מבנים דיסקרטיים – תרגיל 6 – פתרון

כל סעיף שווה 10 נקודות

שאלה 1

א. יהי $(R,+,\cdot)$ חוג ו-$S \subseteq R$ תת קבוצה של R. הוכיחו כי $(S,+,\cdot)$ הוא חוג אם ורק אם:

a. $S \neq \phi$

b. לכל $a,b \in S$ מתקיים $a+b, ab, -a \in S$.

ב. הראו בעזרת סעיף א או בכל דרך אחרת כי הקבוצה $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| a \in \mathbb{R} \right\} \subseteq M_{2\times 2}(\mathbb{R})$ עם כפל וחיבור מטריצות היא חוג. הראו גם כי יש לו יחידה והיא *שונה* ממטריצת היחידה.

פיתרון

סעיף א: כוון א: נניח כי $(S,+,\cdot)$ חוג. אזי $(S,+)$ חבורה ולכן $S \neq \phi$ (כי $0_S \in S$), כלומר הוכחנו את a. אם $a,b \in S$ אז $a+b, -a \in S$ כי $(S,+)$ חבורה ו-$ab \in S$ כי $(S,\cdot)$ מונויד. לכן הוכחנו את b, כדרוש.

כוון ב: נניח כי a ו-b מתקיימים.

נראה כי $(S,+)$ חבורה: נתון $S \neq \phi$ ושלכל $a,b \in S$ מתקיים $a+b, -a \in S$. לכן $(S,+)$ תת חבורה של $(R,+)$, בפרט $(S,+)$ חבורה.

נראה כי $(S,\cdot)$ אגודה: סגירות נובעת מ-b. לכל $a,b,c \in S$ מתקיים $(ab)c = a(bc)$ כי הכפל ב-R אסוציאטיבי, לכן פעולת הכפל על S גם אסוציאטיבית.

נראה כי דיסטריביוטיביות מתקיימת: יהיו $a,b,c \in S$. אזי $a,b,c \in R$ ומהדיסטריביוטיביות של R נובע $a(b+c) = ab+ac$ ו-$(b+c)a = ba+ca$. לכן, דיסטריביוטיביות מתקיימת.

לסיכום, $(S,+,\cdot)$ חוג, כדרוש. **מש"ל.**

הערה: סעיף א הוא משפט ואתם רשאים להשתמש בו בהוכחות במבחן ובתרגילי הבית.

סעיף ב: מספיק להראות כי S מקיימת את תנאים a ו-b מסעיף א. באמת, $S \neq \phi$ כי $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$.

בנוסף, אם $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} \in S$ אז

$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a+b & 0 \\ 0 & 0 \end{bmatrix} \in S$,

$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} \in S$,

$-\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} -a & 0 \\ 0 & 0 \end{bmatrix} \in S$ ולכן מתקיים b ונובע (מסעיף א) כי $(S,+,\cdot)$ חוג.

נראה כי $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in S$ יחידה של S (ברור כי היא שונה ממטריצת היחידה). באמת, לכל $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in S$ מתקיים $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, כדרוש.

שאלה 2

הראו כי כל אחד מהבאים הוא חוג. קבעו האם הוא חילופי והאם יש לו יחידה.

א. $R=\mathbb{Z}[\sqrt{3}]:=\{a+b\sqrt{3}\mid a,b\in\mathbb{Z}\}$ עם כפל וחיבור של מספרים ממשיים.

ב. $R=\left\{\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}\middle| a,b\in\mathbb{R}\right\}$ עם כפל וחיבור מטריצות.

ג. $(\mathbb{R}_+,\oplus,\otimes)$ באשר $a\oplus b=ab$ ו-$a\otimes b=e^{\ln a\cdot\ln b}$.

