פתרון תרגיל בית 3 במבנים אלגבריים
89-214 סמסטר א' תש"ף

שאלה 1. כתבו את לוחות הכפל של $\mathbb{Z}_2 \times \mathbb{Z}_3$ ושל $GL_2(\mathbb{F}_2)$. האם הן אבליות? האם הן ציקליות? תזכורת: בשדה $\mathbb{F}_2$ יש שני איברים $\{0,1\}$ ופעולות החיבור והכפל הן מודולו 2.

פתרון.

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

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

נשים לב כי $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,2) \rangle$ (מי עוד יוצר את החבורה?), ולכן החבורה ציקלית, ובפרט אבלית.

בחבורה $GL_2(\mathbb{F}_2)$ יש ששה איברים. נסמן אותם

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$d = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

איבר היחידה הוא e. בדקו שאתם מבינים מדוע אין עוד איברים בחבורה. נחשב את לוח הכפל:

$\cdot$	a	b	c	d	e	f
a	d	c	f	e	a	b
b	f	e	d	c	b	a
c	b	a	e	f	c	d
d	e	f	b	a	d	c
e	a	b	c	d	e	f
f	c	d	a	b	f	e

לוח הכפל של $GL_2(\mathbb{F}_2)$

נשים לב שהחבורה לא אבלית, כי למשל $c = ab \neq ba = f$. לכן היא גם לא ציקלית.

שאלה 2. תהי G חבורה אבלית. נסמן ב-T את אוסף האיברים מסדר סופי ב-G. הוכיחו כי $T \leq G$.

פתרון. נוכיח זאת לפי הקריטריון הפחות מקוצר, כלומר נוכיח:

א. $e \in T$.

ב. אם $g_1, g_2 \in T$, אזי $g_1 g_2 \in T$. כלומר סגירות לפעולה.

ג. אם $g \in T$, אזי $g^{-1} \in T$. כלומר סגירות להופכי.

אכן,

א. $e \in T$, כי $o(e) = 1 < \infty$.

ב. נניח ש-$g_1, g_2 \in T$. נניח כי $m = o(g_1), n = o(g_2)$ עבור $n, m < \infty$. כיוון שהחבורה G אבלית,

$$(g_1 g_2)^{mn} = g_1^{mn} g_2^{mn} = (g_1^m)^n (g_2^n)^m = e^n e^m = e$$

הוכחנו שקיים $k = mn < \infty$ שעבורו $(g_1 g_2)^k = e$. לכן, $o(g_1 g_2) \leq k < \infty$, כלומר $g_1 g_2 \in T$.

ג. הוכחנו בתרגול ש-$o(g) = o\left(g^{-1}\right)$ לכל $g \in G$. בפרט, אם $g \in T$, אזי $o(g) < \infty$, ולכן גם $o\left(g^{-1}\right) = o(g) < \infty$.

בסך הכל קיבלנו $T \leq G$.

שאלה 3. לכל תמורה σ מהתמורות הבאות, כתבו את σ כמכפלת מחזורים זרים וחשבו את σ^2, את σ^{10} ואת $o(\sigma)$.

א. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 5 & 2 & 4 & 6 \end{pmatrix} \in S_7$

ב. $\sigma = (3\,1\,2)\,(1\,4\,5)\,(2\,3)\,(4\,3\,5) \in S_5$

ג. $\sigma = \tau_1 \circ \tau_2^2 \in S_4$, כאשר $\tau_1 = (2\,3\,4)$ ו-$\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

פתרון.

א. מפרקים לפי הדרך שראינו בתרגול. מקבלים את המעגל הבא:

$$1 \mapsto 7 \mapsto 6 \mapsto 4 \mapsto 5 \mapsto 2 \mapsto 1$$

לכן $\sigma = (1\ 7\ 6\ 4\ 5\ 2)$ (כאשר 3 נשלח לעצמו). נחשב את σ^2, ונקבל:

$$\sigma^2 = (1\ 7\ 6\ 4\ 5\ 2)^2 = (1\ 6\ 5)(2\ 7\ 4)$$

אפשר לחשב ישירות ולראות כי $o(\sigma) = 6$, לכן $\sigma^6 = \mathrm{id}$. מכאן קל לחשב

$$\sigma^{10} = \sigma^6\sigma^4 = \mathrm{id}^6 \cdot \sigma^4 = \left(\sigma^2\right)^2 = (1\ 5\ 6)(2\ 4\ 7)$$

