

## פתרון בוחן במבוא לתורת החבורות 88-211 סמסטר א' תשפ"ד

**מרצה:** ד"ר יונתן בק

**מתרגל:** תומר באואר

**הוראות:**

- יש לענות על כל ארבע השאלות פתרון מלא ומנומק.
- כתבו את תשובתיכם על גבי טופס הבחינה. ניתן להשתמש בשני צידי הדף. מחברת הטיוטה לא תיבדק.
- משך הבוחן: 90 דקות.
- סך הנקודות עולה על 100, אך הציון המקסימלי בבוחן הינו 100.
- חומר עזר: מחשבון פשוט בלבד (וגם אותו לא חייבים).

בהצלחה!

**שאלה 1** (25 נק'). מצאו את האינדקס  $[\mathbb{Z}_{211} \times U_{15} : \langle 8 \rangle \times \langle 8 \rangle]$ .  
עובדות שימושיות: המספר 211 הוא ראשוני, ומשפט לגראנז' הוא נכון.

פתרון. לפי משפט לגראנז' נסיק כי

$$[\mathbb{Z}_{211} \times U_{15} : \langle 8 \rangle \times \langle 8 \rangle] = \frac{|\mathbb{Z}_{211} \times U_{15}|}{|\langle 8 \rangle \times \langle 8 \rangle|}$$

ולכן מספיק לחשב את הסדר של החבורה, והסדר של תת-החבורה שבשאלה. כדאי להזכר כי הפעולה ב- $\mathbb{Z}_{211}$  היא חיבור מודולו 211, ואילו ב- $U_{15}$  זהו כפל מודולו 15. מכאן, שנצפה שהאיבר 8 בכל אחת מן החבורות יתנהג שונה.

ידוע לנו כי  $|\mathbb{Z}_{211}| = 211$ , ובקצת יותר עבודה נחשב  $|U_{15}| = 8$  כי המספרים הטבעיים שקטנים וזרים ל-15 הם  $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ . לכן  $|\mathbb{Z}_{211} \times U_{15}| = 211 \cdot 8$ . כמסקנה ממשפט לגראנז', סדר של איבר בחבורה סופית מחלק את הסדר של החבורה. לכן הסדר של  $8 \in \mathbb{Z}_{211}$  מחלק את 211. קל לבדוק כי  $o(8) \neq 1$ , שהרי 8 אינו איבר היחידה, ובעזרת העובדה השימושית נסיק כי  $o(8) = 211$ . בחבורה  $U_{15}$  איבר היחידה הוא 1, ולכן  $o(8) \neq 1$  גם כאן. כדי לחשב את הסדר של  $8 \in U_{15}$  נחשב חזקות שלו: תחילה  $8^2 \equiv 64 \equiv 4 \pmod{15}$  ואחר כך נחשב

$$8^4 \equiv (8^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{15}$$

ולכן  $o(8) = 4$ . שימו לב שניתן היה לחשב גם את  $8^3$ , אך מפני ש-3 לא מחלק את  $|U_{15}|$ , הסדר של האיבר  $8 \in U_{15}$  לא יכול להיות 3. בסך הכל  $|\langle 8 \rangle \times \langle 8 \rangle| = 211 \cdot 4$ . לכן נקבל

$$[\mathbb{Z}_{211} \times U_{15} : \langle 8 \rangle \times \langle 8 \rangle] = \frac{211 \cdot 8}{211 \cdot 4} = 2$$

אפילו מבלי לחשב מכפלה של "מספרים גדולים".

**שאלה 2** (30 נק'). הוכיחו או הפריכו: לכל  $n \in \mathbb{N}$  ולכל  $\sigma \in S_n$  מתקיים  $o(\sigma) < 4n$ .

פתרון. הפרכה. למי שלא יודע, הסדר של מחזור ב- $S_n$  יכול להיות לכל היותר  $n$ . מכאן, שכדי למצוא דוגמת נגד לטענה בשאלה חייבים לבחור תמורה שהיא הרכבה של לפחות שני מחזורים זרים.

ניתן לבחור  $n = 100$  וכל תמורה  $\sigma \in S_{100}$  שיש לה מבנה מחזורים (51, 49) כמו

$$(1, 2, \dots, 51)(52, 51, \dots, 100)$$

תפריך את הטענה. הרי הסדר שלה הוא

$$\text{lcm}(51, 49) = 51 \cdot 49 = (50 + 1)(50 - 1) = 50^2 - 1^2 = 2499$$

שהוא כמובן יותר גדול מ- $4n = 400$ .

