

## פתרון בוחן ב' בקורס 89-214 תשפ"ב מבנים אלגבריים (מדעי המחשב)

### הוראות

1. יש לפתור את כל **שלוש** השאלות. הציון המרבי הוא 100.
2. **משך הבוחן** הוא 90 דקות.
3. **אין חומר עזר**. אין להשתמש במחשבון, טלפון, מחשב או בכל אמצעי אלקטרוני אחר.
4. כתבו את הפתרון לכל שאלה **בדף נפרד** ונמקו אותו היטב.
5. כתבו בעט כחול או שחור באופן ברור. הקפידו על סדר וניקיון.

**בהצלחה!**

## שאלות

הערה. בפתרון מלא יש לנמק ולפרט את הפתרונות. כאן מוצגות התשובות הסופיות בלבד, עם מעט רמזים.

**שאלה 1.** יהי  $n > 1$  מספר שלם.

1. (12 נק') הוכיחו כי  $n$  זר ל- $n^3 - 1$ .

2. (24 נק') יהי  $m \in \mathbb{N}$ . הביעו את המחלק המשותף המרבי של  $nm$  ושל  $n^3m - m$  כצירוף לינארי שלהם.

פתרון.

1. נשים לב לעובדה כי  $n^3 = n^2 \cdot n$ . לכן  $n^3 - 1 = n^2 \cdot n - 1$ . מכאן שניתן להביע את 1 כצירוף לינארי (עם מקדמים שלמים) של המספרים בשאלה:

$$1 = n^2 \cdot n - 1 \cdot (n^3 - 1)$$

לפי טענה שראינו בכיתה המחלק המשותף המרבי הוא גם הצירוף הלינארי הטבעי המזערי. מפני ש-1 הוא המספר הטבעי הקטן ביותר, אז הוא בהכרח המחלק המשותף המרבי של  $n$  ושל  $n^3 - 1$  לפי הצירוף הלינארי לעיל. כלומר המספרים האלו זרים.

יש הרבה אפשרויות אחרות להוכיח את הטענה הזאת. ניתן להשתמש למשל בטענה שאם  $x = qy + r$  עבור  $q, r \in \mathbb{Z}$  כלשהם (לא בהכרח כאלו שמגיעים מחלוקה אוקלידית), אז  $(x, y) = (y, r)$ . כעת מפני ש- $n^3 - 1 = n^2 \cdot n - 1$ , אז

$$(n^3 - 1, n) = (n, -1) = 1$$

ושב הראנו כי המספרים בשאלה זרים. אפשרות נוספת היא לבצע חלוקה אוקלידית ולקבל כי

$$n^3 - 1 = (n^2 - 1) \cdot n + (n - 1)$$

כאשר ברור כי  $0 \leq n - 1 < n$  לכל  $n$  טבעי. אז בשלב הבא של אלגוריתם אוקלידס נקבל

$$(n^3 - 1, n) = (n, n - 1) = (n - 1, 1) = 1$$

כי  $n = 1 \cdot (n - 1) + 1$ , ושוב הראנו שהמספרים האלו זרים.

2. לפי טענה מתרגיל הבית (שהופיעה גם בתרגול ללא הוכחה) אנחנו יודעים כי

$$(ax, ay) = |a|(x, y)$$

לכל  $a, x, y$  שלמים. אצלנו  $|m| = m$  כי  $m$  טבעי, ולכן עבור  $x = n$  ו- $y = n^3 - 1$  נקבל מהטענה הזו והסעיף הקודם כי המחלק המשותף המרבי  $(mx, my) = m \cdot 1$  הוא  $m$ . אפשר להשתמש בצירוף הלינארי של  $n$  ו- $n^3 - 1$  שמצאנו בסעיף הקודם, ולהכפיל אותו ב- $m$ :

$$\begin{aligned} m \cdot 1 &= m(n^2 \cdot n - 1 \cdot (n^3 - 1)) \\ m &= n^2 \cdot nm - 1 \cdot (mn^3 - m) \end{aligned}$$

כלומר המקדם של  $nm$  הוא  $n^2$  והמקדם של  $mn^3 - m$  הוא  $-1$ . ללא שימוש בהוכחות יותר ארוכות מצאנו את המחלק המשותף המרבי, שהוא  $m$ , והצגנו אותו כצירוף לינארי.

