שיעור 2
חוגים מתמטיים

2.1 הפונקצית אוילר

הגדרה 2.1 פונקצית אוילר

יהי m מספר שלם. הפונקצית אוילר מסומנת $\phi(m)$ ומוגדרת להיות כמות השלמים שקטנים ממש מ- m וזרים ביחס ל- m.

$$\phi(m) := \left|\left\{a \in \mathbb{N} \,\middle|\, \gcd(a,m)=1,\ a<m\right\}\right| \ .$$

דוגמה 2.1

מכיוון ש- $26 = 2 \times 13$, הערכים של a עבורם $\gcd(a,26)=1$ הם

$$\{1,3,5,7,9,11,15,17,19,21,23,25\} \ .$$

ז"א יש בדיוק 12 ערכים של a עבורם $\gcd(a,26)=1$.

$$\phi(26)=12 \ .$$

משפט 2.1 הפירוק לראשוניים של פונקצית אוילר

יהי $m \geq 2$ מספר שלם ונניח כי הפירוק למספרים ראשוניים שלו הוא

$$m = \prod_{i=1}^{n} p_i^{e_i} \ .$$

אזי

$$\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i-1}\right) \ .$$

דוגמה 2.2

מצאו את $\phi(60)$.

פתרון:

$60 = 2^2 \times 3^1 \times 5^1$ לכן

$$\phi(60) = \left(2^2-2^1\right)\left(3^1-3^0\right)\left(5^1-5^0\right) = (2)(2)(4) = 16 \ .$$

■

דוגמה 2.3

חשבו את $\phi(24)$

פתרון:

$$24 = 2^3 3^1 \ .$$

לכן

$$\phi(24) = (2^3 - 2^2)(3^1 - 3^0) = (8-4)(3-1) = 8 \ .$$

■

משפט 2.2

אם p מספר ראשוני אז

$$\phi(p) = p - 1 \ .$$

הוכחה: תרגיל בית. ■

משפט 2.3

אם p מספר ראשוני אז

$$\phi\left(p^n\right) = p^n - p^{n-1} \ .$$

הוכחה: תרגיל בית. ■

משפט 2.4

אם a, b שלמים זרים (כלומר $\gcd(a,b) = 1$) אז

$$\phi\left(a \cdot b\right) = \phi(a) \cdot \phi(b) \ .$$

הוכחה:

הוכחה: נשתמש בנוסחה

$$\varphi(n) = \prod_{p^e \| n} \left(p^e - p^{e-1}\right)$$ (שקולה ל- $\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$.)

פרקו $a = \prod p_i^{\alpha_i}$ ו- $b = \prod q_j^{\beta_j}$ עם $\gcd(a,b) = 1$, ולכן קבוצות הראשוניים $\{p_i\}$ ו- $\{q_j\}$ זרות. אזי

$$\varphi(ab) = \prod_i \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) \cdot \prod_j \left(q_j^{\beta_j} - q_j^{\beta_j - 1}\right) = \varphi(a)\,\varphi(b).$$

■ ■

משפט 2.5

אם p ו- q מספרים ראשוניים שונים אז

$$\phi(p \cdot q) = (p-1)(q-1) \ .$$

הוכחה: תרגיל בית. ■

משפט 2.6 משפט אוילר

אם a,n שלמים ו- $\gcd(a,n)=1$ אז

$$a^{\phi(n)} \equiv 1 \pmod{n} .$$

משפט 2.7

אם a,n שלמים ו- $\gcd(a,n)=1$ אז

$$a^{-1} \equiv a^{\phi(n)-1} \pmod{n} .$$

דוגמה 2.4

חשבון את האיבר ההופכי ל- 5 ב- $\mathbb{Z}_{11}$.

