

פתרון תרגיל 4

שאלה 1:

(א) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ עם חיבור וכפל של מספרים שלמים (שימו לב

שהקבוצה שהגדרנו היא תת קבוצה של המספרים הממשיים \mathbb{R})

פתרון: נתחיל עם הטענה כי $\mathbb{Z}[\sqrt{2}]$ ביחס לחיבור היא חבורה כיוון שהיא

תת קבוצה של הממשיים זה שקול להוכיח כי היא תת חבורה שלהם. נשתמש

בקריטריון הקצר:

לכל $a + b\sqrt{2}, x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ מתקיים

$$(a + b\sqrt{2}) - (x + y\sqrt{2}) = (a - x) + (b - y)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

בנוסף $0 \in \mathbb{Z}[\sqrt{2}]$

טענה הכפל ב $\mathbb{Z}[\sqrt{2}]$ מוגדר וקיבוצי:

מוגדר: לכל $a + b\sqrt{2}, x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ מתקיים

$$(a + b\sqrt{2})(x + y\sqrt{2}) = (ax + 2by) + (ay + bx)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

קיבוציות: נובע מקיבוציות של מספרים ממשיים

פילוג/חילופיות גם נובע מפילוג/חילופיות של מספרים ממשיים.

בחוג $\mathbb{Z}[\sqrt{2}]$ היחידה היא $1 \in \mathbb{Z}[\sqrt{2}]$

החוג $\mathbb{Z}[\sqrt{2}]$ אינו עם חילוק כי ל 2 אין הופכי. למה?

נניח בשלילה כי קיים $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ כך ש $2(a + b\sqrt{2}) = 1$ זה גורר כי

$2a - 1 = b\sqrt{2}$ בצד ימין יש מספר שלם. ולכן גם המספר בצד משאל שלם. זה

קורה אמ"מ $b = 0$. זה גורר $2a - 1 = 0$ כלומר $a = \frac{1}{2}$ סתירה לכך ש $a \in \mathbb{Z}$

(ב) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ עם חיבור וכפל של מספרים שלמים (שימו לב

שהקבוצה שהגדרנו היא תת קבוצה של המספרים הממשיים \mathbb{R})

פתרון: פתרון דומה לסעיף הקודם של $\mathbb{Z}[\sqrt{2}]$. ההבדל הוא ש $\mathbb{Q}[\sqrt{2}]$ הינו חוג

עם חילוק (ובעצם שדה).

הוכחה: יהא $(a + b\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$ $0 \neq$ צריך למצוא לו הופכי כלומר $c +$

$d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ המקיים

$$(a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

זה שני משוואות בשני נעלמים c, d

$$ac + 2bd = 1$$

$$(ad + bc)\sqrt{2} = 0\sqrt{2}$$

זה מתרגם למערכת המשוואות:

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

יש לה פתרון אמ"מ $a^2 - 2b^2 \neq 0$ $\det\left(\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\right) = a^2 - 2b^2 \neq 0$ וזה אכן המצב.

הוכחה: נניח בשלילה כי $a^2 - 2b^2 = 0$ זה גורר כי $\left(\frac{a}{b}\right)^2 = 2$ או $b = 0$

אם $\left(\frac{a}{b}\right)^2 = 2$ אז $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ סתירה.

אם $b = 0$ אז $a = 0$ גם כן ואז נקבל סתירה לכך ש $0 \neq (a + b\sqrt{2})$

(ג) הקבוצה $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ עם כפל וחיבור מטריצות.

פתרון: נתחיל עם הטענה כי R ביחס לחיבור היא חבורה כיוון שהיא תת קבוצה של המטריצות זה שקול להוכיח כי היא תת חבורה שלהם. נשתמש בקריטריון הקצר:

לכל $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} \in R$ מתקיים כי

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{pmatrix} \in R$$

בנוסף $0 \in R$.

טענה הכפל ב R מוגדר וקיבוצי:

מוגדר: לכל $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} \in R$ מתקיים כי

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 \\ 0 & 0 \end{pmatrix} \in R$$

קיבוציות: נובע מקיבוציות של מטריצות פילוג- גם נובע מפילוג של מטריצות.

R אינו חילופי כי =

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

בחוג R אין יחידה

הוכחה: אחרת נסמן אותה ב $\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}$. צריך להתקיים לכל $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}$$

אבל

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 \\ 0 & 0 \end{pmatrix}$$

ולכן

$$\begin{pmatrix} a_1 a_2 & a_1 b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}$$

שזה לא אפשרי (אם נבחר את $a_1 = 1$ זה גורר כי $b_2 = b_1$ אבל b_1 יכול להיות כמה אפשריות)

כיוון ש R ללא יחידה אז הוא אינו חוג עם חילוק.

