

פתרון תרגיל בית 3 במבנים אלגבריים 89214 סמסטר א' תשפ"ג

שאלה 1 (חימום). מצאו את כל האיברים מסדר סופי בחבורות הבאות: \mathbb{Z} , \mathbb{Q}^* , \mathbb{R}^* . הפעולות בחבורות האלו מופיעות בנספח "חבורות מוכרות" בחוברת מערכי התרגול. פתרון. ב- \mathbb{Z} האיבר היחיד מסדר סופי הוא 0. אכן, $a \in \mathbb{Z}$ הוא מסדר סופי n אם ורק אם $na = 0$, אם ורק אם $a = 0$. ב- \mathbb{Q}^* וב- \mathbb{R}^* הפתרון דומה, ולכן נפתור את שני המקרים ביחד. a הוא מסדר סופי n אם ורק אם $a^n = 1$. אבל השורשים הממשיים היחידים של 1 הם ± 1 (אפשר למשל לבדוק קודם שהערך המוחלט של a חייב להיות 1), ולכן אלו האיברים היחידים מסדר סופי ב- \mathbb{Q}^* וב- \mathbb{R}^* .

שאלה 2. כתבו את לוח הכפל של החבורה $\mathbb{Z}_2 \times \mathbb{Z}_3$. הוכיחו שהיא ציקלית, ומצאו את כל היוצרים שלה.

+	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 1)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)
(0, 2)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 1)	(1, 1)	(1, 2)	(1, 0)	(0, 1)	(0, 2)	(0, 0)
(1, 2)	(1, 2)	(1, 0)	(1, 1)	(0, 2)	(0, 0)	(0, 1)

$\mathbb{Z}_2 \times \mathbb{Z}_3$ של הכפל

פתרון. על ידי חישוב ישיר בדקו כי $\langle (1, 1) \rangle = \langle (1, 2) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$.

שאלה 3. בתרגיל הבית הקודם הוכחתם שקבוצת המטריצות

$$H = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_2 \right\}$$

היא תת-חבורה של $GL_3(\mathbb{Z}_2)$. מצאו את הסדר של H ואת הסדר של איברי H . האם H ציקלית?

פתרון. עבור כל אחד מ- a, b, c יש לנו שתי אפשרויות בלתי תלויות לבחירה. לכן ישנם $2^3 = 8$

איברים בחבורה H . כלומר $|H| = 8$. היא לא ציקלית, כי היא לא אבלית. למשל

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

הסדר של האיברים הוא 1 עבור איבר היחידה (מטריצת הזהות), שני האיברים שבהם $a = b = 1$ הם מסדר 4 ושאר האיברים מסדר 2. מפני שאין איבר מסדר 8, זו עוד דרך להוכיח כי H אינה ציקלית.

שאלה 4. תהי קבוצה $S = \{a, b, c, d\}$ עם ארבעה איברים. השלימו את לוח הכפל הבא כך שתתקבל חבורה:

*	a	b	c	d
a	a	b	c	d
b		a		
c			a	
d				a

האם החבורה המתקבלת אבלית? האם היא ציקלית?

פתרון. נשים לב כי $a^2 = a$ גורר $a = e$, כלומר a איבר היחידה:

*	a	b	c	d
a	a	b	c	d
b	b	a		
c	c		a	
d	d			a

אז צריך להסביר שעבור bc לא ייתכן שנמלא בטבלה a , כי יש הופכי יחיד ל- b (שהוא b בעצמו). לא יתכן שנמלא b כי אז $bc = b$ גורר $b = a$ שהרי הם שונים, באופן דומה נפסול למלא c וכן הלאה. לבסוף נקבל

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

לפי בדיקה ישירה (שיקוף לגבי האלכסון) רואים שהחבורה אבלית. היא לא ציקלית, כי הסדר של כל איבר הוא לכל היותר 2, כי מתקיים $x^2 = a$ לכל $x \in S$, ואילו החבורה מסדר 4.

שאלה 5. תהי G חבורה אבלית. נסמן ב- T את אוסף האיברים מסדר סופי ב- G . הוכיחו כי $T \leq G$

פתרון. נסמן $e = e_G$. נשתמש בקריטריון המקוצר:

$$o(e) = 1 < \infty \text{ זה נכון כי } e \in T \text{ א.}$$

ב. נניח $a, b \in T$. צריך להוכיח $ab^{-1} \in T$. נסמן $m = o(a)$, $n = o(b)$. מכיוון ש- G חבורה אבלית מתקיים:

$$(ab^{-1})^{mn} = a^{mn}b^{-mn} = (a^m)^n (b^n)^{-m} = e^n e^{-m} = e$$

מכאן קיבלנו ש- $mn \leq o(ab^{-1})$ ולכן $ab^{-1} \in T$.

שאלה 6. תהי G חבורה ותהי $H \subseteq G$ תת-חבורה לא ריקה.

א. הוכיחו שאם G חבורה סופית, אז כדי להוכיח ש- H היא תת-חבורה של G מספיק לבדוק סגירות לפעולה.

ב. הפריכו את הסעיף הקודם כאשר G אינסופית.

