9. מבוא לתורת החבורות

בסעיף 1.3, עסקנו בקצרה בפעולות החשבון מודולו n. כזכור אנו אומרים ש- $a \equiv b(\bmod m)$ אם המספר (a–b) מתחלק ב- m ללא שארית. בעצם כולנו יודעים לחבר ולחסר מודולו 12. אם השעה כרגע היא 10 בבוקר, אנו יודעים שבעוד 5 שעות השעה תהיה 3 אחר הצהרים. במושגים מתמטיים, אמרנו בכך כי $10+5 \equiv 3(\bmod 12)$. אנו רוצים לשים כאן את הדגש על פעולת ה"חיבור" שראינו זה עתה. מצד אחד היא דומה מאוד לפעולת החיבור המוכרת לנו מאז ומתמיד, אך יש גם הבדלים. הרבה מן ההגדרות החשובות במתמטיקה מתקבלות על ידי כך שאנו מתבוננים במבנה מתמטי מוכר היטב, ומנסים למצות ממנו באופן מופשט את התכונות המרכזיות שלו. לאור הערה זו, הבה נתבונן במספרים השלמים ובפעולת החיבור ביניהם. מהן אבני הבניין העיקריות של המבנה המתמטי הבסיסי הזה? מדובר כאן בקבוצה $\mathbb{Z}$ ובפעולת החיבור + המוגדרת על איברי הקבוצה. יש בקבוצה זו איבר מיוחד הנקרא **אפס**, שפעולת החיבור איתו אינה משנה דבר. כמו-כן יש גם פעולה הופכית לפעולת החיבור, הלא היא פעולת החיסור. ולבסוף, פעולת החיבור היא אסוציאטיבית. כלומר, כאשר מחברים שלושה מחוברים זה לזה, אין זה משנה מהו הסדר שבו מתבצעות הפעולות.
לפני שניגש להגדרה הכללית של חבורה, עלינו לומר עוד במפורש למה אנו מתכוונים במילה **פעולה**. פעולת החיבור בין מספרים שלמים מתאימה לזוג איברים מ- $\mathbb{Z}$ איבר מסוים מ- $\mathbb{Z}$. לכן, פעולת החיבור במספרים שלמים אינה אלא פונקציה $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. כך למשל $f(-3,8) = 5$ מייצג את העובדה ש- $5 = 8 + (-3)$. דיון זה מביא אותנו אל ההגדרה של חבורה.

9.1. מושג החבורה

הנושאים שיוצגו: *חבורה, טבלת הפעולה של חבורה, החבורה הציקלית* $\mathbb{Z}_n$*, החבורה הכפלית* $\mathbb{Z}_n^*$*, חבורה קומוטטיבית.*

הגדרה 9.1.1: חבורה $(G,\bullet)$ מורכבת מקבוצה G ופעולה שתסומן ב- $\bullet$, ומקיימת את התכונות הבאות:

1. הפעולה $\bullet$ היא פונקציה מ- $G\times G$ אל G, כלומר לכל $x,y\in G$ מתקיים $x\bullet y\in G$.
2. הפעולה $\bullet$ **אסוציאטיבית**, כלומר לכל $x,y,z\in G$ מתקיים $(x\bullet y)\bullet z=x\bullet(y\bullet z)$.
3. בקבוצה G יש איבר מיוחד הנקרא **איבר היחידה** של G שיסומן ב- e, כך שלכל $x\in G$ מתקיים $e\bullet x=x\bullet e=x$.
4. לכל איבר $x\in G$ יש **איבר הופכי** ב- G שיסומן ב- x^{-1} ומקיים $x\bullet x^{-1}=x^{-1}\bullet x=e$.

נחזור ונביט בשתי הדוגמאות המוכרות לנו.

דוגמה 9.1.2: במקרה של המספרים השלמים, מקובל כמובן להשתמש בסימון + במקום ב- $\bullet$. איבר היחידה הוא $0\in\mathbb{Z}$. ואת האיבר ההופכי של x מקובל לסמן ב- $-x$. נסמן חבורה זו ב- $(\mathbb{Z},+)$.

דוגמה 9.1.3 (חיבור מודולו 12): כאן הקבוצה היא $G=\{0,1,\ldots,11\}$, המסומנת לרוב על ידי $\mathbb{Z}_{12}$. איבר היחידה הוא שוב 0. הפעולה היא פעולת החיבור מודולו 12, והיא תסומן על ידי $+_{12}$. כך למשל, $5+_{12}8=1$ כי $5+8\equiv 1(\mathrm{mod}\,12)$. באופן כללי יתקיים $a+_n b=c$ אם $a+b\equiv c(\mathrm{mod}\,n)$. מה בדבר פעולת ההופכי? גם כאן נסמן את ההופכי של x על ידי $-x$. כך למשל בחבורה זו ההופכי של 5 הוא 7, כי $5+_{12}7=0$.

סימון מקובל לחבורה זו הוא $(\mathbb{Z}_{12},+_{12})$. בניגוד לחבורה $(\mathbb{Z},+)$, החבורה $(\mathbb{Z}_{12},+_{12})$ היא סופית. מסיבה זו אפשר לתאר את החבורה הזאת בעזרת **טבלת הפעולה** שלה.

$+_{12}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

מהטבלה נוח לראות למשל ש- $-3=9$, וזאת מכיוון ש- $9+_{12}3=0$.

אין קושי להכליל את הדוגמה לחבורה $\mathbb{Z}_n$ של החיבור מודולו n, עבור n כלשהו. כך לדוגמה בחבורה $(\mathbb{Z}_{14},+_{14})$ מתקיים $-5=9$ וזה מפני ש- $5+9\equiv 0(\mathrm{mod}\,14)$.

הגדרה 9.1.4: החבורה $(\mathbb{Z}_n, +_n)$ נקראת גם **החבורה הציקלית מסדר n**.

חבורות כפליות

האם ניתן לבנות דוגמאות דומות גם תוך שימוש בפעולת הכפל המוכרת לנו? נחזור שוב אל המספרים השלמים. האם הם מהווים חבורה גם עם פעולת הכפל? בטרם ניתן את התשובה (השלילית), נברר מהו כאן איבר היחידה. דהיינו, מהו המספר e המקיים $e \cdot x = x$? זהו כמובן המספר 1. לכן, אם $\mathbb{Z}$ חבורה ביחס לפעולת הכפל, אז איבר היחידה הוא בהכרח 1. אבל עתה קל לראות ש- $\mathbb{Z}$ אינה חבורה ביחס לפעולת הכפל, מפני שאין בה הופכי כדרוש. כך למשל, ההופכי למספר $7 \in \mathbb{Z}$ הוא מספר שלם x המקיים $7 \cdot x = 1$. כמובן שאין מספר שלם כזה. קושי חמור יותר נובע מן הצורך למצוא הופכי למספר $0 \in \mathbb{Z}$, ולכן 0 אינו יכול להיות איבר בחבורה עם פעולת הכפל. קשיים אלה מוליכים באופן טבעי להגדרת המספרים הרציונאליים. כך למשל קל לבדוק שהמספרים הרציונאליים השונים מ- 0 מהווים חבורה ביחס לפעולת הכפל (ראו תרגיל 1).

במקרה של פעולת החיבור, ראינו מלבד החבורה $(\mathbb{Z}, +)$ גם חבורות סופיות דומות, הלא הן $(\mathbb{Z}_n, +_n)$. האם $\mathbb{Z}_n$ היא חבורה גם ביחס לפעולת הכפל מודולו n? נעיין בבעיה. שוב איבר היחידה חייב להיות 1. כמו בדיון שלנו במספרים הרציונאליים, גם כאן עלינו לפסול את 0, אבל פסילה זו גוררת מסקנות נוספות. כך למשל, אם ננסה להגדיר חבורה עם פעולת הכפל על איברי הקבוצה $\mathbb{Z}_{12} \setminus \{0\}$, אז גם העובדה ש- $3 \cdot 4 \equiv 0 \pmod{12}$ יוצרת לנו בעיה. הרי אם 3 ו- 4 הם איברים של החבורה, אז בהכרח גם התוצאה $3 \cdot 4$ צריכה להיות איבר בחבורה. אולם, כאמור, 0 אינו יכול להיות איבר בחבורה. באופן דומה נפסלים כל האיברים ב- $\mathbb{Z}_{12}$ שיש להם גורם משותף עם 12. כך למשל, ל- 8 גורם משותף עם 12, ואכן $8 \cdot 3 \equiv 0 \pmod{12}$. נותרים לכן רק האיברים הזרים ל- 12, דהיינו 1, 5, 7, 11 (כזכור, שני מספרים זרים אם המחלק המשותף המקסימלי שלהם הוא 1, ראו הגדרה 4.6.8).

דוגמה 9.1.5: נראה שהקבוצה $\{1,5,7,11\}$ היא חבורה ביחס לפעולת הכפל מודולו 12. הפעולה תסומן במקרה זה על ידי $\bullet_{12}$. נבנה תחילה את טבלת הפעולה של החבורה.

$\bullet_{12}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

כך למשל $7 \cdot 11 \equiv 5 \pmod{12}$. ניתן לראות מהטבלה שהאיבר 1 הוא אכן איבר היחידה של החבורה. באופן דומה קל לוודא שלכל איבר יש הופכי. כך למשל, $7 = 7^{-1}$, ואכן $7 \cdot 7 \equiv 1 \pmod{12}$. לכן הטבלה אכן מתארת חבורה.

הדוגמה הזו היא כללית, ולכל מספר טבעי n, ניתן להגדיר חבורה שאיבריה הם קבוצת כל המספרים הטבעיים $1 \le k \le n-1$ הזרים ל- n, והפעולה היא כפל מודולו n. במקרה זה תסומן הפעולה על ידי $\bullet_n$ והקבוצה על ידי $\mathbb{Z}_n^*$, כלומר:

$$\mathbb{Z}_n^* = \{k \mid 1 \le k \le n-1 \text{ ,זרים } k,n\}$$

ואילו $a \bullet_n b = c$ אם $a \cdot b \equiv c (\bmod n)$.

בפרק 4 חישבנו את מספרם של המספרים הטבעיים בין 1 ל- $(n-1)$ הזרים ל- n (משפט 4.6.10). התשובה ניתנה באמצעות פונקצית אוילר $\phi(n)$. שימו לב שאם n ראשוני אז כל המספרים הקטנים מ- n זרים לו, ולכן במקרה זה $\mathbb{Z}_n^* = \{1,2,...,n-1\}$.

