# 4 חבורות תמורות

כזכור, חבורת התמורות על קבוצה $X$ מסומנת ב-$S_X$ ואם $|X| = n$ הסדר שלה הוא $n!$. במקרה כזה ניתן להתאים לכל $x \in X$ "אינדקס" בין 1 ל-$n$ ולזהות את התמורות על איברי $X$ עם התמורות המתאימות של האינדקסים. קל לבדוק שזיהוי זה הוא איזומורפיזם $S_X \cong S_n$.

מסתבר שכל חבורה היא תת-חבורה של חבורת תמורות:

משפט קיילי

**משפט 4.1 (משפט קיילי, Cayley)** תהי $G$ חבורה מסדר $n$. אזי $G$ איזומורפית לתת-חבורה של $S_n$.

למעשה, משפט זה נכון, ועם אותה הוכחה, גם לחבורות מסדר אינסופי.

**הוכחה:** ראינו כבר כי $G$ פועלת על עצמה על-ידי כפל משמאל

$$g_1 . g_2 = g_1 g_2,$$

והזכרנו (טענה 3.4) כי כל פעולה של $G$ על קבוצה בגודל $n$ מתאימה להומומורפיזם $\varphi : G \to S_n$. למשל, אם איברי החבורה הם $\{g_1 = e, g_2, \ldots, g_n\}$, ניתן להגדיר את $\varphi$ על-ידי:

$$\varphi(g)(i) = j \iff g g_i = g_j.$$

ההומומורפיזם זה הוא חח"ע, כלומר $\ker \varphi = \{e\}$, שכן אם $\varphi(g)(i) = i$ לכל $i$, או אפילו ל-$i$ יחיד, אזי $g g_i = g_i$ ומכלל הצמצום $g = e$. זהו, אם כן, שיכון, ולכן לפי משפט האיזומורפיזם הראשון נקבל

$$G \cong \operatorname{Im} \varphi \leq S_n.$$

■

אין לטעות ולגזור ממשפט קיילי שדי לנו לחקור את חבורות התמורות כדי לנתח את כלל החבורות. בשיכון שמספק לנו משפט קיילי אנו משכנים חבורה בגודל $n$ בחבורה גדולה הרבה יותר: בגודל $n!$. חקר החבורה הגדולה לרוב לא יחשוף בפנינו תכונות של החבורה הקטנה. (למשל, ראו תרגילים 4.9 או 7.21 להלן.)

## 4.1 תמורות בכתיב מחזורים

עד כה סימנו איברים מ-$S_n$ בצורה של טבלה שמתארת, לפי הסדר, לאן עובר כל מספר ב-$\{1, \ldots, n\}$. למשל

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 7 & 5 & 1 & 4 & 3 \end{pmatrix}.$$

בדרך זו ניתן לכתוב כל פונקציה, לאו דווקא תמורה, מהקבוצה $\{1, \ldots, n\}$ לעצמה. מסתבר שישנה דרך יעילה יותר לרישום תמורות שגם מנצלת את התכונות המיוחדות של תמורה כפונקציה חח"ע ועל: כתיב מחזורים. כתיב זה קצר יותר, וכפי שנראה להלן, גם מציג בצורה מאירת עיניים תכונות חשובות

של התמורה כמו הסדר שלה או מחלקת הצמידות שהיא משתייכת לה בתוך $S_n$. למשל, התמורה שלעיל תכתב כך:

$$(1\,6\,4\,5)\,(3\,7)$$

כדי להסביר צורת כתיבה זו נתאר תחילה מחזור יחיד. יהיו $x_1, x_2, \ldots, x_\ell \in \{1, \ldots, n\}$ רשימה של $\ell$ מספרים שונים. אזי הכתיב

$$\sigma = (x_1\, x_2\, x_3\, \ldots\, x_\ell)$$

מתאר תמורה $\sigma$ שמעבירה את $x_j$ ל-$x_{j+1}$ (בסדר מעגלי: $x_\ell$ עובר ל-$x_1$), ואת כל יתר האיברים מותירה במקום, כלומר

$$\sigma = \begin{pmatrix} \ldots & x_j & \ldots & y & \ldots \\ \ldots & x_{j+1} & \ldots & y & \ldots \end{pmatrix}$$

(כאשר $y \neq x_j$ לכל $j$).

$\ell$-מחזור

**הגדרה 4.2** תמורה $\sigma \in S_n$ מצורה זו נקראת **מחזור (צקלוס**, cycle), או **$\ell$-מחזור** (אם רוצים להדגיש את אורך המחזור).

הנה כמה עובדות קלות הקשורות לכתיב זה של מחזורים (ודאו שאתם מבינים מדוע הן נכונות):

- אם $\sigma = (x_1\, x_2\, \ldots\, x_\ell)$ אז $\sigma^{-1} = (x_\ell\, x_{l-1}\, \ldots\, x_1)$.
- הסדר של $\sigma$ הוא $\ell$.
- נניח כי $\sigma, \sigma'$ מחזורים **זרים**, כלומר $\sigma = (x_1\, x_2\, \ldots\, x_\ell)$ ו-$\sigma' = (y_1\, y_2\, \ldots\, y_m)$ כאשר $x_i \neq y_j$ לכל $i, j$. אזי $\sigma$ ו-$\sigma'$ מתחלפים: $\sigma\sigma' = \sigma'\sigma$.

**טענה 4.3** כל תמורה $\sigma \in S_n$ ניתנת לכתיבה כמכפלה של מחזורים זרים.

**הוכחה:** נבחר מספר כלשהו $x \in \{1, \ldots, n\}$ ונכתוב את סדרת התמונות שלו דרך $\sigma$:

$$x, \sigma(x), \sigma^2(x), \ldots$$

בסופו של דבר, מכיוון שהקבוצה $\{1, \ldots, n\}$ סופית, נגיע בהכרח לאיבר שכבר היה בסדרה. נניח כי $\sigma^r(x)$ הוא האיבר הראשון שחוזר על עצמו. בהכרח $\sigma^r(x) = x$, כי אחרת $\sigma^r(x) = \sigma^i(x)$ בעבור $1 \leq i \leq r-1$ מסוים. אך אז, הפעלה של $\sigma^{-1}$ על שני האגפים תראה ש-$\sigma^{r-1}(x) = \sigma^{i-1}(x)$, כלומר האיבר $\sigma^{r-1}(x)$ היה גם הוא איבר חוזר, בסתירה למינימליות של $r$. כך קיבלנו מחזור

$$\left(x\ \sigma(x)\ \ \sigma^2(x)\ \ldots\ \sigma^{r-1}(x)\right).$$

נעיר שאם $r = 1$, כלומר אם $\sigma(x) = x$, קיבלנו מחזור באורך 1 שנסמנו פשוט $(x)$.

כעת, אם נותרו עוד איברים מחוץ למחזור, נבחר $y$ כלשהו כזה, ונבנה את המחזור שלו. אותו טיעון

יראה שאנחנו שוב מקבלים מחזור. יתר על כן, המחזור החדש זר למחזור שכבר קיבלנו קודם: אלמלא כן יהי $\sigma^i\left(y\right)$ האיבר הראשון במחזור החדש שהופיע גם במחזור הקודם, נניח כ-$\sigma^j\left(x\right)$ (ברור כי $i \geq 1$ לפי בחירת $y$). שוב, משום ש-$\sigma$ חח״ע ועל, יש לה תמורה הפכית, ועל-ידי הפעלת התמורה ההפכית נקבל כי גם $\sigma^{j-1}\left(x\right) = \sigma^{i-1}\left(y\right)$ (אם $j = 0$ אז $\sigma^{r-1}\left(x\right) = \sigma^{i-1}\left(y\right)$), בסתירה לכך ש-$\sigma^i\left(y\right)$ היה הראשון במחזור החדש שהופיע גם בקודם. כך נמשיך עד שלא ייוותרו איברים ב-$\{1, \ldots, n\}$ שלא כתבנו. ■

**כתיב מחזורים קאנוני**: לרוב נהוג להשמיט בכתיב המחזורים את נקודות השבת של התמורה (ואז זוכרים כי מספר שאינו מופיע הוא נקודת שבת). לדוגמה:

$$.\ (1\,2\,5)\,(4)\,(3\,6) = (1\,2\,5)\,(3\,6)$$

כמובן, ישנן דרכים רבות לרשום אותה תמורה כמכפלת מחזורים זרים: סדר המחזורים אינו משנה, ואף כל מחזור באורך $r$ ניתן לרשום ב-$r$ אופנים שונים (צריך לבחור את האיבר הראשון שכותבים מבין $r$ האיברים). לעתים נעדיף להיצמד לצורת כתיבה קאנונית (אז, למשל, אפשר לדעת מיד אם שתי תמורות הן זהות אם לאו). הנה צורת כתיבה נוחה ומקובלת:

- תחילה נכתוב את $1$ ואת המחזור שלו.
  למשל, בעבור התמורה $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 7 & 5 & 1 & 4 & 3 \end{pmatrix}$ נרשום $(1\,6\,4\,5)$.
- אח״כ נמצא את המספר הקטן ביותר שטרם כתבנו, ונוסיף את המחזור שלו.
  בדוגמה שלנו זהו $2$. ונקבל: $(2)\,(1\,6\,4\,5)$.
- כך נמשיך עד אשר כתבנו את כל המספרים.
  בדוגמה שלנו אנחנו צריכים להוסיף את המחזור של 3: $(3\,7)\,(2)\,(1\,6\,4\,5)$ וכעת כל המספרים כבר כתובים.
- לבסוף, נשמיט את המחזורים שבאורך 1, כלומר את נקודות השבת.
  וכך נקבל $(3\,7)\,(1\,6\,4\,5)$.

שימו לב שכאשר כותבים את התמורה ללא נקודות שבת, למשל את $(3\,7)\,(1\,6\,4\,5)$, לעתים איננו יכולים לדעת אם זו תמורה ב-$S_7$, או, למשל, ב-$S_9$. עם זאת, לרוב נבין זאת מתוך ההקשר, ולעתים זה לא באמת ישנה: הרי $S_7$ משוכנת באופן טבעי בתוך $S_9$, ועל כל תמורה ב-$S_7$ אפשר לחשוב כעל תמורה ב-$S_9$.