ב. נסמן את התמורה הנתונה σ. פה התמורה לא נתונה בצורה נוחה, ולכן נכתוב אותה כמטריצה כשנמצא לאן נשלח כל אחד מן המספרים $\{1, 2, 3, 4, 5\}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$

לכן קל לראות שיש פה מעגל אחד, כלומר $\sigma = (1\ 4\ 3\ 2)$ היא מחזור. נחשב את σ^2:

$$\sigma^2 = (1\ 4\ 3\ 2)^2 = (1\ 3)(4\ 2)$$

קל לחשב ולראות כי $o(\sigma) = 4$ (למעשה, סדר של מחזור הוא אורכו). לכן $\sigma^4 = \mathrm{id}$ ונקבל

$$\sigma^{10} = \left(\sigma^4\right)^2 \sigma^2 = \mathrm{id}^2 \cdot \sigma^2 = (1\ 3)(4\ 2)$$

ג. נעקוב בזהירות לאן נשלח כל אחד מהמספרים $\{1, 2, 3, 4\}$, כאשר מפעילים תחילה את τ_2 פעמיים ואז את τ_1. נקבל

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

כלומר שוב קיבלנו מחזור $\sigma = (1\ 2\ 4)$, ואפשר לחשב ולראות כי

$$\sigma^2 = (1\ 2\ 4)^2 = (1\ 4\ 2)$$

וכן $o(\sigma) = 3$. לכן באופן דומה לסעיפים הקודמים

$$\sigma^{10} = \left(\sigma^3\right)^3 \sigma = \mathrm{id}^3 \cdot \sigma = \sigma = (1\ 2\ 4)$$

שאלה 4. תהי $G = \{a_1, a_2, \ldots, a_n\}$ חבורה אבלית סופית. יהי האיבר $b = a_1a_2 \cdots a_n$.

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. לפי ההגדרה של העלאה בריבוע,

$$b^2 = (a_1 a_2 \dots a_n)^2 = a_1 a_2 \dots a_n a_1 a_2 \dots a_n$$

כיוון ש-G אבלית, לא משנה סדר המכפלה של האיברים ב-b^2. נשים לב שב-b^2 כל איבר בחבורה מופיע פעמיים. נסדר את המכפלות כך שכל איבר יהיה ליד ההופכי שלו $b^2 = a_1 a_1^{-1} a_2 a_2^{-1} \cdots a_n a_n^{-1}$. אז קל לראות מצמצום כי $b^2 = e$.

ב. נזכור 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 $b = e$.
פתרון אחר: ראינו שבסעיף הקודם $b^2 = e$, ולכן הסדר של b מחלק את 2. כלומר הוא 1 או 2. לפי הנתון, אין איבר מסדר 2 בחבורה, ולכן הסדר של b הוא 1, כלומר $b = e$.

ג. כיוון שהטיפוס של unsigned char יכול להכיל מספרים מהתחום $0, 1, \dots, 255$, נשים לב שהחיבור שלהם מתנהג בדיוק כמו $\mathbb{Z}_{256}$. למשל, $255 + 1 = 0$, 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 יצטצמם עם הנגדי 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 5. תהינה G, H חבורות. האם כל תת־חבורה K של $G \times H$ היא בהכרח מהצורה $K_1 \times K_2$, כאשר K_1 תת־חבורה של G ו-K_2 תת־חבורה של H? הוכיחו או תנו דוגמה נגדית.

פתרון. התשובה היא **לא**!
ניקח $G = H = \mathbb{Z}_2$ (אפשר לקחת כל חבורה לא טריוויאלית). כלומר $G \times H = \mathbb{Z}_2 \times \mathbb{Z}_2$. נסתכל על

$$K = \langle (1,1) \rangle = \{(0,0), (1,1)\}$$

מהגדרת K (כתת־החבורה הנוצרת על ידי $(1,1)$) ברור כי $K \leq \mathbb{Z}_2 \times \mathbb{Z}_2$. אבל אי אפשר להציג את K כמכפלה של תת־חבורות $K_1 \times K_2$ כנ"ל. הרי אז $0, 1 \in K_1$ וגם $0, 1 \in K_2$, ומקבלים $K_1 = K_2 = \mathbb{Z}_2$, כלומר $K_1 \times K_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \neq K$.
כעת נציג את **ההוכחה השגויה** הנפוצה. ההוכחה הולכת ככה: תהי $K \leq G \times H$ תת־חבורה. נגדיר

$$K_1 = \{g \in G \mid \exists h \in H : (g,h) \in K\}$$
$$K_2 = \{h \in H \mid \exists g \in G : (g,h) \in K\}$$

אז קל לבדוק ש-$K_1 \leq G$ ו-$K_2 \leq G$ (הקריטריון המקוצר, למשל). עכשיו אומרים "ברור ש-$K = K_1 \times K_2$", ולכן סיימנו.