הגדרה 9.1.6: החבורה $\left(\mathbb{Z}_n^*, \bullet_n\right)$ נקראת **החבורה הכפלית מודולו n**.

לכל החבורות שנדונו עד עתה הייתה תכונה חשובה משותפת: הן קומוטטיביות. פירוש הדבר הוא שבדוגמאות הקודמות אם x,y איברים של החבורה G אז $x \bullet y = y \bullet x$.

הגדרה 9.1.7: תהי $(G,\bullet)$ חבורה. אם לכל $x,y \in G$ מתקיים $x \bullet y = y \bullet x$, אז הפעולה • היא **חילופית** או **קומוטטיבית**. במקרה זה נאמר שהחבורה קומוטטיבית.

זו בהחלט איננה תכונה הנדרשת מחבורה, ולאמיתו של דבר חבורות קומוטטיביות סופיות הן מוגבלות למדי. עיקר עושרה של תורת החבורות בא מהעיסוק בחבורות לא קומוטטיביות, כפי שנראה בסעיף הבא.

תרגילים

1. הוכיחו שהמספרים הרציונאליים החיוביים הם חבורה ביחס לפעולת הכפל.
2. בנו את טבלת הפעולה של החבורה הכפלית $\mathbb{Z}_{18}^*$.
3. בנו את טבלת הפעולה של החבורה הכפלית $\mathbb{Z}_7^*$.

9.2. חבורות וסימטריה

הנושאים שיוצגו: *החבורה הסימטרית* S_n*, חבורת הסימטריות של הארבעון, תת-חבורה, חבורה הפועלת על קבוצה, איזומורפיזם בין חבורות.*

כיצד נבנה חבורות לא קוממוטיביות? גם כאן נתחיל ממבנה קלאסי ומוכר היטב. כמובן ביסודה של כל חבורה מצויה פעולה. ניזכר בפעולת **ההרכבה** של פונקציות (ראו סעיף 1.4). אם $f: A \to B$ ו- $g: B \to C$ פונקציות, אז כזכור הפונקציה $g \circ f: A \to C$ היא ההרכבה שלהן,

והיא מוגדרת על ידי $g \circ f(a) = g(f(a))$ לכל $a \in A$. זו אכן פעולה, אך הפעולה בחבורה צריכה כזכור להתאים לכל $x,y \in G$ איבר $x \bullet y$ ב- G, ואילו כאן הפונקציות f,g שייכות לקבוצות שונות. הפונקציה f שייכת לאוסף כל הפונקציות מ- A ל- B, בעוד שהפונקציה g שייכת לאוסף כל הפונקציות מ- B ל- C. לכן, נראה שיהיה עלינו להניח ש- $A = B = C$ על מנת לממש את תוכניתנו.
לא קשה לראות מי אמור להיות איבר היחידה בחבורה שאנו מנסים לבנות. אנו נבחר את e כפונקציית הזהות מ- A ל- A המוגדרת על ידי $e(x) = x$ לכל $x \in A$. אין קושי לברר שלכל פונקציה $f : A \to A$ מתקיים $e \circ f = f \circ e = f$, כנדרש מאיבר היחידה של חבורה.
הדיון מוביל אותנו באופן ישיר להגדרה המתבקשת של האיבר ההופכי. האיבר ההופכי לפונקציה f, איננו אלא הפונקציה ההופכית של f. מכאן מתבררת מיד עובדה נוספת: עלינו להגביל את הדיון לפונקציות $f : A \to A$ שהן חח"ע (ולכן גם על, כי A קבוצה סופית).
תהי A קבוצה סופית, ונניח ש- $A = \{1,\dots,n\}$. כזכור, פונקציה חח"ע ועל מ- A לעצמה, אינה אלא תמורה של $\{1,\dots,n\}$ (ראו משפט 4.2.7 והדיון בעקבותיו). נזכיר שאנו מציינים תמורה π על ידי סדרת המספרים $(\pi(1), \pi(2),\dots, \pi(n))$. הגענו אם כן אל ההגדרה המבוקשת.

הגדרה 9.2.1: החבורה $(S_n, \circ)$ נקראת **החבורה הסימטרית מסדר n**, או **חבורת התמורות**. איברי החבורה S_n הם כל $n!$ התמורות של $\{1,\dots,n\}$, והפעולה היא פעולת ההרכבה של פונקציות.

דוגמה 9.2.2: נתבונן בחבורה $(S_3, \circ)$. בחבורה זו יש $3! = 6$ איברים, וטבלת הפעולה היא כדלקמן. לשם פשטות נסמן תמורה ללא הסוגריים.

∘	**123**	**132**	**213**	**231**	**312**	**321**
123	123	132	213	231	312	321
132	132	123	312	321	213	231
213	213	231	123	132	321	312
231	231	213	321	312	123	132
312	312	321	132	123	231	213
321	321	312	231	213	132	123

כך למשל, אם $\sigma = (2,3,1)$ ו- $\pi = (2,1,3)$ אז $\sigma \circ \pi = (3,2,1)$ מפני ש-

$$\sigma(\pi(1)) = \sigma(2) = 3$$
$$\sigma(\pi(2)) = \sigma(1) = 2$$
$$\sigma(\pi(3)) = \sigma(3) = 1$$

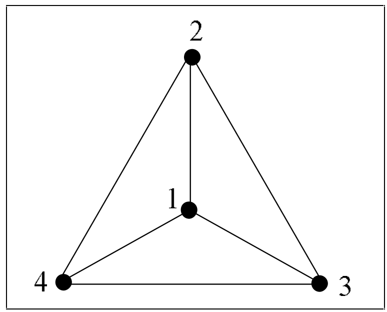
החבורה הזו אינה קומוטטיבית. כך למשל, $\sigma \circ \pi \neq \pi \circ \sigma$ כי ראינו ש- $\sigma \circ \pi = (3,2,1)$, ואילו

$$\pi \circ \sigma = (2,1,3) \circ (2,3,1) = (1,3,2).$$

חבורות וסימטריה גיאומטרית

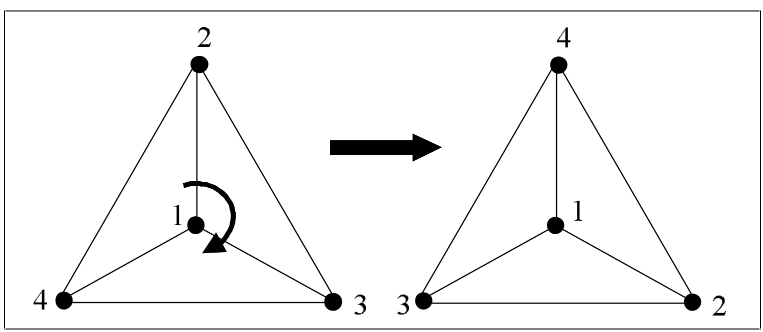
עד כה דנו בעיקר בשתי משפחות של חבורות: החבורות הציקליות $\mathbb{Z}_n$ והחבורות הסימטריות S_n. נרצה לדון עתה בעוד דוגמה שתאפשר לנו להאיר היבט חשוב של תורת החבורות, אשר מתקשר גם לבעיות מניה ולשאלות אחרות במתמטיקה בדידה.

נתבונן בארבעון משוכלל (פירמידה משוכללת הקרויה גם **סימפלקס** תלת-ממדי). לארבעון יש ארבעה קדקודים שאותם נסמן ב- $\{1,2,3,4\}$. בתרשים 9.2.1 אפשר לראות את הארבעון במבט מלמעלה.



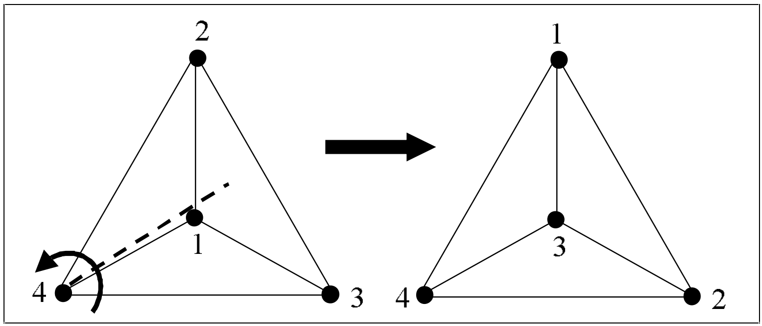
תרשים 9.2.1: הארבעון במבט מלמעלה.

נרצה לחקור את אוסף כל התמורות של $\{1,2,3,4\}$ המתקבלות מסיבובים קשיחים של הארבעון. כך למשל, אם נסובב את הארבעון סיבוב של 120° בכיוון השעון, על ציר העובר דרך הקדקוד 1 וניצב למישור הדף, נקבל את המצב המתואר בתרשים 9.2.2. התמורה שמשרה סיבוב זה על הקדקודים היא $(1,3,4,2)$.



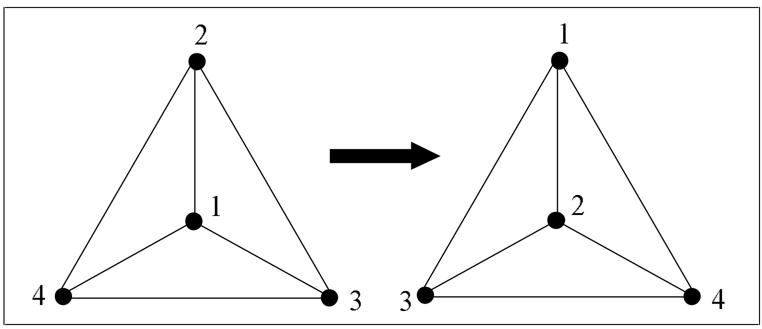
תרשים 9.2.2: סיבוב הארבעון ב- 120° על ציר העובר דרך הקדקוד 1.

נחזור למצב היסודי של הארבעון בתרשים 9.2.1, ונסובב אותו עתה 120° נגד כיוון השעון, על ציר העובר דרך הקדקוד 4 ודרך אמצע הפיאה 1,2,3. תרשים 9.2.3 מתאר את התוצאה. במקרה זה התקבלה התמורה $(2,3,1,4)$.