פתרון:

לפי משפט פרמט 5.9:

$$5^{-1} = 5^{11-2} \pmod{1}1 = 5^{9} \pmod{1}1 .$$

לפי הנוסחת לשארית **??** :

$$5^9 \ \% \ 11 = 5^9 - 11 \left\lfloor \frac{5^9}{11} \right\rfloor = 9$$

לכן $5^{-1} \in \mathbb{Z}_{11} = 9$. ■

2.2 החוג $\mathbb{Z}_m$

הגדרה 2.2 החוג $\mathbb{Z}_m$

החוג $\mathbb{Z}_m$ מוגדר להיות הקבוצה של מספרים שלמים

$$\mathbb{Z}_m = \{0,1,\ldots,m-1\}$$

יחד עם הפעולות $\oplus$ ו- $\odot$ המוגדרות כך:

לכל $a,b\in\mathbb{Z}_m$,

$$a\oplus b = (a+b) \ \% \ m , \qquad a\odot b = ab \ \% \ m .$$

במילים אחרות, $\mathbb{Z}_m$ היא קבוצת השארית בחלוקה ב-m.

מכאן ואילך נסמן חיבור וכפל ב- $\mathbb{Z}_m$ עם הסימנים הרגילים $+$ ו- $\times$ או $\cdot$.

דוגמה 2.5

חשבון את 11×13 ב- $\mathbb{Z}_{16}$.

פתרון:

$11\times 13=143$. נמצא את השארית בחלוקה ב- 16:

$$(11\times 13) \ \% \ 16 = 143 \ \% \ 16 = 15 .$$

לפיכך $15 = 13 \times 11$ ב- $\mathbb{Z}_{16}$.

■

משפט 2.8 תכונות של החוג $\mathbb{Z}_m$

לכל $a, b, c \in \mathbb{Z}_m$ התנאים הבאים מתקיימים.

1. סגירה תחת חיבור:
$$a + b \in \mathbb{Z}_m \ .$$

2. חוק החילוף לחיבור:
$$a + b = b + a \ .$$

3. חוק הקיבוץ לחיבור:
$$(a + b) + c = a + (b + c) \ .$$

4. קיום איבר הניטרלי ביחס לחיבור:
$$a + 0 = 0 + a = a \ .$$

5. האיבר הנגדי של a הוא $m - a$, ז"א $-a = m - a$. הסבר:
$$a + (m - a) = (m - a) + a = m = 0$$
ב- $\mathbb{Z}_m$.

6. סגירה תחת כפל:
$$ab \in \mathbb{Z}_m \ .$$

7. חוק החילוף לכפל:
$$ab = ba \ .$$

8. חוק הקיבוץ לכפל:
$$(ab)c = a(bc) \ .$$

9. קיום איבר הניטרלי ביחס לכפל:
$$a \times 1 = 1 \times a = a \ .$$

10. חוק הפילוג:
$$(a + b)c = (ac) + (bc) \ .$$

תכונות 1, 3-5 אומרות כי $\mathbb{Z}_m$ הינו "חבורה מתמטית".
יחד עם תכונה 2, $\mathbb{Z}_m$ הוא חבורה אָבֶּלִית.
כל התכונות 1-10 אומרות כי $\mathbb{Z}_m$ הוא חוג מתמטי.

הגדרה 2.3 איבר ההופכי ב- $\mathbb{Z}_m$

יהי $a \in \mathbb{Z}_m$. האיבר ההופכי של a מסומן ב- a^{-1} ומקיים את התנאי
$$a^{-1}a \equiv 1 \mod m \qquad \text{וגם} \qquad aa^{-1} \equiv 1 \mod m \ .$$

משפט 2.9

נתון היחס שקילות
$$ax \equiv y \mod m \ .$$
יש פתרון יחיד $x \in \mathbb{Z}_m$ לכל $y \in \mathbb{Z}_m$ אם ורק אם $\gcd(a,m)=1$.

הוכחה:

ללא הגבלת כלליות נניח כי $a > m$.

נניח כי יש פתרון יחיד. נוכיח דרך השלילה כי ו- $\gcd(a,m)=1$.

כלומר, נניח כי יש פתרון יחיד אך $\gcd(a,m)=d>1$.

יהי $x_1 = a^{-1}y$ פתרון ל- $ax \equiv y \mod m$.

נשים לב ש- $ax_1 + \frac{am}{d} = ax_1 + km \equiv ax_1 \mod m$, כאשר $k = \frac{a}{d}$ שלם.
ז"א גם $x_1 + \frac{m}{d}$ פתרון.

זאת בסתירה לכך שהפתרון יחיד.