הוכחה

סעיף א: היות ו-$\mathbb{Z}[\sqrt{3}]\subseteq\mathbb{R}$, נעזר בשאלה 1 סעיף א כדי להוכיח ש-$\mathbb{Z}[\sqrt{3}]$ חוג (או, ליתר דיוק, תת חוג של $(\mathbb{R},+,\cdot)$): באמת, $\mathbb{Z}[\sqrt{3}]\neq\phi$ כי $0=0+0\cdot\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$. אם $a+b\sqrt{3},c+d\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$ (כאשר $a,b,c,d\in\mathbb{Z}$) אז

$$\left(a+b\sqrt{3}\right)+\left(c+d\sqrt{3}\right)=(a+b)+(c+d)\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$$
$$\left(a+b\sqrt{3}\right)\left(c+d\sqrt{3}\right)=(ac+3bd)+(ad+bc)\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$$
$$-\left(a+b\sqrt{3}\right)=(-a)+(-b)\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$$

לכן, תנאים a ו-b משאלה 1 סעיף מתקיימים ונובע כי $\left(\mathbb{Z}[\sqrt{3}],+,\cdot\right)$ חוג.

<u>$\mathbb{Z}[\sqrt{3}]$ חוג חילופי</u> כי הכפל ב-$\mathbb{R}$ חילופי.

<u>ל-$\mathbb{Z}[\sqrt{3}]$ יש יחידה:</u> $1=1+0\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$ (בדקו!).

סעיף ב: היות ו-$R\subseteq M_{2\times2}(\mathbb{R})$ והכפל והחיבור ב-R הם כפל וחיבור מטריצות, מספיק לוודא את תנאים a ו-b משאלה 1 סעיף א כדי להראות ש-R חוג. באמת, $R\neq\phi$ כי $\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\in R$. אם $\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix},\begin{bmatrix}c & d\\ 0 & 0\end{bmatrix}\in R$ (כאשר $a,b,c,d\in\mathbb{R}$) אז

$$\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}+\begin{bmatrix}c & d\\ 0 & 0\end{bmatrix}=\begin{bmatrix}a+c & b+d\\ 0 & 0\end{bmatrix}\in R$$
$$\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}\begin{bmatrix}c & d\\ 0 & 0\end{bmatrix}=\begin{bmatrix}ac & ad\\ 0 & 0\end{bmatrix}\in R$$
$$-\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}=\begin{bmatrix}-a & -b\\ 0 & 0\end{bmatrix}\in R$$

ולכן R חוג (ביחס לכפל וחיבור מטריצות).

<u>R לא חילופי</u> כי $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$ אבל $\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$.

<u>ל-R אין יחידה:</u> נניח בשלילה ש-$\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}\in R$ יחידה. אזי $\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$ (השוויון הימני נובע מההנחה ש-$\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}$ יחידה והשוויון השמאלי נובע מכפל מטריצות רגיל). כלומר, $\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$. אבל $\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$ לא יחידה כי $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\neq\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$ וקיבלנו סתירה להנחה. לכן ל-R אין יחידה.

הערה: דרך אחרת להפריך את קיום היחידה: אפשר להראות שיש שתי יחידות שמאליות שונות. לדוגמא, $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$ ו-$\begin{bmatrix}1 & 7\\ 0 & 0\end{bmatrix}$.

סעיף ג: כאן אין דרך להשתמש בשאלה 1 סעיף א, אז נוכיח כי R חוג לפי ההגדרה:

<u>נראה כי $(\mathbb{R}_+,\oplus)$ חבורה:</u> הפעולה $\oplus$ היא כפל מספרים ממשיים וכבר ציינו בכיתה ש-$(\mathbb{R}_+,\cdot)$ היא חבורה.

<u>נראה כי $(\mathbb{R}_+,\otimes)$ אגודה:</u> נבדוק סגירות: לכל $a,b\in\mathbb{R}_+$ מתקיים $a\otimes b=e^{\ln a\cdot\ln b}>0$ לכן סגירות מתקיימת. נבדוק אסוציאטיביות: יהיו $a,b,c\in\mathbb{R}_+$. אזי

$$(a\otimes b)\otimes c=e^{\ln a\ln b}\otimes c=e^{\ln e^{\ln a\ln b}\ln c}=e^{\ln a\ln b\ln c}=e^{\ln a\ln e^{\ln b\ln c}}=$$