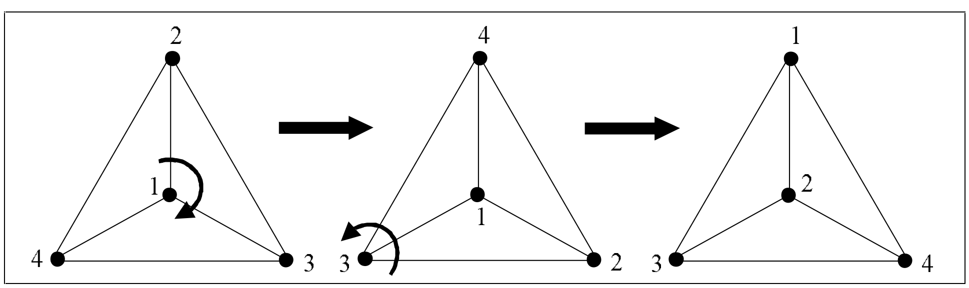
תרשים 9.2.3: סיבוב הארבעון ב- 120° על ציר העובר דרך הקדקוד 4 ואמצע הפיאה 1,2,3.

הבה נחשב את ההרכבה של שתי התמורות: $(1,3,4,2)\circ(2,3,1,4)=(2,1,4,3)$. כיצד זה מתבטא בארבעון שלנו? הנה:



תרשים 9.2.4: הרכבה של שני הסיבובים.

וביתר פירוט על ידי שילוב שני הסיבובים:



תרשים 9.2.5: תיאור ההרכבה של שני הסיבובים.

כל הזזה קשיחה המחזירה את הארבעון למקומו, משרה אם כן תמורה על ארבעת הקדקודים. אוסף התמורות המתקבלות כך הוא חבורה, מפני שהרכבה של שתי הזזות קשיחות אף היא הזזה קשיחה. לפנינו חבורה של תמורות על $\{1,2,3,4\}$ שאותה תיארנו במונחים גיאומטריים (של הזזות קשיחות). אנו נקרא לחבורה זו **חבורת הסימטריות של הארבעון** וננסה להבין כעת מהי חבורה זו.

עד כה תיארנו חבורה רק באמצעות טבלת הפעולה שלה. נתחיל אם כן בניסיון למצוא את רשימת כל התמורות המתקבלות כך על $\{1,2,3,4\}$. אנו טוענים שמספר התמורות המבוקשות הוא בדיוק 12. על מנת לתאר את מצבו של הארבעון המונח על מישור הדף, עלינו לומר מיהו הקדקוד הבולט מעל המישור, ואותו ניתן לבחור ב- 4 דרכים. עתה ניתן לסובב את הארבעון ב- 3 אופנים (ובמילים אחרות, ניתן לבחור מי משלוש הצלעות של בסיס המשולש פונה לחזית). מדובר לכן ב- $3\cdot 4 = 12$ תמורות. להלן רשימת כל התמורות האלה:

$$\begin{array}{cccccc}(1,2,3,4) & (1,3,4,2) & (1,4,2,3) & (2,1,4,3) & (2,3,1,4) & (2,4,3,1)\\ (3,1,2,4) & (3,2,4,1) & (3,4,1,2) & (4,1,3,2) & (4,2,1,3) & (4,3,2,1)\end{array}$$

אין כעת כל צורך בחישוב מפורש של טבלת הפעולה. התמורות שלעיל הן תמורות בחבורה S_4, והפעולה ביניהן היא הרכבה של תמורות. במילים אחרות, טבלת הפעולה של חבורת הסימטריות של הארבעון היא פשוט חלק מטבלת הפעולה של החבורה הסימטרית $(S_4,\circ)$. במינוח המקובל חבורה זו היא **תת-חבורה** של S_4. פורמלית נגדיר זאת כך.

הגדרה 9.2.3: תהי $(G,\bullet)$ חבורה, ותהי $H \subseteq G$ קבוצה חלקית כלשהי של G. נאמר ש- H **תת-חבורה** של G אם גם $(H,\bullet)$ חבורה.

מרכיב עיקרי בפיתוח של תורת החבורות הוא מתן תיאור של רשימת התת-חבורות של כל חבורה שדנים בה. דיון כזה הוא מעבר לגבולותיו של ספר זה, והוא נעשה בקורסים מתקדמים יותר באלגברה המוקדשים לתורת החבורות.

נחזור ונעיין בחבורת הסימטריות של הארבעון. חבורה זו הוגדרה במונחים גיאומטריים, אולם נוח היה לנו לחשוב עליה כחבורת תמורות חלקית ל- S_4. המינוח המקובל הוא שזו חבורה **הפועלת** על הקבוצה $X = \{1,2,3,4\}$. ההגדרה הבאה עוסקת במקרה הכללי.

הגדרה 9.2.4: תהי X קבוצה ויהי G אוסף של פונקציות חח״ע $\pi : X \to X$ כך שמתקיימים:

1. האוסף G **סגור להופכי**: אם $\pi \in G$ אז גם הפונקציה ההופכית π^{-1} שייכת ל- G.
2. האוסף G **סגור להרכבה**: אם $\pi,\sigma \in G$ אז גם פונקצית ההרכבה $\pi\circ\sigma : X \to X$ שייכת ל- G.

במקרה זה נאמר ש- G **חבורה הפועלת על הקבוצה** X.

הדוגמאות שבחנו עד כה נראו שונות למדי. החבורה הציקלית $\mathbb{Z}_n$ מוגדרת בעזרת פעולה הדומה לפעולת החיבור המוכרת לנו. החבורה הסימטרית S_n, וחבורות תמורות בכלל (שהן תת-חבורות

של S_n), מוגדרות בעזרת פעולת ההרכבה בין תמורות. חבורת הסימטריות של הארבעון מוגדרת בעזרת טרנספורמציות גיאומטריות. אנו נוכיח עתה שניתן לראות כל חבורה סופית G כחבורה של תמורות, ולפיכך גם כחבורה G הפועלת על קבוצה X. בטרם ניגש לניסוח המשפט ולהוכחתו, עלינו להגדיר מתי נאמר ששתי חבורות G_1,G_2 זהות זו לזו. אינטואיטיבית, נרצה לומר ש- G_1,G_2 זהות, אם G_2 מתקבלת מ- G_1 פשוט על ידי שינוי שמות האיברים ב- G_1 ותו לא. פורמלית נגדיר זאת כך:

הגדרה 9.2.5: יהיו $(G_1,\bullet_1)$, $(G_2,\bullet_2)$ שתי חבורות סופיות. נאמר שהן **איזומורפיות** אם יש פונקציה $f:G_1\to G_2$ כך שמתקיים:

1. f חח"ע ועל.
2. f שומרת על הופכי: לכל $a\in G_1$ מתקיים $f(a^{-1})=\left(f(a)\right)^{-1}$.
3. f שומרת על הפעולה: לכל $a,b\in G_1$ מתקיים $f(a\bullet_1 b)=f(a)\bullet_2 f(b)$.

פונקציה f כנ"ל נקראת **איזומורפיזם** בין G_1 ל- G_2.

נחזור לרגע להסבר האינטואיטיבי שנתנו מקודם: אם a איבר כלשהו ב- G_1, אז הוא קיים גם בחבורה G_2, אבל שם הוא מכונה f(a).

נשים לב שכל חבורה סופית G איזומורפית לעצמה כמובן, מפני שפונקציית הזהות $e:G\to G$ המוגדרת על ידי $e(a)=a$ לכל $a\in G$, היא איזומורפיזם. בתרגיל 2 נראה שניתן לפעמים למצוא גם פונקציות אחרות שהן איזומורפיזם מ- G לעצמה.

הגדרה 9.2.6: איזומורפיזם מ- G לעצמה נקרא **אוטומורפיזם**.

משפט 9.2.7: כל חבורה סופית $(G,\bullet)$ איזומורפית לחבורת תמורות.

הוכחה: רעיון ההוכחה פשוט ביותר. לכל איבר $a\in G$ נתאים את הפונקציה $\pi_a:G\to G$ המוגדרת באמצעות $\pi_a(x)=a\bullet x$. כלומר, הפונקציה π_a מעתיקה כל איבר $x\in G$ לאיבר $a\bullet x\in G$. נוכיח תחילה שהפונקציה π_a חח"ע ועל:

א. π_a חח"ע: נניח כי $\pi_a(x)=\pi_a(y)$. לכן, $a\bullet x=a\bullet y$. נכפיל את שני אגפי השוויון בהופכי של a ונקבל $x=a^{-1}\bullet a\bullet x=a^{-1}\bullet a\bullet y=y$.

ב. π_a על: בעצם אין מה להוכיח, מפני ש- π_a פונקציה חח"ע מקבוצה סופית G לעצמה, ולפיכך היא בהכרח גם על. אולם נוכיח זאת גם באופן ישיר. ואכן, בהינתן איבר $y\in G$, נרצה למצוא $x\in G$ כך ש- $\pi_a(x)=y$. קל לראות ש- $x=a^{-1}\bullet y$ הוא איבר כזה, כי $\pi_a(x)=a\bullet x=a\bullet a^{-1}\bullet y=y$ כנדרש.

הראינו ש- π_a חח"ע ועל, ולכן π_a היא תמורה של איברי הקבוצה G.

נראה כעת שאוסף התמורות $P=\{\pi_a\mid a\in G\}$ עם פעולת ההרכבה, הוא חבורה איזומורפית ל- G. כדי להוכיח זאת נראה שהפונקציה $f:G\to P$ המוגדרת על ידי $f(a)=\pi_a$ היא

איזומורפיזם בין G ל- P. לא קשה לבדוק ש- f חח״ע ועל. אכן, הפונקציה f על, כי התאמנו לכל $a\in G$ פונקציה π_a. כדי לוודא ש- f חח״ע נראה כי $\pi_a \neq \pi_b$ לכל $a \neq b$. יהי e איבר היחידה של החבורה G. אז:

$$\pi_a(e) = a \bullet e = a \neq b = b \bullet e = \pi_b(e).$$

כלומר, הפונקציות π_a, π_b אינן מסכימות על איבר היחידה e, ולכן הן שונות כנדרש. עלינו לבדוק עוד שני תנאים:

א. f משמרת הופכי: עלינו להוכיח כי $f(a^{-1}) = \left(f(a)\right)^{-1}$, כלומר ש- $\pi_{a^{-1}} = \left(\pi_a\right)^{-1}$. על מנת לבדוק ששתי הפונקציות $\pi_{a^{-1}}$ ו- $\left(\pi_a\right)^{-1}$ זהות, יש להראות שהן מתלכדות על כל איבר $x\in G$. ואכן, $\pi_{a^{-1}}(x) = a^{-1} \bullet x$. נניח כי $\left(\pi_a\right)^{-1}(x) = y$. לכן $\pi_a(y) = x$, כלומר $a \bullet y = x$. על ידי הכפלת השוויון האחרון ב- a^{-1}, נקבל $y = a^{-1} \bullet a \bullet y = a^{-1} \bullet x$. לכן $\left(\pi_a\right)^{-1}(x) = y = a^{-1} \bullet x = \pi_{a^{-1}}(x)$ כדרוש.

