

פתרון תרגיל מספר 10 מבנים אלגבריים

1. יהי R חוג, ונניח שקיימים $a, b \in R$ איברים נילפוטנטיים. הוכיחו או הפריכו:

(א) $a + b$ נילפוטנטי.

(ב) ab נילפוטנטי.

(ג) שני הסעיפים הקודמים עם R קומוטטיבי.

פתרון:

א. לא נכון. למשל ב $M_2(\mathbb{R})$ האיברים $a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ הינם נילפוטנטיים, אבל החיבור ביניהם

היא מטריצה הפיכה $a + b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ שאיננה מחלקת אפס, ובפרט לא נילפוטנטית.

ב. לא נכון. באותה דוגמא נקבל $ab = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = A$. נשים לב שמתקיים:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

ולכן נקבל שזו מטריצה שלכל n מתקיים $A^n = A \neq 0$.

ג. סעיף א הראנו בתרגול שכיון ש- R קומוטטיבי ניתן להשתמש בנוסחת הבינום ולקבל שאם $a^n = b^m = 0$ אז

$$(a + b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} = \sum_{k=0}^n \binom{n+m}{k} a^k \cdot 0 + \sum_{k=n+1}^{n+m} \binom{n+m}{k} 0 \cdot b^{n+m-k} = 0$$

כאשר המעבר אחד לפני האחרון נובע מהעובדה שאם $k \leq n$ אז $n + m - k \geq m$ ולכן $b^{n+m-k} = 0$ ואם $k > n$ אז $a^k = 0$.

סעיף ב, בדומה, אם $a^n = b^m = 0$ אז $(ab)^n = a^n b^n = 0 \cdot b^n = 0$.

2. מצאו חוג R עבורו הקבוצות הבאות אינן תת-חוג:

(א) $S \subseteq R$ אוסף האיברים שאינם הפיכים.

(ב) $S \subseteq R$ אוסף האיברים הנילפוטנטיים.

פתרון:

א.ב. לפי שאלה קודמת נקבל שבחוג $M_2(\mathbb{R})$ שתי הקבוצות אינן תת חוג כי אינן סגורות לחיבור, שהרי האיברים

$a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ שאינם הפיכים והינם נילפוטנטיים, סכומם הפיך וכמובן לא נילפוטנטי.

3. יהא $f(x) \in \mathbb{F}[x]$ פולינום מדרגה n . ראינו בתרגול כי $\mathbb{F}[x]/I(f) = \{[g] \mid \deg(g) < n, g \in \mathbb{F}[x]\}$. הוכיחו כי בקבוצה זאת האיברים שונים. כלומר, יהיו g_1, g_2 שני פולינומים מדרגה קטנה מ n . הוכיחו כי

$$[g_1] = [g_2] \iff g_1 = g_2$$

(להזכירכם היחס השקילות הוא $g \sim_I g' \iff (g - g') \in I$.)

פתרון:

(\Leftarrow) ברור.

(\Rightarrow) נתון $[g_1] = [g_2]$ אזי $g_1 \sim_I g_2$ כלומר $g_1 - g_2 \in I(f)$. ומכאן כי

$$\exists g \in \mathbb{F}[x] : g_1 - g_2 = fg$$

נרצה להראות כי $g = 0$. נניח בשלילה כי $g \neq 0$ אזי

$$\deg(fg) = \deg(f) + \deg(g) \geq \deg(f) = n$$

מצד שני

$$\deg(g_1 - g_2) \leq \max\{\deg(g_1), \deg(g_2)\} < n$$

בסתירה. לכן $g = 0$ ולכן $g_1 = g_2$.

4. עבור הפולינומים $a(x) = 1 + 2x^2, b(x) = 2 + x \in \mathbb{R}[x]$ מתקיים כי $1 = \gcd(a, b)$ ומתקיים

$$1 = \frac{1}{9}a(x) - \frac{2x-4}{9}b(x)$$

מצאו פולינום $f(x)$ המקיים

$$f(x) \sim_{a(x)} 5$$

$$f(x) \sim_{b(x)} x$$

כאשר $f \sim_{a(x)} g$ פירושו $f \sim_{I(a(x))} g$ או יותר מפורש $f - g \in I(a(x))$. [השתמשו ברעיון דומה למשפט השאריות הסיני]

