם.
פתרון: נתחיל בחילוק:

$$\begin{array}{c|c}
q_1(x) = x^3 + x^2 - 2 & \\
\hline
x^6 + x^5 + x^4 + x^2 + 1 & x^3 + x + 1 \\
x^6 + x^4 + x^3 & \\
\downarrow & \\
x^5 - x^3 + x^2 + 1 & \\
x^5 + x^3 + x^2 & \\
\downarrow & \\
-2x^3 + 1 & \\
-2x^3 - 2x - 2 & \\
\downarrow & \\
r_1(x) = 2x + 3 &
\end{array}$$

בסה"כ: $a(x) = q_1(x) \cdot b(x) + r_1(x)$ או בפולינומים עצמם:

$$x^6 + x^5 + x^4 + x^2 + 1 = \left(x^3 + x^2 - 2\right)\left(x^3 + x + 1\right) + 2x + 3$$

כעת אנחנו יודעים: $gcd(a,b) = gcd(b,r_1)$. נחלק שוב:

$$\begin{array}{c|c}
q_2 = \frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8} & \\
\hline
x^3 + x + 1 & 2x+3 \\
x^3 + \frac{3}{2}x^2 & \\
\downarrow & \\
-\frac{3}{2}x^2 + x + 1 & \\
-\frac{3}{2}x^2 - \frac{9}{4}x & \\
\downarrow & \\
\frac{13}{4}x + 1 & \\
\frac{13}{4}x + \frac{39}{8} & \\
\downarrow & \\
r_2 = -\frac{31}{8} &
\end{array}$$

קיבלנו: $b = q_2r_1 + r_2$, ומתקיים: $gcd(a,b) = gcd(b,r_1) = gcd(r_1,r_2)$.
הערה: אם בשלב מסויים מקבלים שארית קבועה $r_k = c \in \mathbb{F}$ אז בוודאות נקבל $r_{k+1} = 0$, ולכן $gcd = r_k$. הסבר: שימו לב ש מהפיכות r_k מתקיים: $r_2|r_1$ כי:

$$r_1 = 2x + 3 = -\frac{31}{8} \cdot \left(-\frac{16}{31}x - \frac{24}{31}\right)$$

ולכן r_2 הוא מחלק משותף מקסימלי שאיננו מתוקן, נתקן וניקח

$$gcd(a,b) = 1$$

נותר לנו כעת למצוא $m(x), n(x)$ כך ש־:

$$1 = m(x)a(x) + n(x)b(x)$$

המשוואה האחרונה שקיבלנו היא: $b = q_2r_1 + r_2$, ולאחר העברת אגפים: $r_2(x) = b(x) - q_2(x)r_1(x)$. או במספרים:

$$-\frac{31}{8} = \underbrace{x^3 + x + 1}_{b(x)} - \underbrace{\left(\frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8}\right)(2x+3)}_{q_2(x)r_1(x)}$$

כעת נשתמש בשלב הראשון: $a(x) = q_1(x) \cdot b(x) + r_1(x)$ כלומר, נוכל להציב:

$$r_1(x) = a(x) - q_1(x)b(x)$$

במשוואה לעיל:

$$r_2(x) = b(x) - q_2(x)r_1(x) = b(x) - q_2(x)\left(a(x) - q_1(x)b(x)\right) =$$

$$= b(x)\left(1+q_1(x)q_2(x)\right)+a(x)\left(-q_2(x)\right)$$

בספרים:

$$-\frac{31}{8} = b(x)\left(1+q_1(x)q_2(x)\right)+a(x)\left(-q_2(x)\right)$$

ולכן:

$$gcd(a,b) = 1 = -\frac{8}{31}\left(b(x)\left(1+q_1(x)q_2(x)\right)+a(x)\left(-q_2(x)\right)\right) =$$

$$= \underbrace{-\frac{8}{31}\left(1+q_1(x)q_2(x)\right)}_{=n(x)}\cdot b(x)+\underbrace{\frac{8}{31}q_2(x)}_{=m(x)}\cdot a(x)$$

2. עבור $a(x) = x^3+4x^2+2x-3, b(x) = x^2+2x-3$ מצאו $gcd(a,b)$ והציגו אותו כצ"ל שלהם:

$$\begin{array}{c|c} q_1(x) = x+2 & \\ \hline x^3+4x^2+2x-3 & x^2+2x-3 \\ x^3+2x^2-3x & \\ \downarrow & \\ 2x^2+5x-3 & \\ 2x^2+4x-6 & \\ \downarrow & \\ r_1(x) = x+3 & \end{array}$$

ולכן:

$$a(x) = q_1(x)b(x)+r_1(x)$$

$$x^3+4x^2+2x-3 = (x+2)(x^2+2x-3)+x+3$$

כעת נמשיך לחלק את b ב־ r_1:

$$\begin{array}{c|c} q_2(x) = x-1 & \\ \hline x^2+2x-3 & x+3 \\ x^2+3x & \\ \downarrow & \\ -x-3 & \\ -x-3 & \\ \downarrow & \\ r_2(x) = 0 & \end{array}$$

ולכן $r_1(x) = gcd(a,b)$. נמצא אותו כעת כצ"ל שלהם:

$$r_1(x) = a(x) - q_1(x)b(x)$$

כלומר, $m(x) = 1, n(x) = -q_1(x)$.