ב. f משמרת את הפעולה: עניין זה ינבע מהאסוציאטיביות של הפעולה בחבורות. עלינו להוכיח כי $f(a \bullet b) = f(a) \circ f(b)$, כלומר ש- $\pi_{a\bullet b} = \pi_a \circ \pi_b$, כאשר $\pi_a \circ \pi_b$ היא ההרכבה של שתי התמורות הנ״ל (אנו מדגישים כי $\bullet$ מציין את הפעולה של החבורה G, בעוד ש- $\circ$ מציין הרכבה של תמורות). כמקודם, יהי $x\in G$ איבר כלשהו, ונראה ש- $\pi_{a\bullet b}(x) = \pi_a \circ \pi_b(x)$. מצד אחד:

$$\pi_a \circ \pi_b(x) = \pi_a\left(\pi_b(x)\right) = \pi_a\left(b \bullet x\right) = a \bullet \left(b \bullet x\right).$$

מצד שני $\pi_{a\bullet b}(x) = \left(a \bullet b\right) \bullet x$, ושני הביטויים זהים בגלל האסוציאטיביות של $\bullet$.

הוכחנו ש- f איזומורפיזם בין G ל- P. □

דוגמה 9.2.8: נראה למשל איך החבורה הציקלית $\mathbb{Z}_n$ מיוצגת כחבורת תמורות. נוח יהיה לראות את $\mathbb{Z}_n$ כחבורת תמורות של $\{0,1,\ldots,n-1\}$. ואכן לכל איבר $a \in \mathbb{Z}_n$ מתאימה התמורה π_a המוגדרת על ידי $\pi_a(x) = a +_n x = (a + x) \bmod n$ לכל $x\in\{0,1,\ldots,n-1\}$.

תרגילים

1. יהיו G_1,G_2 חבורות סופיות איזומורפיות, ותהי f איזומורפיזם ביניהן. יהיו $e_1\in G_1$, $e_2\in G_2$ איברי היחידה של החבורות.
   א. הוכיחו כי $f(e_1) = e_2$.
   ב. הוכיחו כי הפונקציה ההופכית $f^{-1}: G_2 \to G_1$ גם היא איזומורפיזם.

2. תהי $(G,\bullet)$ חבורה סופית ויהי $a\in G$ איבר כלשהו. נביט בפונקציה $f: G \to G$ המוגדרת על ידי $f(x) = a \bullet x \bullet a^{-1}$. הוכיחו ש- f אוטומורפיזם של G. לאוטומורפיזם כזה אנו קוראים **הצמדה** ב- a.

3. מצאו אוטומורפיזם של S_3 השונה מהעתקת הזהות.

4. תהי $(G,\bullet)$ חבורה ו- $H \subseteq G$. הוכיחו ש- H תת-חבורה אם ורק אם מתקיים:
   א. H סגורה לפעולה: אם $x,y \in H$ אז גם $x \bullet y \in H$.
   ב. H סגורה להופכי: אם $x \in H$ אז גם $x^{-1} \in H$.

5. אפיינו את כל התת-חבורות של החבורה הציקלית $\mathbb{Z}_n$.

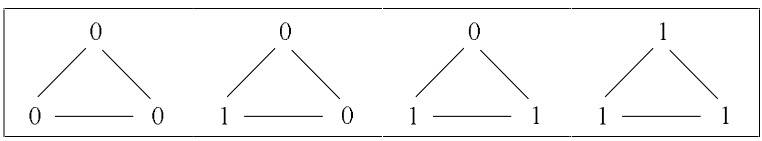
9.3. מסלולים ומחרוזות מעגליות

הנושאים שיוצגו: *מחרוזת מעגלית, מסלול, המשפט הקטן של פרמה, משפט ברנסייד*.

ניגש עתה לדון בבעיית מנייה קונקרטית שפתרונה יצריך שימוש במושגים שלמדנו על חבורות.

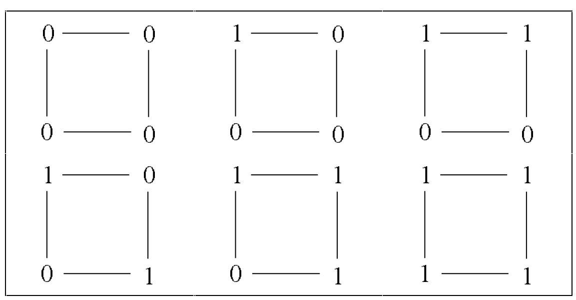
בעיה: מהו מספרן של המחרוזות המעגליות באורך n הבנויות מאפסים ואחדים?

באופן ציורי יותר אפשר לתאר זאת כך: יש לנו מאגר בלתי מוגבל של חרוזים מכסף ומזהב. כמה מחרוזות שונות מאורך n ניתן לבנות מהן? למשל, כש- $n = 3$ התשובה היא 4 כפי שאפשר לראות בתרשים 9.3.1.



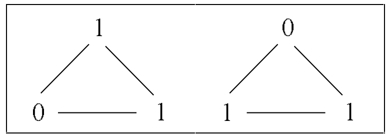
תרשים 9.3.1: המחרוזות המעגליות באורך 3.

ואילו כש- $n = 4$ מספר המחרוזות הוא 6 כפי שאפשר לראות בתרשים 9.3.2.



תרשים 9.3.2: המחרוזות המעגליות באורך 4.

שימו לב ששתי מחרוזות הן זהות אם הן מתקבלות זו מזו על ידי סיבוב. כך למשל, המחרוזות הבאות מאורך 3 הן זהות:



תרשים 9.3.3: שתי מחרוזות זהות באורך 3.

במהלך פתרון הבעיה אנו נפתח כלים נוספים שיועילו גם בהקשרים אחרים. האבחנה הראשונה היא שאותה החבורה G יכולה לפעול על קבוצות שונות. בהקשר של הבעיה שלנו אנו נגדיר פעולה של החבורה הציקלית $\mathbb{Z}_n$ על הקבוצה $X = \{0,1\}^n$ של כל הסדרות באורך n של אפסים ואחדים. נפתח בתיאור אינטואיטיבי של פעולה זו. האיבר $j \in \mathbb{Z}_n$ פועל על סדרה $(x_1,\ldots,x_n) \in X$ על ידי סיבובה שמאלה j מקומות. כלומר, לכל איבר $0 \le j \le n-1$ של החבורה הציקלית $\mathbb{Z}_n$, נתאים את הפונקציה π_j המוגדרת על ידי

$$\pi_j(x_1,\ldots,x_n) = (x_{j+1}, x_{j+2}, \ldots, x_n, x_1, x_2, \ldots, x_j) \,.$$

לרוב נרשום זאת בקיצור על ידי $\pi_j(x_1,\ldots,x_n) = (x_{j+1}, x_{j+2}, \ldots, x_j)$, ונחשב את האינדקסים של הסדרה שמימין מודולו n. כלומר האיבר ה- i בסדרה $(x_{j+1}, x_{j+2}, \ldots, x_j)$ הוא $x_{(j+i) \bmod n}$.

הערה: מכאן ועד סוף הפרק יהיה לנו נוח לשנות מעט את הסימונים בפעולת החיבור מודולו n בציון האינדקסים של הסדרות. במקום לעבוד עם הערכים $0,1,\ldots,n-1$ מודולו n, אנו נעבוד עם הערכים $1,2,\ldots,n$. השוני היחיד למעשה הוא שבמקום 0 נרשום n, מה שאינו משנה שהרי $n \equiv 0 \pmod n$. כך נוכל להמשיך ולציין קואורדינטות בסדרה $(x_1,\ldots,x_n)$ על ידי $1,2,\ldots,n$ כמקובל (ולא על ידי האינדקסים $0,1,\ldots,n-1$).

דוגמה 9.3.1: כש- $n = 7$ הפונקציה π_3 מקיימת $\pi_3(0,1,1,0,0,0,1) = (0,0,0,1,0,1,1)$. קל גם לראות שהפונקציה π_0 היא פונקצית הזהות, ואילו הפונקציות π_3, π_4 הופכיות זו לזו. כך למשל:

$$\pi_4(0,0,0,1,0,1,1) = (0,1,1,0,0,0,1)$$

באופן כללי, הפונקציה ההופכית של π_j, כאשר $j \neq 0$, היא: $\pi_j^{-1} = \pi_{n-j}$. ואילו ההרכבה של פונקציות אלה מוגדרת על ידי $\pi_k \circ \pi_j = \pi_{(j+k) \bmod n}$. למשל, $\pi_3 \circ \pi_4 = \pi_{(3+4) \bmod 7} = \pi_0$, כלומר ההרכבה של הפונקציות π_3, π_4 היא פונקצית הזהות π_0 (כפי שאכן אמור להיות כשמרכיבים פונקציה עם ההופכי שלה). ואילו $\pi_3 \circ \pi_2 = \pi_{(2+3) \bmod 7} = \pi_5$.

משפט 9.3.2: נתבונן בקבוצת כל הפונקציות האלה $A=\{\pi_j \mid 0\le j\le n-1\}$, ונגדיר פונקציה $f:\mathbb{Z}_n\to A$ על ידי $f(j)=\pi_j$. הפונקציה f היא איזומורפיזם בין $(\mathbb{Z}_n,+_n)$ ל- $(A,\circ)$.

הוכחה: השלימו את ההוכחה! יש להראות ש- f חח״ע ועל, וכן שההופכי והפעולה נשמרות על ידי f. הקבוצה A עם הפעולה $\circ$ היא לכן חבורה הפועלת על $X=\{0,1\}^n$, והיא איזומורפית לחבורה הציקלית $\mathbb{Z}_n$. □

נשים לב שהפעולה של $\mathbb{Z}_n$ (ושל A) על $X=\{0,1\}^n$, משרה יחס שקילות על X.

הגדרה 9.3.3: נאמר ש- $(x_1,...,x_n),(y_1,...,y_n)$ הם איברים **שקולים** ב- X, ונסמן זאת על ידי $(x_1,...,x_n)\sim(y_1,...,y_n)$, אם יש $0\le j\le n-1$ כך ש- $\pi_j(x_1,...,x_n)=(y_1,...,y_n)$.