הבעיה, כמו שניחשתם, היא בזה שמה שכתוב "ברור ש-" לא ברור. למעשה, הוא לא נכון. בדוגמה הנגדית להלן, מקבלים ש-$K_1 = K_2 = \mathbb{Z}_2$, ואז $K_1 \times K_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \neq K$.

שאלה 6. תהי $\sigma \in S_n$ תמורה, ונגדיר את התומך של σ להיות

$$\mathrm{supp}(\sigma) = \{i \,|\, \sigma(i) \neq i\}$$

במילים אחרות, אלו הם המספרים ש-σ "מזיזה". נאמר ששתי תמורות σ ו-τ הן זרות אם $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \varnothing$.

א. תנו דוגמה לתמורות לא זרות שאינן מתחלפות.

ב. תנו דוגמה לתמורות לא זרות שמתחלפות.

ג. הוכיחו שאם $i \in \mathrm{supp}(\sigma)$, אז גם $\sigma(i) \in \mathrm{supp}(\sigma)$.

ד. הוכיחו שכל זוג תמורות זרות מתחלף.

פתרון.

א. נבחר $\sigma = (1\ 2) \in S_3$ ואת $\tau = (2\ 3) \in S_3$. התמורות האלו לא זרות כי חיתוך התומכים שלהן הוא $\{2\}$. כבר חישבנו בכיתה כי

$$\sigma\tau = (1\ 2\ 3) \neq (1\ 3\ 2) = \tau\sigma$$

ב. אפשר לבחור חזקות של אותה תמורה. למשל אם $\sigma = (1\ 5\ 3)(4\ 7) \in S_7$, אז $\sigma\sigma^2 = \sigma^3 = \sigma^2\sigma$ כאשר $\sigma^2 = (1\ 3\ 5)$. חיתוך התומכים של σ ו-σ^2 הוא $\{1,3,5\}$, ולכן הן לא זרות.

ג. אם $i \in \mathrm{supp}(\sigma)$, אז $\sigma(i) \neq i$. נניח בשלילה כי $\sigma(i)$ לא שייך לתומך של σ. לכן $\sigma(\sigma(i)) = \sigma(i)$. מפני ש-$\sigma$ היא פונקציה הפיכה נוכל להפעיל σ^{-1} על המשוואה האחרונה ולקבל $\sigma(i) = i$, שזו סתירה.

ד. תהינה $\sigma, \tau \in S_n$ תמורות זרות ונרצה להראות $\sigma\tau = \tau\sigma$. יהי $i \in \{1, \ldots, n\}$. אם $i \notin \mathrm{supp}(\sigma)$ וגם $i \notin \mathrm{supp}(\tau)$, אז בוודאי

$$\sigma(\tau(i)) = \sigma(i) = i = \tau(i) = \tau(\sigma(i))$$

אם $i \in \mathrm{supp}(\sigma)$, אז הוא לא שייך ל-$\mathrm{supp}(\tau)$. כלומר $\tau(i) = i$, ולכן $\sigma(\tau(i)) = \sigma(i)$. לפי הסעיף הקודם גם $\sigma(i) \in \mathrm{supp}(\sigma)$ ולכן $\sigma(i)$ גם לא שייך ל-$\mathrm{supp}(\tau)$. לכן $\tau(\sigma(i)) = \sigma(i)$. באופן דומה מוכיחים את המקרה שבו $i \in \mathrm{supp}(\tau)$. בדקנו שלכל $i \in \{1, \ldots, n\}$ מתקיים $\sigma\tau(i) = \tau\sigma(i)$ ולכן $\sigma\tau = \tau\sigma$.

שאלה 7 (רשות)**.** הוכיחו כי אם שני מחזורים שאינם זרים מתחלפים זה עם זה, אז כל אחד מהם הוא חזקה של השני.

הדרכה: יהיו σ, τ שני מחזורים מתחלפים שאינם זרים. ראשית הראו כי $\mathrm{supp}(\sigma) = \mathrm{supp}(\tau)$. אפשר להניח ש-$\sigma = (1\ 2\ \ldots\ n)$, ו-$\tau(1) = 1 + k$. הראו כי $\tau = \sigma^k$.

בהצלחה!