

פתרון שיעורי בית 4

1. הגדרה: יהיו (G_1, \star) , (G_2, \ast) חבורות אזי גם $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$ חבורה ביחס לפעולה • המוגדרת ע"י:

$$(g_1, g_2) \bullet (\tilde{g}_1, \tilde{g}_2) = (g_1 \star \tilde{g}_1, g_2 \ast \tilde{g}_2)$$

היחידה היא (e_{G_1}, e_{G_2}) וההופכי של כל איבר $(g_1, g_2) \in G_1 \times G_2$ הוא: $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. לחבורה זו קוראים המכפלה (הקרטיזית) של G_1 ו G_2 . למשל, $\mathbb{Z}_2 \times \mathbb{Z}_3$ שראינו בתירגול. הוכיחו או הפריכו:

(א) אם $G_1 \times G_2$ ציקלית אז גם G_1, G_2 ציקליות.

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

(ב) אם G_1 וגם G_2 ציקליות אז $G_1 \times G_2$ ציקלית.

פתרון: לא נכון. \mathbb{Z}_n ציקלית (1 יוצר) אבל ראינו בתרגול שהחבורה $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה ציקלית.

2. הוכיחו כי החבורות הבאות אינן ציקליות:

(א) S_n עבור $n > 2$.

פתרון: היא לא אבליית ולכן לא ציקלית.

(ב) \mathbb{Q} .

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

(ג) $\mathbb{Z}_4 \times \mathbb{Z}_6$.

פתרון: נשים לב שזו חבורה עם 24 איברים. לכן מספיק להראות שאין איבר מסדר 24:

יהי $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$ מתקיים: $(a, b)^{12} = (12a, 12b) = (0, 0)$ ולכן $o((a, b)) \leq 12 < 24$.

3. מצאו את הסדרים של האיברים הבאים:

(א) $\sigma = (1, 2)(3, 4, 2) \in S_5$.

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

ולכן הסדר הוא 4 (כאורך המחזור).

(ב) באופן כללי: תהא $\sigma \in S_n$ ויהא $\sigma = \tau_1 \cdots \tau_m$ הפירוק למחזורים זרים. אזי $o(\sigma) = lcm\{o(\tau_i)\}_{i=1}^m$ (כאשר lcm הוא הכפולה המשותפת המינמאלית. למשל $lcm\{2, 8, 20, 10\} = 40$).

פתרון: נסמן $d = lcm\{o(\tau_i)\}$ אזי $\sigma^d = \tau_1^d \cdots \tau_m^d = id$ (כי d מחלק את $o(\tau_i)$ לפי הגדרתו).

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

(ג) $\tau\sigma \in D_4$.

פתרון: נחשב: $(\tau\sigma)^2 = \tau(\sigma\tau)\sigma = \tau(\tau\sigma^{-1})\sigma = id$. לכן $o(\tau\sigma) = 2$ (בחזקת 1 זה עצמו, והוא לא הזהות).

(ד) $\tau\sigma \in D_5$.

פתרון: בדיוק כמו הסעיף הקודם.

(ה) $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ בחבורת הקוטרניונים.

פתרון: נחשב: $k^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$. כיון ש- $(-1)^2 = 1$ נקבל $o(k) = 4$.

4. תהא G חבורה סופית, ויהיו $a, b \in G$. הוכיחו/הפריכו:

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

פתרון: לא נכון. ניקח $a = (1, 2)(3, 4), b = (2, 3) \in S_4$ אזי $o(ab) = o((1, 2, 4, 3)) = 4 = 2 \cdot 2 = o(a) \cdot o(b)$ אבל הם לא מתחלפים: $ab = (1, 2, 4, 3) \neq (1, 3, 4, 2) = ba$

(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 $b = a^4$ אז $\langle b \rangle \subseteq \langle a \rangle$

פתרון: נכון. יהא $x \in \langle b \rangle = \langle a^4 \rangle$ 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 שלמה של a^{-1} , ובפרט שייך לחבורה הנוצרת על ידו.

5. תהא G חבורה. $g \in G$. נניח כי $g^k = e$. הוכיחו כי

$$o(g) | k$$

כלומר הסדר של g מחלק את k .