פתרון:

$$1 = \frac{1}{9}a(x) - \frac{2x-4}{9}b(x)$$

לכן

$$\frac{1}{9}a(x) \sim_{b(x)} 1, \quad -\frac{2x-4}{9}a(x) \sim_{a(x)} 0$$

$$-\frac{2x-4}{9}b(x) \sim_{b(x)} 0, \quad -\frac{2x-4}{9}b(x) \sim_{a(x)} 1$$

ומכאן שנגדיר

$$f(x) = x \cdot \left[\frac{1}{9}a(x) \right] + 5 \cdot \left[-\frac{2x-4}{9}b(x) \right]$$

יקיים

$$f(x) \sim_{a(x)} 5 \cdot \left[-\frac{2x-4}{9}b(x) \right] \sim_{a(x)} 5 \cdot 1 = 5$$

ובנוסף

$$f(x) \sim_{b(x)} x \cdot \left[\frac{1}{9}a(x) \right] \sim_{b(x)} x \cdot 1 = x$$

כנדרש.

5. תזכורת: יהיו R_1, R_2 חוגים. פונקציה $\phi : R_1 \rightarrow R_2$ תקרא הומומורפיזם של חוגים אם

1. לכל מתקיים $x, y \in R_1$ $\phi(xy) = \phi(x)\phi(y)$

2. לכל מתקיים $x, y \in R_1$ $\phi(x+y) = \phi(x) + \phi(y)$

הערה: נסמן $R_1 \cong R_2$ (R_1 איזומורפי ל R_2) אם קיים $\phi : R_1 \rightarrow R_2$ הומומורפיזם חח"ע ועל.

(א) הוכיחו כי הגרעין $\ker \phi = \{x \in R_1 \mid \phi(x) = 0\}$ הוא אידיאל של R_1 .

(ב) הוכיחו כי $Im(\phi) = \{\phi(x) \mid x \in R_1\}$ הוא תת חוג של R_2 (כלומר הוא חוג ביחס לפעולות של R_2).

פתרון:

א. נוכיח $\ker \phi$ תת חבורה ביחס לחיבור .

1. סגירות (קריטריון מקוצר): יהיו $x_1, x_2 \in \ker \phi$ צ"ל $x_1 - x_2 \in \ker \phi$.אכן מתקיים: $\phi(x_1) = 0, \phi(x_2) = 0$ ולכן $\phi(x_1 - x_2) = \phi(x_1) - \phi(x_2) = 0 - 0 = 0$ (המעבר הראשון נובע מהגדרת הומו' של חבורות). ולכן $x_1 - x_2 \in \ker \phi$.

2. נטרלי: כיוון ש $\phi(0) = 0$ (כי ϕ בפרט הומומורפיזם בין החבורות $(R_1, +)$ ל $(R_2, +)$) נקבל כי $0 \in \ker \phi$.
נוכיח כי $\ker \phi$ בולע:

יהא $x \in \ker \phi$ ו $r \in R_1$ אזי $\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0 = 0$ לכן $rx \in \ker \phi$. באופן דומה גם $xr \in \ker \phi$ וסיימנו.

ב. נוכיח $Im(\phi)$ תת חבורה ביחס לחיבור .

1. סגירות: יהיו $\phi(x_1), \phi(x_2) \in Im(\phi)$ אזי $\phi(x_1) - \phi(x_2) = \phi(x_1 - x_2) \in Im(\phi)$.

2. נטרלי: כיוון ש $\phi(0) = 0$ נקבל כי $0 \in Im(\phi)$.

נוכיח כי הכפל מוגדר (קיבוציות ופילוג מתקיימת כי זה תת קבוצה של R_2):

יהיו $\phi(x_1), \phi(x_2) \in Im(\phi)$ אזי $\phi(x_1)\phi(x_2) = \phi(x_1x_2) \in Im(\phi)$.

6. משפט האיזומורפיזם הראשון לחוגים: יהיו R_1, R_2 חוגים ויהא $\phi : R_1 \rightarrow R_2$ הומומורפיזם של חוגים אזי

$$R_1/\ker \phi \cong Im(\phi)$$

(א) יהא \mathbb{F} שדה, $\mathbb{K} \subseteq \mathbb{F}$ תת שדה שלו ו $a \in \mathbb{F}$. נגדיר $\phi : \mathbb{K}[x] \rightarrow \mathbb{F}$ ע"י $\phi(f) = f(a)$ (פונקציה זאת נקראת הומומורפיזם ההצבה). הוכיחו כי ϕ הומומורפיזם.

