

שיעורי בית 3

1. הכרה של עוד חבורות:

(א) הקוטרניונים: נגדיר

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}$$

8 מטריצות מרוכבות. עובדה: קבוצה זאת ביחס למכפלת מטריצות היא חבורה. האם חבורה זאת קומטטיבית?

פתרון: לא חילופית, למשל

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

ואילו

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

(ב) המרוכבים: נגדיר

$$G = \left\{ A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{R}^{2 \times 2} : \det(A) = a^2 + b^2 \neq 0 \right\}$$

הוכיחו כי קבוצה זאת ביחס למכפלת מטריצות היא חבורה. האם חבורה זאת קומטטיבית?

פתרון: מוגדרות

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + ba' \\ -ba' - ab' & -bb' + aa' \end{pmatrix}$$

שזה מהצורה

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

כאשר $x = aa' - bb'$, $y = ab' + ba'$

כעת

$$\det\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\right) = \det\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) \cdot \det\left(\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) \neq 0$$

כמפלה של שני מספרים שונים מאפס.

קיבוציות- נובע מקיבוציות של מכפלת מטריצות

איבר היחידה- $I \in G$ (אם ניקח $a = 1, b = 0$)

הופכי: יהא $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$ אזי מחישוב ישיר נקבל כי

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

שזה מהצורה

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

כאשר $x = \frac{a}{a^2 + b^2}$, $y = \frac{-b}{a^2 + b^2}$ ובנוסף

$$\det\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\right) = \frac{1}{\det\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right)} \neq 0$$

ולכן ההופכי שייך ל G .

בנוסף, החבורה חילופית כי

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + ba' \\ -ba' - ab' & -bb' + aa' \end{pmatrix}$$

ששווה ל

$$\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a'a - b'b & a'b + b'a \\ -b'a - a'b & -b'b + a'a \end{pmatrix}$$

2. תזכורת מש.ב. הקודמים: עבור $\sigma \in S_n$ ומחזור $(i_1, i_2, \dots, i_m) \in S_n$ מתקיים השיויון $\sigma(i_1, i_2, \dots, i_m) \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \dots, \sigma(i_m))$

(א) יהא $n > 2$. הוכיחו כי לכל מחזור $\tau \in S_n$ מאורך לפחות 2 קיימת תמורה $\sigma \in S_n$ כך ש $\sigma\tau \neq \tau\sigma$
פתרון: יהא $\tau = (i_1, i_2, \dots, i_m) \in S_n$ מחזור נתון. נשים לב כי לכל $\sigma \in S_n$ מתקיים $[\sigma\tau\sigma^{-1} = \tau] \iff [\sigma\tau = \tau\sigma]$ ולכן נראה
 קיימת תמורה $\sigma \in S_n$ כך ש $\sigma\tau\sigma^{-1} \neq \tau$.

אם $3 \leq m$ נוכל לכתוב $\tau = (i_1, i_2, i_3, \dots, i_m)$ ואז נגדיר $\sigma = (i_1, i_2)$ ואז $\sigma\tau\sigma^{-1} = (i_2, i_1, i_3, \dots, i_m)$. לפי תזכורת. כעת,
 $\sigma\tau\sigma^{-1}[i_1] = i_3 \neq i_2 = \tau[i_1]$ כי $\sigma\tau\sigma^{-1} \neq \tau$.

אם $m = 2$ אז $\tau = (i_1, i_2)$ ואז נבחר $t \in \{1, \dots, n\} \setminus \{i_1, i_2\}$ (אפשרי כי $n > 2$) ונגדיר $\sigma = (i_1, t)$ ואז $\sigma\tau\sigma^{-1} = (t, i_2)$ לפי
 תזכורת. כעת, $\sigma\tau\sigma^{-1}[i_m] = t \neq i_1 = \tau[i_m]$ כי $\sigma\tau\sigma^{-1} \neq \tau$.

(ב) יהא $n > 2$. הוכיחו כי $Z(S_n) = \{id\}$

פתרון: יהא $\sigma' \in Z(S_n)$ נראה כי $\sigma' = id$. נניח בשלילה כי $\sigma' \neq id$. יהא $\sigma' = \tau_1 \cdots \tau_m$ פירוק שלה למחזורים שונים. אם $m = 1$
 סיימנו לפי סעיף קודם. אחרת $m > 1$ ונוכל לרשום $\sigma' = \tau_1\tau_2 \cdots \tau_m$.