נניח כי $\gcd(a,m)=1$. נוכיח בשלילה כי הפתרון יחיד.
נניח כי $\gcd(a,m)=1$ וקיימים שני פתרונות שונים: $x_1 \not\equiv x_2 \mod m$.

ז"א
$$ax_1 \equiv y \mod m \ , \qquad \text{וגם} \qquad ax_2 \equiv y \mod m \ .$$
לכן
$$ax_1 \equiv ax_2 \mod m \ .$$
לכן
$$m \mid ax_1 - ax_2 \ .$$
$\gcd(a,m)=1$ לפיכך
$$m \mid x_1 - x_2 \ ,$$
ז"א
$$x_1 \equiv x_2 \mod m \ ,$$
בסתירה לכך ש- $x_1 \not\equiv x_2 \mod m$.

■

מסקנה 2.1

יהי $a \in \mathbb{Z}_m$. קיים איבר הופכי $a^{-1} \in \mathbb{Z}_m$ אשר לפי הגדרתו 2.3 מקיים את התנאי
$$aa^{-1} \equiv 1 \mod m \ ,$$
אם ורק אם $\gcd(a,m)=1$.

הוכחה: משפט 2.9. ■

דוגמה 2.6

הוכיחו שקיים איבר הופכי ל- 11 ב- $\mathbb{Z}_{26}$ ואם כן מצאו אותו.

פתרון:

קיים איבר הופכי של a ב- $\mathbb{Z}_m$ אם ורק אם $\gcd(a,m)=1$. לכן נבדוק את ה- $\gcd(26,11)$ באמצעות האלגוריתם של אוקליד המוכלל.

יהיו $a=26, b=11$.

$$\begin{aligned} r_0 &= a = 26\ , & r_1 &= b = 11\ , \\ s_0 &= 1\ , & s_1 &= 0\ , \\ t_0 &= 0\ , & t_1 &= 1\ . \end{aligned}$$

שלב $i=1$:	$r_2=26-2\cdot 11=4$	$s_2=1-2\cdot 0=1$	$t_2=0-2\cdot 1=-2$	$q_1=2$
שלב $i=2$:	$r_3=11-2\cdot 4=3$	$s_3=0-2\cdot 1=-2$	$t_3=1-2\cdot(-2)=5$	$q_2=2$
שלב $i=3$:	$r_4=4-1\cdot 3=1$	$s_4=1-1\cdot(-2)=3$	$t_4=-2-1\cdot(5)=-7$	$q_3=1$
שלב $i=4$:	$r_5=3-3\cdot 1=0$	$s_5=-2-3\cdot(3)=-11$	$t_5=5-3\cdot(-7)=28$	$q_4=3$

$$\gcd(a,b)=r_4=1\ , \qquad x=s_4=3\ , \qquad y=t_4=-7\ .$$

$$ax+by=3(26)-7(11)=1\ .$$

מכאן אנחנו רואים כי $\gcd(26,11)=1$ ולכן לפי משפט 2.9 ההופכי של 11 קיים ב- $\mathbb{Z}_{26}$.

מחשבים את האיבר ההופכי לפי השיטה הבאה:

$$-7(11)=1-9(26) \quad\Rightarrow\quad -7(11)=1 \mod 26 \quad\Rightarrow\quad 19(11)=1 \mod 26 \quad\Rightarrow\quad 11^{-1}=19 \mod 26\ .$$

■

כלל 2.1

האיברים של $\mathbb{Z}_{26}$ שעבורם קיימים איברים הופכיים הינם

1^{-1}	3^{-1}	5^{-1}	7^{-1}	9^{-1}	11^{-1}	15^{-1}	17^{-1}	19^{-1}	21^{-1}	23^{-1}	25^{-1}
1	9	21	15	3	19	7	23	11	5	17	25

הגדרה 2.4 פונקצית אוילר $\phi(m)$

נתון החוג $\mathbb{Z}_m$ כאשר $m\geq 2$ מספר טבעי.

$\phi(m)$ תוגדר להיות הפונקציה הנותנת את מספר איברים ב- $\mathbb{Z}_m$ אשר זרים ל- m.