(ד) קבוצת הפונקציות מהממשיים לממשיים $\{f: \mathbb{R} \rightarrow \mathbb{R} : f \text{ is function}\}$ עם חיבור פונקציות $(f+g)(x) = f(x)+g(x)$ וכפל מטריצות המוגדר כמכפלה $(fg)(x) = f(x)g(x)$

פתרון: נתחיל עם הטענה כי R ביחס לחיבור היא חבורה חילופית. חיבור פונקציות הוא מוגדר כי $f+g$ אכן פונקציה מהממשיים לממשיים לפי הגדרה.

חיבור פונקציות הוא חילופי כי $f+g = g+f$ כי $(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$

הנטרלי ביחס לחיבור זה פונקציה האפס המוגדרת $0(x) = 0$ [אכן $f+g = g$].
כי $(0+g)(x) = 0(x)+g(x) = 0+g(x) = g(x)$

יש נגדי: לכל פונקציה $f \in R$ הפונקציה $g \in R$ המוגדרת $g(x) = -f(x)$ תהיה נגדית כי $g+f = 0$ [אכן $(g+f)(x) = g(x)+f(x) = -f(x)+f(x) = 0$]

בנוסף הכפל ב R מוגדר וקיבוצי. נובע ממוגדרות וקיבוציות ב \mathbb{R} פילוג' יהיו $f, g, h \in R$ אזי $f \cdot g = fg = gf$ וקיבוציות ב \mathbb{R} נובע $(f+g)h(x) = f(x)h(x) + g(x)h(x) = (fh)(x) + (gh)(x)$ וכך בצד השני.

R חילופי כי $fg = gf$ מחילופיות ב \mathbb{R} ($fg(x) = f(x)g(x) = g(x)f(x)$ לכל x)

בחוג R יש יחידה וזוהי הפונקציה ששווה זהותי ל 1 , כלומר $1(x) = 1$
 R אינו חוג עם חילוק כי למשל לפונקציה $f(x) = x^2$ אין הופכית. למה? נניח שיש אזי $gf = 1$ נבחר $x = 0$ ונקבל כי $1(0) = 1 = gf(0) = g(0)f(0) = g(0) \cdot 0 = 0$ סתירה.

(ה) הקבוצה $\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} : z, w \in \mathbb{C} \right\} \subseteq \mathbb{C}^{2 \times 2}$ עם חיבור וכפל מטריצות.

פתרון: נתחיל עם הטענה כי \mathbb{H} ביחס לחיבור היא חבורה חילופית.

חיבור מוגדר כי $\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} + \begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1+z_2 & w_1+w_2 \\ -\bar{w}_1-\bar{w}_2 & \bar{z}_1+\bar{z}_2 \end{pmatrix}$

$\begin{pmatrix} z_1+z_2 & w_1+w_2 \\ -(\bar{w}_1+\bar{w}_2) & \bar{z}_1+\bar{z}_2 \end{pmatrix} \in \mathbb{H}$. בנוסף חיבור מטריצות הוא חילופי.

הנטרלי ביחס לחיבור זה מטריצת האפס שאכן שייכת ל \mathbb{H}
יש נגדי: לכל $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \in \mathbb{H}$ הנגדי $\begin{pmatrix} -z & -w \\ \bar{w} & -\bar{z} \end{pmatrix} \in \mathbb{H}$

\mathbb{H} נמצא גם כן ב \mathbb{H}
בנוסף הכפל ב \mathbb{H} מוגדר כי

$$\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} \begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1z_2 - w_1\bar{w}_2 & z_1w_2 + w_1\bar{z}_2 \\ -z_2\bar{w}_1 - \bar{z}_1\bar{w}_2 & -\bar{w}_1w_2 + \bar{z}_1\bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1z_2 - w_1\bar{w}_2 & z_1w_2 + w_1\bar{z}_2 \\ -z_1w_2 + w_1\bar{z}_2 & z_1z_2 - w_1\bar{w}_2 \end{pmatrix} \in \mathbb{H}$$

וקיבוצי כי הכפלת מטריצות היא קיבוצית
פילוג מתקיים כי חיבור וכפל מטריצות מקיים את תכונת הפילוג.
 R אינו חילופי כי =

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

ואילו

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

בחוג R יש יחידה וזוהי מטריצת הזהות.
 R הוא חוג עם חילוק. יהא $\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} \in \mathbb{H}$ מטריצה שונה מאפס. אזי הדטר' שלה היא

$$|z_1|^2 + |w_1|^2 \neq 0$$

ולכן היא הפיכה. נראה שההופכית גם שייכת ל \mathbb{H} . אכן

$$\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix}^{-1} = \frac{1}{|z_1|^2 + |w_1|^2} \begin{pmatrix} \bar{z}_1 & -w_1 \\ \bar{w}_1 & z_1 \end{pmatrix} \in \mathbb{H}$$