אם קיים $1 \leq i \leq m$ כך ש τ_i מחזור מאורך לפחות 3 אז בה"כ זהו τ_1 (אחרת, נמספרת את המחזורים באינדקסים אחרים) ונוכל לרשום
 $\sigma = (i_1, i_2, i_3, \dots, i_m)$ כמו קודם נגדיר $\sigma = \sigma^{-1}$ ומתחלפת עם המחזורים τ_2, \dots, τ_m (כי הם זרים ל τ_1) ואז

$$\sigma\sigma'\sigma^{-1} = \sigma\tau_1\tau_2 \cdots \tau_m\sigma^{-1} = \sigma\tau_1\sigma^{-1}\tau_2 \cdots \tau_m$$

אם $\sigma\sigma'\sigma^{-1} = \sigma'$ אז נוכל בהכפלה של $(\tau_2 \cdots \tau_m)^{-1}$ נקבל כי $\sigma\tau_1\sigma^{-1} = \tau_1$ סתירה. ולכן $\sigma\sigma'\sigma^{-1} \neq \sigma'$.

במקרה הנוסף: לכל $1 \leq i \leq m$ מתקיים כי τ_i מחזור באורך 2. בפרט $\tau_1 = (x, y), \tau_2 = (z, w)$ עבור x, y, z, w שונים. נגדיר
 $\sigma = (x, z)$ ואז σ מתחלפת עם המחזורים τ_3, \dots, τ_m (כי הם זרים) ואז

$$\sigma\sigma'\sigma^{-1} = \sigma\tau_1\tau_2 \cdots \tau_m\sigma^{-1} = \sigma\tau_1\tau_2\sigma^{-1} \cdots \tau_m$$

אם $\sigma\sigma'\sigma^{-1} = \sigma'$ אז נוכל בהכפלה של $(\tau_3 \cdots \tau_m)^{-1}$ נקבל כי $\sigma\tau_1\tau_2\sigma^{-1} = \tau_1\tau_2$ אבל $\sigma\tau_1\tau_2\sigma^{-1} = (x, z)(x, y)(z, w)(x, z) =$
 $(x, w)(z, y) \neq (x, y)(z, w) = \tau_1\tau_2$. סתירה.

3.

(א) תהא G חבורה ציקלית. הוכיחו כי G קוממטיבית.

פתרון: כיוון ש G ציקלית קיים $g \in G$ כך ש $G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}$. נראה ש G קוממטיבית. אכן, יהיו $a, b \in G$ ונראה כי
 $ab = ba$

כיוון ש $a, b \in G = \langle g \rangle$ קיימים n, m טבעיים כך ש $a = g^n, b = g^m$ ואז

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba$$

כנדרש.

(ב) הוכח כי S_n אינה ציקלית עבור $n > 2$

פתרון: ראינו כי S_n אינה קוממטיבית ולכן אינה ציקלית. לפי סעיף קודם.

4. הגדרה: יהיו $(G_1, \star), (G_2, \circ)$ חבורות אזי גם $G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$ חבורה ביחס לפעולה • המוגדרת • (g_1, g_2)

$$(g_1, g_2) \in G_1 \times G_2 \text{ וההופכי של כל איבר } (e_{G_1}, e_{G_2}) \text{ היחידה היא } (\tilde{g}_1, \tilde{g}_2) = (g_1 \star \tilde{g}_1, g_2 \circ \tilde{g}_2)$$

הוא $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. לחבורה זאת קוראים המכפלה (הקרטיזית) של G_1 ו G_2 . למשל, $\mathbb{Z}_2 \times \mathbb{Z}_3$ שראינו בתירגול.

(א) הוכיחו כי $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה ציקלית עבור $n > 1$

פתרון: נניח בשלילה כי החבורה ציקלית. אזי קיים $g = (m_1, m_2) \in G$ כך ש $\langle g \rangle = G$.

ב G יש n^2 איברים. הסדר של g הוא לכל היותר n כי $g^n = (n \cdot m_1, n \cdot m_2) = (0, 0) = e$ ולכן $|G| = n < n^2 = |\langle g \rangle|$ סתירה.

(ב) יהיו G_1, G_2 חבורות הוכח/הפרך: אם $G_1 \times G_2$ ציקלית אז גם G_2 וגם G_1 ציקלית.