קל להיווכח כי ההפכי של התמורה

$$(x_1\ \ldots\ x_\ell)\,(y_1\ \ldots\ y_m)\ldots(u_1\ldots u_t)$$

הכתובה כמכפלת מחזורים זרים הוא פשוט

$$(x_\ell\ \ldots\ x_1)\,(y_m\ \ldots\ y_1)\ldots(u_t\ldots u_1)$$

(לאו דווקא בכתיב הקאנוני). למשל, ההפכי של $(3\,7)\,(1\,6\,4\,5)$ הוא $(7\,3)\,(5\,4\,6\,1)$, או בכתיב הקאנוני $(3\,7)\,(1\,5\,4\,6)$. וכיצד מכפילים שתי תמורות הכתובות בכתיב זה? למשל,

$$.\ (1\,6\,4\,5)\,(3\,7)\cdot(2\,7\,4)\,(3\,6\,5) = ?$$

כאן יש לזכור שתמורות הן פונקציות (מהקבוצה $\{1,\ldots,n\}$ לעצמה) ולכן מפעילים קודם את התמורה **הימנית** במכפלה. למשל, במכפלה המסוימת כאן, התמורה הימנית משאירה את 1 במקום, ואז התמונה שלו, כלומר 1, עוברת ל-6 על-ידי התמורה השמאלית. לכן ניתן להתחיל לכתוב את תוצאת המכפלה כך: $(1\,6\,\ldots)$. כעת 6 עובר בתמורה הימנית ל-5, ואז ל-1 בתמורה השמאלית, ולפיכך סגרנו מחזור במכפלה: $(1\,6)$. כעת נעבור למספר הבא שטרם רשמנו: 2. מספר זה עובר ל-7 שעובר ל-3. וקיבלנו $(1\,6)\,(2\,3\ldots)$. כעת $4 \to 6 \to 3$ ולכן $(1\,6)\,(2\,3\,4\ldots)$, ואילו $2 \to 2 \to 4$, ושוב סגרנו מחזור $(1\,6)\,(2\,3\,4)$. אם נשלים את התהליך נקבל $(1\,6)\,(2\,3\,4)\,(5\,7)$, וזו המכפלה המבוקשת, כתובה בכתיב מחזורים קאנוני.

## 4.2 מחלקות הצמידות של $S_n$

חלוקה

**הגדרה 4.4** יהי $n \in \mathbb{N}$. **חלוקה** (partition) של $n$ היא $k$-יית מספרים טבעיים $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k \geq 1$ ($k$ כלשהו) שסכומם $n$.

כל תמורה ב-$S_n$ מגדירה חלוקה של $n$ לפי אורכי המחזורים שלה. למשל, התמורה $(3\,7)\,(1\,6\,4\,5)$ ב-$S_7$ מגדירה את החלוקה $7 = 4 + 2 + 1$, ואילו $(4\,5)\,(2\,6\,3)$ מגדירה את החלוקה $7 = 3 + 2 + 1 + 1$. מסתבר שמחלקת הצמידות של תמורה נקבעת בדיוק לפי החלוקה שהיא מגדירה:

**טענה 4.5** שתי תמורות ב-$S_n$ צמודות אם ורק אם יש להן אותו מבנה מחזורים.
("אותו מבנה מחזורים" פירושו שלשתי התמורות יש אותם אורכי מחזורים, כולל ריבוי.)

**הוכחה:** נראה תחילה שאם שתי תמורות הן צמודות אזי יש להן אותו מבנה מחזורים. תהיינה $\sigma, \tau \in S_n$, ונתבונן בתמורות $\sigma$ ו-$\tau\sigma\tau^{-1}$. נשים לב שאם $\sigma$ מעבירה את $i$ ל-$j$, אז $\tau\sigma\tau^{-1}$ מעבירה את $\tau(i)$ ל-$\tau(j)$:

$$\tau\sigma\tau^{-1}\left(\tau\left(i\right)\right) = \tau\left(\sigma\left(i\right)\right) = \tau\left(j\right)$$

לפיכך, אם בכתיב מחזורים $\sigma$ היא

$$\left(x_1^1\,x_2^1\,\ldots\,x_{r_1}^1\right)\left(x_1^2\,x_2^2\,\ldots\,x_{r_2}^2\right)\ldots\left(x_1^q\,x_2^q\,\ldots\,x_{r_q}^q\right)$$

אז $\tau\sigma\tau^{-1}$ תכתב כך (לאו דווקא בכתיב קאנוני):

$$\left(\tau\left(x_1^1\right)\,\tau\left(x_2^1\right)\,\ldots\,\tau\left(x_{r_1}^1\right)\right)\left(\tau\left(x_1^2\right)\,\tau\left(x_2^2\right)\,\ldots\,\tau\left(x_{r_2}^2\right)\right)\ldots\left(\tau\left(x_1^q\right)\,\tau\left(x_2^q\right)\,\ldots\,\tau\left(x_{r_q}^q\right)\right)$$

ואכן יש להן אותו מבנה מחזורים.

כעת נראה שאכן כל שתי תמורות עם אותו מבנה מחזורים הן צמודות. תהיינה $\sigma, \pi \in S_n$ תמורות עם אותו מבנה מחזורים. נכתוב את שתי התמורות בכתיב מחזורים זו תחת זו, כך שכל מחזור יישב מתחת

למחזור באורך זהה. הפעם נכתוב גם את המחזורים שבאורך $1$, כלומר את נקודות השבת:

$$\begin{aligned}\sigma &= \left(x_1^1\, x_2^1\, \ldots\, x_{r_1}^1\right)\left(x_1^2\, x_2^2\, \ldots\, x_{r_2}^2\right)\ldots\left(x_1^q\, x_2^q\, \ldots\, x_{r_q}^q\right)\\ \pi &= \left(y_1^1\, y_2^1\, \ldots\, y_{r_1}^1\right)\left(y_1^2\, y_2^2\, \ldots\, y_{r_2}^2\right)\ldots\left(y_1^q\, y_2^q\, \ldots\, y_{r_q}^q\right)\end{aligned}$$

ונגדיר את התמורה $\tau \in S_n$ שמעבירה כל $x$ ל-$y$ שמתחתיו, כלומר:

$$\tau\left(x_j^i\right) = y_j^i \quad \forall 1 \le i \le q,\, 1 \le j \le r_i$$

וכעת ברור כי $\pi = \tau\sigma\tau^{-1}$.

■

**הערה 4.6** שימו לב שהתמורה $\tau$ שבנינו בסוף ההוכחה (ככזו שמצמידה את $\sigma$ ל-$\pi$) איננה יחידה.

**תרגיל 4.7**

1. יהיו $G$ חבורה ו-$\sigma \in G$. הוכיחו כי יש התאמה חח״ע בין מחלקת הצמידות $\sigma^G$ לבין המחלקות השמאליות של הרכז $C_G(\sigma)$.
2. יהי $\sigma \in S_n$ מחזור מלא (כלומר, $n$-מחזור). הוכיחו כי $C_{S_n}(\sigma) = \langle\sigma\rangle$.
3. יהי $\sigma = (1\,2\,3\,\ldots\,r) \in S_n$ (כלומר, מחזור לאו-דווקא מלא). מהו $C_{S_n}(\sigma)$?

**מסקנה 4.8** מספר מחלקות הצמידות ב-$S_n$ שווה למספר החלוקות של $n$.

את מספר החלוקות של $n$ נהוג לסמן $p(n)$, כאשר לפונקציה $p$ קוראים **פונקציית החלוקה**. למשל, ב-$S_5$ יש $p(5) = 7$ מחלקות צמידות, המתאימות לחלוקות הבאות. $\boxed{p(n)}$

$1, 1, 1, 1, 1$
$2, 1, 1, 1$
$2, 2, 1$
$3, 1, 1$
$3, 2$
$4, 1$
$5$

פונקציית החלוקה היא פונקציה חשובה בקומבינטוריקה, ונתקל בה פעם נוספת בחלק זה של הספר (בסוף פרק 7). נציין, ללא הוכחה, כי אסימפטוטית, $p(n)$ מתנהגת בערך כמו הפונקציה $e^{\sqrt{n}}$.

**תרגיל 4.9** באמצעות משפט קיילי (משפט 4.1), מצאו שיכון של החבורה $\mathbb{Z}_p^d = \underbrace{\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{d \text{ times}}$ בתוך $S_{p^d}$, והוכיחו כי כל שני איברים לא טריוויאליים (כלומר, שונים מאיבר היחידה) של $\mathbb{Z}_p^d$ נשלחים דרך השיכון לשתי תמורות צמודות.

## 4.3 סימן של תמורה

חילוף

**הגדרה 4.10** **חילוף**, או **טרנספוזיציה**, הוא תמורה מהצורה $(i\,j)$ כאשר $i \neq j$.

החילופים משחקים תפקיד חשוב במושג הסימן של תמורה. לפני שנגדיר מושג זה, נראה כי קבוצת החילופים יוצרת את $S_n$. למעשה, די לקחת חילופים מסוג מסוים, כפי שמדגימה הטענה הבאה:

**טענה 4.11**

1. $S_n = \langle \{(i\,j) \mid 1 \leq i < j \leq n\} \rangle$
2. $S_n = \langle \{(i\,i+1) \mid 1 \leq i \leq n-1\} \rangle$
3. $S_n = \langle \{(1\,i) \mid 2 \leq i \leq n\} \rangle$

**הוכחה:** בשביל (1) מספיק לראות שניתן ליצור כל מחזור על-ידי חילופים, ואכן

$$(x_1\,x_2\,\ldots\,x_r) = (x_1\,x_2)\,(x_2\,x_3)\ldots(x_{r-1}\,x_r)$$

(ודאו זאת). כדי להוכיח את (2) משהוכחנו את (1), די להראות כי הקבוצה ב-(2) יוצרת את כל החילופים. ואכן, אם $i < j$,

$$(i\,j) =$$
$$(i\;\;i+1)\,(i+1\;\;i+2)\cdots(j-2\;\;j-1)\,(j-1\;\;j)\,(j-2\;\;j-1)\cdots(i+1\;\;i+2)\,(i\;\;i+1)$$

(שוב, ודאו זאת). בעבור (3) נשים לב כי כל חילוף $(i\,j)$ ניתן לקבל כך:

$$(i\,j) = (1\,i)\,(1\,j)\,(1\,i)\,.$$

■

למעשה, די בשני איברים על מנת ליצור את $S_n$ כולה, כפי שמראה התרגיל הבא:

**תרגיל 4.12** הוכיחו כי $S_n = \langle (1\,2)\,,(1\,2\,\ldots\,n) \rangle$.

ישנן דרכים רבות לכתוב תמורה נתונה כמכפלה של חילופים, וכמובן שמספר החילופים בכל מכפלה עשוי להיות שונה. אולם ישנה תכונה אחת שנשמרת בכל מכפלה: זוגיות מספר החילופים. כלומר, אם באחת ההצגות של תמורה $\sigma$ כמכפלת חילופים יש מספר זוגי של חילופים, כך יהיה בכל מכפלה אחרת, ואם $\sigma$ היא מכפלה של מספר אי-זוגי של חילופים, אז בכל מכפלה שנותנת את $\sigma$ יהיה מספר אי-זוגי של חילופים. כדי להוכיח זאת עלינו להגדיר מהו סימן של תמורה.