$a \otimes e^{\ln b \ln c} = a \otimes (b \otimes c)$
כדרוש.
<u>נראה דיסטריביוטיביות משמאל:</u> יהיו $a, b, c \in \mathbb{R}_+$, אזי $a \otimes (b \oplus c) = a \otimes bc = e^{\ln a \ln bc} =$ $e^{\ln a \ln b + \ln a \ln c} = e^{\ln a \ln b} e^{\ln a \ln c} = (a \otimes b) \oplus (a \otimes c)$, כדרוש.
<u>אין צורך להוכיח דיסטריביוטיביות מימין כי $(\mathbb{R}_+, \oplus, \otimes)$ חוג חילופי:</u> באמת, לכל $a, b \in \mathbb{R}_+$ מתקיים $a \otimes b = e^{\ln a \ln b} = e^{\ln b \ln a} = b \otimes a$.
<u>ל-$(\mathbb{R}_+, \oplus, \otimes)$ יש יחידה</u> והיא e: באמת, $a \otimes e = e^{\ln a \ln e} = e^{\ln a \cdot 1} = e^{\ln a} = a$ לכל $a \in \mathbb{R}_+$ (אין צורך לבדוק ש-$e \otimes a = a$ כי $(\mathbb{R}_+, \oplus, \otimes)$ חוג חילופי).

הערה: למעשה, $(\mathbb{R}_+, \oplus, \otimes)$ שדה והוא איזומורפי ל-$(\mathbb{R}, +, \cdot)$. מה האיזומורפיזם?

שאלה 3

הראו כי כל אחת מהקבוצות הבאות <u>אינה</u> חוג ביחס לפעולות הנתונות.

א. $(\mathbb{C}, \oplus, \otimes)$ באשר $z \oplus w = z + w + 1$ ו-$z \otimes w = zw$ לכל $z, w \in \mathbb{C}$.
ב. $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, d \in \mathbb{R},\ c \in \mathbb{Z} \right\}$ עם כפל וחיבור מטריצות.
ג. $(\mathbb{N}, \oplus, \otimes)$ באשר $a \oplus b = \max\{a, b\}$ ו-$a \otimes b = a + b$.

פיתרון

סעיף א: $(\mathbb{C}, \oplus, \otimes)$ לא חוג כי <u>דיסטריביוטיביות לא מתקיימת</u>. לדוגמא,
$(0 \oplus 0) \otimes 2 = (0 + 0 + 1) \otimes 2 = 1 \otimes 2 = 1 \cdot 2 = 2$ אבל
$(0 \otimes 2) \oplus (0 \otimes 2) = (0 \cdot 2) \oplus (0 \cdot 2) = 0 \oplus 0 = 0 + 0 + 1 = 1$.
כלומר, $(0 \oplus 0) \otimes 2 \neq (0 \otimes 2) \oplus (0 \otimes 2)$.

הערה: $(\mathbb{C}, \oplus)$ חבורה (איבר ה-0 הוא -1) ו-$(\mathbb{C}, \otimes)$ מונויד.

הערה: דרך אחרת לפיתרון: הראו כי איבר ה-0 של $(\mathbb{C}, \oplus, \otimes)$ (תחת הנחה שהוא חוג) הוא -1. אם $(\mathbb{C}, \oplus, \otimes)$ באמת חוג אז לכל $a \in \mathbb{C}$ צריך להתקיים $a \otimes (-1) = a$. אבל $1 \otimes (-1) = -1 \neq 1$, כלומר קיבלנו סתירה.

סעיף ב: R לא חוג כי <u>אין סגירות לכפל</u> (בפרט, $(R, \cdot)$ לא אגודה ואפילו לא מאגמה). לדוגמא,
$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0.5 \end{bmatrix} \in R$ אבל $\begin{bmatrix} 0 & 0 \\ 0 & 0.5 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0.5 & 0 \end{bmatrix} \notin R$.

סעיף ג: $(\mathbb{N}, \oplus, \otimes)$ לא חוג כי $(\mathbb{N}, \oplus)$ לא חבורה. בתרגיל בית 1 שאלה 2 סעיף ג הוכחנו כי $(\mathbb{N}, \oplus)$ הוא מונויד שאינו חבורה.

הערה: $(\mathbb{N}, \otimes)$ הוא מונויד ו-$(\mathbb{N}, \oplus, \otimes)$ מקיים דיסטריביוטיביות.