פתרון: נכון. נניח (g_1, g_2) יוצר. אזי - טענה: g_i יוצר של G_i לכל $1 \leq i \leq 2$. נוכיח עבור g_1 : יהא $a \in G_1$ אזי קיים n כך ש

$(g_1^n, g_2^n) = (g_1, g_2)^n = (a, e)$ ולכן $\langle g_1 \rangle \subseteq G_1$. ההכלה השניה תמיד נכונה ולכן קיים שיוויון. באופן דומה $G_2 = \langle g_2 \rangle$.

(ג) יהיו G_1, G_2 חבורות הוכח/הפרך: אם G_1 וגם G_2 ציקליות אז $G_1 \times G_2$ ציקלית.

פתרון: לא נכון. \mathbb{Z}_n ציקלית (1 יוצר) אבל לפי סעיף בשאלה זאת $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה ציקלית

5. הוכח כי החבורות הבאות אינן ציקליות

(א) $\mathbb{Z} \times \mathbb{Z}$

פתרון: נניח כשהיא ציקלית אזי קיים $\langle (a, b) \rangle = \mathbb{Z} \times \mathbb{Z}$ כך ש $\langle (a, b) \rangle = \mathbb{Z} \times \mathbb{Z}$ אזי קיים n שלם כך ש $(1, 0) = n(a, b) = (na, nb)$

ולכן $n = a = \pm 1$ ומנימוק דומה $b = \pm 1$ ולכן לכל n שלם מתקיים

$$n(a, b) = (\pm n, \pm n) \neq (2, 3)$$

(ב) \mathbb{Q}

פתרון: נניח שציקלית. אזי $\langle \frac{a}{b} \rangle = \mathbb{Q}$ עבור a, b שלמים. יהא p ראשוני שאינו מחלק את b אזי $\langle \frac{a}{b} \rangle \notin \frac{1}{p}$. הוכחה: אחרת קיים n כך ש

$\frac{1}{p} = n \frac{a}{b} = \frac{na}{b}$ ולכן $b = nap$ ומכאן ש p מחלק את b . סתירה.

6. ב S_5 מצאו את הסדרים של

(א) $\sigma = (1, 3, 2)$

פתרון: סדר של מחזור הוא האורך שלו ולכן $o(\sigma) = 3$.

(ב) $\sigma = (1, 2)(3, 4, 5)$

פתרון: כיוון ש σ בצורה של מחזורים זרים מתקיים כי

$$\sigma^k = (1, 2)^k (3, 4, 5)^k$$

לכל k טבעי. כל k שהוא כפולה של 2 נקבל כי $(1, 2)^k = id$ ואחרת $(1, 2)$ וכל k שהוא כפולה של 3 נקבל $(3, 4, 5)^k = id$ ואחרת

$(3, 5, 4)$ או $(3, 4, 5)$. ולכן בשביל ש $\sigma^k = id$ צריך להתקיים כי k כפולה של 2 וגם של 3 ולכן הוא כפולה של 6. הכפולה הכי קטנה

של 6 היא 6 בעצמה ולכן $k = 6$ הוא הקטן ביותר המקיים $\sigma^k = id$

(ג) $\sigma = (1, 2)(3, 4, 2)$

פתרון: מתקיים $\sigma = (1, 2)(3, 4, 2) = (1, 2, 3, 4)$

ולכן הסדר הוא 4 (כאורך המחזור)

(ד) באופן כללי: תהא $\sigma \in S_n$ ו $\sigma = \tau_1 \cdots \tau_m$ הפירוק למחזוריים זרים. אזי $o(\sigma) = lcm \{o(\tau_i)_{i=1}^m\}$ (כאשר lcm הוא המכפלה המשותפת

המינימאלית. למשל $lcm\{2, 8, 20, 10\} = 40$

פתרון: נסמן $d = lcm \{o(\tau_i)\}$ אזי $\sigma^d = \tau_1^d \cdots \tau_m^d = id$

. בנוסף, אם $\sigma^k = \tau_1^k \cdots \tau_m^k = id$ אזי לכל i מתקיים $\tau_i^k = id$ (כי המחזוריים זרים) ולכן $o(\tau_i) | k$ ולכן $lcm \{o(\tau_i)\} | k$ בפרט קטן שווה לו.