פתרון.

א. נסמן $e = e_G$. נראה שמתקיים הקריטריון המקוצר עבור H :

(א) $H \neq \emptyset$. זה נתון בשאלה.

(ב) נניח $a, b \in H$. צריך להוכיח $ab^{-1} \in H$. ראשית נראה כי $b^{-1} \in H$:

$$b^{-1} = e \cdot b^{-1} = \left(b^{o(b)}\right)^2 b^{-1} = b^{2o(b)-1} \in H$$

כאשר השתמשנו בעובדה שהמספר $2o(b) - 1$ הוא שלם חיובי. כלומר קיבלנו $a, b^{-1} \in H$ ולכן מסגירות לפעולה $ab^{-1} \in H$.

ב. נבחר $G = (\mathbb{Z}, +)$ ו- $H = (\mathbb{N}, +)$. אכן G אינסופית ו- $H \neq \emptyset$ סגורה לחיבור. תת-הקבוצה H אינה חבורה מכיוון שאין לה איבר יחידה.

שאלה 7. תהי $G = \{a_1, a_2, \dots, a_n\}$ חבורה אבלית סופית. יהי האיבר $b = a_1 a_2 \dots a_n$.

א. הוכיחו $b^2 = e$.

ב. הוכיחו שאם אין ב- G איבר מסדר 2, אז $b = e$.

ג. בשפת התכנות C הניחו שהיצוג של הטיפוס `unsigned char` הוא של 8 סיביות (כלומר משתנה מטיפוס זה הוא בין 0 לבין 255 כולל). הסבירו מה תהיה התוצאה של קטע הקוד הבא בעזרת הסעיפים הקודמים:

```
1 unsigned char b=0;
2 unsigned int i=0;
3 for (i=0; i <= 255; i++) {
4     b += i;
5 }
6 printf("%d\n", b);
```

פתרון.

א. נגדיר פונקציה $i: G \rightarrow G$ לפי $i(g) = g^{-1}$ לכל $g \in G$. הפונקציה i חח"ע ועל. אז

$$b^2 = \left(\prod_{i=1}^n g\right) \left(\prod_{i=1}^n i(g)\right) = \prod_{i=1}^n [g \cdot i(g)] = \prod_{i=1}^n e = e$$

כאשר בשיויון האמצעי נעזרו באבליות של G .

ב. נזכר כי איבר $e \neq a \in G$ הוא מסדר 2 אם ורק אם $a^2 = e$, כלומר אם ורק אם $a^{-1} = a$. אם אין ב- G איבר מסדר 2, אז לכל $a \in G$ שאינו e האיברים a ו- a^{-1} הם שונים ומופיעים במכפלה $a_1 a_2 \dots a_n$. שוב, כיוון ש- G אבלית, אפשר לשים אותם אחד ליד השני, ולצמצם אותם. כך נישאר רק עם איבר היחידה, ונקבל $b = e$. נניח שב- G אין איבר מסדר 2. בסעיף הקודם ראינו כי $b^2 = e$, לכן $o(b) \leq 2$. מכיוון ש- $o(b) \neq 2$, בהכרח $o(b) = 1$ ולכן $b = e$.

ג. כיוון שהטיפוס של unsigned char יכול להכיל מספרים מהתחום $0, 1, \dots, 255$, נשים לב שהחיבור שלהם מתנהג בדיוק כמו בחבורה \mathbb{Z}_{256} . למשל, $1 + 255 = 0$, או בייצוג עם סיביות:

$$00000001 + 11111111 = 00000000$$

אז בעצם האיבר b שהוגדר בתוכנית הוא סכום כל האיברים ב- \mathbb{Z}_{256} . לכן, הוא בדיוק האיבר b שהוגדר בשאלה עבור $G = \mathbb{Z}_{256}$ (כי אצלנו הפעולה היא חיבור במקום כפל). כמו בהסבר של הסעיף הקודם, כל איבר שאינו מסדר 2 יצטמצם עם ההופכי שלו. לכן, יישארו רק האיברים מסדר 2. קל לוודא שהאיבר היחיד מסדר 2 ב- \mathbb{Z}_{256} הוא 128, ולכן זו התוצאה של החיבור.

שאלה 8 (תכנות). נתבונן בחבורה $G = SL_2(\mathbb{Z}_p)$ עבור p ראשוני אי זוגי.

- כתבו פונקציה המקבלת את הראשוני p ומחזירה את הסדר המקסימלי של איבר ב- G .
- הדפיסו את הערכים הראשוניים של הפונקציה שכתבתם. האם תוכלו לזהות חוקיות בסדר המקסימלי?
- (אתגר) מצאו והוכיחו תיאור עבור איבר מסדר מקסימלי (יש יותר מאיבר אחד כזה). נסו להוכיח שהאיבר שמצאתם הוא אכן מהסדר הנכון, אך אין צורך להוכיח שהסדר שלו מקסימלי ב- G . (רמז: כדאי להיזכר באלגברה לינארית 2. הסתכלו על המטריצות מהסדר המקסימלי ולמצוא בהן חוקיות.)