שאלה 4

נגדיר תת קבוצה H של $M_{2\times 2}(\mathbb{C})$ ע"י $H = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \middle| z, w \in \mathbb{C} \right\}$.

א. העזרו בשאלה 1 סעיף א כדי להוכיח ש-H חוג.
ב. הראו כי H חוג עם חילוק (כלומר כל איבר למעט 0 הפיך) ושהוא אינו חילופי.

הערה: החוג H נקרא לעיתים *המספרים הקווטרניונים*.

הוכחה

סעיף א: נראה כי תנאים a ו-b משאלה 1 סעיף א מתקיימים עבור H.

באמת, $H \neq \phi$ כי $\begin{bmatrix} 0 & 0 \\ -\bar{0} & \bar{0} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in H$.

אם $\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}, \begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} \in H$ אז

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} + \begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} = \begin{bmatrix} z+x & w+y \\ -\bar{w}-\bar{y} & \bar{z}+\bar{x} \end{bmatrix} = \begin{bmatrix} z+x & w+y \\ -\overline{(w+y)} & \overline{z+x} \end{bmatrix} \in H$$

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} = \begin{bmatrix} zx - w\bar{y} & zy + w\bar{x} \\ -\bar{w}x - \bar{y}\bar{z} & -\bar{w}y + \bar{z}\bar{x} \end{bmatrix} = \begin{bmatrix} zx - w\bar{y} & zy + w\bar{x} \\ -\overline{zy + w\bar{x}} & \overline{zx - w\bar{y}} \end{bmatrix} \in H$$

(נעזרנו כאן בעובדות הבאות: לכל $z, w \in \mathbb{C}$: $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$ ו- $z = \bar{\bar{z}}$)

$-\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} = \begin{bmatrix} -z & -w \\ \bar{w} & -\bar{z} \end{bmatrix} \in H$.

לכן, H חוג (ביחס לכפל וחיבור מטריצות). **מש"ל.**

סעיף ב: ראשית נשים לב כי היחידה של H היא $1_H := \begin{bmatrix} 1 & 0 \\ -\bar{0} & \bar{1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$. זו יחידה ביחס לכפל כי מטריצת היחידה היא יחידה ביחס לכפל מטריצות. בנוסף, איבר ה-0 של H הוא $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ (בדקו!).

יהי $\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} \in H$ $\neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ (כאשר $x, y \in \mathbb{C}$). אזי $x \neq 0$ או $y \neq 0$ ולכן $d := \det\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} = x\bar{x} + y\bar{y} = |x|^2 + |y|^2 > 0$, כלומר המטריצה $\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}$ הפיכה ב- $M_{2\times 2}(\mathbb{C})$. מאלגברה לינארית אנחנו יודעים ש- $\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}^{-1} = \frac{1}{d}\begin{bmatrix} \bar{x} & -y \\ \bar{y} & x \end{bmatrix}$. היות ו- $d \in \mathbb{R}$ מתקיים $d = \bar{d}$ ולכן $\frac{1}{d}\begin{bmatrix} \bar{x} & -y \\ \bar{y} & x \end{bmatrix} = \begin{bmatrix} \bar{x}/d & -y/d \\ \bar{y}/d & x/d \end{bmatrix} = \begin{bmatrix} \bar{x}/\bar{d} & -y/d \\ \bar{y}/\bar{d} & x/d \end{bmatrix} = \begin{bmatrix} \overline{x/d} & -y/d \\ -\overline{(-y/d)} & \overline{(\overline{x/d})} \end{bmatrix} \in H$.

קיבלנו ש- $A := \begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}^{-1} \in H$ ומתקיים $A\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} = \begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_H$ ולכן $\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}$ הפיך ב-H.

הראנו שכל איבר שונה מ-0 ב-H הפיך <u>ולכן H חוג עם חילוק</u>.

<u>נראה כי H לא חילופי:</u> לדוגמא, $\begin{bmatrix} i & 0 \\ -\bar{0} & \bar{i} \end{bmatrix} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \in H$ ו- $\begin{bmatrix} 0 & 1 \\ -\bar{1} & \bar{0} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in H$ ומתקיים:

$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$ ו- $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

לכן, $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \neq \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. **מש"ל.**