יש עוד המון דוגמאות אחרות. אפשר לבחור תמורה ב- $S_{100}$  ממבנה מחזורים  $(80, 7)$ , שהסדר שלה הוא  $\text{lcm}(80, 7) = 560$ , שעדיין גדול מ-400. המספר  $n$  הקטן ביותר עבורו ניתן למצוא דוגמת נגד הוא  $n = 12$ , ולבחור תמורה  $\sigma \in S_{12}$  ממבנה מחזורים  $(5, 4, 3)$ . שהסדר שלה הוא  $\text{lcm}(5, 4, 3) = 60$ , שגדול מ- $4n = 48$ .

אגב, מה יהיה ה- $n$  המינימלי כדי להפריך את הטענה עבור  $A_n$ ?

**שאלה 3.** נאמר כי פונקציה  $f: \mathbb{R} \rightarrow \mathbb{R}$  היא לינארית למחצה אם קיימים  $a \in \mathbb{R}^*$  ו- $b \in \mathbb{R}$  עבורם

$$\forall x \in \mathbb{R}: f(x) = ax + b$$

נסמן ב- $G$  את אוסף כל הפונקציות הלינאריות למחצה.

א. (15 נק') הוכיחו כי  $G$  היא חבורה ביחס לפעולת ההרכבה.

ב. (10 נק') הוכיחו או הפריכו: האם החבורה  $G$  אבלית? האם החבורה  $G$  ציקלית?

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

א. ניתן לשים לב כי כל פונקציה לינארית למחצה כפי שהוגדר למעלה היא תמורה על  $\mathbb{R}$  (כי  $a \in \mathbb{R}^*$ ), או במילים אחרות שייכת ל- $S_{\mathbb{R}}$ . זה יותר אלגנטי להוכיח כי  $G \leq S_{\mathbb{R}}$ , אבל נוכיח את ארבע האקסיומות של חבורה ישירות.  
סגירות: תהינה פונקציות לינאריות למחצה  $f, f' \in G$ . כלומר קיימים  $a, a' \in \mathbb{R}^*$  ו- $b, b' \in \mathbb{R}$  כד שמתקיים

$$\forall x \in \mathbb{R}: f(x) = ax + b$$

$$\forall x \in \mathbb{R}: f'(x) = a'x + b'$$

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

$$f \circ f'(x) = f(f'(x)) = f(a'x + b') = a(a'x + b') + b = aa'x + (ab' + b)$$

נשים לב כי  $aa' \in \mathbb{R}^*$  מפני שיש סגירות בחבורה הכפלית  $\mathbb{R}^*$ , ובנוסף  $ab' + b \in \mathbb{R}$  הוא מספר ממשי קבוע. כלומר  $f \circ f'$  היא פונקציה לינארית למחצה עם הקבועים  $aa'$  ו- $ab' + b$ .

קיבוציות: ידוע לנו מהקורס מתמטיקה בדידה שהרכבת פונקציות היא קיבוצית (אסוציאטיבית). לכן לכל  $f, g, h \in G$  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  $f \circ f'$ , מה צריך לקרות כדי שנקבל  $f \circ f' = f$ ? לכל הפחות עבור הצבת  $x = 0$  נרצה שיתקיים  $ab' + b = b$ , ולכן  $ab' = 0$ , ונסיק  $b' = 0$  כי  $a \neq 0$ . כעת, עבור הצבת  $x = 1$  צריך שיתקיים  $aa' = a$ , ולכן בעזרת צמצום  $a$  נקבל כי  $a' = 1$ . לכן נבחר את פונקציית הזהות

$$\text{id}(x) = 1 \cdot x + 0 = x$$

שהיא אכן פונקציה לינארית למחצה, כי  $1 \in \mathbb{R}^*$  וגם  $0 \in \mathbb{R}$ . כלומר  $\text{id} \in G$ , וכבר ראינו שהרכבת העתקת הזהות מימין מקיימת  $f \circ \text{id} = f$ , ובדיקה ישירה תראה שגם  $\text{id} \circ f = f$  לכל  $f \in G$ , כי זה נכון לכל פונקציה מ- $\mathbb{R}$  ל- $\mathbb{R}$ .  
קיום הופכי: תהי פונקציה  $f \in G$  כלשהי המוגדרת בעזרת  $a \in \mathbb{R}^*$  ו- $b \in \mathbb{R}$ . כעת צריך למצוא  $g \in G$  עבורה יתקיים