תהי $\sigma \in S_n$. **חילוף סדר** ב-$\sigma$ הוא זוג איברים שונים $i, j \in \{1,\ldots,n\}$ המקיימים

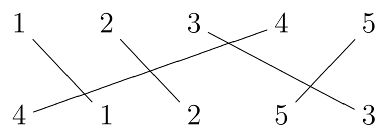
$$i < j$$
$$\sigma(j) < \sigma(i)$$

**הגדרה 4.13** תהי $\sigma \in S_n$, ונסמן ב-$N(\sigma)$ את מספר חילופי הסדר ב-$\sigma$. **הסימן** של $\sigma$ המסומן $\operatorname{sgn}(\sigma)$, מוגדר בתור $(-1)^{N(\sigma)}$. סימן של תמורה

תמורה שסימנה $1$ מכונה **תמורה זוגית**, ותמורה שסימנה $-1$ מכונה **אי-זוגית**. תמורה זוגית

(שימו לב כי $0 \leq N(\sigma) \leq \binom{n}{2}$. בעבור אילו תמורות ב-$S_n$ מספר חילופי הסדר $N(\sigma)$ שווה לאחד הערכים הקיצוניים שלו?)

אפשר לחשוב על חילופי סדר גם באופן גרפי: נרשום את $\sigma$ בצורת טבלה, ונחבר בקו ישר כל מספר בשורה הראשונה עם אותו מספר בשורה השניה. למשל, בעבור $\sigma = (1\,4\,5\,3\,2)$, נקבל:

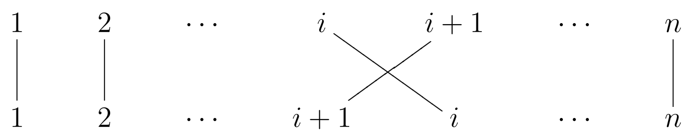



**תרגיל 4.14** הוכיחו כי כל חילוף סדר מתאים לחיתוך של קטעים בשרטוט זה.

לפיכך, מספר חילופי הסדר הוא בדיוק מספר ההצטלבויות. בדוגמה שלנו, יש ארבע הצטלבויות, ולפיכך

$$\operatorname{sgn}(\sigma) = (-1)^4 = 1.$$

**דוגמה 4.15** הסימן של החילוף $(i\ i+1)$ הוא $-1$, שכן יש בדיוק חילוף סדר אחד בתמורה זו:




לפני שנציג מספר הגדרות שקולות למושג הסימן, נוכיח כי פונקצית הסימן היא הומומורפיזם לחבורה שאיבריה הם $\{\pm 1\}$ עם פעולת הכפל. כלומר, פונקצית הסימן משמרת כפל: $\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$. לצורך כך, נתבונן בקבוצת הפולינומים במשתנים $x_1, \ldots, x_n$ עם מקדמים מ-$\mathbb{C}$. קבוצה זו מסומנת[1] $\mathbb{C}[x_1, \ldots, x_n]$. החבורה $S_n$ פועלת על $\mathbb{C}[x_1, \ldots, x_n]$ על-ידי הפעלת התמורה על המשתנים:

$$\sigma.P(x_1, \ldots, x_n) = P\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right) \tag{2}$$

[1] כל פולינום בקבוצה זו הוא סכום סופי של מונומים, וכל מונום הוא ביטוי פורמלי מהצורה $\alpha x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$, עם $r_1, \ldots, r_n$ שלמים אי-שליליים ו-$\alpha \in \mathbb{C}$. נדגיש כי בכל מונום, הסדר של ה-$x_i$-ים אינו חשוב. על קבוצה זו מוגדרים חיבור וכפל בדומה לחיבור ולכפל של פולינומים עם משתנה אחד. למעשה, חיבור וכפל אלו מקנים לקבוצה $\mathbb{C}[x_1, \ldots, x_n]$ מבנה אלגברי של **חוג**, שנכיר בהמשך (ראו סעיף 9.1).

למשל,

$$(1\,2\,3)\,.\,\left[x_1x_2^2-5x_1^4x_2x_3^7\right]=x_2x_3^2-5x_2^4x_3x_1^7$$

**תרגיל 4.16** הוכיחו כי זו אמנם פעולה.

בפרט, נתבונן במסלול של הפולינום

$$f=\prod_{1\le i<j\le n}(x_i-x_j) \tag{3}$$

תחת פעולת $S_n$.

**למה 4.17** לכל $\sigma\in S_n$

$$.\sigma.f=\operatorname{sgn}(\sigma)\cdot f$$

בפרט, המסלול של $f$ תחת פעולת $S_n$ הוא $\{f,-f\}$ (בעבור $n\ge 2$).

**הוכחה:** מתקיים

$$.\sigma.f=\prod_{1\le i<j\le n}\left(x_{\sigma(i)}-x_{\sigma(j)}\right)$$

כל גורם $(x_i-x_j)$ מהמכפלה שמגדירה את $f$ מופיע, עד כדי סימן, גם במכפלה של $\sigma.f$ (ובדיוק פעם אחת): כ-$(x_i-x_j)$ או כ-$(x_j-x_i)$. ולכן $\sigma.f\in\{f,-f\}$. מספר הזוגות $i<j$ שמופיעים ב-$\sigma.f$ עם סימן הפוך, כלומר כ-$(x_j-x_i)$, שווה למספר הזוגות של $i<j$ שבעבורם $\sigma(i)>\sigma(j)$, כלומר בדיוק למספר חילופי הסדר, $N(\sigma)$. ∎

**מסקנה 4.18** פונקציית הסימן היא הומומורפיזם

$$\operatorname{sgn}:S_n\to\{1,-1\}$$

מחבורת התמורות $S_n$ לחבורה $\{1,-1\}$ עם פעולת הכפל. כלומר,

$$.\operatorname{sgn}(\sigma\tau)=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$$

**הוכחה:** מכיוון ש-$S_n$ פועלת על הקבוצה $\{f,-f\}$ לפי המוסבר לעיל, מתקיים

$$\begin{aligned}\operatorname{sgn}(\sigma\tau)f&=(\sigma\tau).f\\&=\sigma.(\tau.f)\\&=\sigma.(\operatorname{sgn}(\tau)\,\mathrm{f})\\&=\operatorname{sgn}(\tau)\cdot\sigma.f\\&=\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)f\end{aligned}$$

ומכאן המסקנה. ∎

**טענה 4.19** כל חילוף $\tau=(i\,j)\in S_n$ הוא תמורה אי-זוגית (כלומר, $\operatorname{sgn}(i\,j)=-1$).

**הוכחה:** כפי שראינו בהוכחת טענה 4.11 $(2)$, ניתן להציג כל חילוף כמכפלת חילופים מהצורה $(i\ i+1)$. יתר על כן, מספר החילופים מצורה זו הדרוש הוא אי-זוגי (השתמשנו שם בדיוק ב-$2(j-i)-1$ חילופים). בדוגמה 4.15 ראינו כי $\operatorname{sgn}(i\ i+1)=-1$. לפיכך, $\operatorname{sgn}(i\ j)$ יהיה שווה ל-

$$\operatorname{sgn}(i\ i+1)\cdot\operatorname{sgn}(i+1\ i+2)\cdot\ldots\cdot\operatorname{sgn}(j-1\ j)\cdot\ldots\cdot\operatorname{sgn}(i+1\ i+2)\cdot\operatorname{sgn}(i\ i+1)$$

כלומר:

$$\operatorname{sgn}(i\ j)=(-1)^{2(j-i)-1}=-1$$

■

**מסקנה 4.20** אם $\sigma=\tau_1\ldots\tau_r$ כאשר $\tau_1,\ldots,\tau_r$ חילופים (לאו דווקא זרים), אזי

$$\operatorname{sgn}(\sigma)=(-1)^r.$$

בפרט, מספר החילופים בהצגת תמורה כמכפלת חילופים הוא לעולם זוגי (אם התמורה זוגית) או לעולם אי-זוגי (אם התמורה אי-זוגית).

**תרגיל 4.21** יהי $\sigma\in S_n$ מחזור. הוכיחו כי אם האורך של $\sigma$ זוגי, אזי הוא תמורה אי-זוגית, ולהפך: אם האורך אי-זוגי, הוא תמורה זוגית.

נסכם את ההגדרות השקולות שנתנו לפונקציית הסימן:

**משפט 4.22** תהי $\sigma\in S_n$ תמורה. אזי כל הביטויים הבאים שווים בערכם, ומספקים לפיכך הגדרות שקולות בעבור $\operatorname{sgn}(\sigma)$:

1. $(-1)^{N(\sigma)}$, כאשר $N(\sigma)$ מציין את מספר חילופי הסדר ב-$\sigma$
2. $\frac{\sigma.f}{f}$, כאשר $f=\prod_{1\le i<j<n}(x_i-x_j)$ והפעולה של $S_n$ מוגדרת במשוואה $(2)$ שבעמוד 81
3. $(-1)^r$ כאשר $\sigma=\tau_1\cdot\tau_2\cdot\ldots\cdot\tau_r$ ו-$\tau_1,\ldots,\tau_r$ חילופים כלשהם
4. $\prod_{1\le i<j\le n}\frac{\sigma(j)-\sigma(i)}{j-i}$
5. $(-1)^{n-t}$ כאשר $\sigma$ תמורה עם בדיוק $t$ מחזורים, כולל נקודות שבת
6. $(-1)^k$ כאשר $\sigma=\gamma_1\cdot\ldots\cdot\gamma_m$ ו-$\gamma_1,\ldots,\gamma_m$ מחזורים כלשהם ו-$k$ מתוכם באורך זוגי

**הוכחה:** את השוויון של שלושת הביטויים הראשונים כבר ראינו בטענות ובמסקנות הקודמות. את השוויון של שלושת הנותרים נותיר כתרגיל.

■

**תרגיל 4.23** השלימו את הוכחת משפט 4.22. כלומר, הראו כי שלושת הביטויים $(6)-(4)$ שווים אף הם לסימן של $\sigma$.

בפרט, שימו לב שניתן "לקרוא" את הסימן של תמורה מתוך מבנה המחזורים שלה.

**הגדרה 4.24** אוסף התמורות הזוגיות מסומן $A_n$, ונקרא באנגלית: Alternating Group.[2]   $\boxed{A_n}$

[2] אין בעברית מונח מוסכם או מקובל בעבור החבורה $A_n$. יש המכנים אותה **חבורת החלופין**, אך גם שם זה איננו רווח.

כמובן, $A_n$ זו תת-חבורה נורמלית של $S_n$: היא הגרעין של הומומורפיזם הסימן. בעבור $n \geq 2$ הסדר של $A_n$ הוא

$$|A_n| = \frac{n!}{2}.$$

הואיל וראינו שכל תמורה של $S_n$ היא מכפלה של חילופים, איברי $A_n$ ניתנים לכתיבה כמכפלה של מספר **זוגי** של חילופים כאלה.