(שימו לב ההגדרה הזאת זהה להגדרה 2.2.1.)

מסקנה 2.2 מספר איברים הפיכיים ב- $\mathbb{Z}_m$

מספר האיברים של החוג $\mathbb{Z}_m$ שעבורם קיימים איברים הופכיים שווה ל- $\phi(m)$.

הוכחה: $\phi(m)$ שווה למספר איברים $a \in \mathbb{Z}_m$
עבורם $\gcd(a,m)$, ולפי משפט 2.1 אותם האיברים הם האיברים ההפיכים של $\mathbb{Z}_m$. ■

2.3 הפיכת מטריצות בחוג $\mathbb{Z}_m$

הגדרה 2.5 המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n\times n}$.

הקופקטור ה- (i,j) של A מוגדר להיות הדטרמיננטה של המטריצה המתקבלת מ-A ע"י מחיקת שורה i ועמודה j, כפול $(-1)^{i+j}$.

המטריצה של קופקטורים של המטריצה A מוגדרת

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$$

כאשר C_{ij} הקופקטור ה- (i,j) של A.

הגדרה 2.6 המטריצה המצורפת

תהי $A \in \mathbb{R}^{n\times n}$. המטריצה המצורפת של A היא מטריצה מסדר $n \times n$ שמסומנת $\mathrm{adj}(A)$ ומוגדרת

$$\mathrm{adj}(A) = C^t$$

כאשר C המטריצה של קופקטורים של A.

משפט 2.10 נוסחת למטריצה הופכית

נניח כי $A \in \mathbb{R}^{n\times n}$ מטריצה ריבועית. אם A הפיכה, (כלומר אם $|A| \neq 0$) אז המטריצה ההופכית נתונה ע"י נוסחת קיילי המילטון:

$$A^{-1} = \frac{1}{|A|}\mathrm{adj}(A) \ ,$$

כאשר $\mathrm{adj}(A)$ המטריצה המצורפת של A.

דוגמה 2.7

מצאו את ההופכית של

$$A = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2} \ .$$

פתרון:

$$|A| = 11 \cdot 7 - 8 \cdot 3 = 53 = 1 \mod 26 \ .$$

$\gcd(1,26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \qquad \Rightarrow \qquad C_{11} = (-1)^{1+1} 7 = 7$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \qquad \Rightarrow \qquad C_{12} = (-1)^{1+2} 7 = -3$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \qquad \Rightarrow \qquad C_{21} = (-1)^{2+1} 8 = -8$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \qquad \Rightarrow \qquad C_{22} = (-1)^{2+2} 11 = 11$$

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} = \begin{pmatrix} 7 & -3 \\ -8 & 11 \end{pmatrix}$$

$$\mathrm{adj}(A) = C^t = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix}$$

$$A^{-1} = |A|^{-1} \mathrm{adj}(A) \ .$$

$$|A|^{-1} = 1^{-1} = 1 \in \mathbb{Z}_{26}$$

לפיכך

$$A^{-1} = |A|^{-1} \mathrm{adj}(A) = 1 \cdot \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 22 \\ 23 & 11 \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2} \ .$$

■

דוגמה 2.8

מצאו את ההופכית של

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

פתרון:

$$|A| = 1 \cdot \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} + 0 \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} + 1 \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = 1 \cdot 15 + 1 \cdot (-10) = 5 \ .$$

$\gcd(15, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{11} = (-1)^{1+1} \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} = 15 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{12} = (-1)^{1+2} \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{13} = (-1)^{1+3} \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = -10 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{21} = (-1)^{2+1} \begin{vmatrix} 0 & 1 \\ 0 & 3 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 1 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 2 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{31} = (-1)^{3+1} \begin{vmatrix} 0 & 1 \\ 5 & 0 \end{vmatrix} = -5 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 0 \\ 0 & 5 \end{vmatrix} = 5 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 15 & 0 & -10 \\ 0 & 1 & 0 \\ -5 & 0 & 5 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 15 & 0 & -5 \\ 0 & 1 & 0 \\ -10 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 15 & 0 & 21 \\ 0 & 1 & 0 \\ 16 & 0 & 5 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