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

שהרי  $\text{id}$  היא איבר היחידה. כל פונקציה ב- $G$  נקבעת לחלוטין לפי זוג מספרים ממשיים. נניח  $g(x) = a'x + b'$  כמו קודם. בהכרח  $aa' = 1$ , ולכן  $a' = a^{-1}$ . בנוסף  $ab' + b = 0$ , ומהעברת אגפים  $ab' = -b$ , ולכן  $b' = -a^{-1}b$ . כעת נבדוק לכל  $x \in \mathbb{R}$  האם אכן זה ההופכי של  $f$  משני הצדדים:

$$\begin{aligned} f \circ g(x) &= f(a^{-1}x - a^{-1}b) = a(a^{-1}x - a^{-1}b) + b \\ &= aa^{-1}x - aa^{-1}b + b = x - b + b = x = \text{id}(x) \\ g \circ f(x) &= g(ax + b) = a^{-1}(ax + b) - a^{-1}b = \\ &= a^{-1}ax + a^{-1}b - a^{-1}b = x = \text{id}(x) \end{aligned}$$

ולכן  $g = f^{-1}$ , כפי שרצינו. שימו לב שהוכחנו שההופכי גם הוא פונקציה לינארית למחצה, כי זה לא מספיק להראות ש- $f$  היא "סתם" פונקציה הפיכה. בסך הכל הוכחנו ש- $G$  היא חבורה לגבי פעולת ההרכבה.

ב. הפרכה בשני המקרים. קל למצוא פונקציות לינאריות למחצה שלא מתחלפות. למשל  $f(x) = x + 1$  לא מתחלפת עם  $g(x) = 2x$ , ויש לבדוק זאת במפורש

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

לכל  $x \in \mathbb{R}$ . אז בפרט  $f \circ g(0) = 1 \neq 2 = g \circ f(0)$  לכן  $G$  לא אבלית, ובפרט לא ציקלית.

**שאלה 4.** (25 נק') מצאו שלוש חבורות לא איזומורפיות מסדר 24 והוכיחו שאינן איזומורפיות זו לזו.

בונוס (5 נק'): מצאו חבורה נוספת מסדר 24 והוכיחו שאינה איזומורפית לאלו שמצאתם.

פתרון. ככל הנראה הכי קל זה לבחור את החבורות  $G_1 = \mathbb{Z}_{24}$ ,  $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_{12}$  ואת  $G_3 = S_4$ . כולן מסדר 24 (כי  $|\mathbb{Z}_n| = n$  וכן  $|S_n| = n!$ ), ונותר להראות שכל זוג מהן לא איזומורפיות. החבורה  $G_1$  היא ציקלית, ואילו  $G_2$  אבלית שאינה ציקלית, כי היא מכפלה ישרה של שתי חבורות אבליות והסדר של כל איבר בה הוא לכל היותר 12, ולכן הן לא איזומורפיות. החבורה  $G_3$  אינה אבלית, ולכן לא איזומורפית לשתי החבורות  $G_1$  ו- $G_2$  שהן אבליות.

מפני שאיזומורפיזם שומר על סדר של איברים, אז ניתן להוכיח זאת גם בעזרת סדרים של איברים. למשל הסדר המרבי של איבר ב- $G_1$  הוא 24, ב- $G_2$  הוא 12 וב- $G_3$  הוא 4, ולכן החבורות האלו לא איזומורפיות זו לזו.

עבור הבונוס, הנה כמה חבורות נוספות מסדר 24: יש את  $G_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$  שהיא אבלית, אבל הסדר המרבי של איבר הוא 6, ולכן לא איזומורפית לאחרות. יש את  $G_5 = S_3 \times \mathbb{Z}_4$ , שהיא לא אבלית ולכן לא איזומורפית ל- $G_1$ ,  $G_2$  ו- $G_4$ . הסדר המרבי של איבר ב- $G_5$  הוא 12 (כמו האיבר  $(1, (123))$ ) וראינו איך מחשבים סדר של איבר במכפלה ישרה, ולכן היא לא איזומורפית ל- $G_3$ . יש את  $G_6 = A_4 \times \mathbb{Z}_2$  שגם היא לא אבלית, ולכן לא איזומורפית ל- $G_1$ ,  $G_2$  ו- $G_4$ . הסדר המרבי ב- $G_6$  הוא 6, ולכן היא לא איזומורפית ל- $G_3$  ול- $G_5$ . דרך אחרת תעזר בחישוב גודל המרכז של כל אחת מן החבורות, ולפצל רק למקרים שבהם המרכזים איזומורפיים.

אגב, ישנן 15 חבורות מסדר 24 עד כדי איזומורפיזם (קישור לרשימה).