משפט 9.3.4: היחס ~ הוא יחס שקילות.

הוכחה: עלינו להראות שהיחס רפלקסיבי, סימטרי וטרנזיטיבי.

היחס רפלקסיבי: מתקיים $\pi_0(x_1,...,x_n)=(x_1,...,x_n)$.

היחס סימטרי: ואכן אם $\pi_j(x_1,...,x_n)=(y_1,...,y_n)$ אז

$$\pi_{n-j}(y_1,...,y_n)=\pi_j^{-1}(y_1,...,y_n)=(x_1,...,x_n).$$

היחס טרנזיטיבי: אם $\pi_j(x_1,...,x_n)=(y_1,...,y_n)$ ו- $\pi_k(y_1,...,y_n)=(z_1,...,z_n)$ אז

$$\pi_k\circ\pi_j=\pi_{(j+k)\bmod n}(x_1,...,x_n)=(z_1,...,z_n).$$

לכן זהו יחס שקילות. □

הערה: בטרם נמשיך בפתרון בעיית המחרוזות המעגליות, נעיר שהחלק האחרון של הדיון שלנו תקף גם בהקשר כללי יותר. אם G חבורה סופית הפועלת על קבוצה X, אז מושרה יחס שקילות על איברי X באופן הבא: $x\sim y$ אם יש $\pi\in G$ כך ש- $\pi(x)=y$. כמקודם זהו יחס סימטרי כי $\pi^{-1}(y)=x$ וגם $\pi^{-1}\in G$ (יש הופכי ב- G). היחס גם טרנזיטיבי כי אם $\pi(x)=y,\ \sigma(y)=z$ אז $\sigma\circ\pi(x)=z$ (כי G סגורה להרכבה).

כזכור, בסעיף 1.3 ראינו שיחס שקילות על קבוצה X, מחלק את X למחלקות שקילות. במקרה שלנו, מחלקות השקילות קרויות **מסלולים** (orbits). ההגדרה הבאה מסכמת את דיוננו עד כה.

הגדרה 9.3.5: תהי G חבורה סופית הפועלת על קבוצה X, ויהי ~ יחס שקילות על איברי X המוגדר על ידי $x\sim y$ אם יש $\pi\in G$ כך ש- $\pi(x)=y$. מחלקות השקילות של היחס ~ נקראות **מסלולים**.

אפשר לנסח מספר גדול של בעיות קומבינטוריות חשובות במונחים של חבורה הפועלת על קבוצה וחקר המסלולים המתאימים. בהמשך נראה כיצד למנות גרפים לא-מתויגים בדרך זו. אולם נחזור כעת אל בעיית המחרוזות המעגליות, ונראה שבמקום לספור אותן ישירות, אנו יכולים לספור את מספר המסלולים (מחלקות השקילות) ביחס ~ שהגדרנו עתה.

דוגמה 9.3.6: נדגים זאת תחילה ל- $n = 4$. להלן רשימת המסלולים בפעולה של $\mathbb{Z}_4$ על $\{0,1\}^4$, כאשר מתחת לכל מסלול מצוירת המחרוזת המעגלית המתאימה.

(0,0,0,0)	(1,0,0,0) (0,1,0,0) (0,0,1,0) (0,0,0,1)	(1,1,0,0) (0,1,1,0) (0,0,1,1) (1,0,0,1)	(1,0,1,0) (0,1,0,1)	(1,1,1,0) (1,1,0,1) (1,0,1,1) (0,1,1,1)	(1,1,1,1)
$\begin{array}{ccc} 0 & \text{——} & 0 \\ \vert & & \vert \\ 0 & \text{——} & 0 \end{array}$	$\begin{array}{ccc} 1 & \text{——} & 0 \\ \vert & & \vert \\ 0 & \text{——} & 0 \end{array}$	$\begin{array}{ccc} 1 & \text{——} & 1 \\ \vert & & \vert \\ 0 & \text{——} & 0 \end{array}$	$\begin{array}{ccc} 1 & \text{——} & 0 \\ \vert & & \vert \\ 0 & \text{——} & 1 \end{array}$	$\begin{array}{ccc} 1 & \text{——} & 1 \\ \vert & & \vert \\ 0 & \text{——} & 1 \end{array}$	$\begin{array}{ccc} 1 & \text{——} & 1 \\ \vert & & \vert \\ 1 & \text{——} & 1 \end{array}$

תרשים 9.3.4: שישה המסלולים בפעולה של $\mathbb{Z}_4$ על $\{0,1\}^4$.

אנו רואים שקיימת התאמה חח״ע בין המחרוזות המעגליות של אפסים ואחדים לבין המסלולים בפעולה של $\mathbb{Z}_4$ על $\{0,1\}^4$. באופן כללי, כל הסדרות השייכות למסלול מסוים, מתקבלות מאותה מחרוזת מעגלית, על ידי פתיחתה במקומות שונים. אנו יכולים אם כך להסיק את המשפט הבא.

משפט 9.3.7: מספר המחרוזות המעגליות באורך n שווה למספר המסלולים בפעולה הנ״ל של $\mathbb{Z}_n$ על $\{0,1\}^n$.

הוכחה: הסדרות $(x_1,...,x_n),(y_1,...,y_n)$ שקולות אם הן מתקבלות זו מזו על ידי סיבוב כלשהו. לכן, שתי סדרות באורך n הן שקולות, ולכן שייכות לאותו המסלול, אם ורק אם הן מתקבלות על ידי פתיחתה של אותה מחרוזת מעגלית. □

הדוגמה המפורטת שראינו למקרה של $n = 4$ מאירה היבט מרכזי ביותר בתורת החבורות. כך, למשל, הסדרה (0,0,0,0) היא מסלול בפני עצמו. הסיבה לדבר היא שלמחרוזת המעגלית המתאימה יש **סימטריות** רבות, כפי שאפשר לראות:

$$\begin{array}{ccc} 0 & \text{——} & 0 \\ | & & | \\ 0 & \text{——} & 0 \end{array}$$

ואכן, מחרוזת זו איננה משתנה כשמסובבים אותה סיבוב כלשהו, ולכן אם נפתח אותה במקומות שונים נקבל את אותה הסדרה (0,0,0,0). בשפת המתמטיקאים, המחרוזת הזאת **אינווריאנטית** לסיבוב.

בקצה השני של טווח האפשריות נמצאת המחרוזת המעגלית הבאה, שלה אין בכלל סימטריות. כל סיבוב של המחרוזת הזאת מעביר אותה למחרוזת שונה. לכן גם המסלול המתאים לה כולל ארבע סדרות.

$$\begin{array}{ccc} 1 & \text{——} & 1 \\ | & & | \\ 0 & \text{——} & 1 \end{array}$$

ואילו בתווך, נמצאת המחרוזת הסימטרית לסיבוב של חצי מעגל, כאשר למחרוזת זאת מתאים מסלול בגודל 2:

$$\begin{array}{ccc} 1 & \text{——} & 0 \\ | & & | \\ 0 & \text{——} & 1 \end{array}$$

נעיר שלא מעט מן המחקר בחבורות נועד לחקור סימטריות במבנים מתמטיים ובמערכות טבע. כך למשל, מקיומן של סימטריות במערכת פיזיקלית, ניתן להסיק שמתקיים בה חוק שימור מתאים. זהו מוטיב מרכזי ביסודות הפיזיקה המודרנית.

נחזור לבעיית המחרוזות המעגליות, אולם בניסוחה החלופי: מהו מספר המסלולים בפעולה הנ״ל של $\mathbb{Z}_n$ על $\{0,1\}^n$? באופן כללי יותר, בהינתן שני מספרים טבעיים k,n, אנו רוצים לדעת מהו מספרן של המחרוזות המעגליות באורך n, כשאיברי המחרוזת הן אותיות מתוך הקבוצה $\{1,2,\ldots,k\}$. אנו נסמן מספר זה ב- f(k,n). עד כה דנו במקרה שבו $k = 2$, כלומר איברי המחרוזות היו רק אפסים ואחדים.
ממש כמקודם, במקום לספור מחרוזות מעגליות נספור מסלולים. גם כאן ניתן להגדיר פעולה של $\mathbb{Z}_n$ על $\{1,\ldots,k\}^n$ באופן הבא: שוב האיבר $j\in\mathbb{Z}_n$ מתאים לתמורה π_j המוגדרת על ידי $\pi_j(x_1,\ldots,x_n) = (x_{j+1},x_{j+2},\ldots,x_n,x_1,x_2,\ldots,x_j)$, אולם הפעם $x_i\in\{1,\ldots,k\}$.

בעיה: מהו המספר f(k,n) של מחרוזות מעגליות מאורך n עם איברים מתוך $\{1,\ldots,k\}$, או במילים אחרות מהו מספר המסלולים בפעולה של $\mathbb{Z}_n$ על $\{1,\ldots,k\}^n$?

קל לראות שיש תמיד k מסלולים מיוחדים המכילים איבר אחד בדיוק, והם המסלולים:

$$(1,1,\ldots,1),\ (2,2,\ldots,2),\ \ldots,\ (k,k,\ldots,k).$$

כל אחד מהאיברים האלה הוא מסלול בפני עצמו, מפני שהסדרות הנ״ל אינן משתנות כשפועל עליהן הסיבוב π_j, וזאת לכל j. מה לגבי יתר המסלולים? נתחיל את דיוננו במקרה ש- n ראשוני.
אנו נראה שבמקרה מיוחד זה, בכל אחד מהמסלולים האחרים יש בדיוק n סדרות.

משפט 9.3.8: יהיו n מספר ראשוני ו- k מספר טבעי כלשהו. אז מספר המחרוזות המעגליות מאורך n עם איברים מתוך $\{1,\ldots,k\}$ הוא $f(k,n)=k+\dfrac{k^n-k}{n}$.