(ב) נתסכל על הומומורפיזם ההצבה הבא: $\phi : \mathbb{Q}[x] \rightarrow \mathbb{R}$ המוגדר ע"י $\phi(f) = f(\sqrt{2})$ (שימו לב שזה דוגמא לסעיף הקודם). הוכיחו כי $Im(\phi) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ומצאו $\hat{f}(x) \in \mathbb{Q}[x]$ כך ש $\mathbb{Q}[x]/I(\hat{f}) \cong \mathbb{Q}[\sqrt{2}]$.

פתרון:

א. לכל $f, g \in \mathbb{K}[x]$ מתקיים כי :

1. $\phi(f+g) = (f+g)(a) = f(a) + g(a) = \phi(f) + \phi(g)$

2. $\phi(f \cdot g) = (f \cdot g)(a) = f(a) \cdot g(a) = \phi(f)\phi(g)$

ב. נשים לב כי $Im(\phi) = \{f(\sqrt{2}) \mid f \in \mathbb{Q}[x]\}$. כיוון שלכל k טבעי מתקיים כי $2^k \in \mathbb{Q}$ וגם $(\sqrt{2})^{2k} = 2^k$

$f(x) \in \mathbb{Q}[x]$ מתקיים $f(\sqrt{2}) = \sum_{i=0}^n a_i(\sqrt{2})^i = a + b\sqrt{2}$ עבור $a, b \in \mathbb{Q}$ נקבל כי לכל פולינום $(\sqrt{2})^{2k+1} = 2^k\sqrt{2}$

(מקבצים את כל החזקות הזוגיות ל- a והאי-זוגיות ל- b). ולכן

$$Im(\phi) = \{f(\sqrt{2}) \mid f \in \mathbb{Q}[x]\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

כנדרש.

בנוסף: $\ker \phi = \{f \in \mathbb{Q}[x] \mid f(\sqrt{2}) = 0\}$. טענה: $\ker \phi = I(\hat{f}(x))$ עבור $\hat{f}(x) = x^2 - 2 \in \mathbb{Q}[x]$. הוכחה:

(\subseteq) יהא $gf \in I(\hat{f})$ אזי $gf(\sqrt{2}) = g(\sqrt{2}) \cdot \hat{f}(\sqrt{2}) = g(\sqrt{2}) \cdot 0 = 0$ ולכן $gf \in \ker \phi$.
 (\supseteq) יהא $f \in \ker \phi$ אזי $f(\sqrt{2}) = 0$ נבצע חילוק פולינומים ונקבל $f = q\hat{f} + r$ עבור $r \equiv 0$ או $\deg(r) < \deg(\hat{f})$.
 לכן $r = f - q\hat{f}$ ולכן

$$r(\sqrt{2}) = f(\sqrt{2}) - q(\sqrt{2})\hat{f}(\sqrt{2}) = 0 - q(\sqrt{2})0 = 0$$

ומכאן ש $r = 0$ כי אחרת דרגתו 0 או 1. כלומר $r(x) = c$ או $r(x) = ax + c$ עבור $a, c \in \mathbb{Q}$ אבל $\sqrt{2}$ אינו שורש של פולינומים כאלה.
 לכן $f = q\hat{f} \in I(\hat{f})$.

.7

(א) הוכיחו כי $f(x) = x^2 + x + 4 \in \mathbb{Z}_{11}[x]$ ראשוני ולכן $\mathbb{F} = \mathbb{Z}_{11}[x]/\langle x^2 + x + 4 \rangle$ שדה.

(ב) מצאו $[3x + 2]^{-1}$ ב \mathbb{F} הנ"ל.

