

**מבוא לתורת החבורות**

**הגדרה**

**חבורה למחצה** היא מבנה מתמטי  $(S, \cdot)$ , כאשר הפעולה  $\cdot$  היא פעולה בינארית אסוציאטיבית, כלומר, מתקיים:

$$\forall x, y, z \in S: (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

**דוגמה**

לכל קבוצה  $A$ ,  $(A^A, \circ)$ , כלומר, קבוצת הפונקציות מ  $A$  לעצמה עם פעולת הרכבת פונקציות, היא חבורה למחצה.

**הוכחה**

יהיו  $f, g, h \in A^A$ .

$$[(f \circ g) \circ h](a) = (f \circ g)(h(a))$$

$$= f(g(h(a)))$$

$$[f \circ (g \circ h)](a) = f((g \circ h)(a))$$

$$= f(g(h(a)))$$

↓

$$(f \circ g) \circ h = f \circ (g \circ h)$$

לכן,  $A^A$  חבורה למחצה.

■

**דוגמה**

יהי  $\mathbb{F}$  שדה,  $V$  מרחב ווקטורי.

$(\mathbb{F}, +)$ ,  $(\mathbb{F}, \cdot)$ ,  $(V, +)$  הם חבורות למחצה.

**הגדרה**

אם קיימת פונקציה חד-חד-ערכית ועל  $f: S \rightarrow S'$  כך ש:

$$\forall x, y \in S: f(x \cdot y) = f(x) * f(y)$$

## הערה

ניתן להגדיר חבורה למחצה ע"י לוח הכפל שלה.

## דוגמה

|         |     |     |     |
|---------|-----|-----|-----|
| $\cdot$ | $a$ | $b$ | $c$ |
| $a$     | $a$ | $a$ | $a$ |
| $b$     | $a$ | $b$ | $b$ |
| $c$     | $a$ | $b$ | $c$ |

## דוגמה

קיימות בדיוק 5 חבורות למחצה עם שני איברים (עד כדי איזומורפיזם):

|       |   |   |
|-------|---|---|
| $min$ | 0 | 1 |
| 0     | 0 | 0 |
| 1     | 0 | 1 |

|          |   |   |
|----------|---|---|
| $\oplus$ | 0 | 1 |
| 0        | 0 | 1 |
| 1        | 1 | 0 |

|   |   |   |
|---|---|---|
|   | 0 | 1 |
| 0 | 0 | 0 |
| 1 | 0 | 0 |

|     |   |   |
|-----|---|---|
| $L$ | 0 | 1 |
| 0   | 0 | 0 |
| 1   | 1 | 1 |

|     |   |   |
|-----|---|---|
| $R$ | 0 | 1 |
| 0   | 0 | 1 |
| 1   | 0 | 1 |

**הערה**

קיימות חבורות למחצה רבות בגודל 3,4,5,...

**הגדרה**

תהי  $(S, \cdot)$  חבורה למחצה.

איבר  $e \in S$  נקרא **יחידה משמאל** אם:

$$\forall x \in S: e \cdot x = x$$

איבר  $e \in S$  נקרא **יחידה מימין** אם:

$$\forall x \in S: x \cdot e = x$$

איבר  $e \in S$  נקרא **איבר יחידה** אם:

$$\forall x \in S: e \cdot x = x \cdot e = x$$

**משפט**

אם  $e$  יחידה משמאל ו-  $e'$  יחידה מימין אז:

$$e = e'$$

**הוכחה**

$e$  יחידה משמאל, לכן:

$$e \cdot e' = e'$$

$e'$  יחידה מימין, לכן:

$$e \cdot e' = e$$

לכן:

$$e = e'$$

■

**מסקנה**

אם קיים איבר יחידה, אז הוא יחיד.

**הגדרה**

חבורה למחצה שיש לה איבר יחידה נקראת **מונואיד** (*monoid*).

**הגדרה**

יהי  $(M, \cdot, 1)$  מונואיד.

איבר  $a \in M$  הוא **הפיך מימין** אם קיים  $b \in M$  כך ש:

$$b \cdot a = 1$$

איבר  $a \in M$  הוא **הפיך משמאל** אם קיים  $b \in M$  כך ש:

$$a \cdot b = 1$$

איבר  $a \in M$  הוא **הפיך** אם קיים  $b \in M$  כך ש:

$$a \cdot b = b \cdot a = 1$$

**הערה**

אם  $a$  הפיך משמאל ומימין, אז הוא הפיך.

**הוכחה**

עפ"י הנתון, קיימים  $b, b'$  כך ש:

$$a \cdot b' = b \cdot a = 1$$

לכן:

$$b' = 1 \cdot b' = (b \cdot a) \cdot b' = b \cdot (a \cdot b') = b \cdot 1 = b$$

לכן:

$$b = b'$$

■

**דוגמה**

תהי  $A$  קבוצה.

$A^A$  היא חבורה למחצה.

זהו מונואיד משום שהזהות היא איבר יחידה.

$f \in A^A$  הפיך משמאל אם ורק אם קיימת  $g \in A^A$  כך ש:  $g \circ f = 1$ , אם ורק אם  $f$  חד-חד-ערכית.

$f \in A^A$  הפיך מימין אם ורק אם קיימת  $g \in A^A$  כך ש:  $f \circ g = 1$ , אם ורק אם  $f$  על. לכן,  $f \in A^A$  הפיך אם ורק אם  $f$  חד-חד-ערכית ועל.