הוכחה: כאמור במקום לספור מחרוזות מעגליות, נספור מסלולים בפעולה של $\mathbb{Z}_n$ על $\{1,\ldots,k\}^n$.
מספר הסדרות באורך n שניתן לבנות מאיברי הקבוצה $\{1,\ldots,k\}$ הוא k^n. אנו נראה שאחרי שמשמיטים את k הסדרות $(1,\ldots,1),\ldots,(k,\ldots,k)$, השייכות למסלולים בגודל 1, כל שאר k^n-k הסדרות משתייכות למסלולים מגודל n בדיוק. לכן, מספר המסלולים הוא $k+\dfrac{k^n-k}{n}$ כנדרש.
ואכן, תהי $(x_1,\ldots,x_n)$ סדרה שאינה אחת מ- k הסדרות מהצורה $(i,i,\ldots,i)$, כלומר לא כל ה- x_j שווים זה לזה. נראה שאם n ראשוני אז כל n הסדרות הבאות, השייכות לאותו מסלול, שונות זו מזו:

$$\pi_0(x_1,\ldots,x_n)=(x_1,\ldots,x_n),\quad \pi_1(x_1,\ldots,x_n)=(x_2,\ldots,x_n,x_1),$$
$$\pi_2(x_1,\ldots,x_n)=(x_3,\ldots,x_n,x_1,x_2),\ldots,\pi_{n-1}(x_1,\ldots,x_n)=(x_n,x_1\ldots,x_{n-1})$$

נניח בשלילה שיש שני אינדקסים $q>p$ כך ש- $\pi_p(x_1,\ldots,x_n)=\pi_q(x_1,\ldots,x_n)$. נוכיח כי בהכרח $x_1=x_2=\ldots=x_n$, וזו תהיה כמובן סתירה לכך שלא כל ה- x_i שווים זה לזה. על ידי הפעלה של התמורה π_p^{-1} ושימוש בהנחתנו כי $\pi_p=\pi_q$, נקבל:

$$\pi_p^{-1}\circ\pi_p(x_1,\ldots,x_n)=\pi_p^{-1}\circ\pi_q(x_1,\ldots,x_n)\,.$$

אולם $\pi_p^{-1}\circ\pi_p=\pi_0$ היא העתקת הזהות. כמו-כן, קל לוודא ש- $\pi_p^{-1}\circ\pi_q=\pi_{q-p}$ (הפעילו על שני האגפים את התמורה π_p). מכאן,

$$\pi_{q-p}(x_1,\ldots,x_n)=\pi_0(x_1,\ldots,x_n)=(x_1,\ldots,x_n)\,.$$

נסמן $j=q-p$, כאשר $j\neq 0$. לכן:

$$(x_1,\ldots,x_n)=\pi_j(x_1,\ldots,x_n)=(x_{j+1},x_{j+2},\ldots,x_n,x_1,\ldots,x_j)$$

נתחיל להשוות את הקואורדינטות. ניתן להסיק כי:

$$x_1=x_{j+1}=x_{2j+1}=x_{3j+1}=\ldots\,.$$

השוויון הראשון מבטא את שוויון הקואורדינטות הראשונות בשני האגפים של השוויון:

$$(x_1,\ldots,x_n)=\pi_j(x_1,\ldots,x_n)=(x_{j+1},x_{j+2},\ldots,x_n,x_1,\ldots,x_j)\,,$$

השוויון השני משווה את הקואורדינטות ה- $(j+1)$ בשני האגפים וכך הלאה. אולם, אם n ראשוני ו- $j\neq 0$, אז הסדרה $1, j+1, 2j+1, 3j+1,\ldots$ כוללת את כל המספרים בקבוצה $\{1,2,\ldots,n\}$, ולכן כל הקואורדינטות של x_i זהות. אחרת, קיימים שני מספרים טבעיים שונים s,t כך ש- $s\cdot j+1=t\cdot j+1$. לכן $(s-t)\cdot j\equiv 0 \pmod n$, דבר שלא ייתכן כאשר n ראשוני. □

מן המשפט האחרון אנו יכולים להסיק משפט קלאסי בתורת המספרים.

משפט 9.3.9 (המשפט הקטן של פרמה): יהיו p מספר ראשוני, ו- a מספר שלם כלשהו. אז $a^p\equiv a\pmod p$.

הוכחה: מהמשפט הקודם נובע ש- $\frac{a^p-a}{p}$ הוא מספר שלם. זאת מכיוון שזהו מספר המחרוזות המעגליות מאורך p ללא סימטריות עם איברים מתוך הקבוצה $\{1,\ldots,a\}$. לכן, a^p-a מתחלק ב- p ללא שארית. □

נחזור לבעיית מניית המסלולים. כזכור $f(k,n)$ מסמן את מספר המסלולים בפעולה של $\mathbb{Z}_n$ על $\{1,\ldots,k\}^n$. ראינו שאם n ראשוני אז $f(k,n)=\frac{k^n-k}{n}+k$. נעבור כעת למקרה של n כללי, לאו דווקא ראשוני. כדי לקבל תחושה נוספת לבעיה, נמשיך את דיוננו במקרה הפרטי של $n = 6$.

דוגמה 9.3.10: ברצוננו להבין את מבנה המסלולים בפעולה של $\mathbb{Z}_6$ על $\{1,\ldots,k\}^6$. כמו במקרה של n ראשוני, אנו מוצאים גם כאן k מסלולים מגודל 1, והם כל המסלולים מהצורה (t, t, t, t, t, t) כאשר $1 \le t \le k$ מספר טבעי כלשהו. באופן דומה אנו מוצאים מסלולים רבים ללא סימטריות מגודל $n = 6$. אולם כאן מופיעים שני סוגים חדשים של מסלולים שלא ראינו במקרה של n ראשוני, מסלולים מגודל 2 ומסלולים מגודל 3. אנו נראה בהמשך שהגודל של כל מסלול הוא בהכרח מחלק של n (ראו טענה 9.3.17). לכן, במקרה זה, כאשר $n = 6$, יש רק מסלולים מגודל 1, 2, 3, 6. נסתמך על כך ונעבור למנות את המסלולים הנ"ל.

אם $1 \le s \ne t \le k$, אז $\{(s,t,s,t,s,t),(t,s,t,s,t,s)\}$ הוא מסלול מגודל 2. מספרם של המסלולים מגודל 2 הוא $\binom{k}{2}$ מפני שעלינו לבחור זוג לא סדור $\{s,t\}$ כאשר $s \ne t$.

כמו כן, יש גם מסלולים מגודל 3 שצורתם $\{(r,s,t,r,s,t),(s,t,r,s,t,r),(t,r,s,t,r,s)\}$ לכל שלושה מספרים $1 \le r, s, t \le k$, כאשר לא כל שלושת המספרים שווים. מהו מספרם של מסלולים אלה? נשים לב שכל אחת משלוש הסדרות במסלול כזה מאופיינת על ידי חצייה השמאלי, כי הרי חצייה הימני זהה לחצייה השמאלי. לכן, יש התאמה חח"ע ועל בין המסלולים האלה למסלולים מגודל 3 בפעולה של $\mathbb{Z}_3$ על $\{1,\ldots,k\}^3$, היינו המסלולים מהצורה $\{(r,s,t),(s,t,r),(t,r,s)\}$. מספרם של אלה כפי שראינו הוא $\frac{k^3-k}{3}$ מכיוון ש- 3 הוא מספר ראשוני.

להלן אם כן המפקד המלא של המסלולים בפעולה של $\mathbb{Z}_6$ על $\{1,\ldots,k\}^6$. ראינו עד כה שיש:

k מסלולים מגודל 1, $\binom{k}{2}$ מסלולים מגודל 2, $\frac{k^3-k}{3}$ מסלולים מגודל 3.

מספר הסדרות הכללי באורך 6 הוא k^6. נפחית ממספר זה את מספר הסדרות השייכות למסלולים מגודל 1, 2, ו- 3, ונקבל את מספר הסדרות השייכות למסלולים מגודל 6. לכן, מספר המסלולים מגודל 6 הוא:

$$.\frac{k^6-k-2\cdot\binom{k}{2}-3\cdot\frac{k^3-k}{3}}{6}=\frac{k^6-k^3-k^2+k}{6}$$

ולכן מספר המסלולים הכולל הוא:

$$.\ f(k,6)=k+\binom{k}{2}+\frac{k^3-k}{3}+\frac{k^6-k^3-k^2+k}{6}=\frac{k^6}{6}+\frac{k^3}{6}+\frac{k^2}{3}+\frac{k}{3}$$

נחזור לדיון הכללי. הפתרון מסתמך על המשפט הבא. נזכיר שאם π תמורה של איברי X, אז x היא נקודת שבת של π אם $\pi(x)=x$. שימו לב, במקרה שלנו איברי הקבוצה X הם סדרות, ולכן $\pi(x)=x$ פירושו שהפונקציה π מעתיקה את הסדרה x לעצמה.

משפט 9.3.11 (ברנסייד Burnside): מספר המסלולים בפעולה של החבורה G על הקבוצה X הוא $\frac{1}{|G|}\sum_{\pi\in G}\mathrm{fix}(\pi)$, כאשר $\mathrm{fix}(\pi)$ הוא מספר נקודות השבת של תמורה $\pi\in G$ בפעולתה על X.

נדחה לרגע את הוכחת משפט ברנסייד ונשתמש בו תחילה על מנת לקבוע את $f(k,n)$.

משפט 9.3.12: $f(k,n)=\frac{1}{n}\sum_{r|n}\phi\left(\frac{n}{r}\right)k^r$, כאשר $\phi(n)$ היא פונקצית אוילר.

הערה: נזכיר שהסימון $r\,|\,n$ פירושו ש- r מחלק את n ללא שארית. ואילו, פונקצית אוילר הוגדרה בסעיף 4.6 על ידי $\phi(1)=1$, ולכל $n>1$, $\phi(n)$ הוא מספר המספרים הטבעיים מתוך הקבוצה $\{1,2,\dots,n\}$ שזרים ל- n. נזכיר גם את הנוסחה $\phi(n)=n\prod_{i=1}^{t}(1-\frac{1}{p_i})$ כאשר $p_1,p_2,\dots,p_t$ היא רשימת כל המספרים הראשוניים השונים המחלקים את n (משפט 4.6.10).

