©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש״ף:
בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור,
ד״ר חיה קלר, ד״ר אלעד אייגנר-חורב
נכתב ע"י בר אלון

חבורות

<u>תרגיל:</u>

יהי $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. האם $(S,\cdot)$ מהווה חבורה?

<u>פתרון:</u>

נראה ש$(S,\cdot)$ איננה חבורה. כדי לראות זאת, נעבור על האקסיומות המגדירות חבורה, על מנת לזהות היכן הבעיה. תחילה נשים לב כי S סגורה תחת כפל. אכן, בהינתן $a + b\sqrt{2}$ וגם $c + d\sqrt{2}$, איברים מS, ניתן לראות כי

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ad + 2bd) + (ad + bc)\sqrt{2} \in S$$

שנית, $1 = 1 + 0\sqrt{2}$ מהווה איבר ניטרלי בS ביחס לכפל. לבסוף, פעולת הכפל היא פעולה אסוציטיבית. כעת נראה כי לא לכל איבר בS קיים הופכי ביחס לכפל. נקבע $a + b\sqrt{2} \in S$ ונניח כי יש לו הופכי $c + d\sqrt{2} \in S$. אזי

$$1 = \left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ad + 2bd) + (ad + bc)\sqrt{2}$$

ולכן $\sqrt{2} = \frac{1-ad-2bd}{ad+bc}$ מספר רציונלי, סתירה.

<u>תרגיל:</u>

יהי

$$S = \{\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 1,1\rangle\}$$

הפעולה $*$ מעל S מוגדרת בעזרת הטבלה הבאה:

$*$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$
$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$
$\langle 0,1\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$
$\langle 1,0\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$
$\langle 1,1\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$

הוכיחו כי $(S,*)$ מהווה חבורה אבלית.

הערה: למעשה $(S,*)$ היא המכפלה הקרטזית של החבורה $(Z_2,+)$ בעצמה. כלומר

$$(S,*) = (Z_2,+) \times (Z_2,+)$$

<u>פתרון:</u>

עלינו לבדוק את ארבעת התכונות בהגדרה של חבורה.

סגירות: אכן, מהגדרת הפעולה $a * b \in S$ לכל $a, b \in S$.

אסוציטיביות: עלינו להראות שמתקיים $(a * b) * c = a * (b * c)$ לכל $a, b, c \in S$. ניתן להראות זאת על ידי כך שנעבור על כל האפשרויות להציב, אך נעשה זאת בדרך אחרת. נסמן $a = \langle a_1, a_2 \rangle$, $b = \langle b_1, b_2 \rangle$ ו-$c = \langle c_1, c_2 \rangle$. נשים לב כי

$$\langle a_1, a_2 \rangle * \langle b_1, b_2 \rangle = \langle (a_1 + b_1) \bmod 2, (a_2 + b_2) \bmod 2 \rangle$$

מכיוון שהוכח בהרצאה שחיבור מודולו 2 הינה פעולה אסוציטיבית, נקבל כי מתקיים

$$\begin{aligned}
(a * b) * c &= (\langle a_1, a_2 \rangle * \langle b_1, b_2 \rangle) * \langle c_1, c_2 \rangle \\
&= \langle (a_1 + b_1) \bmod 2, (a_2 + b_2) \bmod 2 \rangle * \langle c_1, c_2 \rangle \\
&= \langle (a_1 + b_1 + c_1) \bmod 2, (a_2 + b_2 + c_2) \bmod 2 \rangle \\
&= \langle a_1, a_2 \rangle * \langle (b_1 + c_1) \bmod 2, (b_2 + c_2) \bmod 2 \rangle \\
&= \langle a_1, a_2 \rangle * (\langle b_1, b_2 \rangle * \langle c_1, c_2 \rangle) \\
&= a * (b * c)
\end{aligned}$$

קיום איבר ניטרלי: על פי האבחנה נוכל לומר כי $\langle 0,0 \rangle$ הוא איבר ניטרלי (ניתן לראות זאת גם מהטבלה).

קיום הופכי: מהאבחנה (או מהטבלה) ניתן לומר כי כל איבר הוא ההופכי של עצמו.

אבליות: מכיוון שחיבור מודולו 2 הינה פעולה קומוטטיבית, ניתן לראות שפעולה $*$ קומוטטיבית. ניתן לראות זאת גם מהעובדה שהטבלה סימטרית ביחס לאלכסון הראשי.

תרגיל:

יהי $S = \{\langle a, b \rangle : a, b \in \mathbb{R}, a \neq 0\}$. נגדיר את הפעולה $*$ מעל S באופן הבא:

$$\langle a, b \rangle * \langle c, d \rangle = \langle ac, bc + d \rangle$$

הוכיחו כי $(S,*)$ מהווה חבורה שאיננה אבלית.