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

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

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

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

6. 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). הוכיחו כי

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

היעזרו בתרגיל מספר 5.

פתרון: מצד אחד $(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m (b^m)^n = e^m e^n = e$ 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 5 $n|km$, וכיוון ש n, m זרים נקבל כי $n|k$. באופן דומה נקבל כי $m|k$. שוב, כיוון שאלו מספר זרים, נקבל כי $m \cdot n|k$, ובפרט $mn \leq k$.

7. כמה יוצרים יש ל $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ (עם פעולת חיבור מודולו 6)?

פתרון: ברור כי 1 יוצר. לפי דג 5 גם $-1 = 5$ 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.

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

פתרון: מצד אחד

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

$$o(g^k) \leq \frac{n}{\gcd(k, n)}$$

מצד שני נניח

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

צריך להראות: $\frac{n}{\gcd(k, n)} \leq m$. מההנחה נובע ש- $g^{km} = e$, ומכאן ש $\exists t : nt = km$ (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 ש- $\frac{n}{\gcd(k, n)}, \frac{k}{\gcd(k, n)}$ זרים (אחרת זה סתירה להגדרת \gcd) נקבל כי $\frac{n}{\gcd(k, n)} | m$ (כי $\frac{n}{\gcd(k, n)} | m$ מחלק את $\frac{k}{\gcd(k, n)} m$) בפרט נקבל כי

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

9. האם הקבוצות הבאות הן תת חבורות:

(א) $A_n \subseteq S_n$ (כלומר, האם תת קבוצת התמורות הזוגיות היא תת חבורה של חברות התמורות?).

פתרון: נכון. ראשית, $id \in A_n$ כי היא זוגית, אין היפוכי סדר.

בנוסף, צריך להראות שלכל $\sigma_1, \sigma_2 \in A_n$ מתקיים: $\sigma_1 \sigma_2^{-1} \in A_n$. כלומר זוגית. לצורך זה נוכיח ש- $sgn(\sigma^{-1}) = sgn(\sigma)$: נרשום את σ כהרכבת מס' זוגי, m , של חילופים: $\sigma = \tau_1 \dots \tau_m$, לכן $\sigma^{-1} = \tau_m^{-1} \dots \tau_1^{-1} = \tau_m \dots \tau_1$, שזה גם הרכבה של מספר זוגי, m , של חילופים. לכן סימנה $sgn(\sigma) = (-1)^m = 1$ ומכאן, אם $\sigma_1, \sigma_2 \in A_n$ אז $sgn(\sigma_1) = sgn(\sigma_2) = 1$ ולכן $sgn(\sigma_1 \sigma_2^{-1}) = 1 \cdot 1 = 1$

(ב) $\{(i, j) | 1 \leq i < j \leq n\} \cup \{id\} \subseteq S_n$ (כלומר, היחידה ואוסף החילופים).
פתרון: לא נכון עבור $n > 2$, כי אין סגירות: $(1, 2)(2, 3) = (1, 2, 3)$, שזה לא חילוף ולא הזהות.

(ג) $\{0, 2, 4\} \subseteq \mathbb{Z}_5$

פתרון: לא נכון, ל-4 אין הופכי, כי 1 לא נמצא (טוב, זה גם חוסר סגירות, כי זה כמו $4 \cdot 4$).

(ד) $\{0, 3\} \subseteq \mathbb{Z}_6$

פתרון: נכון. כי $3 + 3 \equiv 0 \pmod{6}$, ולכן הוא ההופכי של עצמו, וכל התנאים מתקיימים.

10. תהי G חבורת הקוטרניונים, ותהי $H \leq G$ תת חבורה. הוכיחו: אם $j, k \in H$ אז $H = G$.

פתרון: הוכחה:

נניח $j, k \in H$. נשים לב $j^{-1} = -j, k^{-1} = -k$, ולכן גם הם נמצאים ב- H .

בנוסף, $j^2 = -1, j^4 = 1$, לכן גם $\pm 1 \in H$.

לבסוף, $kj = -i, kj = -i$, ולכן גם $\pm i \in H$. ובסה"כ $H = G$.