ראינו לעיל כי מחלקות הצמידות ב-$S_n$ נקבעות לפי מבנה המחזורים של התמורה. יתר על כן, מבנה המחזורים קובע את סימן התמורה, ועל כן $A_n$ היא איחוד של מחלקות צמידות שלמות, המחלקות "הזוגיות", של $S_n$. עם זאת, מסתבר כי ב-$A_n$ מבנה המחזורים כבר אינו קובע את מחלקת הצמידות, כפי שמראה התרגיל הבא.

**תרגיל 4.25** מצאו שתי תמורות זוגיות ב-$S_5$ שהן צמודות ב-$S_5$ אך אינן צמודות ב-$A_5$.

**תרגיל 4.26** נגדיר העתקה $f : S_n \to \mathrm{GL}_n(\mathbb{R})$ ששולחת את התמורה $\sigma$ למטריצה שבה יש 1 במקום $(i, \sigma(i))$ לכל $1 \leq i \leq n$, וכל יתר האיברים הם 0.

1. הוכיחו כי $f$ היא מונומורפיזם.
2. הוכיחו כי $\det \circ f = \mathrm{sgn}$. כלומר, הפונקציה sgn כמוה כצמצום של הפונקציה (שהיא בפרט הומומורפיזם) $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ לתת-החבורה (האיזומורפית ל-$S_n$).
   שימו לב שבכך קיבלנו הוכחה נוספת למסקנה 4.18.

**תרגיל 4.27** המרחק בין שני קדקודים בגרף קשיר הוא אורך המסילה הקצר ביותר בינהם. הקוטר של גרף קשיר הוא המרחק הגדול ביותר בין זוג קדקודים. בתרגיל זה נראה כי הקוטר של גרף קיילי

$$\mathrm{Cay}(S_n, \{(1\,2), (1\,2\,\ldots\,n)\})$$

הוא מסדר גודל ריבועי ב-$n$ (את המושג גרף קיילי הכרנו בסעיף 1.4.2 לעיל).

תרגיל 4.12 פירושו שכל תמורה $\theta \in S_n$ שווה למילה כלשהי באיברים $\tau, \sigma, \sigma^{-1}$ כאשר $\tau = (1\,2)$ ו-$\sigma = (1\,2\,\ldots\,n)$. נסמן ב-$\ell(\theta)$ את האורך של המילה הקצרה ביותר ב-$\tau, \sigma^{\pm 1}$ שמייצגת את $\theta$.

1. הוכיחו כי קיים $0 < c_1 \in \mathbb{R}$ כך ש-$\ell(\theta) < c_1 n$ לכל <u>חילוף</u> $\theta \in S_n$ ולכל $n \geq 1$.
2. הוכיחו כי קיים $0 < c_2 \in \mathbb{R}$ כך ש-$\ell(\theta) < c_2 n^2$ לכל <u>תמורה</u> $\theta \in S_n$ ולכל $n \geq 1$.
3. לכל $\pi \in S_n$ ולכל שלשה של מספרים $i, j, k$, נאמר שהשלשה $\{i, j, k\}$ היא "טובה" אם הסדר הצקלי שלה נשמר ב-$\pi$, ו"רעה" אחרת. באופן פורמלי, נניח כי $1 \leq i < j < k \leq n$, נמיין את $\{\pi(i), \pi(j), \pi(k)\}$ מהקטן לגדול. התמורה המושרית מ-$\pi$ במקומות $i, j, k$ היא התמורה ב-$S_3$ ששולחת את 1 למיקום היחסי של $\pi(i)$, את 2 למיקום היחסי של $\pi(j)$ ואת 3 לזה של $\pi(k)$.
   למשל, אם $\pi(k) < \pi(i) < \pi(j)$, התמורה המושרית היא $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. נאמר ששלשה היא "רעה" ביחס לתמורה $\pi \in S_n$ אם הסימן של התמורה המושרית הוא $-1$, ונגדיר פונקציה $f\colon S_n \to \mathbb{N}_{\geq 0}$ כך ש-$f(\pi)$ הוא מספר השלשות הרעות ביחס ל-$\pi$.
   הוכיחו כי $f(\pi) = f(\pi\sigma) = f(\pi\sigma^{-1})$ וכי $|f(\pi) - f(\pi\tau)| < n$.
4. התבוננו בתמורה $\beta_n = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ n & n-1 & n-2 & \ldots & 1 \end{pmatrix} \in S_n$. העזרו בסעיף הקודם על מנת להראות שקיים $0 < c_3 \in \mathbb{R}$ כך ש-$\ell(\beta_n) \geq c_3 n^2$ לכל $n$.
5. הסבירו מדוע נובע מהסעיפים הקודמים כי הקוטר של $\mathrm{Cay}(S_n, \{(1\,2), (1\,2\,\ldots\,n)\})$ הוא בתחום $[c_3 n^2, c_2 n^2]$, ולכן מסדר גודל ריבועי ב-$n$.

## 4.4 פשטות $A_n$ בעבור $n \geq 5$

ציינו כבר (הגדרה 3.38) כי חבורה פשוטה היא חבורה לא טריוויאלית שאין לה תת-חבורות נורמליות (פרט לעצמה ול-$\{e\}$, כמובן). עד כה, החבורות היחידות שהוכחנו שהן פשוטות היו החבורות הצקליות $\mathbb{Z}_p$ ($p$ ראשוני). להלן נוכיח קיום של משפחה אינסופית נוספת של חבורות פשוטות: החבורות $A_n$ בעבור $n \geq 5$. למעשה, הוכחת הפשטות של חבורות אלו, ובפרט של $A_5$, היוותה ציון דרך קריטי בהתפתחות תורת החבורות, ואפשרה למתמטיקאים אבל (Abel) וגלואה (Galois) להוכיח כי אין "נוסחה כללית" למציאת שורש של פולינום ממעלה חמישית (על כך בפרק 18).

לפני שנצלול להוכחה, נשים לב כי $A_4$ אמנם אינה פשוטה:

$$\{e, (1\,2)\,(3\,4)\,, (1\,3)\,(2\,4)\,, (1\,4)\,(2\,3)\} = V \trianglelefteq A_4$$

חבורה זו, $V$, נקראת גם **חבורת קליין** (Klein), והיא איזומורפית ל-$\mathbb{Z}_2 \times \mathbb{Z}_2$. בעבור $n = 3$ מתקיים $A_3 \cong \mathbb{Z}_3$ ולכן $A_3$ דווקא כן פשוטה. בעבור $n = 1, 2$, $A_n$ היא טריוויאלית (ועל כן אינה פשוטה). חבורת קליין

**תרגיל 4.28**

1. הוכיחו כי אכן $V \trianglelefteq A_4$.
2. הוכיחו כי בעבור $n \geq 3$, המרכז של $S_n$ הוא טריוויאלי.

**טענה 4.29** החבורה $A_n$ ($n \geq 1$) נוצרת על-ידי כל ה-3-מחזורים.
למעשה, ה-3-מחזורים מהצורה $(1\,i\,j)$ מספיקים.

**הוכחה:** ראינו בטענה 4.11 (3) כי $S_n$ נוצרת על-ידי החילופים מהצורה $(1\ i)$. בפרט, כל תמורה זוגית היא מכפלה של מספר זוגי של חילופים כאלה. על כן, די להוכיח שמכפלת כל זוג חילופים כאלה מתקבלת כמכפלת 3-מחזורים. ואכן, כל אימת ש-$j \neq i$ מתקיים $(1\,i)\,(1\,j) = (1\,j\,i)$. ■

**למה 4.30** יהי $n \geq 5$, ותהי $N \trianglelefteq A_n$. אם $N$ מכילה 3-מחזור, אז $N = A_n$.

**הוכחה:** נניח כי $(a\,b\,c) \in N$. נראה כי כל 3-מחזור נמצא ב-$N$ ובכך נסיים לפי טענה 4.29. נתבונן ב-3-מחזור $(i\,j\,k)$. לפי טענה 4.5, קיימת תמורה $\tau \in S_n$ כך ש-

$$.\tau\,(a\,b\,c)\,\tau^{-1} = (i\,j\,k)$$

אם במקרה $\tau \in A_n$, סיימנו. אחרת, מכיוון ש-$n \geq 5$, קיימים $d, e \in \{1, \ldots, n\}$ השונים מ-$a$, $b$ ו-$c$, ואז $(a\,b\,c)$ ו-$(d\,e)$ תמורות מתחלפות. מכיוון ש-$\tau$ תמורה אי-זוגית, $\tau\,(d\,e) \in A_n$ תמורה זוגית. ואז

$$.N \ni (\tau\,(d\,e))\,(a\,b\,c)\,(\tau\,(d\,e))^{-1} = \tau\,(d\,e)\,(a\,b\,c)\,(e\,d)\,\tau^{-1} = \tau\,(a\,b\,c)\,\tau^{-1} = (i\,j\,k)$$

■

**משפט 4.31** החבורה $A_n$ פשוטה לכל $n \geq 5$.

**הוכחה:** תהי $\{e\} \neq N \trianglelefteq A_n$. עלינו להראות כי $N = A_n$. נבחין בין המקרים הבאים, לפי הפירוק של איברי $N$ למכפלות של מחזורים זרים:

1. נניח כי $N$ מכילה תמורה שאחד המחזורים בה באורך 4 לפחות. כלומר:

$$N \ni \sigma = (a_1\, a_2\, \ldots\, a_r)\,(b_1\, \ldots\, b_s)\ldots(c_1\, \ldots\, c_t)$$

פירוק למחזורים זרים עם $r \geq 4$. או אז נביט בתמורה

$$.N \ni \tau = \underbrace{(a_1\, a_2\, a_3)\,\sigma\,(a_1\, a_2\, a_3)^{-1}}_{\in N}\,\underbrace{\sigma^{-1}}_{\in N}$$

ראינו כבר כי אם תמורה נתונה $\gamma$ שולחת את $i$ ל-$j$, אזי ההצמדה שלה על-ידי התמורה $\delta$ שולחת את $\delta(i)$ ל-$\delta(j)$. לפיכך,

$$\begin{aligned}\sigma\,(a_1\, a_2\, a_3)^{-1}\,\sigma^{-1} &= \sigma\,(a_3\, a_2\, a_1)\,\sigma^{-1}\\ &= (\sigma(a_3)\ \sigma(a_2)\ \sigma(a_1))\\ &= (a_4\, a_3\, a_2)\end{aligned}$$

וקיבלנו

$$\begin{aligned}N \ni \tau &= (a_1\, a_2\, a_3)\,\sigma\,(a_1\, a_2\, a_3)^{-1}\,\sigma^{-1}\\ &= (a_1\, a_2\, a_3)\,(a_4\, a_3\, a_2)\\ &= (a_1\, a_2\, a_4)\end{aligned}$$

כלומר $N$ מכילה 3-מחזור וסיימנו לפי הלמה.