2 אידאלים

תרגילים:

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

$$(a+b) - (x+y) = (a-x) + (b-y) \in I_1 + I_2$$

בליעה: יהי $r \in R, x + y \in I_1 + I_2$ אז:

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

ובאותצו אופן:

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

2. הוכיחו: $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$
פתרון: $\subseteq$: יהי $4a + 6b \in 4\mathbb{Z} + 6\mathbb{Z}$, לכן נקבל:

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

$\supseteq$: יהי $2a \in 2\mathbb{Z}$ צריך למצוא $b, c \in \mathbb{Z}$ כך ש־ $2a = 4b+6c$. נשים לב $2 = gcd(4,6)$, ולכן (יישום של משפט מההרצאה, ממ"מ ניתן לרשום כצ"ל של הגורמים):

$$2 = 4 \cdot (-1) + 6 \cdot 1$$

ולכן:

$$2a = 4 \cdot (-a) + 6 \cdot a$$

כלומר, נבחר $b = -a, c = a$.

3. הוכיחו שהקבוצה $I = \{d(x) \in \mathbb{F}[x] \mid d(0) = 0\}$ אידאל ראשי בחוג הפולינומים.
פתרון: צריך למצוא פולינום $f(x) \in \mathbb{F}[x]$ כך ש־

$$I = \langle f \rangle = \{g \cdot f \mid g \in \mathbb{F}[x]\}$$

נשים לב שב־I נמצאים כל הפולינומים שהמקדם החופשי שלהם הוא 0 (כי כאשר מציבים בפולינום 0 מקבלים את המקדם החופשי). אצלנו ניקח x $f(x) =$. ונוכיח $I = \langle x \rangle$:

$\subseteq$: יהי $d(x) = \sum_{k=1}^{n} a_k x^k$ (דילגנו על $a_0 x^0$ כי איבר ב־I מקיים $a_0 = 0$), ולכן:

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

$\supseteq$: יהי $d(x) = xf(x) \in \langle x \rangle$. כדי להוכיח שהוא ב־$I$ צריך להראות שמתאפס ב־0:

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

ולכן $d(x) \in I$.

3 ראשוניות

בהרצאה הופיע ללא הוכחה המשפט: יהי $p(x) \in \mathbb{F}[x]$. מתקיים: p ראשוני אמ"ם הוא אי־פריק. בתרגיל תוכיחו את הכיוון $\Leftarrow$. נוכיח כעת $\Rightarrow$:

כלומר, יהי p אי־פריק, נראה שהוא ראשוני. נניח ש־ $p(x)|a(x)b(x)$ צ"ל: $p(x)|a(x) \vee p(x)|b(x)$.

נסמן $d(x) = gcd(p(x), a(x))$ בפרט, $d(x)|p(x)$ מה שאומר שקיים $q(x)$ כך ש־ $p(x) = d(x)q(x)$. נתון p אי פריק, ולכן אם $p = dq$ אז $\deg(d) = 0, \deg(q) = 0$. נחלק למקרים:

- אם $\deg(q) = 0$ זאת אומרת ש־ $q \in \mathbb{F}$ ולכן הוא הפיך, ונקבל:

$$p = dq \Rightarrow d = q^{-1} p$$

ונקבל $p|d$. בנוסף מהגדרת $d = gcd(p, a)$ מקבלים $d|a$, ומטרנזיטיביות החילוק נקבל: $p|a$ כמו שרצינו.

- אם $\deg(d) = 0$ אז בגלל שאנחנו דורשים פולינום מתוקן כ־ממ"מ נקבל:

$$gcd(p, a) = 1$$

לכן קיימים $m,n \in \mathbb{F}[x]$ כך ש־

$$1 = mp + na$$

נכפיל את המשוואה ב־b ונקבל:

$$b = mpb + nab$$

התחלנו מכך ש־ $p|ab$ מה שאומר קיים c כך ש־ $ab = cp$, ולכן נוכל להציב ולקבל:

$$b = mpb + ncp = p(mb + nc)$$

ולכן $p|b$.