# שיעור 4
# תמורות וצופן אניגמה

## 4.1 תמורות

**הגדרה 4.1 תמורה**

תמורה על קבוצה סופית $\Sigma = \{x_1, \ldots, x_n\}$ היא פונקציה $\pi : \Sigma \to \Sigma$ אשר היא חד-חד ערכית ו "על" $\Sigma$.
בהינתן $x_i \in \Sigma$ ותמורה $\pi$. אזי

$$\pi(x_i) = x_j \in \Sigma \ .$$

תזכורת:

- $\pi$ חד-חד ערכית. ז"א אם $x_i \neq x_j$ אזי $\Sigma(x_i) \neq \Sigma(x_j)$.
- $\pi$ "על" $\Sigma$. ז"א לכל $y \in \Sigma$ קיים $x \in \Sigma$ כך ש- $\pi(x) = y$.

כתוצאה מכך, אם $\pi$ פועלת על כל האיברים של $\Sigma$ אזי נקבל אותה קבוצה $\Sigma$ רק לא באותו בסדר של הסדר המקורי:

$$\{\pi(x_1) \ , \ \pi(x_2) \ , \quad \ldots \quad \pi(x_n)\} \ .$$

**דוגמה 4.1**

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\pi(x)$ | 4 | 1 | 6 | 5 | 2 | 3 |

**דוגמה 4.2**

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\sigma(x)$ | 2 | 1 | 5 | 4 | 6 | 3 |

**דוגמה 4.3**

[] תהי $\Sigma$ קבוצה סופית ותהי $\pi : \Sigma \to \Sigma$ פונקציה. הוכיחו: אם $\pi$ חד-חד ערכית אז היא תמורה.

**פתרון:**
נתון לנו הפונקציה $\pi : \Sigma \to \Sigma$ כאשר $\Sigma$ קבוצה נוצר סופית. כדי להוכיח כי $\pi$ תמורה יש להראות כי $\pi$ חד-חד-ערכית ו"על" $\Sigma$. כבר נתון לנו ש- $\pi$ חח"ע אז נשאר רק להראות כי $\pi$ על $\Sigma$.

$\Sigma$ היא קבוצה סופית לכן קיים שלם $n \geq 0$ עבורו $|\Sigma| = n$. תהי $\pi(\Sigma)$ התמונה של $\pi$. מכיוון ש- $\pi$ היא פונקציה מהקבוצה $\Sigma$ אל הקבוצה $\Sigma$, אזי התמונה שלה היא תת-קבוצה של $\Sigma$, כלומר:

$$\pi(\Sigma) \subseteq \Sigma \ .$$

לכן

$$|\pi(\Sigma)| \leq |\Sigma| = n \ .$$

נראה כי $|\Sigma| = |\pi(\Sigma)|$. נניח בשלילה כי $|\Sigma| < |\pi(\Sigma)|$. אז בהכרח קיימים איברים $x_1, x_2 \in \Sigma$ כך ש:

$\Sigma(x_1)=\Sigma(x_2)$, בסתירה לכך ש: $\pi$ חד-חד-ערכית. לכן הוכחנו דרך השלילה כי

$$|\pi(\Sigma)| = |\Sigma| = n \ .$$

הוכחנו כי $\pi(\Sigma)\subseteq\Sigma$ וגם $|\pi(\Sigma)|=|\Sigma|$ אז בהכרח

$$\pi(\Sigma)\,\Sigma$$

ולפיכך $\pi:\Sigma\to\Sigma$ היא פונקציה "על" $\Sigma$.

■

**הגדרה 4.2 הרכבה של תמורות**

[] תהי $\Sigma$ קבוצה נוצר סופית ותהיינה $\pi:\Sigma\to\Sigma$ ו- $\sigma:\Sigma\to\Sigma$ תמורות על הקבוצה $\Sigma$. ההרכבה של $\pi$ ו- $\sigma$ מוגדרת להיות הפונקציה שמסומנת $\sigma\pi$ ומוגדרת לפי התנאי:
לכל $x\in\Sigma$, אם $\pi(x)=y\in\Sigma$ ואם $\sigma(y)=z\in\Sigma$ אזי

$$\sigma\pi(x)=z \ .$$

**משפט 4.1**

[] תהי $\Sigma$ קבוצה נוצר סופית ותהיינה $\pi:\Sigma\to\Sigma$ ו- $\sigma:\Sigma\to\Sigma$ תמורות על הקבוצה $\Sigma$. ההרכבה $\sigma\pi$ היא תמורה על $\Sigma$.

**הוכחה:** מספיק להוכיח כי $\sigma\pi$ היא פונקציה חד-חד-ערכית ו"על" $\Sigma$.

- **חח"ע"**

  נניח בשלילה כי $\sigma\pi$ לא חח"ע. אזי קיימים $x_1,x_2\in\Sigma$ כך ש- $\sigma(\pi(x_1))=\sigma(\pi(x_2))$. נסמן $y_1=\pi(x_1)$ ו- $y_2=\pi(x_2)$. מכיוון ש- $\pi$ תמורה אז $\pi$ חח"ע ולכן $y_1\neq y_2$. ומכיוון ש- $\sigma$ תמורה אזי $\sigma(y_1)\neq\sigma(y_2)$. לכן

  $$\sigma(\pi(x_1))\neq\sigma(\pi(x_2)) \ ,$$

  בסתירה לכך ש- $\sigma(\pi(x_1))=\sigma(\pi(x_2))$.

  לכן הוכחנו דרך השלילה כי $\sigma\pi$ פונקציה חח"ע.

- **על**

  נניח בשלילה כי $\sigma\pi$ לא על. נסמן $\sigma\pi(\Sigma)$ התמונה של $\sigma\pi$. אזי

  $$\sigma\pi(\Sigma)\neq\Sigma \ .$$

  ראשית מכיוון ש- $\sigma\pi(\Sigma)$ הוא התמונה של $\sigma\pi$ אזי $\sigma\pi(\Sigma)\subseteq\Sigma$. לכן אם $\sigma\pi(\Sigma)\neq\Sigma$ אז $\sigma\pi(\Sigma)\subset\Sigma$. ומכאן

  $$|\sigma\pi(\Sigma)|<|\Sigma| \ .$$

  לכן בהכרח קיים לפחות שני איברים $x_1,x_2\in\Sigma$ עבורם $\sigma\pi(x_1)=\sigma\pi(x_2)$. זאת בסתירה לכך ש- $\sigma\pi$ חח"ע, שמוכח בסעיף הקודם.

  לכן הוכחנו דרך השלילה כי הפונקציה $\sigma\pi$ היא "על" $\Sigma$.

■