■

### הגדרה

מונויד שבו כל האיברים הפיכים נקרא **חבורה**.

כלומר, חבורה היא מבנה אלגברי  $(G, \cdot, 1)$  כך שמתקיימות התכונות הבאות:

$$(1) \quad \forall x, y, z \in G: (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$(2) \quad \forall x \in G: x \cdot 1 = 1 \cdot x = x$$

$$(3) \quad \forall x, y \in G: x \cdot y = y \cdot x = 1$$

### הגדרה

יהי  $M$  מונויד.

$M$  בעל צמצום משמאל אם:

$$\forall x, y, z \in M: x \cdot y = x \cdot z \rightarrow y = z$$

### הערה

אם  $x$  הפיך משמאל, אז ניתן לצמצם  $x$  משמאל.

### הוכחה

עפ"י הנתון, קיים  $x'$  כך ש:

$$x' \cdot x = 1$$

לכן:

$$xy = xz$$

↓

$$y = 1 \cdot y = x'xy = x'xz = 1 \cdot z = z$$

לכן:

$$y = z$$



### מסקנה

כל מונויד שבו כל איבר הפיך משמאל הוא בעל צמצום משמאל.

כל חבורה היא מונויד בעל צמצום משמאל.

### משפט

מונויד סופי עם צמצום משמאל הוא חבורה.

### טענה

אם במונויד  $M$  כל איבר הפיך מימין, אז כל איבר הפיך, כלומר,  $M$  חבורה.

### הוכחה

יהי  $a \in M$ .

עפ"י הנתון, קיים  $a' \in M$  כך ש:

$$a \cdot a' = 1$$

עפ"י הנתון, קיים  $a'' \in M$  כך ש:

$$a' \cdot a'' = 1$$

לכן:

$$a'' = 1 \cdot a'' = (aa') \cdot a'' = a \cdot (a'a'') = a \cdot 1 = a$$

לכן:

$$aa' = a'a = 1$$

לכן,  $a$  הפיך.

לכן,  $M$  חבורה.

■

### הוכחה

עפ"י הטענה, מספיק להוכיח שכל איבר הפיך מימין.

יהי  $a \in M$ .

נגדיר פונקציה:  $f: M \rightarrow M$  ע"י:

$$f(x) = ax$$

אם:

$$f(x) = f(y)$$

אז:

$$ax = ay$$

עפ"י הצמצום משמאל:

$$x = y$$

לכן,  $f$  חד-חד-ערכית.

$M$  סופית, לכן  $f$  על.

בפרט, קיים  $b$  כך ש:

$$f(b) = 1$$

לכן:

$$ab = 1$$

לכן,  $a$  הפיך מימין.

לכן,  $M$  חבורה.

■

### הגדרה

יהי  $M$  מונויד.

נכתב על ידי יהונתן רגב

אם  $M', M' \subseteq M$ , סגור לפעולה ו-  $1_M \in M'$ , אז  $M'$  נקראת **תת מונויד**.

כלומר, תת מונויד הוא תת קבוצה שהיא מונויד ביחס לפעולה המקורית, עם אותו איבר יחידה.

### הערה

תת מונויד של מונויד עם צמצום משמאל הוא עם צמצום משמאל.

תת מונויד של חבורה אינו בהכרח חבורה.

### דוגמה

$(\mathbb{Z}, +, 0)$  חבורה.

$(\mathbb{N}, +, 0)$  מונויד עם צמצום משמאל, אבל לא חבורה.

### הגדרה

יהי  $M$  מונויד.

יהי  $a \in M$  איבר הפיך.

האיבר  $b \in M$  המקיים:

$$ab = ba = 1$$

נקרא **האיבר ההפכי** של  $a$ , ויסומן ב-  $a^{-1}$ .

### טענה

לאיבר הפיך יש הפכי יחיד.

### הוכחה

נניח כי  $b, b'$  איברים הפכיים ל-  $a$ .

לכן:

$$b' = 1 \cdot b' = (ba) \cdot b' = b \cdot (ab') = b \cdot 1 = b$$

לכן:

$$b = b'$$

■

### טענה



אם  $a$  הפיך, אז  $a^{-1}$  הפיך ו:

$$(a^{-1})^{-1} = a$$

אם  $a, b$  הפיכים, אז  $ab$  הפיך ו:

$$(ab)^{-1} = b^{-1}a^{-1}$$

### הגדרה

יהי  $M$  מונויד.

נגדיר את חבורת ההפיכים של  $M$ :

$$\mathcal{U}(M) := \{a \in M \mid a \text{ הפיך}\}$$

$\mathcal{U}(M)$  היא חבורה.

### דוגמה

תהי  $A$  קבוצה.

$A^A$  מונויד.

$$S_A := \mathcal{U}(A^A) = \{f: A \rightarrow A \mid f \text{ חד ערכית ועל}\}$$

### דוגמה

יהי  $\mathbb{F}$  שדה ו-  $n \geq 1$ .

$(M_n(\mathbb{F}), \cdot, I_n)$  מונויד.

$$GL_n(\mathbb{F}) := \mathcal{U}(M_n(\mathbb{F})) = \{A \in M_n(\mathbb{F}) \mid A \text{ הפיכה}\}$$

■