## שאלה 2. נתבונן בחבורה

$$G = \langle (1 \ 8 \ 9)(2 \ 1 \ 4)(4 \ 7 \ 9)(10 \ 3 \ 1)(6 \ 4 \ 1 \ 5) \rangle \cap A_{10}$$

שהיא חיתוך של שתי תת-חבורות של  $S_{10}$ .

1. (16 נק') הוכיחו או הפריכו: החבורה  $G$  היא ציקלית.
2. (16 נק') מצאו את  $|G|$ .

פתרון.

1. הוכחה. לצורך נוחות נסמן את התמורה בשאלה ב- $\sigma$ . כלומר  $G = \langle \sigma \rangle \cap A_{10}$ . נשים לב כי  $\langle \sigma \rangle$  היא חבורה ציקלית (הרי היא נוצרת על ידי איבר אחד, והוא התמורה  $\sigma$ ). בנוסף  $G$  היא תת-חבורה של  $\langle \sigma \rangle$ , כי חיתוך תת-חבורות הוא חבורה ולפי בדידה  $G \subseteq \langle \sigma \rangle$ . זה ש- $G$  היא גם תת-חבורה של  $A_{10}$  לא מעניין אותנו כעת. כל תת-חבורה של חבורה ציקלית היא בעצמה ציקלית (תרגיל שהוכחנו בכיתה), ולכן  $G$  ציקלית. הערות: שימו לב שההוכחה הייתה קצרה במיוחד, ואפילו לא היה צורך להציג את  $\sigma$  כמכפלת מחזורים זרים או למצוא יוצר מפורש של  $G$ . אפשר למצוא יוצר של  $G$ , לא באופן הכי מפורש, מבלי להתאמץ יותר מדי. נזכר כי הסימן הוא כפלי גם לתמורות שאינן זרות, ולכן  $\sigma$  היא מסימן  $-1 = (-1) \cdot 1 \cdot 1 \cdot 1 \cdot 1$ . כלומר  $\sigma \notin A_{10}$  כי  $A_{10}$  כוללת רק תמורות זוגיות, ולכן  $\sigma \notin G$ . אבל החזקה הטבעית הכי קטנה של  $\sigma$  שכן נמצאת ב- $G$  תהיה היוצר שלה לפי פתרון התרגיל (לפיו כל תת-חבורה של חבורה ציקלית היא ציקלית). הריבוע של כל תמורה הוא תמורה זוגית, ולכן  $\sigma^2 \in G$  היא החזקה הקטנה ביותר של, ונסיק  $G = \langle \sigma^2 \rangle$ .

2. הסדר של חבורה ציקלית שווה לסדר של היוצר שלה. בכל מקרה כדאי להציג את  $\sigma$  כמכפלת מחזורים זרים, וחישוב מפורט (שלא כתבנו כאן) יראה כי:

$$\sigma = (1\ 5\ 6\ 7)(2\ 8\ 9)(3\ 4\ 10)$$

כלומר מבנה המחזורים של  $\sigma$  הוא  $(4, 3, 3)$ , ולכן הסדר שלה הוא  $[4, 3, 3] = 12$ . לפי הטענה שסדר של תמורה הוא הכפולה המשותפת המזערית (lcm) של אורכי המחזורים. מפני ש- $G = \langle \sigma^2 \rangle$  לפי הסעיף הקודם, אז אפשר לחשב כי  $o(\sigma^2) = 6$ . לפי תרגיל לחישוב סדר של חזקה. כלומר  $|G| = 6$ . אפשרויות אחרות לחישוב הוא קודם למצוא את

$$\sigma^2 = ((1\ 5\ 6\ 7)(2\ 8\ 9)(3\ 4\ 10))^2 = (1\ 6)(5\ 7)(2\ 9\ 8)(3\ 10\ 4)$$

שהיא ממבנה מחזורים  $(3, 3, 2, 2)$  ולכן  $|G| = o(\sigma^2) = [3, 3, 2, 2] = 6$ . אם לא מצאנו יוצר מפורש עבור  $G$ , עדיין אפשר לחשב כמה איברים נמצאים ב- $G$ . נשים לב כי  $\text{sign}(\sigma) = -1$  וגם שהסימן כפלי. האיברים ב- $G$  הם מן הצורה  $\sigma^i$  כי  $G \subseteq \langle \sigma \rangle$  והם גם תמורות זוגיות כי  $G \subseteq A_{10}$ . לכן כדי לחשב את הסימן של  $\sigma^i$  לכל  $0 \leq i < 12$  מספיק לשים לב שהתשובה תלויה רק בזוגיות של  $i$ , שהרי

$$\text{sign}(\sigma^i) = \text{sign}(\sigma)^i = (-1)^i$$

ומפני שיש 6 מספרים זוגיים בקטע  $[0, 12)$ , אז ב- $G$  יש בדיוק 6 איברים.

