

## פתרון בוחן א' 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, לרוב בעזרת משפטים בעברית. אם משתמשים במשפט או טענה שלמדנו בכיתה, צריך לצטט אותם במלואם ולא להסתפק בנימוק "לפי משפט מההרצאה" או "לפי טענה מהתרגול".

**שאלה 1.** נתבונן בחבורה  $G = GL_2(\mathbb{Z}_2)$ .

1. (24 נק') מצאו את  $|G|$ .

2. (24 נק') בחרו איבר אחד  $g \in G$  שאינו איבר היחידה. הציגו את התמורה  $\Phi(g) \in S_{|G|}$  כמכפלת מחזורים זרים, כאשר  $\Phi$  הוא שיכון קיילי.

פתרון. מתברר שהחבורה  $GL_2(\mathbb{Z}_2)$  איזומורפית ל- $S_3$ , ולכן זו שאלה איזומורפית לתרגיל שעשינו בתרגול.

1. החבורה  $GL_2(\mathbb{Z}_2)$  מכילה את קבוצת כל המטריצות ההפיכות מעל השדה  $\mathbb{Z}_2$ . יש  $2^{2 \cdot 2} = 16$  מטריצות בגודל  $2 \times 2$  מעל  $\mathbb{Z}_2$ , ובמקום לבדוק את הדטרמיננטה של כל אחת מהן, אפשר להזכר במעט אלגברה לינארית. אם במטריצה יש שורת אפסים, עמודת אפסים, שתי שורות זהות או שתי עמודות זהות, אז היא לא הפיכה. זה מייד פוסל 10 מתוך המטריצות לעיל. שאר המטריצות הן משולשיות או אנטי-משולשיות, ולכן קל לחשב את הדטרמיננטה שלהן כמכפלת האיברים באלכסון הראשי או באלכסון המשני, ובשדה  $\mathbb{Z}_2$  החישוב תמיד יוצא  $1 \cdot 1 = 1 \neq 0$ .

בסעיף הבא נפרט מי הן המטריצות בחבורה. בסך הכל  $|G| = 6$ . ישנה דרך אחרת להגיע לחישוב הזה עם עוד טיפה אלגברה לינארית. יהי  $F$  שדה סופי עם  $q$  איברים. בשאלה  $q = 2$ . בחבורה  $GL_2(F)$  האיברים הם מטריצות שהשורות בהן לא תלויות לינארית (ובפרט אינן אפס). לכן לשורה הראשונה יש  $q^2 - 1$  אפשרויות, כי יש  $q^2$  וקטורים ב- $F^2$  ומוציאים את וקטור האפס. לשורה השנייה יש לנו  $q^2 - q$  אפשרויות, כי שוב יש  $q^2$  וקטורים שמהם מפחיתים את  $q$  הוקטורים שתלויים בשורה הראשונה. בסך הכל יש  $(q^2 - 1)(q^2 - q)$  איברים בחבורה. אצלנו החישוב יוצא  $3 \cdot 2 = 6$ .

2. נתאים, כמו שעשינו בכיתה, לכל אחת משש המטריצות בחבורה  $G$  מספר שייצג אותן ב- $S_{|G|}$ :

$$\begin{array}{lll} 1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 2 \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} & 3 \leftrightarrow \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ 4 \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 5 \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & 6 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \end{array}$$

איבר היחידה הוא מטריצת הזהות (המסומנת 1 לעיל), לכן נבחר את המטריצה המסומנת 2 בתור האיבר  $g$ . שיכון קיילי  $\Phi$  שולח את  $g$  לפונקציה  $l_g$  של כפל בשמאל ב- $g$ . כלומר  $\Phi(g) = l_g$  כאשר  $l_g(h) = gh$  לכל  $h \in G$ . נכפול את כל המטריצות משמאל ב- $g$ :

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} &\implies & \Phi(g)(1) = 2 \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} &\implies & \Phi(g)(2) = 3 \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\implies & \Phi(g)(3) = 1 \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} &\implies & \Phi(g)(4) = 6 \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} &\implies & \Phi(g)(5) = 4 \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &\implies & \Phi(g)(6) = 5 \end{aligned}$$

כך שהתמורה המתקבלת היא  $\Phi(g) = (123)(465)$ . זאת יוצאת בדיוק אותה התמורה מהדוגמה למשפט קיילי בתרגול.

אפשר לבדוק את התשובה, לפי זה שהאיבר  $g$  הוא מסדר 3, ולכן הוא תמונתו תחת שיכון קיילי היא תמורה שהיא מכפלה של  $2 = \frac{6}{3}$  מחזורים זרים מאורך 3. האיבר המסומן 3 הוא ההופכי של  $g$ , אז גם את תמונתו קל למצוא. האיברים המסומנים 4, 5, 6 הם מסדר 2, ולכן תמונתם תהיה תמורה שהיא מכפלה של  $3 = \frac{6}{2}$  חילופים זרים.

**שאלה 2.** תהי  $G$  חבורה מסדר  $125 = 5^3$ .

1. (16 נק') הוכיחו או הפריכו: קיים ב- $G$  איבר מסדר 5.

2. (16 נק') הוכיחו או הפריכו: קיים ב- $G$  איבר מסדר 25.

פתרון. התשובה בכל סעיף צריכה להתחיל במילה "הוכחה" או במילה "הפרכה", או ניסוח דומה שמסביר לקוראים מה התשובה תכיל.