7. תהא G חבורה סופית. יהיו $a, b \in G$. הוכח/הפרך

(א) אם a, b מתחלפים אז $o(ab) = o(a) \cdot o(b)$

פתרון: לא נכון. ניקח $a = b = 2 \in \mathbb{Z}_4$ אזי $o(ab) = o(0) = 1$ אבל $o(a)o(b) = 2 \cdot 2$

(ב) $\langle a \rangle = \langle a^3 \rangle$

פתרון: לא נכון. ניקח $a = 1 \in \mathbb{Z}_3$ אזי $o(3a) = o(0) = 1$ אבל $o(1) = 3$

(ג) אם $b = a^4$ אזי $\langle ab \rangle \subseteq \langle a \rangle$

פתרון: נכון. יהא $x \in \langle ab \rangle = \langle a^4 \rangle$ אזי $x = (a^4)^n = a^{4n}$ עבור n שלם כלשהו. אזי בפרט x הוא חזקה של a ולכן שייך ל $\langle a \rangle$

(ד) $\langle a \rangle = \langle a^{-1} \rangle$

פתרון: נכון. נראה הכלה בכיוון אחד (הכיוון השני דומה). יהא $x \in \langle a \rangle$ אזי $x = a^n$ עבור n שלם כלשהו. אזי $x = (a^{-1})^{-n}$ ולכן הוא חזקה של a^{-1} ובפרט שייך לחבורה הנוצרת על ידו.

8. תהא G חבורה. $g \in G$. נניח כי $g^k = e$. הוכח כי

$$o(g) | k$$

כלומר הסדר של g מחלק את k .

הדרכה: בצע חילוק עם שארית של k ב $o(g)$

פתרון: נסמן $a = o(g)$ אזי לפי חילוק עם שארית קיימים q, r כך ש $k = qa + r$ ו $0 \leq r < a$

$$e = g^k = g^{qa+r} = (g^a)^q \cdot g^r = e^q \cdot g^r = g^r$$

כיון ש a הוא הסדר של g ו $r < a$ נקבל כי $r = 0$. לכן $k = qa$

9. תהא G חבורה חילופית. יהיו $a, b \in G$ בעלי סדרים זרים. כלומר, נסמן $o(a) = n, o(b) = m$ אזי $\gcd(n, m) = 1$ (ל n, m אין מחלק משותף פרט ל-1). הוכח כי

$$o(ab) = m \cdot n$$

היעזר בתרגיל מספר 8

פתרון: מצד אחד $e = e^m e^n = (a^n)^m (b^m)^n = a^{mn} b^{mn} = (ab)^{mn}$. כעת אם $(ab)^k = a^k b^k = e$. נעלה את שני האגפים בחזקת n ונקבל

$e = (a^k b^k)^n = a^{kn} b^{kn} = b^{km}$ לפי תרגיל 8 $|km|n$ כיוון ש m, n זרים נקבל כי $n | k$ באופן דומה נקבל כי $m | k$. שוב, כיוון שאלו מספר זרים

נקבל כי $mn | k$ ובפרט $mn \leq k$

10. כמה כמה יוצרים יש ל $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ (עם פעולת חיבור מדולו 6)?
פתרון: ברור כי 1 יוצר. לפי 7 $-1 = 5$ גם יוצר. בנוסף כל השאר אינם יוצרים כי $1 \cdot 0 = 3 \cdot 2 = 2 \cdot 3 = 3 \cdot 4 = 0$ ולכן הסדרים שלהם קטנים מ-6.

11. תהא G חבורה ויהא $g \in G$ מסדר n . הוכיחו כי $o(g^k) = \frac{n}{\gcd(k,n)}$
פתרון: מצד אחד

$$(g^k)^{\frac{n}{\gcd(k,n)}} = (g^n)^{\frac{k}{\gcd(k,n)}} = e^{\frac{k}{\gcd(k,n)}} = e$$

ולכן $o(g^k) \leq \frac{n}{\gcd(k,n)}$.
 מצד שני נניח

$$(g^k)^m = e$$

אזי $g^{km} = e$ ומכאן ש $\exists t \text{ } nt = km$ (כי $n|mk$) נחלק את שני האגפים ב $\gcd(k,n)$ ונקבל

$$\frac{n}{\gcd(k,n)}t = \frac{k}{\gcd(k,n)}m$$

מכיוון של $\frac{n}{\gcd(k,n)}, \frac{k}{\gcd(k,n)}$ זרים (אחרת זה סתירה להגדרת gcd) נקבל כי $\frac{n}{\gcd(k,n)} | m$ (כי $\frac{n}{\gcd(k,n)}$ מחלק את $\frac{k}{\gcd(k,n)}m$) בפרט נקבל כי

$$\frac{n}{\gcd(k,n)} \leq m$$