2. נניח כי $N$ מכילה תמורה שיש בה שני מחזורים באורך 3. כלומר:

$$.N \ni \sigma = (a\, b\, c)\,(x\, y\, z)\,(\ldots)\ldots$$

או אז:

$$\begin{aligned}N \ni (b\, c\, x)\,\sigma\,(b\, c\, x)^{-1}\,\sigma^{-1} &= (b\, c\, x)\,\sigma\,(x\, c\, b)\,\sigma^{-1}\\ &= (b\, c\, x)\,(\sigma(x)\ \sigma(c)\ \sigma(b))\\ &= (b\, c\, x)\,(y\, a\, c)\\ &= (a\, x\, b\, c\, y)\end{aligned}$$

וסיימנו לפי מקרה 1.

3. נניח כי $N$ מכילה תמורה שיש בה מחזור באורך 3, ואילו יתר המחזורים בה באורך 2 או 1. כלומר:

$$.N \ni \sigma = (a\,b\,c)\,(x_1\,y_1)\,(x_2\,y_2)\ldots(x_q\,y_q)$$

אך אז $N \ni \sigma^2 = (a\,c\,b)$ ושוב סיימנו לפי הלמה.

4. לבסוף, אם $N$ אינה מכילה אף תמורה כמו באחד המקרים הנ״ל, היא בהכרח מכילה תמורה שכל המחזורים בה באורך 2 או 1:

$$.N \ni \sigma = (a\,b)\,(c\,d)\ldots$$

במקרה זה

$$\begin{aligned} N \ni \tau = (a\,b\,c)\,\sigma\,(a\,b\,c)^{-1}\,\sigma^{-1} &= (a\,b\,c)\,\sigma\,(c\,b\,a)\,\sigma^{-1} \\ &= (a\,b\,c)\,(d\,a\,b) \\ &= (a\,c)\,(b\,d) \end{aligned}$$

ואז בעבור $e \notin \{a, b, c, d\}$

$$\begin{aligned} N \ni (a\,b\,e)\,\tau\,(a\,b\,e)^{-1}\,\tau^{-1} &= (a\,b\,e)\,\tau\,(e\,b\,a)\,\tau^{-1} \\ &= (a\,b\,e)\,(e\,d\,c) \\ &= (a\,b\,e\,d\,c) \end{aligned}$$

ושוב סיימנו לפי מקרה 1.

■

**תרגיל 4.32** היכן בדיוק נעזרנו בהוכחה בהנחה ש-$n \geq 5$? (יש לפחות שני מקומות כאלה.)

**תרגיל 4.33** בתרגיל זה נראה, בין היתר, הוכחה ישירה לכך ש-$A_5$ פשוטה.

1. תהיינה $G$ חבורה ו-$H \leq G$ תת-חבורה. הוכיחו כי $H \trianglelefteq G$ אם ורק אם $H$ היא איחוד של מחלקות צמידות.
2. בהסתמך על (1) ועל משפט לגרנז', הוכיחו כי ל-$S_5$ יש בדיוק שלוש תת-חבורות נורמליות: $\{e\}$, $A_5$ ו-$S_5$.
(הדרכה: חשבו את הגדלים של מחלקות הצמידות של $S_5$. הראו שלא ניתן להרכיב תת-חבורה אחרת של $S_5$ שתהיה איחוד של מחלקות צמידות.)
3. הוכיחו כי ל-$A_5$ יש בדיוק 5 מחלקות צמידות וכי גדליהן $1, 12, 12, 15$ ו-20.
(הדרכה: אילו ממחלקות הצמידות של $S_5$ מורכבות מתמורות זוגיות? מבין אלה, חשבו אילו נשארות מחלקות צמידות גם ב-$A_5$ ואילו מתפצלות לשתי מחלקות צמידות שונות.)
4. העזרו שוב בסעיף (1) ובמשפט לגרנז' על מנת להוכיח ישירות כי אמנם $A_5$ פשוטה.

**תרגיל 4.34** הוכיחו כי לכל $n \geq 5$, $A_n$ היא תת-החבורה הנורמלית היחידה של $S_n$ (פרט ל-$S_n$ ול-$\{e\}$).

**תרגיל 4.35** הוכיחו ישירות כי $A_6$ פשוטה. פעלו לפי השלבים הבאים שמחקים את הוכחת הפשטות של $A_5$ מתרגיל 4.33:

1. הראו כי ל-$A_6$ יש בדיוק 7 מחלקות צמידות, ושגדליהן $1, 40, 40, 45, 72, 72, 90$.
2. השלימו את ההוכחה בעזרת משפט לגרנז'.

**תרגיל 4.36** בתרגיל זה נספק הוכחה נוספת לכך ש-$A_n$ פשוטה לכל $n \geq 5$, בהסתמך על הפשטות של $A_5$ ושל $A_6$ (שהוכחנו ישירות בתרגילים 4.33 ו-4.35). יהי $n \geq 7$ ותהי $\{e\} \neq N \trianglelefteq A_n$ תת-חבורה נורמלית לא טריוויאלית. נראה כי בהכרח $N = A_n$.

1. תהי $e \neq \sigma \in N$ תמורה לא טריוויאלית ב-$N$, ונניח כי $\sigma(i) = j$ עבור $i \neq j$. יהיו $k, \ell \in \{1, \ldots, n\}$ שני מספרים נוספים ששונים מ-$i$ ומ-$j$, ונתבונן בתמורה $\pi = (j\,k\,\ell)\,\sigma\,(j\,k\,\ell)^{-1}\,\sigma^{-1}$. הוכיחו כי $\pi \in N$ וכי $\pi \neq e$.
2. הוכיחו כי $\pi$ משנה את מיקומם של ששה מספרים לכל היותר (כלומר, יש לה לפחות $n-6$ נקודות שבת).
3. יהי $H$ עותק (כלומר, שיכון) של $A_6$ בתוך $A_n$ שמורכב מכל התמורות הזוגיות על ששת המספרים הללו (אם $\pi$ מזיזה פחות מ-6 מספרים, ניתן לבחור קבוצה כלשהי בגודל 6 המכילה את המספרים ש-$\pi$ מזיזה). הוכיחו כי $H \cap N \trianglelefteq H$ והסיקו כי $H \leq N$ (רמז: השתמשו בכך ש-$\pi \in H \cap N$ וכן בפשטות של $A_6$).
4. הסיקו כי $N$ מכילה 3-מחזור והסיקו כי $N = A_n$ לפי למה 4.30.

# 5 חבורות $p$ ומשפטי סילו

במשפט לגרנז' (משפט 1.81) ראינו כי אם $G$ חבורה סופית מסדר $n$ אז הסדר של כל תת-חבורה של $G$ מחלק את $n$. כמובן, אין להסיק מכך שאם $G$ מסדר $n$ ו-$r|n$ מחלק של $n$ אז קיימת ב-$G$ תת-חבורה מסדר $r$. למשל, ל-$A_5$ אין תת-חבורה מסדר $30$: לו הייתה, הייתה זו תת-חבורה מאינדקס 2 ולפיכך נורמלית (תרגיל 1.89), וזאת בסתירה לפשטות $A_5$.

אולם מסתבר שאם $r$ הוא חזקה של מספר ראשוני, כלומר, אם הסדר של $|G|$ מתחלק ב-$p^\alpha$ כאשר $p$ ראשוני ו-$\alpha \in \mathbb{N}$ כלשהו, אז קיימת ב-$G$ תת-חבורה מסדר $p^\alpha$. עובדה זו היא אחת מבין קובץ עובדות שידועות כ**משפטי סילו** (Sylow) שנוכיח להלן. אך נתחיל בהכרת חבורות מטיפוס מיוחד אשר יופיעו גם במשפטי סילו: חבורות שהסדר שלהן הוא חזקת ראשוני.

## 5.1 חבורות-$p$

חבורת-$p$

**הגדרה 5.1** יהי $p \in \mathbb{N}$ ראשוני. חבורה $G$ נקראת **חבורת-**$p$ אם מתקיים[1]

$$|G| = p^k$$

עם $k \in \mathbb{N}$.

**משפט 5.2** אם $G$ חבורת-$p$ אז המרכז של $G$ **אינו** טריוויאלי.

**הוכחה:** הוכחת משפט זה מתבססת על משפט מסלול-מייצב (2.21): אם חבורה סופית $G$ פועלת על קבוצה $X$, אזי לכל $x \in X$ מתקיים

$$|G| = |O(x)| \cdot |G_x| ,$$

כאשר $O(x)$ המסלול של $x$ ו-$G_x$ המייצב של $x$. נזכיר כי $G$ פועלת על עצמה על-ידי הצמדה, והמסלולים בפעולה זו נקראים מחלקות צמידות. נסמן ב-

$$\{e\} = C_1, C_2, \ldots, C_h$$

את מחלקות הצמידות, כאשר $C_i = g_i^G$, כלומר, $C_i$ זו מחלקת הצמידות של $g_i$, ובפרט

$$. |G| = \sum_{i=1}^{h} |C_i|$$

איברי המרכז $Z(G)$ הם בדיוק נקודות השבת של פעולה זו, כלומר מחלקות הצמידות שגודלן 1. נניח בלי הגבלת הכלליות[2] כי מחלקות הצמידות שבגודל 1 הן $C_1, \ldots, C_r$, כלומר $r = |Z(G)|$ ו-

$$. |G| = |Z(G)| + \textstyle\sum_{i=r+1}^{h} |C_i|$$

---

[1] ניתן להכליל את ההגדרה לחבורות אינסופיות. במקרה זה נאמר כי חבורה $G$, לאו דווקא סופית, היא חבורת-$p$ אם הסדר של כל איבר בה הוא חזקה של $p$ (כולל $1$, כמובן). במקרה הסופי שתי ההגדרות שקולות, כפי שניתן להסיק ממשפט קושי (משפט 2.41) וממשפט לגרנז' (משפט 1.81). להלן, אלא אם יצוין אחרת, אנחנו עוסקים במקרה הסופי בלבד.
ניתן להחשיב גם את החבורה הטריוויאלית כחבורת-$p$ (לכל ראשוני $p$), אולם בספר זה לרוב נתכוון רק לחבורות לא טריוויאליות.

[2] כאשר מניחים דבר מה "בלי הגבלת הכלליות" (בקיצור: בה"כ), הכוונה היא שגם אם מוכיחים את הטענה תחת הנחה נוספת זו, ברור כי נובע מכך שהטענה נכונה גם במקרה הכללי.