1. הוכחה. תהי  $G$  חבורה מסדר 125. כמסקנה ממשפט לגראנז', הסדר של כל איבר מחלק את סדר החבורה. לכן הסדרים האפשריים בחבורה הם 1, 5, 25, 125. יש רק איבר אחד מסדר 1 והוא איבר היחידה. אם קיים איבר מסדר 5, סיימנו.

אם קיים איבר  $a \in G$  מסדר 25, אזי  $a^{25} = e$ . נעזר בכך ש- $25 = 5 \cdot 5$  ונתבונן באיבר  $b = a^5$ . נוכיח כי  $o(b) = 5$  באופן ישיר:

$$b^1 = a^5 \neq e$$

$$b^2 = a^{10} \neq e$$

$$b^3 = a^{15} \neq e$$

$$b^4 = a^{20} \neq e$$

$$b^5 = a^{25} = e$$

כאשר הסתמכנו על כך ש- $a^i \neq e$  לכל  $1 \leq i < 25$ , לפי הגדרת סדר של איבר. אם קיים איבר  $c \in G$  מסדר 125, אפשר להוכיח באופן דומה לחישוב לעיל כי  $c^5$  הוא איבר מסדר 25, מה שגורר ש- $c^{25} = (c^5)^5$  הוא איבר מסדר 5 לפי מה שהוכחנו עבור  $b$ .

2. הפרכה. נתבונן בחבורה  $G = \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$  שהיא מכפלה ישרה של שלושה עותקים של  $\mathbb{Z}_5$ . באופן דומה להוכחה לפיה החבורה  $\mathbb{Z}_n \times \mathbb{Z}_n$  לא ציקלית, נראה שהסדר של כל איבר בחבורה  $G$  אינו עולה על 5. יהי  $(x, y, z) \in G$  איבר כלשהו. אז

$$(x, y, z)^5 = (x, y, z) + \dots + (x, y, z) = (5x, 5y, 5z) \stackrel{*}{=} (0, 0, 0) = e_G$$

כאשר ההצדקה למעבר  $*$  היא שהפעולה בחבורה הזו היא חיבור מודולו 5 בכל רכיב. לכן הסדר של כל איבר קטן או שווה (למעשה מחלק את) 5, ובפרט אין בה איבר מסדר 25.

**שאלה 3 (40 נק').** נתונות חמש החבורות הבאות:

$$\langle a \rangle, \quad A_4, \quad \mathbb{Z}_{12}, \quad \mathbb{Z}_2 \times \mathbb{Z}_6, \quad S_{12}$$

כאשר  $a = 3 \in \mathbb{Z}_{36}$ . קבעו והוכיחו אילו מבין החבורות לעיל איזומורפיות ואילו לא. פתרון. יש  $\binom{5}{2} = 10$  זוגות של חבורות שצריך לבדוק. נראה שאפשר לקצר את הבדיקה, כי יש הרבה זוגות של חבורות לא איזומורפיות שאפשר להוכיח בבת-אחת. המספר הכי חשוב עבור חבורה סופית הוא הסדר שלה. החבורה  $S_{12}$  היא מסדר 12!, ואילו כל שאר החבורות האחרות בשאלה הן מסדר 12. ניתן לחשב זאת ישירות עבור  $\mathbb{Z}_{12}$ . עבור  $\langle a \rangle$  נשים לב שהסדר שלה הוא שווה לסדר של היוצר שלה  $o(a) = 12$ . בחבורה  $\mathbb{Z}_{36}$  עבור  $A_4$  ראינו את הנוסחה  $|A_4| = 4!/2$  וכן  $|\mathbb{Z}_2 \times \mathbb{Z}_6| = 2 \cdot 6$ . המסקנה המיידית היא ש- $S_{12}$  לא איזומורפית לאף אחת מן החבורות האחרות משיקולי גודל, שהרי איזומורפיזם הוא (בפרט) פונקציה חח"ע ועל, ולכן שומר על סדר החבורות. מבין ארבע החבורות שנותרו החבורה היחידה שאינה אבלית היא  $A_4$  (למשל כי (123) לא מתחלף עם (234)), ואילו שאר החבורות  $\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6, \langle a \rangle$  הן אבליות. לכן

$A_4$  לא איזומורפית לאף אחת משאר החבורות, מפני שאיזומורפיזם שומר על אבליות של חבורה.

החבורה  $\langle a \rangle$  היא ציקלית ממש לפי הגדרתה, וראינו בכיתה כי  $\mathbb{Z}_{12}$  היא ציקלית (למשל היא נוצרת על ידי 1). כל זוג חבורות ציקליות מאותו הסדר הן איזומורפיות (גם את זה הזכרנו בכיתה), ולכן  $\langle a \rangle$  איזומורפית ל- $\mathbb{Z}_{12}$ . החבורה  $\mathbb{Z}_2 \times \mathbb{Z}_6$  לא ציקלית, כי היא מסדר 12 ואין בה איבר מסדר 12, ולכן לא איזומורפית לאף חבורה אחרת מהרשימה. אפשר להוכיח זאת על ידי בדיקה שהסדר המרבי בחבורה הזו הוא 6: יהי  $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_6$  ונחשב בשיטה דומה לסעיף השני בשאלה הקודמת כי

$$(x, y)^6 = (6x, 6y) = (0, 0)$$

ולכן הסדר של  $(x, y)$  מחלק את 6, ובפרט קטן ממש מ-12. לסיכום, רק החבורות  $\langle a \rangle \cong \mathbb{Z}_{12}$  איזומורפיות זו לזו, וכל שאר החבורות לא איזומורפיות זו לזו ולא לזוג החבורות הזה.