$$A^{-1} = |A|^{-1}\text{adj}(A) \ .$$

$$|A|^{-1} = 5^{-1} = 21 \in \mathbb{Z}_{26}$$

לפיכך

$$A^{-1} = |A|^{-1}\text{adj}(A) = 21 \cdot \begin{pmatrix} 15 & 0 & 21 \\ 0 & 1 & 0 \\ 16 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 315 & 0 & 441 \\ 0 & 21 & 0 \\ 336 & 0 & 105 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

$$315 \ \texttt{\%} \ 26 = 315 - 26 \cdot \left\lfloor \frac{315}{26} \right\rfloor = -23 \equiv 3 \mod 26 \qquad \Rightarrow \qquad 315 \equiv 3 \mod 26 \ .$$

$$441 \ \texttt{\%} \ 26 = 441 - 26 \cdot \left\lfloor \frac{441}{26} \right\rfloor = 25 \qquad \Rightarrow \qquad 441 \equiv 25 \mod 26 \ .$$

$$336 \ \texttt{\%} \ 26 = 336 - 26 \cdot \left\lfloor \frac{336}{26} \right\rfloor = 24 \qquad \Rightarrow \qquad 336 \equiv 24 \mod 26 \ .$$

$$105 \,\%\, 26 = 105 - 26 \cdot \left\lfloor \frac{105}{26} \right\rfloor = 1 \quad \Rightarrow \quad 105 \equiv 1 \mod 26 \ .$$

לפיכך

$$A^{-1} = \begin{pmatrix} 3 & 0 & 25 \\ 0 & 21 & 0 \\ 24 & 0 & 1 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

בדיקה:

$$A \cdot A^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 3 & 0 & 25 \\ 0 & 21 & 0 \\ 24 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 27 & 0 & 26 \\ 0 & 105 & 0 \\ 78 & 0 & 53 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mod 26 \ .$$

■

2.4 תמורות

הגדרה 2.7 תמורה

נתונה קבוצה מסודרת נוצר סופית $X = \{x_1, x_2, \ldots, x_n\}$ ללא חזרות. תמורה היא פונקציה חד-חד-ערכית ועל $\pi : X \to X$ שמקבלת X ומחזירה הקבוצה X ומשנה את הסדר של האיברים.

דוגמה 2.9

- תמורות של הקבוצה (a,b):

$$\pi_1(a,b) = (a,b) \ , \quad \pi_2(a,b) = (b,a) \ .$$

הראשון הוא מקרה פרטי של תמורה, אשר הוא פונקצית הזהות. קיימים $2!$ תמורות. תמורות.

- תמורות של הקבוצה (a,b,c):

$$\begin{aligned} &\pi_1(a,b,c) = (a,b,c) \ , \quad \pi_2(a,b,c) = (c,a,b) \ , \quad \pi_3(a,b,c) = (b,c,a) \ , \\ &\pi_4(a,b,c) = (b,a,c) \ , \quad \pi_5(a,b,c) = (a,c,b) \ , \quad \pi_6(a,b,c) = (c,b,a) \ . \end{aligned}$$

קיימים $3!$ תמורות.

- תמורות של הקבוצה $(\alpha,\beta,\gamma,\delta)$:

$$\pi_1(\alpha,\beta,\gamma,\delta) = (\delta,\alpha,\gamma,\beta) \ , \ldots$$

קיימים $4!$

- תמורות של הקבוצה (ד, ג, ב, א):

$$\pi_1(\text{א},\text{ב},\text{ג},\text{ד}) = (\text{ב},\text{א},\text{ג},\text{ד}) \ , \qquad \pi_2(\text{א},\text{ב},\text{ג},\text{ד}) = (\text{ב},\text{ג},\text{ד},\text{א}) \ , \ldots$$

קיימים $4!$ תמורות.

משפט 2.11

יהי X קבוצה מסודרת נוצר סופית ללא חזרות של אורך n.
קיימות $n!$ תמורות.