כזכור, גודל מסלול מחלק את גודל החבורה (זהו חלק ממשפט 2.21 - משפט מסלול-מייצב). מכיוון ש- $|G| = p^k$, כל יתר המחלקות הן מגודל שהוא חזקה חיובית של $p$, ובפרט גודל שמתחלק ב-$p$. לכן מתקיים

$$p \mid \left(|G| - \sum_{i=r+1}^{h} |C_i|\right) = |Z(G)|$$

ובפרט $Z(G) \neq \{e\}$. ∎

מכיוון שלכל חבורה מתקיים $Z(G) \trianglelefteq G$, נוכל להסיק:

**מסקנה 5.3** אם $G$ חבורת-$p$ לא אבלית, $G$ אינה פשוטה.

**מסקנה 5.4** אם $|G| = p^2$ אז $G$ אבלית.

**הוכחה:** מכיוון ש-$|Z(G)| \mid p^2$ מתקיים $|Z(G)| \in \{1, p, p^2\}$. אך המרכז אינו טריוויאלי ולכן $|Z(G)| \neq 1$. אם $|Z(G)| = p^2$ סיימנו. נניח אם כן כי $|Z(G)| = p$. יהי[3] $x \in G - Z(G)$. חבורת המנה $G/Z(G)$ היא בגודל $p$ ולפיכך צקלית, ולכן מתקיים

$$G/Z(G) = \langle xZ(G) \rangle.$$

על כן כל איבר ב-$G$ ניתן לרשום כמכפלה $x^j y$ עם $j \in \{0, 1, \ldots, p-1\}$ ועם $y \in Z(G)$. אך מכאן נובע שכל שני איברים ב-$G$ מתחלפים: אם $g_1 = x^{j_1} y_1$ ו-$g_2 = x^{j_2} y_2$, נקבל

$$g_1 g_2 = x^{j_1} y_1 x^{j_2} y_2 = y_1 y_2 x^{j_1} x^{j_2} = y_1 y_2 x^{j_2} x^{j_1} = x^{j_2} y_2 x^{j_1} y_1 = g_2 g_1$$

ולכן $G$ אבלית (למעשה קיבלנו במקרה זה סתירה כי הראינו ש-$Z(G) = G$). ∎

**תרגיל 5.5** תהי $G$ חבורה כלשהי. הוכיחו כי אם $G/Z(G)$ צקלית, אזי $G$ אבלית.

בעבור חבורות-$p$, מתקיים "המשפט ההפוך" למשפט לגרנז', כלומר, ישנה תת-חבורה מכל סדר שמחלק את סדר החבורה:

**משפטון 5.6** אם $|G| = p^k$ אז $G$ מכילה תת-חבורה מסדר $p^i$ לכל $0 \leq i \leq k$.

**הוכחה:** נוכיח באינדוקציה על $k$. בעבור $k = 1$ הטענה ברורה. בעבור $k$ כללי, ראינו כי המרכז $Z(G)$ אינו טריוויאלי, ולכן, לפי משפט קושי (משפט 2.41), קיים איבר $x \in Z(G)$ מסדר $p$. מכיוון ש-$x$ במרכז, הוא מתחלף עם כל $g \in G$, ובפרט $g \langle x \rangle g^{-1} = \langle x \rangle$. לכן $G \trianglelefteq \langle x \rangle$. חבורת המנה $G/\langle x \rangle$ היא מסדר $p^{k-1}$, ולפי הנחת האינדוקציה יש לה תת-חבורות

$$\{e\} = \overline{H_0}, \overline{H_1}, \ldots, \overline{H_{k-1}} = G/\langle x \rangle$$

מסדרים $p^0, p^1, \ldots, p^{k-1}$ בהתאמה. לפי משפט ההתאמה, חבורות אלה מתאימות לתת-חבורות של $G$

$$\langle x \rangle = H_0, H_1, \ldots, H_{k-1} = G,$$

וקל לבדוק שהסדרים של תת-חבורות אלה הם $p, p^2, \ldots, p^k$ בהתאמה. ∎

[3] סימן המינוס ב-$G - Z(G)$ מסמל חיסור קבוצות.

בפרק הבא (מסקנה 6.32) נראה הוכחה נוספת לטענה האחרונה.

**תרגיל 5.7** תהי $G$ חבורה מסדר $p^2$. הוכיחו כי $G \cong \mathbb{Z}_{p^2}$ או $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

**תרגיל 5.8** יהיו $p$ ראשוני, $X$ קבוצה כך ש-$|X| \nmid p$, ו-$G$ חבורת-$p$ הפועלת על $X$. הראו שקיים $x \in X$ כך ש-$G_x = G$.

## 5.2 משפטי סילו

**הגדרה 5.9** תהי $G$ חבורה מסדר $|G| = n = p^r m$ כאשר $p$ ראשוני, $1 \leq r$, ו-$p \nmid m$.
כל תת-חבורה מסדר $p^r$ נקראת **חבורת $p$-סילו**[4] של $G$.
את קבוצת חבורות $p$-סילו של $G$ נסמן ב-$Syl_p\left(G\right)$.

חבורת $p$-סילו

$Syl_p\left(G\right)$

שימו לב שחבורת $p$-סילו של $G$ היא **תת**-חבורה של $G$. בנוסף, תת-חבורה $H \leq G$ היא חבורת $p$-סילו אם ורק אם $H$ היא חבורת-$p$ ו-$p \nmid [G\colon H]$. בשנת 1872 הוכיח המתמטיקאי הנורבגי סילו[5] (Sylow), שמשרתו העיקרית הייתה הוראה בבית-ספר תיכון, סדרת משפטים הקרויים על שמו, אשר מהווים את אחד מעמודי התווך של תורת החבורות הסופיות.

**משפט 5.10 (המשפט ה-I של סילו)** אם $p$ ראשוני ו-$p \mid |G|$ אז יש ל-$G$ חבורת $p$-סילו.

משפט זה, שנוכיח מיד, מספק הוכחה נוספת של משפט קושי (משפט 2.41):

**מסקנה 5.11 (משפט קושי)** אם $p$ ראשוני ו-$p \mid |G|$ אז יש ב-$G$ איבר מסדר $p$.

**הוכחה:** תהי $P \in Syl_p\left(G\right)$ חבורת $p$-סילו של $G$, כלומר $|P| = p^r$. יהי $e \neq x \in P$. לפי משפט לגרנז', הסדר של $x$ מחלק את $p^r$, ולכן

$$|x| = p^b$$

עם $1 \leq b \leq r$ כלשהו. לאיבר $x^{p^{b-1}}$ יש סדר $p$. ■

מכיוון שחבורה בגודל $p^k$ מכילה תת-חבורה מכל סדר $p, p^2, \ldots, p^{k-1}$ (משפטון 5.6), נקבל גם את המסקנה הבאה:

**מסקנה 5.12** יהי $p$ ראשוני ו-$\alpha$ טבעי. אם $p^\alpha \mid |G|$ אז $G$ מכילה תת-חבורה בגודל $p^\alpha$.

**הוכחה: (של המשפט ה-I של סילו)** נניח כי $|G| = n = p^r \cdot m$ עם $(m,p) = 1$. נתבונן בקבוצה

$$\Sigma = \{S \subseteq G \,|\, \text{קבוצה בגודל } p^r \; S\}.$$

שימו לב ש-$\Sigma$ היא קבוצה שכל אחד מאיבריה הוא תת-קבוצה של $G$, ולאו דווקא תת-חבורה. מטרתנו למצוא $S \in \Sigma$ שהיא גם תת-חבורה. עם זאת, לא נעשה זאת ישירות. במקום זאת, נסתכל בפעולת $G$ על $\Sigma$ על-ידי כפל משמאל:

$$G \times \Sigma \to \Sigma \qquad (g,S) \to g \cdot S = \{gs \,|\, s \in S\}$$

[4] אם $p \nmid |G|$, ניתן לומר שתת-החבורה הטריוויאלית $\{e\}$ היא חבורת $p$-סילו של $G$.

[5] למען הדיוק, נציין שהגיית השם Sylow בנורבגית דומה יותר ל״סילוב״, בב׳ רפה, אולם הצורה ״סילו״ דומה יותר להגיה האנגלית שהשתרשה בעולם, ואנו נצמד לה.

(ודאו שאתם מבינים מדוע זו פעולה). מיד נוכיח שלאחד מאיברי הקבוצה, כלומר לתת-קבוצה מסוימת של $G$ בגודל $p^r$, יש מייצב בגודל $p^r$. מכך ינבע המשפט שכן כל מייצב הוא תת-חבורה. (עלינו להדגיש שבמבט ראשון אין זה ברור כלל מה הקשר בין גודל המייצב לבין גודל כל תת-קבוצה ב-$\Sigma$, ומדוע ניתן למצוא מייצב שגודלו כגודל תת-הקבוצות).

**למה א׳** : מספר איברי $\Sigma$,

$$|\Sigma| = \binom{n}{p^r} = \frac{n\,(n-1)\ldots(n-p^r+1)}{p^r\,(p^r-1)\ldots 1} \tag{4}$$

זר ל-$p$.

**הוכחת למה א׳:** אם נוכיח שלכל $0 \leq k < p^r$, החזקה הגבוהה ביותר של $p$ שמחלקת את $n-k$ שווה לחזקה הגבוהה ביותר של $p$ שמחלקת את $p^r-k$, נקבל שמספר הפעמים ש-$p$ מופיע כגורם במונה של (4), שווה למספר הפעמים שהוא מופיע במכנה, ולפיכך הביטוי $(4)$ אמנם זר ל-$p$.

אכן, בעבור $k=0$ הטענה ברורה. בעבור $1 \leq k < p^r$ נרשום $k = p^b \cdot \ell$ כאשר $0 \leq b < r$ ו-$p \nmid \ell$. ואז

$$n-k = p^r \cdot m - p^b \cdot \ell = p^b\left(p^{r-b} \cdot m - \ell\right)$$

ומכיוון ש-$p^{r-b} \cdot m - \ell$ זר ל-$p$, החזקה הגבוהה ביותר של $p$ שמחלקת את $n-k$ היא $p^b$.