פתרון:

עלינו לבדוק את ארבעת התכונות בהגדרה של חבורה.

סגירות: אכן, מהגדרת הפעולה $\langle a, b \rangle * \langle c, d \rangle = \langle ac, bc + d \rangle \in S$ לכל $\langle a, b \rangle, \langle c, d \rangle \in S$ שכן $ac \neq 0$.

אסוציטיביות: עלינו להראות שמתקיים $(a * b) * c = a * (b * c)$ לכל $a, b, c \in S$. תכונה זאת נובעת ישירות מהתכונות המוכרות של מספרים ממשיים.

נכתב ע"י בר אלון

אכן

$$
\begin{aligned}
(\langle a,b\rangle * \langle c,d\rangle) * \langle e,f\rangle &= \langle ac, bc+d\rangle * \langle e,f\rangle \\
&= \langle (ac)e, (bc+d)e+f\rangle \\
&= \langle a(ce), b(ce)+(de+f)\rangle \\
&= \langle a,b\rangle * \langle ce, de+f\rangle \\
&= \langle a,b\rangle * (\langle c,d\rangle * \langle e,f\rangle)
\end{aligned}
$$

<u>קיום איבר ניטרלי:</u> נשים לב כי $\langle 1,0\rangle$ מהווה איבר ניטרלי, כפי שניתן לראות בחישוב הבא:

$$\langle a,b\rangle * \langle 1,0\rangle = \langle a\cdot 1, b\cdot 1+0\rangle = \langle a,b\rangle$$

<u>קיום הופכי:</u> נשים לב כי ההופכי של $\langle a,b\rangle$ הוא האיבר $\langle 1/a, -b/a\rangle$. אכן

$$\langle a,b\rangle * \left\langle \frac{1}{a}, -\frac{b}{a}\right\rangle = \left\langle a\cdot\frac{1}{a}, b\cdot\frac{1}{a} + \left(-\frac{b}{a}\right)\right\rangle = \langle 1,0\rangle$$

כעת נראה שהחבורה איננה אבלית. ניתן לראות זאת מחוסר השוויון הבא:

$$\langle 1,2\rangle * \langle 3,4\rangle = \langle 3,10\rangle \neq \langle 3,6\rangle = \langle 3,4\rangle * \langle 1,2\rangle$$

<u>תרגיל:</u>

תהי $S=\{f_1,\dots,f_6\}$ קבוצה של פונקציות כאשר $f_i\colon \mathbb{R}\setminus\{0,1\} \mapsto \mathbb{R}\setminus\{0,1\}$ נתונות על ידי

$$
\begin{aligned}
f_1(x) &= x, & f_2(x) &= x^{-1}, \\
f_3(x) &= 1-x, & f_4(x) &= \frac{x-1}{x}, \\
f_5(x) &= \frac{x}{x-1}, & f_6(x) &= \frac{1}{1-x}
\end{aligned}
$$

הוכיחו כי $(S,\circ)$ מהווה חבורה שאיננה אבלית.

<u>פתרון:</u>

תחילה, נרשום את טבלת ההרכבות:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1

בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור,
ד״ר חיה קלר, ד״ר אלעד אייגנר-חורב
נכתב ע"י בר אלון

f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

מהטבלה, ניתן לראות את תכונת הסגירות, קיום איבר יחידה f_1, וקיום איבר הופכי (כי בכל שורה ובכל עמודה מופיע f_1). העובדה שהחבורה אינה אבלית נובעת מהעובדה שהטבלה אינה סימטרית ביחס לאלכסון הראשי, לדוגמה

$$(f_2 \circ f_6)(x) = f_3(x) \neq f_5(x) = (f_6 \circ f_2)(x)$$

נותר להראות אסוציטיביות. תכונה זו נובעת מהאסוציטיביות של הרכבת פונקציות:
יהיו $f: X \mapsto W$, $g: Y \mapsto X$, ו$h: Z \mapsto Y$ שלוש פונקציות. אזי
$(f \circ g) \circ h, f \circ (g \circ h): X \mapsto W$ ובנוסף הם שוות, שכן מתקיים

$$\big((f \circ g) \circ h\big)(z) = (f \circ g)\underbrace{\big(h(z)\big)}_{\in Y} = f\underbrace{\Big(g\big(h(z)\big)\Big)}_{\in X}$$

וגם מתקיים

$$\big(f \circ (g \circ h)\big)(z) = f\big((g \circ h)(z)\big) = f\Big(g\big(h(z)\big)\Big)$$