הוכחה: תרגיל בית. ■

הגדרה 2.8 סימון אינדקס של תמורה

יהי $X=(x_1,x_2,\ldots,x_n)$ ויהי $\pi:X\to X$ תמורה.
נניח שאחרי ביצוע של התמורה π על X, האיבר שהיה במיקום ה-i עכשיו במיקום ה-j ($1\leq i,j\leq n$).
אז אנחנו כותבים

$$\pi(i)=j\ .$$

הביטוי הזה נקרא **סימון אינדקס**.

דוגמה 2.10

א) נתונה התמורה

$$\pi(a,b)=(b,a)\ .$$

בסימון אינדקס,

$$\pi(1)=2\ ,\quad \pi(2)=1\ .$$

ב) נתונה התמורה

$$\pi(a,b,c)=(b,c,a)\ .$$

בסימון אינדקס,

$$\pi(1)=3\ ,\quad \pi(2)=1\ ,\quad \pi(3)=2\ .$$

ג) נתונה התמורה

$$\pi(\alpha,\beta,\gamma,\delta)=(\beta,\gamma,\delta,\alpha)\ .$$

בסימון אינדקס,

$$\pi(1)=4\ ,\quad \pi(2)=1\ ,\quad \pi(3)=2\ ,\quad \pi(4)=3\ .$$

הגדרה 2.9 הצגת שתי-שורות והצגת שורת-אחת

יהי $X=(x_1,x_2,\ldots,x_n)$ ויהי $\pi:X\to X$ תמורה שמוגדרת

$$\pi(X)=\left(x_{\pi(1)},x_{\pi(2)},\ldots,x_{\pi(n)}\right)\ .$$

- ההצגה שתי-שורות של התמורה הזאת הינה

$$\pi=\begin{pmatrix}1&2&\ldots&i&\ldots&n\\ \pi(1)&\pi(2)&\ldots&\pi(i)&\ldots&\pi(n)\end{pmatrix}$$

- ההצגה שורת-אחת של התמורה הזאת הינה

$$\pi=\begin{pmatrix}\pi(1)&\pi(2)&\ldots&\pi(i)&\ldots&\pi(n)\end{pmatrix}$$

דוגמה 2.11

א) נתונה התמורה
$$\pi(a,b)=(b,a)\ .$$

בסימון אינדקס: $\pi(1)=2\ ,\ \pi(2)=1.$

הצגת שתי-שורות: $\begin{pmatrix}1&2\\2&1\end{pmatrix}.$

הצגת שורה-אחת: $\begin{pmatrix}2&1\end{pmatrix}.$

ב) נתונה התמורה
$$\pi(a,b,c)=(b,c,a)\ .$$

בסימון אינדקס: $\pi(1)=3\ ,\ \pi(2)=1\ ,\ \pi(3)=2.$

הצגת שתי-שורות: $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$

הצגת שורה-אחת: $\begin{pmatrix}3&1&2\end{pmatrix}.$

ג) נתונה התמורה
$$\pi(\alpha,\beta,\gamma,\delta)=(\beta,\gamma,\delta,\alpha)\ .$$

בסימון אינדקס: $\pi(1)=4\ ,\quad \pi(2)=1\ ,\quad \pi(3)=2\ ,\pi(4)=3.$

הצגת שתי-שורות: $\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}.$

הצגת שורה-אחת: $\begin{pmatrix}4&1&2&3\end{pmatrix}.$

דוגמה 2.12 הרכבה של תמורות

תהיינה $\alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ ו- $\beta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$. חשבו את $\alpha\circ\beta$ ו- $\beta\circ\alpha$.

פתרון:

$$\alpha\circ\beta=\begin{pmatrix}1&2&3\\ \alpha\left(\beta(1)\right)&\alpha\left(\beta(2)\right)&\alpha\left(\beta(3)\right)\end{pmatrix}=\begin{pmatrix}1&2&3\\ \alpha\left(2\right)&\alpha\left(1\right)&\alpha\left(3\right)\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$
$$\beta\circ\alpha=\begin{pmatrix}1&2&3\\ \beta\left(\alpha(1)\right)&\beta\left(\alpha(2)\right)&\beta\left(\alpha(3)\right)\end{pmatrix}=\begin{pmatrix}1&2&3\\ \beta\left(2\right)&\beta\left(3\right)&\beta\left(1\right)\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

■

דוגמה 2.13