באופן דומה,

$$p^r - k = p^b\left(p^{r-b} - \ell\right)$$

וגם החזקה הגבוהה ביותר של $p$ שמחלקת את $p^r-k$ היא $p^b$. ■

**למה ב׳:** לכל $S \in \Sigma$, המייצב $G_S$ הוא חבורת $p$-(אולי טריוויאלית).

**הוכחת למה ב׳:** תהי $S \in \Sigma$, ונסמן ב-$H = G_S$ את המייצב של $S$. כלומר, לכל $s \in S$ ולכל $h \in H$ מתקיים $hs \in S$. לכן, לכל $s \in S$,

$$H \cdot s \subseteq S.$$

לפיכך, $S$ היא איחוד של מחלקות ימניות של $H$, אך כל שתי מחלקות כאלה זרות או מתלכדות, וכולן שוות-גודל. לכן

$$|H| \mid |S| = p^r,$$

ובפרט $H$ היא חבורת-$p$. ■

**הוכחת המשפט:** לפי למה א׳, $|\Sigma|$ זר ל-$p$, ולכן בפעולת $G$ על $\Sigma$ יש בהכרח מסלול מסוים $O(S)$ מסדר זר ל-$p$. לפי למה ב׳, המייצב של אותה $S$ הוא חבורת-$p$. ממשפט מסלול-מייצב (2.21) נובע כעת כי

$$p^r \cdot m = |G| = \underbrace{|G_S|}_{p\text{ חזקת}} \cdot \underbrace{|O(S)|}_{p\text{-זר ל}},$$

ומכאן, בהכרח, $|G_S| = p^r$. ■

### משפט 5.13 (המשפט ה-II של סילו)

1. תהי $P \in Syl_p(G)$ חבורת $p$-סילו של $G$, ותהי $K \leq G$ תת-חבורה כלשהי. אזי יש $a \in G$ כך ש-

$$aPa^{-1} \cap K$$

היא חבורת $p$-סילו של $K$.

2. כל חבורות $p$-סילו ב-$G$ צמודות זו לזו.

לפני שנפנה להוכחת המשפט, הנה שתי מסקנות חשובות הנובעות ממשפט זה:

**מסקנה 5.14** כל תת-חבורה של $G$ שהיא חבורת-$p$, מוכלת בחבורת $p$-סילו.

**הוכחה:** תהי $G \le K$ כך ש-$K$ חבורת-$p$. בפרט, $K$ היא חבורת $p$-סילו של עצמה (היחידה, כמובן). לפי המשפט ה-II של סילו, אם $P \in Syl_p(G)$, קיים $a \in G$ כך ש-$(aPa^{-1} \cap K)$ היא חבורת $p$-סילו של $K$, ובמקרה זה מקבלים

$$aPa^{-1} \cap K = K,$$

כלומר $K \le aPa^{-1}$, והרי $aPa^{-1}$ גם היא תת-חבורה של $G$ וגודלה זהה לזה של $P$, ועל כן גם היא חבורת $p$-סילו של $G$. ■

**מסקנה 5.15** תהי $P \in Syl_p(G)$ חבורת $p$-סילו של $G$. אזי

$$Syl_p(G) = \{P\} \iff P \trianglelefteq G.$$

**תרגיל 5.16** הוכיחו את מסקנה 5.15 בהינתן המשפט ה-II של סילו (שימו לב שיש צורך להסתמך על משפט זה רק באחד משני הכיוונים).

**הוכחת המשפט ה-II של סילו:** ראשית, $(2)$ נובע מ-$(1)$ משום שאם $P_1, P_2 \in Syl_p(G)$, אזי לפי $(1)$ קיים $a \in G$ כך ש-$aP_1a^{-1} \cap P_2$ זו חבורת $p$-סילו של $P_2$, שהיא במקרה זה בדיוק $P_2$ עצמה. כלומר, $aP_1a^{-1} \cap P_2 = P_2$, או

$$P_2 \subseteq aP_1a^{-1},$$

ומשיקולי סדר יש שוויון: $P_2 = aP_1a^{-1}$.

נותר להוכיח את $(1)$. הפעם נסתכל על קבוצת המחלקות השמאליות $G/P$ ועל פעולת $K$ על קבוצה זו על ידי כפל משמאל:

$$\forall k \in K,\, g \in G, \qquad k.(gP) = (kg)P$$

(ודאו כי זו אמנם פעולה חוקית). המייצב של $aP$ הוא

$$\{k \in K \mid kaP = aP\} = \left\{k \in K \,\middle|\, a^{-1}ka \in P\right\} = \left\{k \in K \,\middle|\, k \in aPa^{-1}\right\} = K \cap aPa^{-1}.$$

כזכור, גודל הקבוצה $|G/P| = m$ זר ל-$p$, ולכן קיים $a \in G$ כך שהמסלול $O(aP)$ גודלו זר ל-$p$. אזי, לפי משפט מסלול-מייצב,

$$\left[K : K \cap aPa^{-1}\right] = |O(aP)|$$

זר ל-$p$. מאידך, $aPa^{-1}$ חבורת-$p$ ולכן תת-החבורה שלה $K \cap aPa^{-1}$ גם היא חבורת-$p$. תת-חבורה של $K$ שהיא חבורת-$p$ מאינדקס זר ל-$p$ היא בהכרח חבורת $p$-סילו של $K$. ■

**משפט 5.17 (המשפט ה-III של סילו)** תהי $G$ חבורה סופית מסדר $p^r \cdot m$ עם $p \nmid m$. נסמן ב-$k_p = \left|Syl_p(G)\right|$ את מספר חבורות $p$-סילו של $G$. אזי

1. $k_p \mid m$
2. $k_p \equiv 1 \bmod p$

**הוכחה:** נמספר את חבורות $p$-סילו של $G$ כך:

$$Syl_p\left(G\right) = \{P_1, P_2, \ldots, P_k\}$$

($k = k_p$). בפרט, $G$ פועלת על $Syl_p\left(G\right)$ על-ידי הצמדה, ולפי המשפט ה-II של סילו, פעולה זו טרנזיטיבית (כלומר, בעלת מסלול יחיד — ראו הגדרה 2.12). המייצב של $P_1$ הוא המשמר $N_G\left(P_1\right)$ (ראו[6] סעיף 2.3), ולפי משפט מסלול-מייצב (משפט 2.21):

$$.k = \left|O\left(P_1\right)\right| = \left[G\,:\,N_G\left(P_1\right)\right]$$

אבל מתקיים $P_1 \leq N_G\left(P_1\right)$ ולכן,

$$.k_p = k = \left[G\,:\,N_G\left(P_1\right)\right] = \frac{|G|}{\left|N_G\left(P_1\right)\right|} \mid \frac{|G|}{|P_1|} = \left[G\,:\,P_1\right] = m$$

כדי להוכיח את $(2)$, נתמקד בצמצום של פעולה זו לפעולת $P_1$ על $Syl_p\left(G\right)$ (כמובן, על-ידי הצמדה). מכיוון ש-$P_1$ חבורת-$p$, כל המסלולים הם או בגודל $1$ (נקודות שבת) או בגודל שמתחלק ב-$p$ (לפי משפט מסלול-מייצב). נראה כי רק $P_1$ עצמה היא נקודת שבת, ולכן

$$k_p \equiv 1 \bmod p$$

כדרוש. ברור כי אכן $P_1$ היא נקודת שבת של הפעולה. מאידך, אם $P_j$ היא נקודת שבת של פעולת $P_1$, פירושו של דבר ש-$P_j g P_j g^{-1} = P_j$ לכל $g \in P_1$, ובפרט $P_1 \cdot P_j = P_j \cdot P_1$. לפי תרגיל 3.26, אם עבור $H, K \leq G$ מתקיים $HK = KH$, הרי ש-$HK$ היא תת-חבורה של $G$. לפיכך, $P_1 \cdot P_j$ היא תת-חבורה של $G$. הסדר של תת-חבורה זו הוא

$$\frac{|P_1| \cdot |P_j|}{|P_1 \cap P_j|}$$

(ראו תרגיל 3.37), ועל כן זו חבורת-$p$. אבל $P_1 \leq P_1 \cdot P_j$, ו-$P_1$ היא חבורת-$p$ מקסימלית בתוך $G$, ולכן $P_1 = P_1 \cdot P_j$, כלומר $P_j = P_1$. בכך הראנו כי אמנם נקודת השבת היחידה של פעולת $P_1$ על $Syl_p\left(G\right)$ היא $P_1$ עצמה. ■

שימו לב שבהוכחה הראנו בפרט כי:

**מסקנה 5.18** בסימון $k_p = \left|Syl_p\left(G\right)\right|$ מתקיים $k_p = \left[G\colon N_G\left(P\right)\right]$ בעבור כל חבורת $p$-סילו $P \in Syl_p\left(G\right)$.

**תרגיל 5.19** 1. הראו כי קיימים שיכונים (מונומורפיזמים) $S_n \hookrightarrow S_{n+1}$ וכן $S_n \hookrightarrow A_{n+2}$.

2. מצאו חבורות 2-סילו ב-$A_4, S_4, A_5, S_5, A_6$. מהו טיפוס האיזומורפיזם של כל אחת מהן?
רמזים: העזרו בסעיף הקודם; בעבור $S_4$, חשבו על סימטריות של ריבוע.

**תרגיל 5.20**

1. בעבור $p$ ראשוני כלשהו, מצאו חבורת $p$-סילו ב-$S_n$ בעבור $n = 1, \ldots, p^2 - 1$, והוכיחו כי היא איזומורפית ל-$\underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{k\ \text{פעמים}}$ כאשר $k$ הוא המספר השלם הגדול ביותר כך ש-$kp \leq n$.

[6] למעשה, $Syl_p\left(G\right)$ הוא אחד המסלולים בפעולת $G$ על קבוצת כל תת-החבורות שלה על-ידי הצמדה.

2. בעבור $p$ ראשוני כלשהו, מצאו חבורת $p$-סילו ב-$S_{p^2}$. (שימו לב כי חזקת $p$ המקסימלית שמחלקת את $(p^2)!$ היא $p+1$).

**תרגיל 5.21** כזכור, בעבור $p$ ראשוני, $\mathbb{F}_p$ מסמן את השדה בן $p$ האיברים $\{0,1,\ldots,p-1\}$ עם פעולות החיבור והכפל מודולו $p$.

1. מצאו את הסדר של החבורה $\mathrm{GL}_n(\mathbb{F}_p)$ (את החבורה $\mathrm{GL}_n(F)$ פגשנו כבר בסעיף 1.1.3).
2. נסמן $G=\mathrm{GL}_3(\mathbb{F}_p)$ ו-$P=\left\{\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}\middle| x,y,z\in\mathbb{F}_p\right\}$. הוכיחו כי $P\leq G$ וכי $P$ היא חבורת $p$-סילו של $G$. $P$ נקראת **חבורת הייזנברג מודולו** $p$.
3. מצאו את המרכז $Z(P)$ והראו שהוא איזומורפי ל-$\mathbb{Z}_p$. הסיקו שקיימת חבורה לא אבלית מסדר $p^3$.
4. מצאו חבורת $p$-סילו של $\mathrm{GL}_n(\mathbb{F}_p)$ ($n$ כללי).

**תרגיל 5.22** בתרגיל זה נספק הוכחה חלופית למשפט ה-I של סילו בהינתן המשפט ה-II (על כן, אין להסתמך כאן על משפט 5.10).
יהיו $p$ ראשוני ו-$G$ חבורה סופית כלשהי.