שאלה 2: יהיו $a = 80, n = 567$ מצא $d = \gcd(a, n)$ ומצא p, q כך ש $ap + qn = d$.
 אם $a \equiv 3 \pmod n$ המשוואה את הפתור שלו ופתור את המשוואה $ax \equiv 3 \pmod n$
פתרון: נחשב

$$\begin{aligned} 567 &= 80 \cdot 7 + 7 \\ 80 &= 7 \cdot 11 + 3 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

ולכן

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - (80 - 7 \cdot 11) \cdot 2 = 23 \cdot 7 - 2 \cdot 80 \\ &= 23 \cdot (567 - 80 \cdot 7) - 2 \cdot 80 = 23 \cdot 567 - 163 \cdot 80 \end{aligned}$$

ולכן $\gcd(a, b) = 1$ מכאשר ההופכי של a ממדולו n הוא -163
 לכן הפתרון למשוואה הוא $-163 \cdot 3 = -489 \equiv 78 \pmod n$

(א) נגדיר: $a(x) = 1 + 2x^2, b(x) = 2 + x \in \mathbb{R}[x]$ מצא $d = \gcd(a, b)$ ומצא p, q כך ש $ap + qb = d$
פתרון: נחשב

שאלה 3:

$$\begin{aligned} a(x) &= b(x) \cdot (2x - 4) + 9 \\ b(x) &= (9) \left(\frac{1}{9}x + \frac{2}{9} \right) + 0 \end{aligned}$$

ולכן

$$9 = a(x) - b(x) \cdot (2x - 4)$$

ומכאן ש

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

לכן $\gcd(a, b) = 1$ מכאשר $p(x) = \frac{1}{9}, q(x) = -\frac{2x-4}{9}$
 (ב) נגדיר: $a(x) = 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x, b(x) = x^3 + x^2 \in \mathbb{R}[x]$ מצא $d = \gcd(a, b)$ ומצא p, q כך ש $ap + qb = d$
פתרון: נחשב

$$\begin{aligned} a(x) &= b(x) \cdot (7x^4 - x^3 + 6x^2 - 2x + 5) + (-3x^2 + x) \\ b(x) &= (-3x^2 + x) \left(-\frac{x}{3} - \frac{4}{9} \right) + \left(\frac{4}{9}x \right) \\ (-3x^2 + x) &= \left(\frac{4}{9}x \right) \cdot \left(-\frac{27}{4}x + \frac{9}{4} \right) + 0 \end{aligned}$$

ולכן

$$\begin{aligned} \frac{4}{9}x &= b(x) - (-3x^2 + x) \left(-\frac{x}{3} - \frac{4}{9} \right) \\ &= b(x) - [a(x) - b(x) \cdot (7x^4 - x^3 + 6x^2 - 2x + 5)] \left(-\frac{x}{3} - \frac{4}{9} \right) \\ &= b(x) \left[1 + (7x^4 - x^3 + 6x^2 - 2x + 5) \left(-\frac{x}{3} - \frac{4}{9} \right) \right] + a(x) \left(\frac{x}{3} + \frac{4}{9} \right) \end{aligned}$$

ומכאן ש

$$x = b(x) \frac{[1 + (7x^4 - x^3 + 6x^2 - 2x + 5) (-\frac{x}{3} - \frac{4}{9})]}{4/9} + a(x) \frac{(\frac{x}{3} + \frac{4}{9})}{4/9}$$

$$p(x) = \frac{9}{4} (\frac{x}{3} + \frac{4}{9}), q(x) = \frac{9}{4} [1 + (7x^4 - x^3 + 6x^2 - 2x + 5) (-\frac{x}{3} - \frac{4}{9})]$$

שאלה 4:

יהא $\mathbb{F}_{16} = \mathbb{Z}_2[x] / \langle x^4 + x^3 + 1 \rangle$ שדה. נסתכל על החבורה הכפלית $G = \mathbb{F}_{16} \setminus \{0\}$. הוכח כי $x \in G$ (הפולינום x) הוא יוצר של G . (רמז: לא צריך לחשב את כל החזקות של x אם נעזרים במשפט לגרנג)
פתרון: בחבורה הכפלית יש $16 - 1 = 15$ איברים. ולכן הסדר של כל איבר בחבורה הוא אחד מ $\{1, 3, 5, 15\}$.
כעת:

- רק איבר היחידה הוא מסדר 1.
- $x^3 \neq 1$ ולכן הסדר של x אינו 3
- $x^5 = x^4 x = (x^3 + 1)x = x^4 + x = x^3 + 1 + x \neq 1$ ולכן הסדר של x אינו 5
- מסקנה: הסדר של x הוא 15 ולכן הוא יוצר של החבורה G (כי זה הגודל שלה)