**שאלה 3** (40 נק'). יהי  $n \in \mathbb{N}$ . נסמן ב- $G_n$  את קבוצת כל הפונקציות  $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$  שהן מן הצורה

$$\forall w \in \mathbb{R}^n : f(w) = Aw + v$$

כאשר  $A \in GL_n(\mathbb{R})$  היא מטריצה ו- $v \in \mathbb{R}^n$  הוא וקטור.

1. הוכיחו כי  $G_n$  היא חבורה ביחס לפעולת ההרכבה.

2. הוכיחו או הפריכו: האם החבורה  $G_1$  אבלית? האם החבורה  $G_2$  אבלית?

פתרון. להעשרה נספר שפונקציות מן הצורה בשאלה נקראות העתקות אפיניות. יש להן חשיבות בכל מיני תחומים של מתמטיקה, פיזיקה ומדעי המחשב. למשל בגרפיקה ממוחשבת הן אובייקט סטנדרטי, והמחשב שלכם השתמש בהן פעמים רבות.

1. נוכיח את ארבע האקסיומות של חבורה.

סגירות: תהיינה  $f, g \in G_n$ . כלומר קיימות מטריצות  $A, B \in GL_n(\mathbb{R})$  ווקטורים  $v, u \in \mathbb{R}^n$  כך שמתקיים

$$\forall w \in \mathbb{R}^n : f(w) = Aw + v$$

$$\forall w \in \mathbb{R}^n : g(w) = Bw + u$$

ואנו צריכים לבדוק כי  $f \circ g \in G_n$ . ברור שהרכבת פונקציות מ- $\mathbb{R}^n$  ל- $\mathbb{R}^n$  היא פונקציה מ- $\mathbb{R}^n$  ל- $\mathbb{R}^n$ , אבל יש להוכיח שהיא מן הצורה בשאלה. נבדוק לכל  $w \in \mathbb{R}^n$  כי

$$f \circ g(w) = f(g(w)) = f(Bw + u) = A(Bw + u) + v = ABw + (Au + v)$$

נשים לב כי  $AB \in GL_n(\mathbb{R})$  מפני שיש סגירות בחבורה  $GL_n(\mathbb{R})$  של כל המטריצות ההפיכות בגודל  $n \times n$  לגבי פעולת הכפל. בנוסף  $Au + v \in \mathbb{R}^n$  הוא וקטור קבוע לפי הגדרת כפל מטריצה וקטור וסכום וקטורים. כלומר  $f \circ g$  היא פונקציה מן הצורה בשאלה (במינוח מההעשרה נאמר כי היא העתקה אפינית) עם המטריצה  $AB$  והוקטור  $Au + v$ .

קיבוציות: ידוע לנו מהקורס מתמטיקה בדידה שהרכבת פונקציות היא קיבוצית (אסוציאטיבית). לכן לכל  $f, g, h \in G_n$  מתקיים כי

$$(f \circ g) \circ h = f \circ (g \circ h)$$

ואין צורך לנמק מעבר לכך מדוע הרכבת פונקציות היא קיבוצית. קיום איבר יחידה: מהתבוננות בהרכבה  $f \circ g$ , מה צריך לקרות כדי שנקבל  $f \circ g = f$ ? לכל הפחות צריך כי  $AB = A$ , ולכן בעזרת צמצום  $A$  נקבל כי  $B = I_n$ . בנוסף נרצה שיתקיים  $Au + v = v$ , ולכן  $Au = 0$  לכל  $A$ . זה בודאי יקרה עבור וקטור האפס  $u = 0$ . לכן נבחר את פונקציית הזהות

$$\text{id}(w) = I_n \cdot w + 0 = w$$

שהיא אכן מן הצורה בשאלה, כי  $I_n \in GL_n(\mathbb{R})$  וגם  $0 \in \mathbb{R}^n$ . כלומר  $\text{id} \in G_n$  וכבר ראינו שהרכבת העתקת הזהות מימין מקיימת  $f \circ \text{id} = f$ , ובדיקה ישירה תראה שגם  $\text{id} \circ f = f$  לכל  $f \in G_n$ , כי זה נכון לכל פונקציה מ- $\mathbb{R}^n$  ל- $\mathbb{R}^n$ . קיום הופכי: תהי פונקציה  $f \in G_n$  כלשהי המוגדרת בעזרת המטריצה  $A$  והוקטור  $v$ . כעת צריך למצוא  $g \in G_n$  עבורה יתקיים