הוכחה: נראה איך להסיק את הנוסחה ל- $f(k,n)$ מתוך משפט ברנסייד. במקרה שלנו מדובר בפעולה של החבורה $\mathbb{Z}_n$ על הקבוצה $\{1,\dots,k\}^n$, ולכן לפי משפט ברנסייד:

$$.\ f(k,n)=\frac{1}{|\mathbb{Z}_n|}\sum_{\pi\in\mathbb{Z}_n}\mathrm{fix}(\pi)=\frac{1}{n}\sum_{\pi\in\mathbb{Z}_n}\mathrm{fix}(\pi)$$

לכן, עלינו למצוא לכל $\pi\in\mathbb{Z}_n$, מהו מספר נקודות השבת של π. נניח ש- π_j היא התמורה המתאימה ל- $j\in\mathbb{Z}_n$. דהיינו,

$$.\ \pi_j(x_1,\dots,x_n)=(x_{j+1},x_{j+2},\dots,x_n,x_1,\dots,x_j)$$

עלינו לברר מהו מספר הסדרות $(x_1,\dots,x_n)\in\{1,\dots,k\}^n$ שהן נקודת שבת של π_j, כלומר:

$$.\ \pi_j(x_1,\dots,x_n)=(x_{j+1},x_{j+2},\dots,x_n,x_1,\dots,x_j)=(x_1,\dots,x_n)$$

נוכיח תחילה את טענת העזר הבאה:

טענה 9.3.13: יהי $r = \gcd(n,j)$ המחלק המשותף המקסימלי של j ו- n (ראו סעיף 3.4). אז $(x_{j+1}, x_{j+2}, \ldots, x_n, x_1, \ldots, x_j) = (x_1, \ldots, x_n)$ אם ורק אם לכל i מתקיים $x_i = x_{(r+i) \bmod n}$.

הוכחה: עלינו להוכיח שני כיוונים.

הכרחיות: נניח ש- $x_i = x_{(r+i) \bmod n}$ לכל i, ונוכיח כי $(x_{j+1}, x_{j+2}, \ldots, x_n, x_1, \ldots, x_j) = (x_1, \ldots, x_n)$.

כלומר עלינו להוכיח כי $x_1 = x_{j+1}$, $x_2 = x_{j+2}, \ldots$, ובאופן כללי ש- $x_i = x_{j+i}$ לכל i.

ואכן, לפי ההנחה $x_i = x_{r+i}$ לכל i. כלומר $x_i = x_{r+i} = x_{2r+i} = \ldots$. מכיוון ש- r מחלק את j, נוכל להמשיך כך j/r צעדים ולקבל $x_i = x_{r+i} = x_{2r+i} = \ldots = x_{j+i}$ כנדרש.

מספיקות: מכיוון ש- $r = \gcd(n,j)$ אז לפי האלגוריתם של אוקלידס (ראו משפט 3.4.10), קיימים שני מספרים שלמים a,b כך ש- $a \cdot n + b \cdot j = r$. בפרט $b \cdot j \equiv r \pmod n$. לכן, מכיוון ש- $(x_{j+1}, x_{j+2}, \ldots, x_n, x_1, \ldots, x_j) = (x_1, \ldots, x_n)$, נוכל לטעון כי:

$$x_i = x_{j+i} = x_{2j+i} = \ldots = x_{b \cdot j+i} = x_{r+i}$$

(כזכור כל האינדקסים מחושבים מודולו n). □

מסקנה 9.3.14: תהי π_j התמורה המתאימה ל- $j \in \mathbb{Z}_n$, ויהי $r = \gcd(n,j)$. אז $\mathrm{fix}(\pi_j) = k^r$.

הוכחה: מתוך הדיון הנ״ל נובע התיאור הבא לסדרות $(x_1, \ldots, x_n)$ שהן נקודות שבת של π_j.

בוחרים $x_1, \ldots, x_r$ כאיברים כלשהם מתוך $\{1, \ldots, k\}$, ומכאן ואילך $x_{r+1} = x_1$, $x_{r+2} = x_2, \ldots$. כלומר, אנו חוזרים n/r פעמים על הרצף של r האיברים הראשונים שבחרנו. לכן, מספר נקודות השבת שווה למספר הדרכים לבחור את $x_1, \ldots, x_r$ מתוך $\{1, \ldots, k\}$, וזאת אפשר לעשות ב- k^r דרכים. □

המשך הוכחת משפט 9.3.12: נותר לכן רק לברר לכל r המחלק את n ללא שארית, מהו מספר ה- $0 \le j \le n-1$ כך ש- $\gcd(n,j) = r$ (אנו נגדיר $\gcd(n,0) = n$).

יש שני מקרים פרטיים שכבר ידועים לנו: כאשר $r = 1$ התשובה היא $\phi(n)$, מפני שהתנאי $\gcd(n,j) = 1$ פירושו שהמספרים j ו- n זרים, וכזכור מספר ה- j הזרים ל- n הוא $\phi(n)$. ואילו כאשר $r = n$ התשובה היא $\phi(1) = 1$, מכיוון שרק $j = 0$ מקיים $\gcd(n,j) = n$.

באופן כללי, לא קשה לראות שהתשובה היא $\phi(n/r)$, מפני שהתנאי $\gcd(n,j) = r$ שקול לכך שניתן לרשום $j = r \cdot s$, כאשר $1 \le s \le \frac{n}{r} - 1$ הוא מספר טבעי הזר ל- n/r (מדוע?).

לכן, מספר האינדקסים $j \in \mathbb{Z}_n$ המקיימים $\gcd(n,j) = r$ הוא $\phi(n/r)$. לפי מסקנה 9.3.14, לכל j כזה התמורה π_j מקיימת $\mathrm{fix}(\pi_j) = k^r$. נציב כעת במשפט ברנסייד (משפט 9.3.11):

$$f(k,n) = \frac{1}{n} \sum_{\pi \in \mathbb{Z}_n} \mathrm{fix}(\pi) = \frac{1}{n} \sum_{r|n} \phi\left(\frac{n}{r}\right) k^r$$

ובכך מוכח המשפט. □

דוגמה 9.3.15: נחזור לדוגמה של $n = 6$. כפי שראינו $f(k,6)=\frac{k^6}{6}+\frac{k^3}{6}+\frac{k^2}{3}+\frac{k}{3}$. ואכן, $\phi(1)=\phi(2)=1,\quad \phi(3)=\phi(6)=2$, כלומר

$$f(k,6)=\frac{1}{6}\left[\phi(1)\cdot k^6+\phi(2)\cdot k^3+\phi(3)\cdot k^2+\phi(6)\cdot k^1\right].$$

לכן הדוגמה מתיישבת עם המשפט הכללי.

אנו חייבים עדיין לקוראים את הוכחת משפט ברנסייד. נפתח בהגדרה ובטענה הבאות.

הגדרה 9.3.16: תהי G חבורה סופית הפועלת על קבוצה X. לכל $x\in X$ נגדיר את **המייצב של x** כאוסף כל התמורות $\pi\in G$ כך ש- $\pi(x) = x$. נסמן אוסף זה ב- $stab(x)$.

כלומר $stab(x)$ הוא אוסף כל התמורות ב- G ש- x היא נקודת שבת שלהן.

טענה 9.3.17: לכל $x\in X$ מתקיים $|O_x|\cdot|stab(x)| = |G|$, כאשר O_x הוא המסלול בפעולה של G על X אשר כולל את האיבר x.

הוכחה: אנו נראה שלכל $y\in O_x$, מספר התמורות $\pi\in G$ המקיימות $\pi(x) = y$ הוא בדיוק $|stab(x)|$. במילים אחרות, התמורות ב- G מתחלקות ל- $|O_x|$ תת-קבוצות (אחת כנגד כל איבר $y\in O_x$) שכל אחת מהן בגודל $|stab(x)|$. אם נוכיח זאת תנבע הטענה.

ואכן, יהיה $stab(x) = \{\pi_1,\ldots,\pi_s\}$ המייצב של x. דהיינו $\pi_i(x) = x$ לכל $1 \le i \le s$, וזו רשימת כל התמורות ב- G ש- x היא נקודת שבת שלהן.

יהי $y\in O_x$, ונבחר תמורה כלשהי $\sigma\in G$ המקיימת $\sigma(x) = y$ (יש תמורה σ כזאת כי y שייך למסלול O_x של x). נשים לב ש-

$$\sigma\circ\pi_i(x)=\sigma(\pi_i(x))=\sigma(x)=y$$

לכל $1 \le i \le s$. כמו-כן, כל התמורות $\sigma\circ\pi_i$ שונות זו מזו שהרי השוויון $\sigma\circ\pi_i=\sigma\circ\pi_j$ גורר ש- $\pi_i=\pi_j$. לכן, לכל $y\in O_x$ יש לפחות $s = |stab(x)|$ תמורות שונות $\sigma\circ\pi_i\in G$ המקיימות $\sigma\circ\pi_i(x)=y$.

מצד שני, נראה שאין יותר מ- s תמורות כנ"ל. נניח כי $\rho_1,\ldots,\rho_t\in G$ הן t תמורות שונות המקיימות $\rho_i(x)=y$ לכל $1 \le i \le t$. נראה ש- $s \ge t$. ואכן, נתבונן בתמורות $\sigma^{-1}\circ\rho_1,\ldots,\sigma^{-1}\circ\rho_t$. כמובן מתקיים $\sigma^{-1}\circ\rho_i(x)=\sigma^{-1}(y)=x$ לכל $1 \le i \le t$. כלומר כל אחת מהתמורות $\sigma^{-1}\circ\rho_i$ שייכת לקבוצה $stab(x)$. כמו-כן, התמורות הנ"ל שונות זו מזו ולכן $|stab(x)| = s \ge t$. בכך הוכחה הטענה. □

הוכחת משפט 9.3.11: נחזור לעיין בפעולה של החבורה G על הקבוצה X, ושוב לכל איבר $x\in X$ נסמן ב- O_x את המסלול של x. יהי O מסלול כלשהו, ונשים לב כי $\sum_{x\in O}\frac{1}{|O_x|}=1$ (מכיוון שמדובר במסלולים, הרי אם $x\in O$ אז $O = O_x$. לכן אם $|O| = p$ אז אנו מסכמים כאן p מחוברים שכל אחד מהם שווה ל- $1/p$). מכיוון שהמסלולים זרים, אז אם נסכם על פני כל המסלולים נקבל שמספר

המסלולים בפעולה של G על X הוא $\sum_{x\in X}\frac{1}{|O_x|}$. אולם לפי טענה 9.3.17 לכל $x\in X$ מתקיים $\frac{|stab(x)|}{|G|}=\frac{1}{|O_x|}$. לכן, מספר המסלולים הוא $\sum_{x\in X}\frac{|stab(x)|}{|G|}$.
נשים לב כי $\sum_{\pi\in G}fix(\pi)=\sum_{x\in X}|stab(x)|$ וזאת מכיוון ששני האגפים מונים את מספר הזוגות (π,x) כך ש- $\pi\in G$, $x\in X$ ומתקיים $\pi(x) = x$. לכן, מספר המסלולים הוא:

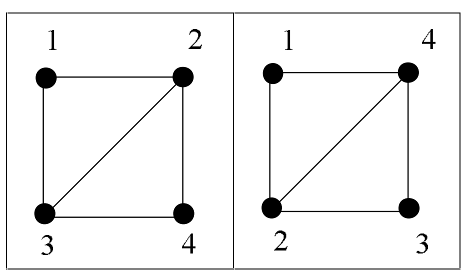
$$\sum_{x\in X}\frac{1}{|O_x|}=\sum_{x\in X}\frac{|stab(x)|}{|G|}=\frac{1}{|G|}\sum_{x\in X}|stab(x)|=\frac{1}{|G|}\sum_{x\in X}fix(x)$$

ובכך הוכחנו את משפט ברנסייד. □

מנייה של גרפים

כאמור המונחים שפיתחנו בפרק זה מספקים לנו מסגרת מושגית לדיון בשאלות רבות נוספות. כך למשל, בסעיף 5.6 דנו במנייה של עצים מתויגים ולא מתויגים. בעוד שמספרם של העצים המתויגים מסדר n ידוע והוא n^{n-2} (משפט 5.6.1), אין לנו נוסחה סגורה למספרם של העצים הלא-מתויגים, וראינו רק כיצד למצוא חסם עליון וחסם תחתון למספר זה. בסעיף זה נראה בקצרה כיצד המינוחים והמושגים שפיתחנו עתה מאפשרים לנו לדון במנייה של גרפים לא-מתויגים.
ואכן, יהי n מספר טבעי ונגדיר את X כאוסף כל הגרפים המתויגים עם n קדקודים. כפי שראינו מספר הגרפים המתויגים מסדר n הוא $2^{\binom{n}{2}}$ (ראו תרגיל 1 בסעיף 5.6). נראה איך החבורה הסימטרית S_n פועלת על X. אם $\pi\in S_n$ תמורה ו- $G\in X$ גרף מתויג, אז גם $\pi(G)$ הוא גרף מתויג. מבחינת צורה, הגרף $\pi(G)$ זהה לגרף G. השוני בין G ל- $\pi(G)$ הוא רק בשמות הקדקודים. קדקוד i בגרף G ייקרא $\pi(i)$ בגרף $\pi(G)$.

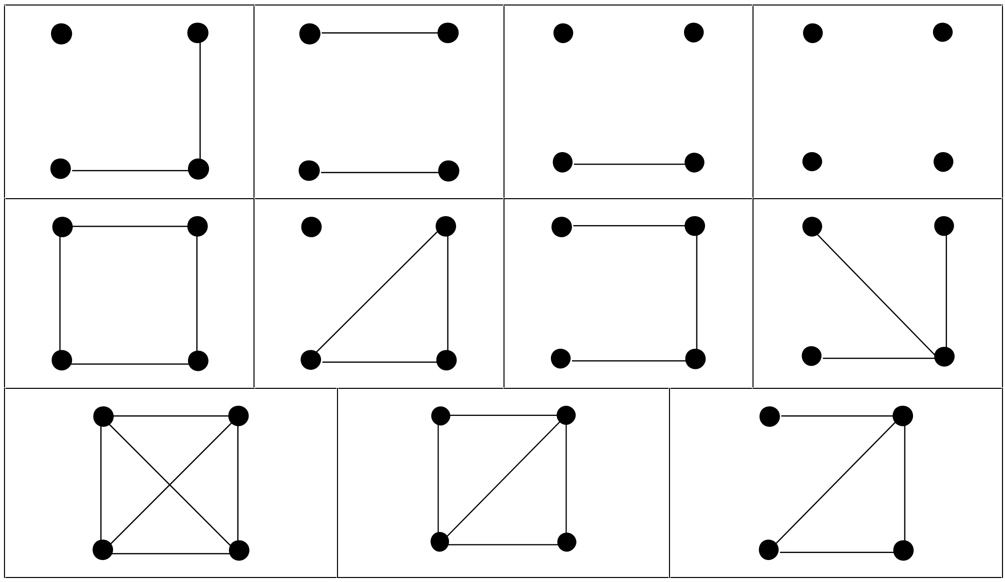
דוגמה 9.3.18: נתבונן בתמורה $\pi=(1,4,2,3)$. בתרשים 9.3.5 אפשר לראות את הגרפים G ו- $\pi(G)$.



תרשים 9.3.5: הגרפים G משמאל ו- $\pi(G)$ מימין.

כעת נתבונן במסלולים השונים המוגדרים על ידי הפעולה של S_n על X. כזכור שני גרפים מתויגים G_1,G_2 יהיו באותו מסלול אם יש תמורה $\pi \in S_n$ כך ש- $\pi(G_1) = G_2$. על פי הגדרה 5.6.7 ניתן לומר ששני גרפים הם באותו המסלול אם ורק אם הם איזומורפיים.

דוגמה 9.3.19: כך למשל, $2^{\binom{4}{2}} = 64$ הגרפים המתויגים מסדר n = 4, מתחלקים ל- **11** מסלולים. בתרשים 9.3.6 אפשר לראות את צורתם של הגרפים השייכים לכל אחד מהמסלולים.



תרשים 9.3.6: אחד עשר המסלולים בפעולה של S_4 על קבוצת הגרפים המתויגים מסדר 4.

עתה נוכל להגדיר את המושג של גרף לא-מתויג.

הגדרה 9.3.20: כל מסלול בפעולה של S_n על קבוצת הגרפים המתויגים X, מוגדר כ**גרף לא מתויג**.

טענה 9.3.21: נתבונן בפעולה של S_n על קבוצת הגרפים המתויגים מסדר n. בכל מסלול בפעולה זו יש לכל היותר !n גרפים מתויגים.
הוכחה: יהי G גרף מתויג. אפילו אם כל הגרפים המתויגים $\pi(G)$ שונים זה מזה, הרי כשעוברים על כל !n התמורות השונות $\pi \in S_n$, אז גודל המסלול הוא !n. אך ודאי לא ייתכן מסלול גדול מזה. □

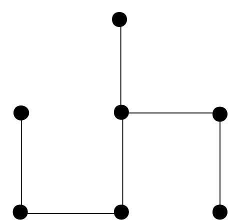
כמסקנה מהטענה האחרונה נקבל חסם תחתון למספר הגרפים הלא-מתויגים.

מסקנה 9.3.22: מספר הגרפים הלא-מתויגים מסדר n הוא לפחות $\frac{2^{n(n-1)/2}}{n!}$.

הוכחה: לפי טענה 9.3.21, בכל מסלול בפעולה של S_n על קבוצת הגרפים המתויגים יש לכל היותר $n!$ גרפים מתויגים. לכן $2^{\binom{n}{2}}$ הגרפים המתויגים מתחלקים לפחות ל- $\frac{2^{\binom{n}{2}}}{n!} = \frac{2^{n(n-1)/2}}{n!}$ מסלולים. מכיוון שכל מסלול כזה מוגדר כגרף לא-מתויג, הרי יש לפחות מספר כזה של גרפים לא-מתויגים. □

תרגילים

1. הראו שאם G חבורה הפועלת על X ואם $x \in X$, אז המייצב stab(x) הוא תת-חבורה של G.
2. כפי שהגדרנו את הפעולה של S_n על קבוצת הגרפים המתויגים, אפשר גם להגדיר פעולה של S_n על קבוצת n^{n-2} העצים המתויגים. באופן דומה, **עץ לא-מתויג** יוגדר כמסלול בפעולה זו. נתחו את הפעולה של S_5 על הקבוצה של כל העצים המתויגים מסדר 5. מהו גודלו של כל מסלול בפעולה זו וכמה מסלולים יש?
3. בתרגיל זה נראה שייתכנו מסלולים בגודל $n!$ בפעולה של S_n על הקבוצה של כל העצים המתויגים מסדר n.
   א. הראו שהמסלול המתאים לעץ הלא-מתויג הבא מסדר 7 הוא בגודל $7!$.



   ב. הראו שאם n הוא מספר מהצורה $n = \binom{k}{2} + 1$ כאשר $k \geq 4$, אז יש עץ לא-מתויג שבמסלול המתאים לו יש $n!$ עצים מתויגים.
4. הוכיחו שאם G חבורה ו- H תת-חבורה שלה, אז מספר האיברים ב- H מחלק את מספר האיברים ב- G, כלומר $|H|$ מחלק את $|G|$.

הערות היסטוריות

ויליאם ברנסייד William Burnside (אנגליה 1852-1927). החל את עבודתו בתחומי ההידרודינמיקה והאנליזה המרוכבת. מתוך עבודתו באנליזה מרוכבת, החל ברנסייד להתעניין במשפחות מסוימות של פונקציות מרוכבות הסגורות להרכבה ומהוות לכן חבורה. מכאן הייתה דרכו מהירה לחקר תורת החבורות וההצגות שלהן. הוא כתב את הספר הראשון באנגלית שהוקדש לתורת החבורות. השפעתו על תורת החבורות ניכרת עד ימינו. באחד המאמרים

החשובים ביותר בתורת החבורות הוכיחו פיית ותומפסון Feit and Thompson ב- 1962 את השערתו של ברנסייד על המבנה של החבורות הנקראות חבורות פשוטות. חבורות אלה מהוות אבן בניין בסיסית לכל החבורות הסופיות.

פייר דה פרמה Pierre de Fermat (צרפת 1665-1601). תרומתו העיקרית של פרמה היא בתורת המספרים. כך למשל, הוכחנו בפרק זה את המשפט הקטן של פרמה (ראו משפט *9.3.9*). פרמה גם הוכיח שכל מספר ראשוני מהצורה $p = 4k+1$, ניתן להציג כסכום של שני ריבועים (אף כי ההוכחה המלאה הראשונה ניתנה כנראה על ידי אוילר).
תהילתו העיקרית של פרמה בקרב הציבור הרחב נובעת מההשערה המפורסמת שלו הנקראת המשפט האחרון של פרמה. השערה זו טוענת שלא ניתן למצוא פתרון במספרים טבעיים חיוביים x,y,z למשוואה $x^n + y^n = z^n$ כאשר $n \geq 3$. פרמה רשם בשולי ספר מתמטיקה שהיה לו, כי ידוע לו פתרון הבעיה ורק המקום המצומצם שבשולי הספר מונע ממנו לרשום את הפתרון במלואו. אפשר לשער בוודאות רבה למדי כיום שלא הייתה לו הוכחה כזאת, ורק למעלה מ- 300 שנים אחר כך, ב- 1994, הצליח אנדרו ווילס Andrew Wiles להוכיח את השערת פרמה. הניסיונות לפתור את השערת פרמה הובילו במהלך השנים לכמה מן ההתפתחויות המרתקות במתמטיקה.