1. הראו ש-$G$ ניתנת לשיכון ב-$\mathrm{GL}_n(\mathbb{F}_p)$ בעבור $n$ כלשהו.
2. השתמשו בתרגיל הקודם ובמשפט ה-II של סילו כדי להסיק שיש ל-$G$ חבורת $p$-סילו.

### 5.2.1 חבורות $p\cdot q$

משפטי סילו הם משפטים רבי-עוצמה בכל שקשור לניתוח של חבורות סופיות. כדוגמה לשימוש בהם, נוכיח את התוצאה הבאה על חבורות מסדר $pq$ כאשר $p$ ו-$q$ ראשוניים שונים:

**משפט 5.23** אם $p<q$ ראשוניים ו-

$$q\not\equiv 1 \bmod p$$

אז כל חבורה מסדר $pq$ היא צקלית.

בפרט, פירוש הדבר שבתנאים אלה יש חבורה יחידה מסדר $pq$ עד כי איזומורפיזם. למשל, כל חבורה מסדר 15 היא צקלית (ולכן יש רק חבורה אחת מסדר 15 עד כדי איזומורפיזם).

**הוכחה:** תהי $G$ חבורה מסדר $pq$ ותהיינה $P\in Syl_p(G)$ ו-$Q\in Syl_q(G)$. לפי המשפט ה-III של סילו, $k_p\mid q$ ולכן $k_p=1$ או $k_p=q$. אבל בנוסף, $k_p\equiv 1\,(\mathrm{mod}\,p)$, ונתון ש-$q\not\equiv 1\,(\mathrm{mod}\,p)$, ולפיכך בהכרח $k_p=1$. כלומר, $P\trianglelefteq G$. באופן דומה, $k_q\mid p$ ולכן $k_q=1$ או $k_q=p$, אבל $p<q$ ומתקיים $k_q\equiv 1\,(\mathrm{mod}\,q)$, ועל כן בהכרח $k_q=1$. לפיכך $Q\trianglelefteq G$.
מכיוון ששתי החבורות $P$ ו-$Q$ הן מסדר ראשוני, שתיהן צקליות, ונניח כי

$$Q=\langle b\rangle\,,\quad P=\langle a\rangle.$$

נטען כי האיבר $ab$ יוצר את $G$. ראשית, סדר כל איבר ב-$P$ (פרט ליחידה) הוא $p$, בעוד שסדר כל איבר ב-$Q$ (פרט ליחידה) הוא $q$, ולכן $P\cap Q=\{e\}$. נתבונן באיבר $aba^{-1}b^{-1}$:

$$Q\ni\underbrace{aba^{-1}}_{\in Q}\underbrace{b^{-1}}_{\in Q}=\underbrace{a}_{\in P}\underbrace{ba^{-1}b^{-1}}_{\in P}\in P$$

ולכן
$$,aba^{-1}b^{-1} \in P \cap Q = \{e\}$$
כלומר $ab = ba$ ו-$a, b$ מתחלפים. נניח כי הסדר של האיבר $ab$ הוא $n$. בפרט, $(ab)^n = a^n b^n = e$, ואז
$$.a^n = b^{-n} \in P \cap Q = \{e\}$$
לפיכך בהכרח הן $a^n = e$ ולכן $p \mid n$ והן $b^n = e$ ולכן $q \mid n$. לכן $pq \mid n$, ומכאן $n = pq$, ו-$G = \langle ab \rangle$ היא צקלית. ■

**הערה 5.24** להוכחת המשפט האחרון ניתן היה גם להראות שבעבור $P$ ו-$Q$ כמו בהוכחה, מתקיימים תנאי משפט 3.40 ולפיכך $G \cong P \times Q$. ניתן היה אז לסיים לפי משפט השאריות הסיני (משפט 1.50).

**הערה 5.25** אם בניגוד לתנאי המשפט מתקיים $q \equiv 1 \pmod p$, אזי יש חבורה לא אבלית[7] מסדר $pq$. כבר נתקלנו, למשל, ב-$S_3$, חבורה לא-אבלית מסדר 6. כדוגמה נוספת, נבנה חבורה לא אבלית בגודל 21:
$$G = \left\{ a^i b^j \,\middle|\, 0 \le i < 3,\ 0 \le j < 7 \right\}$$
כאשר מתקיימות הזהויות $a^3 = b^7 = e$ וכן $a^{-1}ba = b^2$. משלוש זהויות אלה ניתן לגזור את כל טבלת הכפל של $G$: ראשית, ניתן לראות באינדוקציה פשוטה על $m$ כי $a^{-m}ba^m = b^{2^m}$, שהרי
$$\begin{aligned} a^{-m}ba^m &= a^{-1}\left(a^{-(m-1)}ba^{m-1}\right)a \\ &= a^{-1}b^{2^{m-1}}a \\ &= \left(a^{-1}ba\right)^{2^{m-1}} \\ &= \left(b^2\right)^{2^{m-1}} \\ &= b^{2^m} \end{aligned}$$
או אז
$$\begin{aligned} \left(a^i b^j\right)\left(a^m b^l\right) &= a^{i+m}\left(a^{-m}b^j a^m\right)b^l \\ &= a^{i+m}\left(a^{-m}ba^m\right)^j b^l \\ &= a^{i+m}b^{j\cdot 2^m}b^l \\ &= a^{[(i+m) \bmod 3]}b^{[(j\cdot 2^m+l) \bmod 7]} \end{aligned}$$
כעת צריך לבדוק שבהגדרה זאת מתקיימות אקסיומות החבורה (אסוציאטיביות, קיום יחידה וקיום הפכי). הנקודה שבה מנוצלת השקילות $(q \equiv 1 \bmod p)$ היא בכך שכאשר מציבים $m = 3$ לעיל, מקבלים
$$a^{-3}ba^3 = b^{2^3} = b^{8 \bmod 7} = b$$
כנדרש, שכן $a^3 = e$.

**תרגיל 5.26** הוכיחו כי יש בדיוק 2 חבורות מסדר 6 (עד כדי איזומורפיזם).

[7] למעשה, לכל חבורה כזו יש מבנה של מכפלה חצי ישרה של חבורת $q$-סילו עם חבורת $p$-סילו (ראו תרגיל 3.44).

# 6 סדרות נורמליות וסדרות הרכב

## 6.1 סדרות הרכב

את מושג החבורה הפשוטה הגדרנו כבר בסעיף 3.4, ונתקלנו עד כה בשתי משפחות של חבורות כאלה: החבורה הצקלית $\mathbb{Z}_p$ לכל $p$ ראשוני, וחבורת התמורות הזוגיות $A_n$ לכל $n \geq 5$. ציינו כבר כי החבורות הפשוטות הן, במובנים רבים, אבני הבניין של החבורות. ניתן לדמות זאת למספרים הראשוניים כאבני הבניין של המספרים הטבעיים, או לאטומים כאבני הבניין של כלל הפרודות (המולקולות). בפרק זה נסביר מעט יותר מה טיבן של החבורות הפשוטות כאבני בניין.

כאמור, בהינתן חבורה $G$ ותת-חבורה נורמלית $N \trianglelefteq G$, ניתן לחשוב על $G$ כאילו היא מורכבת מ-$N$ ומחבורת המנה $G/N$. אם $N$ או $G/N$ אינן פשוטות, ניתן להמשיך ולפרק גם אותן. כך אפשר להמשיך עד אשר כל החבורות שמתקבלות הן פשוטות. תיאור זה של התהליך מעורר מיד שאלות ותהיות: למשל, ייתכן שלחבורה נתונה $G$ יש שתי תת-חבורות נורמליות שונות, וניתן לפרק את $G$ דרך זו או דרך זו. כך, כבר הצעד הראשון של תהליך הפירוק אינו יחיד. האם התוצר הסופי של תהליך הפירוק תלוי בצעדי הפירוק השונים? האם לכל חבורה ולכל תהליך פירוק מגיעים בהכרח בסופו של דבר לגורמים שהם חבורות פשוטות? ואם התהליך אמנם מסתיים, האם נגיע בסופו של דבר לאותן חבורות פשוטות, ללא תלות במהלכים שביצענו בדרך? ולבסוף, נניח שאנו יודעים מהן אבני הבניין שמהן בנויה $G$, האם ניתן לשחזר את $G$ מתוכן? כלומר, האם הפירוק של $G$ הוא ייחודי לה, או שייתכן שישנן חבורות נוספות עם אותו פירוק?

לפני שנענה על השאלות הללו, נציג מונחים שייסייעו לנו לנסח שאלות (ותשובות) בעניינים אלה באופן מעט יותר מדויק:

**הגדרה 6.1** תהי $G$ חבורה.

1. סדרה של תת-חבורות
$$\{e\} = H_0 \leq H_1 \leq \ldots \leq H_r = G \qquad (5)$$
נקראת **סדרה נורמלית**[1] **של** $G$ **מאורך** $r$ אם $H_{i-1} \trianglelefteq H_i$ לכל $1 \leq i \leq r$. סדרה נורמלית
2. סדרה נורמלית נקראת **לא מגמגמת** אם $H_{i-1} \ntrianglelefteq H_i$ לכל $1 \leq i \leq r$.
3. סדרה נורמלית אחרת
$$\{e\} = H'_0 \leq H'_1 \leq \ldots \leq H'_s = G$$
נקראת **עידון** של הסדרה הראשונה (5) אם קיימים $0 = j_0 < j_1 < \ldots < j_r = s$ כך ש-$H_i = H'_{j_i}$ לכל $0 \leq i \leq r$. (כלומר, אם הסדרה השניה נוצרה מהראשונה על-ידי דחיפת עוד חבורות ביניים.) עידון של סדרה נורמלית
4. סדרה נורמלית נקראת **סדרת הרכב** של $G$, או **סדרת ז׳ורדן-הולדר** (Jordan-Hölder), אם המנה $H_i/H_{i-1}$ היא חבורה פשוטה (לא טריוויאלית) לכל $1 \leq i \leq r$. סדרת הרכב
5. בהינתן סדרת הרכב, המנות $H_i/H_{i-1}$ נקראות **גורמי ההרכב**, או **גורמי ז׳ורדן-הולדר** של הסדרה. גורמי הרכב

**הערה 6.2** ראינו (משפט ההתאמה — 3.31) שתת-החבורות מהצורה $N \trianglelefteq H_i/H_{i-1}$ הן בהתאמה חח״ע עם תת-החבורות מהצורה $H_{i-1} \trianglelefteq H \trianglelefteq H_i$ (ההתאמה נתונה על ידי $N \longleftrightarrow H/H_{i-1}$). לפיכך, ניתן

[1] יש ספרים שבהם סדרה כזו מכונה **תת-נורמלית**. את המונח ״סדרה נורמלית״ הם שומרים לסדרה $\{e\} = H_0 \leq H_1 \leq \ldots \leq H_r = G$ שבה $H_i \trianglelefteq G$ לכל $i$. (איזה תנאי חזק יותר?)