$$f \circ g = g \circ f = \text{id}$$

כי  $\text{id}$  הוא איבר היחידה. כל פונקציה ב- $G_n$  נקבעת לחלוטין לפי מטריצה ווקטור קבועים. לכן צריך למצוא את המטריצה והוקטור עבור  $g$ , ונסמן אותם כמו קודם  $B$  ו- $u$ . בהכרח  $AB = I_n$ , ולכן  $B = A^{-1}$ . בנוסף  $Au + v = 0$ , ומהעברת אגפים  $-v$ ,  $Au = -v$ , ולכן  $u = -A^{-1}v$ . כעת נבדוק לכל  $w \in \mathbb{R}^n$  האם אכן זה ההופכי של  $f$  משני הצדדים:

$$\begin{aligned} f \circ g(w) &= f(A^{-1}w - A^{-1}v) = A(A^{-1}w - A^{-1}v) + v \\ &= AA^{-1}w - AA^{-1}v + v = w - v + v = w = \text{id}(w) \\ g \circ f(w) &= g(Aw + v) = A^{-1}(Aw + v) - A^{-1}v = \\ &= A^{-1}Aw + A^{-1}v - A^{-1}v = w = \text{id}(w) \end{aligned}$$

ולכן  $g = f^{-1}$  כפי שרצינו.  
 בסך הכל הוכחנו ש- $G_n$  היא חבורה לגבי פעולת ההרכבה.  
 אם רוצים להשתמש בקריטריון המקוצר לתת-חבורה כדי לפתור את הסעיף הזה,  
 חייבים למצוא חבורה ש- $G_n$  היא תת-חבורה שלה. אפשרות סבירה כזו היא  
 החבורה  $S_{\mathbb{R}^n}$  של כל הפונקציות החח"ע ועל מ- $\mathbb{R}^n$  לעצמה, עם פעולת ההרכבה.  
 אין הבדל אמיתי באורך ההוכחה במקרה זה.

2. הפרכה בשני המקרים. בחבורה  $G_1$  האיברים הם פונקציות  $\mathbb{R} \rightarrow \mathbb{R}$ , ומפני  
 ש- $GL_1(\mathbb{R})$  כוללת מטריצות הפיכות בגודל  $1 \times 1$ , אפשר לחשוב עליהן כאיברים  
 של  $\mathbb{R}^*$ . כלומר  $f$  היא מן הצורה

$$f(w) = ax + b$$

כאשר  $a, b \in \mathbb{R}$  וגם  $a \neq 0$ . במילים אחרות  $G_1$  כוללת את כל הפונקציות  
 הלינאריות שאינן קבועות. קל למצוא פונקציות כאלו שלא מתחלפות. למשל  
 $f(w) = w + 1$  לא מתחלפת עם  $g(w) = 2w$ , ויש לבדוק זאת במפורש

$$\begin{aligned} f \circ g(w) &= f(2w) = 2w + 1 \\ g \circ f(w) &= g(w + 1) = 2w + 2 \end{aligned}$$

לכל  $w \in \mathbb{R}$  אז בפרט  $f \circ g(0) = 1 \neq 2 = g \circ f(0)$ . אפשר למצוא דוגמאות  
 כאלו גם ב- $G_2$ . למשל נבחר את המטריצות והוקטורים

$$\begin{aligned} A &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & v &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ B &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} & u &= \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{aligned}$$

וקל לבדוק כי  $A, B \in GL_n(\mathbb{R})$  מפני שהדטרמיננטה שלהן היא מכפלת איברי  
 האלכסון. זו למעשה הכללה של הדוגמה עבור  $G_1$ , ואכן אם נגדיר  $f(w) = Aw + v$   
 וכן  $g(w) = Bw + u$ , אז נקבל

$$\begin{aligned} f \circ g(w) &= ABw + (Au + v) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} w + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ g \circ f(w) &= BAw + (Bv + u) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} w + \begin{pmatrix} 2 \\ 0 \end{pmatrix} \end{aligned}$$

שבוודאי הן פונקציות שונות, אפילו לכל  $w \in \mathbb{R}^2$ , וזו דוגמה שמפריכה כי  $G_2$   
 אבלית.