פתרון:

א. בשיעורי בית קודמים ראינו כי פולינומים עד דרגה 3 הוא ראשוני אמ"מ אין לו שורש. נבדוק שאין ל $f(x)$ שורש.

$$\begin{aligned} f(0) &= 4 \\ f(1) &= 6 \\ f(2) &= 10 \\ f(3) &= 5 \\ f(4) &= 2 \\ f(5) &= 1 \\ f(6) &= 2 \\ f(7) &= 5 \\ f(8) &= 10 \\ f(9) &= 6 \\ f(10) &= 4 \end{aligned}$$

ב. נחשב $\gcd(3x + 2, x^2 + x + 4)$:

$$(3x + 2)(4x + 5) = 12x^2 + 8x + 15x + 10 = x^2 + x + 10$$

ולכן

$$x^2 + x + 4 = (3x + 2)(4x + 5) + 5$$

$$3x + 2 = (5)(5x + 7) + 0$$

ולכן

$$5 = x^2 + x + 4 - (3x + 2)(4x + 5)$$

נכפיל ב $5^{-1} = 9$ ונקבל

$$1 = 9(x^2 + x + 4) + 2((3x + 2)(4x + 5))$$

מודלו $x^2 + x + 4$ נקבל

$$1 \equiv_f (3x + 2) \cdot 2(4x + 5)$$

ולכן

$$(3x + 2)^{-1} \equiv_f 2(4x + 5) = 8x + 10$$

8. יהי $\mathbb{F} = \mathbb{F}_{2^n}$ שדה סופי הוא מקיים כי $1 + 1 = 0$. הוכיחו כי כל איבר בו הוא ריבוע כלומר $\forall x \in \mathbb{F} \exists y \in \mathbb{F} : x = y^2$. הדרכה: נגדיר העתקה $\phi : \mathbb{F} \rightarrow \mathbb{F}$ ע"י $\phi(x) = x^2$ הראו שהעתקה זו היא חח"ע והסיקו כי ϕ על ולכן הטענה מתקיימת.

פתרון:

נראה חח"ע: נניח $\phi(a) = \phi(b)$ אזי $a^2 = b^2$, ולכן:

אם $a = 0$ נקבל ש $b^2 = 0$ שזה גורר כי $b = 0$ (אחרת b הפיך, נכפול בהופכי משני הצדדים ונקבל כי $b = 0$).
אם $b = 0$ נקבל באופן דומה ש $a = 0$.

אחרת, $a, b \neq 0$ אזי $a, b \in \mathbb{F}^\times$ החבורה הכפלית של השדה (חבורה עם $2^n - 1$ איברים) ולכן

$$a^{2^n - 1} = 1 = b^{2^n - 1}$$

מה שגורר כי

$$a^{2^n} = a, b^{2^n} = b$$

כעת נתון ש $a^2 = b^2$. נעלה בחזקת 2^{n-1} ונקבל

$$a = (a^2)^{2^{n-1}} = (b^2)^{2^{n-1}} = b$$

שזה מסיים את ההוכחה כי ϕ חח"ע.

כעת פונקציה מקבוצה סופית לעצמה היא חח"ע אמ"מ היא על ולכן ϕ על. בפרט לכל איבר יש מקור. יהא $x \in \mathbb{F}$ אזי יש לו מקור כלומר קיים $y \in \mathbb{F}$ כך ש $y^2 = \phi(y) = x$.

9. יהא $\mathbb{F} = \mathbb{F}_{p^n}$ שדה עם p^n איברים. הוכיחו כי

$$x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}^\times} (x - \alpha)$$

כאשר השיוון הוא שיוון פולינומים ו $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. יהא p מספר ראשוני אי זוגי אזי

$$(p - 1)! \equiv -1 \pmod{p}$$

פתרון:

כיוון שכל איבר $\alpha \in \mathbb{F}^\times$ מתקיים כי $\alpha^{p^n-1} = 1$ (משפט לגרנז' עבור החבורה הכפלית (\mathbb{F}^\times) נקבל כי כל איבר $\alpha \in \mathbb{F}^\times$ הוא שורש של הפולינום $x^{p^n-1} - 1$. כיוון שלפולינום זה יכול להיות לכל היותר $p^n - 1$ שורשים (כמעלת הפולינום) בעצם מצאנו את כולם ולכן השיוון מתקיים.
 כעת נציב $x = 0$ ונקבל כי

$$-1 = \prod_{\alpha \in \mathbb{F}^\times} -\alpha = (-1)^{|\mathbb{F}^\times|} \prod_{\alpha \in \mathbb{F}^\times} \alpha$$

במקרה הפרטי של השדה \mathbb{Z}_p (כאשר p ראשוני אי זוגי) נקבל כי

$$-1 = (-1)^{p-1} \prod_{i=1}^{p-1} i = (p-1)!$$

שיוון זה מתקיים בשדה שלנו שזה שקול ל

$$(p-1)! \equiv -1 \pmod{p}$$